УТВЕРЖДЕН

Клиентская операционная система с интегрированными пользовательскими приложениями МСВСфера 9 АРМ

Руководство администратора

версия 1.0

2025

Инв. № подл.	Подпись и дата	Взам. инв №	Инв. № дубл.	Подпись и дата

Оглавление

Аннотация **5**

Общие сведения **6**
Назначение и область применения . . . 6
Обеспечение безопасности . . . 6

Установка и начальная настройка системы **9**
Системные требования . . . 9
Создание загрузочного USB-носителя и запись iso-образа дистрибутива . . . 9
Установка системы с USB-носителя . . . 14

Графический интерфейс средств настройки системы **20**
Настройки даты и времени . . . 20
Управление пользователями . . . 22
Просмотр системных журналов . . . 30
Создание защищённых каналов связи (VPN) . . . 34
Ограничение времени работы за компьютером . . . 45
Подключение к удалённому рабочему столу . . . 56

Настройка оборудования **62**
Управление принтерами . . . 62
Удалённое подключение USB-устройств по сети . . . 66

Управление пакетами **72**
Введение и основные понятия . . . 72
Пакетный менеджер DNF . . . 73
Безопасность . . . 79

Идентификация и аутентификация **80**
Введение . . . 80
Добавление нового пользователя . . . 80
Изменение уже имеющихся пользовательских записей . . . 81
Удаление пользователей . . . 82
Добавление группы пользователей . . . 82
Изменение существующей группы пользователей . . . 83
Удаление существующей группы пользователей . . . 83
Создание и изменение пароля пользователя . . . 83
Изменение срока действия учётной записи и пароля пользователя . . . 85
Управление политиками паролей . . . 85
Получение сведений о пользователе . . . 92
Конфигурационный файл /etc/login.defs . . . 93
Конфигурационный файл /etc/pam.d/system-auth . . . 94
Конфигурационный файл /etc/issue . . . 97
Конфигурационный файл /etc/shadow . . . 98
Запуск программ от имени другого пользователя . . . 98

Управление доступом **109**
Введение . . . 109
Установка и изменение прав доступа к файлам и директориям . . . 109
Назначение и изменение владельца файла и директории . . . 110
Изменение группы-владельца файла или директории . . . 110
Просмотр и изменение списков правил контроля доступа для файлов и директорий . . . 111
Просмотр списков контроля доступа . . . 111
Редактирование пользовательских квот для файловой системы . . . 113
Конфигурационный файл /etc/profile . . . 114
Конфигурационный файл /etc/security/limits.conf . . . 116
Конфигурационный файл /etc/fstab . . . 119

Регистрация событий безопасности **121**
Введение . . . 121
Создание и удаление правил регистрации событий безопасности . . . 121
Добавление правила регистрации событий безопасности . . . 122
Поиск данных регистрации событий безопасности . . . 122
Генерация отчётов по данным регистрации событий безопасности . . . 123
Конфигурационный файл /etc/audit/auditd.conf . . . 124

Ограничение программной среды **125**
Введение . . . 125
Включение программ в автозагрузку . . . 125
Управление системными службами . . . 125
Настройка запуска программ по расписанию . . . 126
Управление программными пакетами . . . 127
Установка последней версии пакета/группы пакетов . . . 128

Стирание данных **129**
Введение . . . 129
Заполнение случайными числами места, занятого файлами . . . 129
Стирание данных в свободном пространстве раздела, в котором находится директория . . . 129
Стирание данных в разделах подкачки . . . 130
Стирание данных в оперативной памяти . . . 130

Контроль целостности **132**
Введение . . . 132
Вычисление и сверка контрольной суммы файла . . . 132
Проверка целостности данных . . . 133

Обеспечение надёжного функционирования **135**
Введение . . . 135
Архивация файлов и директорий . . . 135

Создание архивов и извлечение файлов из них . . . 136
Резервное копирование данных . . . 136
Создание дисковых RAID-массивов . . . 137

Фильтрация сетевого потока **139**
Введение . . . 139
Настройка файрвола (брандмауэра) . . . 139
Конфигурационный файл /etc/firewalld/firewalld.conf . . . 140

Мониторинг функционирования **142**
Введение . . . 142
Анализ системных журналов . . . 142
Получение информации о выполняемых процессах . . . 142
Получение информации о состоянии текущих процессов . . . 143
Мониторинг и анализ сетевого трафика . . . 143
Получение информации о сеансах пользователей . . . 143
Получение информации о последних выполненных командах . . . 144

Создание виртуальной машины **145**
Создание виртуальной машины с помощью утилиты virt-install . . . 145

Панель управления Cockpit **150**
Описание панели управления Cockpit . . . 150
Установка и настройка Cockpit . . . 151
Создание диагностических отчётов . . . 151
Настройка мультитерминального режима . . . 155
Расширение USBGuard для Cockpit . . . 160
Расширение Bootloader для Cockpit . . . 167
Подключение к домену . . . 171
Расширение Aide для Cockpit . . . 174
Расширение LibreOffice для Cockpit . . . 178
Расширение Quota для Cockpit . . . 181
Расширение «Виртуальные терминалы» для Cockpit . . . 185

Аннотация

Настоящее руководство предназначено для администраторов клиентской операционной системы с интегрированными пользовательскими приложениями МСВСфера 9 АРМ. Руководство ориентировано на специалистов, знакомых с операционными системами типа Linux и имеющих минимальный практический опыт работы с ними. Руководство снабжено примерами, сделанными в операционной системе МСВСфера 9 АРМ, установленной в базовой конфигурации.

Общие сведения

Назначение и область применения

МСВСфера 9 АРМ (АРМ — автоматизированное рабочее место) — клиентская операционная система на основе ядра Linux с набором интегрированных пользовательских приложений, включающим пакет офисных программ, браузер, почтовую программу, редакторы текстов и графики, проигрыватели аудио и видео, менеджеры файлов и архивов, программу сканирования документов, множество других программ, а также средства администрирования и защиты информации. МСВСфера 9 АРМ представляет собой комплекс решений, предназначенных для организации и оптимизации работы, обладает высокой степенью гибкости и адаптивности.

В данном руководстве приведён перечень подготовительных процедур, направленных на обеспечение безопасности при внедрении и использовании операционной системы МСВСфера 9 АРМ, дано краткое описание порядка её установки и настойки, а также описание интерфейсов основных средств администрирования и их функциональных возможностей.

МСВСфера 9 АРМ включена в Реестр отечественного ПО, запись №16242 от 30.12.2022.

Обеспечение безопасности

Внедрению и использованию операционной системы должны предшествовать подготовительные процедуры, направленные на обеспечение безопасности при приемке установочного дистрибутива операционной системы от поставщика, на обеспечение безопасной установки, настройки и запуска операционной системы и на создание безопасной среды её функционирования. Реализация подготовительных процедур должна обеспечиваться необходимыми ресурсами и сопровождаться назначением ответственных за их выполнение должностных лиц.

Процедуры безопасной приемки должны предусматривать меры подтверждения подлинности установочного дистрибутива операционной системы, исключающие возможности преднамеренного или непреднамеренного внесения изменений в поставляемую версию, т.е. замены её фальсифицированной или неработоспособной версией. К таким мерам в общем случае относятся:

- проверка подлинности источника поставки путем визуального контроля наличия и целостности специальных защитных стикеров (наклеек, знаков) на упаковке комплекта
- поставки, а также целостности самой упаковки;
- проверка комплектности поставки в соответствии с заявкой, договорными материалами и спецификацией, сверка маркировки и номера версии;
- проверка целостности установочного дистрибутива с помощью программного средства контроля целостности путем сравнения с эталонным значением

контрольной суммы или с помощью средств электронной подписи.

Процедуры безопасной установки, настройки, запуска операционной системы и создания безопасной среды её функционирования в общем случае должны предусматривать меры, обеспечивающие:

- совместимость операционной системы со средствами вычислительной техники, на которых планируется её установка и использование;
- установку, конфигурирование, настройку, запуск и управления операционной системой в соответствии с эксплуатационной документацией и принятой политикой безопасности;
- защиту от действий, направленных на нарушение физической целостности средств вычислительной техники, на которых она функционирует;
- доверенную загрузку операционной системы, контроль доступа к процессу загрузки, блокирование попыток несанкционированной загрузки, контроль целостности компонентов загружаемой операционной среды;
- наличие ресурсов для выполнения функциональных возможностей безопасности операционной системы, хранения создаваемых резервных копий, а также защищенное хранение данных операционной системы и защищаемой информации;
- ограничение на установку программного обеспечения и его компонентов, не задействованных в технологическом процессе обработки информации;
- доверенный маршрут между операционной системой и пользователями;
- доверенный канал передачи данных между операционной системой и средствами вычислительной техники, на которых происходит обработка информации, а также с которых происходит их администрирование;
- невозможность отключения или обхода компонентов операционной системы и средств защиты информации.
- препятствие несанкционированному копированию информации, содержащейся в операционной системе, на съемные носители информации, в том числе контроль вноса (выноса) в (из) контролируемую зону съемных носителей информации;
- проверку целостности получаемых от поставщика внешних модулей уровня ядра перед их установкой в операционную систему;
- выделение вычислительных ресурсов для процессов в соответствии с их приоритетами;
- профессиональную компетентность и надежность персонала, ответственного за администрирование системы, его способность выполнять свои обязанности в точном соответствии с принятой политикой безопасности и эксплуатационной документацией;

- возможность генерации аутентификационной информации, соответствующей заданной метрике качества;
- недоступность аутентификационной информации для лиц, не уполномоченных на ее использование;
- разделение полномочий пользователей и администраторов с назначением им минимально необходимых прав и привилегий;
- исключение в процессе использования системы доступа пользователей к приложениям, выполняющимся с более высокими правами доступа, чем права,
- предоставленные им согласно матрице доступа;
- завершение администраторами приложений, запущенных ими с административными правами после окончания работы с ними;
- запрет пользователям на передачу посторонним лицам своей личной идентификационной и аутентификационной информации, а также на регистрацию кого-либо в системе под своим именем и паролем

Установка и начальная настройка системы

Системные требования

Минимальные

Для использования операционной системы требуется компьютер со следующими минимальными характеристиками:

- Процессор:
  - Intel или AMD версии не ниже x86-64-v2 (Intel Nehalem и более поздние, AMD Bulldozer и более поздние).
  - 64-битной архитектуры от ARM — aarch64 (МСВСфера ОС 9.5 и более поздние версии).
- 2 Гбайта оперативной памяти.
- 20 Гбайт свободного пространства памяти на жёстком диске в зависимости от используемой конфигурации.

Рекомендуемые

Для полнофункционального использования операционной системы рекомендуется использовать компьютер со следующими характеристиками:

- Процессор:
  - Intel или AMD версии не ниже x86-64-v2 (Intel Nehalem и более поздние, AMD Bulldozer и более поздние).
  - 64-битной архитектуры от ARM — aarch64 (МСВСфера ОС 9.5 и более поздние версии).
- 8 Гбайт оперативной памяти.
- 40 Гбайт свободного пространства памяти на жёстком диске в зависимости от используемой конфигурации.

Установка МСВСфера 9 АРМ может осуществляться различными способами: с оптического диска, с жесткого диска, по сети. В данном документе описывается стандартная установка с загрузочного USB-носителя. См. *Установка системы с USB-носителя*.

Создание загрузочного USB-носителя и запись iso-образа дистрибутива

В настоящее время наиболее удобным способом установки операционной системы МСВСфера 9 АРМ является использование USB-носителя с записанным на него дистрибутивом. Ниже мы рассмотрим, как создать загрузочный USB-носитель и записать на него iso-образ дистрибутива.

Программное обеспечение, рекомендуемое для создания загрузочного USB-носителя и записи iso-образа дистрибутива МСВСфера 9 АРМ:

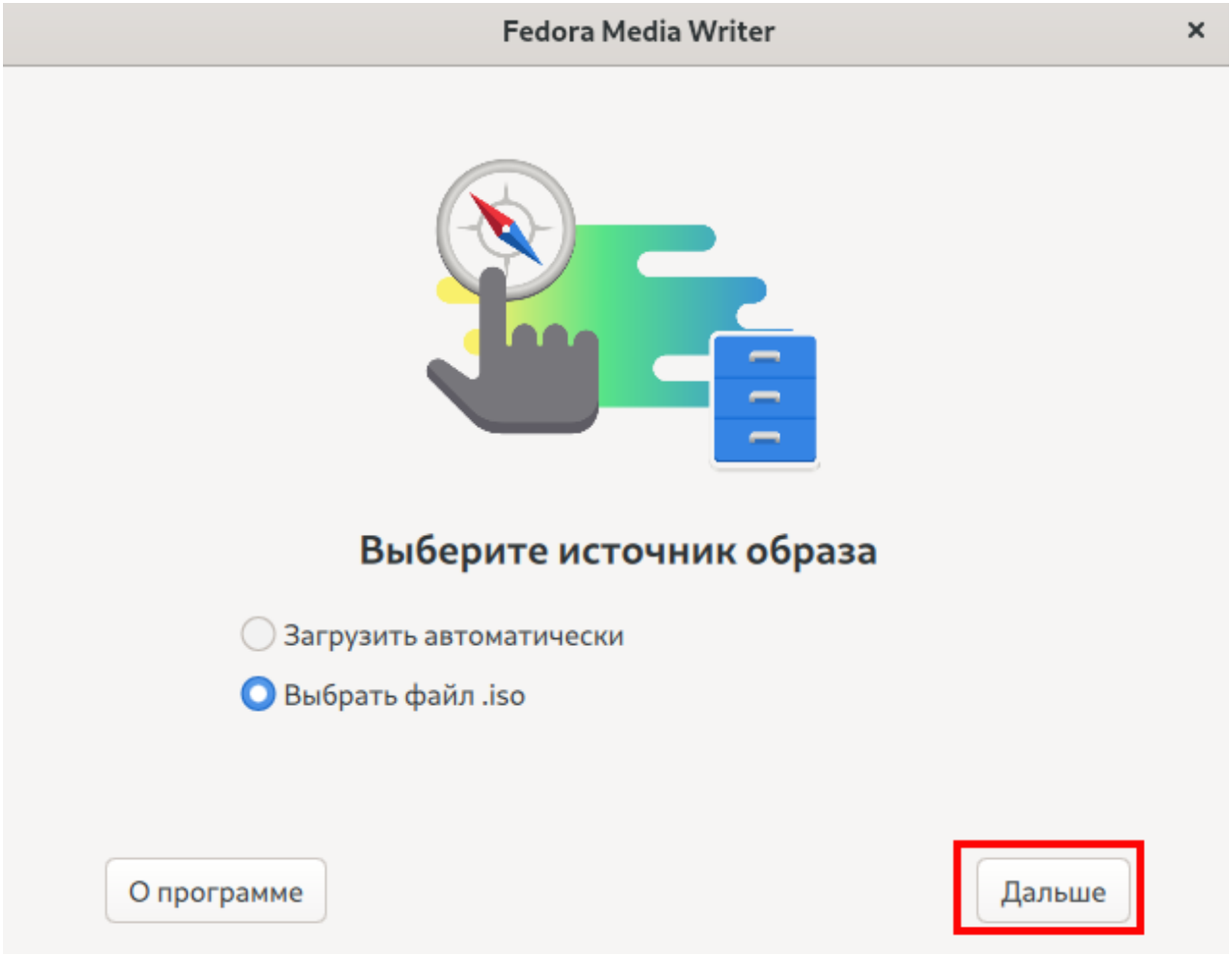
- Fedora Media Writer — для операционных систем семейства Windows, Linux и macOS;
- balenaEtcher — для операционных систем семейства Windows, Linux и macOS;
- Win32 Disk Imager — для операционных систем семейства Windows;
- Утилита командной строки dd — для операционных систем семейства Linux.

Интерфейс указанного программного обеспечения интуитивно понятный, дополнительные инструкции вы можете найти в документации соответствующего ПО.

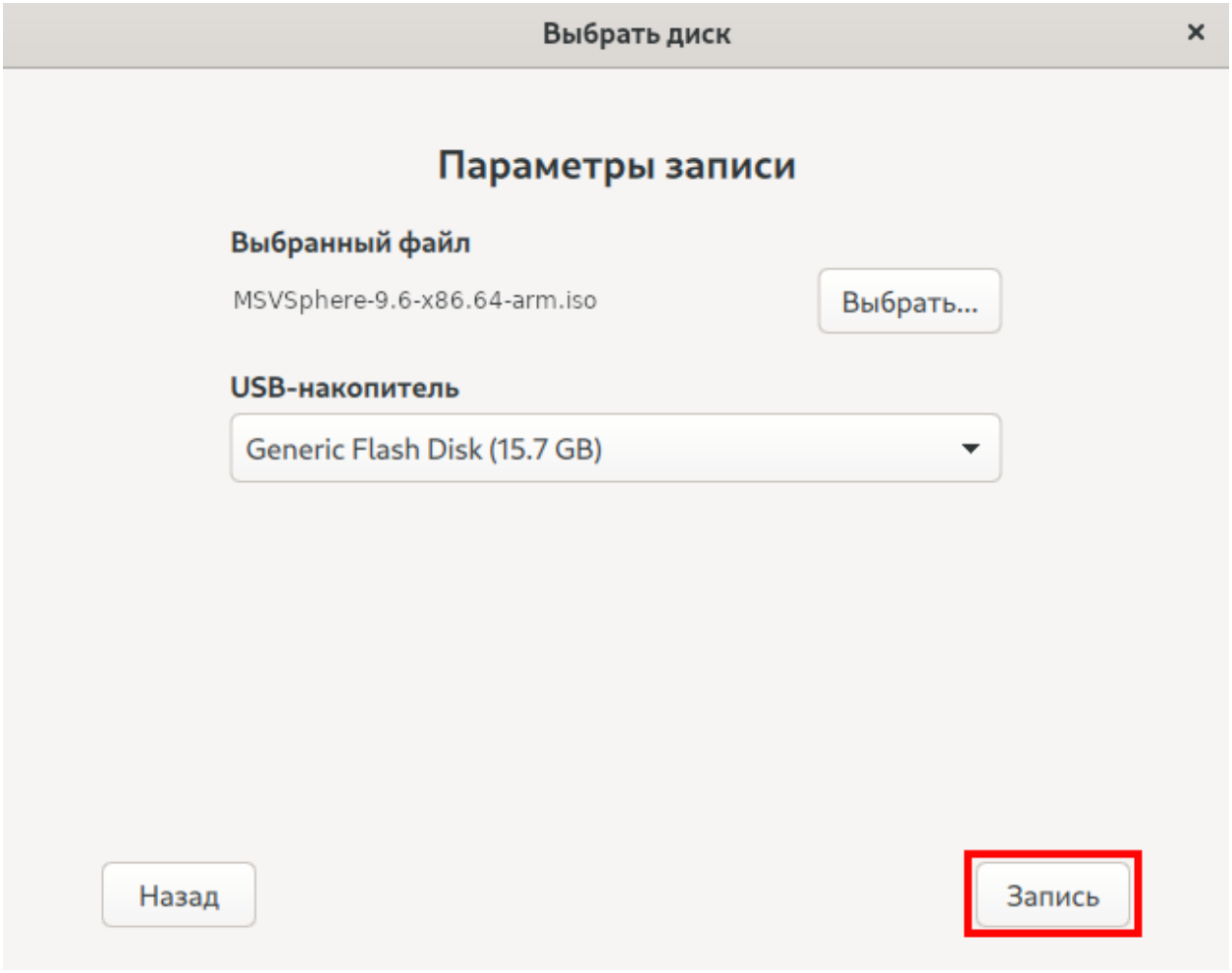
В качестве примера рассмотрим процесс создания загрузочного USB-носителя и записи iso-образа дистрибутива МСВСфера 9 АРМ в программе Fedora Media Writer в операционной системе семейства Windows и с использованием утилиты командной строки `dd` в операционной системе семейства Linux.

Пример создания загрузочного USB-носителя и записи iso-образа дистрибутива МСВСфера 9 АРМ в программе Fedora Media Writer (Windows)

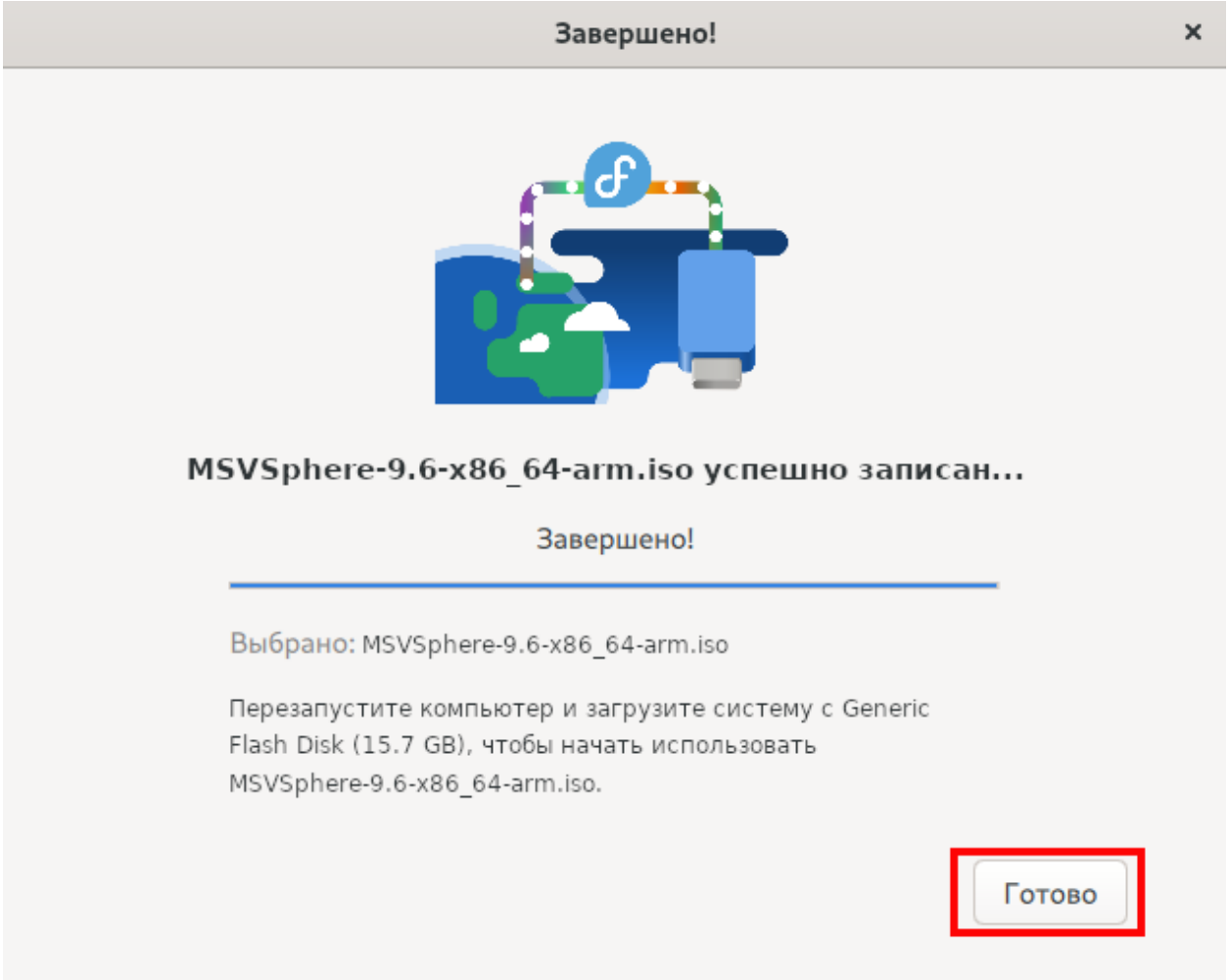
1. Скачайте последнюю версию Fedora Media Writer для Windows на ваше устройство.
2. Запустите установочный файл и выполните установку Fedora Media Writer на ваше устройство.
3. Вставьте USB-носитель, на который вы планируете записывать iso-образ дистрибутива. Убедитесь, что на нём достаточно места.
4. Скачайте актуальный iso-образ МСВСфера 9 АРМ: https://repo1.msvsphere-os.ru/msvsphere/9/isos/x86_64/.
5. Запустите Fedora Media Writer.
6. Выберите источник образа — «Выбрать файл iso» и нажмите «Дальше».



7. В окне «Выбрать диск» → «Параметры записи» → «Выбранный файл» нажмите на кнопку «Выбрать» для выбора iso-образа МСВСфера 9 АРМ, загруженного ранее.
8. USB-накопители определяются автоматически. Если у вас подключено несколько USB-носителей, выберите необходимый из списка.
9. После выбора iso-образа МСВСфера 9 АРМ нажмите «Запись».



10. При необходимости укажите пароль администратора для подтверждения записи.
11. Начнётся запись iso-образа МСВСфера 9 АРМ на USB-носитель. Это может занять некоторое время.
12. После завершения записи нажмите «Готово».



13. Вы успешно создали загрузочный USB-носитель МСВСфера 9 АРМ! Теперь можно приступать к установке системы (см. «usb-setup-server»).

Пример создания загрузочного USB-носителя и записи iso-образа дистрибутива МСВСфера 9 АРМ с помощью утилиты командной строки dd (Linux)

1. Вставьте USB-носитель, на который вы планируете записывать iso-образ дистрибутива. Убедитесь, что на нём достаточно места.
2. Скачайте актуальный iso-образ МСВСфера 9 АРМ: https://repo1.msvsphere-os.ru/msvsphere/9/isos/x86_64/.
3. Откройте «Терминал».
4. Введите команду для записи iso-образа:

```
$ sudo dd oflag=dsync if=MSVSphere-9.3-x86_64-arm.iso of=/dev/sdc bs=1M status=progress;sync
```

При необходимости измените `9.3` на ту версию, которую вы устанавливаете.

Установка системы с USB-носителя

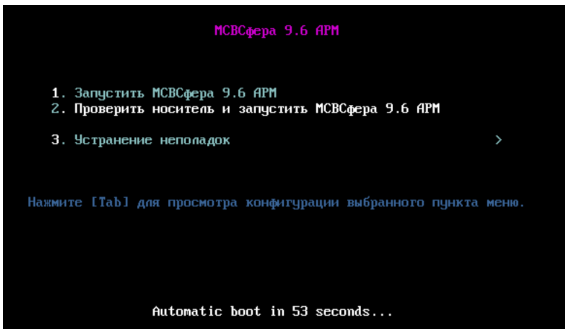
Для установки МСВСфера 9 АРМ с USB-носителя необходимо перед началом установки выбрать приоритетную загрузку с USB-носителя в BIOS устройства, либо выбрать загрузку с USB-носителя однократно в процессе инициализации компьютера.

Для установки и загрузки МСВСфера 9 АРМ может потребоваться отключить параметр Secure Boot в BIOS устройства, на которое производится установка.

Для начала установки подключите USB-носитель с установочным дистрибутивом к компьютеру.

Рассмотрим пример установки МСВСфера 9 АРМ.

Сначала установка будет проходить в текстовом режиме.



Доступны следующие варианты:

- Запустить МСВСфера 9 АРМ — начнётся установка МСВСфера 9 АРМ на ваше устройство.
- Проверить носитель и запустить МСВСфера 9 АРМ — программа установки проверит контрольные суммы образа диска, подтверждая что скачивание образа и запись на загрузочный носитель прошли без ошибок.
- Устранение неполадок — вы сможете перейти в режим восстановления, который представляет собой минимальную среду МСВСфера 9 АРМ, загружаемую с загрузочного носителя. В этом режиме используются утилиты командной строки, с помощью которых вы можете монтировать или не монтировать файловые системы, заносить в чёрный список и добавлять драйверы, устанавливать и обновлять системные пакеты, а также управлять разделами.

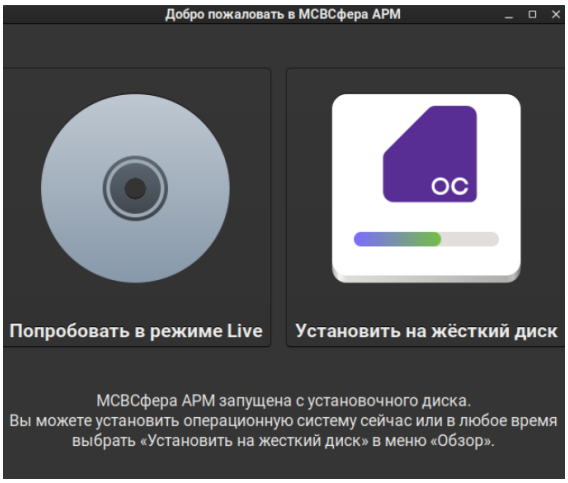
При нажатии на «Запустить МСВСфера 9 АРМ» система будет запущена с установочного диска и готова для работы в режиме Live. В этом режиме вы можете

ознакомиться с функциональными возможностями МСВСфера 9 АРМ без установки системы на жёсткий диск, а также проверить совместимость и корректную работу программного и аппаратного обеспечения.

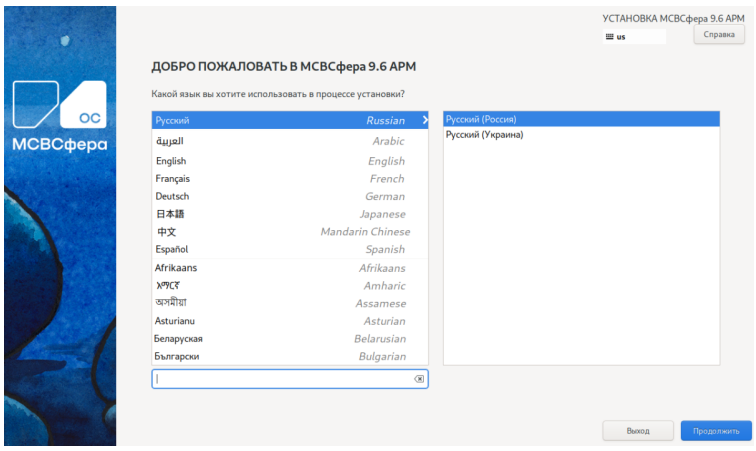
Примечание

Обратите внимание, что все настройки, выполненные в режиме Live, будут потеряны (не сохранятся) после перезагрузки.

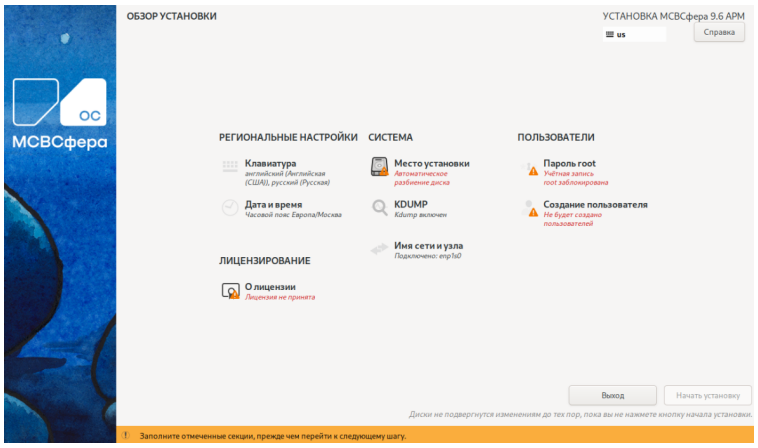
Для полноценной установки МСВСфера 9 АРМ выберите «Установить на жёсткий диск».



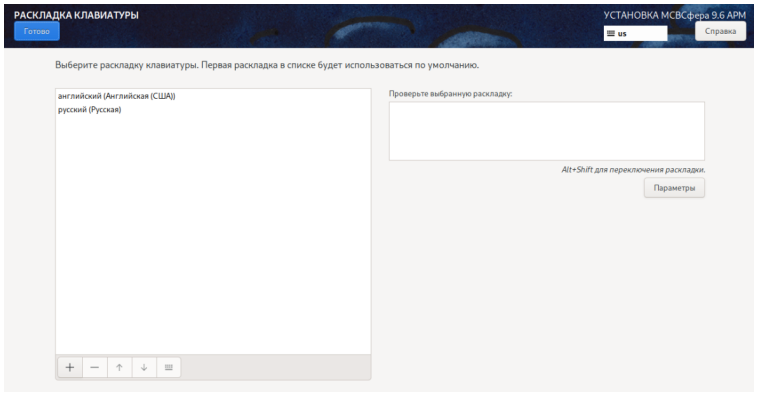
После этого установка продолжится в графическом режиме и на экране монитора компьютера появится окно с предложением выбрать язык установки.



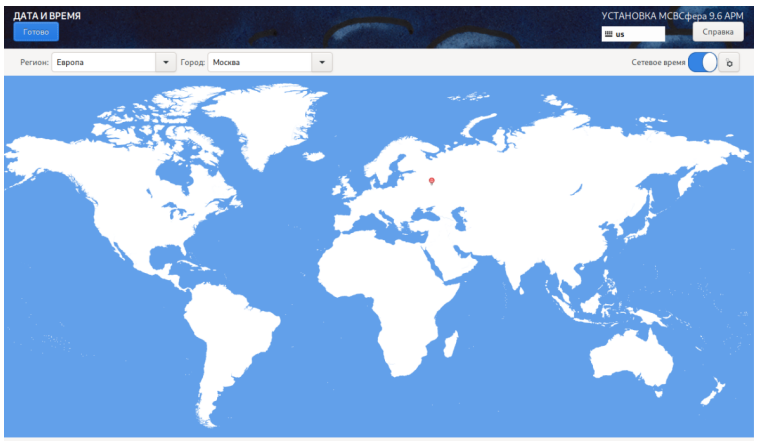
Затем появится окно «Обзор установки», с помощью которого, последовательно нажимая кнопку «Готово», можно будет произвести все необходимые настройки.



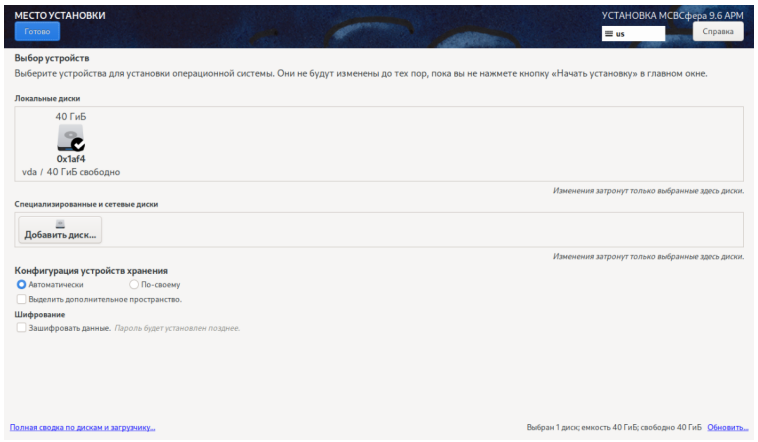
Раскладка клавиатуры.



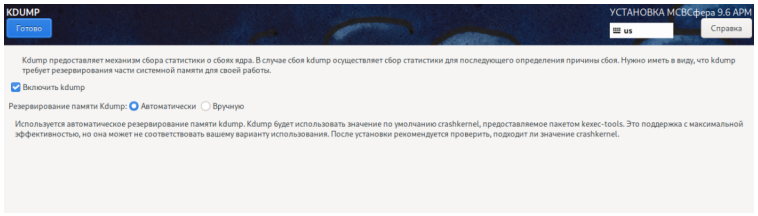
Дата и время.



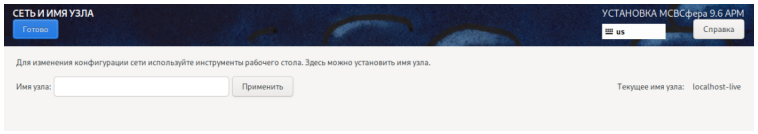
Место установки.



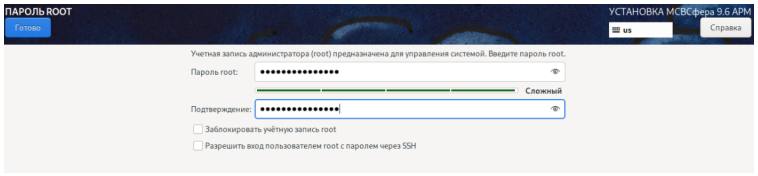
Диагностика сбоев ядра.



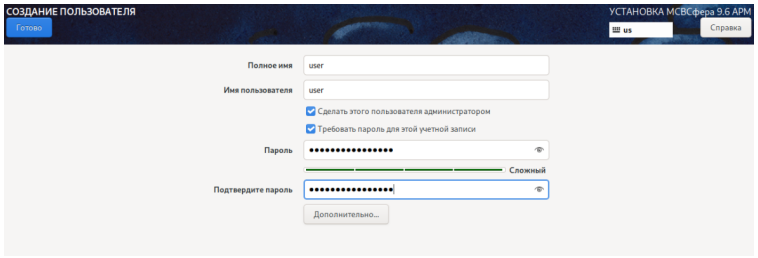
Имя сети и узла.



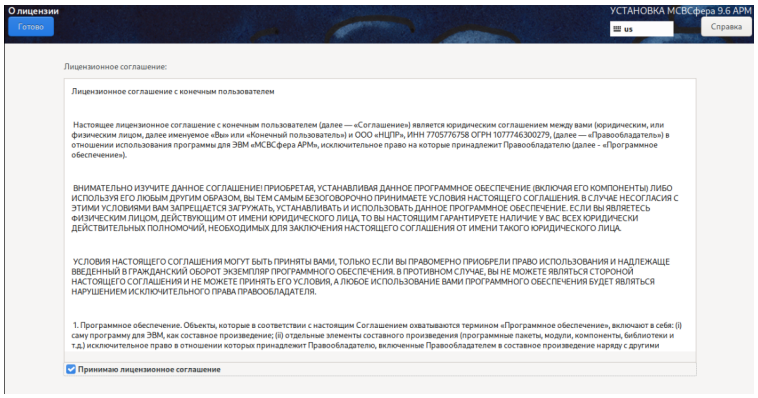
Задать пароль суперпользователя root.



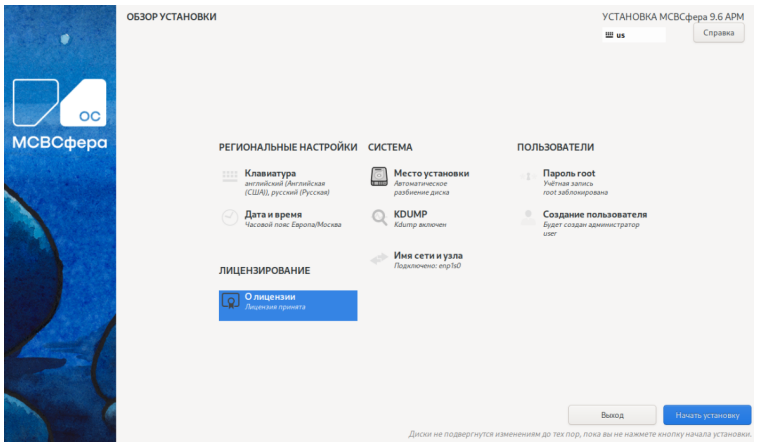
И создать нового пользователя.



Ознакомьтесь с текстом лицензионного соглашения и примите его, поставив галочку.

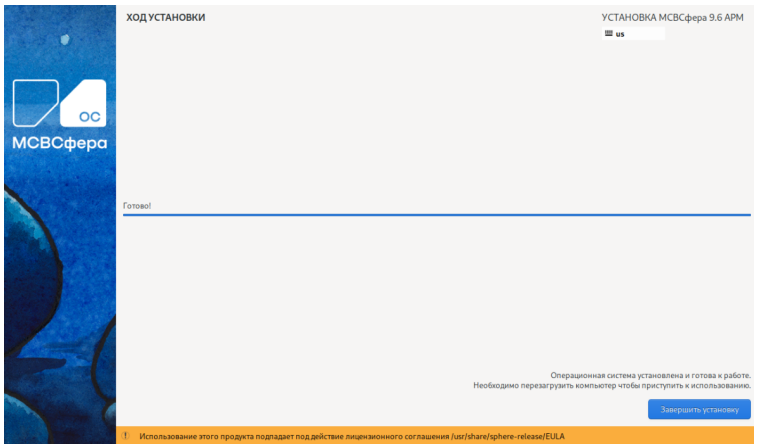


После того, как все необходимые настройки произведены, нажмите на кнопку «Начать установку» и процесс установки начнётся.



Продолжительность установки может составить примерно 20-30 минут, в зависимости от быстродействия оборудования и выбранной конфигурации программного обеспечения.

По завершении установки на экране монитора появится соответствующее уведомление с предложением произвести перезагрузку.



После извлечения USB-носителя с установочным дистрибутивом и перезагрузки системы появится приглашение войти в систему, пройдя идентификацию и аутентификацию.

Графический интерфейс средств настройки системы

Настройки даты и времени

Введение

Настройка даты и времени в графическом интерфейсе МСВСфера ОС производится в приложении «**Настройки**». Перейти в «**Настройки**» вы можете из главного меню, набрав в строке поиска «настройки» и нажав на приложение правой кнопкой мыши, или нажав значок «**Шестерёнки**» в системной панели или в главном меню.

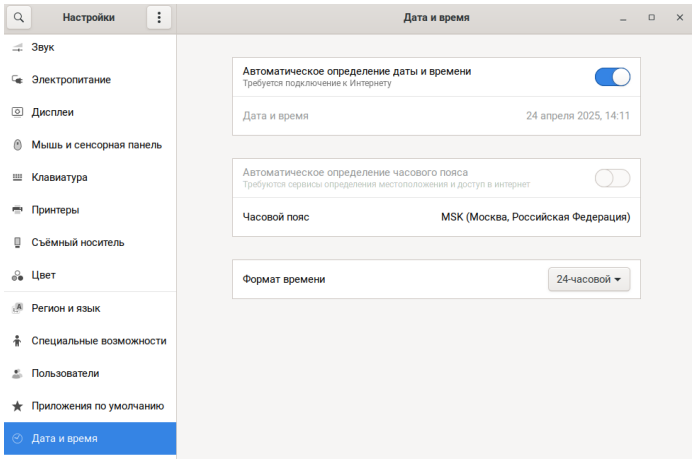
Зачастую настройка даты и времени производится при начальной установке системы (см. «*Установка и начальная настройка системы*»), но вы всегда можете изменить изначально заданную конфигурацию в приложении «**Настройки**».

При изменении настроек даты и времени перезагрузка операционной системы как правило не требуется, все изменения применяются сразу.

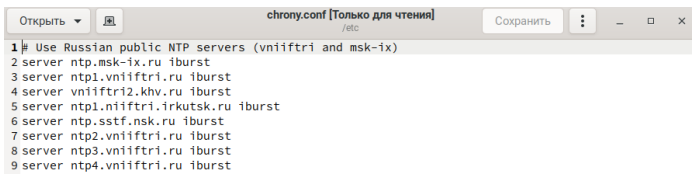
Включение и выключение автоматической синхронизации времени

Откройте приложение «**Настройки**» любым удобным способом и перейдите в раздел «**Дата и время**».

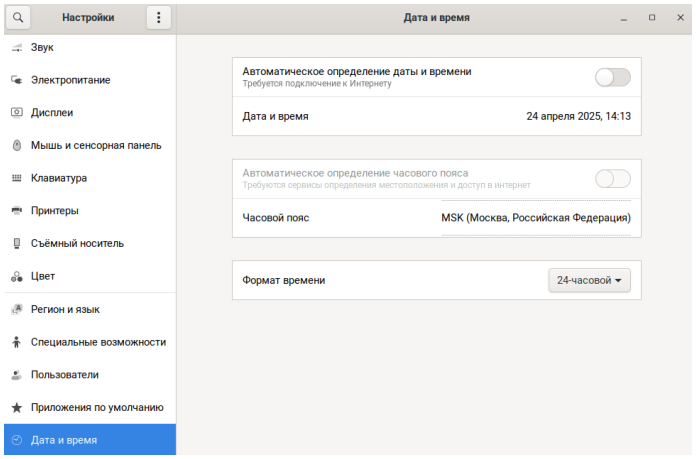
По умолчанию включено автоматическое определение даты и времени.



Для автоматической синхронизации времени используются российские NTP-серверы, список которых вы можете посмотреть в файле `/etc/chrony.conf`.



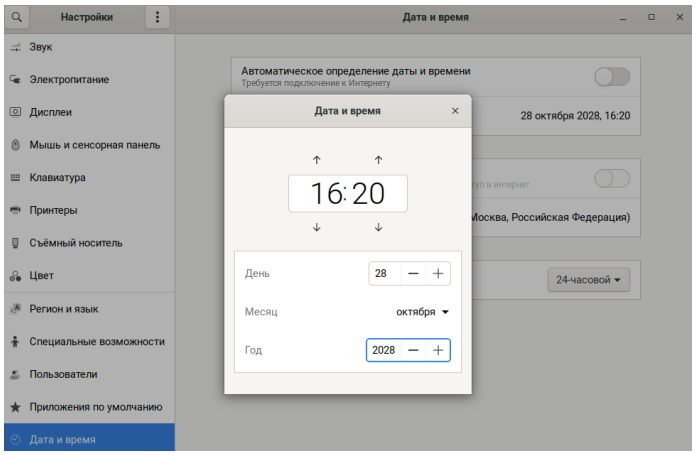
Для отключения автоматического определения даты и времени передвиньте ползунок в неактивное состояние. Вы увидите, что станет активной строка «**Дата и время**»



Установка даты и времени вручную

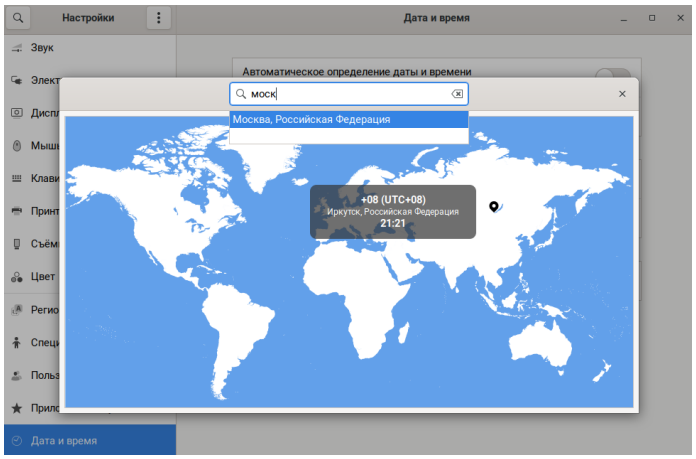
Для установки даты и времени вручную сначала отключите автоматическое определение даты и времени (см. «*Включение и выключение автоматической синхронизации времени*»).

Затем нажмите на строку «**Дата и время**», откроется окно, в котором вы можете задать дату и время вручную.



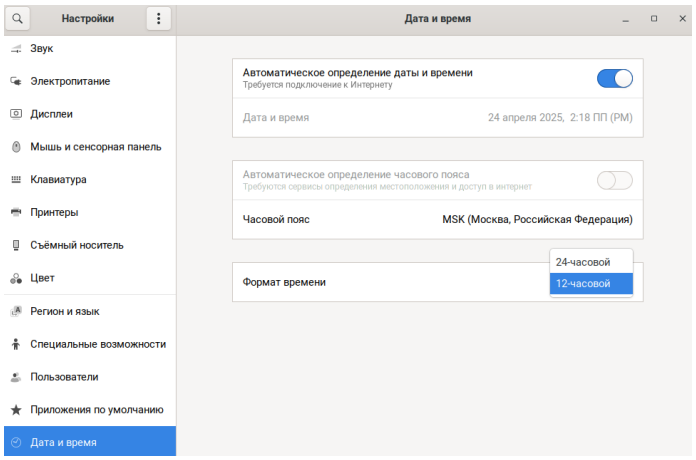
Установка и смена часового пояса

Для установки или смены часового пояса нажмите на строку «**Часовой пояс**», откроется окно, в котором отображается карта с текущим часовым поясом. Начните вводить название города/местности в строке поиска, затем выберите требуемый город из выпадающего списка. Или просто укажите точку на карте. Часовой пояс поменяется на пояс, ассоциированный с выбранным городом/местностью, что отобразится на карте. После завершения настройки закройте окно.



Изменение формата времени

Для изменения формата времени нажмите на выпадающий список в строке «**Формат времени**» и выберите требуемый вид. При 12-часовом формате времени «**ПП (PM)**» значит «после полудня», а «**ДП (AM)**» — до полудня.



Управление пользователями

Введение

Управление пользователями в графическом интерфейсе МСВСфера ОС производится в приложении «**Настройки**». Перейти в «**Настройки**» вы можете из главного меню, набрав в строке поиска «настройки» и нажав на приложение правой кнопкой мыши, или нажав значок «**Шестерёнки**» в системной панели или в главном меню.

Для пользователей, созданных при начальной установке системы (см. «*Установка и начальная настройка системы*»), вы всегда можете изменить изначально заданные параметры в приложении «**Настройки**».

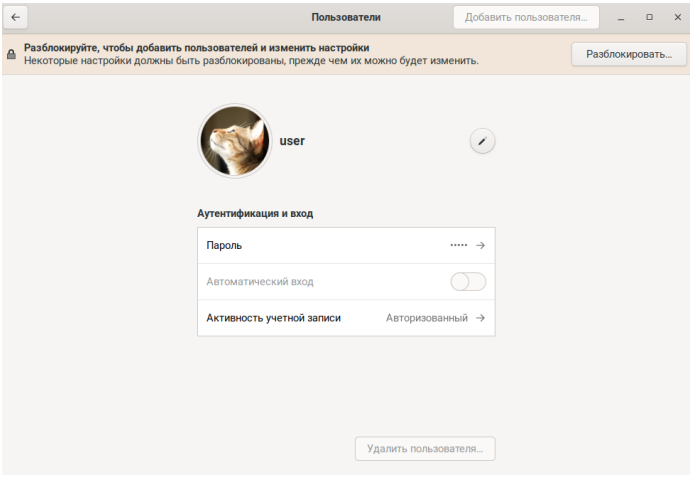
Приложение предоставляет различные функции управления пользователями, включая создание, удаление и изменение учётных записей пользователей, управление паролями, настройку прав доступа, а также администрирование групп пользователей.

Создание пользователя

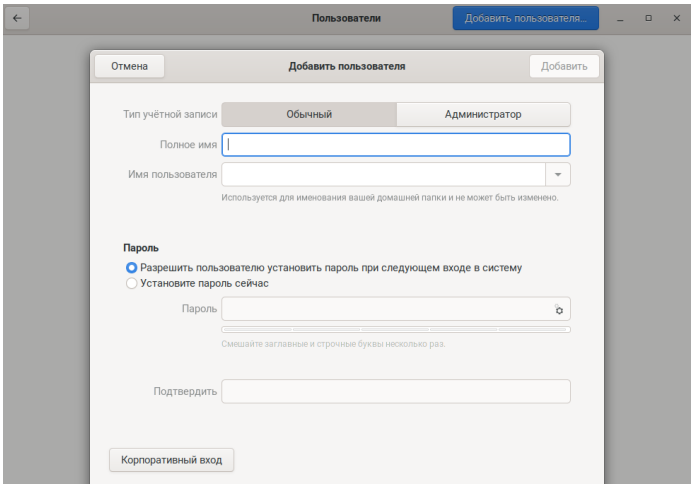
Рассмотрим процедуру создания учётной записи обычного пользователя и администратора.

Откройте приложение «**Настройки**» любым удобным способом и перейдите в раздел «**Пользователи**».

Для любой учётной записи (кроме суперпользователя) при начальном входе некоторые настройки будут заблокированы. Для разблокировки необходимо указать пароль.



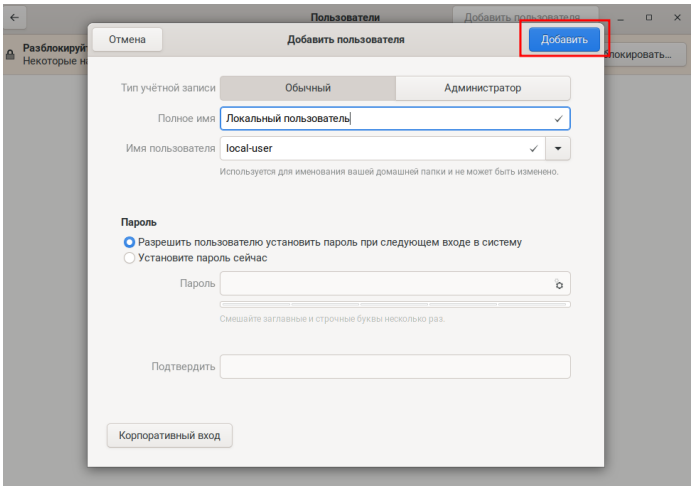
После успешного прохождения аутентификации активируется кнопка «**Добавить пользователя**» в правом верхнем углу окна. Нажмите на неё, откроется окно «**Добавить пользователя**».



Заполните необходимые поля.

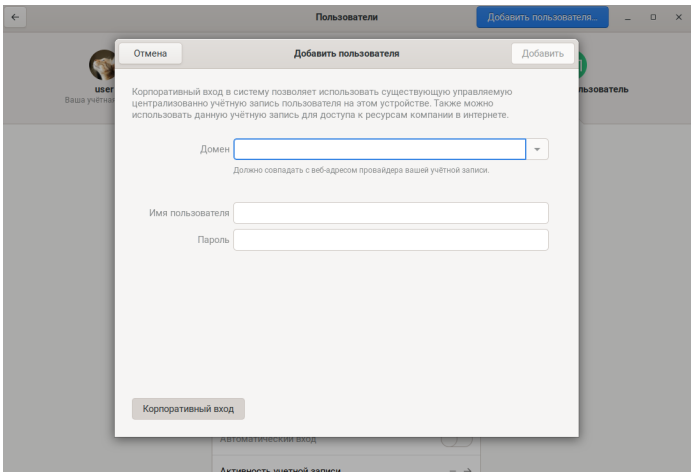
- Тип учётной записи — «Обычный» или «Администратор».
- Полное имя — обычно указывается ФИО или название роли (например, «локальный администратор»).
- Имя пользователя — обычно указывается в английской раскладке и используется для именования домашней папки пользователя. Не может быть изменено. Например, для имени пользователя `user` домашняя папка будет иметь вид `/home/user/`.
- Пароль — выберите, будет ли пароль задан при первом входе в систему или установлен при создании пользователя. При установке пароля во время создания пользователя вы можете воспользоваться функцией автоматической генерации пароля, нажав на значок «**Шестерёнки**».

После успешного заполнения всех полей активируется кнопка «**Добавить**» в правом верхнем углу. Нажмите её для добавления пользователя. По запросу системы снова выполните аутентификацию. Пользователь будет добавлен и сразу отобразится в приложении «**Настройки**» — «**Пользователи**»



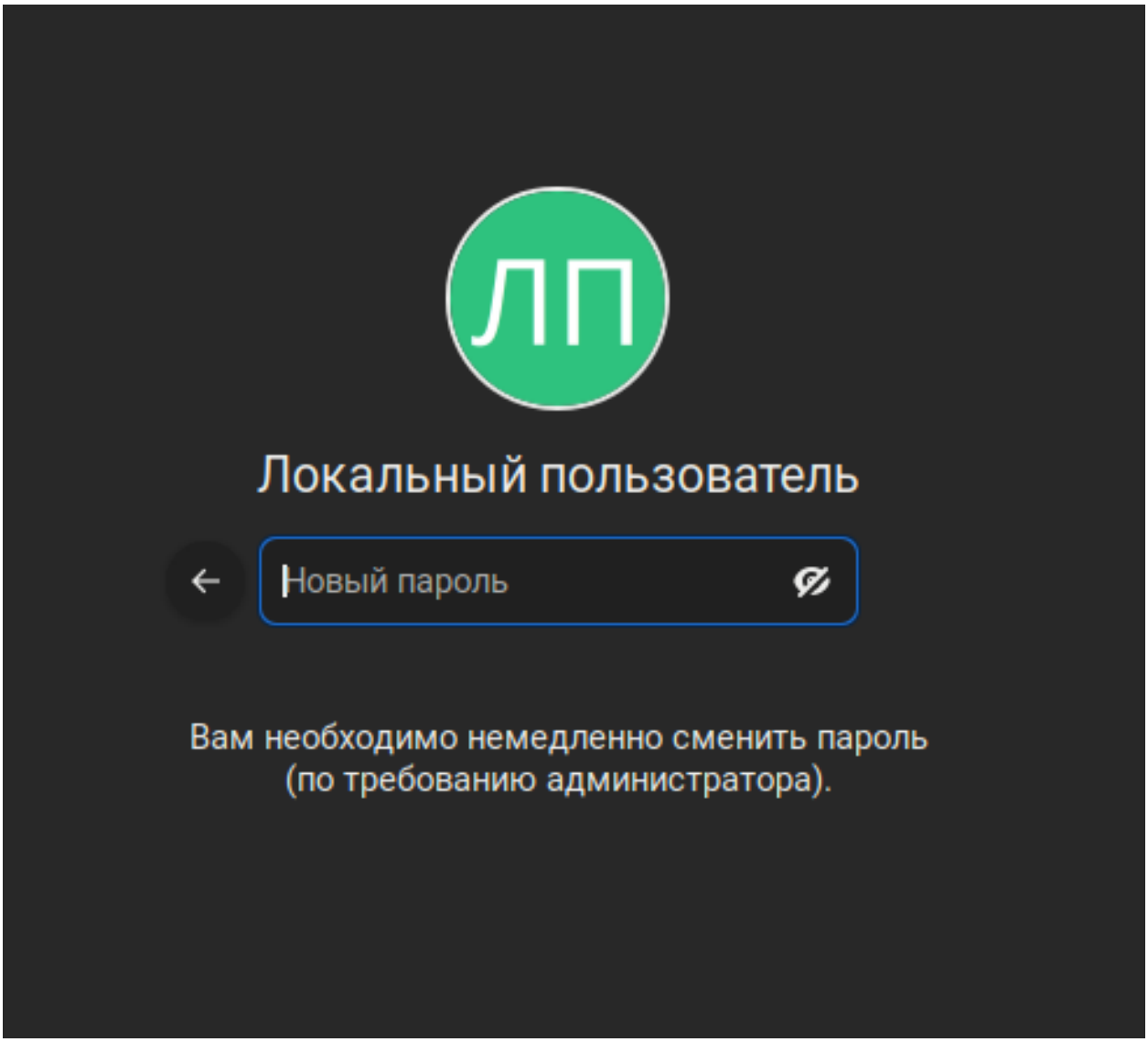
Корпоративный вход

Если в вашей компании используется централизованное управление доступом и учётными записями, то вы можете добавить корпоративную учётную запись пользователя сразу при его создании. Необходимые данные для корпоративного входа обычно могут быть предоставлены администраторами вашей компании.

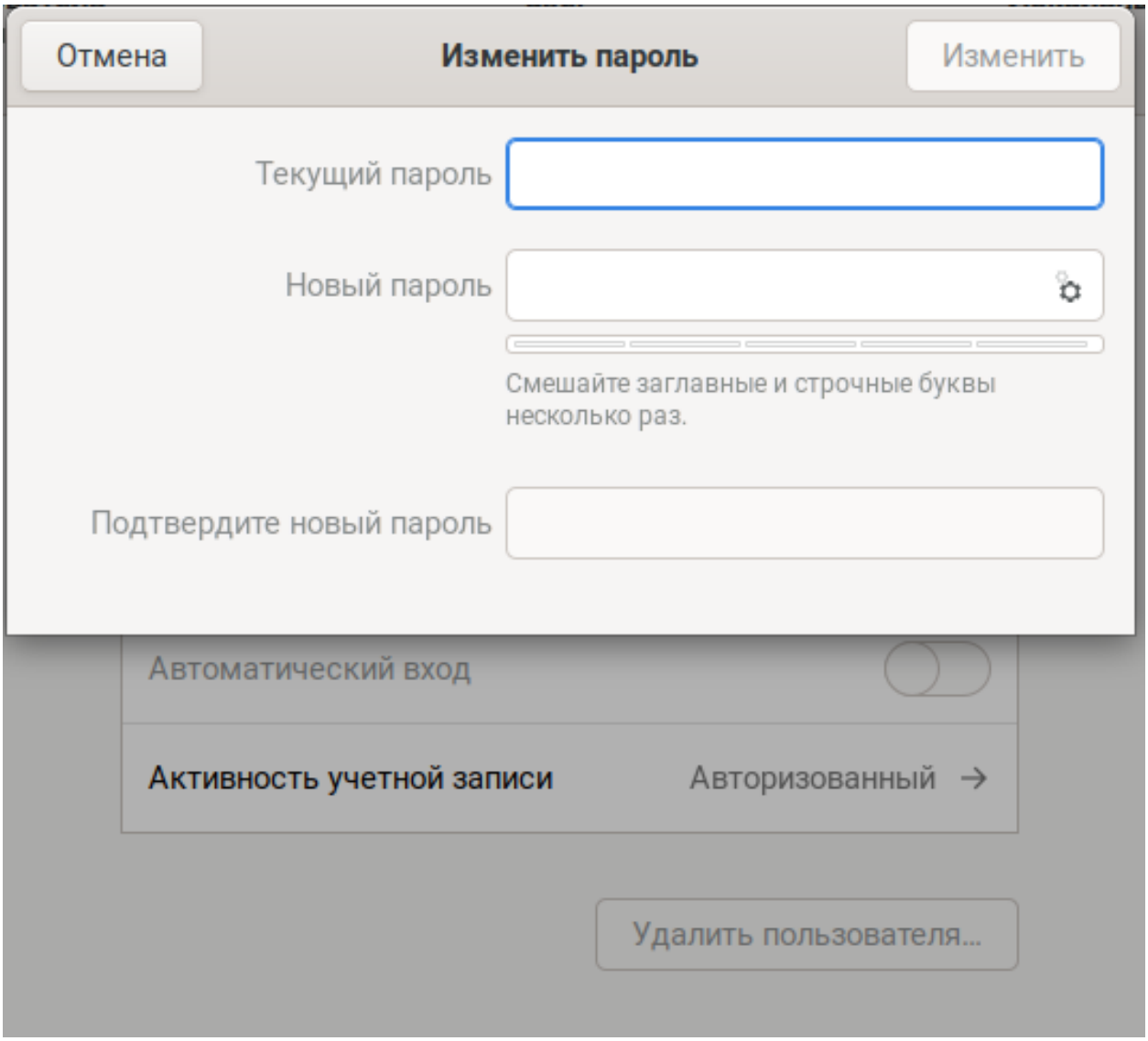


Установка и изменение пароля пользователя

Если при создании учётной записи пользователя было выбрано задание пароля при первом входе в систему, то пользователю будет предложено установить пароль.



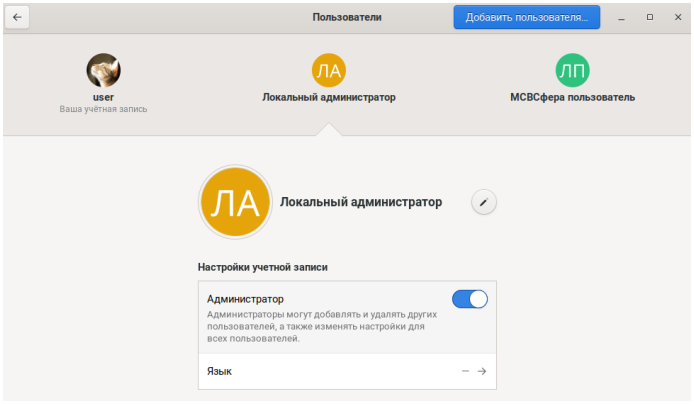
Обычный пользователь всегда может изменить свой пароль в приложении «**Настройки**» — «**Пользователи**» — «**Аутентификация и вход**», строка «**Пароль**». Для изменения пароля потребуется указать текущий пароль. После успешного указания всех требуемых данных, нажмите на кнопку «**Изменить**» в правом верхнем углу.



Администратор может менять как свой пароль, так и пароли обычных пользователей.

Изменение типа учётной записи

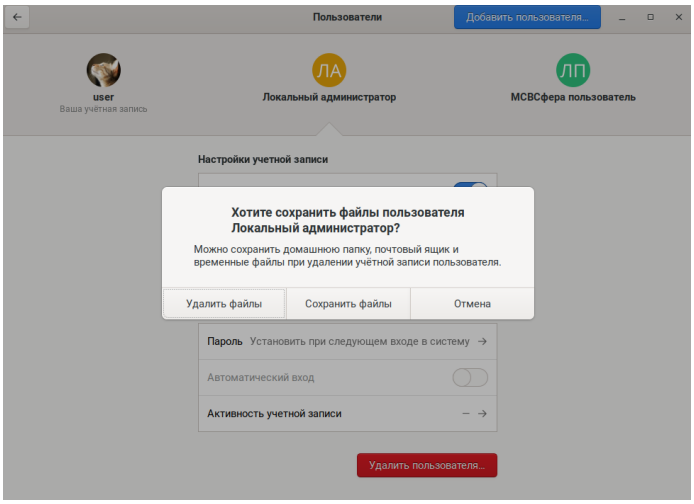
Изменение типа учётной записи доступно только для администратора. Для изменения типа учётной записи перейдите в раздел «**Пользователи**» приложения «**Настройки**» любым удобным способом. Затем передвиньте переключатель в строке «**Администратор**» требуемое положение.



Удаление пользователя

Удаление учётной записи доступно только для администратора, также нельзя удалить учётную запись, если она является единственной на этом устройстве.

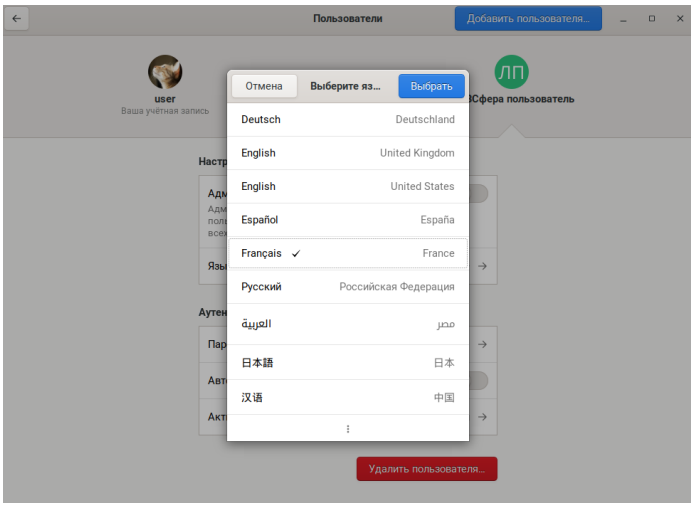
Для удаления учётной записи перейдите в раздел «**Пользователи**» приложения «**Настройки**» любым удобным способом. Затем нажмите на кнопку «**Удалить пользователя**», выберите сохранять ли файлы удаляемого пользователя и подтвердите своё решение.



Изменение языка для пользователя

Изменение языка доступно только для администратора.

Для изменения языка перейдите в раздел «**Пользователи**» приложения «**Настройки**» любым удобным способом. Выберите «**Язык**», откроется окно выбора языка. Выберите необходимый язык и нажмите «**Выбрать**» в правом верхнем углу.

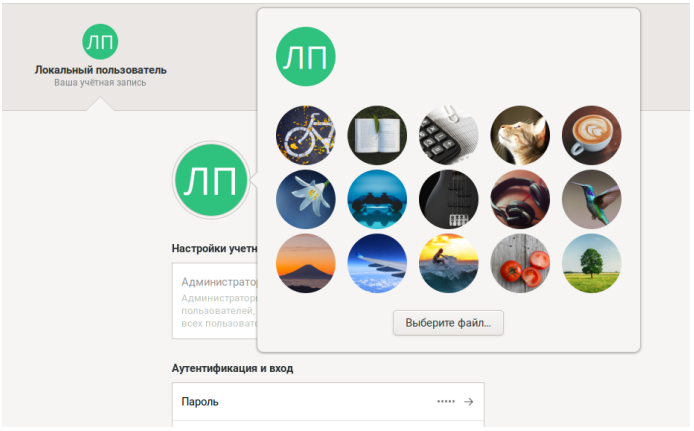


Изменение имени и графического представления для пользователя

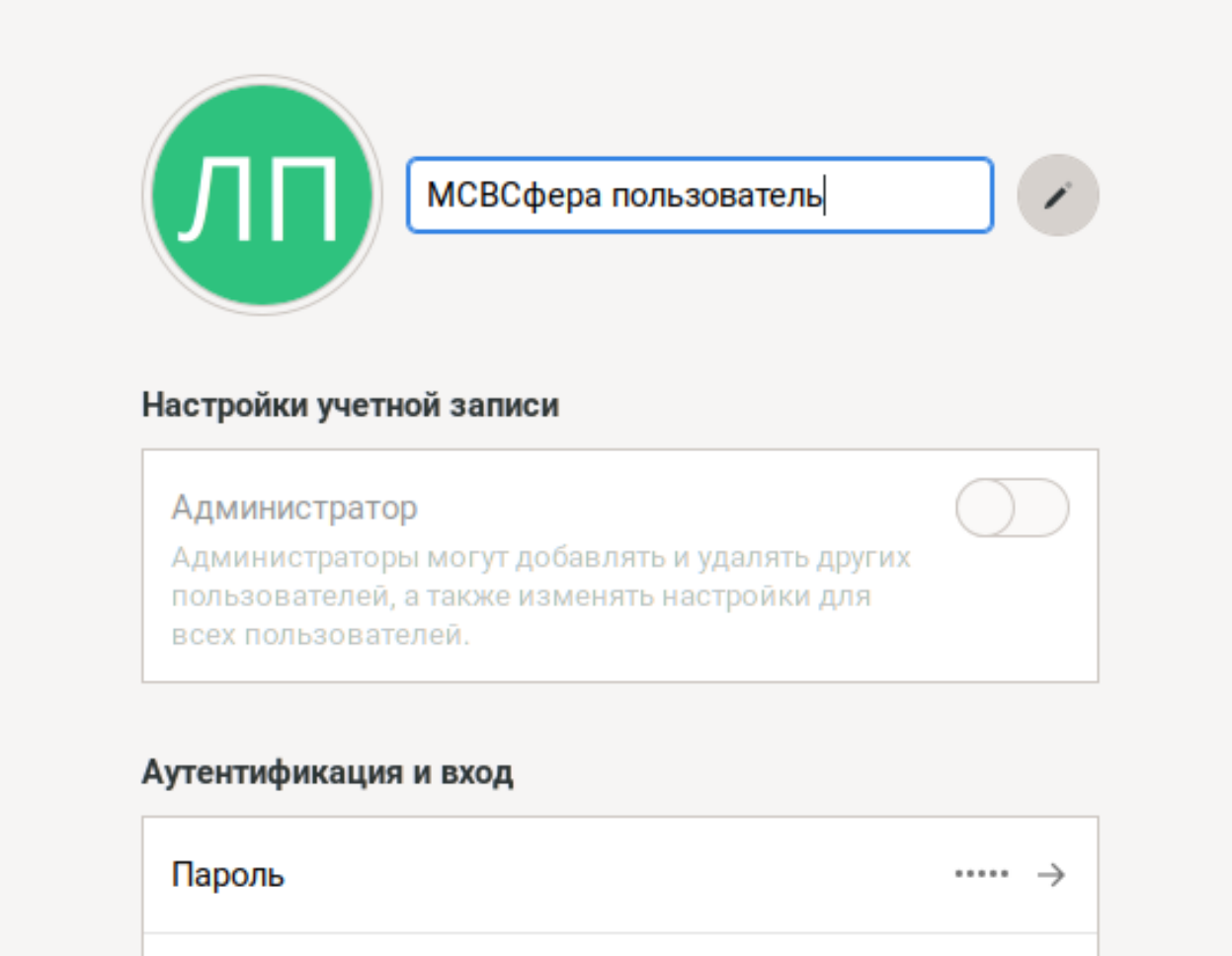
Пользователь также может изменить имя и графическое представление (изображение). Обычный пользователь может изменить только свои настройки, администратор может изменять настройки других пользователей.

Для изменения имени и графического представления перейдите в раздел «**Пользователи**» приложения «**Настройки**» любым удобным способом.

Для изменения графического представления нажмите на текущее изображение, затем выберите изображение из предлагаемых или из файла на компьютере.



Для изменения имени нажмите на изображение «**карандаша**», текущее имя пользователя станет доступным для изменения. При изменении имени пароль, а также имя домашней папки не изменятся.

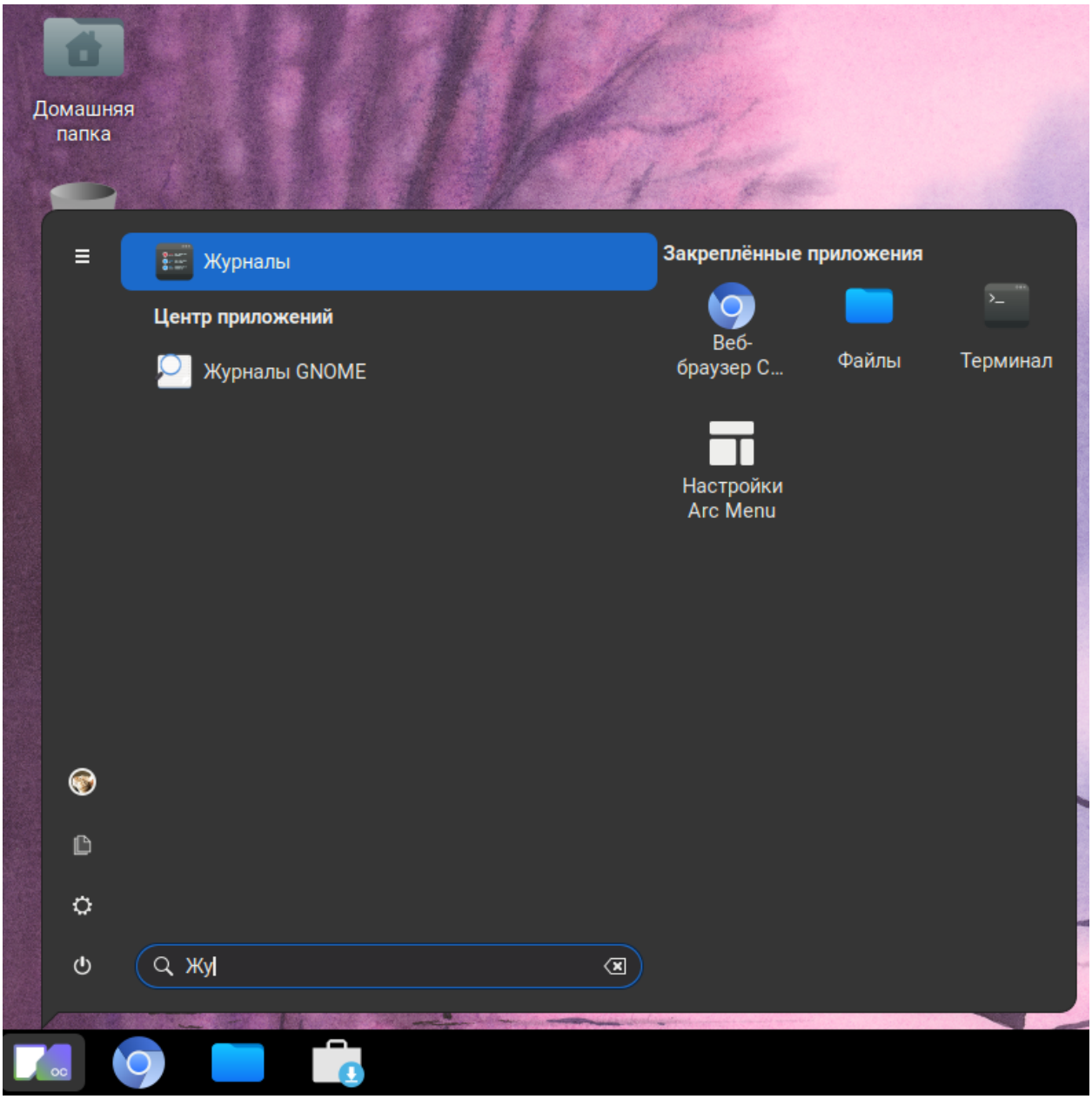


Для выхода без сохранения изменений просто закройте окно приложения «**Настройки**».

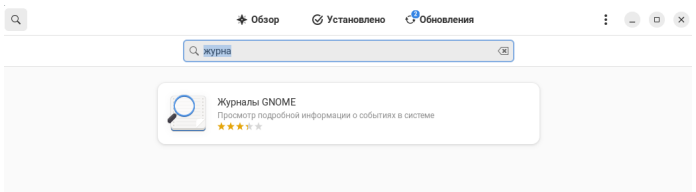
Просмотр системных журналов

Введение

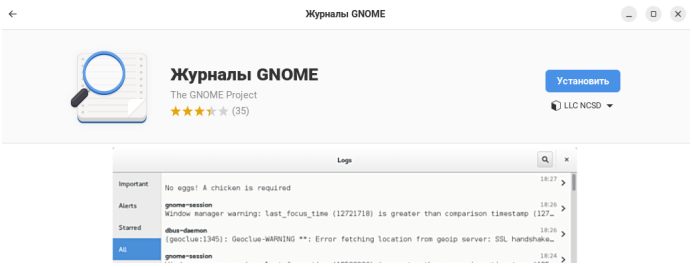
Просмотр системных журналов в графическом интерфейсе МСВСфера ОС производится в приложении «**Журналы GNOME**». Перейти в приложение «**Журналы GNOME**» вы можете из главного меню, набрав в строке поиска «журналы» и нажав на приложение правой кнопкой мыши.



Если приложение не установлено по умолчанию, его можно установить из «**Центра приложений**». Для этого перейдите в «**Центр приложений**» любым удобным способом и в строке поиска наберите «Журналы GNOME», нажмите правой клавишей мыши на найденное приложение, вы перейдёте на страницу приложения.



Далее нажмите на кнопку «**Установить**». После окончания установки приложение появится в главном меню.

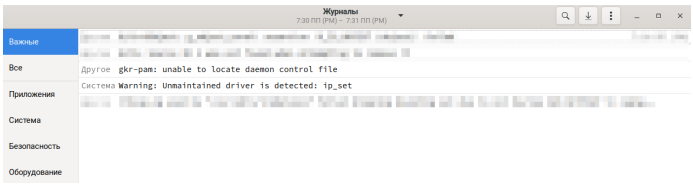


Записи в системном журнале

После запуска приложения вы попадёте на главную страницу. Слева показаны категории, справа список событий.

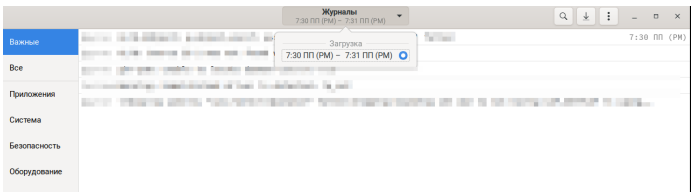
Доступны следующие категории:

- «Важные»;
- «Все»;
- «Приложения»;
- «Система»;
- «Безопасность»;
- «Оборудование».



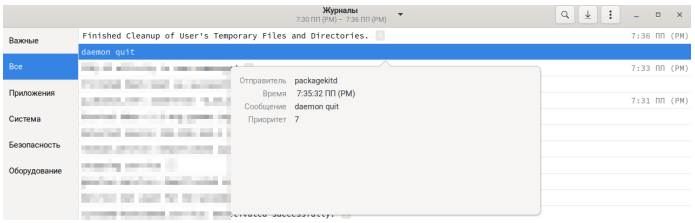
По умолчанию на главной странице отображаются события из категории «Важные».

Вы также можете выбрать загрузку, для которой показывать системный журнал, для этого нажмите на стрелку рядом с надписью «**Журналы**» в верхей части экрана.

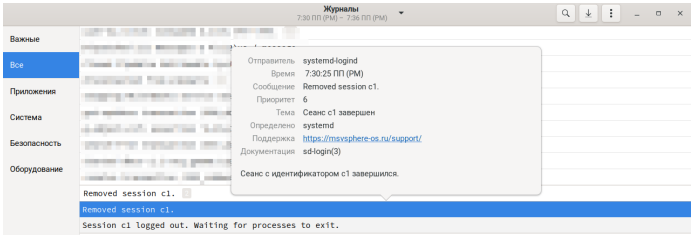


Просмотр информации о событии

Для просмотра информации о событии, нажмите на него правой клавишей мыши.



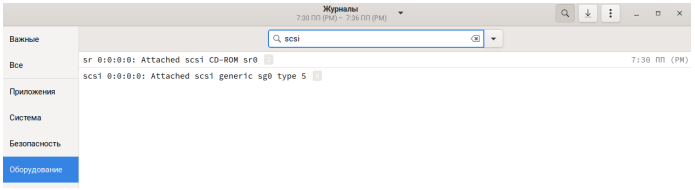
Если в одно событие попадает несколько сообщений, то рядом с событием отображается цифра, соответствующая числу сообщений. При нажатии на такое событие сначала раскрывается список сообщений, а затем, по нажатию правой клавишей мыши на сообщение, отображается подробная информация.



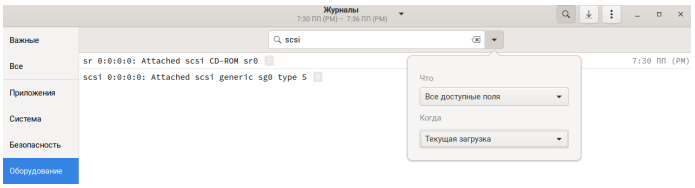
Поиск определённого события

Для поиска определённого события вы можете вызвать строку поиска, нажав на соответствующее изображение в правом верхнем углу экрана.

В строке поиска укажите ключевое слово, по которому будет осуществляться поиск — это может быть тип события, например, «error» или «warning», или же идентификатор устройства, например, «scsi».

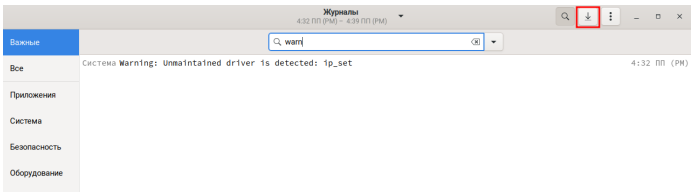


Для выбора дополнительных параметров поиска нажмите на стрелочку рядом с поисковой строкой, откроется выпадающее меню, в котором вы можете выбрать дополнительные параметры фильтрации — поле журнала и диапазон меток времени.



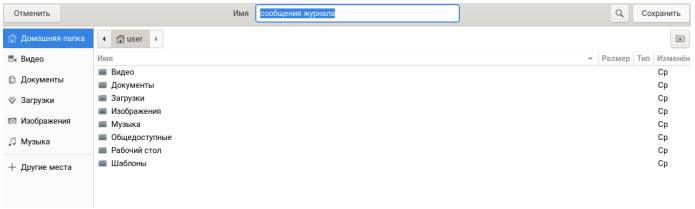
Экспорт журнала

Вы можете сохранить журнал для дальнейшего анализа или для других целей, предусмотренных политикой безопасности вашей компании, для этого нажмите на соответствующую иконку в правом верхнем углу (выделена красным на снимке экрана).



Обратите внимание, что если перед экспортом вы выполняли поиск, то экспорт будет выполнен только для найденных событий.

Укажите имя файла и куда его сохранять и нажмите на кнопку «**Сохранить**» в правом верхнем углу экрана.



Файл будет сохранён в указанное место, открыть его вы можете обычным текстовым редактором.

Создание защищённых каналов связи (VPN)

Создание защищённых VPN-туннелей, использующих контроль заголовков IP-пакетов в соответствии с ГОСТ Р 34.12-2015

Введение

Данный раздел описывает процедуру настройки VPN-туннеля на базе OpenVPN с контролем заголовков IP-пакетов в соответствии с ГОСТ Р 34.12-2015

«Информационная технология. Криптографическая защита информации. Блочные шифры».

Все команды, описанные в данном разделе, необходимо выполнять с привилегиями системного администратора (`root`).

Предварительные требования

На сервере и на клиентских компьютерах необходимо установить последнюю версию криптографических политик и пакет `openssl-gost-engine`, добавляющий поддержку ГОСТ алгоритмов в OpenSSL:

```
$ dnf install openssl-gost-engine
$ dnf upgrade crypto-policies
```

Затем подключите модуль `TLSGOST` к текущей политике:

```
# отобразить на экран название текущей политики
$ update-crypto-policies --show
DEFAULT

# добавить к политике "DEFAULT" модуль "TLSGOST"
$ update-crypto-policies --set DEFAULT:TLSGOST
```

Дополнительную информацию о криптографических политиках и модулях вы можете получить из раздела «gost-alg».

Настройка сервера OpenVPN

Установка сервера OpenVPN

На компьютере, который будет выполнять роль сервера OpenVPN, установите соответствующий пакет:

```
$ dnf install openvpn
```

Настройка удостоверяющего центра

Для настройки сервера OpenVPN с авторизацией по сертификатам TLS необходимо настроить собственный удостоверяющий центр (англ. Certification authority, CA), основной функцией которого является управление сертификатами сервера и клиентов OpenVPN, в том числе их создание и отзыв.

В данном примере в качестве рабочего каталога для удостоверяющего центра будет использоваться каталог `/root/CA`. Создайте необходимую структуру каталогов, а также файлы `index.txt`, `serial` и `crlnumber`, требуемые для работы центра:

```
$ mkdir -p /root/CA/{certs,crl,newcerts,private}
$ touch /root/CA/index.txt
$ echo 1000 > /root/CA/serial
$ echo 01 > /root/CA/crlnumber
```

Создайте конфигурационный файл для OpenSSL:

```
$ cat > /root/CA/openssl.conf << EOF
[ca]
default_ca          = CA_default

[CA_default]
dir                 = /root/CA
certs               = \$dir/certs
crl_dir             = \$dir/crl
new_certs_dir       = \$dir/newcerts
database            = \$dir/index.txt
serial              = \$dir/serial
crlnumber           = \$dir/crlnumber
private_key         = \$dir/private/ca.key
certificate         = \$dir/certs/ca.crt
crl                 = \$dir/crl/ca.crl
policy              = policy_strict
default_days        = 365
default_crl_days    = 30
default_md          = gost12_512
preserve            = no

[policy_strict]
countryName         = match
stateOrProvinceName = match
organizationName    = match
commonName          = supplied

[req]
default_bits        = 2048
prompt              = no
encrypt_key         = no

[v3_ca]
basicConstraints    = CA:TRUE
keyUsage            = critical,keyCertSign,cRLSign

[server]
basicConstraints    = CA:FALSE
keyUsage            = digitalSignature,keyAgreement
extendedKeyUsage    = serverAuth

[client]
basicConstraints    = CA:FALSE
keyUsage            = digitalSignature,keyAgreement
extendedKeyUsage    = clientAuth
EOF
```

Создайте секретный ключ удостоверяющего центра, защищённый паролем:

```
$ openssl genpkey -aes256 -algorithm gost2012_512 -pkeyopt paramset:A \
    -out /root/CA/private/ca.key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

В тестовом окружении вы можете использовать секретный ключ без пароля — для этого из приведённой выше команды необходимо убрать аргумент `-aes256`. Однако, в условиях промышленной эксплуатации ключ обязательно нужно защищать паролем и хранить в надёжном месте.

Далее создайте самоподписанный сертификат удостоверяющего центра:

```
$ openssl req -x509 -new -config /root/CA/openssl.conf \
    -extensions v3_ca -key /root/CA/private/ca.key \
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    -subj '/C=RU/ST=Moscow/O=MyVPN/CN=MyCA' \
    -days 3650 -out /root/CA/certs/ca.crt
Enter pass phrase for /root/CA/private/ca.key:
```

Перед запуском установите для полей аргумента `-subj` значения, соответствующие вашей организации: `C=RU` — страна, `ST=Moscow` — область, `O=MyVPN` — название организации, `CN=MyCA` — название удостоверяющего центра. Параметр `-days` определяет количество дней, в течение которых сертификат будет считаться действительным. В этом примере сертификат выпускается на 3650 дней (10 лет).

Затем, создайте список отозванных сертификатов:

```
$ openssl ca -config /root/CA/openssl.conf -gencrl \
    -out /root/CA/crl/ca.crl -md gost12_512 crldays 30
Using configuration from /root/CA/openssl.conf
Enter pass phrase for /root/CA/private/ca.key:
```

На этом процедуру создания удостоверяющего центра можно считать завершённой.

Конфигурация и запуск сервера OpenVPN

Создайте файл секретного ключа для сервера OpenVPN:

```
$ openssl genpkey -algorithm gost2012_512 -pkeyopt paramset:A \
    -out /root/CA/server.key
```

Создайте CSR запрос (Certificate Signing Request) на выпуск сертификата для сервера OpenVPN:

```
$ openssl req -new -config /root/CA/openssl.conf \
    -key /root/CA/server.key -subj '/C=RU/ST=Moscow/O=MyVPN/CN=server' \
    -out /root/CA/server.csr -md_gost12_512
```

Перед запуском установите для полей аргумента `-subj` значения, соответствующие вашей организации: `C=RU` — страна, `ST=Moscow` — область, `O=MyVPN` — название организации, `CN=server` — название сервера OpenVPN. В результате выполнения команды будет создан файл CSR запроса */root/CA/server.csr*, который затем будет использован для выпуска сертификата сервера OpenVPN удостоверяющим центром.

Для выпуска сертификата сервера OpenVPN выполните следующую команду:

```
$ openssl ca -config /root/CA/openssl.conf -in /root/CA/server.csr \
    -out /root/CA/server.crt -extensions server -md gost12_512 -batch
Using configuration from /root/CA/openssl.conf
Enter pass phrase for /root/CA/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'RU'
stateOrProvinceName   :ASN.1 12:'Moscow'
organizationName      :ASN.1 12:'MyVPN'
commonName            :ASN.1 12:'server'
Certificate is to be certified until May 15 15:19:27 2026 GMT (365 days)
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Write out database with 1 new entries
Database updated
```

Выпущенный ключ будет записан в файл `/root/CA/server.crt`.

Затем необходимо сгенерировать файл с параметрами безопасности Диффи-Хеллмана для создания безопасного TLS соединения:

```
$ openssl dhparam -out /root/CA/dh2048.pem 2048
Generating DH parameters, 2048 bit long safe prime
...
```

Скопируйте созданные файлы в рабочий каталог сервера OpenVPN и установите безопасные права на файл секретного ключа:

```
$ cp -f /root/CA/certs/ca.crt \
    /root/CA/server.key \
    /root/CA/server.crt \
    /root/CA/dh2048.pem \
    /root/CA/crl/ca.crl \
    /etc/openvpn/server/

$ chmod 600 /etc/openvpn/server/server.key
```

где:

- `/root/CA/certs/ca.crt` — публичный сертификат удостоверяющего центра;
- `/root/CA/server.key` — секретный ключ сервера OpenVPN;
- `/root/CA/server.crt` — публичный сертификат сервера OpenVPN;
- `/root/CA/dh2048.pem` — параметры безопасности Диффи-Хеллмана;
- `/root/CA/crl/ca.crl` — список отозванных клиентских сертификатов.

Далее, создайте конфигурационный файл сервера OpenVPN:

```
$ cat > /etc/openvpn/server/server.conf << EOF
mode server
topology subnet
;local 192.168.10.38
port 1194
proto udp
dev tun
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/server.crt
key /etc/openvpn/server/server.key
dh /etc/openvpn/server/dh2048.pem
crl-verify /etc/openvpn/server/ca.crl

server 10.10.4.0 255.255.255.0
;push "route 192.168.10.0 255.255.255.0"
;push "dhcp-option DNS 192.168.10.1"

keepalive 10 120
cipher kuznyechik-cbc
user openvpn
group openvpn
persist-key
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
persist-tun
verb 3
explicit-exit-notify 1
data-ciphers kuznyechik-cbc
auth id-tc26-gost3411-12-512
EOF
```

По умолчанию сервер OpenVPN принимает запросы со всех сетевых интерфейсов, раскомментируйте директиву `local` и укажите ей в качестве значения IP-адрес интерефейса, на котором должен принимать подключения сервер.

Далее, разрешите доступ к порту `1194`, на котором принимает подключения OpenVPN, в настройках брандмауэра:

```
$ firewall-cmd --permanent --add-service=openvpn
$ firewall-cmd --reload
```

После этого активируйте и запустите службу сервера OpenVPN:

```
$ systemctl enable --now openvpn-server@server.service
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn-server@server.service → /usr/
↪lib/systemd/system/openvpn-server@.service.
```

Проверить статус службы можно с помощью следующей команды:

```
$ systemctl status openvpn-server@server.service
● openvpn-server@server.service - OpenVPN service for server
   Loaded: loaded (/usr/lib/systemd/system/openvpn-server@.service; enabled; preset: disabled)
   Active: active (running) since Thu 2025-05-15 17:07:57 UTC; 5s ago
...
```

В диагностических целях системный журнал службы сервера OpenVPN можно просмотреть с помощью следующей команды:

```
$ sudo journalctl -u openvpn-server@server.service
```

Создание клиентских сертификатов

Для подключения к серверу OpenVPN для каждого клиента необходимо создать собственный секретный ключ и сертификат, все операции проводятся на сервере, выполняющем роль удостоверяющего центра.

Создайте файл сектретного ключа `/root/CA/client1.key`:

```
$ openssl genpkey -algorithm gost2012_512 -pkeyopt paramset:A \
    -out /root/CA/client1.key
```

Создайте CSR запрос на выпуск сертификата:

```
$ openssl req -new -config /root/CA/openssl.conf -key /root/CA/client1.key \
    -subj "/C=RU/ST=Moscow/O=MyVPN/CN=client1" \
    -out /root/CA/client1.csr -md_gost12_512
```

Перед запуском команды внесите необходимые изменения в поля аргумента `-subj`.

Создайте клиентский сертификат:

```
$ openssl ca -config /root/CA/openssl.conf -in /root/CA/client1.csr \
    -out /root/CA/client1.crt -extensions client -md gost12_512 -batch
Using configuration from /root/CA/openssl.conf
Enter pass phrase for /root/CA/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'RU'
stateOrProvinceName   :ASN.1 12:'Moscow'
organizationName      :ASN.1 12:'MyVPN'
commonName            :ASN.1 12:'client1'
Certificate is to be certified until May 15 18:54:10 2026 GMT (365 days)

Write out database with 1 new entries
Database updated
```

В результате выполнения команды будет создан файл `/root/CA/client1.crt`.

Затем, необходимо сгенерировать конфигурационный файл (в этом примере — `client1.ovpn`) для последующей передачи на клиентский компьютер:

```
$ cat > client1.ovpn << EOF
client
dev tun
proto udp
remote 192.168.10.38 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher kuznyechik-cbc
verb 3
data-ciphers kuznyechik-cbc
auth id-tc26-gost3411-12-512

<ca>
$(cat /root/CA/certs/ca.crt)
</ca>

<cert>
$(openssl x509 -in /root/CA/client1.crt)
</cert>

<key>
$(cat /root/CA/client1.key)
</key>
EOF
```

Замените `192.168.10.38` на реальный IP-адрес вашего сервера OpenVPN. Созданный конфигурационный файл необходимо передать на клиентский компьютер. Используйте только защищённые каналы связи поскольку в этом файле находится в том числе и секретный ключ доступа к VPN.

Настройка клиента OpenVPN

Установка клиента OpenVPN

На компьютере, который будет выполнять роль клиента OpenVPN, установите соответствующий пакет:

```
$ sudo dnf install openvpn
```

Если этот компьютер является графической рабочей станцией, установите также расширение для NetworkManager, которое позволяет настраивать подключение к OpenVPN через графический интерфейс:

```
$ sudo dnf install NetworkManager-openvpn-gnome
```

Настройка клиента OpenVPN в режиме командной строки

Для настройки клиента OpenVPN в режиме командной строки скопируйте созданный ранее файл `client1.ovpn` в каталог `/etc/openvpn/client/` под именем `client.conf` и установите для него безопасные права доступа:

```
$ sudo cp client1.ovpn /etc/openvpn/client/client.conf
$ sudo chown root:root /etc/openvpn/client/client.conf
$ sudo chmod 600 /etc/openvpn/client/client.conf
```

Следующая команда активирует и запустит службу клиента OpenVPN:

```
$ sudo systemctl enable --now openvpn-client@client.service
```

Посмотреть статус службы можно следующим образом:

```
$ sudo systemctl status openvpn-client@client.service
● openvpn-client@client.service - OpenVPN tunnel for client
   Loaded: loaded (/usr/lib/systemd/system/openvpn-client@.service; disabled; preset: disabled)
   Active: active (running) since Fri 2025-05-16 00:50:08 MSK; 16min ago
```

После запуска службы и успешного подключения к VPN-серверу в системе появится новый сетевой интерфейс `tun0`:

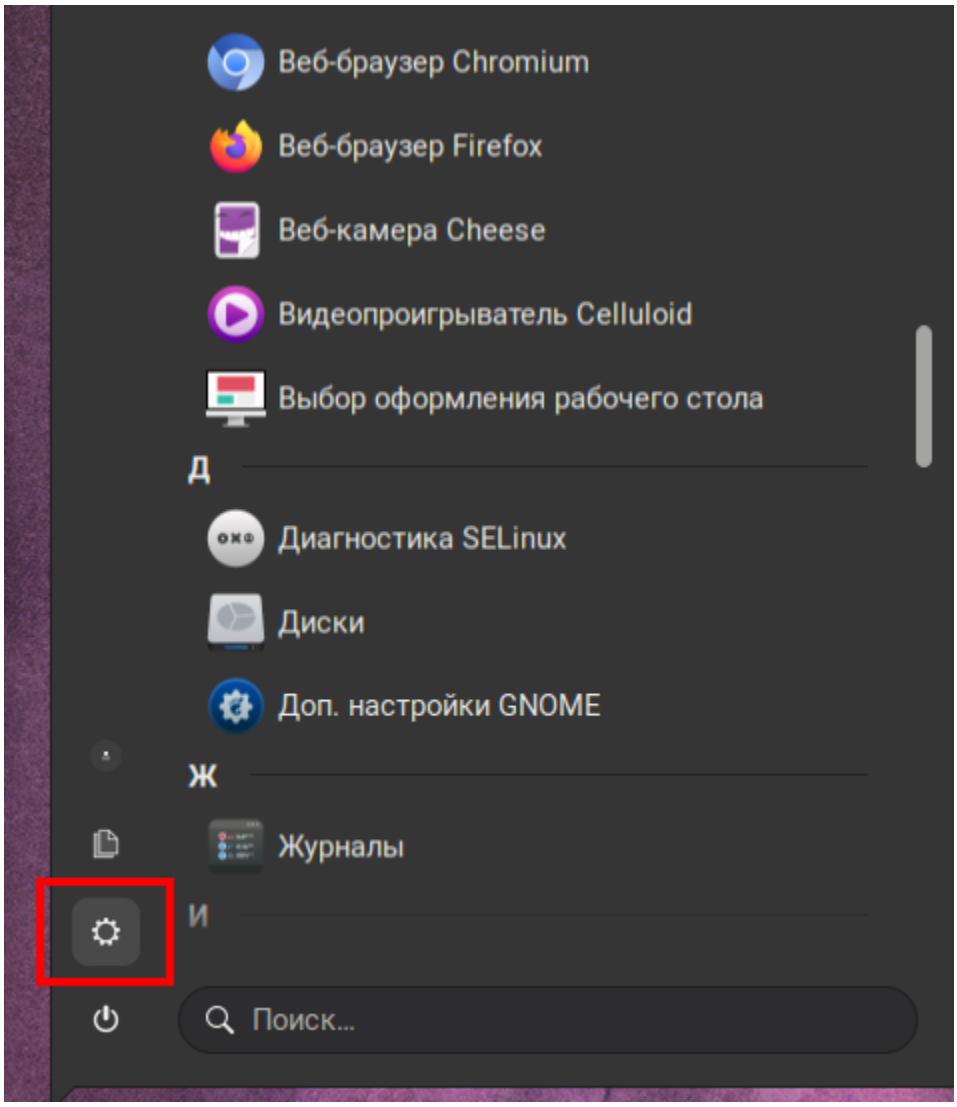
```
...
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group␣
↪default qlen 500
  link/none
  inet 10.10.4.2/24 scope global tun0
     valid_lft forever preferred_lft forever
  inet6 fe80::640:643d:d512:52ce/64 scope link stable-privacy
     valid_lft forever preferred_lft forever
```

В диагностических целях системный журнал клиента OpenVPN можно просмотреть с помощью следующей команды:

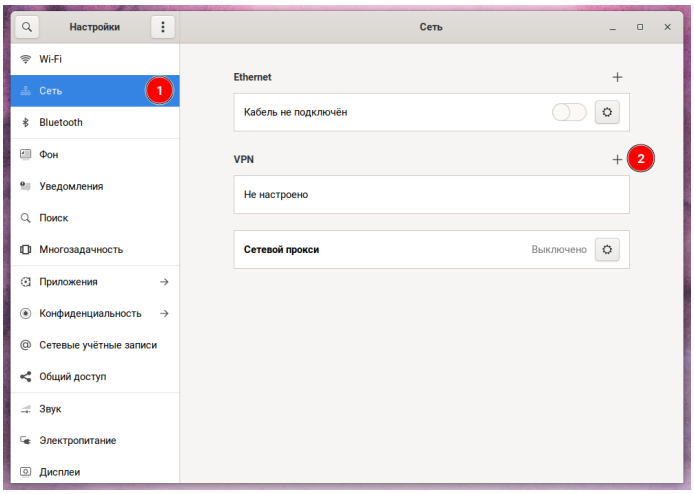
```
$ sudo journalctl -u openvpn-client@client.service
```

Настройка клиента OpenVPN в графическом режиме

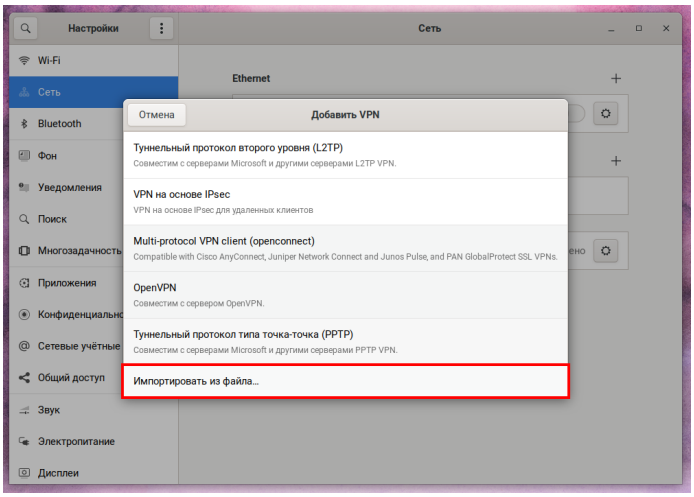
Для настройки подключения к OpenVPN через графический интерфейс откройте главное меню системы и запустите приложение «Настройки» (помечено красной рамкой на снимке экрана ниже):



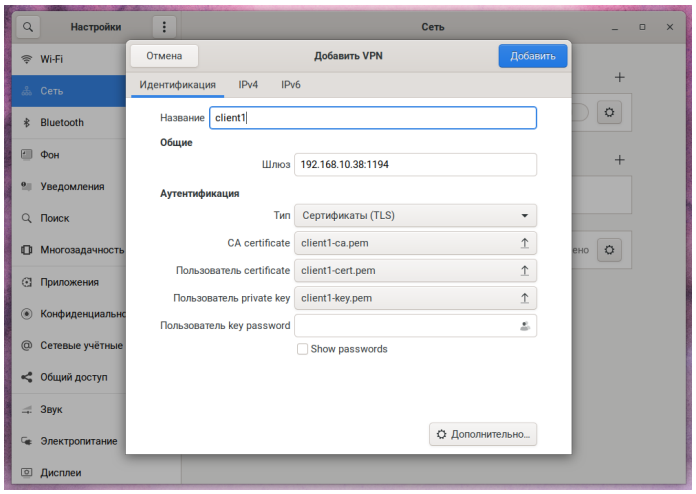
В левом меню выберите пункт «Сеть» (отмечен цифрой 1 на снимке экрана ниже), после этого откроется панель настройки сетевых подключений, где в блоке «VPN» вам необходимо нажать на значок + (отмечен цифрой 2 на снимке экрана ниже):



В появившемся окне «Добавить VPN» нажмите на пункт «Импортировать из файла...», отмеченный красной рамкой на снимке экрана ниже:

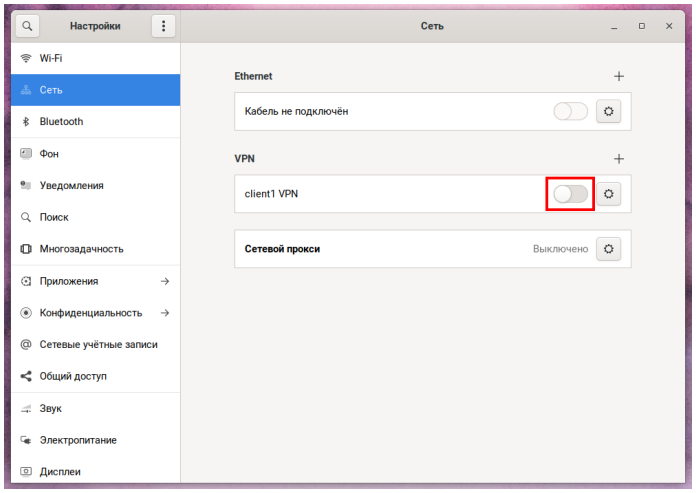


В открывшемся окне выбора файлов выберите ранее созданный файл `client1.ovpn` и нажмите кнопку «Открыть» — после этого появится окно добавления нового VPN-подключения, представленное на следующем снимке экрана:



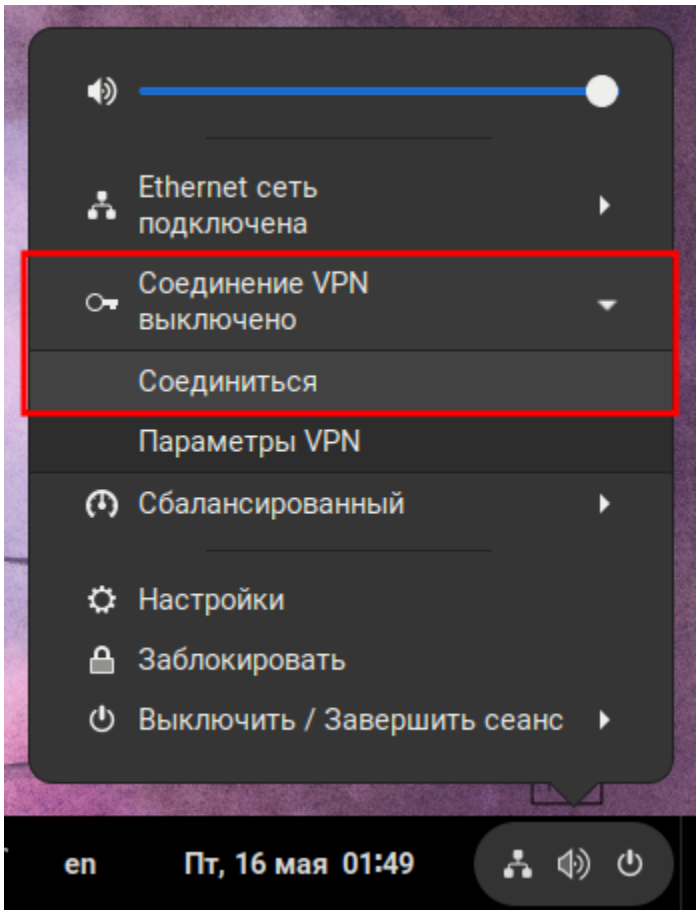
В случае необходимости вы можете изменить название подключения, IP-адрес или TCP-порт сервера. После завершения настройки нажмите на кнопку «Добавить».

После этого новое VPN-соединение появится в блоке «VPN» панели сетевых настроек:



Для подключения к VPN активируйте соответствующий переключатель, отмеченный красной рамкой на снимке экрана выше.

Также вы можете подключиться к ранее созданному VPN-соединению, нажав на группу иконок в правом нижнем углу экрана (справа от часов) и выбрав там пункт «Соединиться» в соответствующем блоке, отмеченном красной рамкой на снимке экрана:



Ограничение времени работы за компьютером

Введение

В состав операционной системы МСВСфера входит приложение **Timekpr-nExT**, которое предназначено для контроля и ограничения времени, проведённого пользователем за компьютером.

Установка

Для установки **Timekpr-nExT** выполните следующую команду:

```
$ sudo dnf install timekpr-next
```

Также установку можно выполнить с помощью Центра приложений.

Компоненты системы

Служба timekpr

Основным компонентом **Timekpr-nExT** является системная служба `timekpr`, которая осуществляет учёт времени, проведённого пользователем за компьютером, и применение соответствующих ограничений.

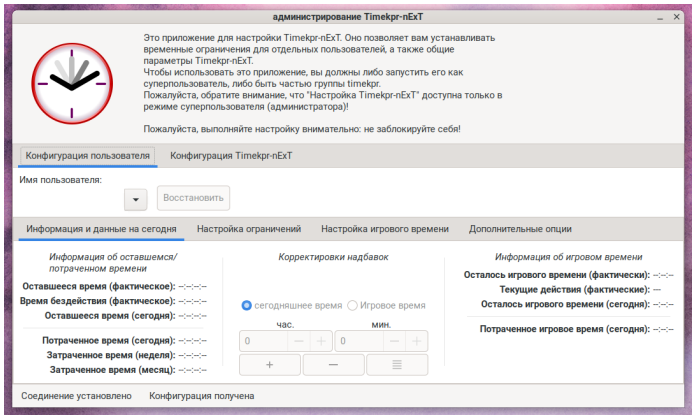
Сервис `timekpr` запускается автоматически после установки RPM пакета и в процессе загрузки компьютера, проверить статус можно с помощью следующей команды:

```
$ systemctl status timekpr
● timekpr.service - Timekpr-nExT daemon service
     Loaded: loaded (/usr/lib/systemd/system/timekpr.service; enabled; preset: disabled)
     Active: active (running) since Tue 2025-05-27 10:11:37 MSK; 36s ago
       Docs: file:/etc/timekpr/timekpr.conf
   Main PID: 1606 (timekprd)
      Tasks: 3 (limit: 50155)
     Memory: 14.2M
        CPU: 98ms
     CGroup: /system.slice/timekpr.service
             └─1606 /usr/bin/python3 /usr/lib/python3.9/site-packages/timekpr/server/timekprd.py␣
↪/usr/bin/timekprd

мая 27 10:11:37 sphere-96-arm systemd[1]: Started Timekpr-nExT daemon service.
```

Панель управления

Для настройки системы используется графическая панель управления:



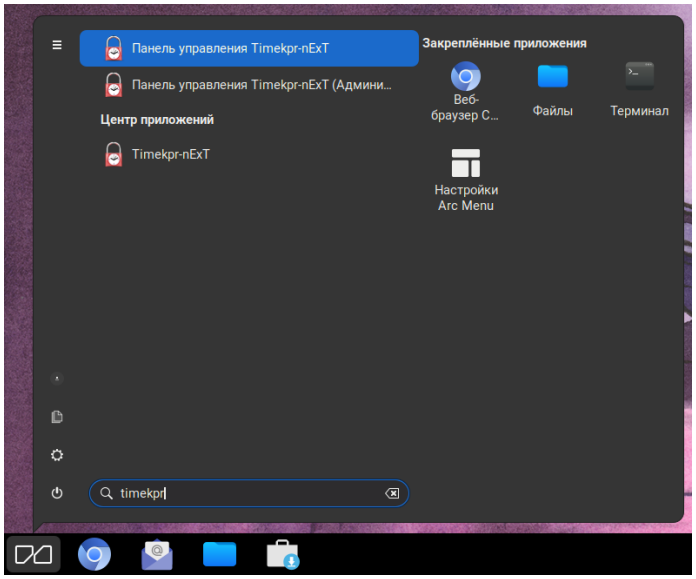
Для работы с панелью управления пользователь, выполняющий роль администратора системы учёта времени, должен либо обладать привилегиями системного администратора, либо быть участником системной группы `timekpr`. Второй вариант является предпочтительным с точки зрения информационной безопасности.

Для добавления пользователя в группу `timekpr` выполните следующую команду (замените `user` на реальное имя пользователя):

```
$ sudo gpasswd -a user timekpr
Добавление пользователя user в группу timekpr
```

После добавления в группу пользователю необходимо выйти из системы и зайти повторно для применения изменений.

Для запуска панели управления используйте пункт главного меню `Панель управления Timekpr-nExT`:



Либо выполните следующую команду в терминале:

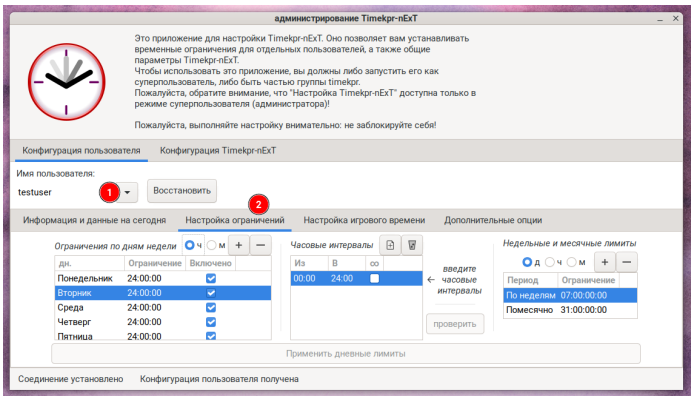
```
$ timekpra
```

Если по каким-то причинам вы не можете добавить пользователя в группу `timekpr`, то вам необходимо использовать пункт меню `Панель управления Timekpr-nExT (Администратор)` либо команду `sudo timekpra`. В таком случае система попросит вас ввести пароль.

Процедура настройки системы контроля времени с помощью панели управления описывается в следующих разделах.

Настройка ограничений времени

Для настройки ограничений рабочего времени запустите `Панель управления Timekpr-nExT`, выберите пользователя, для которого необходимо установить ограничения, в выпадающем списке пользователей (отмечен цифрой `1` на снимке экрана) и перейдите во вкладку `Настройка ограничений` (отмечена цифрой `2` на снимке экрана):



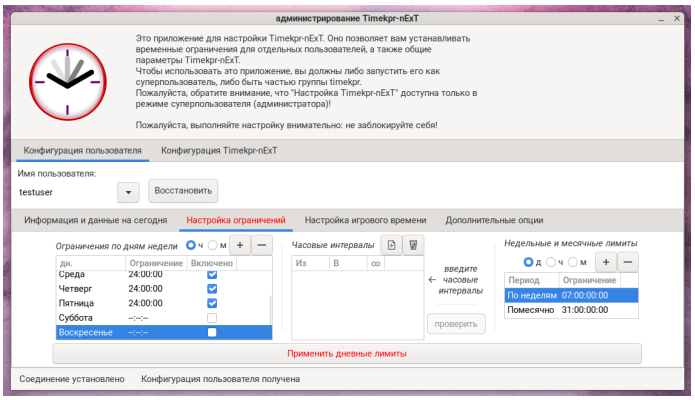
Для каждого пользователя можно установить следующие типы лимитов:

- days_of_week — определяет в какие дни недели пользователь может использовать компьютер и суммарное количество времени, доступное для каждого дня;
- hours — определяет конкретные временные интервалы, в которых пользователь может использовать компьютер в течение дня;
- weeks_and_months — определяет суммарное количество времени, доступное пользователю в течение недели и месяца.

Ограничения по дням недели

Лимит «Ограничения по дням недели» позволяет задать список дней, в которые пользователь может работать за компьютером, а также указать количество времени, доступное для каждого дня.

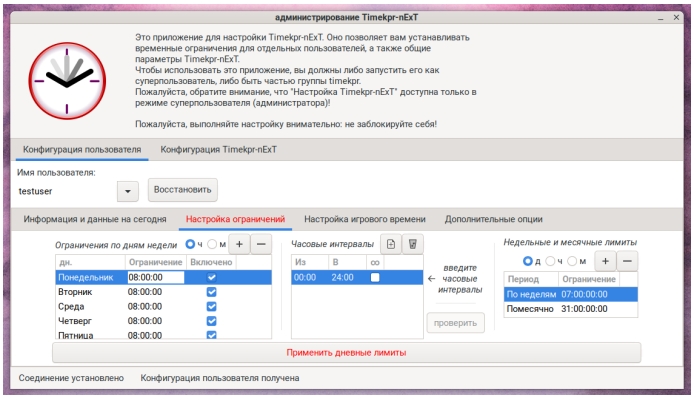
Для запрета работы в определённый день недели уберите флажок в колонке «Включено». На следующем снимке экрана в качестве примера установлен запрет на работу с компьютером в выходные дни:



Также вы можете ограничить суммарное количество времени для каждого дня: для этого выберите в таблице день недели, нажмите на соответствующую ячейку

в колонке «Ограничение» и укажите необходимое значение в формате `ЧЧ:ММ:СС` (`Часы:Минуты:Секунды`). Значение по умолчанию - `24:00:00`, что означает отсутствие ограничений по времени. В качестве альтернативного способа вы можете использовать переключатель `Ч/М` (`Часы/Минуты`) и кнопки `+/-` для изменения значения.

На следующем снимке экрана доступное время в будние дни ограничено восемью часами:

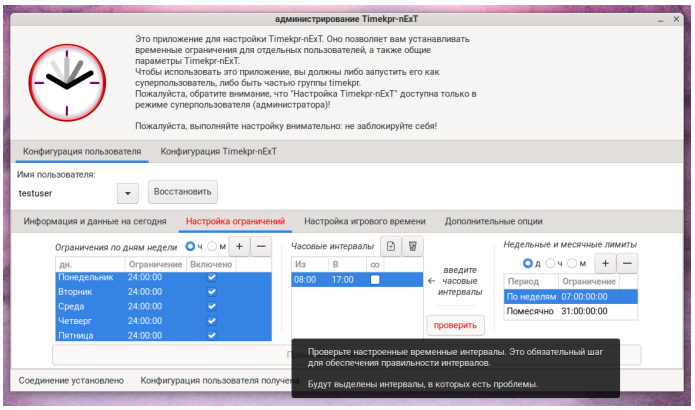


Часовые интервалы

С помощью часовых интервалов вы можете определить, в какие промежутки времени в течение дня пользователь может использовать компьютер. Настраивать их можно как для одного, так и для нескольких дней одновременно.

В конфигурации по умолчанию для всех дней задан один интервал с `00:00` до `24:00` — фактически это означает отсутствие ограничений.

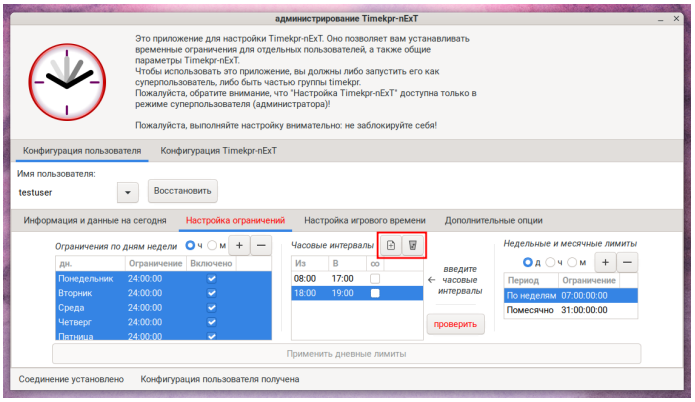
Для изменения существующего интервала выберите один или несколько дней в таблице «Ограничения по дням недели», затем в колонке «Из» установите начальное время, а в колонке «В» — конечное время интервала. На снимке экрана ниже показана установка временного интервала с `8:00` до `17:00` для всех будних дней:



После установки временного интервала вам необходимо нажать кнопку «проверить» для верификации введённых данных. В случае обнаружения ошибок проблемные

интервалы будут выделены, а в строке состояния программы отобразится описание ошибки.

Вы можете настроить несколько временных интервалов — используйте соответствующие кнопки, выделенные красной рамкой на снимке экрана ниже, для добавления нового и удаления выбранного интервала:



При настройке интервалов следует придерживаться следующих правил:

- интервалы не должны пересекаться;
- даже минутный перерыв между интервалами активирует ограничения;
- в течение одного часа не может начинаться и заканчиваться больше одного интервала.

Также следует упомянуть переключатель в колонке «∞» — его активация приведёт к тому, что выбранный интервал будет считаться свободным от ограничений и не будет учитываться в общем дневном лимите. Это может быть полезно, например, если ребёнок посещает онлайн курсы и время, проведённое на них, не должно приводить к уменьшению доступного для других активностей времени.

Недельные и месячные лимиты

С помощью блока недельных и месячных лимитов вы можете настроить максимально допустимое время использования компьютера за неделю или месяц. В конфигурации по умолчанию лимиты отсутствуют: для недельного ограничения установлено значение 7 дней, а для месячного — 31 день.

Для определения значений используется формат `Дни:Часы:Минуты:Секунды`. При вводе вы можете использовать сокращения, например: значение `6` будет преобразовано в `06:00:00:00`, а `6:12:30` — в `06:12:30:00`.

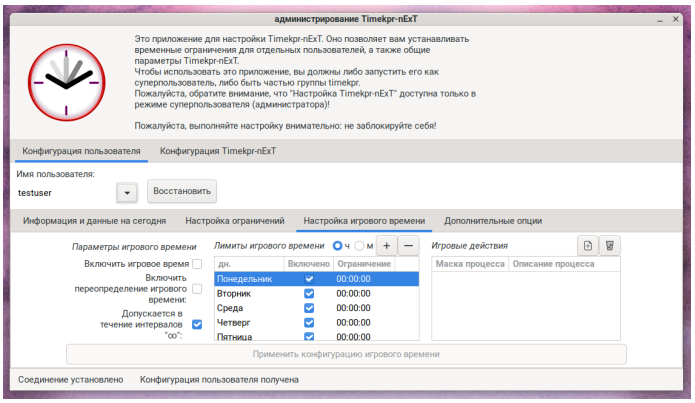
Недельные и месячные лимиты работают одновременно с дневными лимитами — система всегда будет использовать наименьшее из действующих ограничений.

Сохранение настроек

После установки необходимых ограничений нажмите кнопку «Применить дневные лимиты» для сохранения настроек. В случае успешного сохранения настроек программа отобразит подтверждающее сообщение в статусной строке — после этого вы можете перейти к настройкам лимитов для другого пользователя, либо закрыть программу.

Ограничение времени для отдельных процессов

В системе **Timekpr-nExT** также реализована функция ограничения времени использования отдельных процессов. Изначально этот модуль был разработан для ограничения времени, проведённого в играх детьми, однако может быть использован для контроля использования любых процессов. Настройки данной функции доступны во вкладке «Настройка игрового времени»:



В блоке «Параметры игрового времени» находится группа переключателей, отвечающая за общие настройки модуля:

- *Включить игровое время* — активирует функцию учёта времени использования отдельных процессов для выбранного пользователя. Также для работы этой функции потребуется включить соответствующий переключатель в системных настройках **Timekpr-nExT**;
- *Включить переопределение игрового времени* — активация этого переключателя отключает стандартные лимиты времени, учёт будет выполняться только для процессов, перечисленных в блоке «Игровые действия»;
- *Допускается в течение интервалов «∞»* — разрешает запуск процессов, определённых в блоке «Игровые действия» в интервалах, помеченных как свободные (∞) в блоке «Часовые интервалы» вкладки «Настройка ограничений».

В блоке «Лимиты игрового времени» настраиваются дни и часы, в которые пользователь сможет запускать процессы, определённые в блоке «Игровые действия».

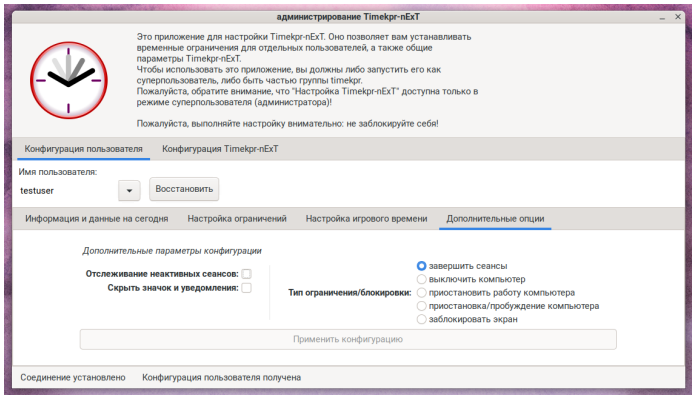
Процедура настройки идентична настройке часовых интервалов во вкладке «Настройка ограничений».

Блок «Игровые действия» является ключевым для данного модуля — в нём настраивается список процессов, для которых необходимо применять ограничение. В поле «Маска процесса» необходимо ввести название команды без пути и аргументов командной строки (используйте команды `top -c -d 1`, `htop` и т.п., чтобы получить информацию о запущенных в системе процессах). В поле «Описание процесса» вы можете добавить опциональный комментарий. Также вы можете включить системную настройку «Улучшенный мониторинг активности» — в этом случае будет активирована поддержка регулярных выражений и аргументов командной строки в поле «Маска процесса».

Для сохранения изменений нажмите кнопку «Применить конфигурацию игрового времени».

Дополнительные опции

Во вкладке «Дополнительные опции» находятся дополнительные параметры, которые могут быть настроены для каждого пользователя:



- *Отслеживание неактивных сеансов* — активирует учёт времени, даже когда экран компьютера заблокирован или пользователь работает в аппаратной консоли;
- *Скрыть значок и уведомления* — скрывает иконку клиентского приложения **Timekpr-nExT** на панели задач рабочего стола и отключает предупреждения о скором завершении сеанса;
- *Тип ограничения/блокировки* — определяет действие, которое должно быть выполнено по достижении лимита времени пользователем:
  - *завершить сеансы* — принудительно завершает сессию пользователя. В случае повторного входа в систему сессия будет также незамедлительно закрыта;

- *выключить компьютер* — выключает компьютер по достижении лимита. Используйте эту опцию с осторожностью, особенно в многопользовательских окружениях;
- *приостановить работу компьютера* — переводит компьютер в спящий режим. Пользовательская сессия при этом не завершается — при включении экран будет заблокирован. Если выход из спящего режима был осуществлён до сброса лимитов, компьютер будет повторно переведён в спящий режим;
- *приостановка/пробуждение компьютера* — действует так же, как и предыдущая опция, но компьютер будет автоматически выведен из спящего режима в указанном интервале этого же дня. Некоторое оборудование может быть несовместимо с этим режимом — как минимум требуется поддержка RTC (Real Time Clock) в BIOS/UEFI и именно программа **Timekpr-nExT** должна перевести компьютер в спящий режим. Если следующий период разблокировки лимитов не попадает в указанный в настройках опции интервал, компьютер не будет автоматически выводиться из спящего режима;
- *заблокировать экран* — по исчерпании лимита экран компьютера блокируется.

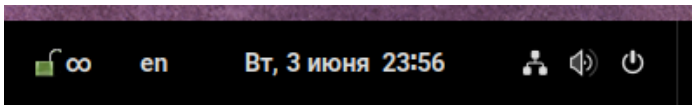
Последние три варианта не являются надёжными способами блокировки, а больше подходят для самоконтроля. В производственных условиях рекомендуется использовать варианты «завершить сеансы» или «выключить компьютер».

После внесения изменений нажмите кнопку «Применить конфигурацию» для сохранения настроек.

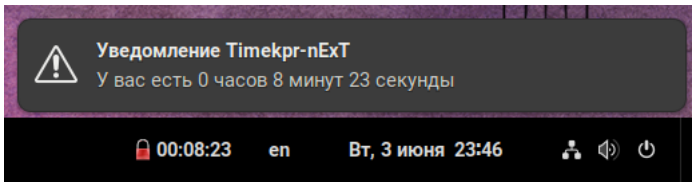
Пользовательское приложение

После установки и активации системы **Timekpr-nExT** у каждого пользователя на панели задач появится иконка приложения, отображающая текущий статус.

В случае отсутствия настроенных ограничений иконка будет иметь вид открытого замка с символом «∞»:

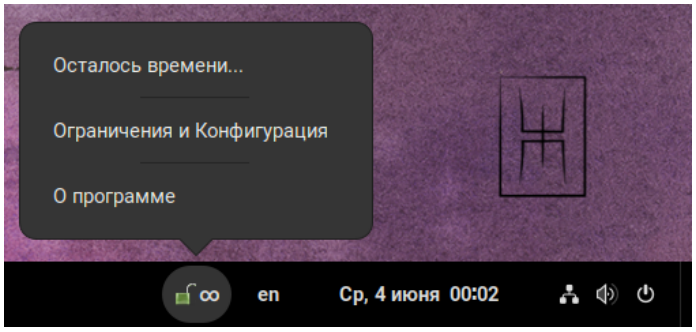


Если же лимиты активны, то иконка будет иметь вид закрытого замка и счётчика оставшегося времени до завершения сессии:

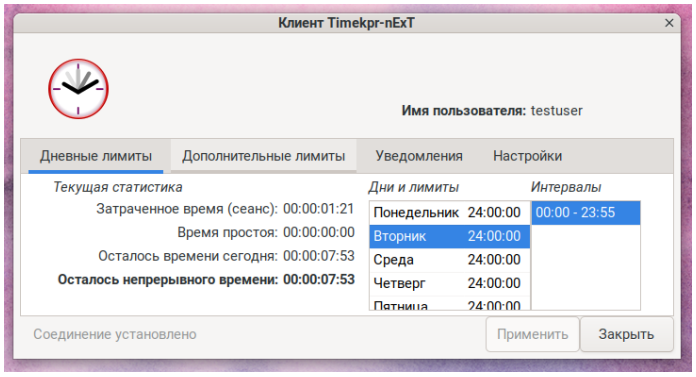


С заданной в настройках системы периодичностью пользователю будет отображаться всплывающее уведомление о количестве оставшегося времени до завершения сеанса.

Нажав на иконку приложения, пользователь вызовет контекстное меню:

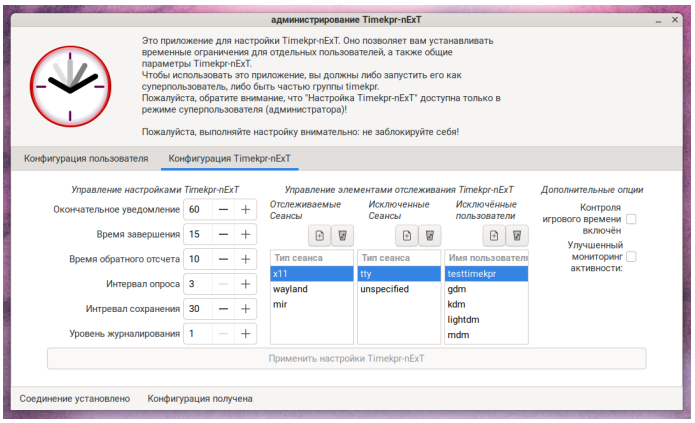


- *Осталось времени* — отобразит всплывающее уведомление о том, сколько времени осталось до блокировки сеанса;
- *О программе* — отобразит окно с информацией о версии программы **Timekpr-nExT**, её разработчиках и лицензии;
- *Ограничения и Конфигурация* — отобразит основное окно пользовательского приложения, в котором можно будет посмотреть статистику использования времени и настроить уведомления системы:



Системные настройки

Для доступа к системным настройкам **Timekpr-nExT** вам необходимо запустить панель управления с привилегиями системного администратора и перейти на вкладку «Конфигурация Timekpr-nExT»:



Для большинства сценариев использования конфигурация по умолчанию является оптимальной и не требует изменения.

Блок «Управление настройками Timekpr-nExT»:

- *Окончательное уведомление* — определяет, за сколько секунд до истечения выделенного времени пользователю будет показано финальное уведомление о предстоящем завершении сеанса;
- *Время завершения* — определяет, за сколько секунд до истечения выделенного времени будет применяться блокировка сеанса;
- *Время обратного отсчета* — определяет, за сколько секунд будет начат обратный отсчёт в реальном времени перед блокировкой сеанса;
- *Интервал опроса* — задаёт интервал в секундах, с которым система пересчитывает оставшееся время и анализирует сеансы пользователя;
- *Интервал сохранения* — задаёт интервал в секундах, с которым система будет сохранять статистику активности пользователя на диск;
- *Уровень журналирования* — задаёт уровень детализации сообщений в системном журнале службы:
  - *1* — стандартный (рекомендуется к использованию в производственной среде);
  - *2* — отладочный (включает дополнительную диагностическую информацию);
  - *3* — расширенный отладочный (включает вывод максимального количества диагностической информации, включая содержимое внутренних структур. Он используется, в основном, разработчиками системы).

Блок «Управление элементами отслеживания Timekpr-nExT»:

- *Отслеживаемые сеансы* — определяет типы сеансов, для которых будет выполняться учёт времени. В конфигурации по умолчанию отслеживаются

только сеансы «x11» (Xorg), «wayland» и «mir», что является достаточным для большинства сценариев использования. **Timekpr-nExT** предполагает, что существуют только эти типы сеансов и сеансы, указанные в списке «Исключённые сеансы»;

- *Исключенные сеансы* — список сеансов, для которых не будет осуществляться учёт времени. В конфигурации по умолчанию в этот список входят «tty» (аппаратные консоли, `Ctrl+Alt+F[1-7]`) и «unspecified» (все остальные типы сеансов, которые не входят в списки отслеживаемых и исключённых сеансов);
- *Исключенные пользователи* — список пользователей, для которых не должен осуществляться учёт времени. Как правило, это системные пользователи, от имени которых запускаются менеджеры входа в систему (GDM и т.п.).

Блок «Дополнительные опции»:

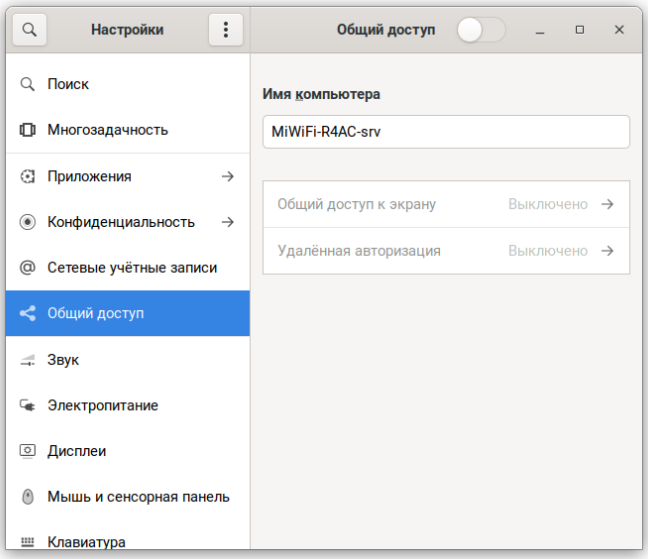
- *Контроль игрового времени включён* — включает или отключает функцию учёта игрового времени. Если этот переключатель выключен, то функция будет отключена для всех пользователей, даже если для отдельно взятого пользователя она активирована во вкладке «Настройка игрового времени»;
- *Улучшенный мониторинг активностей* — если эта опция включена, то функция учёта игрового времени будет отслеживать процессы по полной строке запуска процесса, включая аргументы командной строки, а если отключена, то отслеживание будет осуществляться только по названию команды. В некоторых случаях эта функция может быть полезна для отслеживания процессов, которые запускаются через интерпретаторы.

Для сохранения изменённых настроек нажмите кнопку «Применить настройки Timekpr-nExT».

Подключение к удалённому рабочему столу

Введение

В разделе настроек «Общий доступ» вы можете запустить встроенный в GNOME сервер VNC/RDP, который позволяет удалённо подключаться к рабочему пространству пользователя. В зависимости от версии операционной системы МСВСфера протокол подключения может отличаться.



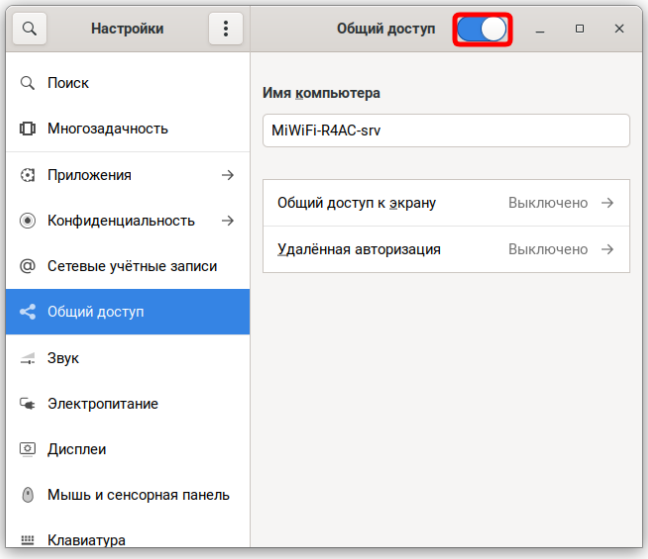
Установка

Установите пакет `gnome-remote-desktop`, для этого выполните следующую команду в «Терминале»:

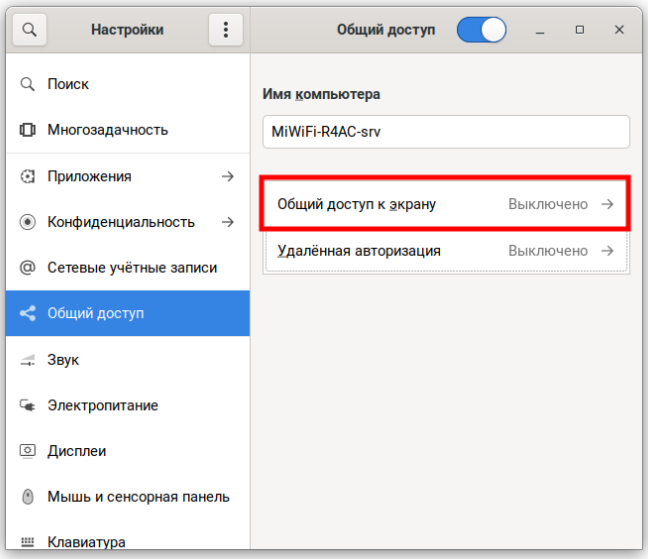
```
$ sudo dnf install gnome-remote-desktop
```

Использование раздела «Общий доступ» в МСВСфера 8/9

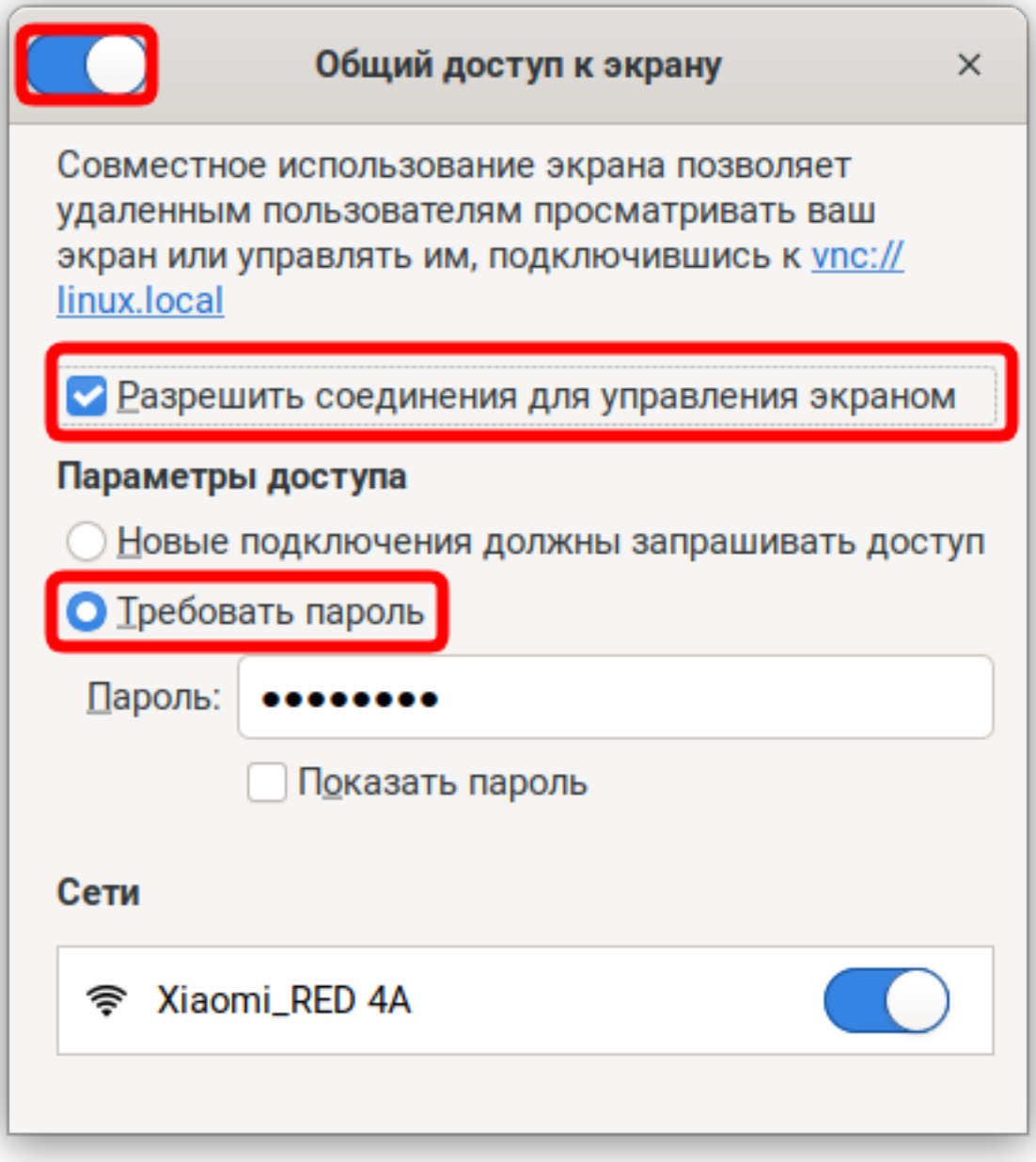
Перейдите в настройки и найдите раздел «Общий доступ», затем включите его.



После включения перейдите во вкладку «Общий доступ к экрану».



Включите функцию «Общий доступ к экрану» с помощью переключателя. Если вы хотите, чтобы пользователь имел доступ к управлению вашим экраном, поставьте галочку в строке «Разрешить соединения для управления экраном». Также при подключении рекомендуется использовать пароль, для этого выберите «Требовать пароль» и укажите его в специальном поле.



Чтобы удалённое подключение к рабочему столу стало возможным, откройте порт `5900` и перезагрузите `firewall`:

```
$ sudo firewall-cmd --permanent --add-port=5900/tcp
$ sudo firewall-cmd --reload
```

Существует проблема подключения к удалённой рабочей машине с помощью `vncviewer`. Она заключается в невозможности согласовать тип механизма безопасности, используемого в `gnome-remote-desktop`. Если вы

хотите использовать только `vncviewer`, то в качестве временного решения вы можете отключить шифрование в `gnome-remote-desktop` с помощью следующей команды:

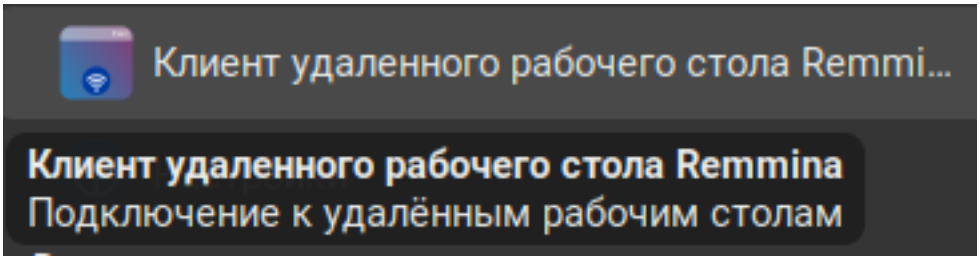
```
$ gsettings set org.gnome.desktop.remote-desktop.vnc encryption "['none']"
```

Удалённое подключение к МСВСфера 8/9 с помощью Remmina

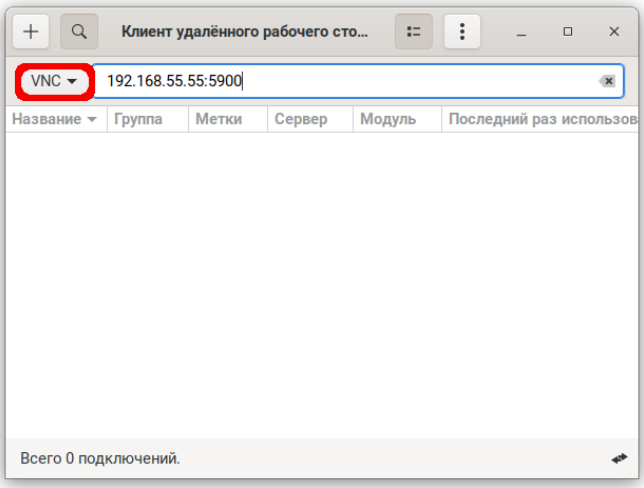
Установите приложение для удалённого подключения «Remmina», выполнив в «Терминале» следующую команду:

```
$ sudo dnf install remmina
```

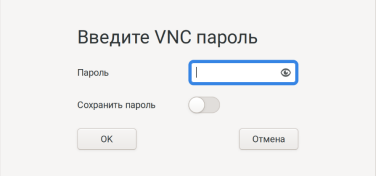
В главном меню появится ярлык приложения «Remmina»



Откройте приложение, поменяйте протокол подключения на VNC, укажите IP-адрес и порт, затем нажмите «Ввод» на клавиатуре.



Для завершения подключения к устройству, укажите пароль.



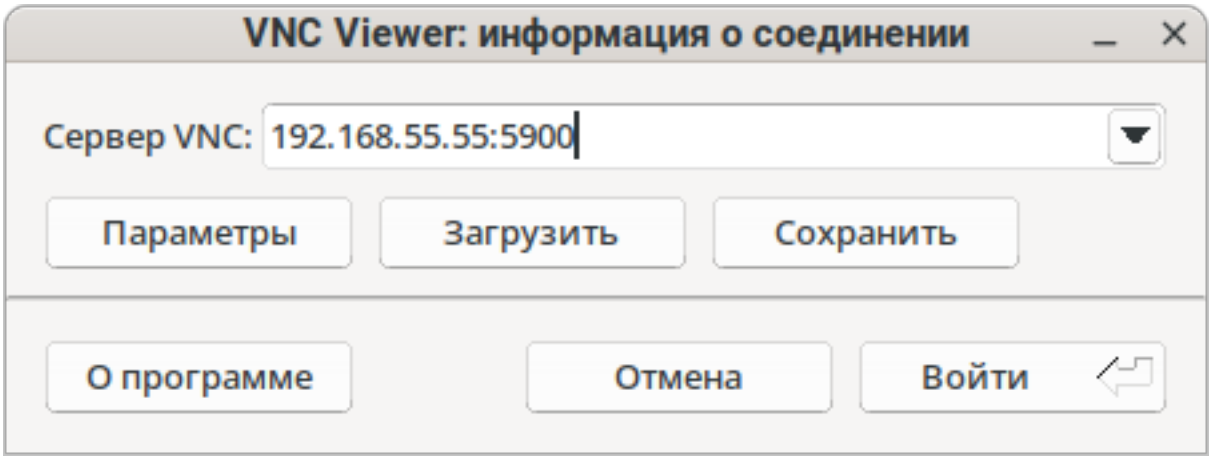
Удалённое подключение к МСВСфера 8/9 с помощью TigerVNC

Установите приложение для удалённого подключения «TigerVNC», выполнив в «Терминале» следующую команду:

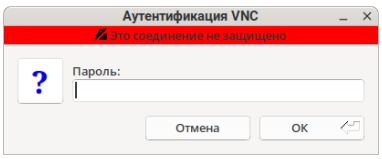
```
$ sudo dnf install tigervnc
```

В главном меню появится ярлык приложения «TigerVNC»:

Откройте приложение и укажите IP-адрес и порт, затем нажмите «Ввод» на клавиатуре.



Для завершения подключения к устройству, укажите пароль.



Настройка оборудования

Управление принтерами

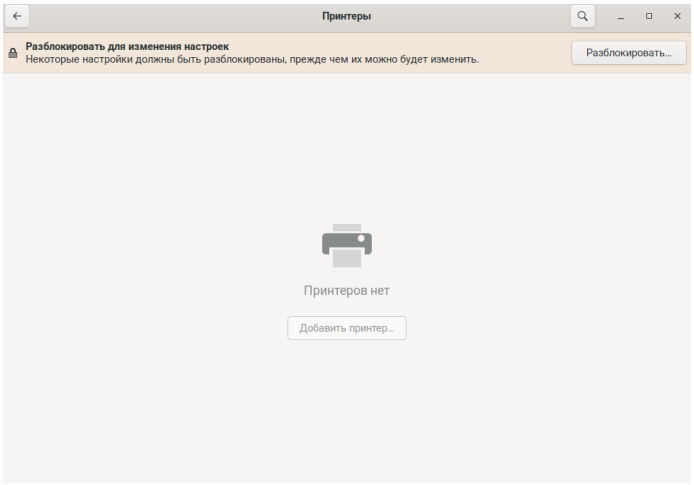
Введение

Настройка и управлении принтерами в графическом интерфейсе МСВСфера ОС производится в приложении «**Настройки**». Перейти в «**Настройки**» вы можете из главного меню, набрав в строке поиска «настройки» и нажав на приложение правой кнопкой мыши, или нажав значок «**Шестерёнки**» в системной панели или в главном меню. Перед добавлением и настройкой принтера убедитесь, что он подключён к сети питания и включён.

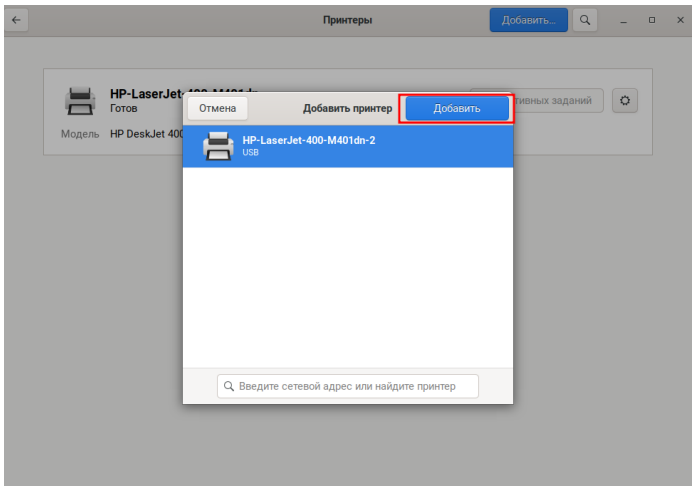
Добавление принтера в систему

Откройте приложение «**Настройки**» любым удобным способом и перейдите в раздел «**Принтеры**».

Для любой учётной записи (кроме суперпользователя) при начальном входе некоторые настройки будут заблокированы. Для разблокировки необходимо пройти аутентификацию.



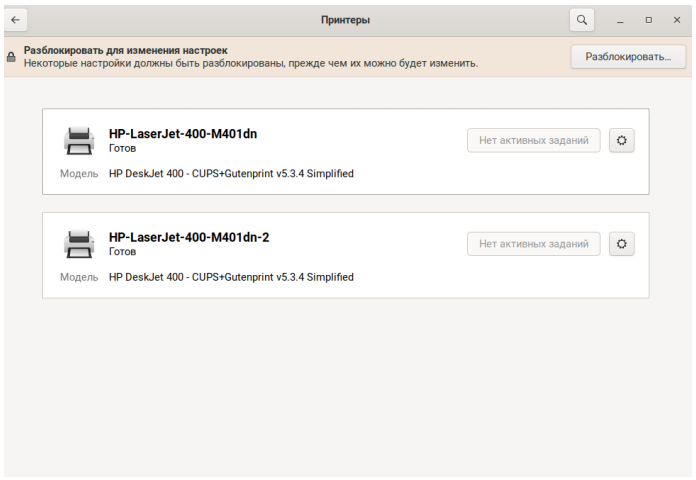
После успешного прохождения аутентификации активируется кнопка «**Добавить принтер**». Нажмите на неё, откроется окно «**Добавить принтер**».



Примечание

Обычно при подключении принтера, он добавляется в систему автоматически и сразу будет виден в разделе «Настройки» → «Принтеры». При поиске принтера вы также можете указать его сетевой адрес вручную в строке поиска.

Выберите принтер и нажмите «**Добавить**». Принтер появится в списке.

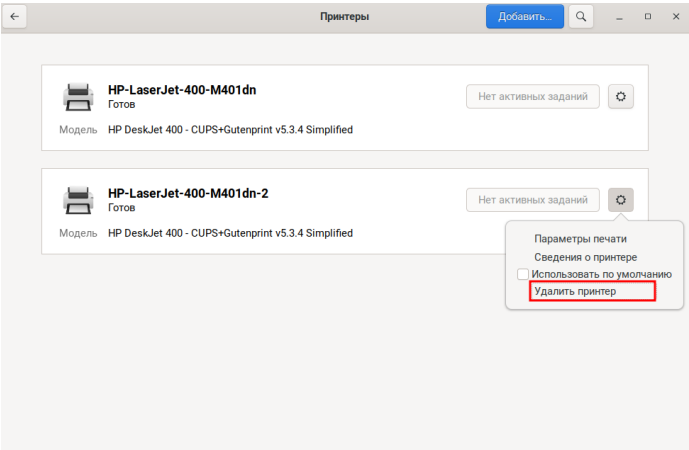


Удаление принтера

Откройте приложение «**Настройки**» любым удобным способом и перейдите в раздел «**Принтеры**».

Для любой учётной записи (кроме суперпользователя) при начальном входе некоторые настройки будут заблокированы. Для разблокировки необходимо пройти аутентификацию.

Выберите необходимый принтер из списка и нажмите на значок «Шестерёнки», в открывшемся выпадающем списке нажмите на «Удалить принтер». Принтер будет удалён немедленно и перестанет отображаться в списке.

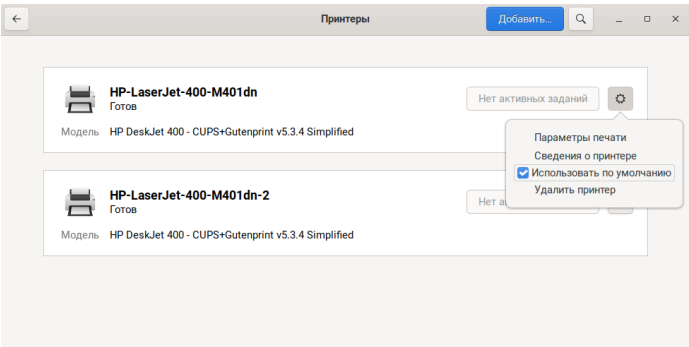


Изменение принтера по умолчанию

Откройте приложение «**Настройки**» любым удобным способом и перейдите в раздел «**Принтеры**».

Для любой учётной записи (кроме суперпользователя) при начальном входе некоторые настройки будут заблокированы. Для разблокировки необходимо пройти аутентификацию.

Выберите необходимый принтер из списка и нажмите на значок «Шестерёнки», в открывшемся выпадающем списке поставьте галочку в пункте «Использовать по умолчанию».

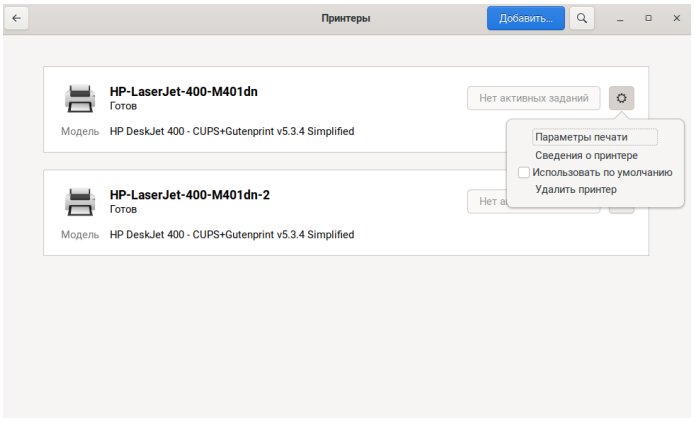


Настройка параметров печати

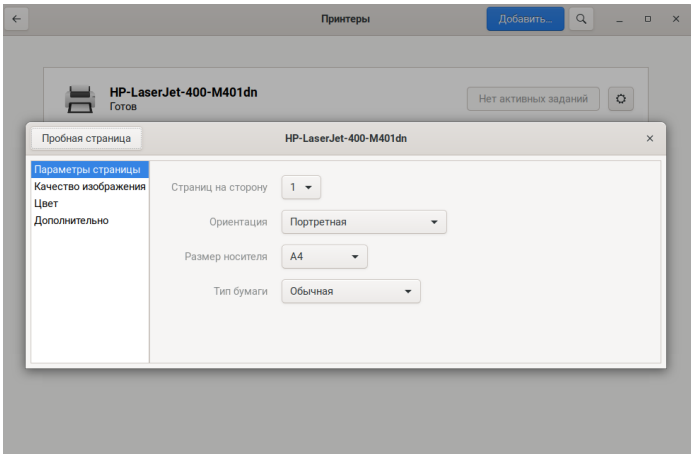
Откройте приложение «**Настройки**» любым удобным способом и перейдите в раздел «**Принтеры**».

Для любой учётной записи (кроме суперпользователя) при начальном входе некоторые настройки будут заблокированы. Для разблокировки необходимо пройти аутентификацию.

Выберите необходимый принтер из списка и нажмите на значок «Шестерёнки», в открывшемся выпадающем списке выберите «Параметры печати».



В открывшемся окне с названием принтера вы можете настроить все необходимые параметры.



Добавление водяных знаков (watermark) на документах при печати

Функция добавления водяных знаков на печатаемых документах в МСВСфера ОС реализована с помощью фильтра для системы печати cups. Фильтр работает таким образом, что в момент печати он перехватывает отправляемый на печать документ и добавляет в него фоном PDF-документ, содержащий водяные знаки. С помощью этого фильтра вы можете добавить водяные знаки на любой печатаемый документ — PDF-документ, изображение, текстовый или табличный документ любого формата. Функция также распространяется на печать из браузера.

PDF-документ, содержащий водяные знаки, находится в `/usr/share/cups/data/default-watermark.pdf`.

Вы также можете создать свой собственный PDF-документ с требуемыми водяными знаками и положить его по следующему адресу `/usr/share/cups/data/custom-watermark.pdf`. После этого водяные знаки будут браться уже из вашего PDF-документа.

Для начала работы с фильтром установите пакет `cups-filter-watermark` следующей командой (и при необходимости перезагрузите компьютер):

```
$ sudo dnf install cups-filter-watermark
```

Удалённое подключение USB-устройств по сети

Введение

USBIP — программное обеспечение, которое позволяет подключать по сети USB-устройства, физически подключённые к удалённому компьютеру, и использовать их так же, как если бы они были подключены к локальному компьютеру. Далее компьютер, к которому физически подключено USB-устройство, будет называться сервером, а тот, который будет использовать это устройство по сети — клиентом.

Обязательные условия

Для работы USBIP необходимо, чтобы клиент имел доступ к порту `3240` сервера. Пользователь, который настраивает USBIP на клиенте и на сервере, должен иметь административный доступ (`sudo`).

Установка и настройка ПО

Для установки USBIP и на сервере, и на клиенте нужно выполнить следующую команду:

```
$ sudo dnf install usbip kmod-usbip
```

Для установки графического интерфейса выполните следующую команду:

```
$ sudo dnf install usbip-gui
```

Настройка автоматического запуска служб

На сервере необходимо включить службу `usbip-server`:

```
$ sudo systemctl enable --now usbip-server
```

На клиенте — включить службу `usbip-client`:

```
$ sudo systemctl enable --now usbip-client
```

Настройка межсетевого экрана firewalld

Предупреждение

В приложении не реализованы функции аутентификации и авторизации при организации удалённого доступа к службе USBIP. Поэтому администратор должен настроить межсетевой экран таким образом, чтобы удалённый доступ был возможен только с авторизованных рабочих мест с фиксированными IP-адресами.

Настройка доступа при помощи межсетевого экрана firewalld

Для доступа USBIP удалённые компьютеры подключаются к порту `3240` по протоколу TCP. Например, чтобы открыть доступ к USBIP для компьютера, имеющего адрес `192.168.1.10`, нужно выполнить следующие команды:

```
$ sudo firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source address="192.168.1.10
↪" port port="3240" protocol="tcp" accept'
```

При необходимости повторить выполнение команд для дополнительных адресов, после этого перезапустить `firewalld`:

```
$ sudo systemctl restart firewalld
```

Альтернативный способ

Создать новую зону, например, `allowedips`:

```
$ sudo firewall-cmd --permanent --new-zone=allowedips
```

Добавить доверенные IP-адреса в список источников (sources) этой зоны:

```
# Для 192.168.1.10
$ sudo firewall-cmd --permanent --zone=allowedips --add-source=192.168.1.10
```

```
# Для 192.168.1.20
$ sudo firewall-cmd --permanent --zone=allowedips --add-source=192.168.1.20
```

Открыть порт `3240/tcp` в созданной зоне:

```
$ sudo firewall-cmd --permanent --zone=allowedips –add-port=3240/tcp
```

Применить изменения:

```
$ sudo systemctl –reload firewalld
```

Настройка привязки устройства на сервере

Чтобы на стороне сервера сделать устройство доступным по сети, его нужно привязать к службе `usbipd`. Для этого нужно выполнить следующие действия. Предположим, нам нужно передать на клиентский компьютер USB-устройство «Aktiv Rutoken ECP». Сначала выясним идентификатор шины устройства. Для этого необходимо выполнить команду:

```
$ usbip list -l
- busid 1-1.2 (2357:0604)
  TP-Link : unknown product (2357:0604)

- busid 1-1.3 (17ef:60ee)
  Lenovo : unknown product (17ef:60ee)

- busid 1-1.4 (046d:c52b)
  Logitech, Inc. : Unifying Receiver (046d:c52b)

- busid 1-3 (0a89:0030)
  Aktiv : Rutoken ECP (0a89:0030)

- busid 1-7.1 (0d8c:0103)
  C-Media Electronics, Inc. : CM102-A+/102S+ Audio Controller (0d8c:0103)

- busid 1-7.2 (046d:082d)
  Logitech, Inc. : HD Pro Webcam C920 (046d:082d)
```

Из приведённого вывода команды видно, что значение `busid` (идентификатор шины) устройства `Rutoken ECP` равно `1-3`.

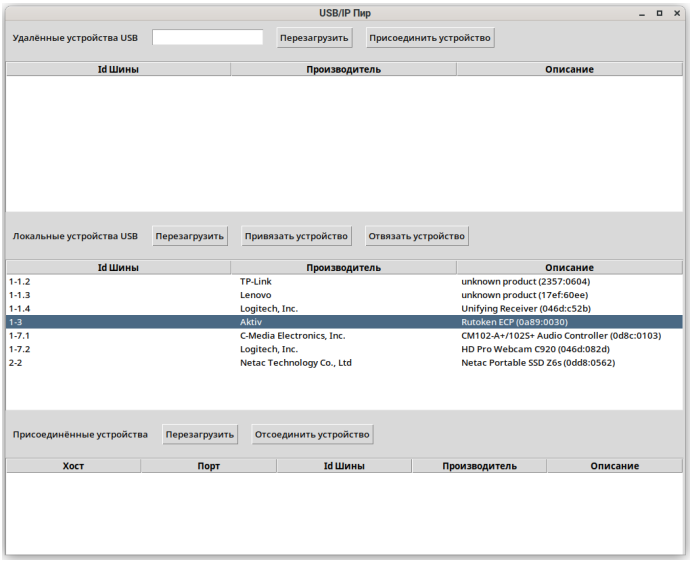
Далее необходимо выполнить привязку устройства:

```
$ sudo usbip bind -b 1-3
usbip: info: bind device on busid 1-3: complete
```

Для отключения устройства используется команда `unbind`:

```
$ sudo usbip unbind -b 1-3
usbip: info: unbind device on busid 1-3: complete
```

Эту же операцию можно выполнить при помощи графического интерфейса. Для этого запустите утилиту «Управление USBIP» из главного меню. В разделе «Локальные устройства USB» найдите нужное устройство, выделите его и нажмите кнопку «Привязать устройство». Для отключения устройства выделите устройство и нажмите кнопку «Отвязать устройство».



Подключение устройства к клиенту

Чтобы подключить устройство к клиенту, сначала нужно выполнить просмотр устройств, доступных на сервере. Для этого выполните команду:

```
$ sudo usbip list -r 192.168.10.62
Exportable USB devices
======================
- 192.168.10.62
      1-3: Aktiv : Rutoken ECP (0a89:0030)
         : /sys/devices/pci0000:00/0000:00:14.0/usb1/1-3
         : (Defined at Interface level) (00/00/00)
```

Где `192.168.10.62` — адрес сервера (можно указать также имя узла).

Таким образом видно, что устройство с `busid 1-3` привязано на сервере.

Подключение устройства:

```
$ sudo usbip attach -r 192.168.10.62 -b 1-3
```

Проверка подключения устройства:

```
$ lsusb | grep Rutoken
Bus 003 Device 004: ID 0a89:0030 Aktiv Rutoken ECP
```

Как видно, устройство `Rutoken` теперь подключено к клиентскому компьютеру.

Для отключения устройства сначала нужно определить, к какому порту виртуального хаба подключено устройство.

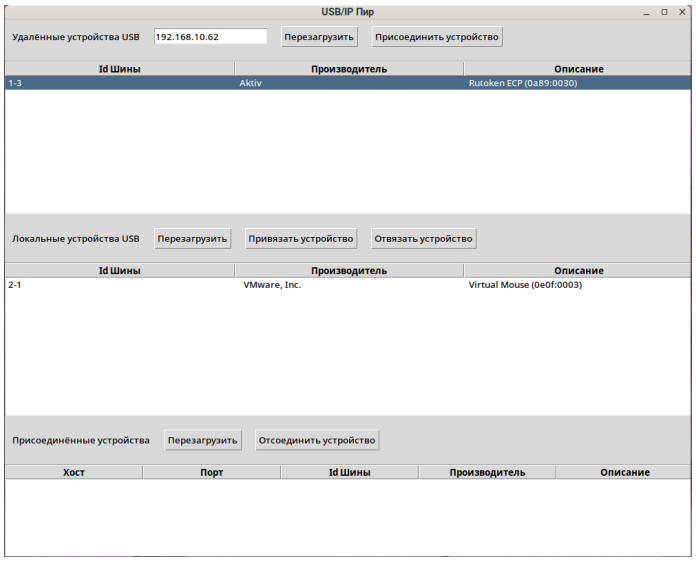
```
$ sudo usbip port
Imported USB devices
====================
Port 00: <Port in Use> at Full Speed(12Mbps)
     Aktiv : Rutoken ECP (0a89:0030)
     3-1 -> usbip://192.168.10.62:3240/1-3
         -> remote bus/dev 001/027
```

Из этого вывода видно, что устройство подключено к порту `0`. Теперь можно отключить его:

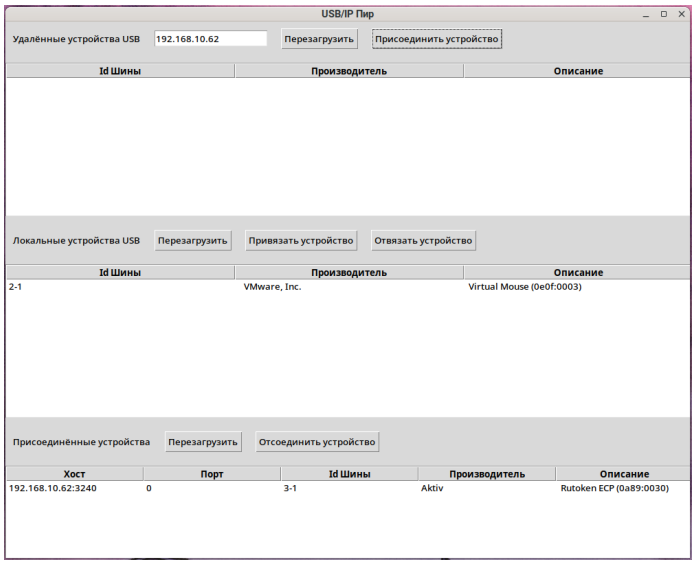
```
$ sudo usbip detach -p 0
usbip: info: Port 0 is now detached!
```

Подключение с использованием графического интерфейса

Для подключения устройства с помощью графического интерфейса запустите утилиту «Управление USBIP», введите адрес сервера в поле «Удалённые устройства USB» и нажмите кнопку «Перезагрузить». После этого устройство должно появиться в списке доступных. Для подключения устройства выделите его и нажмите кнопку «Присоединить устройство».



После этого устройство пропадает из списка доступных и появляется в списке присоединённых.



Для отключения выделите устройство в списке присоединённых и нажмите кнопку «Отсоединить устройство».

Управление пакетами

Введение и основные понятия

МСВСфера 9 АРМ представляет собой комплексную систему, которая обеспечивает стабильную и безопасную работу для пользователей.

Так как МСВСфера 9 АРМ собрана на базе ядра Linux, то в ней несколько приложений могут использовать одни и те же библиотеки или, например, одно приложение может использовать другое. С одной стороны это даёт возможность освободить место, занимаемое приложением, и снизить потребление ресурсов, а с другой стороны возникает необходимость обеспечения целостности системы.

Информация о всех необходимых приложению бинарных и конфигурационных файлах, о том, как их следует разместить в файловой системе, а также данные о зависимостях хранится в архиве специального формата, называемом **пакетом**.

В МСВСфера 9 АРМ форматом пакета является RPM (рекурсивный акроним RPM Package Manager, ранее Red Hat Package Manager), а сами файлы, содержащие пакеты, имеют расширение `.rpm`.

Как было упомянуто выше, приложения могут совместно использовать одни и те же библиотеки или даже целые программы, и здесь возникает понятие **зависимости**: в приложении может не хватать чего-то для работы, и ему для этого нужно другое приложение или библиотека. То есть один пакет начинает зависеть от другого. И удалив, например, одну библиотеку можно нарушить работу сразу нескольких приложений.

Для работы с пакетами и обеспечения целостности системы используются программы, называемые **пакетными менеджерами**. Они управляют пакетами: устанавливают, удаляют, обновляют, ведут учёт, выводят информацию, отслеживают версии и зависимости и пр..

В МСВСфера 9 АРМ пакетным менеджером является **DNF**.

Так как пакеты зависят друг от друга, то зачастую недостаточно установить только один пакет — нужно устанавливать сразу несколько, поэтому разработчики создают и поддерживают специальные централизованные серверы, называемые **репозиториями**, где хранятся различные пакеты. Пакетный менеджер видит зависимости каждого пакета, сам находит подходящие пакеты в репозитории и предлагает их установить.

Дистрибутив МСВСфера 9 АРМ имеет набор собственных репозиториев для всех поддерживаемых выпусков и архитектур, в которых содержится огромное количество приложений и программ.

Обычно некоторые пакеты, которые часто используют вместе, объединены в **группы**. Посмотреть список доступных групп поможет пакетный менеджер DNF.

Кроме групп также есть **модули**, которые тоже содержат сразу несколько пакетов, но при этом пакеты в модуле связаны версиями.

Пакетный менеджер DNF

Рассмотрим основные операции с пакетами, которые может выполнить пакетный менеджер DNF.

Найти нужный пакет

Для поиска пакета (даже не зная его точного имени) выполните следующую команду:

```
$ dnf search имя_пакета
```

В имени пакета вы можете использовать шаблоны, а также указывать только те буквы из названия, которые помните.

Пример: найдём пакет по первым буквам:

```
$ dnf search *fox
==== Имя совпадение: *fox ==================
firefox.x86_64 : Mozilla Firefox Web browser
```

Установить нужный пакет

Для установки пакета выполните следующую команду:

```
$ dnf install имя_пакета
```

DNF проверит все зависимости и при обнаружении нужных, но ещё не установленных пакетов, установит их, пользуясь всеми доступными репозиториями.

Пример: установим пакет `firefox.x86_64` :

```
$ sudo dnf install firefox.x86_64
Зависимости разрешены.
================================================================================
Пакет              Архитектура Версия                    Репозиторий Размер
================================================================================
Установка:
 firefox           x86_64      102.14.0-2.el9_2.inferit appstream   107 M

Установка зависимостей:
 sphere-indexhtml  noarch      9-3.el9                   appstream   33 k

Результат транзакции
================================================================================
Установка  2 Пакета

Объем загрузки: 107 M
Объем изменений: 276 M
Продолжить? [д/Н]: д
Загрузка пакетов:
(1/2): sphere-indexhtml-9-3.el9.noarch.rpm          170 kB/s |  33 kB     00:00
(2/2): firefox-102.14.0-2.el9_2.inferit.x86_64.rpm  7.7 MB/s | 107 MB     00:13
--------------------------------------------------------------------------------
Общий размер                                        7.6 MB/s | 107 MB     00:14
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Выполнение транзакции
 Подготовка       :                                        1/1
 Установка        : sphere-indexhtml-9-3.el9.noarch        1/2
 Установка        : firefox-102.14.0-2.el9_2.inferit.x86_64   2/2
 Запуск скриптлета: firefox-102.14.0-2.el9_2.inferit.x86_64   2/2
 Проверка         : firefox-102.14.0-2.el9_2.inferit.x86_64   1/2
 Проверка         : sphere-indexhtml-9-3.el9.noarch        2/2

Установлен:
 firefox-102.14.0-2.el9_2.inferit.x86_64  sphere-indexhtml-9-3.el9.noarch

Выполнено!
```

Обновить установленные пакеты

Для проверки наличия обновлений выполните следующую команду:

```
$ dnf check-upgrade

MSVSphere 9 - AppStream          7.2 MB/s | 9.6 MB     00:01
MSVSphere 9 - BaseOS             4.2 MB/s | 3.6 MB     00:00
MSVSphere 9 - CRB                3.0 MB/s | 2.7 MB     00:00
MSVSphere 9 - Extras             1.8 MB/s | 989 kB     00:00

NetworkManager.x86_64            1:1.42.2-6.el9_2.inferit  baseos
NetworkManager-adsl.x86_64       1:1.42.2-6.el9_2.inferit  baseos
NetworkManager-bluetooth.x86_64  1:1.42.2-6.el9_2.inferit  baseos
NetworkManager-libnm.x86_64      1:1.42.2-6.el9_2.inferit  baseos
NetworkManager-team.x86_64       1:1.42.2-6.el9_2.inferit  baseos
NetworkManager-tui.x86_64        1:1.42.2-6.el9_2.inferit  baseos
NetworkManager-wifi.x86_64       1:1.42.2-6.el9_2.inferit  baseos
NetworkManager-wwan.x86_64       1:1.42.2-6.el9_2.inferit  baseos
```

Для обновления всей системы выполните следующую команду:

```
$ sudo dnf upgrade
```

Для обновления определённого пакета (и его зависимостей) выполните следующую команду:

```
$ sudo dnf upgrade имя_пакета
```

Удалить установленный пакет

Для удаления пакета выполните следующую команду:

```
$ dnf remove имя_пакета
```

Пример: удалим пакет `firefox.x86_64`:

```
$ sudo dnf remove firefox.x86_64
Зависимости разрешены.
================================================================================
 Пакет               Архитектура  Версия                     Репозиторий  Размер
================================================================================
Удаление:
firefox              x86_64       102.9.0-3.el9_1.inferit.3  @appstream   276 M
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Удаление
неиспользуемых
зависимостей:
sphere-indexhtml     noarch        9-3.el9                   @appstream   35 k

Результат транзакции
================================================================================
Удаление  2 Пакета

Освобожденное место: 276 M
Продолжить? [д/Н]: д
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
 Подготовка       :                                                 1/1
 Запуск скриптлета: firefox-102.9.0-3.el9_1.inferit.3.x86_64    1/2
 Удаление         : firefox-102.9.0-3.el9_1.inferit.3.x86_64    1/2
 Запуск скриптлета: firefox-102.9.0-3.el9_1.inferit.3.x86_64    1/2
 Удаление         : sphere-indexhtml-9-3.el9.noarch             2/2
 Запуск скриптлета: sphere-indexhtml-9-3.el9.noarch             2/2
 Проверка         : firefox-102.9.0-3.el9_1.inferit.3.x86_64    1/2
 Проверка         : sphere-indexhtml-9-3.el9.noarch             2/2

Удален:
 firefox-102.9.0-3.el9_1.inferit.3.x86_64   sphere-indexhtml-9-3.el9.noarch
```

Вы можете увидеть, что также были удалены все пакеты, которые зависят от удаляемого.

Проверить целостность пакета

Для проверки целостности rpm-пакета выполните следующую команду:

```
$ rpm -V имя_rpm_пакета
```

В результате работы команды будет указана следующая информация:

- размер пакета
- полномочия
- тип
- владелец
- группа
- MD5-сумма
- дата последнего изменения пакета

Получить информацию об установленном пакете

Для получения подробной информации об установленном пакете выполните следующую команду:

```
$ dnf info имя_пакета
```

Пример работы команды для пакета `firefox.x86_64`:

```
$ dnf info firefox.x86_64
Установленные пакеты
Имя          : firefox
Версия       : 102.14.0
Выпуск       : 2.el9_2.inferit
Архитектура  : x86_64
Размер       : 276 M
Источник     : firefox-102.14.0-2.el9_2.inferit.src.rpm
Репозиторий  : @System
Из репозитор : appstream
Краткое опис : Mozilla Firefox Web browser
URL          : https://www.mozilla.org/firefox/
Лицензия     : MPLv1.1 or GPLv2+ or LGPLv2+
Описание     : Mozilla Firefox is an open-source web browser, designed for standards
             : compliance, performance and portability.
```

Рассмотрим основные операции с модулями.

Посмотреть список доступных модулей

Для просмотра списка доступных модулей выполните следующую команду:

```
$ dnf module list
```

Установить выбранный модуль

Для установки выбранного модуля выполните следующую команду:

```
$ sudo dnf module install имя_модуля:версия
```

Например, для установки модуля `ruby:3.1` используйте следующую команду:

```
$ sudo dnf module install ruby:3.1
```

Удалить указанный модуль

Для удаления указанного модуля выполните следующую команду:

```
$ sudo dnf module remove имя_модуля:версия
```

Например, для удаления пакета `ruby:3.1` используйте следующую команду:

```
$ sudo dnf module remove ruby:3.1
```

Описание репозиториев МСВСфера 9 АРМ

Рассмотрим репозитории МСВСфера 9 АРМ.

- **MSVSphere 9 - AppStream** — приложения общего назначения.
- **MSVSphere 9 - BaseOS** — базовый набор пакетов операционной системы.
- **MSVSphere 9 - CRB** — дополнительные пакеты для разработчиков.
- **MSVSphere 9 - Extras** — набор дополнительных приложений.
- **MSVSphere 9 - HighAvailability** — пакеты для создания кластеров высокой доступности.
- **MSVSphere 9 - NFV** — компоненты для виртуализации сетевых служб.
- **MSVSphere 9 - ResilientStorage** — пакеты для создания кластерных хранилищ.
- **MSVSphere 9 - RT** — набор пакетов для системы реального времени.

Посмотреть список включённых и доступных репозиториев

Для просмотра списка включенных репозиториев выполните следующую команду:

```
$ dnf repolist
```

Для просмотра списка включенных и отключенных репозиториев выполните следующую команду:

```
$ dnf repolist all
```

Для вывода подробного описания для каждого включенного репозитория выполните следующую команду:

```
$ dnf repolist -v
```

Для вывода списка отключённых репозиториев выполните следующую команду:

```
$ dnf repolist disabled
```

Для получения подробной информации о конкретном репозитории выполните следующую команду:

```
$ dnf repolist название репозитория -v
```

Пример: вывести подробную информацию о репозитории BaseOS:

```
$ dnf repolist BaseOS -v
...
...
ИД репозитория             : baseos
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Имя репозитория             : MSVSphere 9 - BaseOS
Статус репозитория          : включено
Версия репозитория          : 9.2
Метки дистрибутива          : [cpe:/o:ncsd:msvsphere:9]:  , 9, M, S, S, V, e, e, h, p, r
Репозиторий обновлен        : Пт 25 авг 2023 15:33:16
Пакеты репозитория          : 1 164
Пакеты-в-репозитории        : 1 164
Размер-репозитория          : 1.2 G
Зеркала-репозитория         : https://mirrors.inferitos.ru/mirrorlist/9/baseos
Базовый-URL-репозитория     : https://repo1.msvsphere-os.ru/msvsphere/9/isos/x86_64/ (0 more)
Истечение срока репозитория: 86 400 секунд(а) (осталось: Пт 25 авг 2023 16:05:43)
Имя файла репозитория       : /etc/yum.repos.d/msvsphere-baseos.repo
Всего пакетов               : 1 164
```

Здесь мы видим, что репозиторий включен, количество пакетов в репозитории и его размер, а также другие важные параметры.

Зеркала репозитория — это серверы, дублирующие содержимое этого репозитория. Они позволяют снизить нагрузку с основных серверов.

Добавить в систему сторонний репозиторий

Иногда возникает необходимость установить приложение, которого нет в имеющихся репозиториях. В этом случае есть возможность добавить в систему сторонний репозиторий.

Важно

Рекомендуем быть предельно осторожными при подключении сторонних репозиториев и тщательно соблюдать меры безопасности.

Вы можете подключить сторонний репозиторий, если есть `.repo`-файл, с помощью следующей команды:

```
$ dnf config-manager --add-repo путь_к_.repo_файлу
```

Пример подключения `.repo`-файла docker.io:

```
$ dnf config-manager --add-repo https://download.docker.com/linux/rhel/docker-ce.repo
```

Включить или отключить репозиторий

Вы можете по необходимости временно включать и отключать репозитории, чтобы установить приложение из конкретного репозитория. При этом репозиторий не будет удалён.

Команда включения репозитория:

```
$ sudo dnf config-manager --set-enabled имя_репозитория
```

Команда отключения репозитория:

```
$ sudo dnf config-manager --set-disabled имя_репозитория
```

При необходимости вы можете вывести справку по команде `config-manager`:

```
$ dnf config-manager --help-cmd
```

Безопасность

Использование сторонних репозиториев/пакетов

Так как сторонние репозитории и пакеты загружаются из Интернета, то при их скачивании и установке необходимо быть уверенными в безопасности устанавливаемых приложений. Важно быть уверенным, что никакая третья сторона не изменяла содержимое пакета при передаче его от автора к пользователю. Подписание пакета является способом защиты пакета для конечного пользователя. Поэтому репозитории и все пакеты в них подписываются специальным цифровым ключом.

Приватный ключ есть только у разработчиков. Публичный ключ может располагаться на сайте репозитория, либо распространяться вместе с операционной системой.

Разработчики подписывают пакеты приватным ключом, а с помощью публичного ключа конечный пользователь может убедиться, что это тот самый пакет и никакая третья сторона не изменяла его.

Ниже мы рассмотрим, как проверить цифровую подпись пакета.

Цифровые подписи пакетов и их проверка

Для проверки цифровой подписи пакета выполните следующую команду (находясь в папке с пакетом):

```
$ rpm --checksig имя_пакета.rpm
```

Пример: проверим цифровую подпись пакета `VirtualBox-7.0-7.0.10_158379_el9-1.x86_64.rpm`:

```
$ rpm --checksig VirtualBox-7.0-7.0.10_158379_el9-1.x86_64.rpm
VirtualBox-7.0-7.0.10_158379_el9-1.x86_64.rpm: rsa sha1 (md5) pgp md5 OK
```

Вы можете также использовать опцию `-v` для вывода более полной информации о проверке.

Идентификация и аутентификация

Введение

Средства идентификации и аутентификации предоставляют возможности идентификации объектов доступа, идентификации и проверки подлинности субъектов доступа при входе в систему и при доступе к защищаемым объектам, управления идентификаторами, в том числе их создания, присвоения и уничтожения, управления аутентификационными данными, в том числе их инициализации, защищенного хранения, блокирования и разблокирования, проверки соответствия аутентификационной информации заданной метрике качества, защиты обратной связи при вводе аутентификационной информации, а также другие возможности.

Добавление нового пользователя

Для добавления нового пользователя используется утилита `useradd`. Она позволяет добавить учетную запись нового пользователя. Режимы ее работы и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 1: Опции утилиты `useradd` и их значения

Опция	Значение
`-c, --comment`	Любая текстовая строка. Используется как поле для имени и фамилии пользователя, длина этого поля не должна превосходить 128 символов.
`-b, --base-dir`	Базовый системный каталог по умолчанию, если не указан другой каталог. Базовый каталог объединяется с именем учётной записи для определения домашнего каталога.
`-d, --home`	Для создаваемого пользователя в качестве начального каталога будет использован базовый каталог. По умолчанию это значение получается объединением имени пользователя с базовым каталогом и используется как имя домашнего каталога.
`-d, --home-dir`	Задать домашний каталог нового пользователя. Если данная опция не используется, то в качестве домашнего каталога выбирается каталог типа `/базовый_системный_каталог/имя_пользователя`.
`-D, --defaults`	Вывести значения стандартных опций.
`-e, --expiredate`	Дата окончания срока действия учётной записи пользователя. Задаётся в формате `ГГГГ-ММ-ДД`.
`--f, --inactive`	Число дней, которые должны пройти после окончания срока действия пароля, чтобы учётная запись заблокировалась. Если указано значение `0`, то учётная запись блокируется сразу после окончания срока действия пароля, а при значении `-1` данная возможность не используется. По умолчанию используется значение `-1`.
`-g, --gid`	Название группы нового пользователя или её идентификационный номер. Указываемое название группы или её номер должны существовать в системе.
`-G, --groups`	Список дополнительных групп, в которых числится пользователь. Перечисление групп осуществляется через запятую без пробелов. На указанные группы действуют те же ограничения, что и для группы, указанной в опции `-g`.
`-m, --create-home`	Создает начальный домашний каталог нового пользователя, если он ещё не существует. Если каталог уже существует, добавляемый пользователь должен иметь права на доступ к указанному каталогу.
`-M, --no-create-home`	Позволяет не создавать домашний каталог нового пользователя.
`-K, --key`	Используется для изменения значений по умолчанию для параметров, хранимых в конфигурационном файле `/etc/login.def`.
`-N, --no-user-group`	Позволяет добавить нового пользователя в группу, указанную в опции `-g` или заданную по умолчанию в конфигурационном файле `/etc/default/useradd`, не создавая группу, название которой совпадает с именем нового пользователя. Если опции `-g`, `-N`, `-U` не указаны, то настройки групп по умолчанию определяются в конфигурационном файле `/etc/login.defs`.
`-o, --non-unique`	Позволяет создать учётную запись с уже имеющимся, не уникальным идентификатором.
`-p, --password`	Позволяет задать новый пароль для учётной записи.
`-r, --system`	Позволяет создать системную учётную запись. По умолчанию для данной категории учетных записей домашний каталог не создаётся вне зависимости от значения соответствующего параметра конфигурационного файла `/etc/login.defs`. Для создания домашнего каталога системного пользователя необходимо вместе с опцией `-r` задать опцию `-m`.
`-s, --shell`	Полный путь к программе, используемой в качестве начального командного интерпретатора для пользователя сразу после регистрации. Длина этого поля не должна превосходить 256 символов. Если задать пустое значение, то будет использоваться оболочка по умолчанию.
`-u, --uid`	Позволяет задать идентификационный номер (численное неотрицательное значение идентификатора) пользователя. Это значение должно быть уникальным, если не задействована опция `-o`.
`U, --user-group`	Позволяет создать группу, название которой совпадает с именем пользователя, присоединив данного пользователя к этой группе.
`-h, --help`	Показать краткую справку об утилите.

Пример: создадим пользователя с именем `user` и зададим для него основную группу `users` и две дополнительные группы `ftp` и `developers`, к которым он будет приписан.

Для этого выполним следующую команду:

```
$ sudo useradd -g users -G ftp,developers user
```

Изменение уже имеющихся пользовательских записей

Для изменения уже имеющихся пользовательских записей используется утилита `usermod`. Она позволяет изменить данные существующей учётной записи пользователя. Режимы ее работы и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 2: Опции утилиты `usermod` и их значения

Опция	Значение
`-a, --append`	Добавить пользователя в дополнительную группу. Следует использовать только вместе с параметром `-G`.
`-c, --comment`	Новое значение поля комментария.
`d, --home`	Новый домашний каталог учётной записи. Если указан параметр `-m`, то содержимое текущего домашнего каталога будет перемещено в новый домашний каталог, который будет создан, если он ещё не существует.
`-e, --expiredate`	Установить дату окончания срока действия учётной записи в формате `ГГГГ-ММ-ДД`.
`-f, --inactive`	Установить пароль после окончания срока действия учётной записи в `INACTIVE`. Если указано значение `0`, то учётная запись блокируется сразу после окончания срока действия пароля, а при значении `-1` данная возможность не используется. По умолчанию используется значение `-1`.
`-g, --gid`	Принудительно назначить первичную группу.
`-G, --groups`	Список дополнительных групп.
`-l, --login`	Новое значение учётной записи.
`-L, --lock`	Заблокировать пароль пользователя. Это делается помещением символа `!` в начало шифрованного пароля, что приводит к его блокировке. Не следует использовать этот параметр вместе с `-p` или `-U`.
`-m, --move-home`	Переместить содержимое домашнего каталога пользователя в новое место. Если новый домашний каталог не существует, то он создаётся автоматически. Данная опция используется только вместе с опцией `-d`.
`-o, --non-unique.`	При использовании с параметром `-u` этот параметр позволяет указывать не уникальный числовой идентификатор пользователя.
`-p, --password`	Задать новый пароль для учётной записи.
`-s, --shell`	Задать новую оболочку для учётной записи.
`-u, --uid`	Новый идентификационный номер для учётной записи.
`-U, --unlock`	Разблокировать учетную запись.

Пример: изменим срок действия учётной записи пользователя с идентификатором `user6`.

Для этого выполним следующую команду:

```
$ sudo usermod -e 2020-05-01 user6
```

где 2020-05-01 — дата истечения срока действия учётной записи в формате `ГГГГ-ММ-ДД`.

Пример: изменим идентификатор (значение учётной записи) пользователя с `user6` на `user7`.

Для этого выполним следующую команду:

```
$ sudo usermod -l user7 user6
```

Удаление пользователей

Для удаления пользователей используется утилита `userdel`. Она позволяет удалить существующую учетную запись пользователя. Режимы ее работы и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 3: Опции утилиты `userdel` и их значения

Опция	Значение
`-f, --force`	С этой опцией учётная запись будет удалена, даже если пользователь в этот момент работает в системе. Она также заставляет утилиту удалить домашний каталог пользователя и почтовый ящик, даже если другой пользователь использует тот же домашний каталог или если почтовый ящик не принадлежит данному пользователю. **Внимание! Перед использованием этого параметра убедитесь в необходимости этого действия! Этот параметр может привести систему в нерабочее состояние!**
`-r, --remove`	Файлы в домашнем каталоге пользователя будут удалены вместе с самим домашним каталогом и почтовым ящиком. Пользовательские файлы, расположенные в других файловых системах, нужно искать и удалять вручную.
`-n`	Задает, сколько месяцев идентификатор пользователя должен устаревать перед повторным использованием. Задайте `-1`, чтобы указать, что идентификатор пользователя никогда не должен использоваться повторно. Задайте `0`, чтобы указать, что идентификатор пользователя можно немедленно использовать повторно. Если опция `-n` не задана, то идентификатор будет устаревать стандартное количество месяцев перед повторным использованием.
`-h, --help`	Показать краткую справку.

Пример: удалим пользователя с идентификатором `user7`.

Для этого выполним следующую команду:

```
$ sudo userdel -r user7
```

Добавление группы пользователей

Для добавления группы пользователей используется утилита `groupadd`. Режимы ее работы и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 4: Опции утилиты `groupadd` и их значения

Опция	Значение
`-f`	Вернуть статус успешного выполнения, если группа уже существует. Если используется вместе с параметром `-g` и указанный идентификатор группы уже существует, то выбирается другой уникальный идентификатор группы, то есть параметр `-g` игнорируется.
`-g`	Числовое значение идентификатора группы. Значение должно быть уникальным, если не задан параметр `-o`. Значение должно быть не отрицательным. По умолчанию берётся значение больше 999 и больше идентификатора любой другой группы. Значения от 0 и до 999 обычно зарезервированы под системные группы.
`-K`	Изменить значения по умолчанию для параметров, которые хранятся в конфигурационном файле `/etc/login.defsм`.
`-o`	Разрешить добавление группы с не уникальным идентификатором.
`-r, --system`	Создать системную группу.
`-h, --help`	Показать краткую справку.

Пример: создадим группу `group2` с числовым значением идентификатора `8285`.

Для этого выполним следующую команду:

```
$ sudo groupadd group2 -g 8285
```

Изменение существующей группы пользователей

Для изменения существующей группы пользователей используется утилита `groupmod`. Режимы ее работы и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 5: Опции утилиты `groupmod` и их значения

Опция	Значение
`-g, --gid`	Изменить идентификатор группы.
`-n, --new-name`	Изменить имя группы.
`-o, --non-unique`	Позволяет использовать не уникальный идентификатор группы.
`-p, --password`	Изменить пароль.
`-h, --help`	Показать краткую справку.

Пример: изменим идентификатор группы пользователей `users` на `ftp`.

Для этого выполним следующую команду:

```
$ sudo groupmod -g ftp users
```

Удаление существующей группы пользователей

Для удаления существующей группы пользователей используется утилита `groupdel`. Утилита позволяет удалить определение группы из системы путем удаления записи о соответствующей группе из файла `/etc/group`. Однако она не удаляет идентификатор группы из файла паролей. Удаленный идентификатор действует для всех файлов и каталогов, которые его имели.

Пример: удалим группу с именем `group3`.

Для этого выполним следующую команду:

```
$ sudo groupdel group3
```

Создание и изменение пароля пользователя

Для создания и изменения пароля пользователя (в том числе для блокировки учётной записи пользователя) используется утилита `passwd`. Обычный пользователь может изменить пароль только своей учётной записи, суперпользователь `root` может изменить пароль любой учётной записи.

При изменении пароля проверяется информация об устаревании пароля, чтобы убедиться, что пользователю разрешено изменять пароль в настоящий момент. Если выяснится, что не разрешено, то утилита не производит изменение пароля и завершает работу.

При изменении пароля пользователь должен будет сначала ввести старый пароль, если он был. Введенное пользователем значение старого пароля зашифровывается и сравнивается со значением зашифрованного текущего пароля. Затем пользователю необходимо будет дважды ввести новый пароль. Значение второго ввода сравнивается с первым, и они должны совпасть. После этого пароль тестируется на сложность подбора, т.е. его значение не должно быть легко угадываемым.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 6: Опции утилиты `passwd` и их значения

Опция	Значение
`-a, --all`	Эту опцию можно использовать только вместе с `-S` для вывода статуса всех пользователей.
`-d, --delete`	Удалить пароль пользователя (сделать его пустым). Это быстрый способ заблокировать пароль учётной записи.
`-e, --expire`	Немедленно сделать пароль устаревшим. Это заставит пользователя изменить пароль при следующем входе в систему.
`-i, --inactive`	Эта опция используется для блокировки учётной записи по прошествии заданного числа дней после устаревания пароля. То есть если пароль устарел и прошло больше дней, чем указано, то пользователь больше не сможет использовать свою учётную запись.
`-l, --lock`	Заблокировать указанную учётную запись. Эта опция блокирует учётную запись путем изменения значения пароля на такое, которое не может быть ранее указанным зашифрованным паролем.
`-m, --mindays`	Задать минимальное количество дней между сменой пароля. Нулевое значение этого поля указывает на то, что пользователь может менять свой пароль тогда, когда захочет.
`-S, --status`	Показать состояние учётной записи. Информация о состоянии содержит семь полей. Первое поле содержит имя учётной записи. Второе поле указывает, заблокирована ли учётная запись, она без пароля или у неё есть рабочий пароль. Третье поле хранит дату последнего изменения пароля. В следующих четырёх полях хранятся минимальный срок, максимальный срок, период выдачи предупреждения и период неактивности пароля. Все эти сроки измеряются в днях.
`-u, --unlock`	Разблокировать указанную учётную запись. Этот параметр активирует учётную запись путем изменения пароля на прежнее значение, которое было перед использованием параметра `-l`.
`-w, --warndays`	Установить число дней выдачи предупреждения, перед тем как потребуется смена пароля.
`-x, --maxdays`	Установить максимальное количество дней, в течение которых пароль остаётся рабочим, после чего его надо будет изменить.
`-h, --help`	Показать краткую справку.

Пример: зададим пароль пользователю `user4`. Работа команды `passwd`:

```
$ sudo passwd user4
Изменяется пароль пользователя user4.
Новый пароль :
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
```

Пример: посмотрим состояние учётной записи `user4`. Работа команды `passwd`:

```
$ sudo passwd -S user4
user4 PS 2023-07-04 0 99999 7 -1 (Пароль задан, шифр SHA512.)
```

Где:

- `user4` — имя пользователя.
- `PS` — статус пароля.
- `2023-07-04` — отображает время последнего изменения пароля.
- `0` и `99999` — минимальный и максимальный срок действия пароля.
- `7` — срок вывода предупреждения.

- `-l` — срок деактивации пароля.

Изменение срока действия учётной записи и пароля пользователя

Утилита `chage` позволяет установить дату завершения срока действия учётной записи пользователя, минимальный и максимальный срок действия пароля, дату завершения срока действия пароля, а также количество дней, в течение которых пользователю будут выводиться предупреждения о приближении завершения срока действия пароля.

Командой `chage` может пользоваться только суперпользователь, за исключением использования её с параметром `-l`, который позволяет непривилегированным пользователям определить время, когда истекает их личный пароль или учетная запись.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 7: Опции утилиты `chage` и их значения

Опция	Значение
`-m`	Меняет значение `mindays` на минимальное число дней между сменой пароля. Значение `0` в этом поле обозначает, что пользователь может изменять свой пароль когда угодно.
`-M`	Меняет значение `maxdays` на максимальное число дней, в течение которых пароль будет действителен. Когда сумма `maxdays` и `lastday` меньше, чем текущий день, у пользователя будет запрошен новый пароль до начала работы в системе.
`-d`	Меняет значение `lastday` на день, когда пароль был изменен последний раз (число дней с 1 января 1970). Дата также может быть указана в формате `ГГГГ-ММ-ДД`.
`-E`	Используется для задания даты, с которой учетная запись пользователя станет недоступной. Дата также может быть указана в формате `ГГГГ-ММ-ДД`.
`-I`	Используется для задания количества дней «неактивности», то есть дней, когда пользователь вообще не входил в систему, после которых его учетная запись будет заблокирована. Значение `0` отключает этот режим.
`-W`	Используется для задания числа дней, когда пользователю начнет выводиться предупреждение об истечении срока действия его пароля и необходимости его изменения.
`-l`	Просмотреть текущую информацию о дате истечения срока действия пароля для пользователя.

Пример: просмотрим текущую информацию о дате истечения срока действия пароля для пользователя `user4`. Работа команды `chage`:

```
$ sudo chage -l user4
Последний раз пароль был изменён: мар 12, 2023
Срок действия пароля истекает: никогда
Пароль будет деактивирован через: никогда
Срок действия учётной записи истекает: никогда
Минимальное количество дней между сменой пароля: 0
Максимальное количество дней между сменой пароля: 99999
Количество дней с предупреждением перед деактивацией пароля: 7
```

Управление политиками паролей

В данном разделе описана процедура управления политиками паролей на локальной системе, не подключённой к LDAP-каталогу пользователей (FreeIPA, Microsoft

Active Directory и т.д.). В случае использования LDAP-каталога обратитесь к соответствующему руководству по администрированию.

Для управления политиками паролей в МСВСфера ОС используется системная утилита `authselect`, которая оперирует профилями аутентификации. В первую очередь необходимо убедиться, что выбран профиль аутентификации. Вы можете это сделать с помощью команды `authselect current`:

```
# вывод для систем, подключённых к каталогу пользователей FreeIPA
$ sudo authselect current
Profile ID: sssd
Enabled features:
- with-mkhomedir
- with-sudo

# вывод для систем, использующих профиль "minimal"
$ sudo authselect current
Profile ID: minimal
Enabled features: None

# вывод для систем, не использующих профиль authselect
$ sudo authselect current
Конфигурация не обнаружена. / No existing configuration detected.
```

Если система не настроена на использование профиля аутентификации, то необходимо выбрать его, чтобы получить возможность настраивать политики паролей.

Просмотреть список доступных профилей `authselect` вы можете следующим образом:

```
$ sudo authselect list
- minimal              Local users only for minimal installations
- sssd                 Enable SSSD for system authentication (also for local users only)
- winbind              Enable winbind for system authentication
- custom/minimal_gost  Local users only for minimal installations and gost support
- custom/sssd_gost     Enable SSSD with GOST support for system authentication (also for local␣
↪users only)
```

Выбрать профиль вы можете с помощью команды `authselect select`. Для локальной системы рекомендуется использовать профиль `minimal`:

```
$ sudo authselect select minimal --force
[error] File [/etc/authselect/system-auth] is still present
[error] File [/etc/authselect/password-auth] is still present
[error] File [/etc/authselect/fingerprint-auth] is still present
[error] File [/etc/authselect/smartcard-auth] is still present
[error] File [/etc/authselect/postlogin] is still present
[error] File [/etc/authselect/nsswitch.conf] is still present
[error] File [/etc/authselect/dconf-db] is still present
[error] File [/etc/authselect/dconf-locks] is still present
[error] Link [/etc/pam.d/system-auth] points to [/etc/authselect/system-auth]
[error] Symbolic link [/etc/pam.d/system-auth] to [/etc/authselect/system-auth] still exists!
[error] Link [/etc/pam.d/password-auth] points to [/etc/authselect/password-auth]
[error] Symbolic link [/etc/pam.d/password-auth] to [/etc/authselect/password-auth] still exists!
[error] Link [/etc/pam.d/fingerprint-auth] points to [/etc/authselect/fingerprint-auth]
[error] Symbolic link [/etc/pam.d/fingerprint-auth] to [/etc/authselect/fingerprint-auth] still␣
↪exists!
[error] Link [/etc/pam.d/smartcard-auth] points to [/etc/authselect/smartcard-auth]
[error] Symbolic link [/etc/pam.d/smartcard-auth] to [/etc/authselect/smartcard-auth] still␣
↪exists!
[error] Link [/etc/pam.d/postlogin] points to [/etc/authselect/postlogin]
[error] Symbolic link [/etc/pam.d/postlogin] to [/etc/authselect/postlogin] still exists!
[error] Link [/etc/nsswitch.conf] points to [/etc/authselect/nsswitch.conf]
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
[error] Symbolic link [/etc/nsswitch.conf] to [/etc/authselect/nsswitch.conf] still exists!
[error] Link [/etc/dconf/db/distro.d/20-authselect] points to [/etc/authselect/dconf-db]
[error] Symbolic link [/etc/dconf/db/distro.d/20-authselect] to [/etc/authselect/dconf-db] still␣
↪exists!
[error] Link [/etc/dconf/db/distro.d/locks/20-authselect] points to [/etc/authselect/dconf-locks]
[error] Symbolic link [/etc/dconf/db/distro.d/locks/20-authselect] to [/etc/authselect/dconf-
↪locks] still exists!
Backup stored at /var/lib/authselect/backups/2024-10-08-16-28-25.N8QZyv
Profile "minimal" was selected.
The following nsswitch maps are overwritten by the profile:
- aliases
- automount
- ethers
- group
- hosts
- initgroups
- netgroup
- networks
- passwd
- protocols
- publickey
- rpc
- services
- shadow
```

Проверить корректность применения профиля вы можете следующим образом:

```
$ sudo authselect current
Profile ID: minimal
Enabled features: None

$ sudo authselect check
Current configuration is valid.
```

Управление требованиями к качеству паролей

По умолчанию МСВСфера ОС предъявляет следующие требования к качеству паролей пользователя:

- пароль должен иметь длину как минимум 8 символов;
- пароль должен отсутствовать в словаре известных паролей программы `cracklib`.

За проверку качества паролей отвечает PAM-модуль `pam_pwquality`, который включён по умолчанию для всех профилей аутентификации.

Модуль настраивается через конфигурационный файл `/etc/security/pwquality.conf`, который по умолчанию имеет следующий вид (для переменных указаны значения по умолчанию, описание параметров переведено на русский язык и добавлены комментарии):

```
# Количество символов в новом пароле, которые не должны присутствовать в старом
# пароле. Значение 0 полностью отключает проверку на пересечение символов, за
# исключением попытки использования идентичного пароля.
# difok = 1

# Минимально допустимое количество символов в новом пароле (плюс один, если
# использование кредитов не отключено, что является поведением по умолчанию).
# Пароль не может быть короче 6 символов.
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# minlen = 8

# Максимальное количество кредитов, начисляемое за наличие цифр в новом пароле.
# Если значение меньше 0, то это минимальное количество цифр в новом пароле.
# dcredit = 0

# Максимальное количество кредитов, начисляемое за наличие прописных букв в
# новом пароле. Если значение меньше 0, то это минимальное количество прописных
# букв в новом пароле.
# ucredit = 0

# Максимальное количество кредитов, начисляемое за наличие строчных букв в
# новом пароле. Если значение меньше 0, то это минимальное количество строчных
# букв в новом пароле.
# lcredit = 0

# Максимальное количество кредитов, начисляемое за наличие других символов в
# новом пароле. Если значение меньше нуля, то это минимальное количество других
# символов в новом пароле.
# ocredit = 0

# Минимальное количество требуемых классов символов в новом пароле
# (цифры, буквы в нижнем регистре, буквы в верхнем регистре, другие символы).
# minclass = 0

# Максимальное количество разрешённых повторяющихся символов в новом пароле.
# Проверка отключается, если значение равно 0.
# maxrepeat = 0

# Максимальное количество повторяющихся символов из одного класса, разрешённое
# в новом пароле. Проверка отключается, если значение равно 0.
# maxclassrepeat = 0

# Проверять, есть ли слова из поля GECOS пользователя в новом пароле. Проверка
# отключается, если значение равно 0.
# gecoscheck = 0

# Проверять наличие пароля в словаре cracklib, если значение не равно 0.
# dictcheck = 1

# Проверять наличие имени пользователя в новом пароле. Проверка отключается,
# если значение равно 0.
# usercheck = 1

# Длина подстрок из имени пользователя, которую нужно проверить на наличие
# в новом пароле. Эта проверка выполняется, если значение больше 0 и значение
# usercheck равно 1.
# usersubstr = 0

# Включить принудительную проверку нового пароля пользователя, новый пароль,
# не соответствующий требованиям, будет отклонён, если значение не равно 0.
# enforcing = 1

# Путь к словарям cracklib. Если не задан, будет использован стандартный
# словарь cracklib.
# dictpath =

# Сколько раз запрашивать новый пароль пользователя прежде чем выводить ошибку.
# Значение по умолчанию - 1.
# retry = 3

# Применять требования к качеству пароля пользователя root, если опция
# раскомментирована.
# enforce_for_root

# Применять требования к качеству пароля только для локальных пользователей,
# присутсвующих в файле /etc/passwd, если эта опция раскомментирована.
# local_users_only
```

Кредиты в параметрах `dcredit`, `ucredit`, `lcredit` и `ocredit` определяют сколько баллов может быть начислено за определённый тип символов, используемый в новом пароле. Если значение параметра больше `0`, то за каждый такой символ к общей длине пароля добавляется определённое количество кредитов.

Пример: если все четыре параметра имеют значение `1` и минимально допустимая длина пароля составляет 7 символов, то при использовании всех 4 типов символов потребуется ввести пароль всего лишь из 7 символов. За каждый неиспользованный тип символа к требуемой длине пароля добавляется штраф, указанный в соответствующем параметре. Так, если не использовать цифры и строчные буквы, то минимальная длина пароля уже составит 9 символов.

Использование механизма кредитов позволяет ослабить требования к длине пароля за счёт использования символов из разных групп.

После внесения правок в конфигурационный файл `/etc/security/pwquality.conf` перезапуск каких-либо сервисов не требуется — PAM применит изменения автоматически и новые настройки будут использованы при следующем изменении пароля.

Дополнительную информацию по использованию модуля `pam_pwquality` вы можете найти в соответствующих руководствах:

- `man pam_pwquality`;
- `man pwquality.conf`.

Ограничение на повторное использование паролей

В конфигурации по умолчанию операционная система не позволяет повторно использовать только текущий пароль пользователя. Это поведение можно изменить с помощью PAM-модуля `pam_pwhistory`, который позволяет хранить историю паролей для каждого пользователя.

Для включения модуля `pam_pwhistory` выполните следующую команду:

```
$ sudo authselect enable-feature with-pwhistory
```

После этого свойство `with-pwhistory` должно появиться в свойствах текущего профиля аутентификации:

```
$ sudo authselect current
Profile ID: minimal
Enabled features:
- with-faillock
- with-pwhistory
```

Модуль настраивается через конфигурационный файл `/etc/security/pwhistory.conf`, который по умолчанию имеет следующий вид (для переменных указаны значения по умолчанию, описание параметров переведено на русский язык и добавлены комментарии):

```
# Раскомментирование этой опции включает вывод отладочной информации.
# debug

# Так же сохранять предыдущие пароли пользователя root, если эта опция
# раскомментирована.
# enforce_for_root

# Количество сохраняемых паролей для каждого пользователя.
# remember = 10

# Сколько раз запрашивать новый пароль пользователя прежде чем выводить ошибку.
# retry = 1

# Каталог, в котором будут храниться предыдущие пароли пользователей.
# file = /etc/security/opasswd
```

Исходя из описания выше, после включения модуля `pam_pwhistory`, система будет хранить последние 10 паролей для каждого пользователя и выдавать ошибку при попытке использовать сохранённый пароль в качестве нового при смене пароля.

Пример ошибки:

```
# на английском языке
$ passwd
Changing password for user test.
Current password:
New password:
Retype new password:
Password has been already used. Choose another.
passwd: Have exhausted maximum number of retries for service

# на русском языке
$ passwd
Изменение пароля пользователя test.
Текущий пароль:
Новый пароль:
Повторите ввод нового пароля:
Этот пароль уже был использован. Выберите другой.
```

Дополнительную информацию по использованию модуля `pam_pwhistory` вы можете найти в соответствующих руководствах:

- `man pam_pwhistory`;
- `man pwhistory.conf`.

Ограничение количества неуспешных попыток аутентификации

В конфигурации по умолчанию операционная система не ограничивает количество неуспешных попыток аутентификации пользователя. Однако, реализация такого ограничения возможна с помощью PAM-модуля `pam_faillock`.

Для включения модуля `pam_faillock` выполните следующую команду:

```
$ sudo authselect enable-feature with-faillock
```

После этого свойство `with-faillock` должно появиться в свойствах текущего профиля аутентификации:

```
$ sudo authselect current
Profile ID: minimal
Enabled features:
- with-faillock
```

Модуль настраивается через конфигурационный файл `/etc/security/faillock.conf`, который по умолчанию имеет следующий вид (для переменных указаны значения по умолчанию, описание параметров переведено на русский язык и добавлены комментарии):

```
# Каталог, в котором хранятся файлы с записями об ошибках аутентификации
# пользователей.
# Внимание: в случае изменения этого пути потребуется дополнительно
# перенастроить правила SELinux.
# dir = /var/run/faillock

# Раскомментирование этой опции включает логирование имён несуществующих
# пользователей в системный журнал.
# audit

# Раскомментирование этой опции отключает вывод информационных сообщений на
# консоль.
# silent

# Раскомментирование этой опции отключает вывод информационных сообщений в
# системный журнал.
# no_log_info

# Раскомментирование этой опции включает отслеживание неудачных попыток
# аутентификации только для локальных пользователей, указанных в файле
# /etc/passwd. В таком случае пользователи из LDAP-каталога будут
# игнорироваться PAM-модулем "faillock". Включение данного параметра позволяет
# избежать ситуаций с двойной блокировкой, когда пользователь будет заблокирован
# и локально, и на уровне каталога пользователей.
# local_users_only

# Блокировать доступ пользователю, если количество последовательных ошибок
# аутентификации за последний промежуток времени превышает N попыток.
# deny = 3

# Временной интервал в секундах, в течении которого ошибки аутентификации
# пользователя считаются последовательными и приводят к блокировке его учётной
# записи. Значение по умолчанию — 15 минут.
# fail_interval = 900

# Автоматически восстановить доступ к заблокированной учётной записи спустя N
# секунд после блокировки. Для перманентной блокировки учётной записи задайте
# значение 0 — в таком случае восстановление доступа будет возможно только
# вручную через команду "faillock". Значение по умолчанию — 10 минут.
# unlock_time = 600

# Раскомментирование этой опции также приведёт к блокировке пользователя
# root в случае неудачных попыток аутентификации. По умолчанию блокируются
# только обычные пользователи.
# even_deny_root

# Автоматически восстанавливать доступ к заблокированной учётной записи
# пользователя root спустя N секунд после блокировки. Если значение не
# определено, модуль "faillock" будет использовать значение параметра "unlock_time".
# root_unlock_time = 900

# Имя группы системных администраторов. Если задано, то для участников этой
# группы будут применяться те же правила, что и для пользователя root
# (к ним будут применяться параметры "even_deny_root" и "root_unlock_time").
# admin_group = <admin_group_name>
```

Исходя из описания выше, при включении PAM-модуля `pam_faillock` будет

автоматически применена следующая конфигурация: локальные пользователи и пользователи из LDAP-каталога будут блокироваться после трёх неудачных попытках входа в течении 15 минут на срок в 10 минут. Пользователь `root` блокироваться не будет.

После внесения правок в конфигурационный файл `/etc/security/faillock.conf` перезапуск каких-либо сервисов не требуется — PAM применит изменения автоматически при обработке следующего запроса на аутентификацию.

Функциональность модуля `pam_faillock` распространяется как на локальную (через графическую или текстовую консоль), так и на сетевую (с помощью SSH) аутентификацию пользователей.

Для просмотра истории неудачных попыток аутентификации пользователя за учётный период `fail_interval` вы можете использовать следующую команду (замените «USERNAME» на имя реального пользователя из вашей системы):

```
$ sudo faillock --user USERNAME
When                Type  Source                                           Valid
2024-10-08 21:12:20 RHOST 192.168.1.4                                         V
2024-10-08 21:12:25 RHOST 192.168.1.4                                         V
2024-10-08 21:12:28 RHOST 192.168.1.4                                         V
```

Для снятия блокировки учётной записи пользователя вы можете использовать следуюзую команду:

```
$ sudo faillock --user USERNAME --reset
```

Дополнительную информацию по использованию модуля `pam_faillock` вы можете найти в соответствующих руководствах:

- `man pam_faillock`;
- `man faillock`;
- `man faillock.conf`.

Получение сведений о пользователе

Утилита `id` позволяет получить сведения об указанном пользователе или о текущем пользователе, запустившем данную утилиту, если он не указал явно имя пользователя.

По умолчанию выводятся числовые идентификаторы пользователя и группы, действующие идентификаторы пользователя и группы, а также идентификаторы других групп, в которых состоит пользователь.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 8: Опции утилиты `id` и их значения

Опция	Значение
`-g, --group`	Выводит только подлинный числовой идентификатор групп.
`-G, --groups`	Выводит все подлинные числовые идентификаторы групп, в которых состоит пользователь.
`-n, --name`	Выводит действующие имена пользователей или групп.
`-r, --real`	Выводит подлинные числовые идентификаторы пользователей или групп.
`-u, --user`	Выводит только подлинный числовой идентификатор пользователя.
`--version`	Выводит информацию о версии утилиты и завершает работу.
`--help`	Выводит справку по этой утилите и завершает работу.

Пример: выведем сведения о текущем пользователе `user`. Работа команды `id`:

```
$ id
uid=1000(user) gid=1000(user) группы=1000(user),100(users) контекст=user_u:user_r:user_t:s0
```

Конфигурационный файл /etc/login.defs

Конфигурационный файл `/etc/login.defs` позволяет задавать параметры, определяющие использование пользователями своих паролей.

```
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_MIN_LEN    Minimum acceptable password length.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
```

Параметры перечислены в таблице:

Таблица 9: Параметры конфигурационного файла `/etc/login.defs` и их описание

Параметр	Описание
`PASS_MAX_DAYS`	Определяет максимальный срок действия пароля, т.е. максимальное число дней, в течение которых действие пароля сохраняется. По истечении этого срока запускается процесс принудительной смены пароля. Если значение параметра не задано, то есть параметр закомментирован символом `#` или ему присвоено значение `-1`, то данное ограничение не установлено (отменяется).
`PASS_MIN_DAYS`	определяет минимальный срок между изменениями пароля, т.е. минимальное число дней между двумя последовательными изменениями пароля. Если значение параметра не задано, то есть параметр закомментирован символом `#` или ему присвоено значение `-1`, то данное ограничение не установлено (отменяется).
`PASS_MIN_LEN`	Определяет минимальную допустимую длину задаваемого пароля.
`PASS_WARN_AGE`	Определяет, за сколько дней до истечения срока действия пароля начнётся вывод предупреждения о необходимости его смены. Если значение параметра не задано, то есть параметр закомментирован символом `#` или ему присвоено значение `-1`, то данное ограничение не установлено (отменяется). Если значение параметра `0`, то предупреждение о необходимости смены пароля будет выведено в день его устаревания.

Пример: выведем на экран текущее заданное значение максимального количества дней действия пароля:

```
$ cat /etc/login.defs | grep PASS_MAX_DAYS
# PASS_MAX_DAYS  Maximum number of days a password may be used.
PASS_MAX_DAYS 30
```

Мы видим, что текущее максимальное количество дней действия пароля — 30 дней.

Конфигурационный файл /etc/pam.d/system-auth

Конфигурационный файл `/etc/pam.d/system-auth` позволяет задавать настройки подключаемых модулей аутентификации.

```
# Generated by authselect on Fri Jul 14 14:08:55 2023
# Do not modify this file manually.

auth        required                                     pam_env.so
auth        required                                     pam_faildelay.so delay=20000
00
auth        sufficient                                   pam_fprintd.so
auth        [default=1 ignore=ignore success=ok]         pam_usertype.so isregular
auth        [default=1 ignore=ignore success=ok]         pam_localuser.so
auth        sufficient                                   pam_unix.so nullok
auth        [default=1 ignore=ignore success=ok]         pam_usertype.so isregular
auth        sufficient                                   pam_sss.so forward_pass
auth        required                                     pam_deny.so

account     required                                     pam_unix.so
account     sufficient                                   pam_localuser.so
account     sufficient                                   pam_usertype.so issystem
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     required                                     pam_permit.so
```

Каждая строка в нем представляет собой правило, состоящее из трёх обязательных полей и одного опционального. Поля разделены символом пробела. Порядок, в котором указаны правила, определяет очередность их проверки.

Синтаксис правила:

```
type control module-path [module-arguments]
```

Поле `type` задаёт тип вызываемого модуля и может принимать одно из четырех допустимых значений:

- `auth` — предназначен для аутентификации пользователя путём запроса и проверки его пароля;
- `account` — используется для контроля доступа к сервису/приложению. Например, может быть произведён запрос о том, не истёк ли срок действия аккаунта пользователя, разрешено ли пользователю работать с определённым сервисом в определённое время, хватает ли системных ресурсов для работы;
- `password` — применятся для установки/изменения паролей;
- `session` — управляет действиями пользователя в рамках активной сессии после его успешной аутентификации в системе.

Поле `control` задаёт действие, которое нужно выполнить после вызова модуля. Доступно несколько действий:

- `required` — модуль должен вернуть положительный ответ. Если он возвращает отрицательный ответ, то пользователь будет уведомлен об этом только после того, как все остальные модули данного типа будут проверены;
- `requisite` — требует от модуля положительный ответ. В случае получения отрицательного ответа последовательная проверка выполнения остальных правил моментально прекращается и пользователь получает сообщение об ошибке аутентификации;
- `sufficient` — в случае, если ни один из модулей с действием `required` или `sufficient`, расположенных перед текущим, не вернул отрицательного ответа, текущий модуль вернёт положительный ответ и все последующие модули будут проигнорированы;
- `optional` — результат проверки модуля важен только в том случае, если действие является единственным для данного модуля;
- `include` — предназначается для добавления строк заданного типа из других файлов конфигурации из каталога `/etc/pam.d/` в файл конфигурации `/etc/pam.d/system-auth`. Название файла указывается в качестве аргумента действия.

Поле `module-path` задаёт путь к вызываемому модулю.

Поле `module-arguments` — дополнительные необязательные параметры модуля, необходимые для определения действий некоторых отдельных модулей в случае успешной авторизации. Так, если в конфигурационном файле найти строку, содержащую `pam_pwquality.so`, и добавить в нее `minlen=8`, то будет установлена минимальная длина пароля, равная 8-ми символам.

Пример: В качестве примера сделаем блокировку учётной записи пользователя, который совершит определенное количество неудачных попыток входа в систему.

Для этого внесем в файл `/etc/pam.d/system-auth` следующие изменения:

1. Сначала допишем в секцию `auth` строку `auth required pam_tally2.so deny=2 onerr=fail`, т.е. подключим модуль `pam_tally2` и установим блокировку пользователя после двух (значение параметра `deny`) неудачных попыток входа.
2. Затем в секции `account` добавим строку `account required pam_tally2.so` и закомментируем строки вида `auth requisite pam_succeed_if.so uid >= 1000 quiet` и `auth required pam_deny.so`.
3. Потом строку `auth sufficient pam_unix.so nullok try_first_pass` заменим на `auth required pam_unix.so nullok try_first_pass`.

После этого пользователь, допустивший подряд две неверных попытки входа, на третьей получит сообщение о том, что его учетная запись заблокирована. И даже

если четвертой попыткой он введет верный пароль, то все равно не получит доступ к системе.

```
$ sudo user2
Пароль:
sudo Сбой при проверке подлинности

$ sudo user2
Пароль:
sudo Сбой при проверке подлинности

$ sudo user2
Пароль:
Учетная запись заблокирована как следствие неудачных попыток входа (всего 3)
sudo Сбой при проверке подлинности

$ sudo user2
Пароль:
Учетная запись заблокирована как следствие неудачных попыток входа (всего 4)
sudo Сбой при проверке подлинности
```

Пример: В качестве другого примера настроим проверку паролей на сложность подбора через `pam_cracklib`.

1. Для этого добавим или изменим следующую строку:

```
password requisite pam_cracklib.so try_first_pass retry=3 type= minlen=6 dcredit=-2 ucredit=-3␣
↪lcredit=-2 ocredit=-1
```

Это значит следующее:

- после трех неуспешных попыток (`retry=3`) модуль вернет ошибку;
- минимальная длина для пароля — 6 символов (`minlen=6`);
- минимальное количество цифр — 2 (`dcredit=-2`);
- минимальное количество символов верхнего регистра — 3 (`ucredit=-3`);
- минимальное количество символов нижнего регистра — 2 (`lcredit=-2`);
- минимальное количество других символов — 1 (`ocredit=-1`).

2. Удалим или закомментируем следующую строку:

```
password requisite pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
```

Результат

- Выполним команду `passwd` для смены пароля пользователя `user2`.
- Зададим пароль из трех символов и увидим сообщение «НЕУДАЧНЫЙ ПАРОЛЬ: слишком короткий».
- Зададим пароль из четырех символов, система выдаст сообщение «НЕУДАЧНЫЙ ПАРОЛЬ: короткий».
- Зададим пароль из шести символов (букв и цифр), в результате чего получим сообщение «НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой».

- После трех неуспешных попыток модуль вернет ошибку.

```
$ passwd
Изменяется пароль пользователя user2.
Смена пароля для user2.
(текущий) пароль Unix:
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: слишком короткий
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: короткий
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой
passwd: Использовано максимальное число попыток, заданное для службы
```

- Зададим пароль достаточной длины из одних цифр и получим сообщение «НЕУДАЧНЫЙ ПАРОЛЬ: не содержит достаточное число РАЗЛИЧНЫХ символов».

- Зададим пароль достаточной длины, содержащий все указанные требования, кроме включения в него отличных от алфавита и цифр символов. Например, `2QyfMOb4`. Получим сообщение «НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой».

```
$ passwd
Изменяется пароль пользователя user2.
Смена пароля для user2.
(текущий) пароль Unix:
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: не содержит достаточное число РАЗЛИЧНЫХ символов
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: короткий
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой
passwd: Использовано максимальное число попыток, заданное для службы
```

- Зададим пароль, соблюдая все установленные требования. Например, `2QyfM*Ob4`. Пароль будет успешно задан (см. листинг).

```
$ passwd
Изменяется пароль пользователя user2.
Смена пароля для user2.
(текущий) пароль Unix:
Новый пароль:
Повторите ввод нового пароля:
passwd: Все данные аутентификации успешно обновлены.
```

Конфигурационный файл /etc/issue

Конфигурационный файл `/etc/issue` позволяет задать текстовое содержание уведомления пользователю перед началом его идентификации и аутентификации для входа в систему. Например, с предупреждением о том, что в ней реализованы меры защиты информации и о необходимости соблюдения соответствующих правил обработки данных. Традиционно в конфигурационном файле присутствуют опции выдачи сведений об операционной системе и ядре. Дополнительно можно добавить опции выдачи текущих даты и времени, количества работающих пользователей и некоторых других сведений.

Конфигурационный файл /etc/shadow

Конфигурационный файл `/etc/shadow` содержит сведения об учетных записях и паролях пользователей в виде строк со следующей структурой:

```
username:id:salt:hashed:lastchanged:min:max:warn:inactive:expire
```

Структура файла:

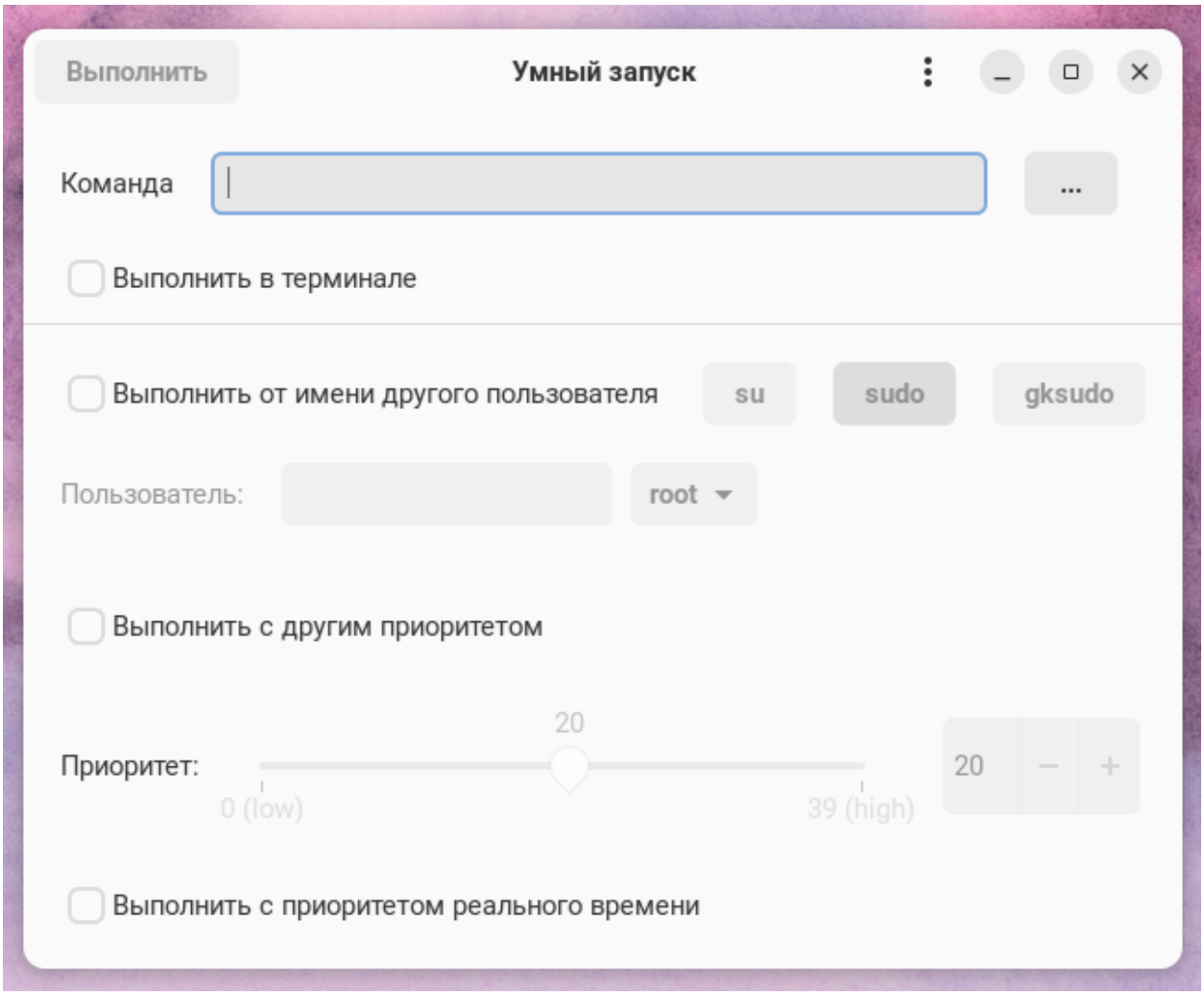
- `username` — имя пользователя:
- `id` — алгоритм шифрования: 1 (алгоритм MD5), 5 (SHA-256), 6 (SHA-512);
- `salt` — «соль», добавляемая к паролю строка из 10-20 случайных символов;
- `hashed` — зашифрованный пароль;
- `lastchanged` — дата последнего изменения пароля;
- `min` — минимальное число дней между двумя последовательными сменами паролей;
- `max` — срок действия пароля, т.е. максимальное число дней, в течение которых пароль будет активен;
- `warn` — за какое количество дней до срока истечения действия пароля пользователь будет уведомлен о том, что его необходимо сменить;
- `inactive` — количество дней после истечения срока действия пароля, спустя которое его учётная запись блокируется;
- `expire` — число дней, прошедших с момента блокирования учётной записи.

Если после имени пользователя `username` вместо `id:salt:hashed` стоит символ `*` либо последовательность из двух символов `!!`, то это означает, что попытки входа в систему от имени данного пользователя заблокированы.

Запуск программ от имени другого пользователя

Утилита smart-launcher

Утилита `smart-launcher` («Умный запуск») предназначена для запуска приложений в графическом или терминальном режиме от имени администратора системы или другого пользователя, а также для запуска приложений с изменённым приоритетом выполнения.



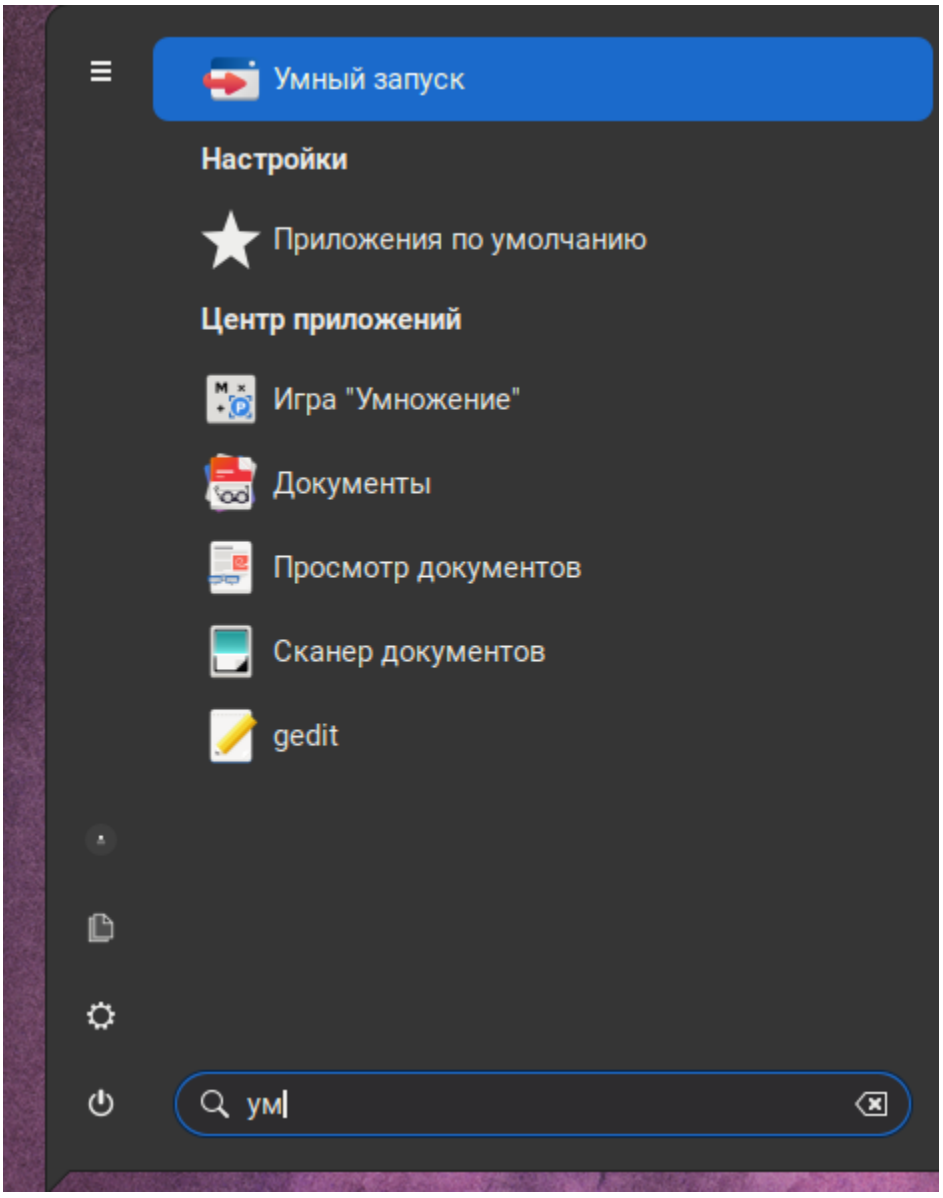
Установка и запуск

Для установки программы `smart-launcher` выполните следующую команду в «Терминале»:

```
$ sudo dnf install smart-launcher
```

Либо установите программу через «Центр приложений».

После установки `smart-launcher` можно запустить, выбрав в главном меню системы пункт «Умный запуск».

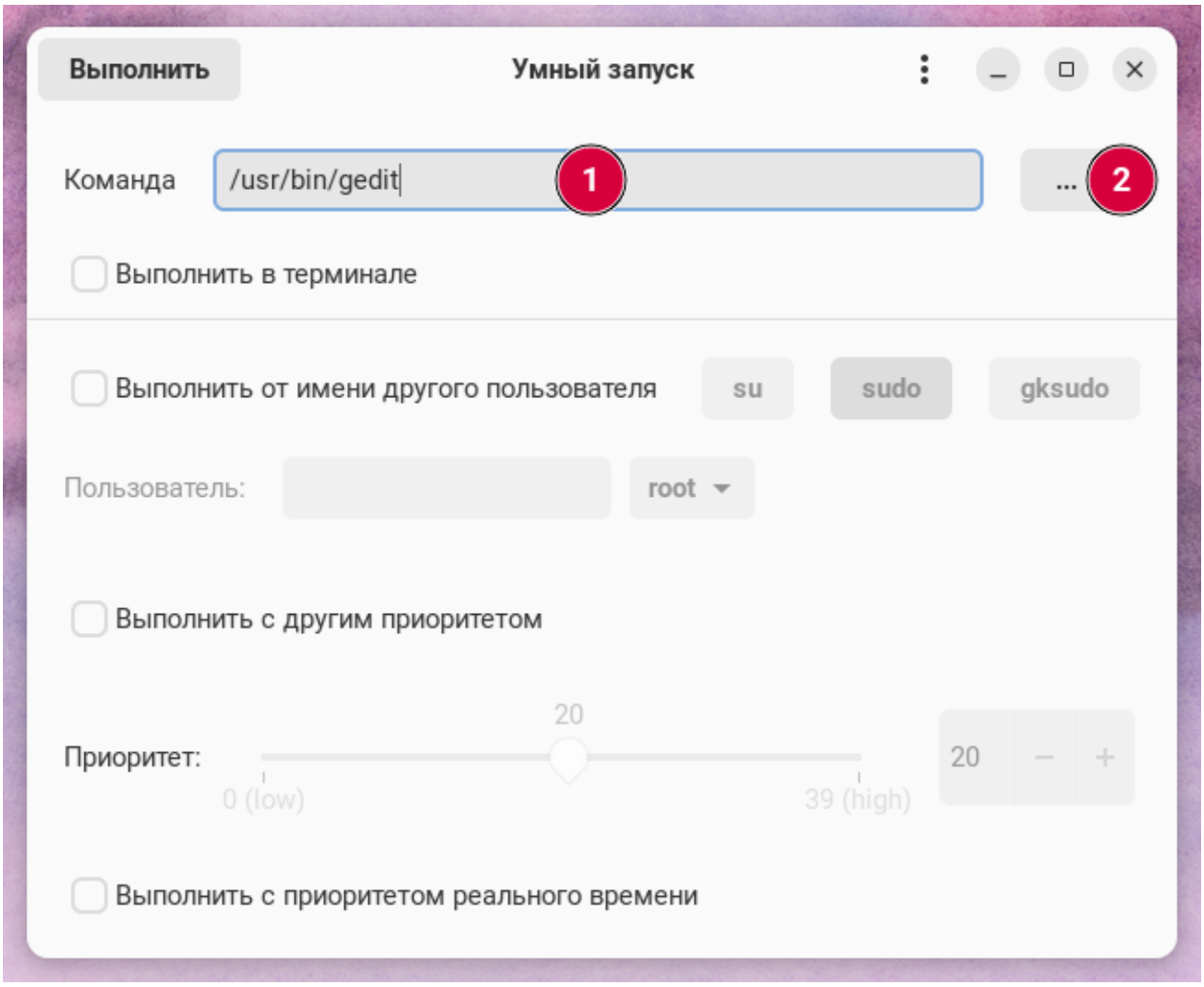


Либо запустив программу через «Терминал»:

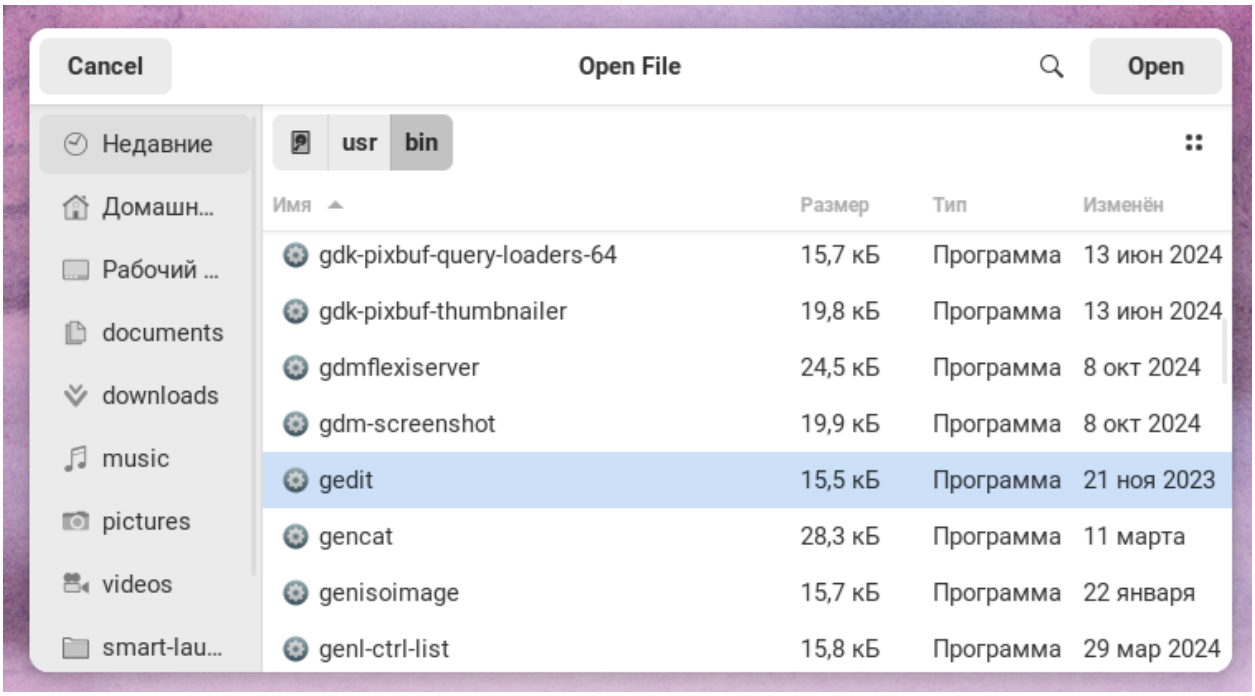
```
$ smart-launcher
```

Запуск графических приложений от имени другого пользователя

Для запуска графических приложений от имени другого пользователя необходимо ввести имя исполняемого файла в поле «Команда» (отмечено цифрой 1 на снимке экрана).

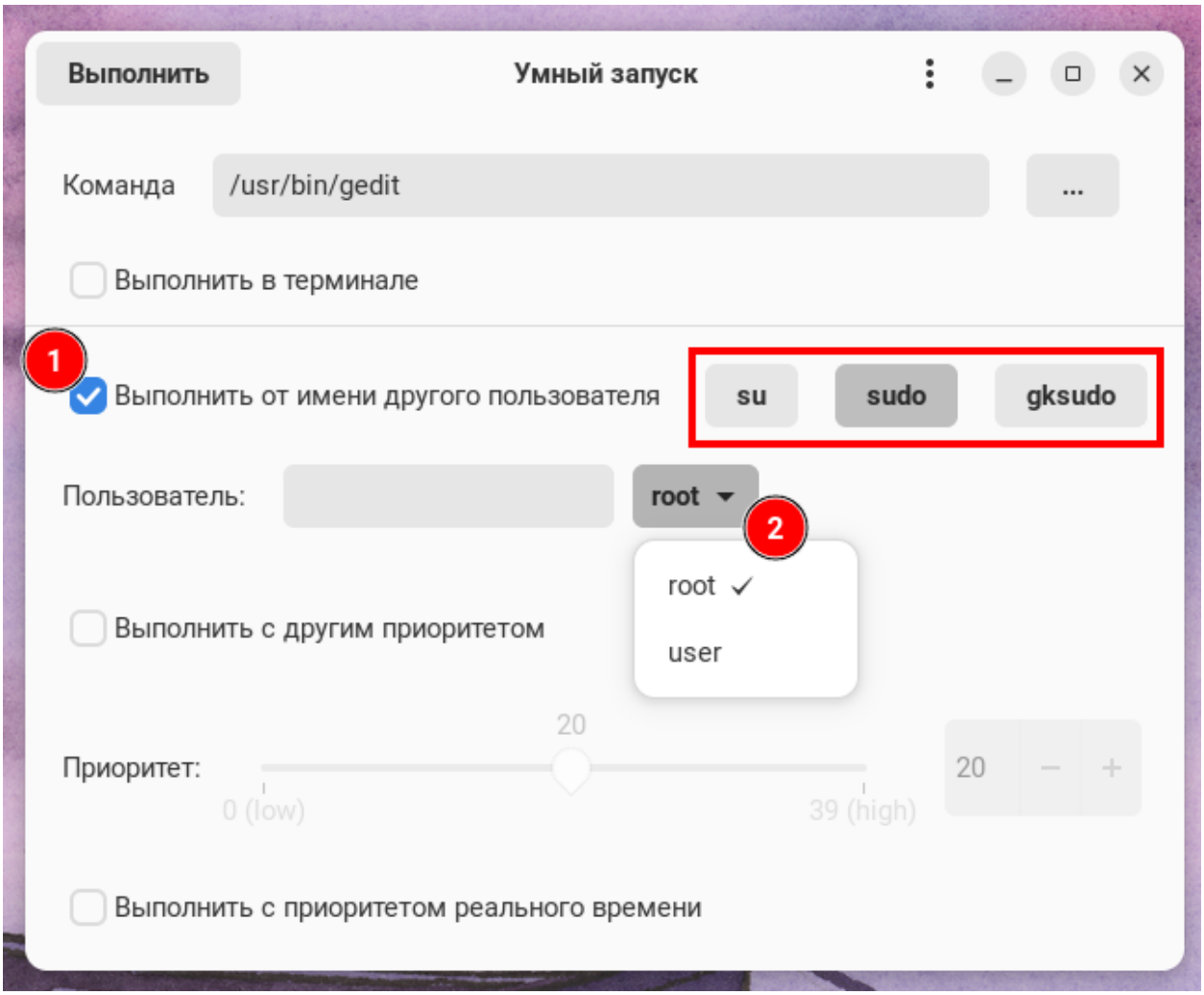


Или вызвать диалог выбора файла (кнопка «...» отмечена цифрой 2 на снимке экрана выше) и выбрать исполняемый файл.

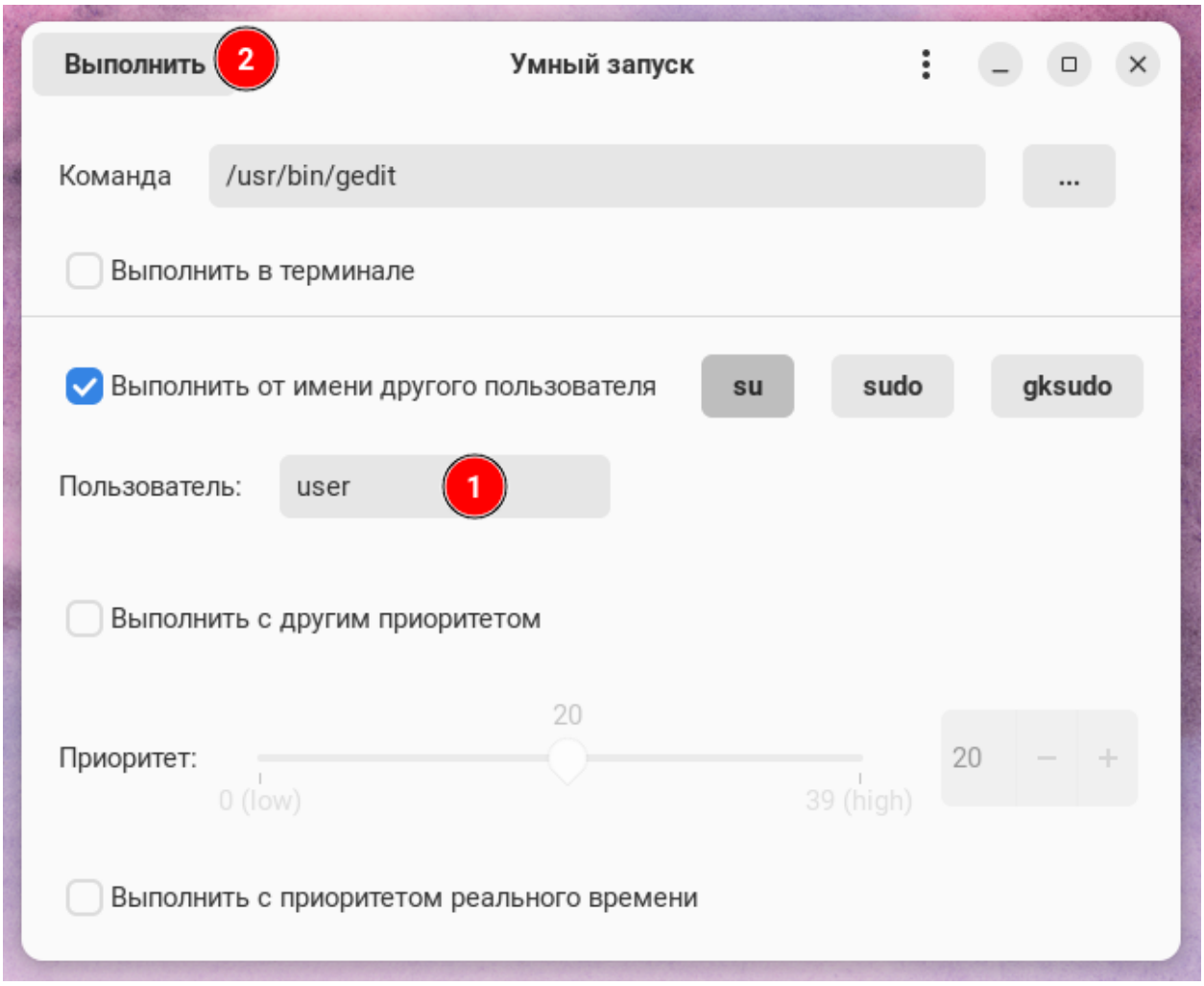


Далее, установите флажок «Выполнить от имени другого пользователя» (отмечен цифрой 1 на следующем снимке экрана) и, в случае необходимости, выберите метод запуска `su`, `sudo` (используется по умолчанию) или `gksudo` (соответствующая группа переключателей выделена красным прямоугольником на снимке экрана).

По умолчанию приложение будет выполнено от имени пользователя `root`, но вы можете выбрать другого пользователя из выпадающего списка локальных пользователей (отмечен цифрой 2 на снимке экрана).



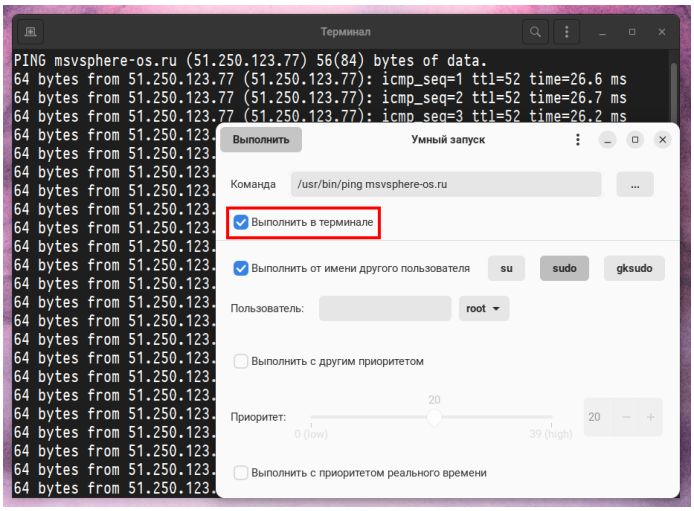
В случае, если пользователь не является локальным (например, пользователь домена Active Directory или FreeIPA), необходимо ввести его имя в поле «Пользователь» (отмечено цифрой 1 на снимке экрана).



Для запуска приложения нажмите кнопку «Выполнить» (отмечена цифрой 2 на снимке экрана выше) — приложение будет запущено в новом окне.

Запуск приложений в терминальном режиме от имени другого пользователя

Для запуска приложения в терминальном режиме от имени другого пользователя необходимо выбрать исполняемый файл, при необходимости ввести имя пользователя и выбрать режим запуска. Далее, необходимо установить флажок «Выполнить в терминале» и нажать кнопку «Выполнить».



Указанная программа будет запущена в графическом терминале.

Запуск приложений с изменённым уровнем приоритета

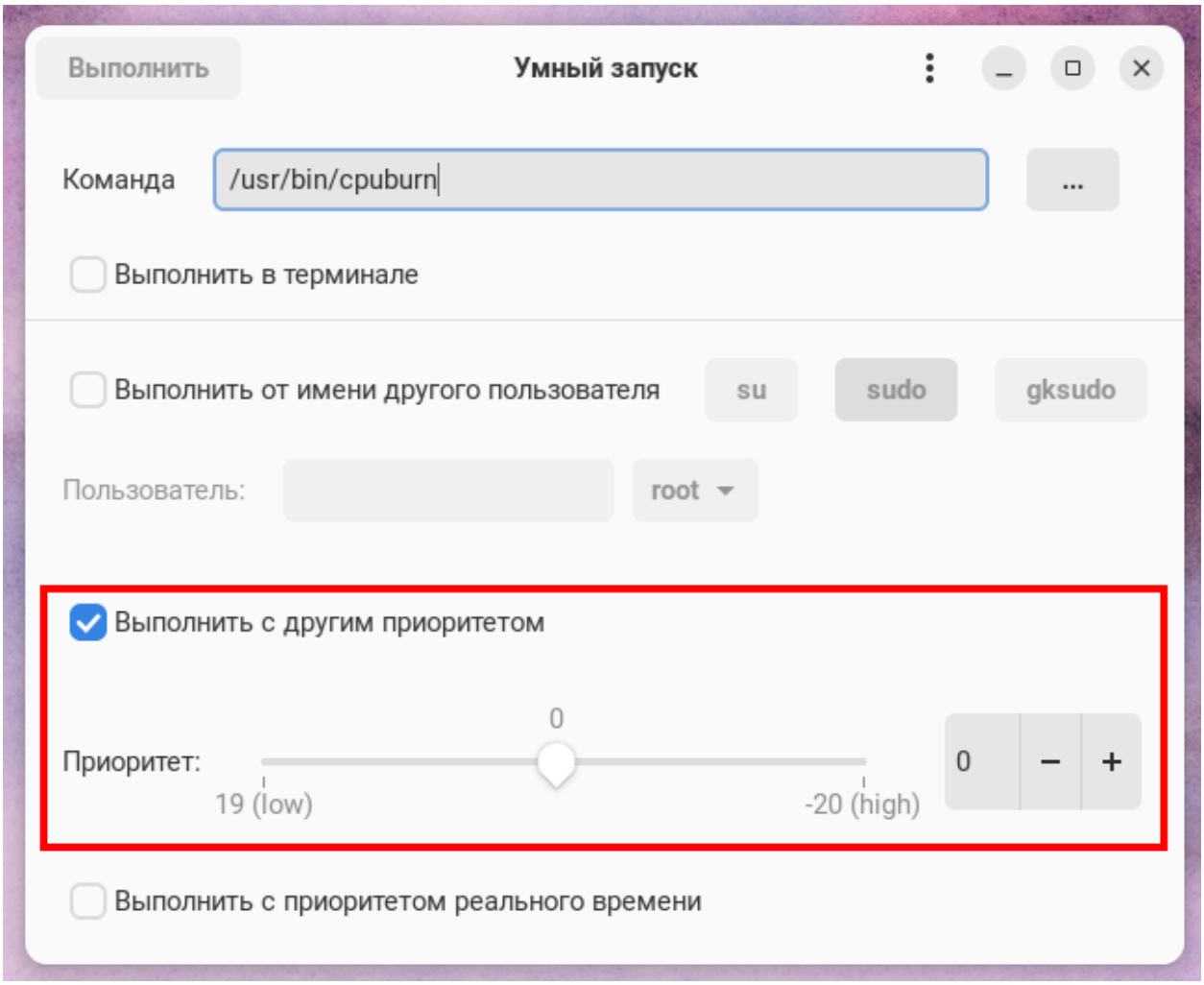
Утилита `smart-launcher` позволяет управлять двумя уровнями приоритета выполнения процесса:

- приоритет выполнения в пользовательском пространстве с использованием утилиты `nice` (см. `man nice`). В таком режиме все процессы делят ресурсы центрального процессора пропорционально установленным приоритетам;
- приоритет выполнения в реальном времени с использованием утилиты `chrt` (см. `man chrt`). Процессы, запущенные в таком режиме, имеют приоритет в реальном времени и могут вытеснять все другие процессы, в том числе и запущенные с `nice = -20`.

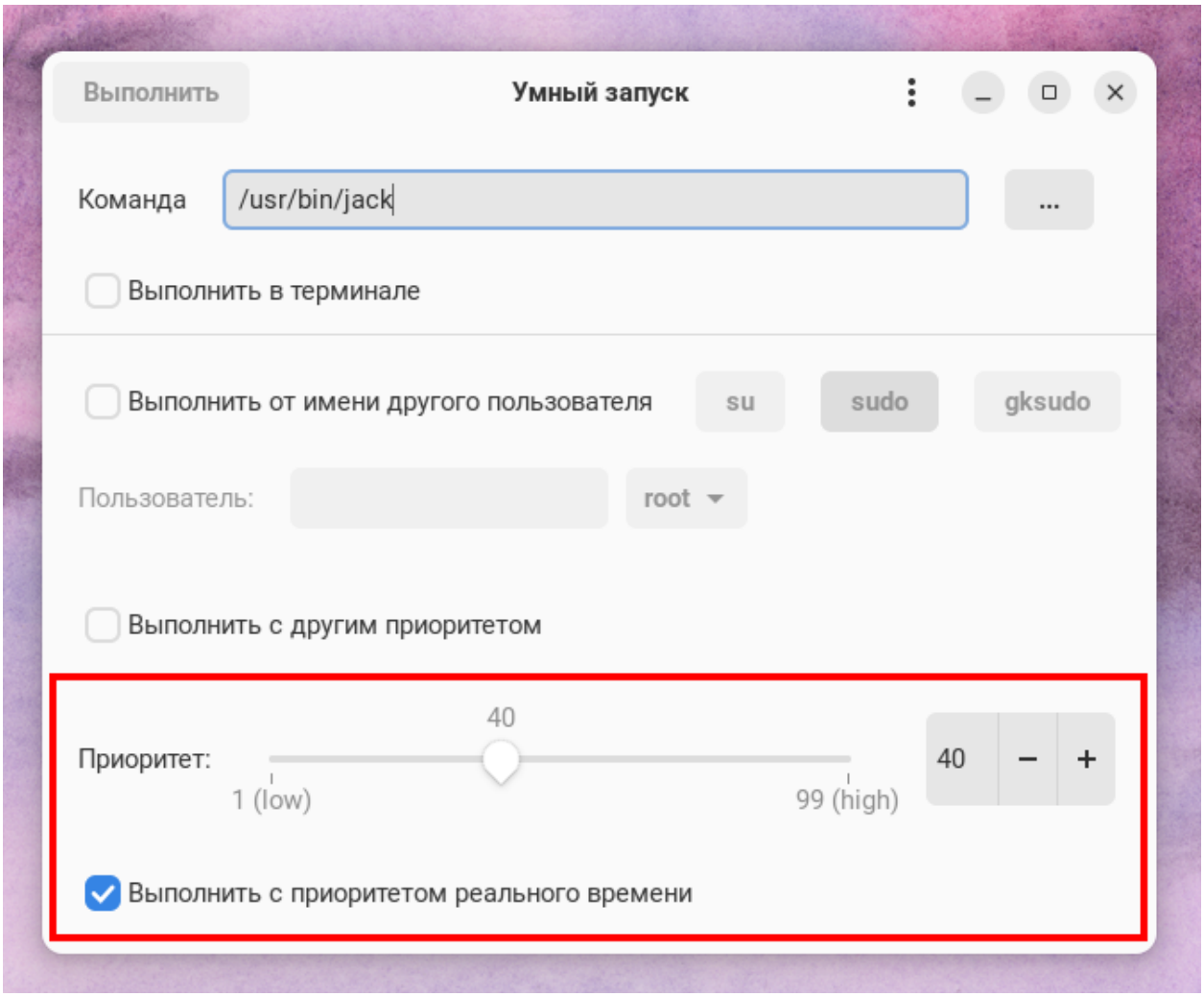
В большинстве случаев не рекомендуется изменять приоритеты реального времени за исключением тех задач, где критично время выполнения: обработка сигналов в реальном времени, промышленные контроллеры, встраиваемые системы с жёсткими требованиями к планированию выполнения процессов.

Чтобы изменить приоритет выполнения процесса вам потребуются привилегии системного администратора.

Для запуска приложения с изменённым приоритетом в пользовательском пространстве вам необходимо выбрать исполняемый файл, установить флажок «Выполнить с другим приоритетом» и установить приоритет от `19` (наименьший приоритет) до `-20` (наибольший приоритет) в поле «Приоритет» используя ползунок, кнопки `-` и `+` или указав нужное число в соответствующем поле ввода.



Для запуска приложения с приоритетом реального времени вам необходимо выбрать исполняемый файл, установить флажок «Выполнить с приоритетом реального времени» и установить приоритет от `1` (минимальный приоритет) до `99` (максимальный приоритет) в поле «Приоритет» используя ползунок, кнопки `-` и `+` или указав нужное число в соответствующем поле ввода.



Запускать приложения с изменением уровня приоритета можно как в графическом режиме, так и в терминальном.

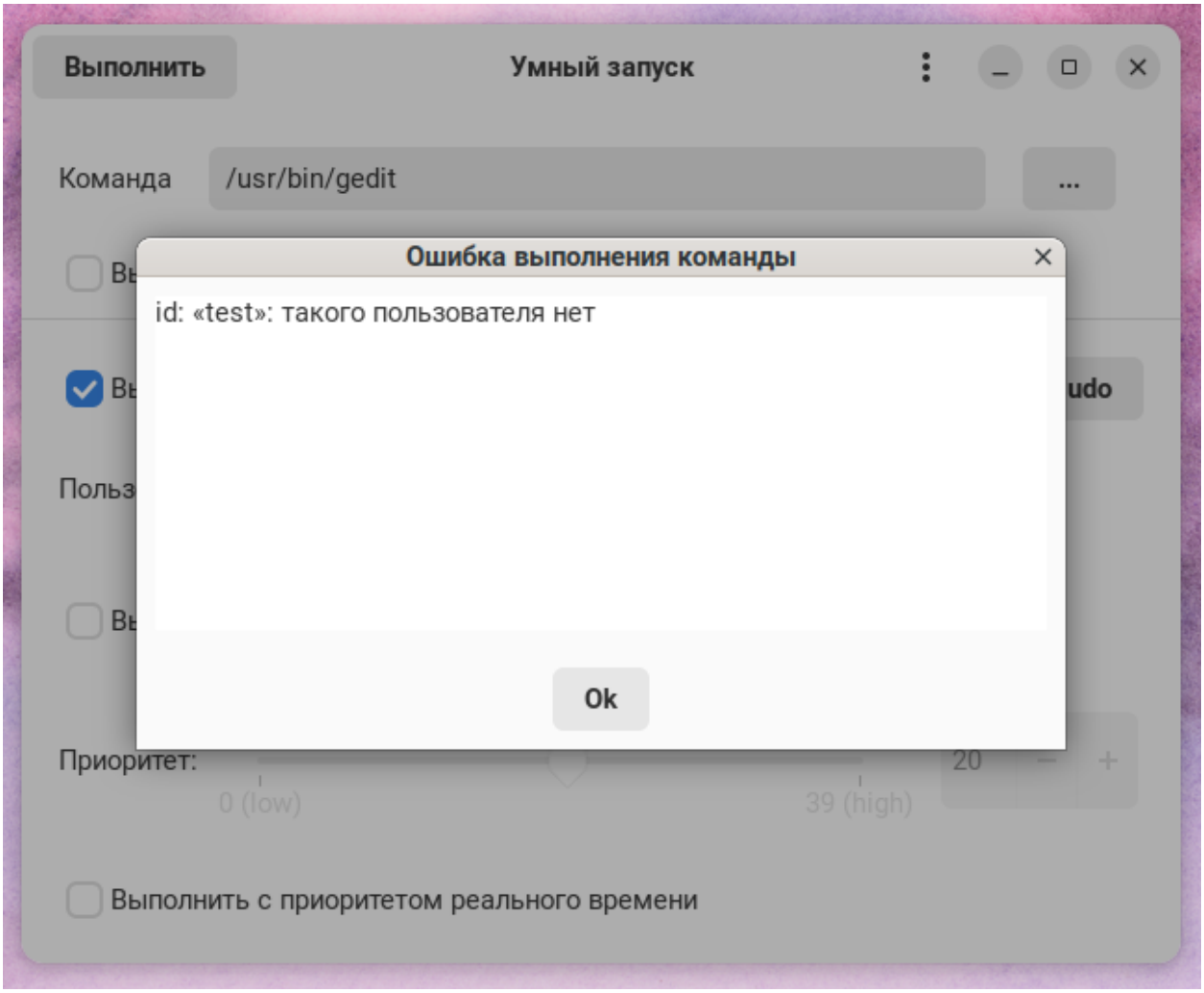
Аутентификация

При запуске приложения от имени другого пользователя с использованием `sudo` или `gksudo` пароль пользователя, в случае необходимости, будет запрошен в отдельном графическом окне.

Если же приложение запускается от имени другого пользователя с использованием `su`, то пароль будет запрошен в отдельном терминальном окне.

Диагностика ошибок

Ошибки, возникающие во время запуска приложения, отображаются в отдельном окне.



Также `smart-launcher` регистрирует возникающие ошибки в файле журнала `~/.cache/smart-launcher/smart-launcher.log`.

Управление доступом

Введение

Средства управления доступом предоставляют возможности ограничения количества одновременно предоставляемых параллельных сеансов доступа пользователей к системе, блокирования сеанса доступа пользователя в систему после истечения установленного периода времени бездействия или по его запросу, поддержки и сохранения атрибутов безопасности, связанных с информацией в процессе её хранения и обработки, разделения полномочий пользователей и администраторов, обеспечивающих функционирование системы, реализации различных методов управления доступом, типов доступа и правил разграничения доступа, назначения приоритетов для использования субъектами доступа вычислительных ресурсов, квотирования предоставляемых вычислительных ресурсов, а также другие возможности.

Установка и изменение прав доступа к файлам и директориям

Утилита `chmod` позволяет устанавливать и изменять права доступа к файлам и директориям. Она принимает описания прав доступа в двух нотациях: численной и буквенной, описываемой ниже.

В соответствии с буквенной нотацией пользователи, которые могут потенциально работать с файлом, разделяются на владельца (`u`), группу владельцев (`g`) и всех остальных пользователей (`o`), а файл может быть читаемым (`r`), записываемым (`w`) и исполняемым (`x`).

Описание прав доступа начинается с символа, соответствующего типу пользователей. Затем идет символ `+` для установки или символ `-` для снятия прав доступа, после чего описание заканчивается последовательностью символов, соответствующей правам доступа.

Например, для определения прав доступа, позволяющих читать и модифицировать файл `file`, может использоваться следующая команда:

```
$ chmod g+rw file
```

Для удаления всех прав доступа на директорию `/directory` для группы и остальных пользователей может использоваться следующая команда:

```
$ sudo chmod go-rwx /directory.
```

Утилита поддерживает опции, перечисленные в таблице:

Таблица 10: Опции утилиты `chmod` и их значения

Опция	Значение
`-R, --recursive`	Рекурсивное изменение прав доступа для директорий и их содержимого.
`-c, --changes`	Подробно описывать действия для каждого файла, чьи права действительно изменяются.
`-f, --silent, --quiet`	Не выдавать сообщения об ошибке для файлов, чьи права не могут быть изменены.
`-v, --verbose`	Подробно описывать действие или отсутствие действия для каждого файла.

продолжение на следующей странице

Таблица 10 – продолжение с предыдущей страницы

Опция	Значение
`--version`	Сообщить информацию о версии.
`--help`	Выводит справку по этой утилите и завершает работу.

Пример: сменим права для файла `file1` так, чтобы владелец файла имел права на чтение и запись, а группа и остальные пользователи — только на чтение:

```
$ chmod u+rw g-wx o-wx file1
```

Назначение и изменение владельца файла и директории

Утилита `chown` позволяет назначить или изменить владельца файла или директории.

Утилита поддерживает следующие опции, перечисленные в таблице:

Таблица 11: Опции утилиты `chown` и их значения

Опция	Значение
`-R, --recursive`	Рекурсивное изменение прав доступа для директорий и их содержимого.
`-c, --changes`	Подробно описывать все изменения.
`-f, --silent, --quiet`	Не выдавать сообщения об ошибке.
`-v, --verbose`	Вывести подробное описание действия.
`--version`	Сообщить информацию о версии.
`--help`	Выводит справку по этой утилите и завершает работу.

Пример: назначим пользователя `user` владельцем файла `file`:

```
$ sudo chown user file
```

Пример: выполним рекурсивный обход директории `directory` и назначим пользователя `user` владельцем всех вложенных файлов:

```
$ sudo chown -R user directory
```

Изменение группы-владельца файла или директории

Утилита `chgrp` позволяет изменить группу-владельца файла или директории.

Утилита поддерживает следующие опции, перечисленные в таблице:

Таблица 12: Опции утилиты `chgrp` и их значения

Опция	Значение
`-R, --recursive`	Рекурсивное изменение группы для каталогов и всего их содержимого.
`-c, --changes`	Подробно описывать действия для каждого файла, чья группа действительно меняется.
`-f, --silent, --quiet`	Не выдавать сообщения об ошибке для файлов, чья группа не может быть изменена.
`-v, --verbose`	Подробно описывать действие или отсутствие действия для каждого файла.
`--version`	Сообщить информацию о версии.
`--help`	Вывести справку по этой утилите и завершить работу.

Пример: изменим группу-владельца файла `file` на новую группу `new_group`:

```
$ sudo chgrp new_group file
```

Просмотр и изменение списков правил контроля доступа для файлов и директорий

Утилита `setfacl` позволяет просматривать и изменять списки правил контроля доступа для файлов и директорий.

Утилита поддерживает следующие опции, перечисленные в таблице:

Таблица 13: Опции утилиты `setfacl` и их значения

Опция	Значение
`-d`	Установить правила контроля доступа по умолчанию.
`-k`	Удалить правила контроля доступа по умолчанию.
`-s`	Заменить правила контроля доступа заданными.
`-m`	Модифицировать правила контроля доступа.
`-x`	Удалить указанное правило контроля доступа.
`-b`	Удалить все правила контроля доступа.
`-v`	Вывести версию и выйти.
`-h`	Вывести справку об использовании утилиты и выйти.

Пример: удалим все правила контроля доступа к файлу `file`:

```
$ sudo setfacl -b file
```

Просмотр списков контроля доступа

Утилита `getfacl` позволяет просматривать списки контроля доступа.

Утилита поддерживает следующие опции, перечисленные в таблице:

Таблица 14: Опции утилиты `getfacl` и их значения

Опция	Значение
`-a, --access`	Выводить список контроля доступа к файлам.
`-d, --default`	Выводить список контроля доступа по умолчанию.
`-c, --omit-header`	Не выводить заголовок с комментариями.
`e, --all-effective`	Выводить комментарии с действующими правами доступа для каждого пользователя.
`-E, --no-effective`	Не выводить комментарии с действующими правами доступа ни для одного пользователя.
`-R, --recursive`	Делать рекурсивный обход директории и выводить списки контроля доступа для каждого файла и директории.
`-v, --version`	Вывести версию и выйти.
`-h, --help`	Вывести справку об использовании утилиты и выйти.

Пример: просмотрим список контроля доступа для файла `cg.conf`:

```
$ getfacl cg.conf
# file: cg.conf
# owner: user
# group: user
user::rwx
group::r-x
other::r-x
```

Пример: зададим дополнительные компоненты списка контроля доступа для пользователя `user` и группы `user` по отношению к файлу `cg.conf`:

```
$ setfacl -m g:user:rxw cg.conf

$ setfacl -m u:user:rxw cg.conf

$ getfacl cg.conf
# file: cg.conf
# owner: user
# group: user
user::rwx
user:user:rwx
group::r-x
group:user:rwx
mask::rwx
other::r-x
```

Пример: от имени администратора модифицируем списки контроля доступа для файлов, владельцем которых он является:

```
$ sudo setfacl -m u:user:rxw ~/file2

$ sudo getfacl ~/file2
getfacl: Removing leading `/` from absolute path names
# file: root/file2
# owner: root
# group: root
user::rw-
user:user:rwx
group::r--
mask::rwx
other::r--
```

Пример: от имени администратора модифицируем списки контроля доступа для файлов, владельцем которых он не является:

```
$ sudo setfacl -m u:user:rxw /home/user3/file2

$ sudo setfacl -m u:user:rxw /home/user3/dir2

$ sudo getfacl /home/user3/file2
getfacl: Removing leading `/` from absolute path names
# file: home/user3/file2
# owner: user3
# group: user3
user::rwx
user:user:rwx
group::---
mask::rwx
other::---

$ sudo getfacl /home/user3/dir2
getfacl: Removing leading `/` from absolute path names
# file: home/user3/dir2/
# owner: user3
# group: user3
user::rwx
user:user:rwx
group::---
mask::rwx
other::---
```

Пример: от имени администратора удалим списки контроля доступа для объектов, владельцем которых он является:

```
$ sudo setfacl -b ~/file2

$ sudo getfacl ~/file2
getfacl: Removing leading `/` from absolute path names
# file: root/file2
# owner: root
# group: root
user::rw-
group::r--
other::r--
```

Пример: от имени администратора удалим списки контроля доступа для объектов, владельцем которых он не является:

```
$ sudo setfacl -b /home/user3/file2

$ sudo getfacl /home/user3/file2
getfacl: Removing leading `/` from absolute path names
# file: home/user3/file2
# owner: user3
# group: user3
user::rwx
group::---
other::---
```

Важно

Пользователь, не обладающий полномочиями администратора, не может удалять списки контроля доступа, которые он не создавал.

Редактирование пользовательских квот для файловой системы

Утилита `edquota` позволяет редактировать пользовательские квоты для файловой системы.

Утилита поддерживает следующие опции, перечисленные в таблице:

Таблица 15: Опции утилиты `edquota` и их значения

Опция	Значение
`-u, --user`	Изменить пользовательскую квоту.
`-g, --group`	Изменить групповую квоту.
`-p, --prototype = protoname`	Дублировать квоты прототипного пользователя. Это обычный механизм, используемый для инициализации квот для групп пользователей.
`-F, --format = имя-формата`	Изменить квоту для указанного формата.
`-f, --filesystem`	Выполнять указанные операции только для заданной файловой системы. По умолчанию операция выполняется для всех файловых систем с квотой.
`-t, --edit-period`	Редактировать мягкие ограничения по времени для каждой файловой системы.
`-T, --edit-times`	Изменить время для пользователя или группы, когда принудительное ограничение установлено.

Конфигурационный файл /etc/profile

Конфигурационный файл `/etc/profile` используется для задания элементов окружения оболочки пользователя. Например, в нём определяются глобальные переменные:

- `PATH` — переменная среды, используемая для указания оболочке списка каталогов, которые будут просматриваться при поиске исполняемых файлов;
- `USER` — имя пользователя при входе в ОС;
- `LOGNAME` — то же, что и `USER`. Некоторые программы считывают значение этой глобальной переменной вместо `USER`;
- `MAIL` — имя файла, в который записывается локальная почта пользователя, а также его расположение;
- `HOSTNAME` — имя хоста;
- `HISTSIZE` — количество исполненных команд, сохраняемых в истории;
- `HISTCONTROL` — политики в отношении команд, сохраняемых в истории. По умолчанию задано значение `ignoredups`, то есть команда, полностью совпадающая с одной из уже записанных в историю, не сохраняется. Если задать политику `ignorespace`, то будут игнорироваться как дублирующиеся команды, так и те, что начинаются с символа пробела.

Также в конфигурационном файле задаётся маска, используемая для определения конечных прав доступа для пользователя.

```
# /etc/profile

# System wide environment and startup programs, for login setup
# Functions and aliases go in /etc/bashrc

# It's NOT a good idea to change this file unless you know what you
# are doing. It's much better to create a custom.sh shell script in
# /etc/profile.d/ to make custom changes to your environment, as this
# will prevent the need for merging in future updates.

pathmunge () {
    case ":${PATH}:" in
        *:"$1":*)
            ;;
        *)
            if [ "$2" = "after" ] ; then
                PATH=$PATH:$1
            else
                PATH=$1:$PATH
            fi
    esac
}


if [ -x /usr/bin/id ]; then
    if [ -z "$EUID" ]; then
        # ksh workaround
        EUID=`/usr/bin/id -u`
        UID=`/usr/bin/id -ru`
    fi
    USER="`/usr/bin/id -un`"
    LOGNAME=$USER
    MAIL="/var/spool/mail/$USER"
fi

# Path manipulation
if [ "$EUID" = "0" ]; then
    pathmunge /usr/sbin
    pathmunge /usr/local/sbin
else
    pathmunge /usr/local/sbin after
    pathmunge /usr/sbin after
fi
```

Пример: определим время бездействия при локальной терминальной сессии равным двум минутам (120 с). Для этого в файле `/etc/profile` после строк

```
HOSTNAME= '/usr/bin/hostname 2>/dev/null'
HISTSIZE=1000
```

Добавим строку `TMOUT=120`. Там же, в строке

```
export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL
```

Необходимо добавить параметр `TMOUT`:

```
export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE TMOUT HISTCONTROL
```

Для подтверждения вступления изменений в силу надо будет завершить сеанс и зарегистрироваться в системе заново. Тогда появится сообщение, что после двух минут бездействия время ожидания ввода вышло, в результате чего интерактивный сеанс был закрыт.

Конфигурационный файл /etc/security/limits.conf

Конфигурационный файл `/etc/security/limits.conf` может использоваться для задания модулю `pam_limits.so` дополнительных ограничений. Для этого каждая его строка включает четыре группы параметров, которые перечислены и описаны ниже:

Важно

По умолчанию все ограничения отключены — все строки закомментированы.

- **`<domain>`:**
  имя пользователя, имя группы с синтаксисом `@group`, подстановочный знак * для записи по умолчанию, подстановочный знак `%`, который также может использоваться с синтаксисом `%group` для ограничения `maxlogin`;
- **`<type>`:**
  - `soft` для установки мягких ограничений;
  - `hard` для установки жестких ограничений.
- **`<item>`:**
  - `core`: ограничивает размер файла ядра в Кб;
  - `data`: максимальный размер данных в Кб;
  - `fsize`: максимальный размер файла в Кб;
  - `memlock`: максимальное адресное пространство, предустановленное в памяти, в Кб;
  - `nofile`: максимальное количество открытых файлов;
  - `rss`: максимальный размер резидентного набора в Кб;
  - `stack`: максимальный размер стека в Кб;

- `cpu`: максимальное время процессора в MIN;
- `nproc`: максимальное количество процессов;
- `as`: ограничение адресного пространства в Кб;
- `maxlogins`: максимальное количество логинов для этого пользователя;
- `maxsyslogins`: максимальное количество входов в систему;
- `priority`: приоритет процессов пользователя;
- `locks`: максимальное количество блокировок файлов, которое может быть обеспечено пользователем;
- `sigpending`: максимальное количество ожидающих сигналов;
- `msgqueue`: максимальный объем памяти, используемый очередями сообщений POSIX, в байтах;
- `nice`: приоритет для запуска процессов утилитой `nice`;
- `rtprio`: максимальный приоритет в реальном времени.

```
# /etc/security/limits.conf
#
#This file sets the resource limits for the users logged in via PAM.
#It does not affect resource limits of the system services.
#
#Also note that configuration files in /etc/security/limits.d directory,
#which are read in alphabetical order, override the settings in this
#file in case the domain is the same or more specific.
#That means, for example, that setting a limit for wildcard domain here
#can be overridden with a wildcard setting in a config file in the
#subdirectory, but a user specific setting here can be overridden only
#with a user specific setting in the subdirectory.
#
#Each line describes a limit for a user in the form:
#
#<domain>        <type>  <item>  <value>
#
#Where:
#<domain> can be:
#        - a user name
#        - a group name, with @group syntax
#        - the wildcard *, for default entry
#        - the wildcard %, can be also used with %group syntax,
#                 for maxlogin limit
#
#<type> can have the two values:
#        - "soft" for enforcing the soft limits
#        - "hard" for enforcing hard limits
#
#<item> can be one of the following:
#        - core - limits the core file size (KB)
#        - data - max data size (KB)
#        - fsize - maximum filesize (KB)
#        - memlock - max locked-in-memory address space (KB)
#        - nofile - max number of open file descriptors
```

Пример: ограничим число параллельных сеансов доступа для каждой учетной записи пользователя. Для этого добавим в конфигурационный файл строку следующего содержания:

```
username hard maxlogins 2
```

Тогда, при условии, что пользователь `username` открыл локальную сессию (учитывая, что при входе в графический сеанс открываются сразу две сессии пользователя) и попытался зайти в систему через ssh-соединение (потенциально ещё один активный сеанс), ему будет выведено сообщение `Too many logins for 'username'` и это соединение будет заблокировано.

Конфигурационный файл /etc/fstab

Конфигурационный файл `/etc/fstab` используется для настройки параметров монтирования различных блочных устройств, разделов на диске и файловых систем. Он состоит из набора так называемых определений, каждое из которых занимает свою строку и состоит из шести полей, разделённых пробелами или символами табуляции:

```
fs_spec fs_file fs_vfstype fs_mntops fs_freq fs_passno
```

Поля предназначены для задания следующих параметров:

- **`fs_spec`**
  Физическое размещение файловой системы, по которому определяется конкретный раздел или устройство хранения для монтирования. Вместо указания размещения файловой системы явным образом можно воспользоваться её уникальным идентификатором UUID.
- **`fs_file`**
  Точка монтирования, куда монтируется корень файловой системы.
- **`fs_vfstype`**
  Тип файловой системы. Поддерживаются следующие типы: adfs, affs, autofs, coda, coherent, cramfs, devpts, efs, ext2, ext3, ext4, hfs, hpfs, iso9660, jfs, minix, msdos, nvpfs, nfs, ntfs, proc, qnx4, reiserfs, romfs, smbfs, sysv, tmpfs, udf, ufs, umsdos, vfat, xenix, xfs.
- **`fs_mntops`**
  Опции монтирования файловой системы. Основные опции: `defaults`, `noauto`, `user`, `owner`, `comment`, `nofail`.
- **`fs_freq`**
  Предназначено для использования утилитой создания резервных копий в файловой системе. Возможные значения: `0` и `1`. Если указано `1`, то утилита создаст резервную копию.
- **`fs_passno`**
  Предназначено для использования программой `fsck` при необходимости проверки целостности файловой системы; возможные значения: `0`, `1` и `2`. Значение `1` указывается только для корневой файловой системы (то есть файловой системы с точкой монтирования `/`). Для остальных файловых систем для проверки утилитой `fsck` задаётся значение `2`. При значении `0` — проверка выполняться не будет.

По умолчанию конфигурационный файл включает:

```
/dev/mapper/MSVSphere-root / xfs defaults 0 0
```

Файловая система `/dev/mapper/MSVSphere-root` примонтирована в каталог `/`, тип файловой системы — `xfs`, используемые опции — `defaults`, резервная копия данных

не создаётся (`fs_freq=0`), проверка целостности файловой системы не выполняется (`fs_passno=0`).

```
UUID=b1bfe9b0-96ea-4876-883c-a9f1b6c74b /boot ext4 defaults 1 2
```

Файловая система с идентификатором `b1bfe9b0-96ea-4876-883c-a9f1b6c74b` смонтирована в `/boot`, тип файловой системы — `ext4`, используемые опции — `defaults`, резервная копия данных создаётся (`fs_freq=1`), проверка целостности файловой системы выполняется (`fs_passno=2`).

```
/dev/mapper/MSVSphere-swap swap defaults 0 0
```

Файловая система `/dev/mapper/MSVSphere-swap` является разделом подкачки `swap`, используемые опции — `defaults`, резервная копия данных не создаётся (`fs_freq=0`), проверка целостности файловой системы не выполняется (`fs_passno=0`).

```
# /etc/fstab
# Created by anaconda on Tue Jun 20 11:58:05 2023
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
/dev/mapper/msvsphere-root /                       xfs     defaults        0 0
UUID=8e41c721-164e-455c-bd65-b60ad5ad7cb4 /boot                   xfs     defaults
```

Регистрация событий безопасности

Введение

Средства регистрации событий безопасности предоставляют возможности включения и исключения событий безопасности в совокупность событий, подвергающихся регистрации, регистрации событий безопасности; предоставления регистрируемой информации в понятном и защищенном от несанкционированного доступа виде; обеспечения непрерывности процесса регистрации при превышении журналом регистрации определенного размера; выборочного просмотра, поиска, сортировки и упорядочения регистрируемой информации; изготовления соответствующих отчетов, а также другие возможности.

Создание и удаление правил регистрации событий безопасности

Утилита `auditctl` позволяет формировать, добавлять или удалять правила регистрации событий безопасности.

Утилита поддерживает следующие опции, перечисленные в таблице:

Таблица 16: Опции утилиты `auditctl` и их значения

Опция	Значение
`-b backlog`	Установить максимальное количество доступных для записи данных регистрации буферов. Значение по умолчанию — 64.
`--backlog_wait_time`	Установить время ожидания до постановки новой партии данных регистрации событий безопасности в очередь и последующей их обработки при достижении предельного значения.
`-e [0..2]`	Установить флаг блокировки: `0` позволит на время отключить регистрацию, `1` позволит включить её обратно, а `2` позволит защитить конфигурацию регистрации от изменений.
`-f [0..2]`	Установить способ обработки для флага сбоя. Эта опция позволяет определить, каким образом ядро будет обрабатывать критические ошибки. Значение по умолчанию: `1`. Для систем с повышенными требованиями к безопасности значение `2` может быть более предпочтительным.
`-h`	Краткая помощь по аргументам командной строки.
`-i`	Игнорировать ошибки при чтении правил из файла.
`-l`	Вывести список всех правил по одному правилу в строке.
`-k ключ`	Установить на правило ключ фильтрации. Ключ фильтрации — это произвольная текстовая строка длиной не больше 31 символа. Ключ помогает уникально идентифицировать записи, генерируемые в ходе аудита за точкой наблюдения.
`-m текст`	Послать в систему регистрации событий пользовательское сообщение. Это возможно только из аккаунта учетной записи суперпользователя `root`.
`-p [r|w|x|a]`	Установить фильтр прав доступа для точки наблюдения. `r` (чтение), `w` (запись), `x` (исполнение), `a` (изменение атрибута).
`-r частота`	Установить ограничение скорости выдачи сообщений в секунду (`0` — нет ограничения). Если эта частота ненулевая, и она превышается в ходе аудита, флаг сбоя выставляется ядром для выполнения соответствующего действия. Значение по умолчанию: `0`.
`-R файл`	Читать правила из файла. Правила должны быть расположены по одному в строке и в том порядке, в каком они должны исполняться. Владельцем файла с правилами должен быть суперпользователь `root`. Данный файл не должен быть доступен для чтения любым другим пользователям, в противном случае операция с опцией не будет позволена.
`-s`	Получить статус регистрации событий.
`-a список, действие`	Добавить правило с указанным действием к концу списка.
`-A список, действие`	Добавить правило с указанным действием в начало списка.
`-d список, действие`	Удалить правило с указанным действием из списка. Правило удаляется только в том случае, если полностью совпали и имя системного вызова, и поля сравнения.
`-D`	Удалить все правила и точки наблюдения.
`-c`	Продолжить загружать правила, несмотря на появление ошибки. Таким образом можно отследить конечный результат загрузки правил. Если хотя бы одно из правил не загрузилось, код возврата будет ненулевой.
`-S [Имя или номер системного вызова | all]`	Любой номер или имя системного вызова может быть использован. Также возможно использование ключевого слова `all`. Если какой-либо процесс выполняет указанный системный вызов, то служба регистрации генерирует соответствующую запись. Если значения полей сравнения заданы, а системный вызов не указан, правило будет применяться ко всем системным вызовам. В одном правиле может быть задано несколько системных вызовов — это положительно сказывается на производительности, поскольку заменяет обработку нескольких правил.

продолжение на следующей странице

Таблица 16 – продолжение с предыдущей страницы

Опция	Значение
`F [n=v | n!=v | n<v | n>v | n<=v | n>=v | n&v | n&=v]`	Задать поле сравнения для правила. Атрибуты поля следующие: объект, операция, значение. Можно задать до 64 полей сравнения в одной команде. Каждое новое поле должно начинаться с `-F`. Служба регистрации событий будет генерировать запись, если произошло совпадение по всем полями сравнения. Допустимо использование одного из следующих 8 операторов: равно, не равно, меньше, больше, меньше либо равно, больше либо равно, битовая маска (`n&v`) и битовая проверка (`n&=v`). Битовая проверка выполняет операцию `and` над значениями и проверяет, равны ли они. Битовая маска просто выполняет операцию `and`. Поля, оперирующие с идентификатором пользователя, могут также работать с именем пользователя — программа автоматически получит идентификатор пользователя из его имени.
`-A list,action`	Добавить правило в начало списка `list` с действием `action`.
`-C [f=f | f!=f]`	Сравнить значения полей между собой. Формат задания сравнения: поле, оператор, поле. Можно в одной команде сравнивать несколько пар полей одновременно. Перед каждой новой парой записывается опция `-C`. Опция снабжена двумя операторами: `=` и `!=`. Доступные для сравнения поля: `-w путь` (добавить точку наблюдения за файловым объектом, находящимся по указанному пути) и `-W путь` (удалить точку наблюдения за файловым объектом, находящимся по указанному пути).

Пример: добавим правило аудита, осуществляющее наблюдение за доступом к файлу `/etc/profile`:

```
$ sudo auditctl -w /etc/profile -p rw -k profile
```

Добавление правила регистрации событий безопасности

Утилита `autrace` позволяет добавлять правила регистрации событий безопасности для того, чтобы следить за использованием системных вызовов в указанном процессе. Она поддерживает опцию `-r`, с помощью которой можно ограничить сбор информации о системных вызовах только теми, которые необходимы для анализа использования ресурсов.

Пример: с помощью утилиты `autrace` от имени администратора получим информацию из журналов аудита:

```
$ sudo autrace /bin/date
Waiting to execute: /bin/date
Пн апр 9 22:56:19 MSK 2023
Cleaning up
Trace complete. You can locate the records with 'ausearch -i -p 12438'
```

Поиск данных регистрации событий безопасности

Утилита `ausearch` используется для поиска данных регистрации событий безопасности по различным критериям.

Утилита поддерживает следующие опции, перечисленные в таблице:

Таблица 17: Опции утилиты `ausearch` и их значения

Опция	Значение
`-a, --event audit-event-id`	Искать события с заданным идентификатором события.
`-c, --comm comm-name`	Искать события с заданным именем исполняемого файла.
`-f, --file file-name`	Искать события с заданным именем файла.
`-tm, --terminal terminal`	Искать события с заданным терминалом.
`-x, --executable executable`	Искать события с заданной исполняемой программой.
`--session Login-Session-ID`	Искать события с заданным идентификатором сессии.

продолжение на следующей странице

Таблица 17 – продолжение с предыдущей страницы

Опция	Значение
`-ua, --uid-all all-user-id`	Искать события, у которых любой из идентификаторов пользователя совпадает с заданным идентификатором пользователя.
`-ue, --uid-effective effective-user-id`	Искать события с заданным эффективным идентификатором пользователя.
`-ui, --uid user-id`	Искать события с заданным идентификатором пользователя.
`-ga, --gid-all all-group-id`	Искать события с заданным эффективным или обычным идентификатором группы.
`-ge, --gid-effective effective-group-id`	Искать события с заданным эффективным идентификатором группы или именем группы.
`-gi, --gid group-id`	Искать события с заданным идентификатором группы или именем группы.
`-hn, --host host-name`	Искать события с заданным именем узла. Имя узла может быть именем узла, полным доменным именем или цифровым сетевым адресом.
`-k, --key key-string`	Искать события с заданным ключевым словом.
`-p, --pid process-id`	Искать события с заданным идентификатором процесса.
`-pp, --ppid parent-process-id`	Искать события с заданным идентификатором родительского процесса.
`-sc, --success syscall-name-or-value`	Искать события с заданным системным вызовом.
`-o, --object SE-Linux-context-string`	Искать события с заданным объектом SELinux.
`se, --context SE-Linux-context-string`	Искать события с заданным контекстом SELinux.
`su, --subject SE-Linux-context-string`	Искать события с заданным субъектом SELinux.
`-sv, --success success-value`	Искать события с заданным флагом успешного выполнения. Допустимые значения: `yes` (успешно) и `no` (неудачно).
`-te, --end [end-date] [end-time]`	Искать события, которые произошли раньше или во время указанной временной точки.
`-ts, --start [start-date] [start-time]`	Искать события, которые произошли после или во время указанной временной точки.
`-w, --word`	Совпадение с полным словом. Поддерживается для имени файла, имени узла, терминала и контекста SELinux.
`-uu, --uuid uuid_гостевой_системы`	Искать событие в гостевой ОС с заданным UUID.
`-vm, --vm-name имя_гостевой системы`	Искать событие в гостевой ОС с заданным именем.
`--just-one`	Остановить поиск после появления первого события, удовлетворяющего критериям поиска.
`-e, --exit exit-code-or-errno`	Искать события по заданному системному вызову: коду возврата или номеру ошибки.
`--input-logs`	Использовать место нахождения файла логов, обозначенное в `/etc/audit/auditd.conf`.
`-h, --help`	Выдать справку об утилите.

Генерация отчётов по данным регистрации событий безопасности

Утилита `aureport` позволяет генерировать отчеты по данным регистрации событий безопасности.

Утилита поддерживает следующие опции, перечисленные в таблице:

Таблица 18: Опции утилиты `aureport` и их значения

Опция	Значение
`-u, --user`	Отчет о пользователях.
`-e, --event`	Отчет о событиях.
`-f, --file`	Отчет о файлах.
`-p, --pid`	Отчет о процессах.
`-s, --syscall`	Отчеты о системных вызовах.
`-t, --log`	Отчет о временных рамках отчета.
`-x, --executable`	Отчет об исполняемых объектах.
`-tm, --terminal`	Отчет о терминалах.
`-l, --login`	Отчет о попытках входа в систему.
`-au, --auth`	Отчет о всех попытках аутентификации.
`-c, --config`	Отчет об изменениях конфигурации.
`-m, --mods`	Отчет об изменениях пользовательских учетных записей.
`--tty`	Отчёт о нажатиях пользователя на клавиатуре.
`-ma, --mac`	Отчет о событиях в системе мандатного управления доступом.
`--success`	Для обработки в отчетах выбирать только удачные события. По умолчанию показываются и удачные, и неудачные события.
`--failed`	Для обработки в отчетах выбирать только неудачные события. По умолчанию показываются и удачные, и неудачные события.
`-te, --end [дата] [время]`	Искать события, которые произошли раньше или во время указанной временной точки.
`-ts, --start [дата] [время]`	Искать события, которые произошли после или во время указанной временной точки.
`--node имя_узла`	Выбрать события, связанные с узлом, имя которого указано после ключа. Можно указать несколько имён узлов. По умолчанию информация собирается со всех узлов.
`--summary`	Генерировать итоговый отчет, который дает информацию только о количестве элементов в том или ином отчете.
`--input-logs`	Использовать место нахождения файла логов, обозначенное в `/etc/audit/auditd.conf`.

Конфигурационный файл /etc/audit/auditd.conf

Конфигурационный файл `/etc/audit/auditd.conf` содержит параметры настройки средств регистрации событий безопасности, в том числе:

Параметр	Описание
`log_file`	Полное имя файла, в котором будут храниться данные регистрации событий безопасности.
`log_group`	Группа, являющаяся владельцем файла регистрации.
`log_format`	Формат хранения данных регистрации. Возможные значения: `raw` (данные записываются в том виде, в каком они были получены от ядра операционной системы) и `nolog` (запись данных отключается).
`priority_boost`	Приоритет выполнения службы регистрации.
`flush`	Режим работы службы регистрации. Возможные значения: `none` (не использовать какие-либо политики записи, т.е. дополнительные действия), `incremental` (запись с периодичностью, определенной параметром `freq`), `data` (запись данных в синхронном режиме), `sync` (запись в синхронном режиме и данных, и метаданных файла).
`freq`	Максимальное число регистрационных записей, которые могут храниться в буфере перед записью буферизованных данных на диск. Используется, только когда параметр `flush` имеет значение `incremental`.
`num_logs`	Максимальное число файлов регистрации на диске. Используется, только когда параметр `max_log_file_action` имеет значение `rotate`. Значение параметра не должно превышать 99.
`disp_qos`	Режим передачи данных между службой регистрации и диспетчером. Возможные значения: `lossy` (блокирование запрещено, т.е. служба регистрации может не передавать диспетчеру некоторые данные о событиях, если очередь данных о событиях полна. При этом данные регистрации будут записаны на диск, если только значение параметра `log_format` не равно `nolog`), `lossless` (блокирование разрешено, т.е. запись данных регистрации о событиях на диск будет остановлена, пока не освободится место в очереди).
`dispatcher`	Место расположения исполняемого файла программы диспетчера.
`name_format`	Порядок разрешения имен хостов. Возможные значения: `none` (имя не используется), `hostname` (имя, возвращенное через запрос `gethostname`), `fqd` (полное имя хоста, возвращенное через DNS запрос) `numeric` (IP-адрес), `user` (строка, определенная в параметре `name`).
`max_log_file`	Максимальный размер файла регистрации в мегабайтах, по достижении которого будет выполнено действие, определенное параметром `max_log_file_action`. Возможные действия: `ignore` (ничего не делать), `syslog` (отправить предупреждение в syslog), `suspend` (остановить запись данных регистрации событий на диск), `rotate` (произвести ротацию файлов регистрации в соответствии с параметром `num_logs`), `keep_logs` (осуществить ротацию, не удаляя при этом старые файлы).
`space_left`	Величина в мегабайтах, определяющая размер оставшегося дискового пространства, по достижении которого будет выполнено действие, определенное параметром `space_left_action`. Возможные действия: `ignore` (ничего не делать), `syslog` (отправить предупреждение в syslog), `email` (отправить письмо аккаунту, определенному в `action_mail_acct`), `exec` (выполнить скрипт), `suspend` (остановить запись на диск и перевести систему в single mode), `halt` (выключить систему).
`admin_space_left`	Величина в мегабайтах оставшегося свободного пространства на диске для предупреждения администратора о том, что надо добавить/очистить свободное пространство. Величина должна быть меньше чем `space_left`. Действия, которые можно определить в `admin_space_left_action`, аналогичны `space_left_action`.
`disk_full_action`	Действия, выполняемые при заполнении всего дискового пространства. Аналогичны `space_left_action`.
`disk_error_action`	Действия, выполняемые при возникновении дисковой ошибки. Аналогичны `space_left_action`.

Ограничение программной среды

Введение

Средства ограничения программной среды предоставляют возможности установки программного обеспечения доверенным образом; применения типовых наборов различных программных конфигураций; управления запуском программного обеспечения, в том числе определения запускаемых программ, настройки параметров запуска и контроля за их запуском; реагирования на попытки запуска, произведенные в нарушение установленных правил, а также другие возможности.

Включение программ в автозагрузку

Утилита `chkconfig` позволяет включать программы в автозагрузку с целью их автоматического запуска при старте операционной системы.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 20: Опции утилиты `chkconfig` и их значения

Опция	Значение
`--level levels`	Определяет уровни, на которых соответствующая программа должна выполняться. Уровни указываются на месте параметра `levels` в качестве строки целочисленных значений в диапазоне от 0 до 6. Так, например, при передаче опции `--level 35` утилите будет передано указание на уровни 3 и 5 соответственно.
`--no-redirect`	Если утилита запущена в системе, использующей утилиту `systemd` в качестве системы инициализации, то `chkconfig` будет перенаправлять команды в `systemd`, если у данной службы существует соответствующий файл, предназначенный для таких обращений. Данная опция отключает процесс перенаправления утилите `systemd` и обеспечивает работу только с символьными ссылками в директориях `/etc/rc[0-6].d`.
`--add name`	Добавляет новую службу для управления утилитой `chkconfig`. Имя службы указывается на месте параметра `name`.
`--del name`	Удаляет службу, имя которой указывается на месте параметра `name`, из-под управления утилитой `chkconfig`. Также из директорий `/etc/rc[0-6].d` удаляются любые символьные ссылки, указывающие на удаляемую службу.
`--override name`	Производит переопределение настроек службы, имя которой указывается на месте параметра `name`, вместо базовых настроек.
`--list name`	Выводит все службы, доступные для `chkconfig`, а также показывает их статус на каждом уровне (вкл/выкл). Если опции передать аргументом имя некоторой службы, которое указывается на месте параметра `name`, то будет выведена информация только об указанной службе.

Управление системными службами

Утилита `systemctl` позволяет управлять системными службами.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 21: Опции утилиты `systemctl` и их значения

Опция	Значение
`-t, --type`	Указывает на тип так называемого юнита (службы, сокета, устройства и т.п.). Может быть в виде списка наименований типов, разделенных запятой, если требуется указать более, чем на один тип.
`-a, --all`	При выведении списка юнитов вывести абсолютно все загруженные юниты вне зависимости от их статуса, включая те из них, которые являются неактивными.
`start [имя сервиса]`	Запускает работу сервиса с указанным именем.
`stop [имя сервиса]`	Останавливает работу сервиса с указанным именем.
`reload [имя сервиса]`	Перезагружает конфигурацию сервиса с указанным именем.
`restart [имя сервиса]`	Перезапускает сервис с указанным именем.
`try-restart [имя сервиса]`	Перезапускает сервис с указанным именем, если данный сервис уже работает на момент запуска утилиты.

продолжение на следующей странице

Таблица 21 – продолжение с предыдущей страницы

Опция	Значение
`reload-or-restart [имя сервиса]`	Перезагрузить конфигурацию сервиса с указанным именем, если сервис поддерживает такую команду, или выполнить перезапуск службы. Если на момент запуска утилиты указанная служба не была запущена, то она запустится после успешного выполнения команды.
`reload-or-try-restart [имя сервиса]`	Перезагрузить конфигурацию сервиса с указанным именем, если сервис поддерживает такую команду, или выполнить перезапуск службы. Если на момент запуска утилиты указанная служба не была запущена, то указанная команда не произведет никаких действий.
`kill [имя сервиса]`	Осуществить принудительную остановку работы службы с указанным именем.
`is-active [имя сервиса]`	Осуществляет проверку, активна ли на момент запуска утилиты служба с указанным именем. Если служба активна, или хотя бы одна из служб, переданных в качестве аргумента данной команде, активна (в случае, если были переданы наименования более, чем одной службы), выведется нулевое значение. В противном случае — ненулевое.
`is-failed [имя сервиса]`	Проверяет, были ли проблемы при запуске указанной службы или служб. Если хотя бы у одной из служб возникали проблемы, будет выведено нулевое значение.
`enable [имя сервиса]`	Добавляет указанный сервис (или их множество) в автозапуск.
`disable [имя сервиса]`	Убирает указанный сервис (или их множество) из автозапуска.
`is-enabled [имя сервиса]`	Проверяет, находится ли указанная служба (или службы, в случае, если в качестве аргумента был передан список наименований) в автозапуске. Если хотя бы одна из указанных служб находится в автозапуске, будет выведено нулевое значение.
`--version`	Вывести информацию о версии утилиты.
`-h, --help`	Вывести справочную информацию об утилите.

Пример: проверим статус сервера печати.

Для этого выполним следующую команду:

```
$ sudo systemctl status cups
cups.service - CUPS Printing Service
  Loaded: loaded (/usr/lib/systemd/system/cups.service; disabled; vendor preset: enabled)
  Active: inactive (dead)
```

Пример: разрешим автоматический запуск сервера печати CUPS при загрузке системы.

Для этого выполним следующую команду:

```
$ sudo systemctl enable cups
Created symlink from /etc/systemd/system/multi-user.target.wants/cups.service to /usr/lib/
↪systemd/system/cups.service.
Created symlink from /etc/systemd/system/printer.target.wants/cups.service to /usr/lib/systemd/
↪system/cups.service.
Created symlink from /etc/systemd/system/sockets.target.wants/cups.service to /usr/lib/systemd/
↪system/cups.socket.
Created symlink from /etc/systemd/system/multi-user.target.wants/cups.path to /usr/lib/systemd/
↪system/cups.path.
```

Настройка запуска программ по расписанию

Утилита `crontab` позволяет настраивать запуск программ по расписанию.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 22: Опции утилиты `crontab` и их значения

Опция	Значение
`-u`	Указывает пользователя, чье расписание должно редактироваться.
`-l`	Вывод текущего файла расписания.
`-r`	Удаление текущего файла расписания.
`-e`	Редактирование файла расписания.

продолжение на следующей странице

Таблица 22 – продолжение с предыдущей страницы

Опция	Значение

Таблица расписания состоит из шести колонок, разделяемых пробелами или символами табуляции. Первые пять колонок задают время выполнения (минута, час, день, месяц, день недели). В них может находиться число, список чисел, разделённых запятыми, диапазон чисел, разделённых дефисом, символы * или /. После полей времени указывается пользователь, от которого запускается программа. Все остальные символы в строке интерпретируются как выполняемая программа с её параметрами.

Пример: установим с помощью утилиты `crontab` ограничения на доступ к системе по времени, с 10:28 до 10:30. Команда `passwd -l user2` блокирует возможность авторизации, дописывая символ восклицательного знака к строке пароля в файле `/etc/shadow`. Команда `passwd -u user2` производит обратную операцию, снимая тем самым блокировку. Заполним файл расписания и выполним команду `service crond restart`:

```
$ sudo crontab -e
crontab: Installing new crontab

$ sudo service crond restart
Redirecting to /bin/systemctl restart crond.service

$ sudo crontab -l
28 10 * * * /usr/bin/passwd -l user2
30 10 * * * /usr/bin/passwd -u user2
```

Управление программными пакетами

Утилита `rpm` позволяет управлять так называемыми программными пакетами, т.е. управлять их установкой, обновлением, проверкой и удалением.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 23: Опции утилиты `rpm` и их значения

Опция	Значение
`-i, --install`	Установка нового пакета.
`-u, --upgrade`	Установка или обновление уже установленного пакета до новой версии. При этом после установки пакета все другие версии удаляются.
`-f, --freshen`	Обновление пакета, но только если предыдущая версия уже установлена.
`--nodeps`	Не выполнять проверку зависимостей перед установкой или обновлением пакета.
`--nosuggest`	Не предлагать пакет(ы) для разрешения отсутствующих зависимостей.
`--noorder`	Не выполнять переупорядочивание пакетов для установки. Список пакетов обычно переупорядочивается для удовлетворения зависимостей.
`--oldpackage`	Разрешает обновить или заменить пакет более старой версией.
`--replacefiles`	Установить пакеты, даже если они заменяют файлы от других установленных пакетов.
`--replacepkgs`	Установить пакеты, даже если они уже установлены в систему.
`--includedocs`	Устанавливать файлы с документацией.
`--excludedocs`	Не устанавливать файлы с документацией.
`-e, --erase`	Удалить заданный пакет.
`--allmatches`	Удалить все версии пакета.
`--nodeps`	Не проверять зависимости перед удалением пакетов.
`--test`	Выполнить только проверку установки пакета.

продолжение на следующей странице

Таблица 23 – продолжение с предыдущей страницы

Опция	Значение
`-q, --query`	Вывести информацию о пакете.
`-a, --all`	Выполняет запрос ко всем установленным пакетам.
`--changelog`	Вывести информацию об изменениях в пакете.
`-l, --list`	Вывести список файлов в пакете.
`-P, --provides`	Вывести функциональность, предоставляемую пакетом.
`-R, --requires`	Вывести пакеты, от которых зависит этот пакет.
`-v, --verify`	Выполнить проверку метаданных пакета и его контрольной суммы.
`--version`	Вывести номер версии утилиты.
`--help`	Вывести справку об использовании утилиты.

Установка последней версии пакета/группы пакетов

Утилита `dnf` используется для установки последней версии пакета или группы пакетов с учетом существующих зависимостей.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 24: Опции утилиты `dnf` и их значения

Опция	Значение
`install`	Используется для установки последней версии пакета с учетом существующих зависимостей.
`reinstall`	Используется для переустановки пакета с идентичной версией.
`update`	Используется для обновления всех пакетов в системе.
`download`	Используется для загрузки пакета из репозитория.
`downgrade`	Используется для понижения версии пакета с версии, установленной на данный момент, до предыдущей самой высокой версии или указанной версии.
`remove`	Используется для удаления указанных пакетов из системы, а также для удаления пакетов, зависящих от удаляемых пакетов.
`info`	Используется для вывода описаний и общей информации о доступных пакетах.
`search`	Используется для поиска пакетов.
`list`	Используется для вывода различной информации о доступных пакетах.
`repolist all`	Используется для вывода списка всех репозиториев.
`clean`	Используется для удаления различных данных, накапливающихся со временем в кэше утилиты.
`history`	Используется для вывода истории использования утилиты.
`groupinstall`	Используется для установки последней версии всех пакетов из группы с учетом существующих зависимостей.
`groupupdate`	Используется для обновления всех пакетов из группы.
`groupremove`	Используется для удаления всех пакетов из группы.
`groupinfo`	Используется для вывода списка пакетов, относящихся к группе.
`grouplist`	Используется для вывода имен всех существующих групп пакетов.
`provides`	Используется, чтобы выяснить, какой пакет предоставляет тот или иной файл.
`repoquery --requires`	Вывести зависимости неустановленного пакета.
`repoquery --requires --resolve`	Вывести список пакетов, которые необходимы для удовлетворения зависимостей.
`-v, --verbose`	Запустить с большим количеством отладочной информации.
`-d, --debuglevel`	Устанавливает уровень отладки.
`-h, --help`	Вывести справку и выйти.

Стирание данных

Введение

Средства стирания данных предоставляют возможности безвозвратного удаления ставших ненужными данных и обеспечения недоступности остаточной информации путем многократной перезаписи использованных мест памяти специальными последовательностям.

Заполнение случайными числами места, занятого файлами

Утилита `shred` позволяет заполнять случайными числами место, занятое файлами.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 25: Опции утилиты `shred` и их значения

Опция	Значение
`-f, --force`	Изменить права для разрешения записи, если это необходимо.
`-n, --iterations=N`	Перезаписать файл N раз вместо 3-х по умолчанию.
`--random-source=FILE`	Перезаписать файл случайными данными, взятыми из файла с именем `FILE`.
`-s, --size=N`	Перезаписать только N байт. Можно использовать суффиксы `K`, `M`, `G` для указания размерности: килобайт, мегабайт, гигабайт.
`-u, --remove`	Обрезать и удалить файл после перезаписи. По умолчанию файлы не удаляются.
`-v, --verbose`	Показывать ход выполнения.
`-x, --exact`	Не округлять размер файла до следующего целого блока.
`-z, --zero`	На последней итерации перезаписать файл нулями.
`--version`	Показать версию утилиты и выйти.
`--help`	Показать справку и выйти.

Пример: заполним место, занятое файлом `filename`, с последующим удалением файла.

Для этого выполним следующую команду:

```
$ sudo shred -u -z filename
```

Стирание данных в свободном пространстве раздела, в котором находится директория

Утилита `sfill` позволяет стирать данные в свободном пространстве раздела, в котором находится заданная директория. Стирание производится в четыре шага:

1. Однократная перезапись числами 255 (0xFF).
2. Пятикратная перезапись случайными числами.
3. Двадцатисемикратная перезапись специальными числами.
4. И еще один раз пятикратная перезапись случайными числами.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 26: Опции утилиты `sfill` и их значения

Опция	Значение
`-f`	Выполнение более быстрым образом за счет пропуска второго и четвертого шагов перезаписи случайными числами.
`-i`	Очистка свободного пространства только индексного дескриптора, но не свободного пространства жесткого диска.
`-I`	Очистка свободного пространства только жесткого диска без затрагивания свободного пространства индексного дескриптора.
`-l`	Выполнение более быстрым образом за счет пропуска третьего и четвертого шагов или путем выполнения только одного шага перезаписи данных нулевыми значениями, если эту опцию задать дважды (например, `sdmem -l -l`).
`-v`	Работа будет сопровождаться выводом динамической строки, показывающей прогресс её выполнения.
`-z`	На четвертом шаге вместо перезаписи случайными числами выполнять перезапись нулями.

Пример: выполним очистку свободного пространства.

Для этого выполним следующую команду:

```
$ sudo sfill -vz /mnt/
Using /dev/urandom for random input.
Wipe mode is secure (38 special passes)
Wiping now ...
Creating /mnt/00000000.000 ... ************************* Wiping inodes ...
Done ... Finished
```

Стирание данных в разделах подкачки

Утилита `sswap` позволяет стирать данные в разделах подкачки. Алгоритм стирания данных абсолютно такой же, как и у утилиты `sfill`.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 27: Опции утилиты `sswap` и их значения

Опция	Значение
`-f`	Выполнение более быстрым образом за счет пропуска второго и четвертого шагов перезаписи случайными числами.
`-l`	Выполнение более быстрым образом за счет пропуска третьего и четвертого шагов или путем выполнения только одного шага перезаписи данных нулевыми значениями, если эту опцию задать дважды.
`-v`	Работа будет сопровождаться выводом динамической строки, показывающей прогресс её выполнения.
`-z`	На четвертом шаге вместо перезаписи случайными числами выполнять перезапись нулями.

Стирание данных в оперативной памяти

Утилита `sdmem` позволяет стирать данные в оперативной памяти. Алгоритм стирания данных почти такой же, как и у утилиты `sfill`, но с тем отличием, что на первом шаге однократная перезапись производится числами 0 (0x00).

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 28: Опции утилиты `sswap` и их значения

Опция	Значение
`-f`	Выполнение более быстрым образом за счет пропуска второго и четвертого шагов перезаписи случайными числами.
`-l`	Выполнение более быстрым образом за счет пропуска третьего и четвертого шагов или путем выполнения только одного шага перезаписи данных нулевыми значениями, если эту опцию задать дважды.
`-v`	Работа будет сопровождаться выводом динамической строки, показывающей прогресс её выполнения.

Контроль целостности

Введение

Средства контроля целостности предоставляют возможности контроля целостности обрабатываемых данных и используемого программного обеспечения.

Вычисление и сверка контрольной суммы файла

Утилита `sha256sum` позволяет вычислять контрольные суммы файлов по алгоритму SHA-256 и осуществлять их сверку с другими контрольными суммами, хранящимися в файле.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 29: Опции утилиты `sha256sum` и их значения

Опция	Значение
`-b, --binary`	Позволяет считывать данные из файлов в двоичном режиме.
`-c, --check`	Позволяет осуществить сверку рассчитанного значения контрольной суммы с некоторым другим значением контрольной суммы, хранящимся в файле, имя которого должно быть передано утилите в качестве аргумента.
`--tag`	Выводить рассчитанную контрольную сумму в формате BSD.
`-t, --text`	Читать в текстовом режиме (по умолчанию).
`-z, --zero`	Завершать каждую выводимую строку NUL, а не символом новой строки и выключить экранирование имени файла.
`--ignore-missing`	Не сообщать или прерываться при отсутствии файлов.
`--quiet`	При сверке контрольных сумм позволяет не выводить сообщение `OK` для каждого успешного случая сверки контрольных сумм.
`--status`	При сверке контрольных сумм позволяет в конце работы утилиты не выводить ничего, кроме кода сверки контрольных сумм.
`--strict`	При сверке контрольных сумм позволяет выводить ненулевое значение для неправильно отформатированных строк контрольной суммы.
`-w, warn`	При сверке контрольных сумм позволяет выводить предупреждения о неправильно отформатированных строках контрольной суммы.
`--version`	Показать версию утилиты и выйти.
`--help`	Показать справку и выйти.

Пример: подсчитаем контрольную сумму файла с журналом аудита по алгоритму SHA-256.

Для этого выполним следующую команду:

```
$ sudo sha256sum /var/log/audit/audit.log
65sh8467h74j8kf36mf76356r853k25748864ud7k835hr2kwuv9l4q73m74x7a49 /var/log/audit/audit.log
```

Также МСВСфера ОС предоставляет возможность вычислять контрольные суммы файлов по алгоритму ГОСТ. Для этого необходимо установить пакет `gostsum`.

Пример: подсчитаем контрольную сумму файла с журналом аудита по алгоритму ГОСТ.

Для этого выполним следующую команду:

```
$ sudo gostsum /var/log/audit/audit.log
054h7j3a8af6kf2h9lk257r67k2974rfh47a5hg34n3h7s25ak3674wrmc475ls5 /var/log/audit/audit.log
```

Проверка целостности данных

Утилита `aide` предоставляет возможности проверки целостности данных.

1. Перед началом использования необходимо установить утилиту `aide` с помощью следующей команды (необходимо по запросу системы указать пароль суперпользователя root):

```
$ sudo dnf install aide
```

2. Затем необходимо инициализировать базу данных для хранения состояний файлов с помощью следующей команды (необходимо по запросу системы указать пароль суперпользователя root):

```
$ sudo aide --init
```

В конфигурации по умолчанию команда `aide --init` проверяет только файлы и директории, заданные в конфигурационном файле `/etc/aide.conf`. Чтобы добавить необходимые файлы и директории в базу AIDE, а также изменить параметры, необходимо внести соответствующие изменения в конфигурационный файл `/etc/aide.conf`.

3. Перед началом использования инициализированной базы данных удалите `.new` из имени файла с помощью следующей команды:

```
$ sudo mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

4. Для изменения места расположения базы AIDE необходимо в файле `/etc/aide.conf` изменить значение параметра `DBDIR`. Для обеспечения дополнительной безопасности рекомендуется хранить базу данных, конфигурацию и файл `/usr/sbin/aide` в безопасном месте.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице.

Таблица 30: Опции утилиты `aide` и их значения

Опция	Значение
`-i, --init`	Инициализирует базу данных хранения состояний файлов. Созданная после инициализации база данных должна быть размещена в таком месте, из которого при осуществлении последующей проверки данные могли бы быть считаны. В противном случае при попытке осуществления проверки будет выведена информация об ошибке считывания.
`-C, --check`	Проверяет базу данных состояний файлов на наличие несоответствий, для чего необходимо иметь инициализированную базу данных. Эта опция выполняется по умолчанию, если не указать никакой другой опции.
`-u, --update`	Проверяет базу данных и обновляет её. При этом входные и выходные базы данных должны быть разными.
`-E, --compare`	Сравнивает две базы данных, которые должны быть определены в конфигурационном файле.
`-D, --config-check`	Осуществляет считывание данных из конфигурационного файла, уведомляя обо всех обнаруженных ошибках.
`-c, --config=configfile`	Позволяет считывать конфигурацию из указанного файла вместо используемого по умолчанию конфигурационного файла `./aide.conf`.
`-B, --before="configparameters"`	Позволяет обрабатывать указанные конфигурационные параметры до считывания данных из конфигурационного файла.
`-A, --after="configparameters"`	Позволяет обрабатывать указанные конфигурационные параметры после считывания данных из конфигурационного файла.

продолжение на следующей странице

Таблица 30 – продолжение с предыдущей страницы

Опция	Значение
`-V verbosity_level, --verbose=verbosity_level`	Определяет детальность обработки данных. На месте параметра `verbosity_level` может находиться целочисленное значение в диапазоне от `0` до `255`. По умолчанию значение данного параметра равно `5`. Если вызвать данную ощию, но не присвоить целочисленное значение параметру `verbosity_level`, то ему автоматически будет присвоено значение, равное `20`. Этот параметр переопределяет значение, установленное в конфигурационном файле.
`-r reporter, --report=reporter`	Определяет место (URL), в которое утилита должна отправлять свои результаты работы.

Пример: проверим систему, сравнив `aide.db` и текущее состояние системы, без обновления `aide.db.new`.

Для этого выполним следующую команду:

```
$ sudo aide --check
AIDE, version 0.15.1
### All files match AIDE database. Looks okay!
```

Если произошло изменение файлов системы, то будет получено соответствующее уведомление:

```
$ sudo aide --check
AIDE 0.15.1 found differences between database and filesystem!
Start timestamp: 2023-03-28 09:12:21
Summary:
   Total number of files: 264416
   Added files:           1
   Removed files:         0
   Changed files:         3
```

Рекомендуется проводить проверку каждый день. Вы можете настроить проведение ежедневной проверки с помощью команды `cron`. Например, настроим проверку на 03:00, добавив в файл `/etc/crontab` следующую строку:

```
00 3 * * * root /usr/sbin/aide --check
```

Также, мы рекомендуем обновлять основную базу AIDE после обновлений системы и пакетов, а также изменений в конфигурационных файлах.

Для обновления основной базу AIDE выполните следующую команду:

```
$ sudo aide --update
```

Будет создан файл `/var/lib/aide/aide.db.new.gz`. Чтобы начать использовать вновь созданный файл для проверки целостности данных, удалите `.new` из имени файла.

Обеспечение надёжного функционирования

Введение

Средства обеспечения надёжного функционирования предоставляют возможности резервного копирования и восстановления данных и программного обеспечения при сбоях и отказах, а также возможности функционирования отдельных экземпляров системы на нескольких технических средствах в отказоустойчивом режиме, обеспечивающем доступность сервисов и данных при выходе из строя одного из технических средств или при исчерпании вычислительных ресурсов.

Архивация файлов и директорий

Утилита `tar` позволяет архивировать файлы и директории со всеми их поддиректориями и файлами, а затем восстанавливать их из архива, т.е. является удобным средством для создания резервных копий.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленным в таблице:

Таблица 31: Опции утилиты `tar` и их значения

Опция	Значение
`-c, --create`	Создать новый архив.
`-r, --append`	Присоединить файлы к концу архива.
`--delete`	Удалить файл из архива.
`-t, --list`	Вывести список содержимого архива.
`-A, --catenate, --concatenate`	Присоединить существующий архив к другому архиву.
`-x, --extract, -get`	Извлечь файлы из архива.
`-u, --update`	Добавить в архив более новые версии файлов.
`-C, --directory=DIR`	Сменить директорию перед выполнением операции на `DIR`.
`--f, --file=ARCHIVE`	Вывести результат в архивный файл или в устройство `ARCHIVE`.
`-d, --diff`	Осуществить проверку на наличие различий между архивом и некоторой файловой системой.
`-v, --verbose`	Выводить подробную информацию о процессе выполнения команды.

Пример: в примере директория `mydir` и все её поддиректории сначала сохраняются в файле `myarch.tar`:

```
$ tar cf myarch.tar mydir
```

а затем извлекаются из архива:

```
$ tar xf myarch.tar
```

А этот скрипт организует хранение четырех последних резервных копий директории `/var/www` в директории `/opt/backup/www-backup`. Первая версия будет всегда иметь номер 0, последняя — номер 3. При создании новых версий старые будут удаляться. Сами резервные копии хранятся в сжатом виде.

```
#! /bin/bash
cd /opt/backup/www-backup
rm www-dump-3.tar.gz
cp www-dump-2.tar.gz www-dump-3.tar.gz
cp www-dump-1.tar.gz www-dump-2.tar.gz
cp www-dump-0.tar.gz www-dump-1.tar.gz
tar --selinux --acls --xattrs --czf www-dump-o.tar.gz /var/www
```

Создание архивов и извлечение файлов из них

Утилита `cpio` используется для создания архивов и извлечения файлов из них, а также для копирования файлов в целях их переноса из текущей директории в другую. Поддерживает множество различных архивных форматов. При извлечении файлов из архива утилита автоматически распознает, каким типом обладает архив, с которым она взаимодействует.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 32: Опции утилиты `cpio` и их значения

Опция	Значение
`-o, --create`	Копировать файлы в архив.
`-A, --append`	Добавить файлы в архив. Может быть использована только в связке с опцией `-O`.
`-i, --extract`	Копирует файлы из архива или выводит список содержимого некоторого архива.
`-p, --pass-through`	Копирует файлы из одной файловой структуры в другую, комбинируя при этом режимы работы, использующиеся при передаче опций `-i` и `-O`, но не используя при этом архивы.
`-a, --reset-access-time`	Сбрасывает времена обращения к входным файлам после их копирования, так что при использовании данной опции будет нельзя распознать, что файлы были скопированы.

Пример: в примере сначала флеш-носитель монтируется как устройство `/mnt`:

```
$ mount /dev/sdb4 /mnt
```

Затем создается и записывается на флеш-носитель резервная копия директории `/lib`:

```
$ find /lib/ | cpio -o > /mnt/2/backup.cpi
```

Для того чтобы восстановить все файлы в директорию `/lib` из созданной ранее архивной копии, необходимо выполнить следующую команду:

```
$ cpio -ivmd /lib/\* < /mnt/2/backup.cpio
```

Резервное копирование данных

Утилита `amanda` обладает возможностью резервного копирования данных, хранящихся на множестве компьютеров в вычислительной сети. Она реализует клиент-серверную модель и использует следующие утилиты:

- **клиентская утилита `amandad`, взаимодействующая с сервером системы.**

  Во время своего выполнения вызывает другие утилиты:

  - `selfcheck` (проверка конфигурации клиента);
  - `sendsize` (оценка объема резервной копии);
  - `sendbackup` (выполнение операции резервного копирования);
  - `amcheck` (проверка конфигурации системы).

- **серверная утилита `amdump`, инициирующая все операции резервного копирования.**

  Во время своего выполнения использует другие утилиты и контролирует их выполнение:

  - `planner` (определение того, что надо копировать);
  - `driver` (интерфейс к внешнему устройству);
  - `dumper` (связывается с клиентским процессом `amandad`);
  - `taper` (запись данных на внешнее устройство);
  - `amreport` (подготовка сообщения о выполненном копировании).

- **административные утилиты:**

  - `amcheck` (проверка готовности системы к работе);
  - `amlabel` (записать метку на сменный носитель перед использованием в системе);
  - `amcleanup` (очистить систему после неплановой перезагрузки сервера или после непланового завершения операции резервного копирования);
  - `amflush` (переписать данные из дискового кэша на внешний носитель);
  - `amadmin` (выполнение большого количества различных административных операций).

- **утилиты восстановления данных:**

  - `amrestore` (восстановление данных с носителей, на которых записаны резервные копии, выполненные системой);
  - `amrecover` (программа для интерактивного восстановления данных с резервных копий).

Создание дисковых RAID-массивов

Утилита `mdadm` позволяет создавать так называемые дисковые RAID-массивы с использованием технологии распределения данных по нескольким дискам с целью достижения избыточности, отказоустойчивости, сокращения задержек и/или увеличения скорости чтения и записи, а также для улучшения возможностей восстановления данных в случае отказа.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 33: Опции утилиты `mdadm` и их значения

Опция	Значение
`-A, --assemble`	Режим сборки ранее созданного массива и его активации.
`-B, --build`	Режим сборки массива без суперблоков.
`-C, --creat`	Режим сборки нового массива.
`-F, --follow, --monitor`	Режим слежения за состоянием устройств.
`-G, --grow`	Режим расширения или уменьшения размера массива.
`-N, --name`	Устанавливает имя массива.
`-n, --raid-devices`	Указывает количество активных устройств в массиве.
`-x, --space-device`	Указывает количество запасных устройств в массиве.
`-z, --size`	Указывает объем пространства, используемого для каждого диска.
`-l, --level`	Устанавливает уровень массива.
`-c, --config`	Указывает файл конфигурации. По умолчанию `/etc/mdadm.conf`.
`-f, --fail`	Помечает перечисленные устройства как неисправные.
`-S, --stop`	Деактивирует массив и освобождает все ресурсы.
`-V --version`	Выводит информацию о версии утилиты.
`-h, --help`	Выводит справку об утилите.

Фильтрация сетевого потока

Введение

Средства фильтрации сетевого потока предоставляют возможности фильтрации входящих и исходящих сетевых потоков на основе установленного набора правил с учетом атрибутов безопасности и используемых сетевых протоколов, а также управления правилами фильтрации сетевых потоков; регистрации и учета выполнения проверок при фильтрации сетевых потоков.

Настройка файрвола (брандмауэра)

Утилита `firewall-cmd` позволяет настраивать работу файрвола (брандмауэра), осуществляющего фильтрацию сетевых потоков при помощи определения так называемых зон, иными словами, наборов правил, которые управляют трафиком на основе уровня доверия к той или иной сети.

Существуют следующие зоны:

- `drop` — самый низкий уровень доверия к сети. Весь входящий трафик сбрасывается без ответа. Поддерживаются только исходящие соединения;
- `block` — эта зона похожа на предыдущую, но при этом входящие запросы сбрасываются с сообщением `icmp-host-prohibited` или `icmp6-adm-prohibited`;
- `public` — эта зона представляет публичную сеть, которой нельзя доверять, однако поддерживает входящие соединения в индивидуальном порядке;
- `external` — зона внешних сетей. Поддерживает маскировку NAT, благодаря чему внутренняя сеть остается закрытой, но с возможностью получения доступа;
- `internal` — обратная сторона зоны `external`. Компьютерам в этой зоне можно доверять.

Доступны дополнительные сервисы:

- `dmz` — используется для компьютеров, расположенных в DMZ (зонах изолированных компьютеров, которые не будут иметь доступа к остальной части сети). Поддерживает только некоторые входящие соединения;
- `work` — зона рабочей сети. Большинству машин в сети можно доверять, доступны дополнительные сервисы;
- `home` — зона домашней сети. Окружению можно доверять, но поддерживаются только определённые пользователем входящие соединения;
- `trusted` — всем машинам в сети можно доверять.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 34: Опции утилиты `firewall-cmd` и их значения

Опция	Значение
`--state`	Вывести состояние файрвола.
`--reload`	Перезагрузить правила из постоянной конфигурации.
`--complete-reload`	Жёсткая перезагрузка правил с разрывом всех соединений.
`--runtime-to-permanent`	Перенести настройки `runtime` в постоянную конфигурацию.
`--permanent`	Использовать постоянную конфигурацию.
`--get-default-zone`	Отобразить зону, используемую по умолчанию.
`--set-default-zone`	Установить зону по умолчанию.
`--get-active-zones`	Отобразить активные зоны.
`--get-zones`	Отобразить все доступные зоны.
`--get-services`	Вывести предопределенные сервисы.
`--list-all-zones`	Вывести конфигурацию всех зон.
`--new-zone`	Создать новую зону.
`--delete-zone`	Удалить зону.
`--list-all`	Вывести всё, что добавлено, из выбранной зоны.
`--list-services`	Вывести все сервисы, добавленные к зоне.
`--add-service`	Добавить сервис к зоне.
`--remove-service`	Удалить сервис из зон.
`--list-ports`	Отобразить порты, добавленные к зоне.
`--add-port`	Добавить порт к зоне.
`--remove-port`	Удалить порт из зоны.
`--query-port`	Показать, добавлен ли порт к зоне.
`--list-protocols`	Вывести протоколы, добавленные к зоне.
`--add-protocol`	Добавить протокол к зоне.
`--remove-protocol`	Удалить протокол из зоны.
`--list-source-ports`	Вывести порты источника, добавленные к зоне.
`--add-source-port`	Добавить порт-источник к зоне.
`--remove-source-port`	Удалить порт-источник из зоны.
`--list-icmp-blocks`	Вывести список блокировок icmp.
`--add-icmp-block`	Добавить блокировку icmp.
`--remove-icmp-block`	Удалить блокировку icmp.
`--add-forward-port`	Добавить порт для перенаправления в NAT.
`--remove-forward-port`	Удалить порт для перенаправления в NAT.
`--add-masquerade`	Включить NAT.
`--remove-masquerade`	Удалить NAT.

Пример: настройка правила блокировки адреса получателя может выглядеть следующим образом:

```
$ sudo firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -d 192.168.10.20 -j DROP
success
```

Пример: настройка правила отбрасывания всех входящих соединений по протоколу IPv4 может выглядеть следующим образом:

```
$ sudo firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -j DROP
success
```

Пример: настройка правила отбрасывания всех исходящих пакетов UDP может выглядеть следующим образом:

```
$ sudo firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p upd -j DROP
success
```

Конфигурационный файл /etc/firewalld/firewalld.conf

Конфигурационный файл `/etc/firewalld/firewalld.conf` содержит основные параметры конфигурации для файрвола `firewalld`.

- `DefaultZone` — устанавливает зону по умолчанию для соединений или интерфейсов;

- `MinimalMark` — с этой опцией блок меток может быть зарезервирован для частного использования. Используются только отметки над этим значением. Значение по умолчанию равно `100`;
- `CleanupOnExit` — если `firewalld` останавливается, он очищает все правила. Если для этого параметра установлено значение `no` или `false`, текущие правила останутся нетронутыми. Значением по умолчанию является `yes` или `true`;
- `Lockdown` — если эта опция включена, изменения `firewalld` с интерфейсом D-Bus будут ограничены приложениями, которые перечислены в белом списке блокировки. Значением по умолчанию является `no` или `false`;
- `IPv6_rpfilter` — если эта опция включена, выполняется проверка фильтра обратного пути для пакета для IPv6. Если ответ на пакет будет отправлен через тот же интерфейс, на который поступил пакет, пакет совпадет и будет принят. В противном случае он будет отброшен. Для IPv4 `rp_filter` управляется с помощью `sysctl`;
- `IndividualCalls` — если этот параметр отключен, используются комбинированные вызовы restore, а не отдельные вызовы, чтобы применить изменения к файрволу. Использование отдельных вызовов увеличивает время, необходимое для применения изменений;
- `LogDenied` — добавление правил ведения журнала непосредственно перед отклонением и удалением правил в цепочках `INPUT`, `FORWARD` и `OUTPUT` для правил по умолчанию, а также окончательных правил отклонения и отбрасывания в зонах для настроенного типа пакета канального уровня. По умолчанию установлено `off` — отключение ведения журнала.
- `AutomaticHelpers` — для безопасного использования протокола IPv4 `iptables` и помощников по отслеживанию соединений этот параметр рекомендуется отключить. Возможные значения: `yes`, `no`, `system`. По умолчанию установлено `system`;
- `FirewallBackend` — выбирает реализацию брандмауэра. Возможные значения: `nftables` (по умолчанию) или `iptables`. Это относится ко всем примитивам `firewalld`. Единственным исключением являются прямые и сквозные правила, которые всегда используют традиционные `iptables`, `ip6tables` и `ebtables`.

Предупреждение

Внимание! Не следует выдавать права `sudo` на утилиту `iptables-save`. Утилита `iptables-save` при помощи ключа `-f` позволяет записывать дамп правил в файл. Соответственно, имея права `sudo`, пользователь сможет переписать любой файл в системе.

Мониторинг функционирования

Введение

Средства мониторинга функционирования предоставляют возможности слежения и сбора информации о выполнении пользовательских процессов и состоянии сетевого трафика.

Анализ системных журналов

Утилита `logwatch` позволяет проводить анализ системных журналов по различным критериям с возможностью составления отчётов.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 35: Опции утилиты `logwatch` и их значения

Опция	Значение
`--detail level`	Уровень детализации отчета. Может быть положительным целым числом или `high`, `med`, `low`, которые соответствуют целым числам 10, 5 и 0 соответственно.
`--debug level`	Уровень отладки. Может варьироваться от 0 до 100.
`--logfile log-file-group`	Обрабатывать только набор указанных файлов журналов.
`--service service-name`	Обрабатывать только указанную службу.
`--print`	Вывести результаты на экран.
`--mailto address`	Отправить результаты по указанному адресу электронной почты.
`--save file-name`	Сохранить вывод в указанный файл вместо отображения на экране или отправки по электронной почте.
`--range range`	Диапазон дат для обработки.
`--archives`	Искать в архивных журналах.
`--logdir directory`	Обрабатывать файлы журналов из указанного каталога, а не из каталога по умолчанию.
`--hostname hostname`	Обрабатывать файлы журналов только указанного хоста.

Получение информации о выполняемых процессах

Утилита `top` предназначена для получения информации о выполняемых процессах.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 36: Опции утилиты `top` и их значения

Опция	Значение
`-u`	Отображать только процессы с заданным идентификатором или именем пользователя.
`-S`	Отображать системные процессы.
`-n`	Изменить число отображаемых процессов на заданное число.
`-i`	Работа в интерактивном режиме. Задается по умолчанию.
`-I`	Не отображать бездействующие процессы. По умолчанию отображаются как активные, так и бездействующие процессы.
`-c`	Переключение отображения командных строк на отображение имён программ и наоборот.
`-s`	Задает временной интервал задержки между обновлениями экрана. По умолчанию 5 секунд.
`-b`	Работа в пакетном режиме. Может использоваться для отправки результатов в другие программы или в файл.
`-o`	Задает имя поля, по которому будет осуществляться сортировка. Используется в основном для пакетного режимах.
`-w`	Задает форматирование вывода по ширине. Количество строк считается неограниченным.
`-v`	Показать версию утилиты и выйти.
`-h`	Показать справку и выйти.

Получение информации о состоянии текущих процессов

Утилита `ps` используется для получения информации о состоянии текущих процессов.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 37: Опции утилиты `ps` и их значения

Опция	Значение
`-u`	Выводить информацию только о процессах с заданными списком эффективными идентификационными номерами или идентификаторами пользователей.
`-Y`	Выводить информацию только о процессах с заданными списком реальными идентификационными номерами или идентификаторами пользователей.
`-g`	Выводить информацию только о процессах с заданными списком идентификационными номерами групп.
`-G`	Выводить информацию только о процессах с заданными списком реальными идентификационными номерами групп.
`-a`	Выводить информацию о состоянии наиболее часто запрашиваемых процессов.
`-e`	Выводить информацию для всех процессов.
`-d`	Выводить информацию о всех процессах, кроме лидеров сеансов.
`-p`	Выводить информацию только для запущенных процессов.
`-G`	Выводить информацию о процессах, чьи реальные номера групп указаны в заданном списке.
`-o`	Выводить информацию в заданном формате.

Мониторинг и анализ сетевого трафика

Утилита `tcpdump` предназначена для мониторинга и анализа сетевого трафика.

Состоит из двух частей: захват пакетов с копированием их в так называемый буфер и отображение захваченных пакетов из буфера.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 38: Опции утилиты `tcpdump` и их значения

Опция	Значение
`-i`	Задает интерфейс, с которого необходимо анализировать трафик.
`-y`	Устанавливает тип канала передачи данных для использования во время захвата пакетов.
`-e`	Включает вывод данных канального уровня.
`-v`	Вывод дополнительной информации.
`-w`	Задает имя файла, в котором будет сохраняться собранная информация.
`-p`	Захватывать только трафик, предназначенный данному узлу.
`-q`	Переводит работу в «бесшумный режим», в котором пакет анализируется на транспортном уровне, а не на сетевом.
`-t`	Отключает вывод меток времени.
`-A`	Вывод пакетов в формате ASCII без заголовков канального уровня.
`-B`	Установить размер буфера захвата.
`-D`	Вывести список доступных сетевых интерфейсов, на которых может осуществляться захват пакетов.

Получение информации о сеансах пользователей

Утилита `ac` предназначена для получения информации о сеансах пользователей.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 39: Опции утилиты `ac` и их значения

Опция	Значение
`-p`	Выводить итоговое время сеансов каждого пользователя.
`-d`	Кроме общих итогов, выводить итоги за каждый день.
`-a`	При выводе ежедневных итогов не пропускать дни, когда входов в систему не было.
`-y`	Выводить год при отображении даты.
`-z`	Если итоговое значение равно нулю, то выводить его. По умолчанию не выводится.
`-v`	Вывести номер версии.
`-h`	Вывести краткую справку.

Получение информации о последних выполненных командах

Утилита `lastcomm` позволяет получить информацию о последних выполненных командах.

Режимы работы утилиты и выполняемые функции задаются набором опций, перечисленных в таблице:

Таблица 40: Опции утилиты `lastcomm` и их значения

Опция	Значение
`-E`	Выводить время начала процесса выполнения команды.
`-S`	Выводить время завершения процесса выполнения команды.
`-c`	Выводить количество использованного процессорного времени.
`-e`	Выводить количество использованного прошедшего времени.
`-s`	Выводить количество использованного системного времени.
`-u`	Выводить количество использованного пользовательского времени.
`-f`	Использовать заданный файл в качестве источника учетных данных. Он может быть либо стандартным, либо расширенным файлом учёта процесса.
`-x`	Использовать текущий расширенный файл учёта процесса.

Создание виртуальной машины

Создание виртуальной машины с помощью утилиты virt-install

Одним из самых простых способов создания виртуальных машин с помощью командной строки является утилита `virt-install`.

Для вызова команды `virt-install` используется стандартный синтаксис:

```
$ virt-install [аргументы]
```

`virt-install` поддерживает как графический режим установки операционной системы с использованием протоколов VNC или SPICE, так и установку в текстовом режиме с помощью последовательной консоли. Во время создания виртуальной машины она может быть настроена на использование одного или нескольких дисков, сетевых интерфейсов, аудио устройств, аппаратных USB или PCI устройств и т.д.

В качестве установочного носителя может использоваться ISO-образ или виртуальный CD-ROM накопитель, установочное дерево дистрибутива, доступное по протоколам HTTP, HTTPS, FTP либо размещённое локально. Также поддерживается сетевая загрузка с использованием протокола PXE, импорт готовых образов дисков, полностью автоматическая установка операционной системы с помощью kickstart-файлов или опции `--unattended`.

Аргументы командной строки virt-install

У многих аргументов команды `virt-install` есть дополнительные параметры, которые указываются следующим образом: `--аргумент опция1=значение опция2=значение`. Используйте синтаксис `--аргумент=?` чтобы увидеть полный список таких параметров, например:

```
$ virt-install --disk=?
```

Большинство аргументов `virt-install` являются опциональными. В случае задания значения опции `--os-variant` либо успешного автоматического определения типа гостевой системы, для таких аргументов будут использованы соответствующие значения по умолчанию, определённые профилем устанавливаемой операционной системы. Профили предоставляются пакетом `osinfo-db`. В случае отсутствия профиля для устанавливаемой ОС потребуется определить как минимум следующие опции: `--memory`, настройки хранилища (`--disk` или `--filesystem`) и метод установки (`--cdrom`, `--location`).

При установке МСВСфера ОС через профили используются следующие значения:

- `jeos` — минимальная серверная конфигурация МСВСФера 9 Сервер.
- `desktop` — конфигурация для рабочих станций МСВСфера 9 АРМ.

Аргументы, передаваемые утилите `virt-install`, можно условно сгруппировать по их назначению:

- Параметры подключения — определяют тип используемого гипервизора и путь (ссылку) для подключения к нему.
- Общие параметры — общие параметры, применимые ко всем типам гостевых систем.
- Параметры установки — определяют каким образом будет выполняться установка гостевой операционной системы.
- Параметры гостевой системы — задают тип устанавливаемой операционной системы либо управляют настройками автоматического определения типа.
- Параметры хранилища — опции, связанные с настройкой хранилища виртуальной машины.
- Параметры сети — опции, связанные с настройкой сети виртуальной машины;
- Параметры графики — опции, связанные с настройкой графической подсистемы виртуальной машины.
- Параметры виртуализации — опции для переопределения используемого механизма виртуализации.
- Параметры устройств — опции для подключения физических и виртуальных устройств к виртуальной машине.
- Другие опции — опции, не вошедшие ни в одну из предыдущих групп.

Примеры использования virt-install

Следующая команда создаст в пользовательской сессии QEMU виртуальную машину `msvsphere-9-server` с двумя гигабайтами оперативной памяти, двумя виртуальными процессорами и виртуальным qcow2-диском объёмом двадцать гигабайт. Виртуальная машина будет запущена в режиме BIOS, в качестве установочного носителя будет использован ISO-образ `/srv/iso/MSVSphere-9.5-x86_64-server.iso`:

```
$ virt-install --name msvsphere-9-server \
      --cdrom /srv/iso/MSVSphere-9.5-x86_64-server.iso \
      --memory 2048 --vcpus 2 --disk size=20 --os-variant msvsphere9
```

Установка операционной системы МСВСфера 9 в режиме UEFI с отключённой поддержкой Secure Boot, в качестве источника установки используется установочное дерево дистрибутива, размещённое на официальном зеркале:

```
$ virt-install --name msvsphere-9-server \
      --memory 2048 --vcpus 2 --disk size=20 --os-variant msvsphere9 \
      --location https://repo1.msvsphere-os.ru/msvsphere/9/BaseOS/x86_64/os/ \
      --boot uefi,loader=/usr/share/edk2/ovmf/OVMF_CODE.fd,loader_ro=yes,loader_type=pflash,
↪nvram_template=/usr/share/edk2/ovmf/OVMF_VARS.fd,loader_secure=no
```

Следующая команда создаст виртуальную машину в системной сессии QEMU и выполнит автоматическую установку операционной системы МСВСфера 9 в режиме

UEFI с включённой поддержкой Secure Boot, сценарий установки определён в kickstart-файле `msvsphere-9.ks`:

```
$ virt-install --name msvsphere-9-server --connect qemu:///system \
      --memory 2048 --vcpus 2 --disk size=20 --os-variant msvsphere9 \
      --location https://repo1.msvsphere-os.ru/msvsphere/9/BaseOS/x86_64/os/ \
      --boot uefi,loader=/usr/share/edk2/ovmf/OVMF_CODE.secboot.fd,loader_ro=yes,loader_
↪type=pflash,nvram_template=/usr/share/edk2/ovmf/OVMF_VARS.secboot.fd,loader_secure=yes \
      --initrd-inject msvsphere-9.ks --extra-args "inst.ks=file:/msvsphere-9.ks"
```

Пример kickstart-файла (`msvsphere-9.ks` в примере выше) для автоматической установки системы в минимальной конфигурации без графического интерфейса:

```
# путь к установочному дереву дистрибутива
url --url https://repo1.msvsphere-os.ru/msvsphere/9/BaseOS/x86_64/kickstart/

# список репозиториев, которые необходимо подключить во время установки
repo --name=BaseOS --baseurl=https://repo1.msvsphere-os.ru/msvsphere/9/BaseOS/x86_64/os/
repo --name=AppStream --baseurl=https://repo1.msvsphere-os.ru/msvsphere/9/AppStream/x86_64/os/

# выполнять установку в текстовом режиме
text
# не выполнять настройку графического сервера Xorg/Wayland
skipx
# автоматически принимать условия лицензии
eula --agreed
# не запускать ассистента по настройке во время первого запуска
firstboot --disabled

# использовать английский язык как во время установки, так и на установленной
# системе. Дополнительно включить поддержку русского языка
lang en_US --addsupport=ru_RU
# настраивает раскладку клавиатуры, в данном случае будет использоваться только
# английская в американском варианте
keyboard us
# установить часовой пояс в московское время (GMT+3), флаг --utc указывает на
# то, что аппаратные часы хранят время в часовом поясе UTC
timezone Europe/Moscow --utc

# автоматически настроить сеть используя протокол DHCP
network --bootproto=dhcp
# включить брандмауэр и отрыть доступ по протоколу SSH
firewall --enabled --service=ssh
# отключить службу kdump и включить службы chronyd, rsyslog и sshd
services --disabled="kdump" --enabled="chronyd,rsyslog,sshd"
# включить SELinux
selinux --enforcing

# настроить вывод на последовательный порт чтобы можно было подключаться к
# консоли виртуальной машины без графической сессии
bootloader --timeout=1 --append="console=tty0 console=ttyS0,115200n8 no_timer_check␣
↪crashkernel=auto net.ifnames=0"
# использовать только диск /dev/vda во время установки
ignoredisk --only-use=vda
# создать новую таблицу разделов на диске /dev/vda
clearpart --initlabel --drives=vda
# использовать автоматическую разбивку диска без отдельного раздела /home
autopart --nohome

# заблокировать вход пользователем root
rootpw --lock
# создать пользователя msvsphere с паролем msvsphere, сделать его
# администратором путём добавления в группу wheel
user --groups="wheel" --name msvsphere --password="msvsphere"

# автоматически перезагрузить систему после завершения установки и извлечь
# установочный носитель
```

(продолжение на следующей странице)

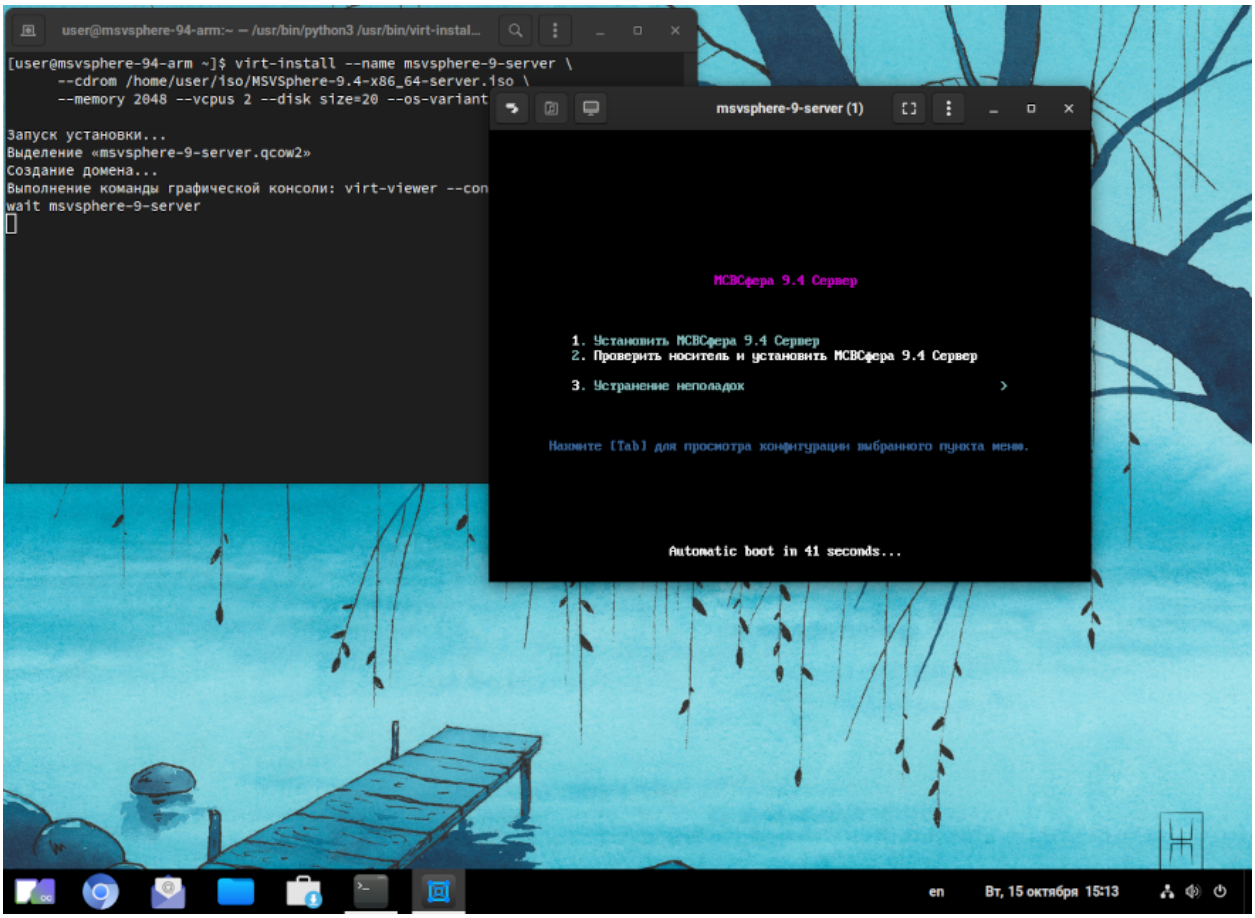
(продолжение с предыдущей страницы)

```
reboot --eject

# блок %packages определяет какие пакеты, группы и модули необходимо установить.
# опция --inst-langs определяет список языков, для которых необходимо добавлять
# поддержку
%packages --inst-langs=en,ru
# установить пакеты из группы core
@core
# установить пакеты из группы guest-agents
@guest-agents
# установить пакеты самоидентификации серверного варианта МСВСфера ОС
sphere-release-identity-server
sphere-release-server
sphere-release
%end

# отключить расширение kdump
%addon com_redhat_kdump --disable
%end
```

На системах с графическим интерфейсом после запуска команды `virt-install` автоматически запустится программа `virt-viewer`, с помощью которой вы сможете взаимодействовать с виртуальной машиной и выполнить установку операционной системы:



На системах без графического интерфейса вы можете использовать последовательную

консоль, если устанавливаемая операционная система поддерживает такой режим. Для большинства ОС на базе GNU/Linux будет достаточно передать следующие аргументы команде `virt-install`:

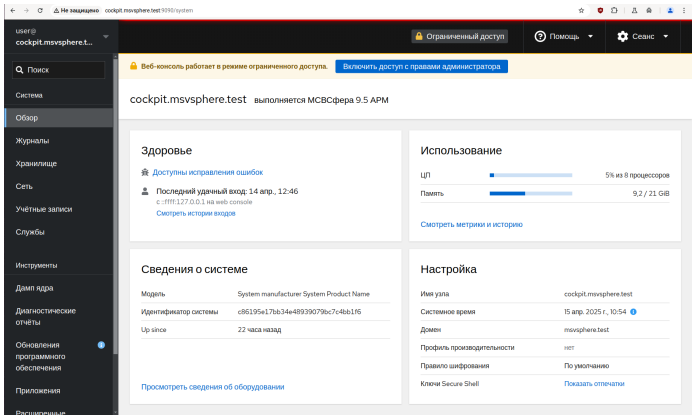
```
$ virt-install ... -console pty,target_type=virtio --graphics none \
      --serial pty --extra-args 'console=ttyS0,115200n8'
```

Панель управления Cockpit

Описание панели управления Cockpit

Введение

Cockpit — это панель управления для администрирования серверов и рабочих станций под управлением МСВСфера ОС. Благодаря использованию веб-интерфейса Cockpit позволяет администрировать как локальную, так и удалённые системы — для работы с панелью требуется только веб-браузер.



Основные функции

Ниже перечислены основные возможности панели управления Cockpit.

- Мониторинг и диагностика:
  - просмотр сведений о системе и конфигурации оборудования;
  - мониторинг использования ресурсов: центрального процессора, оперативной памяти, дискового пространства и сетевых интерфейсов;
  - просмотр и поиск по системным журналам;
  - диагностика ошибок подсистемы SELinux.
- Администрирование:
  - настройка системного времени;
  - ввод компьютера в домен Active Directory или FreeIPA;
  - управление учётными записями пользователей и группами, а также политиками паролей;
  - управление системными службами: (пере)запуск и остановка, настройка автоматического запуска, просмотр журналов;
  - управление обновлениями программного обеспечения;
  - управление сетевыми интерфейсами и настройками брандмауэра;

- управление локальными (LVM, RAID) и сетевыми (NFS, iSCSI) хранилищами;
- управление виртуальными машинами (Libvirt) и контейнерами (Podman);
- настройка аварийного дампа ядра (kdump).

Также следует отметить, что Cockpit является модульной системой, что делает возможной разработку собственных расширений — этот процесс подробно описан в официальной документации проекта.

Установка и настройка Cockpit

Установка

Для установки панели управления Cockpit выполните следующую команду:

```
$ sudo dnf install cockpit
```

Затем, запустите службу `cockpit.socket`:

```
$ sudo systemctl enable --now cockpit.socket
```

После запуска интерфейс системы управления будет доступен по локальному адресу https://localhost:9090/. В случае обращения к удалённому компьютеру укажите вместо `localhost` его IP-адрес или доменное имя.

В зависимости от настроек вашего брандмауэра, также может потребоваться открыть доступ к порту, на котором запущена панель управления Cockpit:

```
$ sudo firewall-cmd --add-service=cockpit --permanent
success

$ sudo firewall-cmd --reload
success
```

Создание диагностических отчётов

Введение

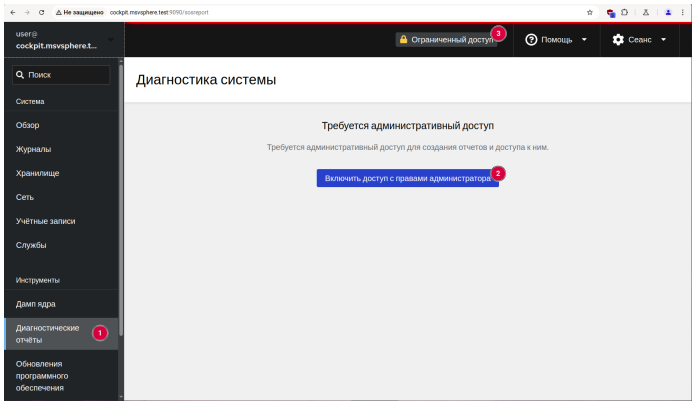
В состав панели управления Cockpit входит модуль для формирования диагностических отчётов, которые затем могут быть переданы для исследования в службу технической поддержки.

Для активации этого модуля предварительно необходимо установить пакет `sos`:

```
$ sudo dnf install sos
```

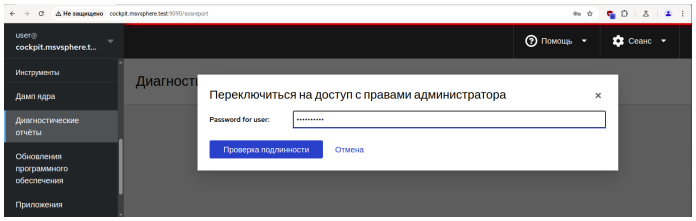
Создание отчёта

Для создания диагностического отчёта войдите в систему управления Cockpit и в левом навигационном меню выберите пункт «**Диагностические отчёты**» (отмечен цифрой 1 на снимке экрана).

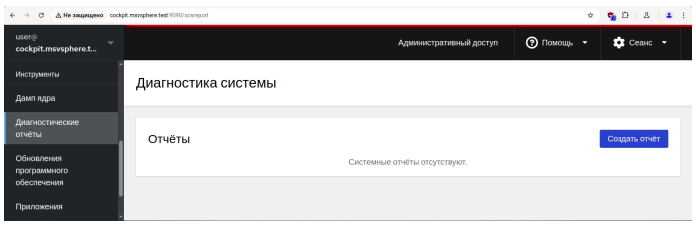


Если вы вошли в панель управления, используя учётную запись непривилегированного пользователя, то получите привилегии администратора либо нажав кнопку «**Включить доступ с правами администратора**» (отмечена цифрой 2 на снимке экрана выше), либо кнопку «**Ограниченный доступ**» (отмечена цифрой 3 на снимке экрана выше).

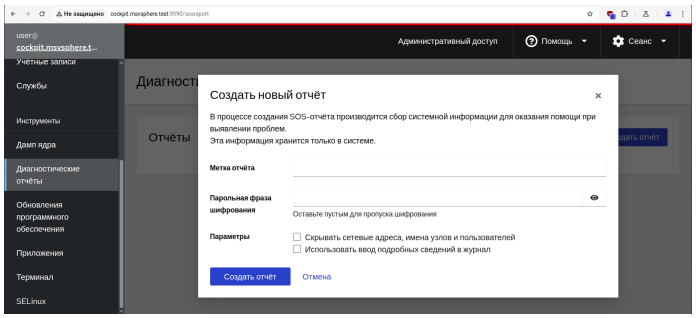
В открывшейся форме необходимо ввести свой пароль и нажать кнопку «**Проверка подлинности**».



После этого на экране появится список ранее созданных отчётов (в данном примере он пустой) и кнопка «**Создать отчёт**».



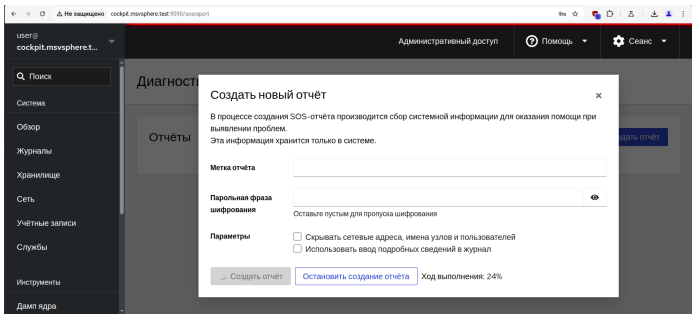
После нажатия на кнопку появится соответствующая форма, в которой вы можете настроить параметры создания отчёта.



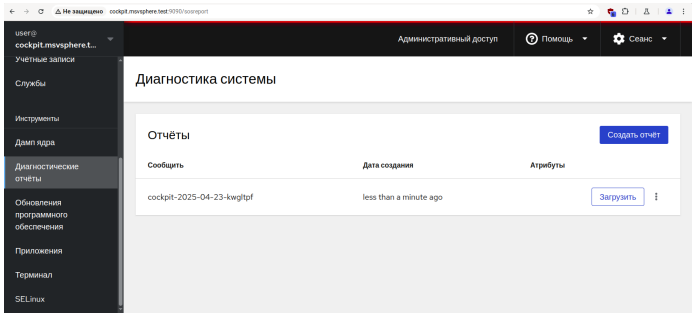
На данный момент для конфигурации доступны следующие опции:

- В поле «**Метка отчёта**» вы можете ввести идентификатор запроса в службе технической поддержки. Если вы не знаете его, оставьте поле пустым.
- В поле «**Парольная фраза шифрования**» вы можете указать пароль, который затем потребуется ввести для открытия файла отчёта. Защита файла отчёта паролем не является обязательным требованием, однако, рекомендуется в случае передачи файла по незащищённым каналам.
- Флажок «**Скрывать сетевые адреса, имена узлов и пользователей**» включает режим обезличивания этих данных в отчёте. Следует отметить, что пароли, ключи и другие приватные данные в любом случае не будут включены в отчёт.
- Флажок «**Использовать ввод подробных сведений в журнал**» включает дополнительную отладочную информацию в отчёт. Используйте его по запросу инженера технической поддержки.

После нажатия на кнопку «**Создать отчёт**» запустится процедура генерации, которая может занять несколько минут в зависимости от размера файлов журналов.



После завершения процедуры форма создания отчёта будет автоматически закрыта, а в списке отчётов появится новая запись, в данном примере — `cockpit-2025-04-23-kwgltpf`.



Для генерации идентификатора отчёта используется шаблон `HOSTNAME-YYYY-MM-DD-ID`, где:

- `HOSTNAME` — имя компьютера;
- `YYYY` — текущий год;
- `MM` — текущий месяц;
- `DD` — текущий день;
- `ID` — уникальный идентификатор.

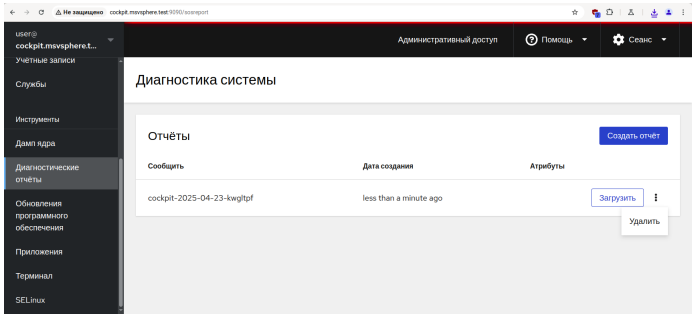
Таким образом, отчёт с именем `cockpit-2025-04-23-kwgltpf` был создан на компьютере *cockpit* 23 апреля 2025 года. Если в форме настройки параметров отчёта была задана «**Метка отчёта**», то эта информация также попадёт в идентификатор созданного отчёта.

Созданный отчёт можно скачать нажав на кнопку «**Загрузить**», после этого его необходимо прикрепить к заявке, созданной на портале технической поддержки, либо передать в службу поддержки иным согласованным способом.

Скачанный файл будет иметь префикс `sosreport-`, если файл не защищён паролем и префикс `secured-sosreport-`, если пароль был установлен. Соответственно, в нашем примере для отчёта `cockpit-2025-04-23-kwgltpf` будет скачан файл `sosreport-cockpit-2025-04-23-kwgltpf.tar.xz`.

Удаление отчёта

Удалить файл отчёта из системы можно нажав на кнопку меню «⊠» справа от кнопки «**Загрузить**» и выбрав там пункт меню «**Удалить**».



Просмотр данных отчёта

Файл отчёта представляет собой tar-архив, сжатый архиватором `xz`, который содержит следующую информацию:

- настройки загрузчика и конфигурационный файл ядра системы;
- конфигурационные файлы различных компонентов из каталога `/etc`;
- список загруженных модулей ядра, запущенных процессов, открытых файловых дескрипторов и т.д.;
- конфигурацию сетевых адаптеров и информацию об оборудовании;
- системные журналы различных компонентов системы.

Для распаковки файлов отчёта в текущий каталог выполните следующую команду (замените имя файла на реальное):

```
$ tar -xJvf sosreport-cockpit-2025-04-23-kwgltpf.tar.xz
```

Если при создании отчёта был установлен пароль, то перед распаковкой необходимо расшифровать файл используя следующую команду (замените имена файлов на реальные):

```
$ gpg -d -o secured-sosreport-cockpit-2025-04-24-azytuxv.tar.xz \
    secured-sosreport-cockpit-2025-04-24-azytuxv.tar.xz.gpg
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
```

После ввода пароля в текущем каталоге будет создан архив `.tar.xz` с указанным именем, который затем можно будет распаковать приведённой выше командой.

Настройка мультитерминального режима

Введение

Мультитерминальный режим — это особая конфигурация компьютера и операционной системы, которая позволяет обеспечить одновременную работу нескольких пользователей за одним компьютером.

В состав операционной системы МСВСфера входит расширение для панели управления Cockpit, которое предоставляет графический интерфейс для настройки работы в мультитерминальном режиме.

Аппаратные требования

Для работы в мультитерминальном режиме необходима следующая конфигурация компьютера:

- отдельная видеокарта для каждого рабочего места. Оптимальный вариант — установить дополнительную видеокарту в компьютер со встроенной видеокартой;
- отдельная клавиатура для каждого рабочего места. Рекомендуется использовать разные модели клавиатур чтобы их было проще отличать друг от друга в интерфейсе управления;
- отдельная мышка (трекбол, тачпад и т.п.) для каждого рабочего места. Как и в случае с клавиатурами, не рекомендуется использование устройств одинаковой модели;
- если требуется обеспечить вывод звука для каждого рабочего места, то вам также потребуется отдельная звуковая карта. В качестве альтернативы можно выводить звук на монитор через HDMI.

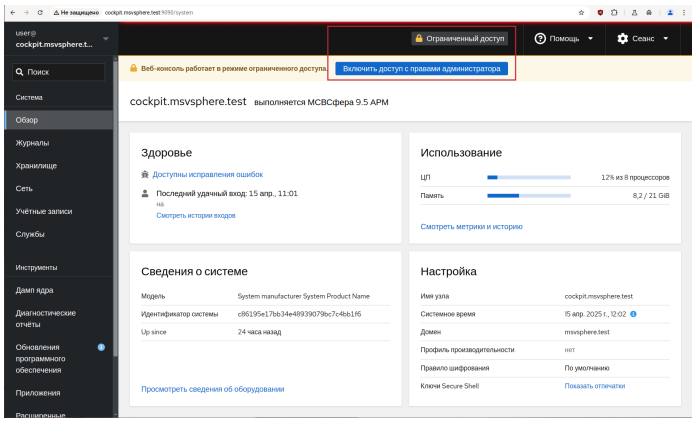
Установка расширения для Cockpit

Для настройки мультитерминальной системы установите соответствующее расширение для панели управления Cockpit:

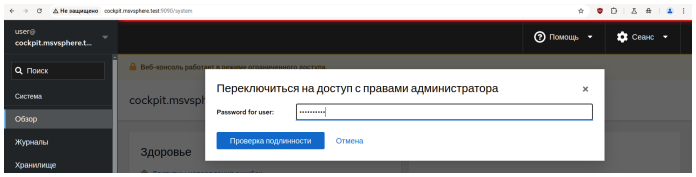
```
$ sudo dnf install cockpit-msvsphere-multi-seat
```

Настройка дополнительного рабочего места

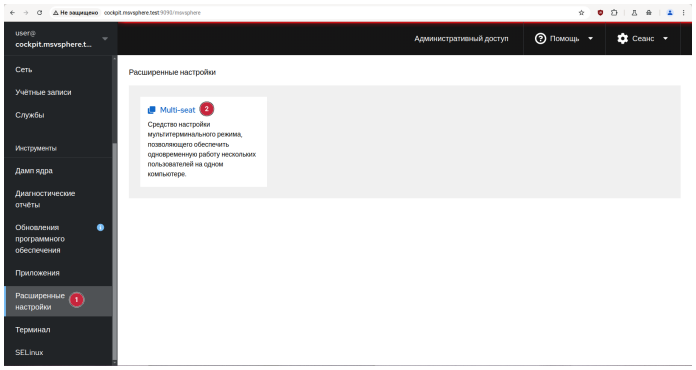
Для настройки мультитерминального режима требуются привилегии администратора: войдите в панель управления Cockpit, на странице «Обзор» нажмите кнопку «Включить доступ с правами администратора» или кнопку «Ограниченный доступ», которая также доступна на других страницах системы управления. На приведённом ниже снимке экрана эти кнопки обозначены красным прямоугольником.



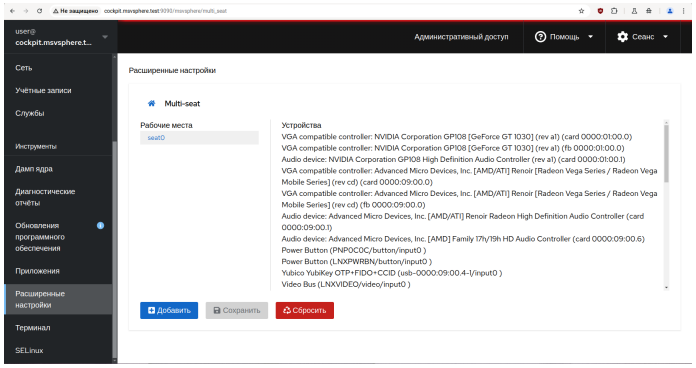
В открывшейся форме необходимо ввести свой пароль и нажать кнопку «Проверка подлинности».



После этого в левой панели откройте страницу «Расширенные настройки» (обозначена цифрой 1 на снимке экрана), там перейдите по ссылке «Multi-seat» (обозначена цифрой 2 на снимке экрана).

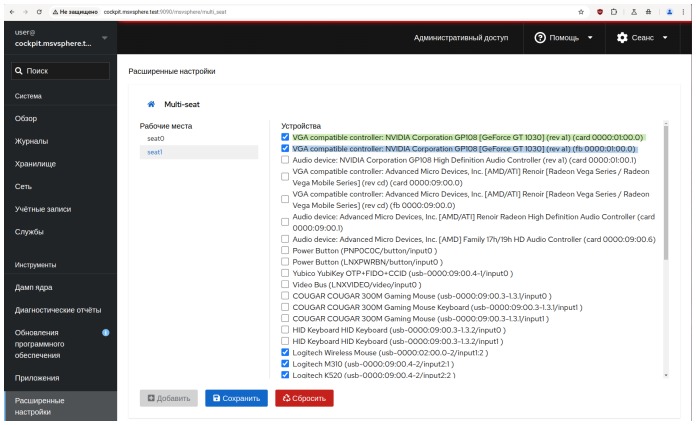


По умолчанию в системе настроено только одно рабочее место (`seat0`), за которым закреплены все доступные устройства. Для добавления ещё одного рабочего места нажмите кнопку «Добавить».

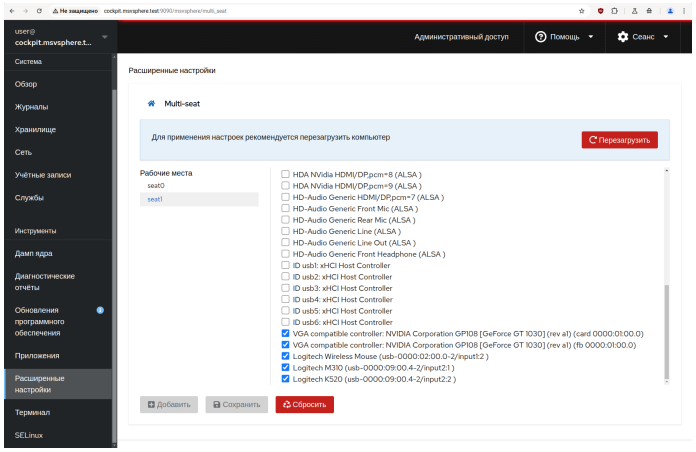


В результате будет создано дополнительное рабочее место (`seat1`) и вам потребуется назначить ему соответствующие устройства ввода-вывода, используя флажки в списке устройств. Минимально работоспособная конфигурация должна включать в себя видеокарту, клавиатуру и мышку (трекбол, тачпад и т.п.).

Также обратите внимание, что для видеокарты в списке отображаются два устройства: тип `card` (выделено зелёным маркером на снимке экрана) и тип `fb` (выделено синим маркером на снимке экрана) — вам необходимо закрепить оба устройства одной видеокарты за рабочим местом.



После завершения конфигурации устройств нажмите кнопку «Сохранить» — система выдаст всплывающее сообщение об успешном добавлении рабочего места и предложит перезагрузить компьютер для активации изменений.

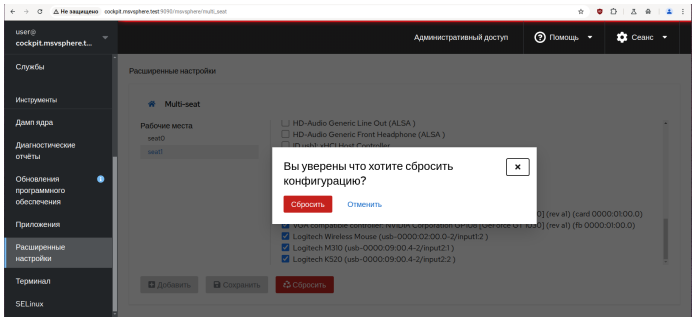


После перезагрузки на каждом из рабочих мест будет запущена собственная графическая сессия и пользователи смогут войти в систему используя свои учётные записи.

Возврат к настройкам по умолчанию

Для возврата системы к базовой конфигурации с одним рабочим местом войдите в панель управления Cockpit, получите привилегии администратора, перейдите на страницу «Расширенные настройки» и выберите там расширение «Multi-seat» как было описано в предыдущем разделе.

На странице расширения нажмите на кнопку «Сбросить», появится соответствующее окно для подтверждения операции.



После подтверждения система выдаст всплывающее сообщение об успешном сбросе конфигурации и предложит перезагрузить компьютер. После перезагрузки система вернётся в исходное состояние с одним рабочим местом.

Расширение USBGuard для Cockpit

Введение

Расширение USBGuard для Cockpit работает на основе программной платформы USBGuard и помогает защитить компьютер от мошеннических USB-устройств, внедряя базовые возможности белого и чёрного списков на основе атрибутов USB-устройств.

Установка расширения для Cockpit

Установите расширение для панели управления `Cockpit` с помощью следующей команды:

```
$ sudo dnf install cockpit-msvsphere-usbguard
```

Запустите сервис `usbguard` с помощью следующей команды:

```
$ sudo systemctl enable --now usbguard.service
```

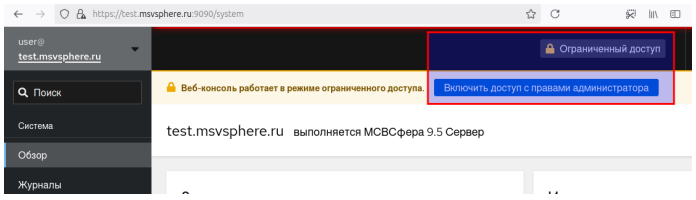
По умолчанию USBGuard блокирует USB-устройства, не соответствующие правилам. После запуска сервиса `usbguard` в «белый» список добавятся все текущие подключённые устройства. Все новые подключённые USB-устройства будут блокироваться.

Настройка

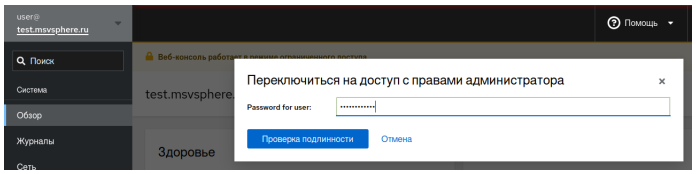
Настройка пользователей

По умолчанию для работы с расширением USBGuard требуются права пользователя `root` или же пользователь должен состоять в группе `wheel`. Изменить настройки и добавить нового пользователя/группу может пользователь с правами администратора. Для этого выполните следующие действия.

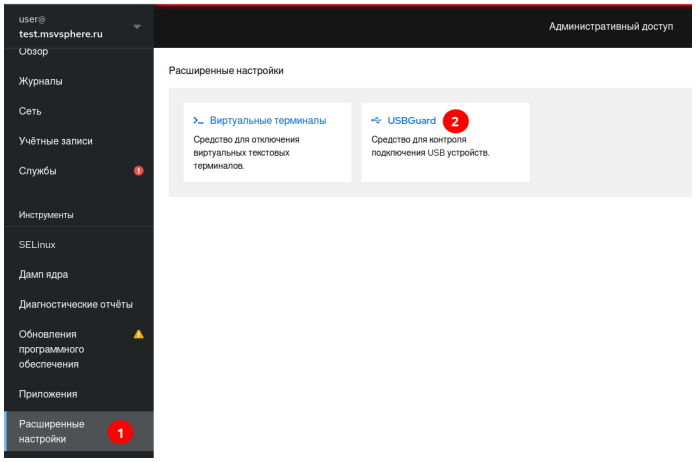
- Войдите в панель управления `Cockpit`. На странице «Обзор» нажмите кнопку «Включить доступ с правами администратора» или кнопку «Ограниченный доступ», которая также доступна на других страницах системы управления. На приведённом ниже снимке экрана эти кнопки выделены красным.



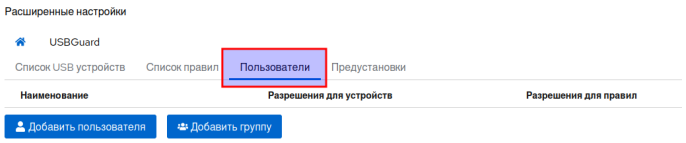
- В открывшейся форме укажите свой пароль и нажмите кнопку «Проверка подлинности».



- После этого в левой панели откройте страницу «Расширенные настройки» (обозначена цифрой 1 на снимке экрана), там перейдите по ссылке «USBGuard» (обозначена цифрой 2 на снимке экрана).

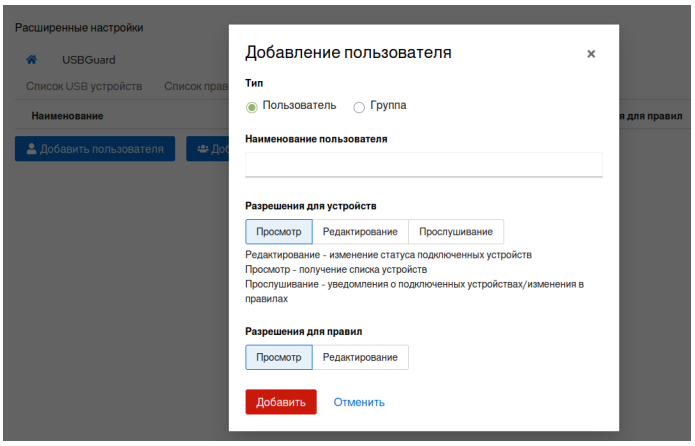


- Перейдите на вкладку «Пользователи».



Добавление пользователя/группы

Для добавления пользователя или группы нажмите кнопку «Добавить пользователя» или «Добавить группу». В открывшемся окне вы можете указать создаваемый тип: «Пользователь» или «Группа», наименование и необходимые разрешения для устройств и правил.



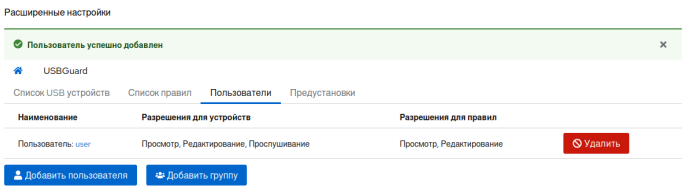
Разрешения для устройств включают следующие значения.

- Просмотр (list) — получать список подключённых USB-устройств и их атрибуты.
- Редактирование (modify) — изменять состояние авторизации USB-устройств (блокировка/разблокировка), включая постоянные изменения (т.е. изменение конкретных правил или устройств в политике).
- Прослушивание (listen) — получать уведомления о подключении устройств и изменении политики устройств.

Разрешения для правил включают следующие значения.

- Просмотр (list) — получать список правил.
- Редактирование (modify) — изменять и удалять правила.

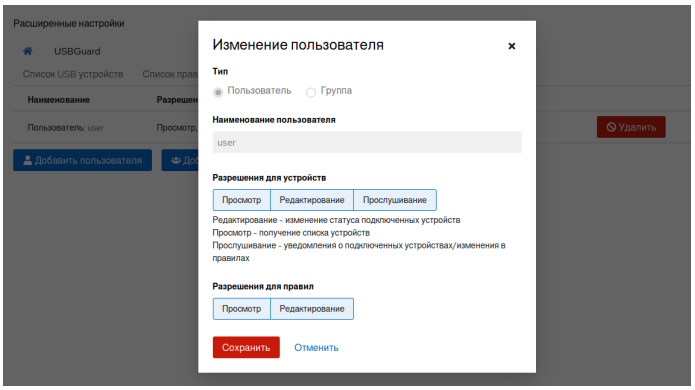
После добавления пользователя сервис `usbguard` будет перезапущен.



В дальнейшем, в зависимости от разрешений, пользователь может получить доступ к интерфейсу USBGuard без повышения привилегий.

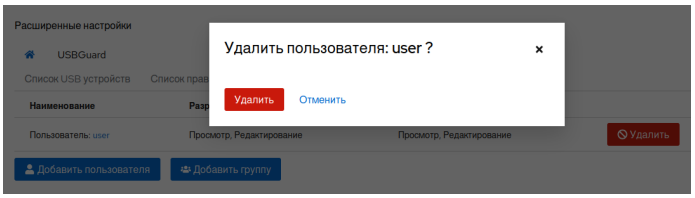
Изменение пользователя/группы

Для изменения пользователя/группы нажмите на него в таблице. В открывшемся окне вы можете изменить требуемые разрешения. После сохранения изменений сервис `usbguard` будет перезапущен.



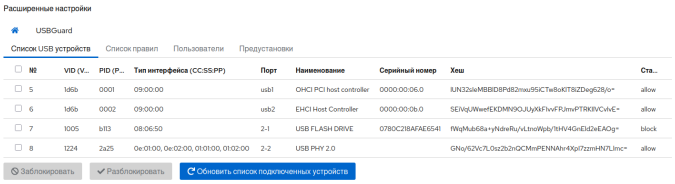
Удаление пользователя/группы

Для удаления пользователя/группы нажмите на кнопку «Удалить» в таблице пользователей и подтвердите действие. После удаления сервис `usbguard` будет перезапущен.



Список USB-устройств

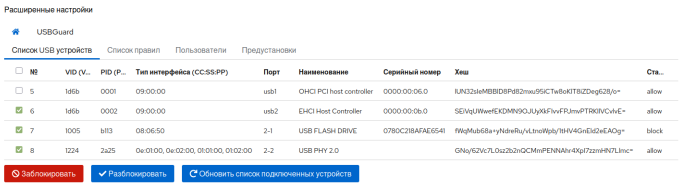
На вкладке отображается список текущих подключённых USB устройств.



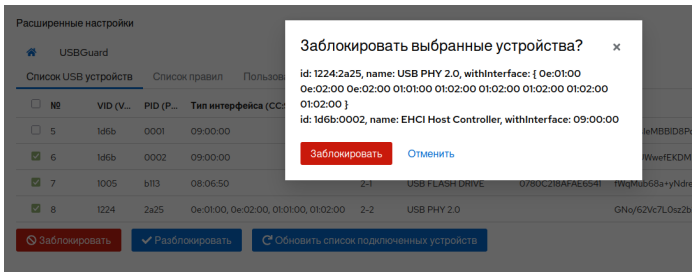
В столбце «Статус» отображается текущее состояние USB-устройства:

- allow — разрешено;
- block — заблокировано.

Для редактирования состояния USB-устройства выделите строку с устройством. В зависимости от текущего статуса устройства станут доступны кнопки «Разблокировать/»Заблокировать».



Нажмите на кнопку выбранного действия и подтвердите его в открывшемся окне.

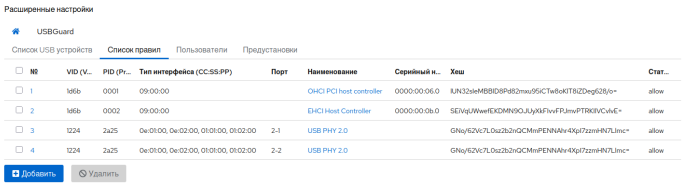


После подтверждения будет добавлено соответствующее правило для выбранных устройств.

Также в данном разделе доступна кнопка «Обновить список подключённых устройств» для обновления списка после подключения или удаления USB-устройств.

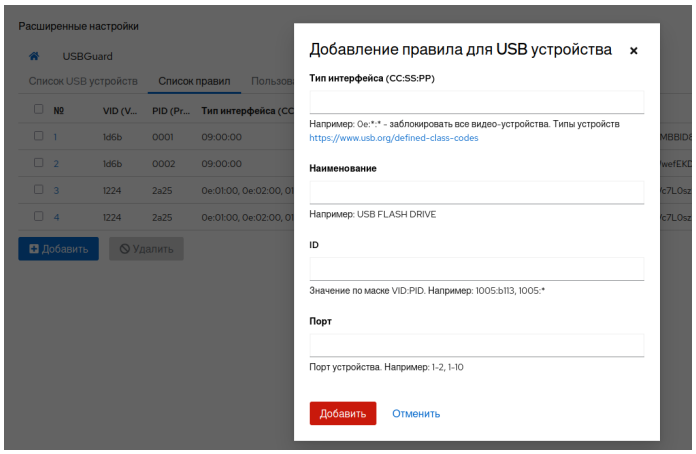
Список правил

На вкладке «Список правил» отображается список текущих правил для USB-устройств, основанный на их атрибутах.



Добавление правила

Для добавления правила нажмите на кнопку «Добавить». Откроется окно с формой добавления.



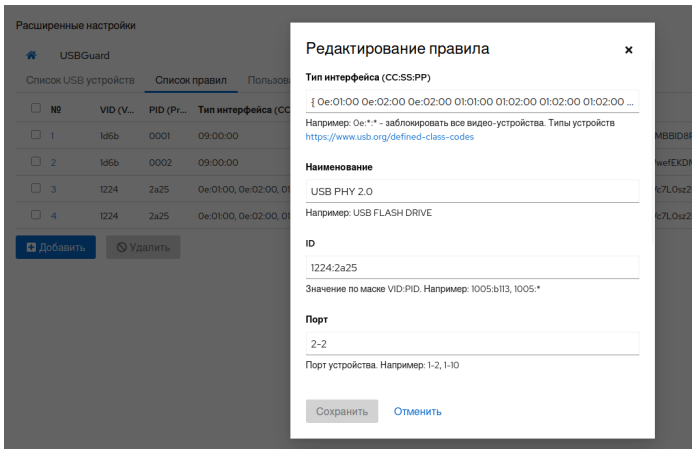
Доступны следующие атрибуты.

- Тип интерфейса (CC:SS:PP) — тип интерфейса указывается как три 8-битных числа в шестнадцатеричном формате, разделённых двоеточием (`CC:SS:PP`). Числа обозначают класс интерфейса (CC), подкласс (SS) и протокол (PP). Пример списка классов. Вместо номера подкласса и протокола можно использовать символ *, чтобы выбрать все подклассы или протоколы. Также есть возможность указать несколько типов, при этом значения должны быть разделены пробелом и обрамлены фигурными скобками. Например: `{ 03:01:01 03:00:00 }`.
- Наименование — название устройства.
- ID — значение по маске `VID:PID` (`<ID вендора>:<ID продукта>`). Формат — 16-битные числа в шестнадцатеричном формате. В значении может быть указан символ *, чтобы выбрать все значения.
- Порт — USB-порт устройства.
- Серийный номер устройства.
- Хеш устройства.
- Статус — может принимать одно из значений: `block` — заблокировать устройство, `allow` — разрешить, `reject` — удалить устройство из системы.

Правило вступает в силу после подключения USB-устройства. Таким образом, если устройство было подключено на момент создания правила, то правило начнёт действовать после его переподключения.

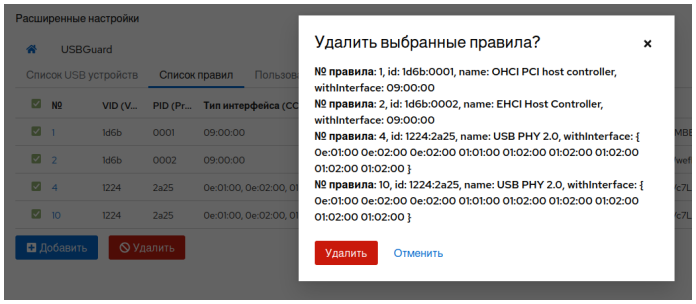
Изменение правила

Для изменения правила нажмите на его номер в столбце «№» или на его имя в столбце «Наименование». Откроется окно редактирования правила.



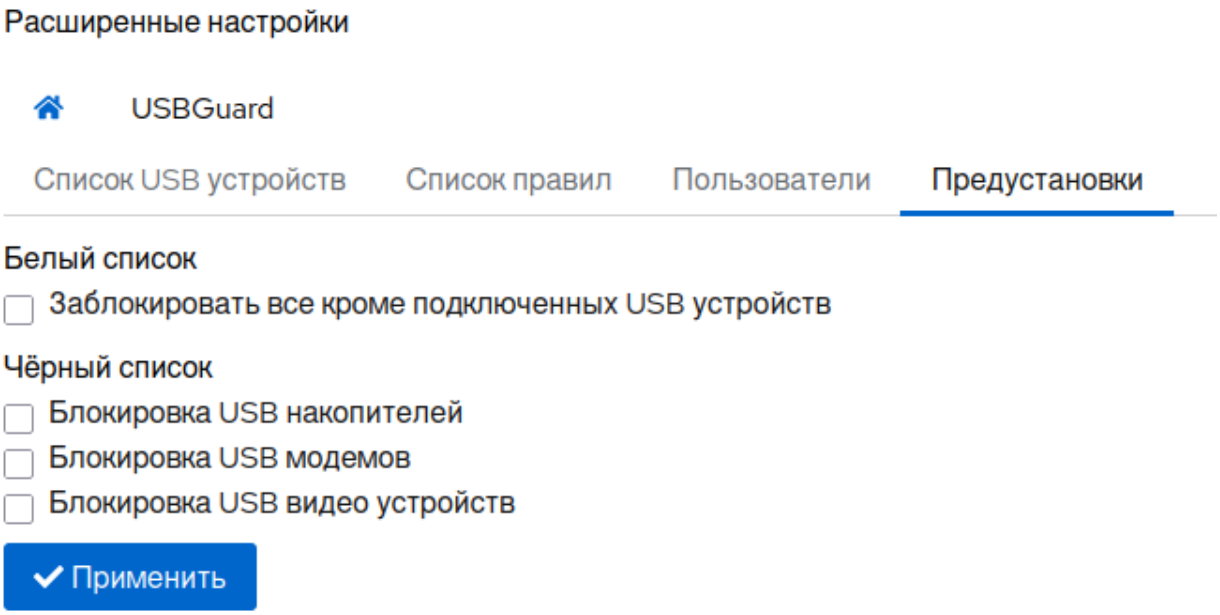
Удаление правил

Для удаления правила выберите его в списке и нажмите на кнопку «Удалить». В открывшемся окне подтвердите свои действия.



Предустановки

В разделе «Предустановки» вы можете отключить правила, а также добавить общие правила для некоторых классов USB-устройств.



Белый список

- `Заблокировать все кроме подключённых USB-устройств` — все текущие правиле будут удалены, затем на основе списка подключённых устройств будут сгенерированы и добавлены новые правила. Также в конфигурационном файле USBGuard `%sysconfdir%/usbguard/rules.conf` значение `ImplicitPolicyTarget` (статус для новых устройств, не подходящих под текущие правила) будет изменено на `block` (по умолчанию).

Чёрный список

- `Блокировка USB накопителей` — добавление правила с типом интерфейса `08:*:*`.
- `Блокировка USB модемов` — добавление правила с типом интерфейса `02:*:*`
- `Блокировка USB видео устройств` — добавление правила с типом интерфейса `0e:*:*`

Расширение Bootloader для Cockpit

Введение

Расширение Bootloader для Cockpit предоставляет интерфейс настройки параметров загрузчика операционной системы.

Установка расширения для Cockpit

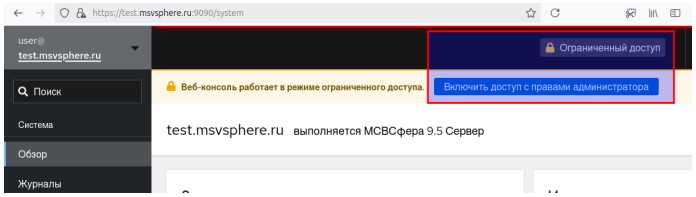
Установите соответствующее расширение для панели управления `Cockpit`:

```
$ sudo dnf install cockpit-msvsphere-bootloader
```

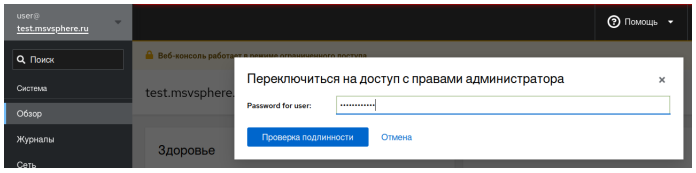
Настройка

Для изменения параметров загрузчика требуются привилегии администратора:

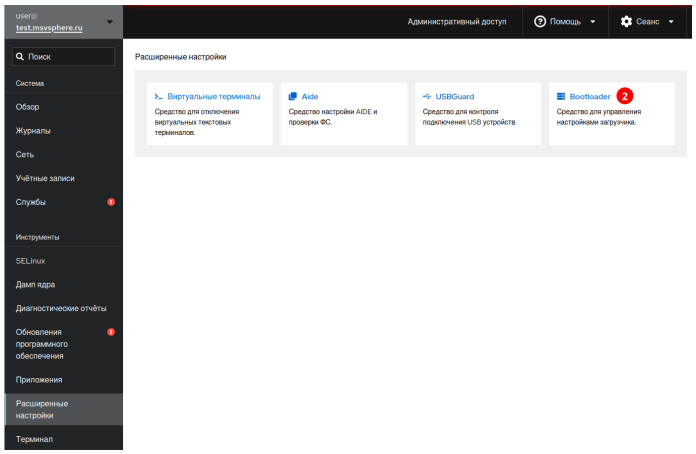
- войдите в панель управления `Cockpit`, на странице «Обзор» нажмите кнопку «Включить доступ с правами администратора» или кнопку «Ограниченный доступ», которая также доступна на других страницах системы управления. На приведённом ниже снимке экрана эти кнопки обозначены красным прямоугольником:



- В открывшейся форме необходимо ввести свой пароль и нажать кнопку «Проверка подлинности»:



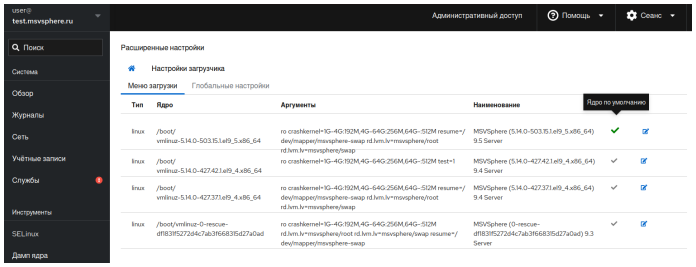
- После этого в левой панели откройте страницу «Расширенные настройки» (обозначена цифрой `1` на снимке экрана), там перейдите по ссылке «Bootloader» (обозначена цифрой `2` на снимке экрана):



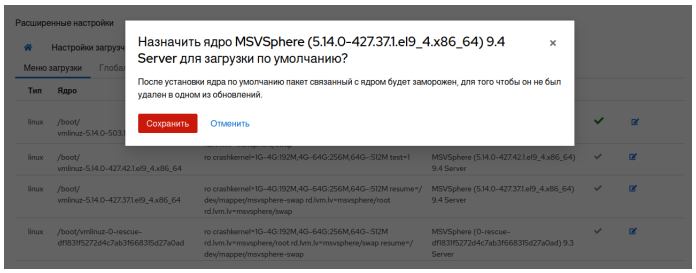
Вкладка «Меню загрузки»

На данной вкладке будут отображены записи из меню загрузки.

Ядро, загруженное по умолчанию, будет отмечено иконкой зелёного цвета.

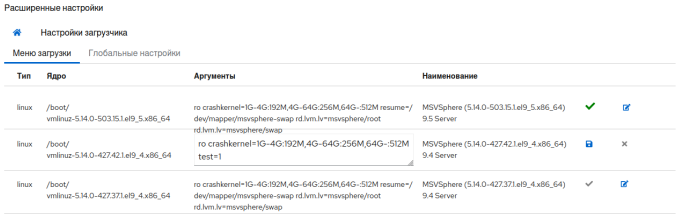


Для того чтобы изменить загружаемое ядро по умолчанию, нажмите иконку на соответствующей записи. После нажатия во всплывающем окне подтвердите свой выбор.



После установки нового ядра для загрузки по умолчанию пакет, связанный с ядром, будет «заморожен» (с помощью `dnf versionlock`), чтобы он не был удалён из системы при последующих обновлениях ядра.

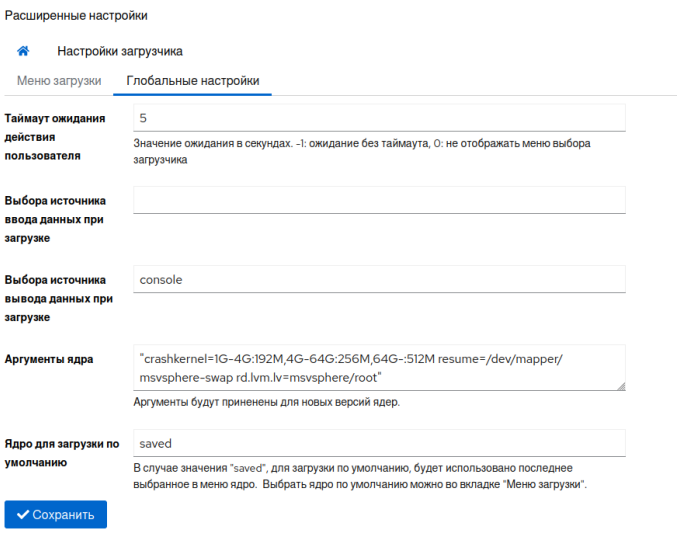
Также в этом разделе есть возможность изменения аргументов ядра.



После изменения значений в текстовом поле нажмите иконку «сохранить».

Вкладка «Глобальные настройки»

В данном разделе представлена форма, позволяющая изменять некоторые глобальные настройки загрузчика путём модификации файла `/etc/default/grub`



Текущие настройки:

- `Таймаут ожидания действия пользователя` — время ожидания действия в секундах. Значение `-1` — ожидание выбора без таймаута, `0` — не отображать меню выбора загрузчика.
- `Выбора источника ввода данных при загрузке` — терминальное устройство ввода. Здесь вы можете выбрать несколько устройств, разделенных пробелами. Допустимые названия терминалов ввода зависят от платформы, но могут включать «console» (консоль собственной платформы), «serial» (последовательный терминал), «serial_<порт>» (последовательный терминал с явным выбором порта), «at_keyboard» (клавиатура PC AT) или «usb_keyboard» (USB-клавиатура). По умолчанию используется собственный терминальный ввод платформы.
- `Выбора источника вывода данных при загрузке` — терминальное устройство вывода. Здесь вы можете выбрать несколько устройств, разделенных пробелами. Допустимые названия выходных данных терминала зависят от платформы, но могут включать «console» (консоль собственной платформы), «serial» (последовательный терминал), «serial_<порт>» (последовательный терминал с явным выбором порта), «gfxterm» (вывод в графическом режиме), «vga_text» (текст VGA вывод), «mda_text» (вывод текста MDA), «morse» (кодировка Морзе с использованием системного звукового сигнала) или «spkmodem» (простой протокол передачи данных с использованием системного динамика).
- `Аргументы ядра` — будут использоваться как аргументы по умолчанию при обновлении/установке новых ядер.
- `Ядро для загрузки по умолчанию` — в случае значения «saved» для загрузки по умолчанию будет использовано последнее выбранное в меню ядро. Выбрать ядро для загрузки по умолчанию также можно во вкладке «Меню загрузки».

Подключение к домену

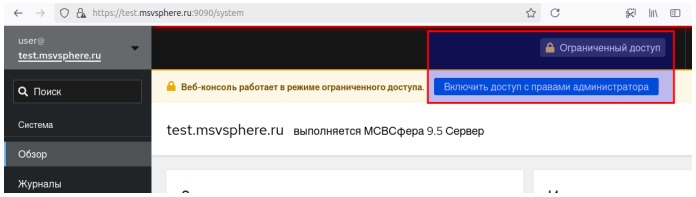
Введение

Cockpit предоставляет возможность подключения к домену.

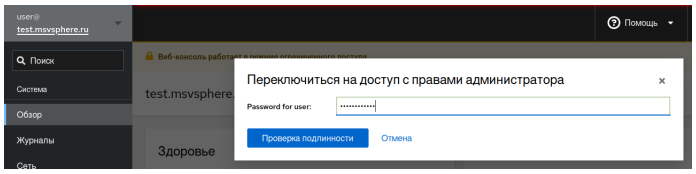
Настройка

Для подключения требуются привилегии администратора.

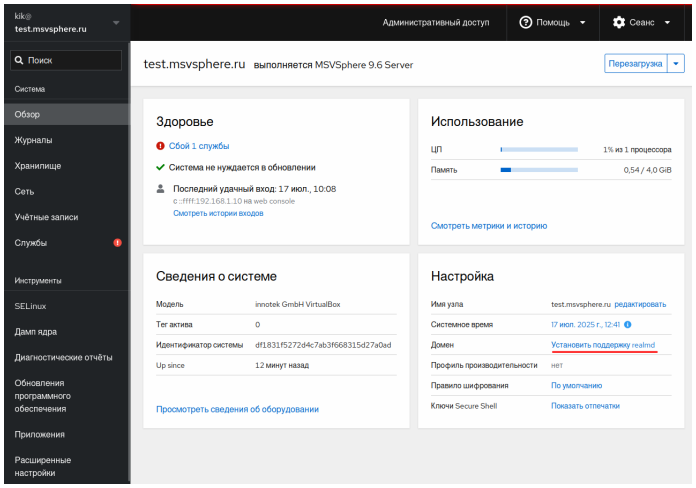
- Войдите в панель управления `Cockpit`, на странице «Обзор» нажмите на кнопку «Включить доступ с правами администратора» или на кнопку «Ограниченный доступ», которая также доступна на других страницах системы управления. На приведённом ниже снимке экрана эти кнопки обозначены красным прямоугольником:



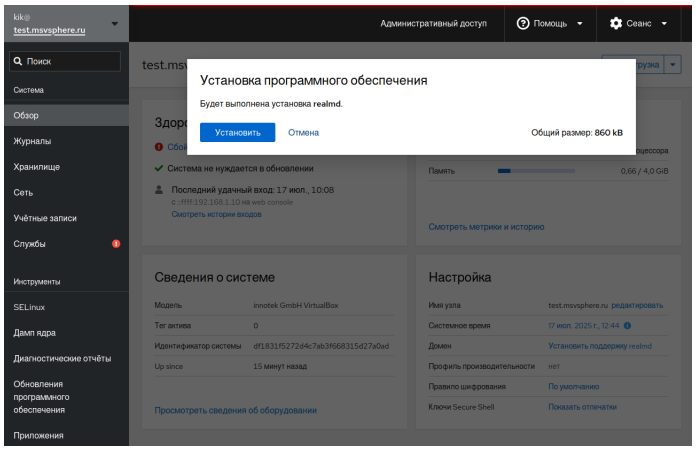
- В открывшейся форме укажите пароль и нажмите на кнопку «Проверка подлинности»:



- После этого в разделе «Настройка» (пункт «Домен») нажмите на ссылку «Установить поддержку realmd»:

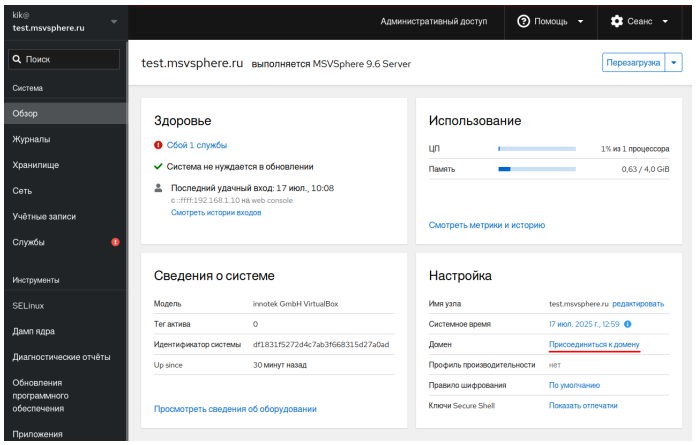


- Затем выполните установку, нажав на кнопку «Установить»:



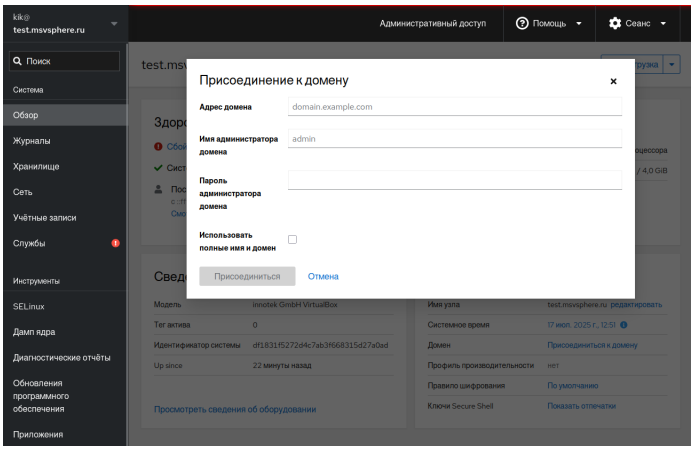
Подключение к домену

После установки пакета `realmd` вы увидите окно с формой для подключения к домену. Или же в разделе «Настройка» (пункт «Домен») нажмите на ссылку «Присоединится к домену».

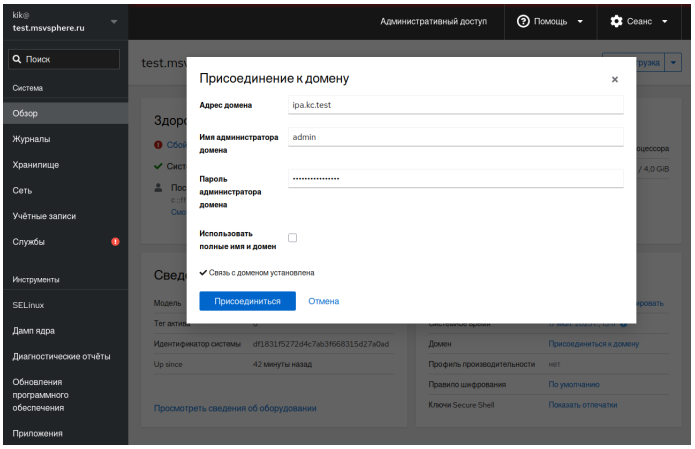


Заполните поля формы:

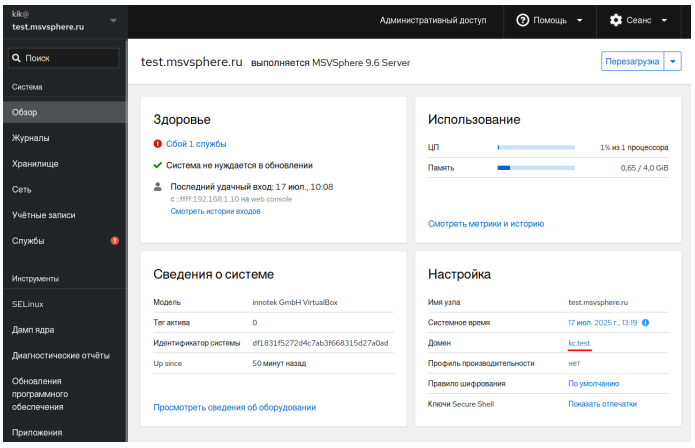
- `Адрес домена` — адрес сервера, управляющего доменом.
- `Имя администратора домена` — по умолчанию `admin`.
- `Пароль администратора домена`.
- `Использовать полные имя и домен` — настройка позволяет разрешить аутентификацию по коротким именам, например `user`, то есть, без указания доменного суффикса в формате `user@domain.ru`. По умолчанию используются короткие имена.



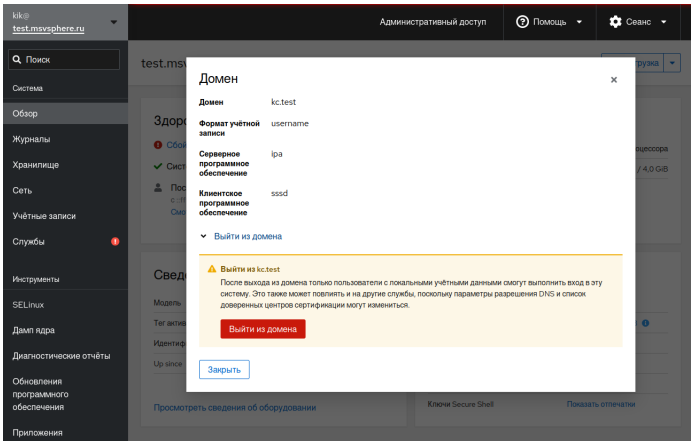
После заполнения поля **Адрес домена** выполняется проверка доступности сервера, в случае ошибки будет выведено сообщение. Если подключение прошло успешно, кнопка «Присоединиться» станет активной.



После нажатия на кнопку «Присоединиться» выполняется попытка подключения к серверу домена. В случае успешного подключения к домену в разделе «Настройка» (пункт «Домен») будет указан подключённый домен.



При нажатии на адрес домена откроется окно, в котором указаны детали подключения и предоставлена возможность отключиться от домена.



Расширение Aide для Cockpit

Введение

AIDE (Advanced Intrusion Detection Environment) — это инструмент для обнаружения вторжений на основе анализа изменений в файловой системе. Он работает по принципу системы обнаружения вторжений на основе хоста (HIDS) и помогает администраторам выявлять несанкционированные изменения в файлах и каталогах.

Установка расширения для Cockpit

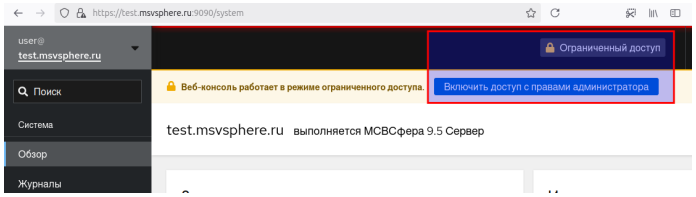
Установите соответствующее расширение для панели управления `Cockpit` с помощью следующей команды:

```
$ sudo dnf install cockpit-msvsphere-security-audit
```

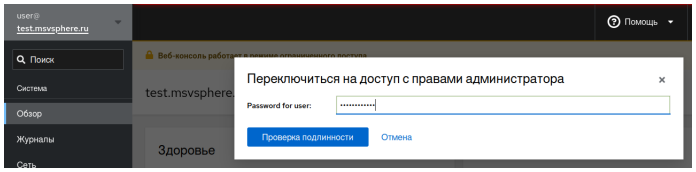
Настройка

Для использования расширения требуются привилегии администратора:

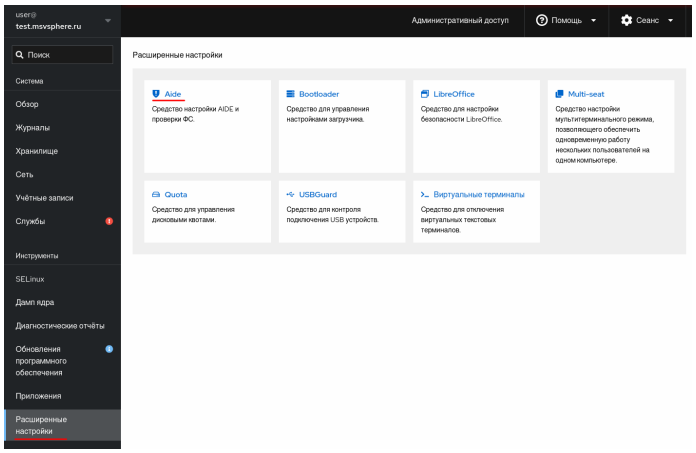
- войдите в панель управления `Cockpit`, на странице «Обзор» нажмите кнопку «Включить доступ с правами администратора» или кнопку «Ограниченный доступ», которая также доступна на других страницах системы управления. На приведённом ниже снимке экрана эти кнопки обозначены красным прямоугольником.



- В открывшейся форме укажите свой пароль и нажмите на кнопку «Проверка подлинности».

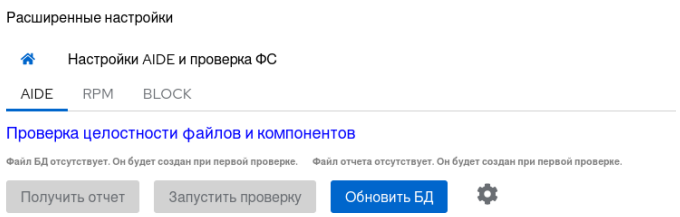


- После этого в левой панели откройте вкладку «Расширенные настройки», там перейдите по ссылке «Виртуальные терминалы».

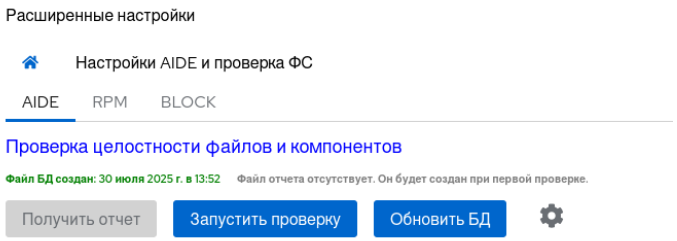


Вкладка «Aide»

После первоначальной установки необходимо инициализировать базу данных Aide. Инициализация заключается в создании базы данных (снимка) всех файлов и каталогов сервера. Для этого нажмите на кнопку «Обновить БД».

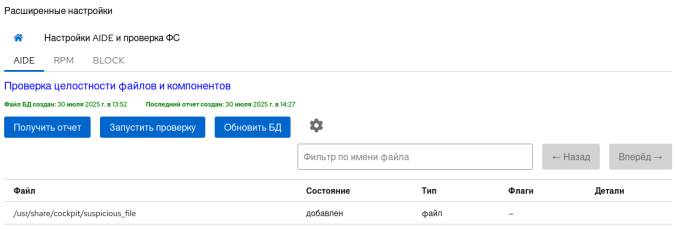


После инициализации базы данных появится возможность запустить проверку, для этого нажмите на соответсвующую кнопку.



В случае, если в системе произошли изменения по сравнению со «снимком» системы, будет выведен соответствующий результат в виде таблицы. В таблице будут указаны следующие данные:

- Файл — путь к файлу/каталогу.
- Состояние — добавлен/изменен/удалён.
- Тип — файл или каталог.
- Флаги — при наведении курсора на столбец будет показана детальная информация.
- Детали — дополнительная информация.



Список флагов:

- `p` — права доступа;
- `i` — номер inode;
- `n` — имя ссылки;
- `u` — владелец файла;
- `g` — группа файла;
- `s` — размер файла;
- `b` — количество блоков;

- `m` — время изменения (`mtime`);
- `a` — время доступа (`atime`);
- `c` — изменение inode (`ctime`).

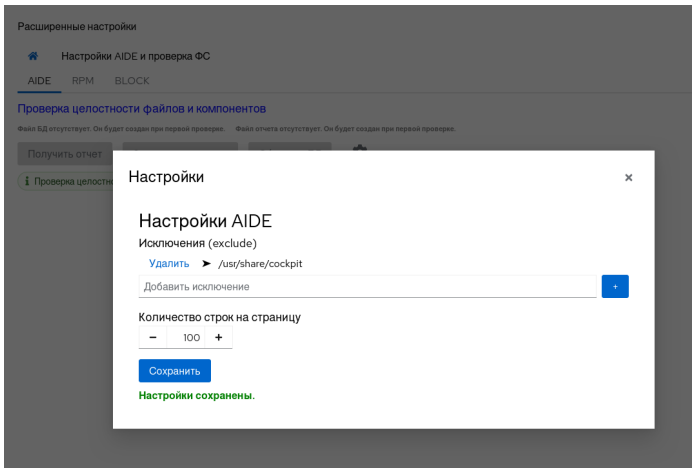
Настройки Aide

Вы можете настроить вывод требуемым образом. Для этого перейдите в «Настройки Aide», нажав на иконку «Шестеренка».

Здесь вы можете настроить следующие параметры вывода:

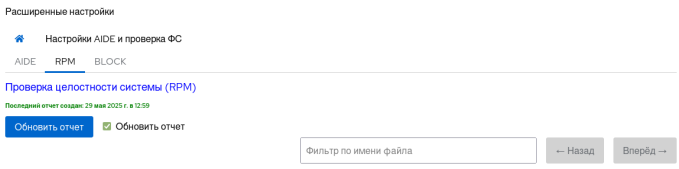
- Исключения — можно указать путь или наименование файла, который будет отфильтровываться в итоговой таблице.
- Количество строк, выводимых на странице.

Настройки применяются после сохранения.



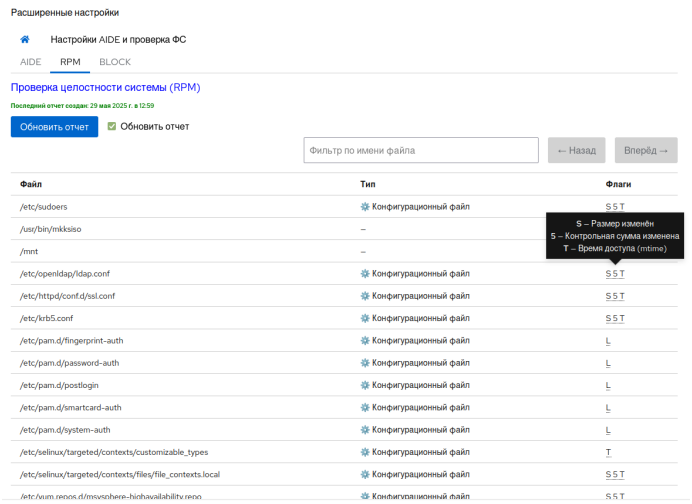
Вкладка «Rpm»

На данной вкладке вы можете запустить проверку целостности системы или просмотреть результат последней проверки. При нажатии на кнопку «Обновить отчёт» будет выполнена команда `rpm --all --verify`.



После окончания выполнения команды результат будет выведен в таблице. Будут указаны следующие данные:

- Файл — полный путь к файлу.
- Тип — тип файла (если известен).
- Флаги — при наведении на столбец будет показана детальная информация.



Список флагов:

- `S` — размер изменён;
- `M` — время модификации изменено;
- `5` — контрольная сумма изменена;
- `D` — номера major/minor изменены;
- `L` — символическая ссылка изменилась;
- `U` — пользователь изменён;
- `G` — группа изменена;
- `T` — время доступа (`mtime`) изменилось.

Расширение LibreOffice для Cockpit

Введение

Расширение `LibreOffice` для Cockpit позволяет отключить использование макросов.

Установка расширения для Cockpit

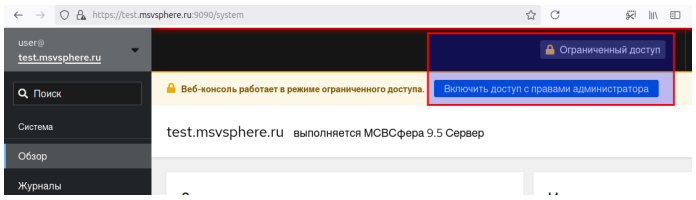
Установите соответствующее расширение для панели управления `Cockpit` с помощью следующей команды:

```
$ sudo dnf install cockpit-msvsphere-libreoffice
```

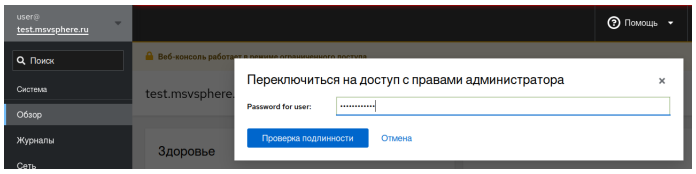
Настройка

Для отключения макросов требуются привилегии администратора:

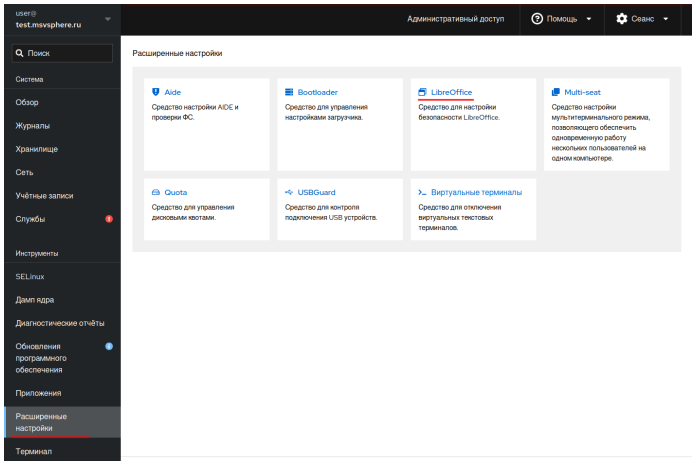
- войдите в панель управления `Cockpit`, на странице «Обзор» нажмите кнопку «Включить доступ с правами администратора» или кнопку «Ограниченный доступ», которая также доступна на других страницах системы управления. На приведённом ниже снимке экрана эти кнопки обозначены красным прямоугольником.



- В открывшейся форме укажите свой пароль и нажмите на кнопку «Проверка подлинности».

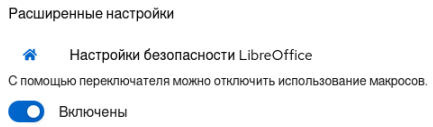


- После этого в левой панели откройте вкладку «Расширенные настройки», там перейдите по ссылке «LibreOffice»:

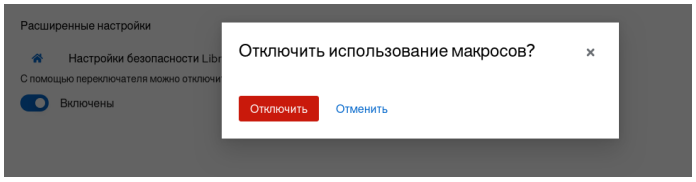


Отключение макросов

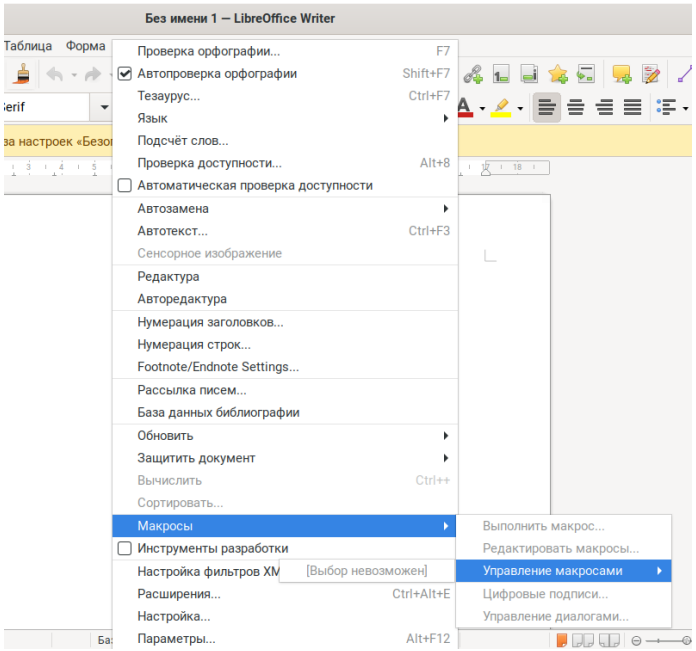
На странице отображается селектор, показывающий текущее состояние макросов (включены/отключены).

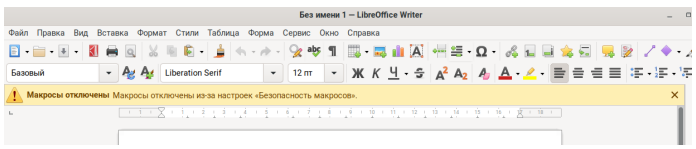


При отключении использования макросов будет показано окно подтверждения.



После подтверждения, использования макросов будет отключено.





Расширение Quota для Cockpit

Введение

Расширение `Quota` для Cockpit позволяет ограничить объем дискового пространства, используемого пользователями или группами, с помощью квот. Подсистема квот управляет ограничениями на использование дискового пространства (`block`) и файлов (`inode`).

Установка расширения для Cockpit

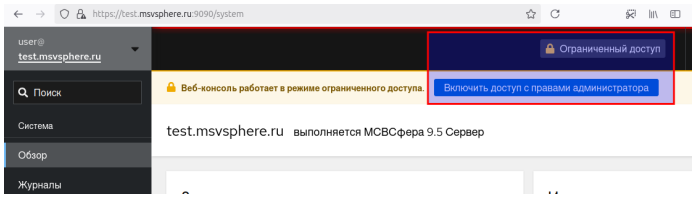
Установите соответствующее расширение для панели управления `Cockpit` с помощью следующей команды:

```
$ sudo dnf install cockpit-msvsphere-quota
```

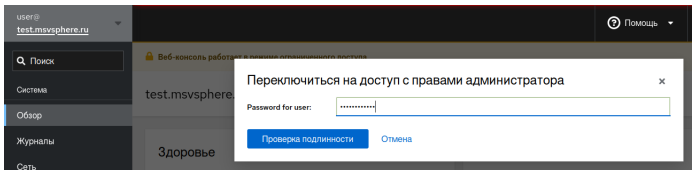
Настройка

Для управления квотами требуются привилегии администратора:

- войдите в панель управления `Cockpit`, на странице «Обзор» нажмите кнопку «Включить доступ с правами администратора» или кнопку «Ограниченный доступ», которая также доступна на других страницах системы управления. На приведённом ниже снимке экрана эти кнопки обозначены красным прямоугольником.



- В открывшейся форме укажите свой пароль и нажмите на кнопку «Проверка подлинности».



- После этого в левой панели откройте вкладку «Расширенные настройки» (обозначена цифрой `1` на снимке экрана), там перейдите по ссылке «Quota» (обозначена цифрой `2` на снимке экрана):

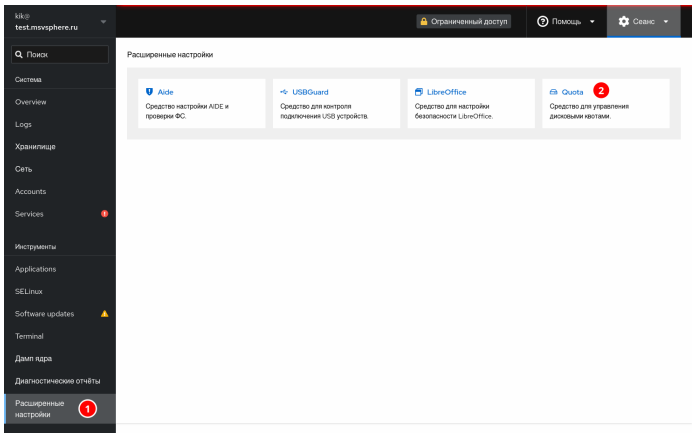
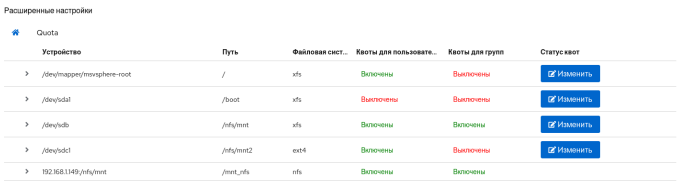


Таблица файловых систем

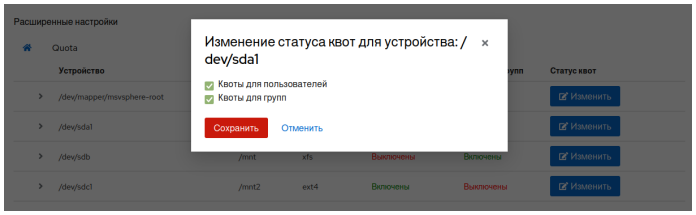
На странице отображаются поддерживаемые файловые системы.

- Устройство — дисковое устройство.
- Путь — путь к каталогу монтирования.
- Файловая система.
- Статус квот для пользователя — включены/выключены.
- Статус квот для групп — включены/выключены.



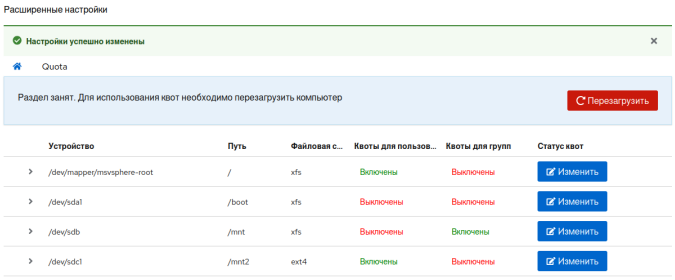
Изменение статуса квот

Для включения или выключения квот для пользователей/групп нажмите на кнопку «Изменить» для выбранной файловой системы. В открывшемся окне укажите нужный статус с помощью селекторов и сохраните изменения.



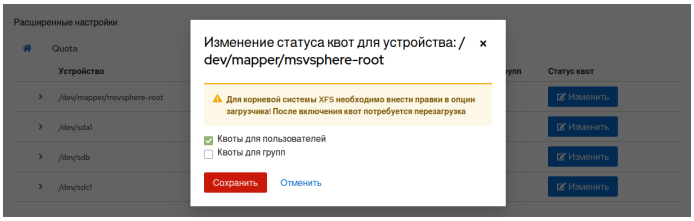
После сохранения, опции для включения квот будут добавлены в файл `/etc/fstab`.

Также будет выполнено перемонтирование раздела. Если раздел занят и используется, для применения изменений необходимо перезагрузить систему.



Важно!

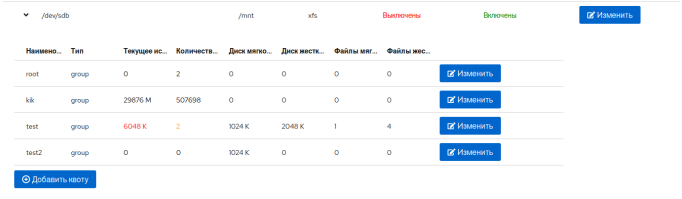
- Для включения квот корневой файловой системы `XFS` необходимо внести правки в опции загрузчика. В случае включения квот для корневой системы, будут добавлены опции для всех установленных ядер.



- Для файловой системы `NFS` нет возможности изменить статус квот. Включение/отключение квот для пользователей или групп нужно выполнять на сервере `NFS`.

Настройка квот пользователей/групп

Для просмотра текущих настроек квот для пользователей/групп нажмите на строку файловой системы, откроется таблица с данными. В зависимости от статуса квот будут отображены только пользователи/группы или все вместе.

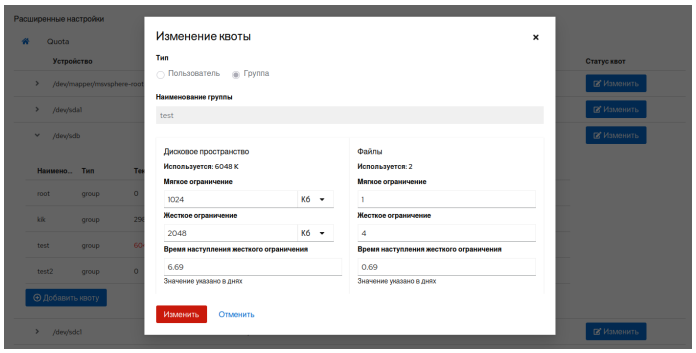


Список квот включает следующие данные:

- Наименование — имя пользователя/группы.
- Тип — пользователь или группа.

- Текущее использование дискового пространства.
- Текущее количество файлов.
- Мягкое ограничение дискового пространства — максимальный объём дискового пространства, доступный пользователю/группе. При его превышении отправляется уведомление, а после включения жёсткого ограничения (по умолчанию через 7 дней), мягкая квота становится жёсткой.
- Жёсткое ограничение дискового пространства — жёсткая квота на объём дискового пространства (при её превышении дальнейшая запись будет запрещена).
- Мягкое ограничение количества файлов — мягкая квота на количество файлов (при её превышении пользователю отправляется уведомление).
- Жёсткое ограничение количества файлов — жёсткая квота на количество файлов (при её превышении дальнейшая запись запрещена).

Для изменения квоты нажмите на кнопку `Изменить` для выбранного пользователя/группы.



Ограничение по объёму можно указать в килобайтах, мегабайтах, гигабайтах или терабайтах. Ограничение по файлам — в единицах. Если для пользователя/группы начался отсчёт времени до наступления жёсткого ограничения, то это значение будет также указано (в днях) и его можно изменить.

Важно!

Для файловой системы `NFS` нет возможности изменить время наступления жёсткого ограничения. Чтобы изменить значение, измените настройки квот на сервере `NFS` для связанной файловой системы.

Если существующий пользователь/группа не указаны в списке, то можно добавить квоту самостоятельно, нажав на кнопку «Добавить квоту».

Расширение «Виртуальные терминалы» для Cockpit

Введение

Расширение «Виртуальные терминалы» позволяет отключить использование виртуальных текстовых терминалов (переключение между ними осуществляется по нажатию клавиш `Ctrl+Alt+F3` — `Ctrl+Alt+F6`).

Установка расширения для Cockpit

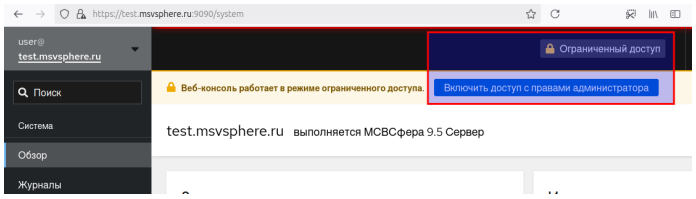
Установите соответствующее расширение для панели управления `Cockpit` с помощью следующей команды:

```
$ sudo dnf install cockpit-msvsphere-virt-terminal
```

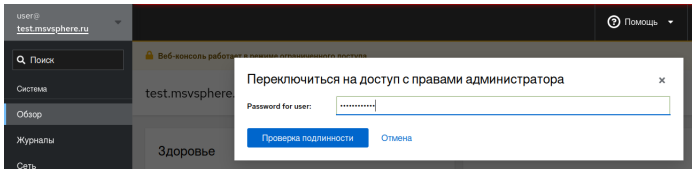
Настройка

Для отключения использование виртуальных терминалов требуются привилегии администратора.

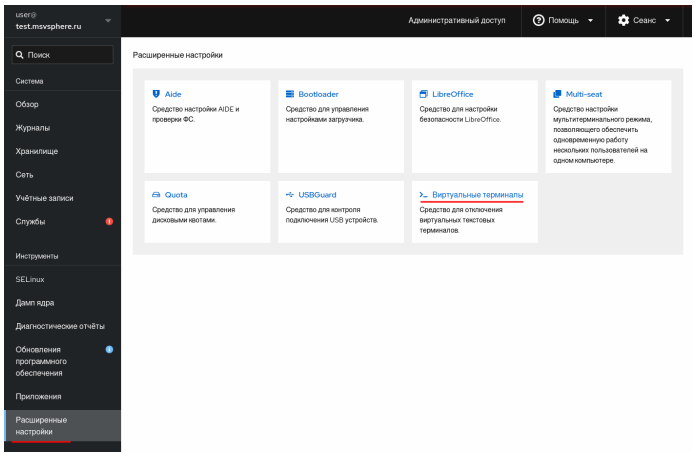
- войдите в панель управления `Cockpit`, на странице «Обзор» нажмите кнопку «Включить доступ с правами администратора» или кнопку «Ограниченный доступ», которая также доступна на других страницах системы управления. На приведённом ниже снимке экрана эти кнопки обозначены красным прямоугольником:



- В открывшейся форме укажите свой пароль и нажмите на кнопку «Проверка подлинности».

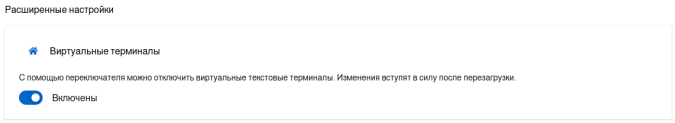


- После этого в левой панели откройте вкладку «Расширенные настройки», там перейдите по ссылке «Виртуальные терминалы».

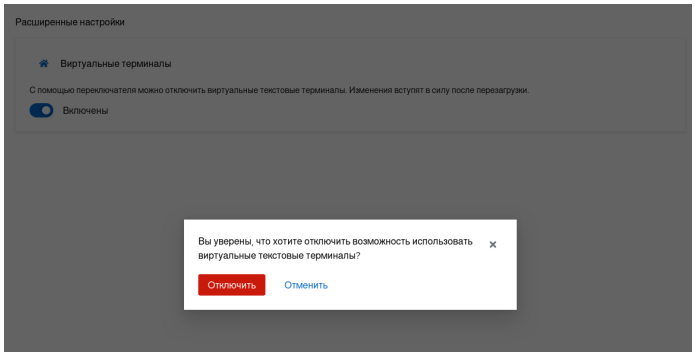


Отключение виртуальных текстовых терминалов

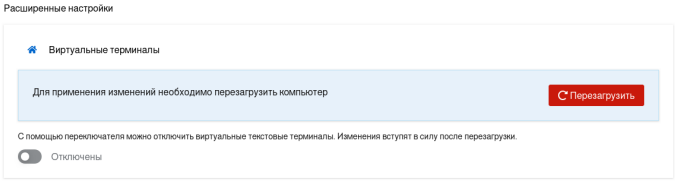
На странице отображается селектор, показывающий текущее состояние виртуальных терминалов (включены/отключены).



При отключении виртуальных терминалов будет показано окно подтверждения.



Настройка будет применена после перезагрузки. После подтверждения будет показана кнопка «Перезагрузить» (перезагрузка будет выполнена сразу после нажатия).



Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводи-тельного докум. и дата	Подп.	Дата
Изм	измененных	замененных	новых	аннулиро-ванных					