УТВЕРЖДЕН

КСФТ.00564-01 91 01-ЛУ

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

ОПЕРАЦИОННАЯ СИСТЕМА РОСА «НИКЕЛЬ»

Руководство пользователя по эксплуатации

КСФТ.00564-01 91 01

Листов 442

2022

Литера $О_1$

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

1.1. Идентификация документа

Название: Операционная система РОСА «НИКЕЛЬ». Руководство пользователя по эксплуатации.

Версия: 1.0.

Обозначение: КСФТ.00564-01 91 01.

Идентификация объекта оценки: Операционная система РОСА «НИКЕЛЬ».

1.2. Аннотация документа

В настоящем документе предоставлена информация, удовлетворяющая требованиям компонента доверия AGD_OPE.1.

Настоящий документ содержит инструкции по эксплуатации программного изделия «Операционная система РОСА «НИКЕЛЬ».

Документ предназначен для администратора ОС и содержит общие сведения об ОС, ее общей структуре, настройке, проверке, контрольных характеристиках развертывания и сообщениях администратору.

Также в документе приведены сведения, необходимые для выполнения операций администрирования:

- начального конфигурирования;
- конфигурирования параметров даты и времени, графической среды, средств ввода и вывода;
- конфигурирования сетей и сетевых служб;
- управления учетными записями и правами доступа пользователей;
- управления системными сервисами и служебными программами;
- настройки специализированного программного обеспечения;
- обновления программного обеспечения;
- просмотра системных журналов;
- управления автозапуском приложений;
- управления параметрами печати;
- работы с носителями информации.

Настоящий документ содержит ссылки на документы:

- КСФТ.00564-01 92 01 Операционная система РОСА «НИКЕЛЬ». Руководство по

подготовительным процедурам (далее – руководство по подготовительным процедурам).

Во 2 главе документа приведены общие сведения об ОС, настройка параметров персонализации и дан перечень предустановленного ПО.

3 главе рассмотрена работа в системе для разных SELinux-пользователей.

Далее в главах 4-21 описаны функциональные возможности и параметры работы ОС.

Команды, для работы в терминальном режиме представлены в документе следующим видом:

```
пример написания команды
```

2. ПРИЕМКА

Проверка подлинности загрузочного модуля проводится сверкой контрольной суммы загрузочного модуля ОС РОСА «НИКЕЛЬ» со значением, указанным в формуляре.

Подсчет и проверка контрольной суммы осуществляются в следующей последовательности:

– включить персональный компьютер (ПК), работающий под управлением любой POSIX-совместимой ОС;

– установить оптический диск в устройство чтения оптических дисков;

– выполнить в консоли команду для расчета контрольной суммы загрузочного модуля:

```
dd if=/dev/cdrom | md5sum
```

– после появления в консоли контрольной суммы ISO-образа оптического диска сравнить ее с эталонным значением;

– извлечь оптический диск из устройства чтения.

Загрузочный модуль является подлинным в случае совпадения контрольной суммы, выданной программой подсчета, со значением, приведенным в документе «Формуляр» КСФТ.00564-01 30 01.

Другие специальные процедуры, необходимые для демонстрации подлинности поставленной ОС РОСА «НИКЕЛЬ», приведены в КСФТ.00564-01 30 01.

3. ОБЩИЕ СВЕДЕНИЯ ОБ ОС

3.1. Установка и настройка

3.1.1. Требования к техническим средствам

Для функционирования ОС необходима следующая минимальная конфигурация оборудования:

- процессор с архитектурой x86_64;
- оперативная память: 2048 МБ;
- дисковое пространство: 20 ГБ;
- VGA-адаптер и монитор с поддержкой разрешения 1024×768 пикс. (24бит);
- устройство чтения оптических дисков;
- клавиатура;
- мышь.

3.1.2. Среда функционирования

Описание среды функционирования приведено в КСФТ.00564-01 30 01. Оценка реализации среды функционирования производится согласно целям безопасности среды функционирования.

3.1.3. Подготовка к установке

Перед началом установки ОС рекомендуется выполнить следующие действия:

- до начала установки необходимо убедиться, что аппаратная конфигурация ПК удовлетворяет минимальным аппаратным требованиям, указанным в настоящем документе, а среда функционирования соответствует требованиям, описанным в настоящем документе;
- убедиться в подлинности DVD-диска с дистрибутивом;
- скопировать с DVD-диска с дистрибутивом ОС образ на USB-носитель (если установка будет производиться с USB-носителя);
- провести (при необходимости) настройку BIOS/UEFI ПК для обеспечения возможности загрузки с выбранного носителя.

3.1.4. Установка настольной версии

Вставить в устройство чтения DVD-дисков загрузочный диск ОС до того, как ПК начнет обращение к загрузочным дискам. Если обращение уже было произведено, и

установка ОС не началась, перезагрузить ПК.

В меню загрузчика (Рисунок 1) с помощью клавиш <↑> и <↓> выбрать пункт «Start Rosa.Nickel.Kde4.B.X86_64». Сделать это необходимо до того, как истечет время ожидания, в противном случае нужно будет перезагрузить ПК. Для перехода к следующему шагу нажать <Enter>.

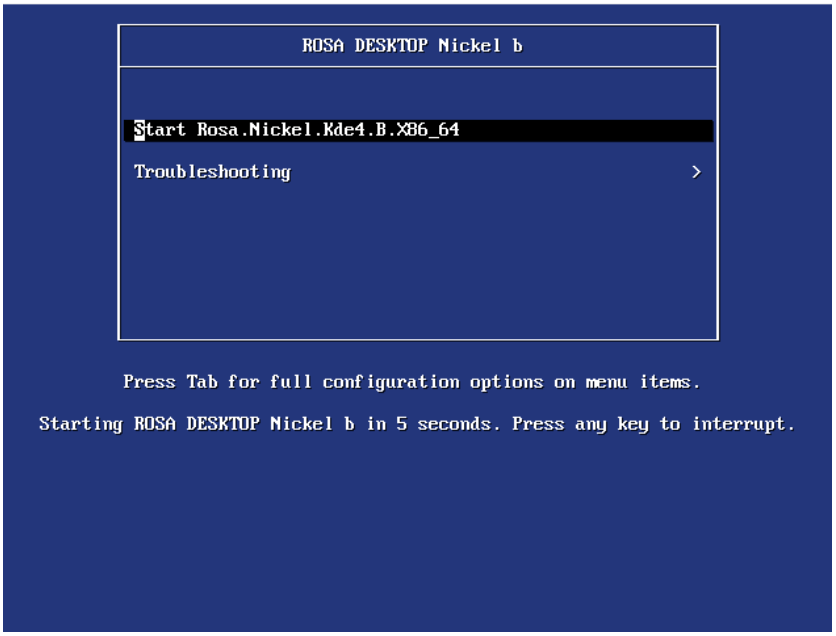


Рисунок 1

Для изменения параметров загрузки навести курсор на пункт «Troubleshooting» и нажать <Enter> (Рисунок 2). Для изменения настройки нажать <Tab>. Для загрузки с указанными вручную параметрами нажать <Enter>. Для возврата к выбору пунктов меню навести курсор на пункт «Return to main menu.» нажать <Enter> .

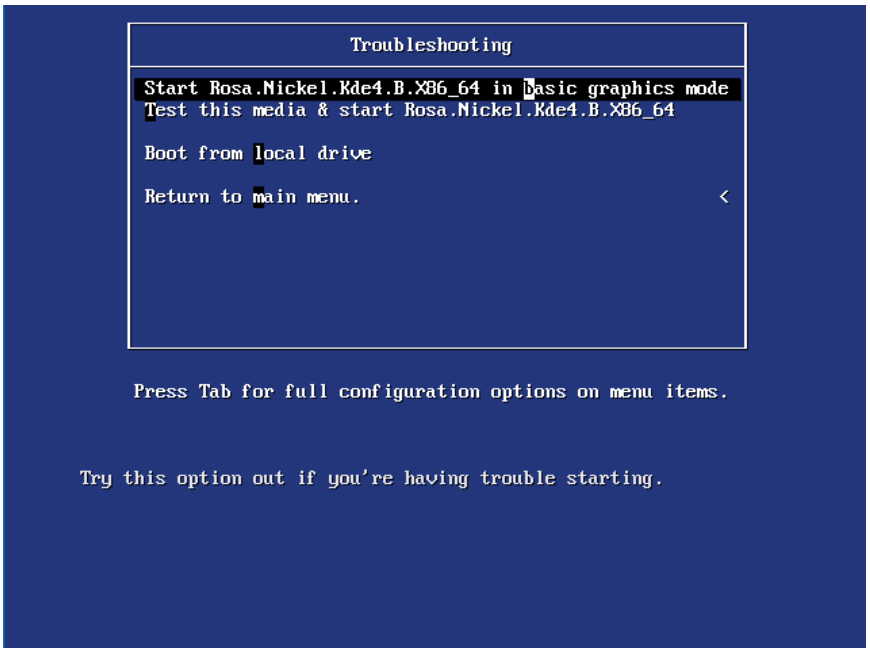


Рисунок 2

В открывшемся окне (Рисунок 3) выбрать из списка требуемый язык интерфейса программы установки. Для отмены установки нажать кнопку [Отменить]. Для перехода к следующему шагу — [Далее] .

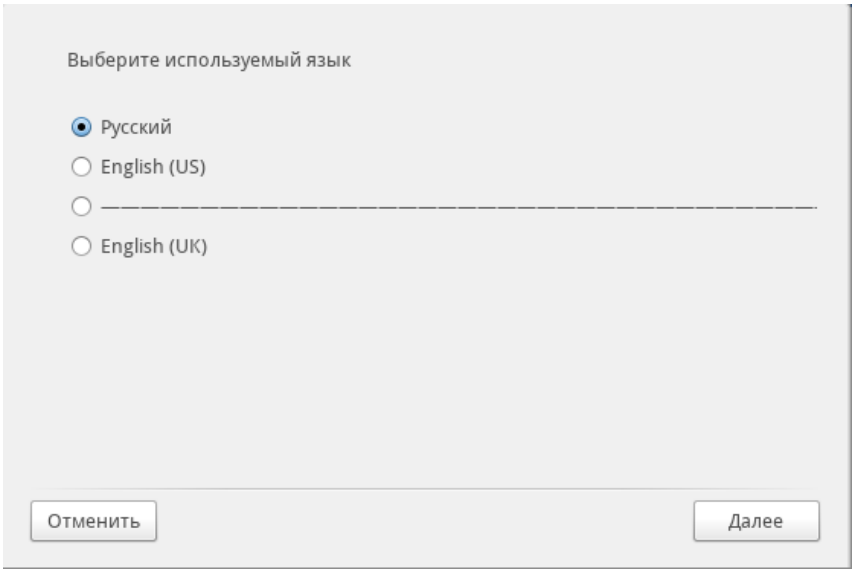


Рисунок 3

В окне с текстом лицензионного соглашения (Рисунок 4) выбрать пункт «Принять». Для отмены установки нажать кнопку [Выйти]. Для перехода к следующему шагу — [OK] .

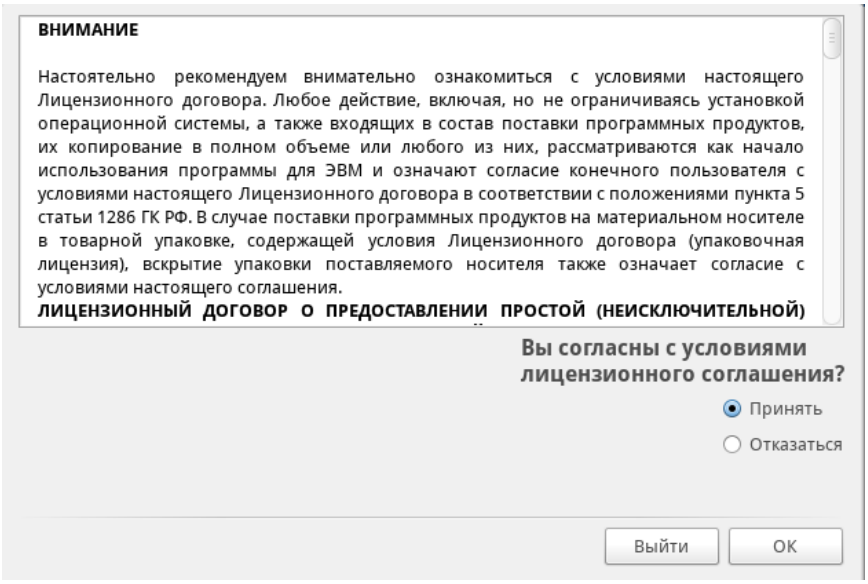


Рисунок 4

В окне настройки раскладки клавиатуры (Рисунок 5) выбрать из списка требуемую раскладку и нажать кнопку [Далее] .

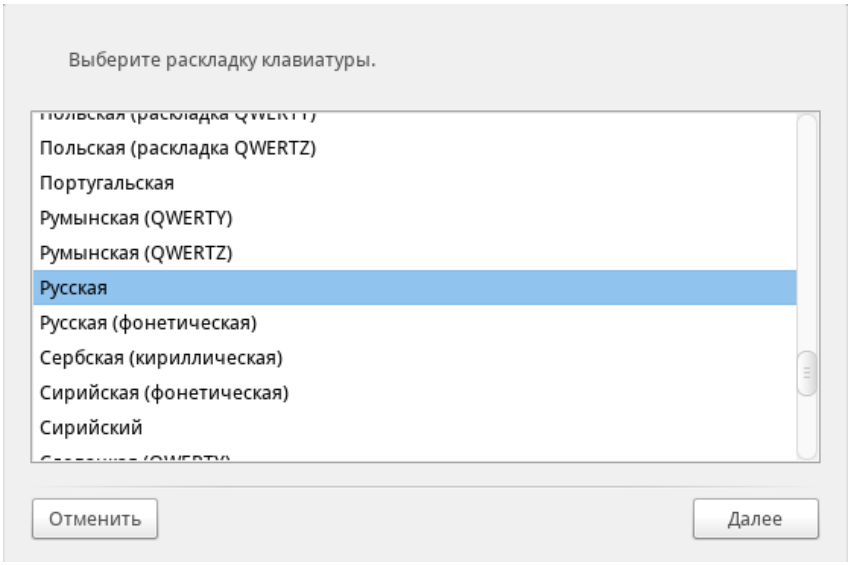


Рисунок 5

В окне настройки способов переключения раскладок клавиатуры (Рисунок 6) выбрать из списка требуемую клавишу или комбинацию клавиш и нажать кнопку [Далее] .

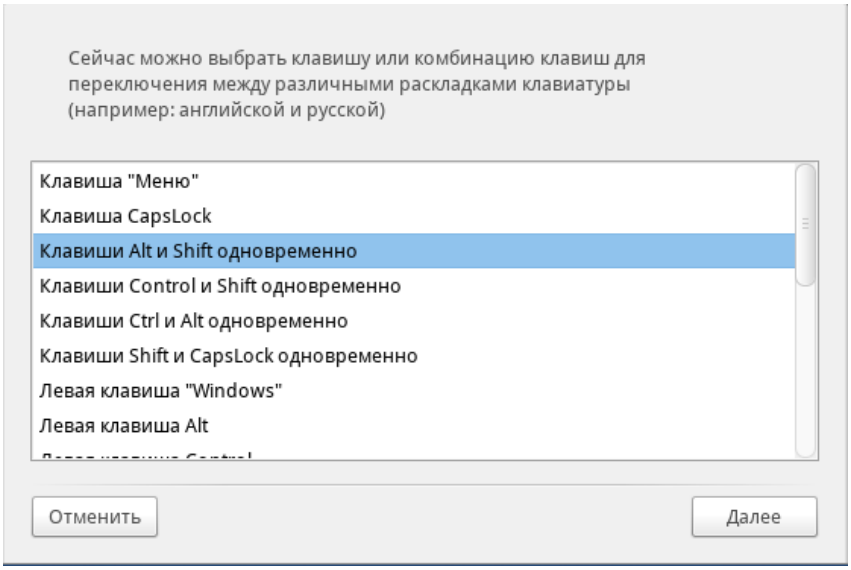


Рисунок 6

В окне выбора часового пояса (Рисунок 7) выбрать из списка город, по часовому поясу которого необходимо выставить время ПК, и нажать кнопку [Далее]. Для отмены установки (как на данном шаге, так и на последующих) нажать кнопку [Отменить] .

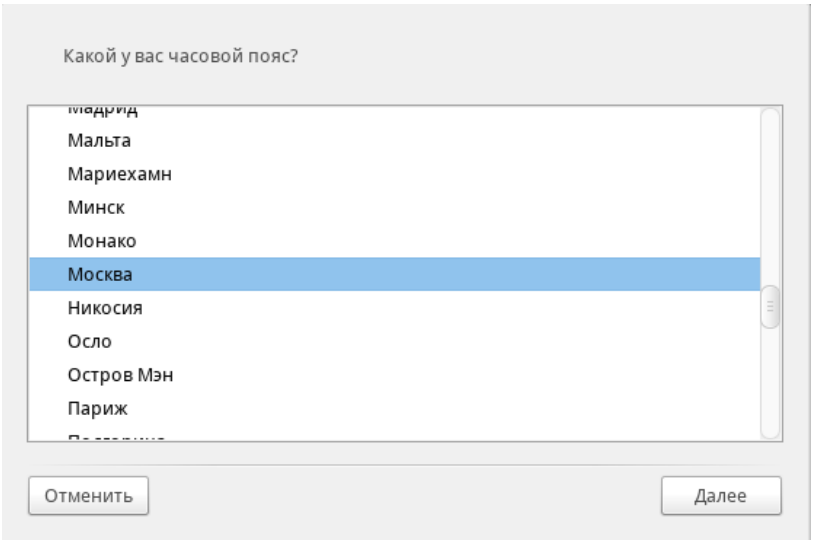


Рисунок 7

В окне настройки даты, времени и часового пояса (Рисунок 8) выбрать пункт «Аппаратные часы выставлены по местному времени» или «Аппаратные часы выставлены по UTC» .

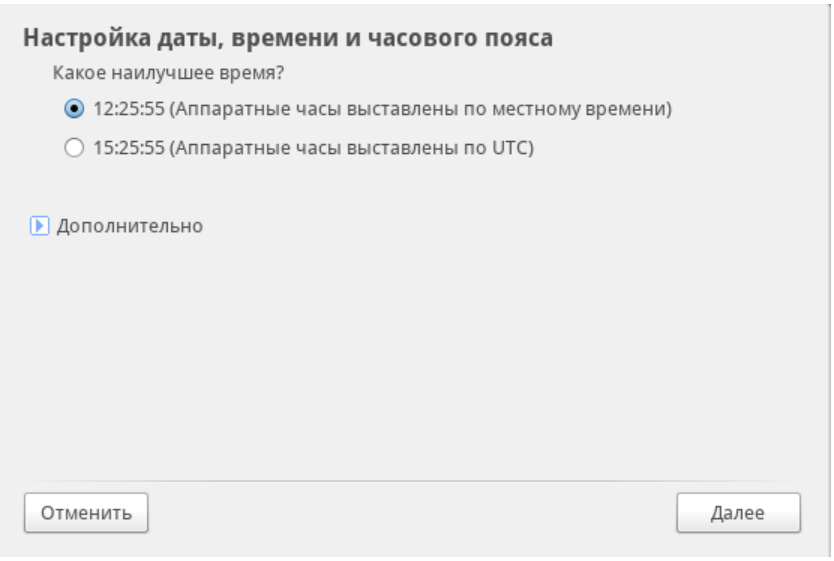


Рисунок 8

Для настройки автоматической синхронизации времени по протоколу NTP нажать вкладку «Дополнительно». В открывшемся окне (Рисунок 9) выбрать пункт «Автоматическая синхронизация времени (через NTP)». Из списка выбрать страну, в которой находится ПК под управлением изделия. Для применения настройки и возврата к предыдущему окну нажать кнопку [OK] .

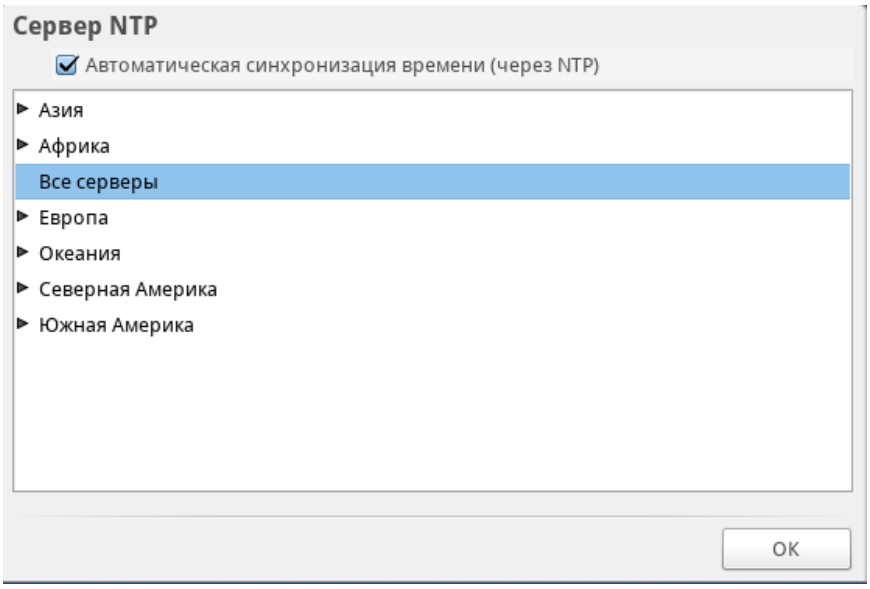


Рисунок 9

Для перехода к следующему шагу нажать кнопку [Далее].

Загрузится рабочий стол (Рисунок 10). Кликнуть дважды на иконку «Установить ОС Роса Никель» .

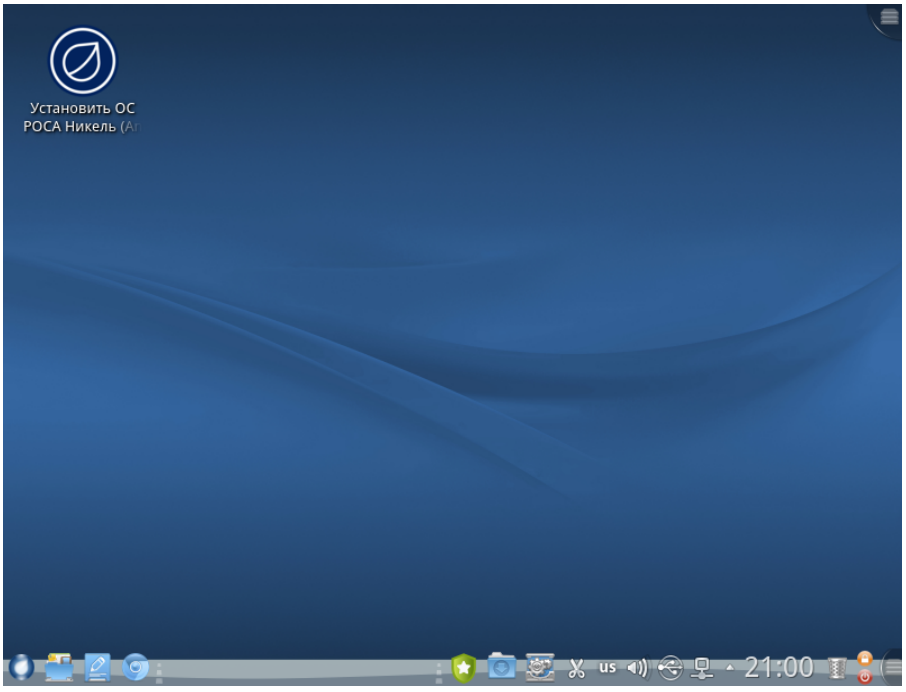


Рисунок 10

В открывшемся окне «Программа установки Anaconda» (Рисунок 11) нажать кнопку [Далее], подтвердив выбор языка установки и системы.

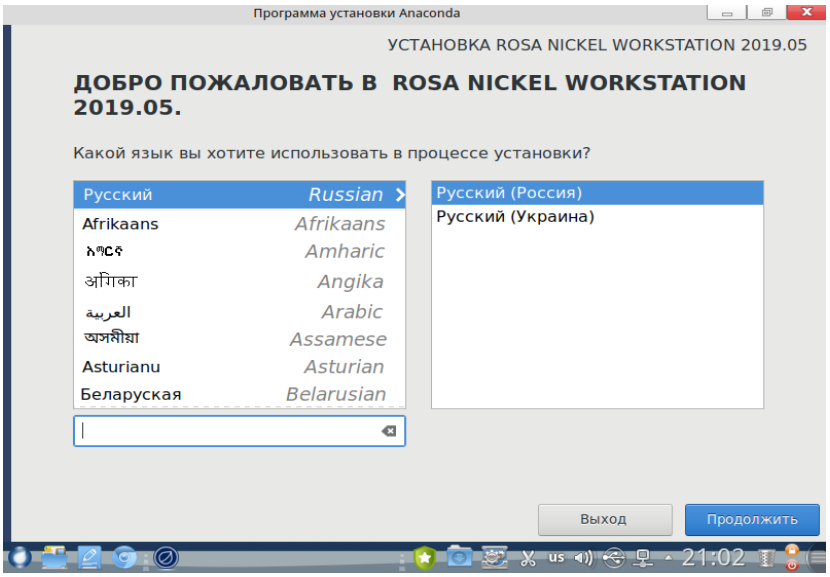


Рисунок 11

На главном экране программы установки (Рисунок 12) указаны пункты настоек. Красным отмечены те, которые требуются изменить для продолжения установки .

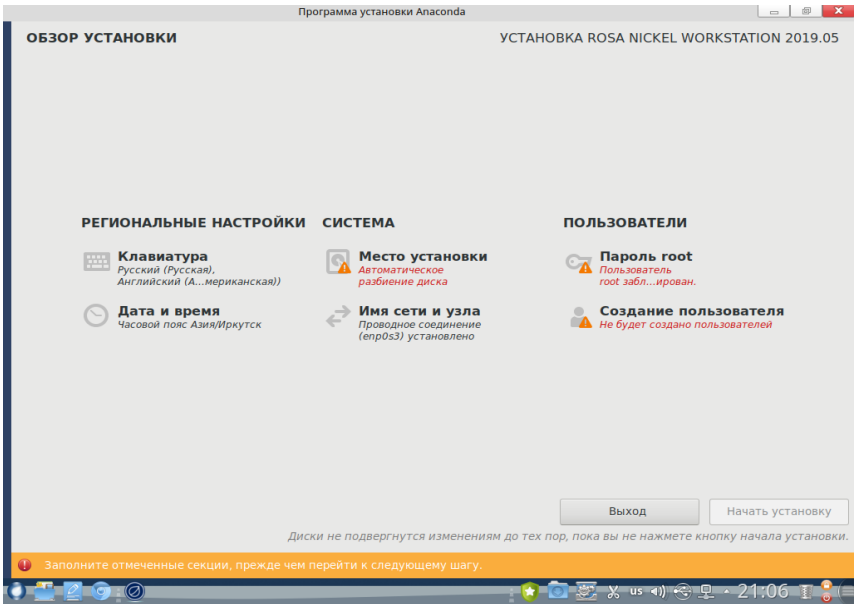


Рисунок 12

Для запуска установки системы необходимо указать место установки (Рисунок 13), пароль технического пользователя root и логин с временным паролем первого пользователя системы.

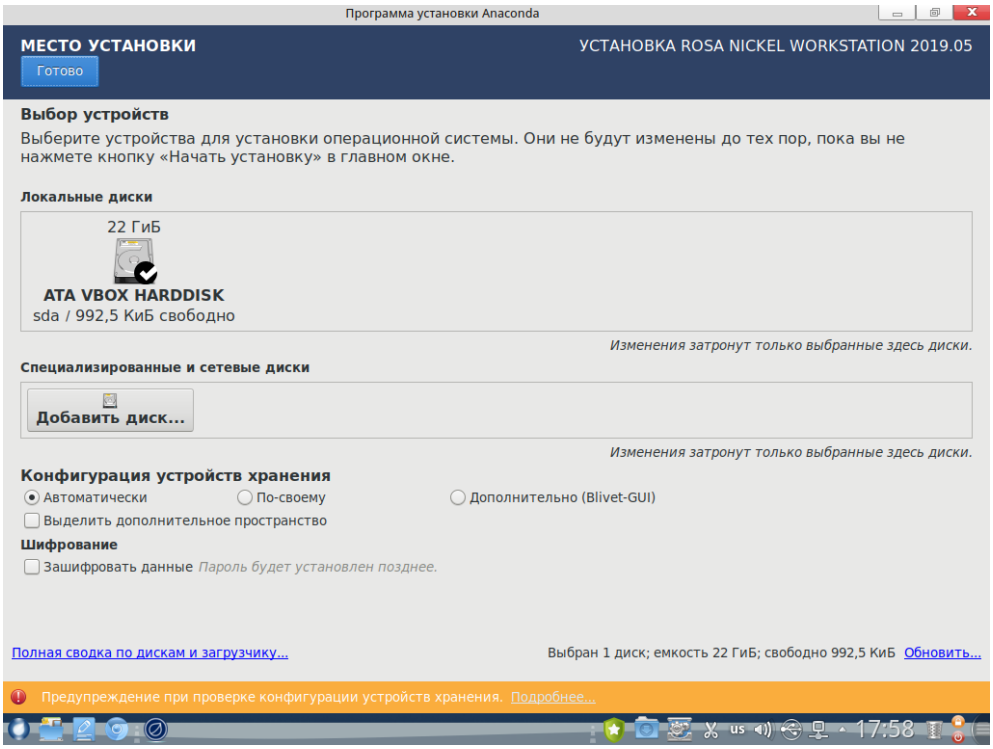


Рисунок 13

Для установки системы необходим диск объемом памяти не менее 20 Гб. Для автоматической установки на единственный пустой диск достаточно нажать кнопку [Готово], при этом будет применена следующая разметка места на диске:

- 5 Гб для раздела /var/log;
- 5 Гб для раздела /var/log/audit;
- до 30 Гб под корень /;
- оставшееся место – для пользовательского раздела /home.

При наличии нескольких жестких дисков необходимо самостоятельно указать диск для установки системы. Для ручной нестандартной разбивки диска переведите переключатель параметра Конфигурация устройств хранения в положение [По-своему] и нажмите на кнопку [Готово].

Раздел или файл подкачки системы автоматически не указывается и не создается установщиком, система рассчитана на безопасную работу без этого раздела только в оперативной памяти. Для работы в небольшом объеме памяти вместо файла подкачки используется сжатие оперативной памяти по технологии zram.

Создание пароля root (Рисунок 14). Пользователь root - технический пользователь, имеющий права на отключение системы безопасности для восстановления системы из резервных копий и отладочных действий в ней. По умолчанию войти в систему под ним нельзя ни в графическом, ни в консольном режиме, пароль root используется только для изменения параметров загрузки grub.

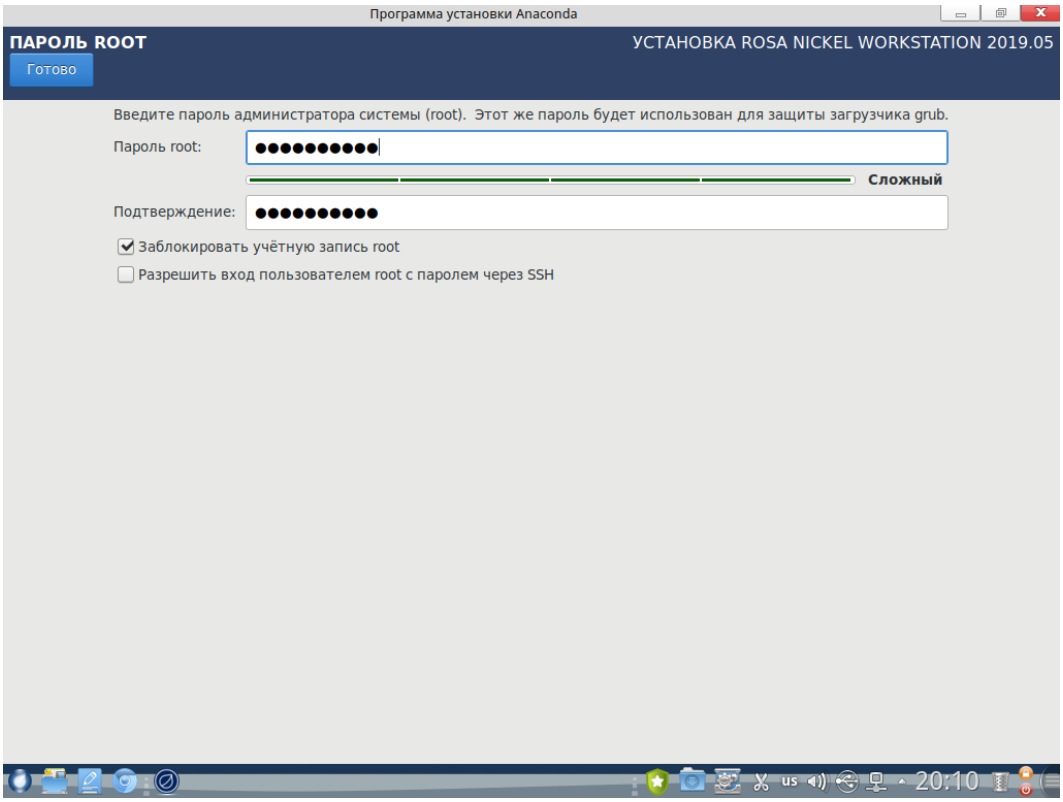


Рисунок 14

Для продолжения установки задайте и повторно подтвердите пароль для пользователя root и нажмите кнопку [Готово].

При задании пароля обратите внимание на требования к сложности пароля:

– длина пароля не менее 8 символов;

– пароль не основан на слове из словаря;

– пароль должен содержать комбинацию минимум трех категорий из перечисленных ниже:

- символы верхнего регистра английского алфавита от A до Z;
- символы нижнего регистра английского алфавита от A до Z;
- цифры от 0 до 9;
- знаки препинания или спецсимволы.

При достаточной секретности индикатор сложности пароля будет подсвечен зеленым.

Создание первого пользователя в системе (Рисунок 15). Первый пользователь системы - пользователь, под которым будет совершен первый вход после установки. Рекомендуемое имя для пользователя: АИБ (aib) - администратор информационной безопасности, штатный администратор системы с правами создания новых пользователей и управления их правами, в том числе и управление правами SELinux.

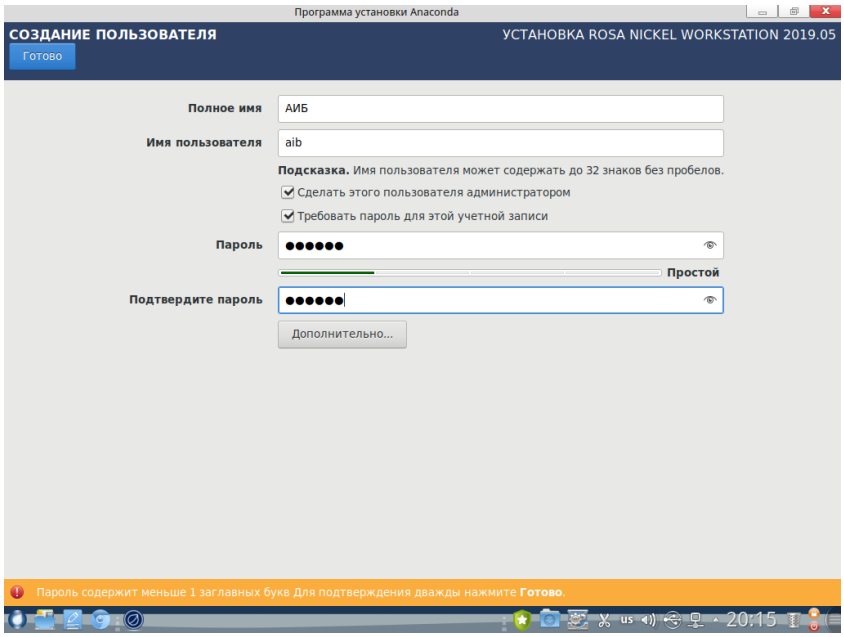


Рисунок 15

Требования к паролю здесь минимальны так как при первом входе будет предложено его сменить на пароль с требованиями, указанными выше.

Таким образом в системе обеспечено разделение ролей установщика системы (root) и администратора (aib), которые по умолчанию не будут знать пароль друг друга.

Установка системы (Рисунок 16). После заполнения отмеченных красным пунктов программы установки становится возможным запуск установки системы на жесткий диск ПК.

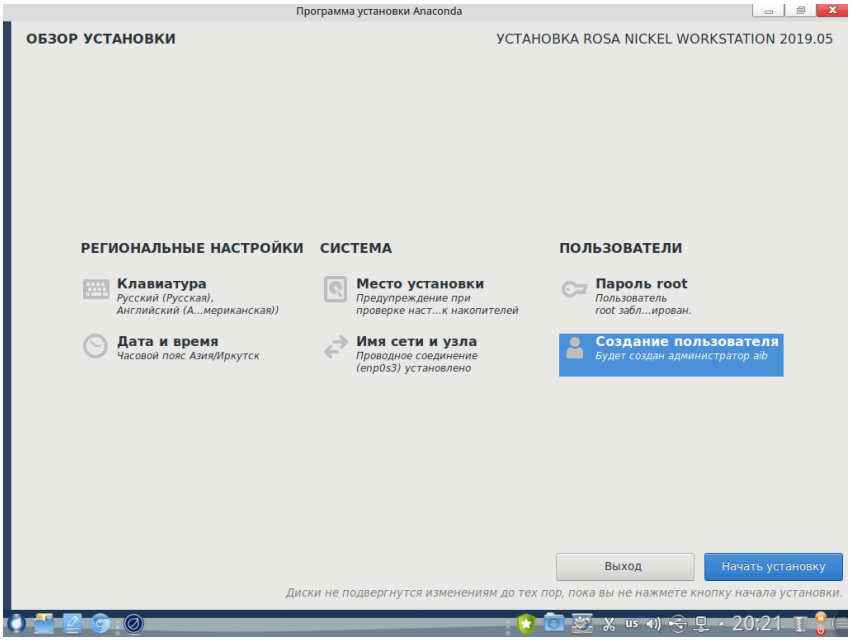


Рисунок 16

Для запуска установки в меню Обзор установки необходимо нажать кнопку [Начать установку]. Процесс установки ОС (Рисунок 17) может занять продолжительное время,

зависящее от аппаратно-технических показателей ПК.

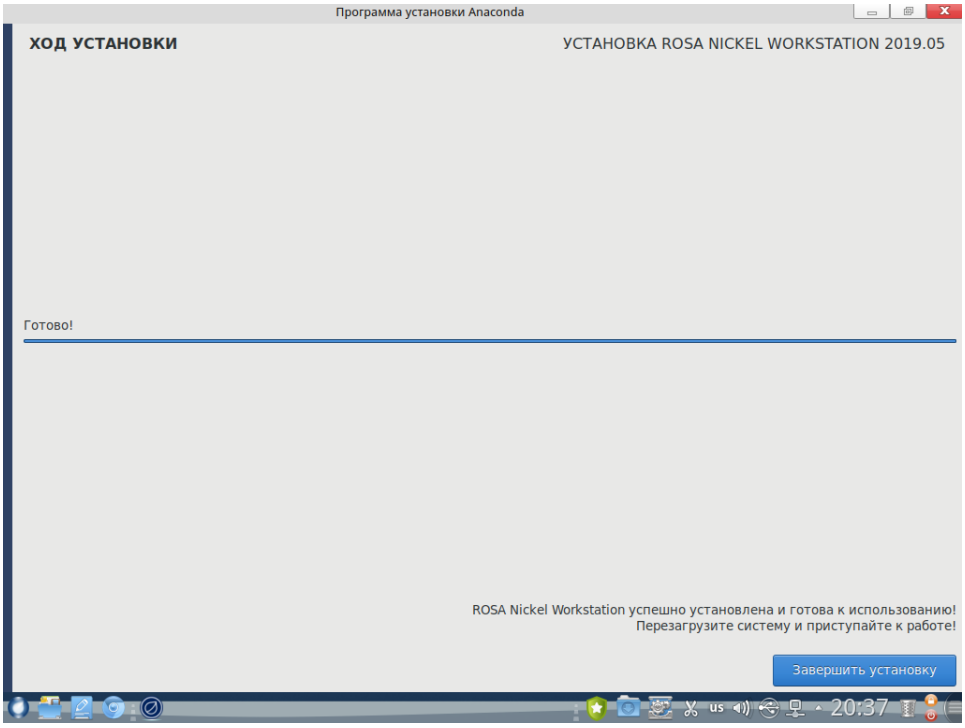


Рисунок 17

Завершение установки. После окончания процесса установки нажмите на кнопку [Завершить установку] и дождитесь закрытия окна установщика, после чего вытащите установочный носитель и перезагрузите систему.

После перезагрузки ОС можно войти под первым пользователем, логин и пароль которого были введены в программе установки.

3.1.5. Установка серверной версии

Для установки серверной версии выполните шаги по установке настольной версии, (см. 3.1.4).

3.2. Интерфейсы ОС

ОС РОСА «НИКЕЛЬ» может управляться посредством графического оконного интерфейса с применением мыши и выбором команд из меню или с помощью текстового интерфейса консоли, доступного администраторам.

По умолчанию система работает в графическом интерфейсе.

Для перехода в консольный режим необходимо запустить программу эмулятора терминала Konsole из главного меню ОС (Рисунок 18).

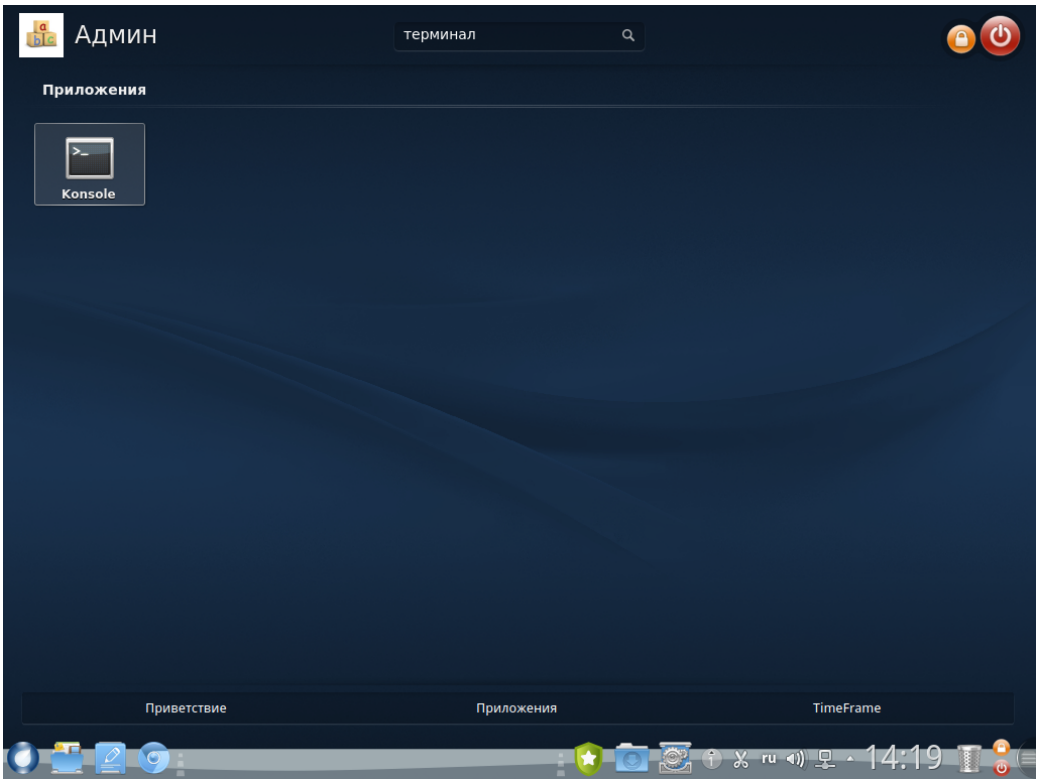


Рисунок 18

Также для входа в терминальный режим можно воспользоваться сочетанием клавиш <Ctrl + Alt + F2> перейти в одну из консолей tty и выполнить вход (Рисунок 19).

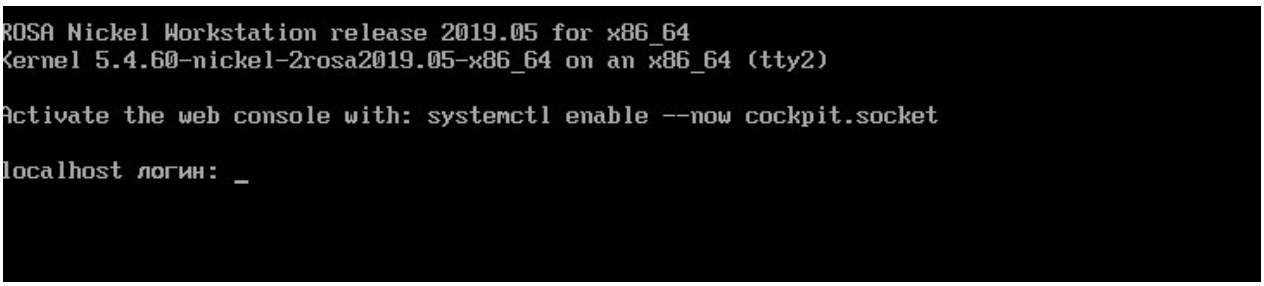


Рисунок 19

Вернуться из tty в графический режим можно воспользовавшись сочетанием клавиш <Ctrl + Alt + F1>.

3.3. Персонализация

Базовые настройки персонализации системы осуществляются в меню [Параметры системы]. Для доступа к меню нажмите на значок в правой части панели задач (Рисунок 20).

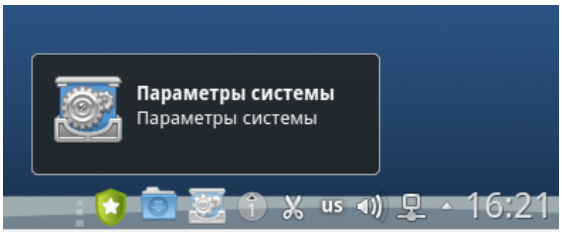


Рисунок 20

В открывшемся меню доступны настройки внешнего вида и среды рабочего стола, основные параметры внешнего вида и поведения ОС, сети и связи, оборудования, а также параметры системного администрирования (Рисунок 21).

Многие из представленных параметров доступны только пользователям с правами администратора.

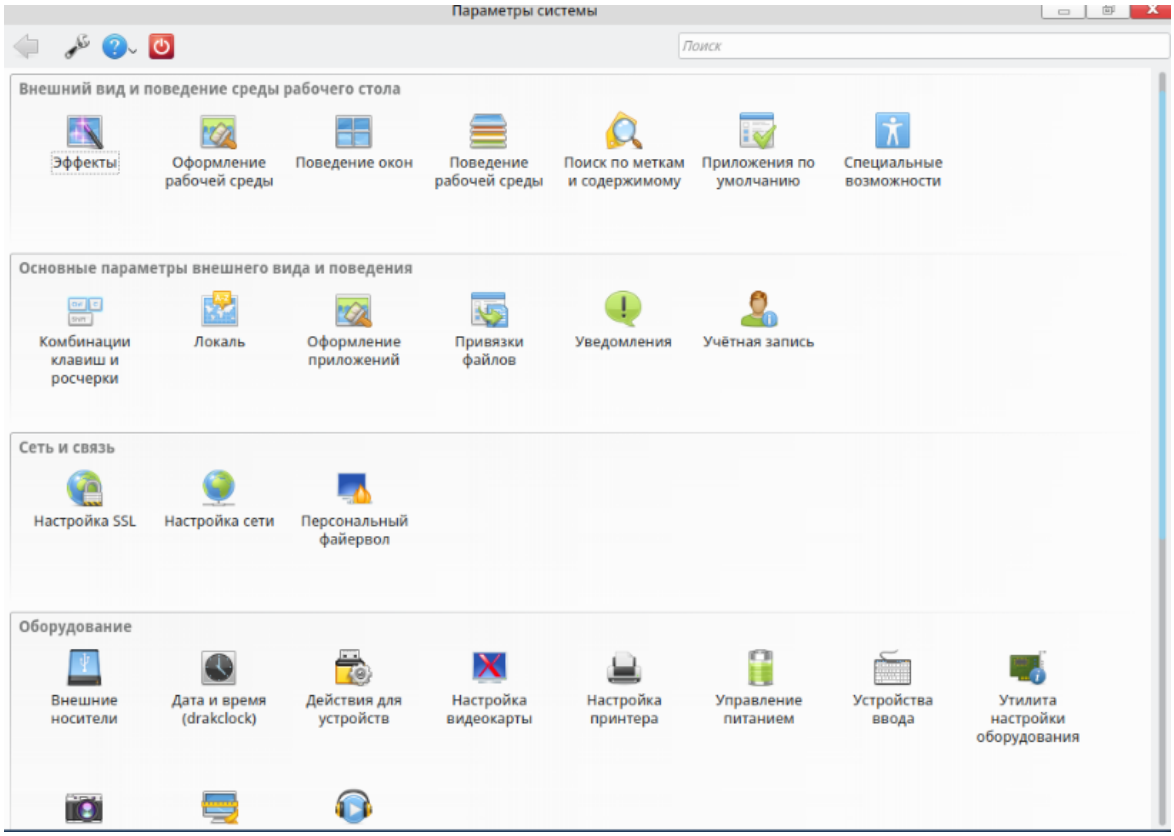


Рисунок 21

3.3.1. Включение и отключение системных служб

Управлять службами можно с помощью утилиты «Управление системными службами» (Рисунок 22), которая находится в блоке [Системное администрирование] программы [Параметры системы].

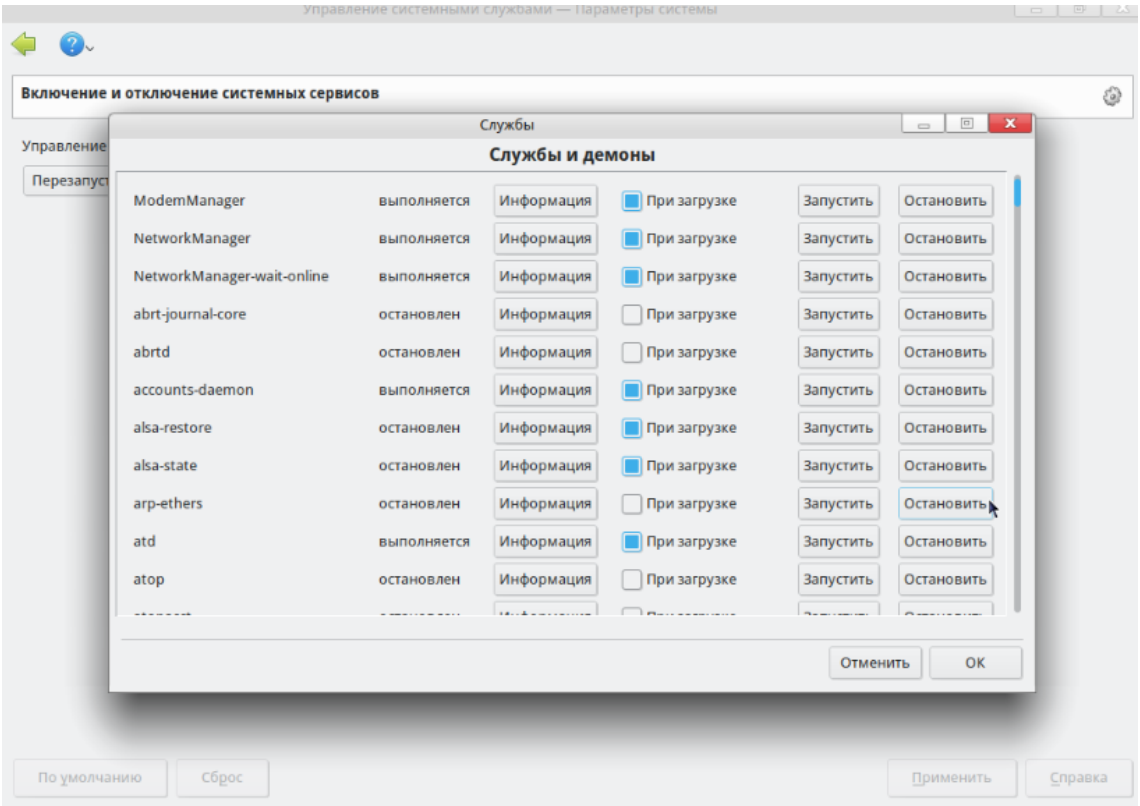


Рисунок 22

Для каждой службы доступны следующие параметры:

– название;

– текущее состояние: выполняется либо остановлен;

– кнопка [Информация] — выводит описание службы;

– флажок [При загрузке]: если он активен, служба будет автоматически запускаться при загрузке системы. Как вариант, если установлен пакет xinetd и выполняется служба xinetd, будет показана опция «Запуск по запросу». Ее установка будет означать активацию этой службы в xinetd;

– кнопка [Запустить] — немедленно запускает службу;

– кнопка [Остановить] — немедленно останавливает службу.

После нажатия кнопок [Запустить] и [Остановить] показывается сообщение, отражающее текущее состояние службы.

Также управление службами может осуществляться через терминальный режим (Рисунок 23). Подробная справка по командам управления системными службами доступна с помощью команды

```
man systemctl
```

Запуск служб ОС осуществляется с помощью systemd, потому в консоли администратора доступны все стандартные для systemd команды для включения, запуска, остановки системных служб. Например, для запуска службы удаленного

управления ssh нужно в консоли администратора ввести команду

```
sudo systemctl start sshd
```

Для проверки состояния службы воспользуйтесь следующей командой:

```
sudo systemctl status sshd
```

Для установки службы в автозагрузку используйте команду:

```
sudo systemctl enable sshd
```

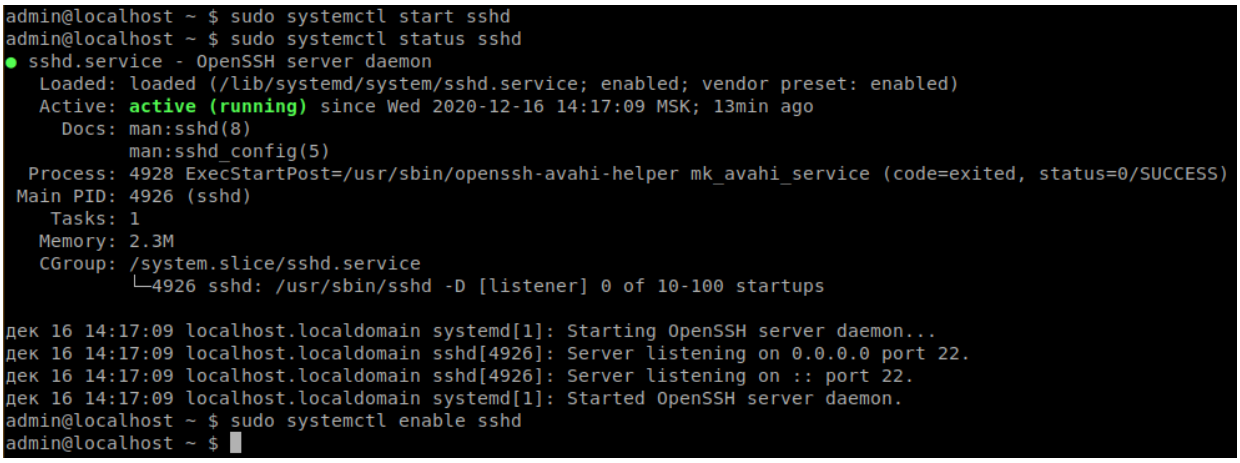


Рисунок 23

3.3.2. Управление шрифтами

Управление шрифтами производится из меню [Параметры системы] → [Управление шрифтами]. В данном меню возможно просматривать установленные шрифты, а с правами администратора системы — устанавливать или удалять их. Главное окно показывает вид выбранного шрифта в определенном размере и начертании (Рисунок 24).

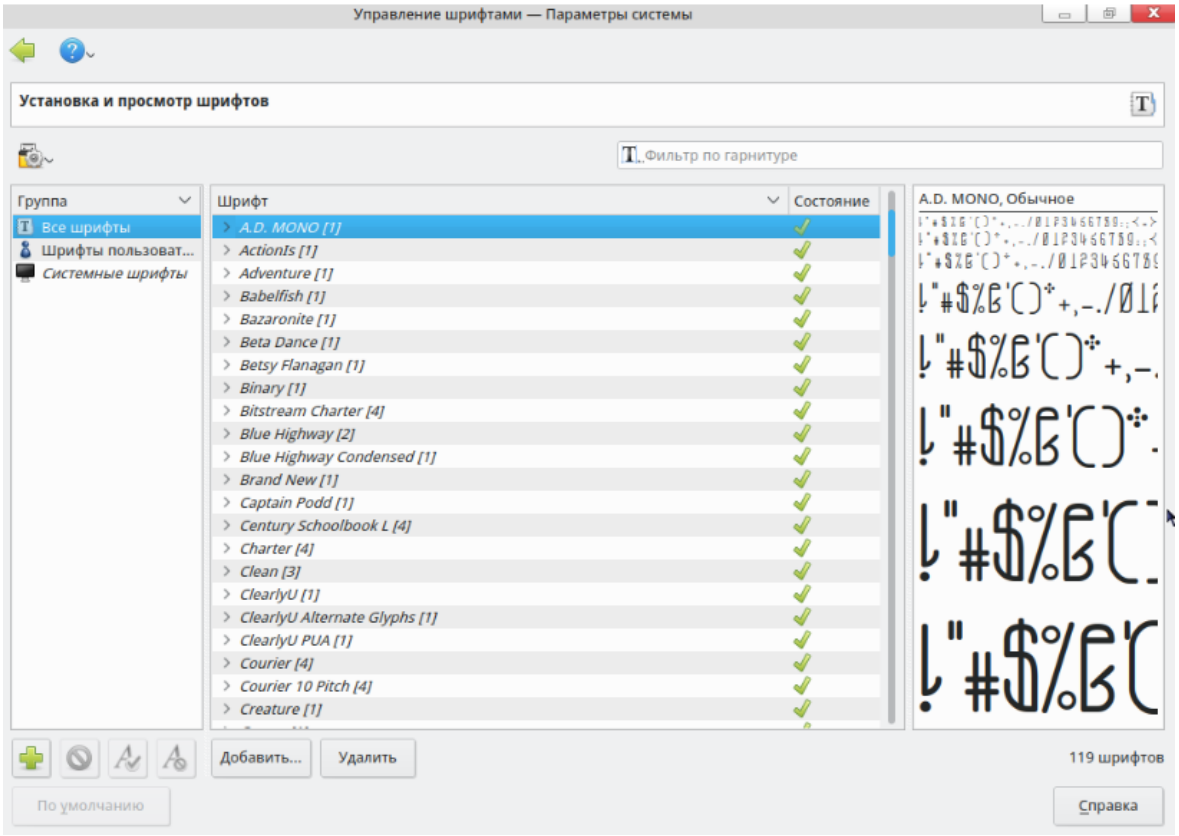


Рисунок 24

С помощью кнопок в нижней части окна возможно создавать новые группы шрифтов, добавлять и удалять шрифты из группы.

Кнопка [Добавить] позволяет вручную добавить шрифты, не входящие в ОС РОСА «НИКЕЛЬ». Поддерживаемые форматы шрифтов: TTF, PFA, PFB, PCF, PFM, GSF. При нажатии на кнопку [Добавить] откроется диалоговое окно, позволяющее указать файл импортируемого шрифта. После того, как вы выбрали все шрифты для импорта, нажмите на кнопку [Установить].

Модуль «Шрифты» программы «Параметры системы»

Этот модуль доступен в рамках утилиты [Оформление приложений] блока [Основные параметры внешнего вида и поведения] программы [Параметры системы] (Рисунок 25).

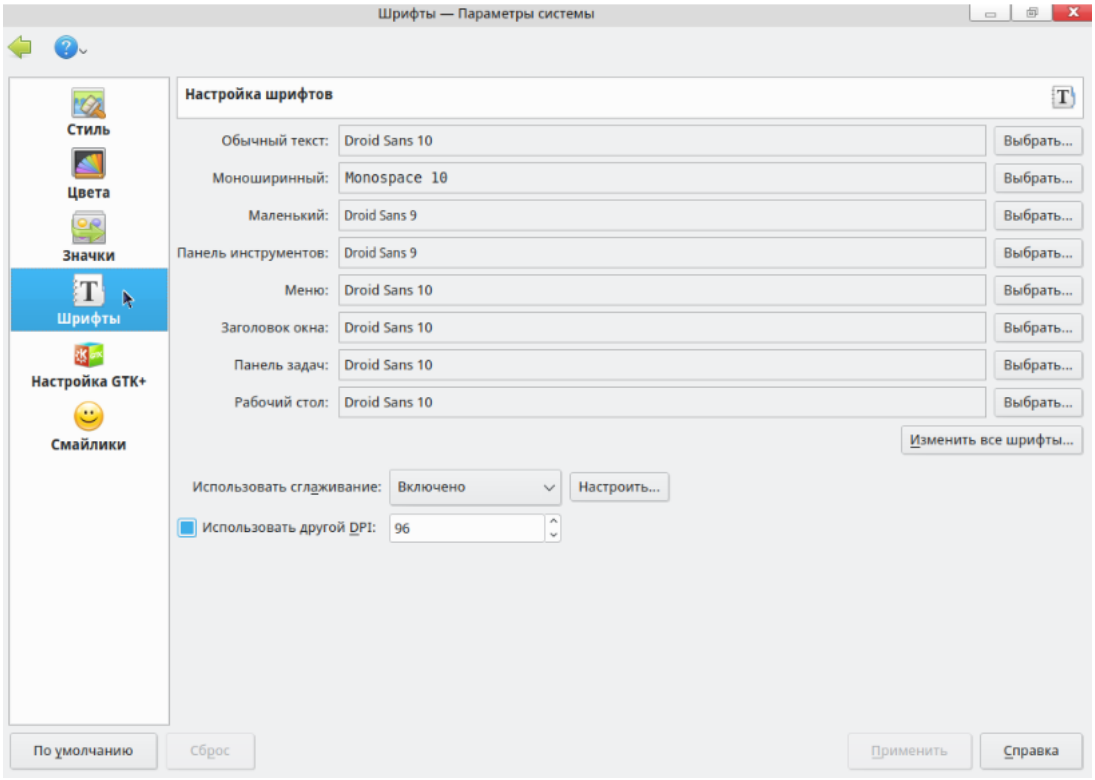


Рисунок 25

В нем можно выбрать, какие шрифты в каком размере и начертании будут использоваться в интерфейсе системы. Выпадающий список [Использовать сглаживание] позволяет включать и отключать функцию, делающую шрифты более плавными. Также в этом окне можно изменить разрешение в DPI (dots per inch, «точек на дюйм»).

3.3.3. Настройка даты и времени

Для настройки системных даты и времени используется программа [Дата и время] (DrakClock) (Рисунок 26). Ее можно найти в блоке [Оборудование] программы [Параметры системы].

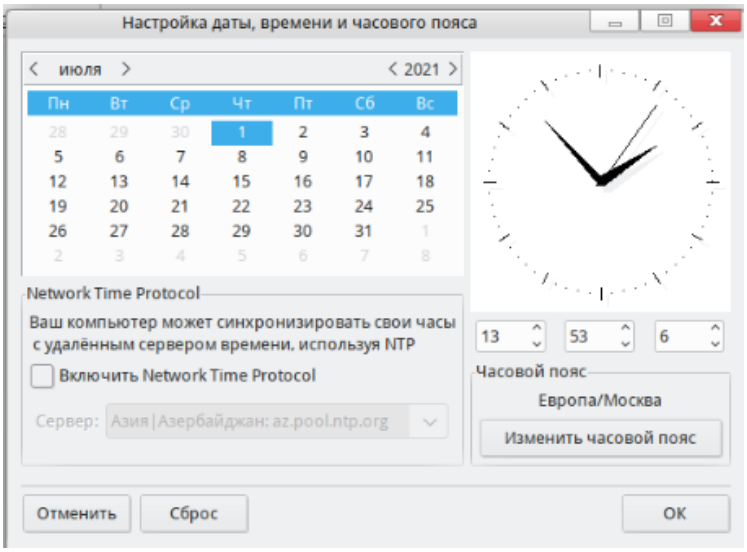


Рисунок 26

Если у вас есть постоянное подключение к интернету, система может синхронизировать часы с серверами точного времени. Для этого установите флажок [Включить Network Time Protocol] и выберите из выпадающего списка ближайший сервер. Если вы знаете имя или IP-адрес другого сервера, вы можете указать его в этом поле.

Установка даты и времени пояснений не требует, однако могут возникнуть вопросы насчет выбора часового пояса. После того, как вы указали часовой пояс, появится диалоговое окно, спрашивающее у вас, установлены ли ваши часы по Гринвичу (GMT). Ответьте [Да], если на ПК установлен только Linux, в противном случае выберите [Нет].

Также установка даты и времени доступна и через интерфейс консоли. Утилита timedatectl предназначена для управления системным временем. Часто используемые опции утилиты timedatectl (Таблица 1). Подробное описание приведено в man timedatectl.

Синтаксис:

```
timedatectl <Опции> <Пользователь>
```

Таблица 1

Опция	Описание
status	Вывод текущей даты и времени, параметров времени
set-time [TIME]	Изменение времени и даты. Формат времени ГГГГ-ММ-ДД и/или ЧЧ:ММ:СС
list-timezones	Вывод доступных часовых поясов
set-timezone [TIMEZONE]	Установка часового пояса

Утилита date также предназначена для управления временем. Утилита timedatectl имеет больший функционал, поэтому настройку времени рекомендуется осуществлять с помощью timedatectl. Подробное описание утилиты date приведено в man date.

Если NTP сервер имеет статус `service: active`, то нужно ввести команду `timedatectl set-ntp 0`, после чего станет возможным менять дату и время по отдельности.

3.3.4. Рабочий стол KDE

Вид рабочего стола (Рисунок 27), на столе можно размещать файлы и каталоги; нажав на файл левой кнопкой мыши дважды, вы откроете его в ассоциированном приложении.

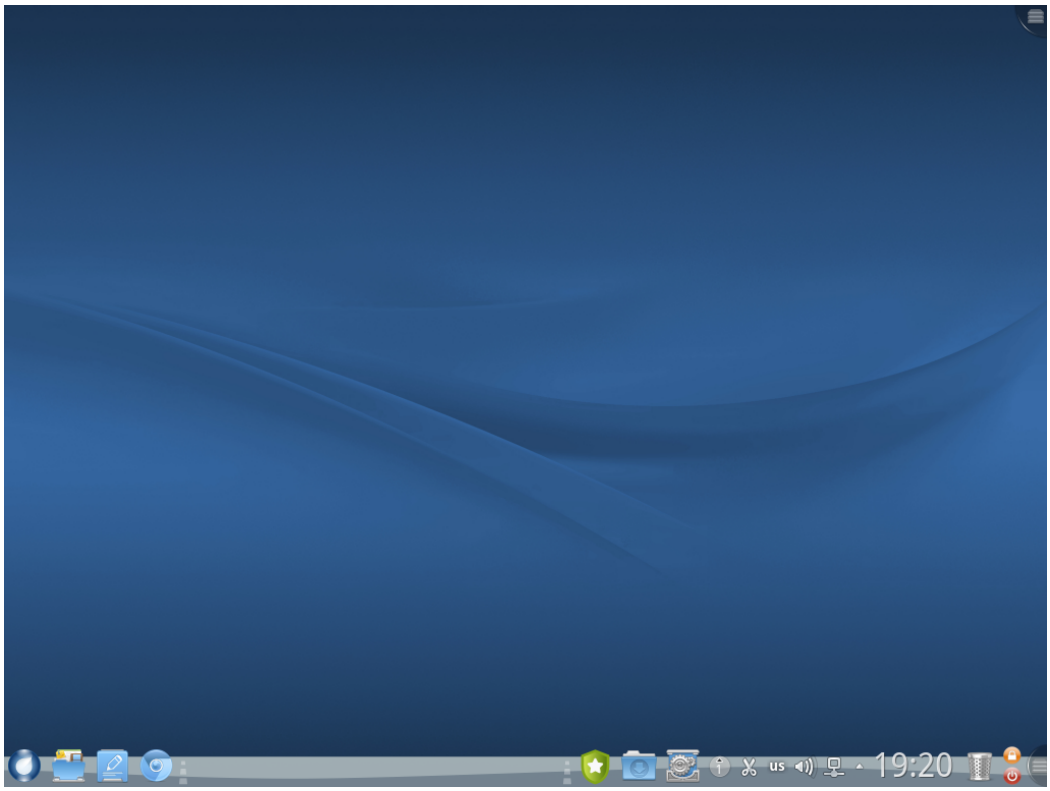


Рисунок 27

Ключевыми объектами рабочего стола KDE являются:

– Панель (панелью задач), расположена в нижней части рабочего стола, на которой можно размещать кнопки запуска приложений, список окон (программ), часы и системный лоток (трей);

– Рабочий стол — область, где находятся виджеты и значки;

– «Просмотр папки» — виджет, который показывает содержимое папки на ПК и обеспечивает быстрый доступ к действиям с файлами и папками;

– Кнопки инструментов Plasma, расположенные в правом верхнем углу экрана и в конце панели. Эти кнопки используются для удобного доступа к настройке параметров рабочего стола.

Окно папки на рабочем столе можно вращать, для чего нужно навести указатель мыши на папку, выбрать на всплывающей панели значок поворота (Рисунок 28), зацепить его и, удерживая кнопку мыши, поворачивать (

Рисунок 29).

Рисунок 28

Рисунок 29

Для быстрого просмотра вложенной папки наведите на нее указатель мыши и нажмите на появившийся значок в виде стрелки. Будет открыто небольшое окно для

просмотра содержимого вложенной папки (Рисунок 30).

Рисунок 30

Если в папке есть изображения, их можно быстро просмотреть таким же способом — просто наведя на значок файла указатель мыши.

Аналогичным образом можно просматривать не только вложенные папки первого уровня, но и папки подкаталогов нижних уровней.

Также в ОС РОСА «НИКЕЛЬ» поддерживается функция Поворот экрана. Для реализации данной функции воспользуйтесь следующей командой в Терминале (о работе в терминале см. подробнее в разделе 6.2.):

```
xrandr –o right; sleep 1; xrandr –o normal
```

3.3.5. Виджеты

Виджетами называют небольшие приложения рабочего стола, которые добавляются на рабочий стол для быстрого доступа. Например, это могут быть часы, прогноз погоды, система перевода единиц измерений, индикатор загрузки процессора и т. п. Оформляются виджеты узнаваемыми графическими значками, которые могут находиться на самом пространстве рабочего стола, на панели задач, на экранной заставке, на приборной панели и в других местах.

Чтобы добавить виджет на рабочий стол, воспользуйтесь кнопкой инструментов Plasma в правом верхнем углу и выберите пункт меню [Добавить виджеты] (Рисунок 31).

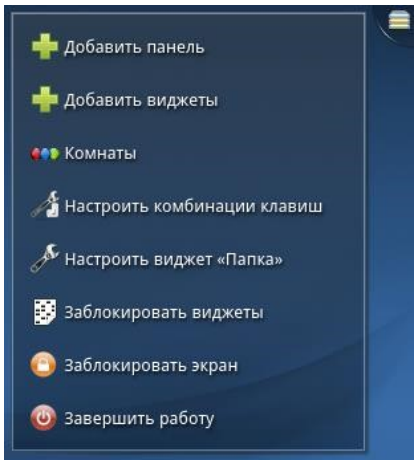


Рисунок 31

Виджет [Папка] (Рисунок 32), как говорит его название, показывает на рабочем столе содержимое выбранной папки. Папка может быть как локальной (на ПК), так и сетевой (подключенной по протоколу FTP, SSH или SMB). Виджет позволяет задать фильтр показа файлов. Например, показывать файлы с определенным расширением, либо только изображения/документы/архивы.

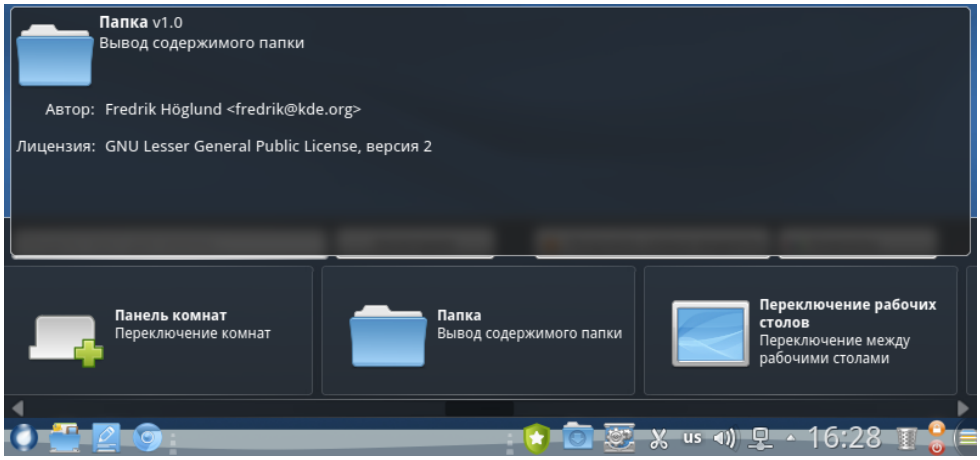


Рисунок 32

3.3.6. Настройка рабочего стола

В разделе [Внешний вид и поведение среды рабочего стола] программы [Параметры системы] пользователь может настроить различные элементы рабочего стола.

Фон рабочего стола

Для смены фона рабочего стола щелкните по нему правой кнопкой и выберите в контекстном меню пункт [Настроить виджет Папка]. Далее в выпадающем меню [Тип комнаты] выберите [Рабочий стол]. Пользователь может выбрать оформление рабочего стола как из предложенных системой вариантов, так и воспользоваться собственной библиотекой изображений, загрузив их из соответствующего каталога с помощью кнопки [Загрузить новые обои] (Рисунок 33).

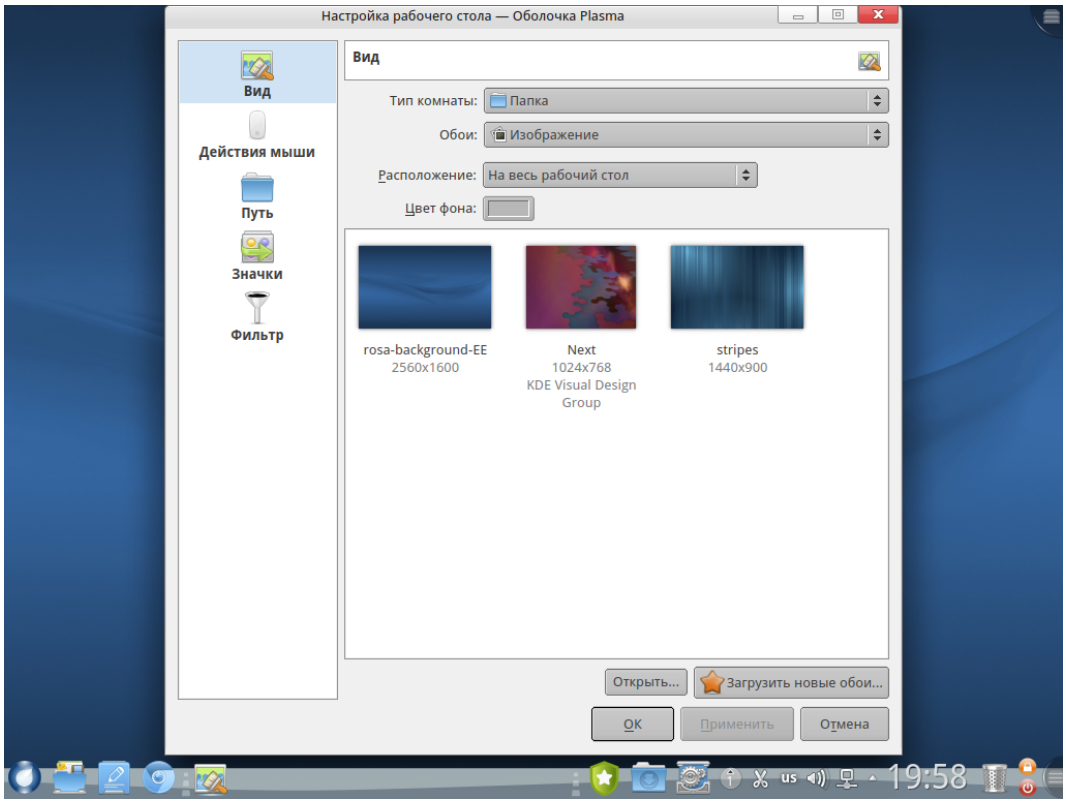


Рисунок 33

На этой же панели можно задать действия, выполняемые с помощью кнопок мыши, и настроить другие параметры.

3.4. Встроенное программное обеспечение

3.4.1. Dolphin — менеджер файлов

Менеджер файлов Dolphin предоставляет пользователю возможность осуществления базовых действий с файлами и каталогами в графическом режиме.

Dolphin запускается нажатием левой кнопки мыши по значку в левой части панели меню или с помощью поиска в системном меню. При первом запуске в окне Dolphin будет показано содержимое домашнего каталога текущего пользователя (`/home/<имя_пользователя>`) (Рисунок 34).

В домашнем каталоге находятся несколько подкаталогов, в которые по умолчанию предлагается сохранять файлы пользователя в зависимости от их вида: «Документы», «Изображения», «Загрузки» и т. п. Можно воспользоваться ими, создавая необходимую структуру каталогов внутри, а можно сделать это и непосредственно в домашнем каталоге.

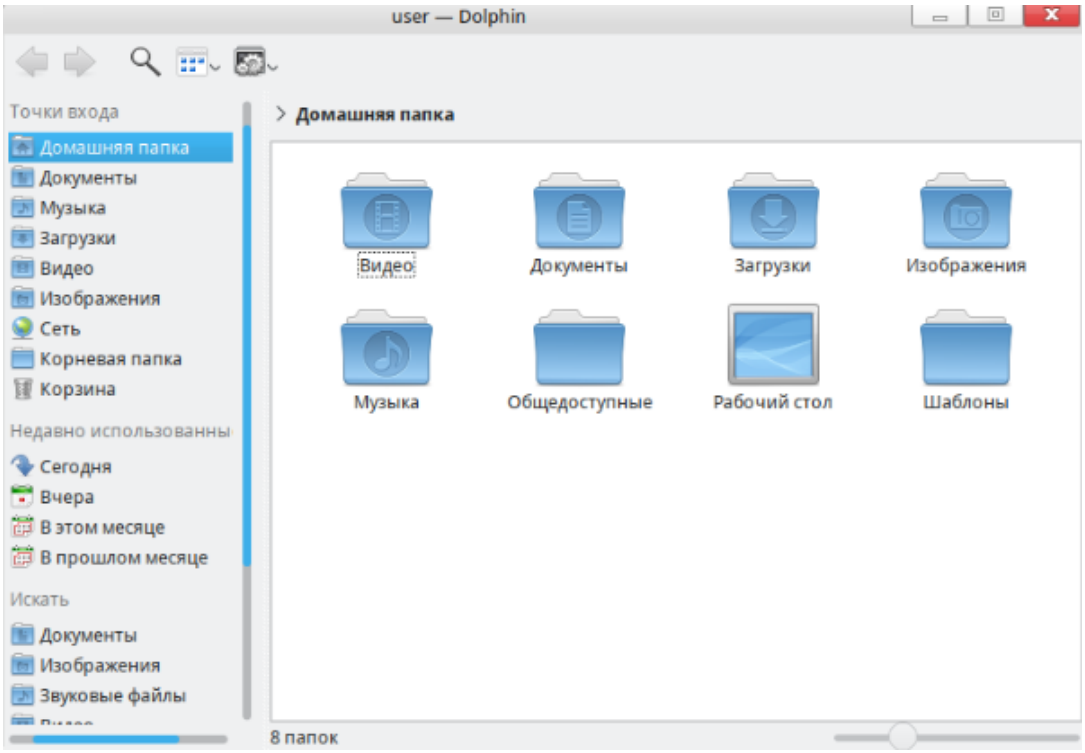


Рисунок 34

Для создания нового каталога нажмите клавишу <F10> или щелкните в окне Dolphin правой кнопкой мыши и выберите в контекстном меню команду «Новая папка». Введите в появившемся окне название для папки вместо предложенного по умолчанию и нажмите на кнопку [OK].

Для переименования каталога выделите его или войдите внутрь, щелкните правой кнопкой и в появившемся контекстном меню выберите команду «Свойства» (или выделите каталог и нажмите клавишу <F2>). Название каталога можно отредактировать на первой же вкладке окна свойств — [Основное] (Рисунок 35).

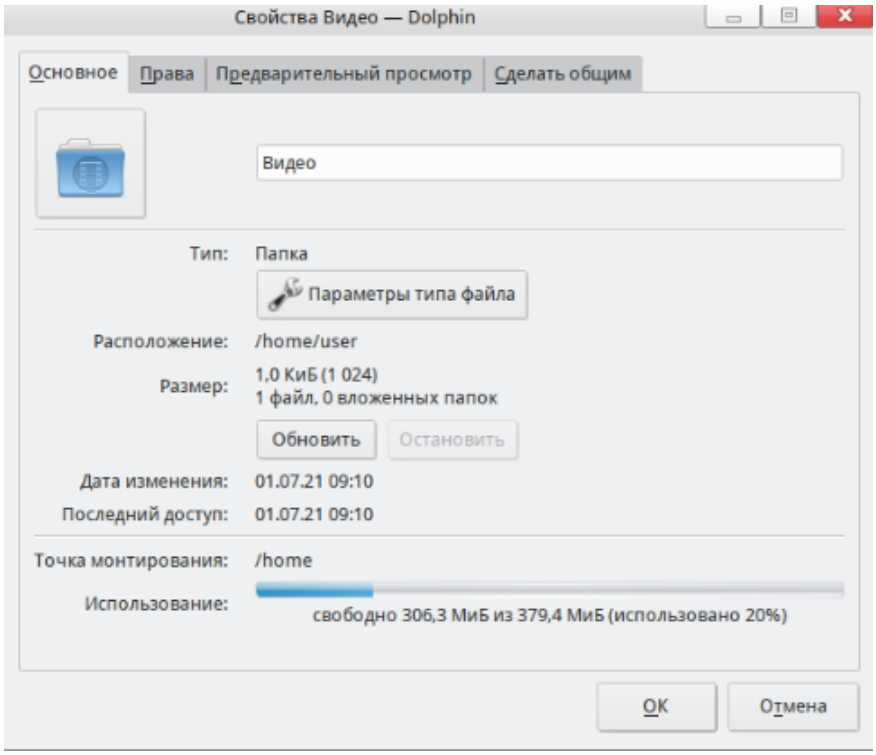


Рисунок 35

Корневой каталог откроет корневой уровень ФС Linux. Здесь в определенной структуре хранятся системные файлы, параметры системы, установленные программы, а также домашние каталоги всех пользователей (в каталогах `home/имя_пользователя`).

Корзина

В корзине хранятся удаленные файлы. Открыв корзину, можно найти и восстановить ошибочно удаленный файл.

Сменные устройства и носители

Сменные устройства и носители монтируются администратором системы с помощью инструмента ROSA Removable drive manager, об этом подробнее см. раздел 10.1. ROSA Removable Drive Manager

Для отключения уже смонтированного USB-устройств пользуйтесь пунктом «Безопасное отключение» контекстного меню соответствующей точки входа. Это предохранит ФС на устройстве от повреждений.

Сеть

Если ПК включен в сеть, эта точка входа предоставляет удобный доступ к сетевым ресурсам. Откройте папку Network или Samba Shares, выберите систему, содержимое которой вы хотите посмотреть, и двигайтесь внутрь до интересующего вас каталога.

Пользовательские точки входа

Чем продуманнее система каталогов для хранения файлов, тем легче найти

нужную информацию. Но когда уровней и разветвлений оказывается много, это также может быть не удобным: чтобы добраться к каталогу с нужными файлами, приходится проходить целый ряд уровней. Перетащите каталоги, с которыми вы часто работаете, на панель точек входа Dolphin. Тем самым вы создадите новые точки входа: щелчок по такой точке будет сразу открывать нужное место. Новая точка входа появится и на вкладке «Приветствие» в системном меню.

Управление точками входа

Все операции управления осуществляются через контекстное меню точек входа или всей панели в целом (при щелчке правой кнопкой мыши на свободном месте панели точек). Если точка не нужна (например, вы не используете Bluetooth), ее можно скрыть командой «Скрыть точку входа», чтобы она напрасно не загромождала список. Собственные точки входа можно удалить аналогичным образом. Чтобы восстановить показ скрытых точек, выберите в меню панели команду [Показать все].

Поиск файлов

Наряду с системным меню, для поиска файлов можно использовать и Dolphin. Панель поиска вызывается щелчком по значку с лупой (Рисунок 36). Поиск начинается при вводе искомого контекста, результаты выводятся в окне ниже. При поиске файла по имени можно использовать маски, в которых звездочка (*) заменяет любое количество любых символов, а вопросительный знак (?) — любой одиночный символ.

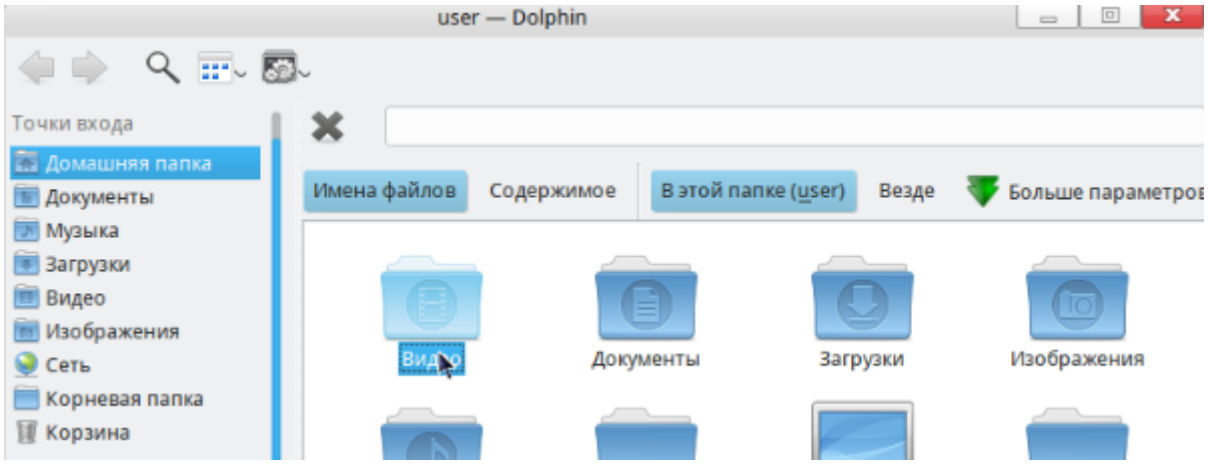


Рисунок 36

Архивирование файлов

Менеджер файлов Dolphin дает возможность архивировать данные в форматы ZIP и распаковки данных из архивов ZIP и RAR, TAR, TAR.BZ2, TAR.GZ, TAR.LZMA, TAR.XZ. Для этого нажмите правой кнопкой мыши на необходимый файл и в контекстном меню выберете параметр Упаковать и далее необходимый формат архива (Рисунок 37).

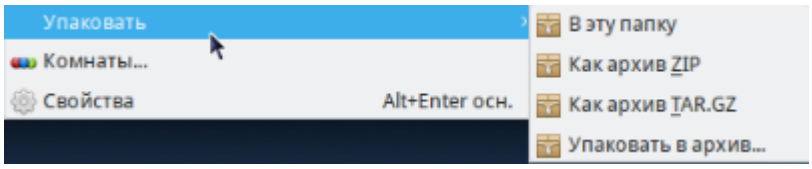


Рисунок 37

3.4.2. Thunderbird — почтовый клиент

Почтовый клиент Thunderbird предоставляет возможность работы с электронной почтой по протоколам POP3, IMAP4 и SMTP.

Далее рассмотрим процесс настройки и основные принципы работы приложения, полное руководство пользователя вы можете найти, перейдя во вкладку [Справка] → [Помощь по Thunderbird] или нажав клавишу [F1].

Настройка учетной записи

При первом запуске Thunderbird вызывается мастер создания учетной записи (Рисунок 38).

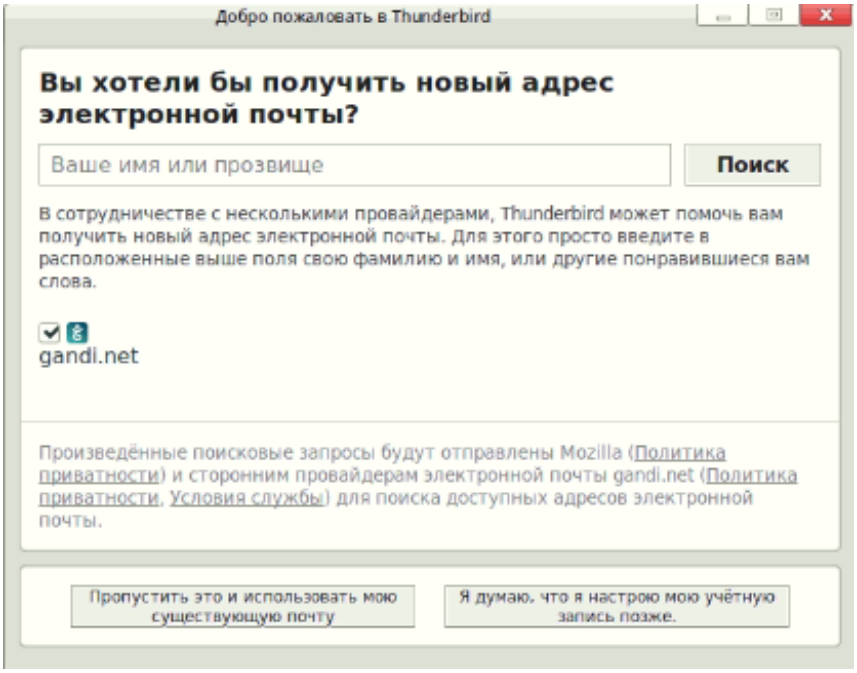


Рисунок 38

Заполнение поля [Ваше имя или прозвище] поможет вашим корреспондентам понять, от кого пришло письмо (Рисунок 39).

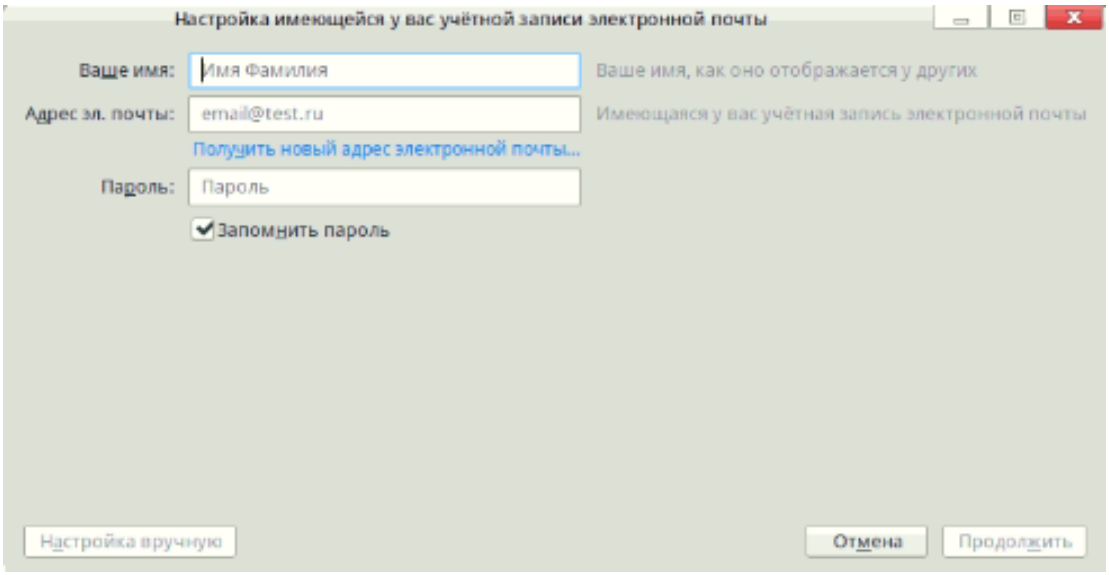


Рисунок 39

Если оставить это поле пустым, в качестве имени отправителя будет показан адрес e-mail. Обратите внимание, что адрес нужно указывать полностью, включая имя домена.

На следующем шаге необходимо подтвердить выбор протокола IMAP для работы с входящей почтой (при этом работа производится с папками на почтовом сервере) или выбрать протокол POP3, в этом случае почта сразу загружается на локальный ПК. После завершения указанных шагов ваша учетная запись будет готова к началу работы.

В дальнейшем на вкладке [Дом] (Рисунок 40) можно будет отредактировать существующую учетную запись или создать новую.

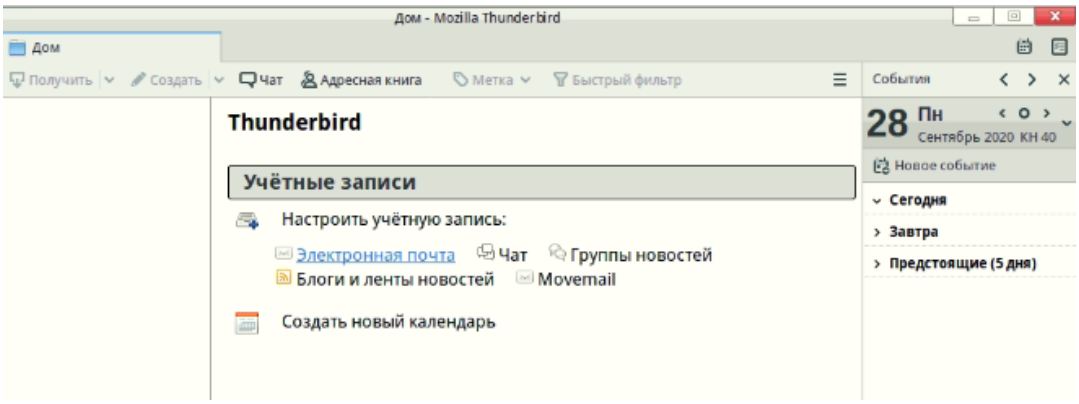


Рисунок 40

Интерфейс Thunderbird

Далее рассмотри интерфейс почтового клиента (Рисунок 41). На рисунке ниже представлена рабочая среда приложения.

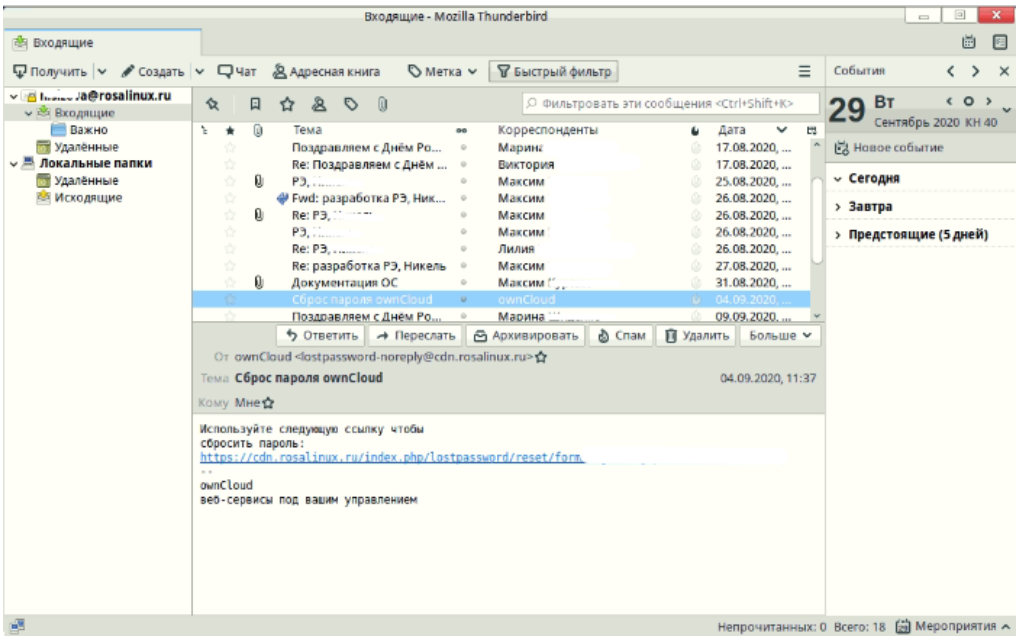


Рисунок 41

В верхней части окна, как обычно, находятся строка меню и инструментальная панель с кнопками для выполнения основных действий.

Вкладки

На открываемой по умолчании вкладке представлена папка «Входящие». Пока вы не начали работу, других вкладок нет. Они появятся при просмотре писем: если вы хотите просмотреть какое-либо сообщение, двойной щелчок по нему откроет его в новой вкладке. В разных вкладках одновременно можно открыть несколько разных писем.

Можно открыть на собственной вкладке и необходимую папку, щелкнув по ней правой кнопкой мыши и выбрав соответствующую команду контекстного меню. Работа со вкладками организована в Thunderbird аналогично работе со вкладками в интернет-браузерах.

Список папок

Список папок показан в левой части экрана. Это «дерево» (вы можете создавать иерархию вложенных папок), вершинами которого являются учетные записи e-mail (т. е. ваша почта на разных серверах), а также локальные папки, которые можно завести для хранения переписки на своем ПК. Черные треугольные стрелки над списком позволяют менять вид списка папок, показывая его более подробно или сжато.

Список сообщений

Список сообщений занимает центральную часть рабочей области. Это таблица, в каждой строке которой показана информация о конкретном сообщении, а столбцы отвечают его параметрам: дата получения, тема, отправитель и т. д. Какую информацию о письмах показывать и в каком порядке, можно выбрать по желанию. Щелкните по строке

заголовков правой кнопкой мыши и выберите нужные поля в контекстном меню.

Если, например, вы храните переписку в папках по определенным темам и переносите в тематические папки как полученные письма, так и свои ответы или первичные сообщения, удобно видеть в списке писем не только поле [От] (от кого письмо), но и поле [Адресат] (кому письмо).

Столбцы списка можно расположить в удобном для вас порядке, просто перетаскивая их мышью.

Список писем показывается с сортировкой по тому столбцу, в заголовке которого стоит голубая стрелочка-треугольник. Щелкнув мышью по заголовку столбца, вы отсортируете список по этому столбцу, повторный щелчок по заголовку поменяет порядок сортировки на обратный.

Обработка спама

Обычно почтовые службы имеют собственные системы распознавания спама, который помещается в соответствующую папку вашей учетной записи. Часто спам-фильтр можно подстроить вручную, сформулировав правила обработки писем, отсекающие нежелательные сообщения. Например, отправлять в папку «Спам» письма, в теме которых обнаружатся заданные слова (подстроки).

Mozilla Thunderbird также поддерживает и самообучающийся анализатор спама, явное составление правил фильтрования для которого не требуется. Для обучения антиспам-фильтра достаточно, увидев среди в папке [Входящие] нежелательное письмо, щелкнуть по нему правой кнопкой и выбрать в контекстном меню команду [Повторить перемещение в Спам]. Или, если письмо было открыто, просто щелкнуть по кнопке [Спам].

Пополнение адресной книги

Открыв письмо, обратите внимание на значок «контур звездочки» рядом с адресами отправителя и получателя (получателей). Щелкните по нему, и значок станет синим — это значит, что адрес был добавлен в вашу адресную книгу.

Если щелкнуть дважды, откроется окно правки контакта, в котором можно ввести реальное имя вашего корреспондента, по которому его легко будет потом найти. Когда имя задано, Thunderbird будет показывать его в полях [От] и [Кому] списка писем и самого письма вместо адреса e-mail (Рисунок 42).

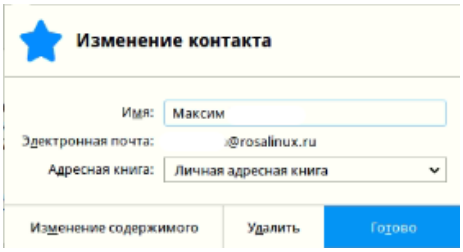


Рисунок 42

Создание сообщения

Если вы начинаете переписку, нажмите на кнопку [Создать]. Если отвечаете на полученное письмо — на кнопку [Ответить] или [Переслать], если требуется отправить письмо другому адресату. Как при пересылке, так и при ответе в создаваемое сообщение включается текст исходного. Также в открывшемся окне вы можете вручную удалить текст сообщений из истории переписки.

Получатели сообщения

При ответе на полученное письмо поле [Кому] (Рисунок 43) будет заполнено сразу же; при создании нового письма или пересылке адрес нужно ввести. Щелкните по следующей строке списка адресатов, и в ее начале появится кнопка [Кому]. Далее необходимо набрать в строке вручную адрес e-mail, или выбрать адрес из вашей адресной книги. Как только вы начнете набирать адрес (не важно — имя, фамилию получателя или часть его e-mail), адресная книга подскажет список подходящих вариантов, и останется только щелкнуть мышью по правильному.

При нажатии на кнопку [Кому] будет открыт список, содержащий еще два варианта отправки: [Копия] и [Скрытая копия]. Получатель копии получит точно такое же письмо и увидит адреса остальных получателей.

Скрытая копия означает, что ее получатель не увидит остальных, как будто письмо было адресовано исключительно ему.

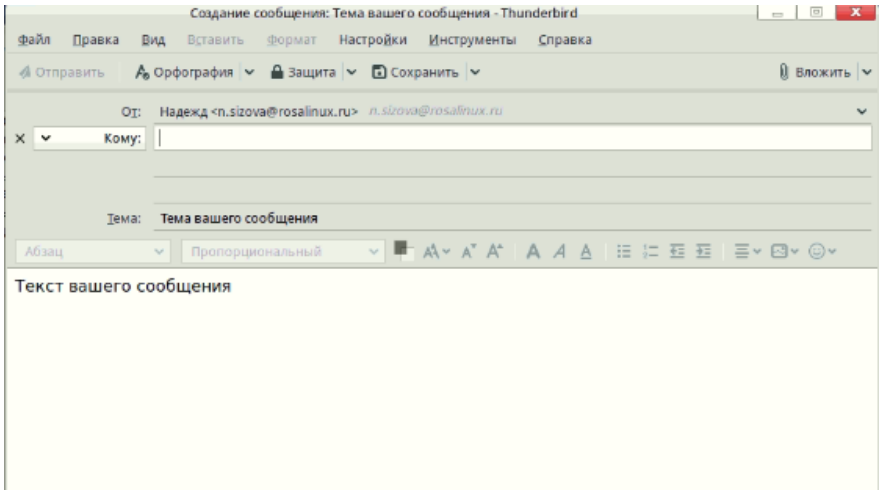


Рисунок 43

3.4.3. Chromium — интернет-браузер

Интернет-браузер Chromium предоставляет возможность просмотра и редактирования веб-страниц, созданных с использованием языков гипертекстовой разметки данных стандарта HTML 4.01, xHTML 1.0 (2 изд.), XML 1.0 (4 изд.), языка JavaScript и технологии CSS, CSS3 Selectors Test и Acid3. Chromium обеспечивает широкую поддержку SVG (уровень поддержки Advanced+), шрифтов SVG, анимации SVG SMIL, MathML, ECMAScript, DOM, обеспечивая поддержку около 95% существующих рекомендованных стандартов.

Для запуска Chromium, нажмите левой кнопкой мыши на иконку Chromium в левой части панели задач (Рисунок 44).

Далее рассмотрим несколько основных особенностей работы с Chromium. Полное руководство пользователя интернет-браузера Chromium можно найти, перейдя в меню браузера, нажав на кнопку ⋮ в правом верхнем углу окна браузера и перейдя во вкладку [О Chromium].

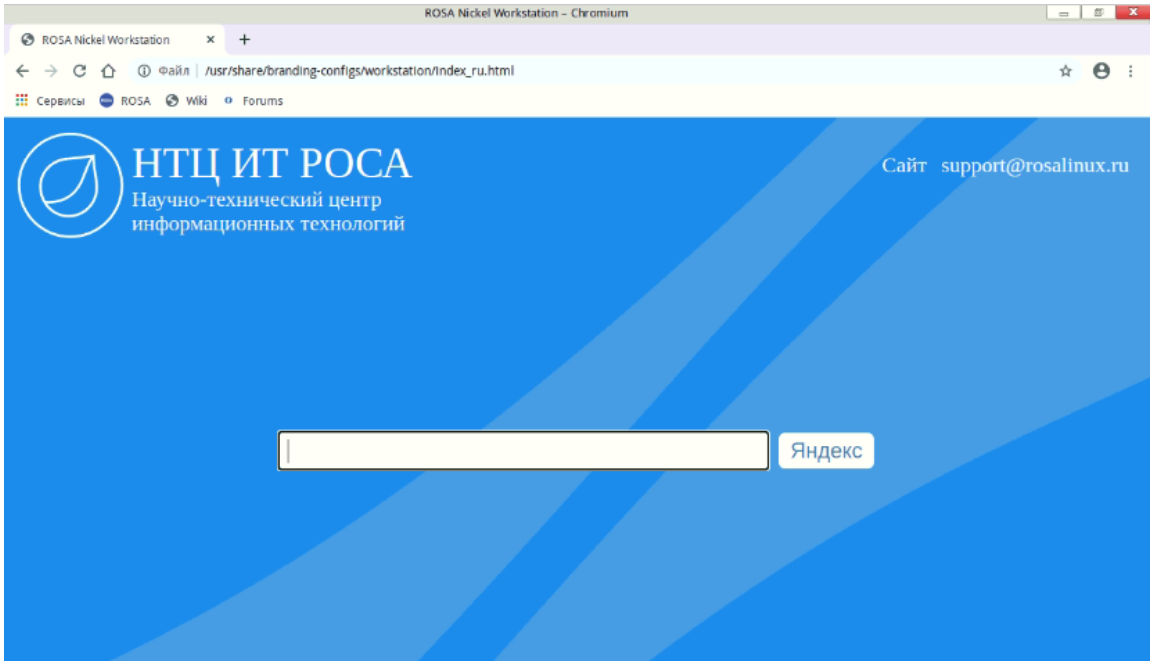


Рисунок 44

Основные элементы интерфейса:

– область просмотра страниц. Здесь отображается содержимое просматриваемых веб-страниц;

– кнопки навигации и адресная строка. Кнопки позволяют переходить вперед и назад по цепочке уже посещенных на этой вкладке страниц, обновлять, прекращать загрузку элементов, переходить на домашнюю страницу. В адресной строке вводится URL нужного сайта или локальной страницы;

Чтобы создать новую вкладку, наберите комбинацию клавиш <Ctrl+T> или нажмите на кнопку <+> справа от текущей вкладки (Рисунок 45).

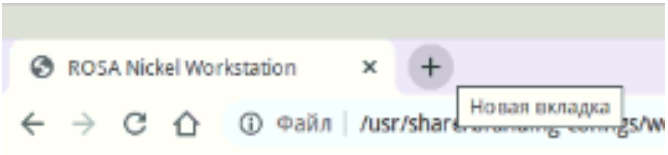


Рисунок 45

Чтобы закрыть вкладку, достаточно щелкнуть на ней правой кнопкой мыши и выбрать пункт [Закрыть вкладку]. Закрыть вкладку можно щелчком на крестике, расположенном в ее правом углу, нажатием клавиш <Ctrl+W>, а также щелчком колесика мыши по любой области вкладки.

Быстрое создание вкладок: нажмите <Ctrl+T> столько раз, сколько вкладок требуется. Нажатие <Ctrl+W> закрывает активную вкладку.

Управление вкладками

Можно закрыть, обновить, запомнить все вкладки «на лету», изменить только активную. Чтобы сделать это, следует щелкнуть на вкладке правой кнопкой мыши и выбрать нужный пункт в контекстном меню.

Вкладки также можно перемещать. Для этого нужно щелкнуть левой кнопкой на вкладке и, удерживая кнопку мыши нажатой, перетащить вкладку туда, куда нужно. Увидев характерный курсор в виде уголка и значка перемещения, можно поместить вкладку на новое место в панели вкладок.

Закладки

Для добавления текущей открытой страницы в закладки нажмите на нажмите на кнопку звездочки (Рисунок 46), находящуюся справа в адресной строке. После чего добавьте имя закладки, если необходимо и назначьте папку, в которой она будет храниться. Далее управление закладками осуществляется во вкладке [Закладки] основного меню браузера.

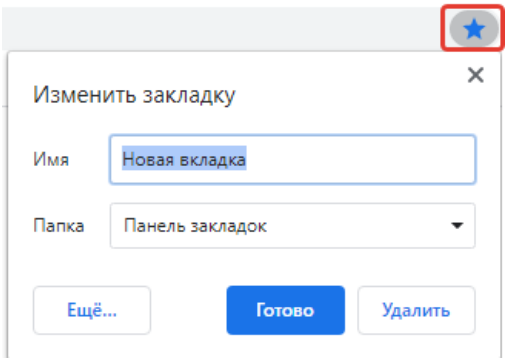


Рисунок 46

3.4.4. Audacious – аудиоплеер

Для воспроизведения аудиофайлов в форматах MP3, WAV, WMA, M4A, FLAC, AAC, ALC, OGG, Vorbis, FLAC, Monkey's Audio в ОС РОСА «НИКЕЛЬ» используется плеер Audacious. Аудиоплеер имеет широкий набор функциональных возможностей, который достигается благодаря набору встроенных плагинов. В этот набор входят плагины для воспроизведения форматов, и плагины для чтения форматов списков воспроизведения Cue, M3U, PLS.

Audacious предоставляет пользователю простой и удобный (Рисунок 47).

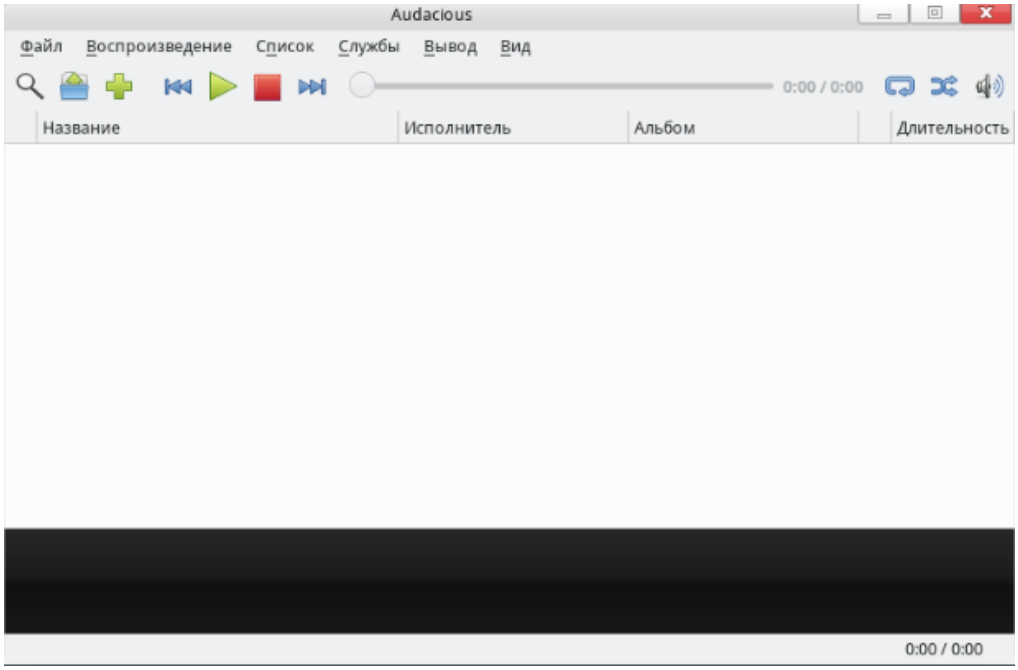


Рисунок 47

В верхней части экрана располагается панель меню программы.

Для настройки параметров приложения перейдите во вкладку [Файл] → [Настройки] (Рисунок 48).

В открывшимся окне доступна настройка внешнего вида приложения, звука, параметров сети, списков воспроизведения, информации о песнях, модулях программы (общие, эффекты, визуализация, ввод, список воспроизведения, транспорт).

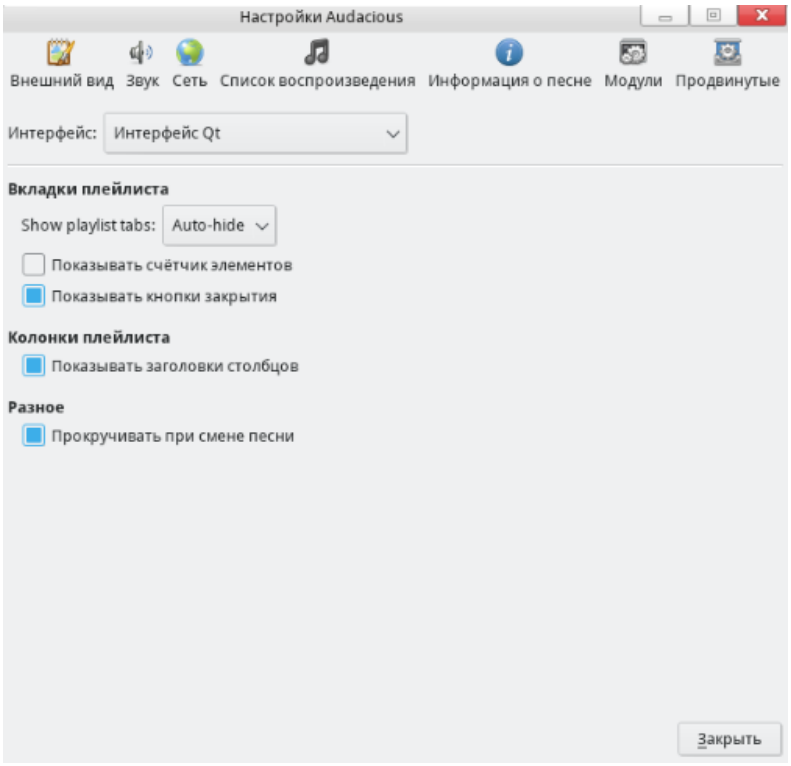


Рисунок 48

Для управления воспроизведением воспользуйтесь вкладкой [Воспроизведение] (Рисунок 49) или кнопками на панели инструментов.

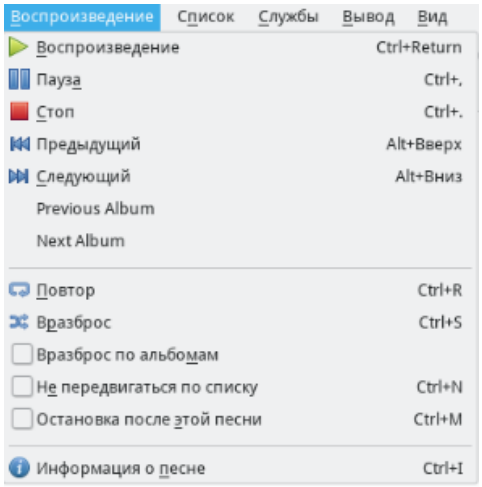


Рисунок 49

Для управления уровнем громкости перейдите во вкладку [Вывод] (Рисунок 50). Также данная вкладка используется для настроек звука и эффектов, и записи звука.

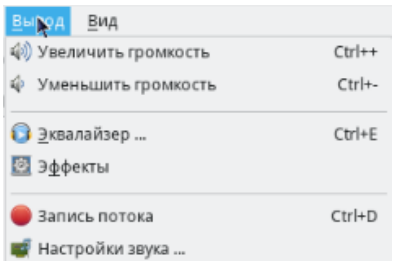


Рисунок 50

Для доступа к эквалайзеру и выполнения пользовательской настройки звука из панели меню перейдите во вкладку [Вывод] → [Эквалайзер] (Рисунок 51).

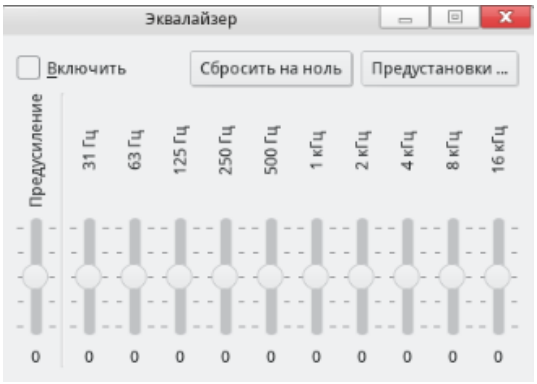


Рисунок 51

Под панелью меню находится панель инструментов (Рисунок 52).

Рисунок 52

Рассмотрим функциональные возможности панели инструментов:

1 – кнопка для поиска файлов в библиотеке;

2 – открытие нового файла (открывает новое окно с файловым менеджером);

3 – добавление нового файла в текущий плейлист;

4 – переход к воспроизведению предыдущей аудиодорожки;

5 – воспроизведение файла;

6 – остановка воспроизведения;

7 – переход к воспроизведению следующей аудиодорожки;

8 – шкала времени, отображающая воспроизведение аудиодорожки;

9 – повтор воспроизведения текущей аудиодорожки;

10 – воспроизведение плейлиста в разброс;

11 – уровень звука воспроизведения.

В центральной части рабочей области отображается выбранный плейлист (список добавленных файлов).

3.4.5. K3b — запись на оптические диски

Приложение предназначено для записи информации на оптические диски (CD, DVD). После запуска K3b необходимо выбрать одну из предлагаемых задач:

- новый проект с данными;
- новый проект AudioCD;
- копирование диска;

– больше действий.

Интерфейс приложения (Рисунок 53).

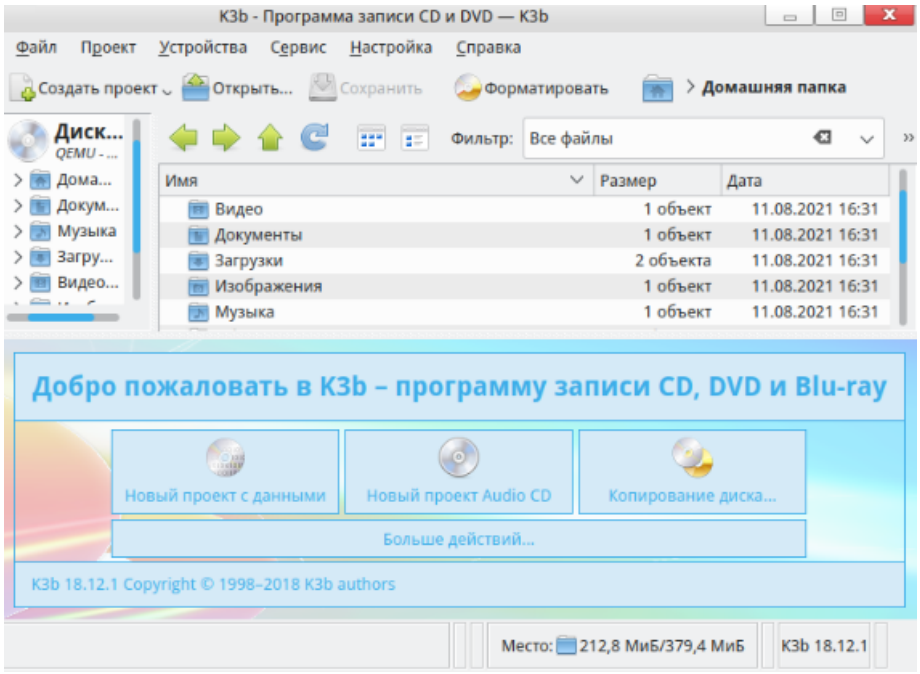


Рисунок 53

Запись диска с данными

После щелчка по кнопке [Новый проект с данными] рабочее окно K3b будет поделено на четыре зоны. Наверху, как и раньше, будут находиться панели обзора ФС. Под ними появятся панели проекта (Рисунок 54), на которые необходимо перетащить те каталоги или отдельные файлы, которые вы хотите записать на диск.

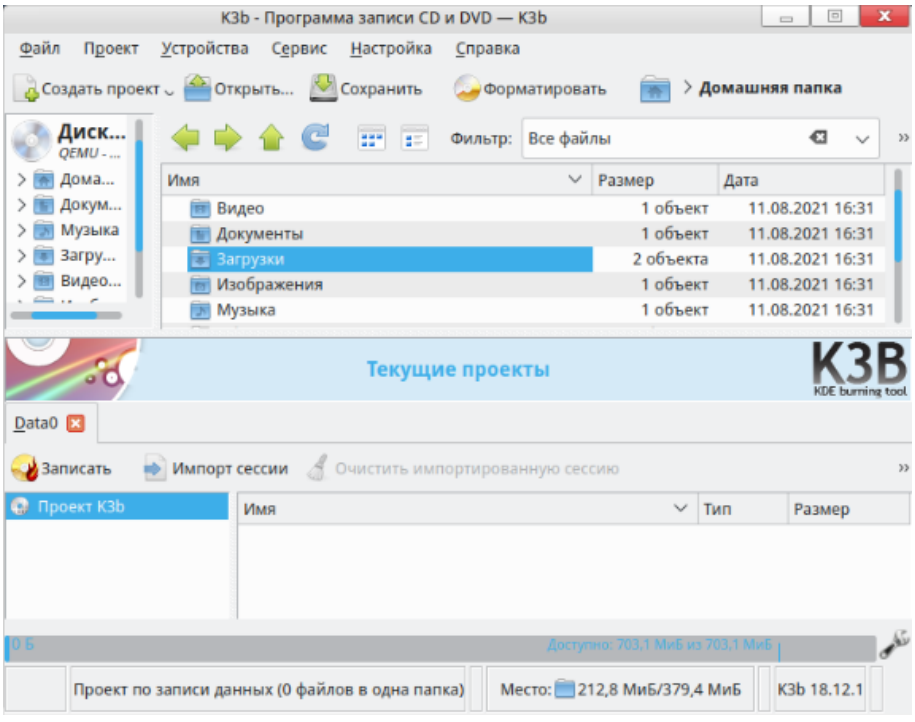


Рисунок 54

В файловом менеджере K3b отсутствуют внешние устройства, поэтому подключенный по USB внешний диск или любой другой внешний носитель информации окажется недоступен. Воспользуйтесь менеджером файлов Dolphin — из его окна вы сможете перетащить в K3b файлы с любого подключенного устройства. Пространство, занятое выбранными файлами и каталогами, будет показано на линейке в нижней части окна. Зеленый цвет означает, что емкость носителя достаточна; желтый — что размер проекта предельный и успешная запись всей информации не гарантируется; красный — что проект слишком велик, и его нужно сократить. При щелчке правой кнопкой мыши по файлу/каталогу в менеджере проектов откроется контекстное меню с командами для удаления и переименования файлов, создания новых (пустых) каталогов и т.д. Файлы и каталоги можно и перетаскивать, формируя таким образом структуру будущего диска.

При переименовании самого верхнего элемента дерева в левой части Менеджера проектов будет изменена и одноименная метка тома.

Щелкните по кнопке записи диска или выберите в меню пункт [Проект] → [Записать] (Рисунок 55). Будет открыто окно настройки параметров записи. Если требуется не записывать реальный диск, а создать его образ (т. е. файл специального формата ISO) для последующего копирования или размещения в сети, здесь можно выбрать соответствующую опцию. Для реальной записи укажите требуемое число копий и выберите в выпадающем меню скорость. При автоматическом выборе K3b выберет наибольшую возможную скорость для вашего пишущего привода диска и вставленного в данный момент записываемого носителя.

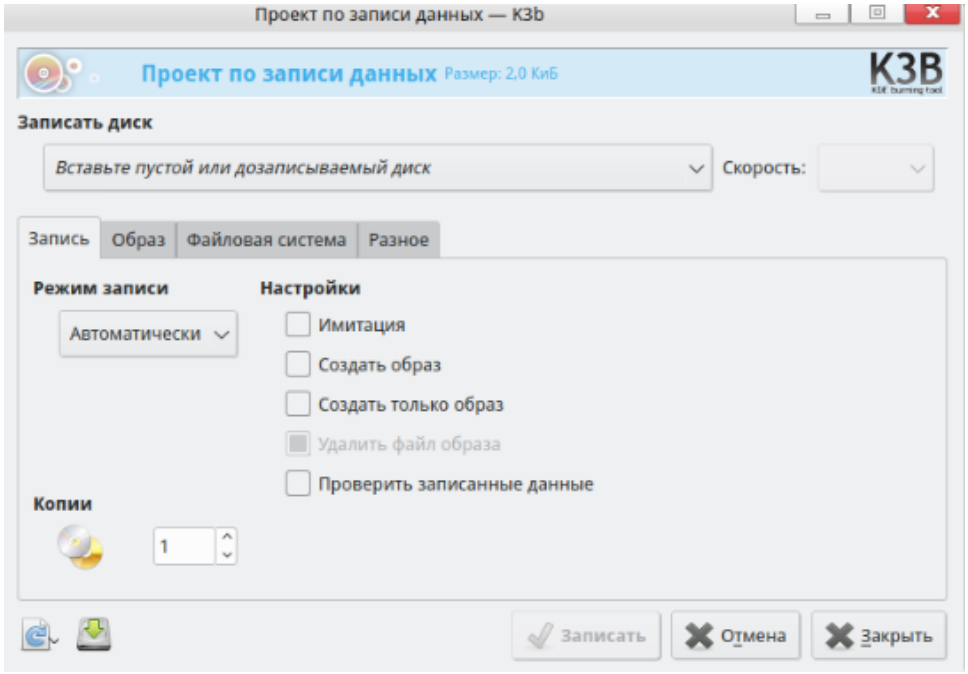


Рисунок 55

На вкладке [Разное] находится важная опция — установка режима сессий записи. Многосессионный режим дает возможность позже записать на оставшееся свободное место дополнительные файлы. Вариант [Нет многосессионной записи] означает, что после завершения записи диск будет финализирован. Дальнейшая запись на этот диск будет невозможна, даже если место на нем останется неиспользованным.

При записи только одной сессии с финализацией диск будет наиболее совместим с различными системами и устройствами воспроизведения, особенно если иметь в виду DVD- или CD-проигрыватели. Вполне возможно, что при попытке использовать на таком устройстве многосессионный диск окажутся доступны только файлы одной из сессий, или диск вообще не будет читаться. В случае прерывания подготовки диска или по окончании работы K3b предложит сохранить проект. Если запись прошла успешно, и вы знаете, что снова записывать такой же диск точно не придется, сохранять проект смысла нет.

Запись из образа ISO

Для записи диска из файла образа (например, загруженного из Интернета) нельзя действовать так же, как и с другими данными, т. е. открыть проект и перетащить в него ISO-файл. Вместо этого выберите в меню K3b команды [Сервис] → [Записать образ]. Будет открыто окно [Записать образ] (Рисунок 56), в котором вы сможете выбрать нужный файл образа и начать процесс записи.

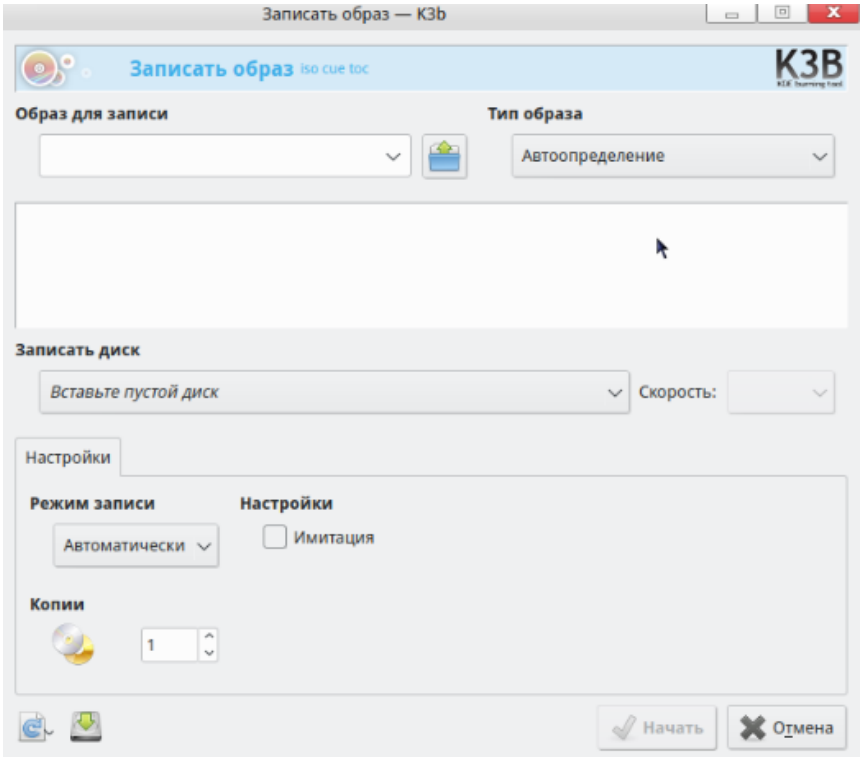


Рисунок 56

Запись Audio CD

Под Audio CD подразумеваются компакт-диски, которые можно воспроизводить с

помощью любого музыкального центра или плеера, в том числе старого, не умеющего работать с цифровыми форматами (MP3, OGG и пр.). Audio CD состоит из звуковых дорожек, которые могут быть созданы из файлов форматов Wave (*.wav), Ogg Vorbis (*.ogg) и MP3 (*.mp3). Дорожки могут быть также скопированы с другого компакт-диска (эту операцию называют ripping, она будет рассмотрена ниже). Как и при записи диска с данными, нужные файлы для записи перетаскиваются на панель текущего проекта (здесь она одна, так как дорожки идут просто друг за другом, а никаких каталогов на Audio CD быть не может). Вместо объема файлов и носителя показана длительность собранной программы, которая не должна превышать 80 минут.

Копирование диска

Если ваш ПК оснащен двумя приводами, один можно использовать для чтения исходного диска, а другой — для записи копии. Обычно оптический привод один, при этом K3b сначала запишет на жесткий диск образ исходного диска, а затем попросит сменить диск в приводе на чистую болванку и запишет копию.

В диалоге настройки копирования можно задать количество копий, выбрать место для записи образа и указать, удалять или нет этот образ по окончании копирования.

Многие DVD с защищенными авторским правом фильмами выпускаются с защитой от копирования. Такой диск K3b копировать с помощью приложения K3b невозможно.

Копирование музыки с Audio CD (ripping)

Чтобы переписать музыку с Audio CD на ПК, воспользуйтесь соответствующим пунктом меню [Сервис] (Рисунок 57). Также можно, вставив диск, дважды щелкнуть по значку привода в файловом менеджере K3b.

Диск будет прочитан и для извлечения будут помечены все дорожки (по умолчанию). Снимите отметки с дорожек, записывать которые не нужно, и нажмите на кнопку с ноткой, чтобы вызвать окно настроек риппинга.

Риппинг требует много места на диске. Запись производится без сжатия, а каждая минута несжатого звука CD-качества занимает на диске более 10 МБ (видео — на порядок больше). Полученные аудиофайлы можно затем перекодировать с помощью Clementine, уменьшив их размеры во много раз.

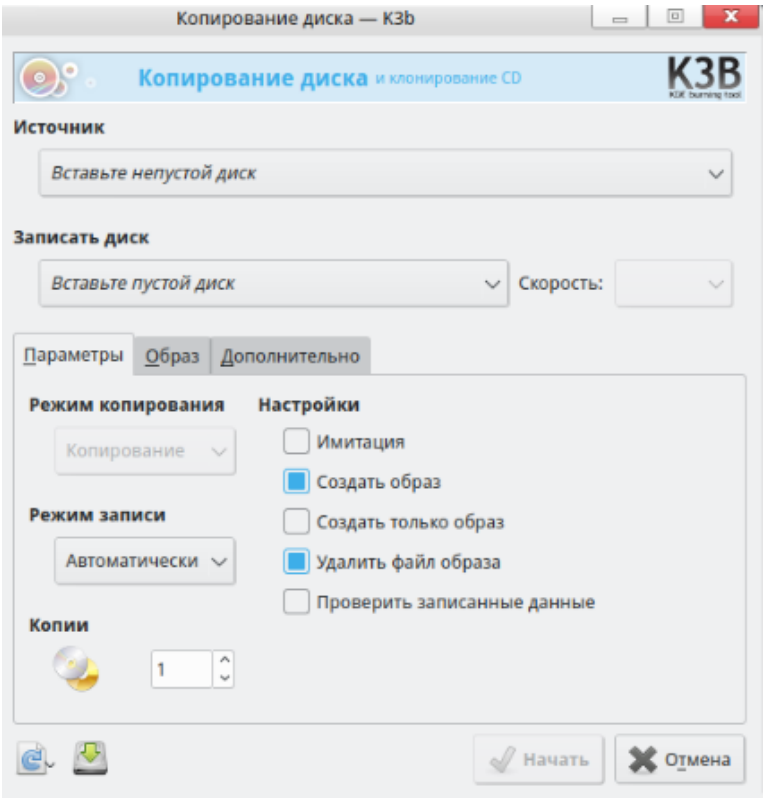


Рисунок 57

С дисков можно переписывать не только музыку, но и видео (DVD, VCD). Доступ к соответствующим операциям дает меню «Сервис».

3.4.6. Gwenview — работа с фотографиями

Для организации работы с изображениями в ОС РОСА «НИКЕЛЬ» предустановлено приложение Gwenview. Программа предоставляет следующие возможности:

- просмотр изображений в форматах BMP, TIFF, TGA, PNG, JPG, JPEG;
- просмотр содержимого каталогов;
- редактор метаданных изображений;
- представление каталогов в виде списка мини-изображений;
- использование плагинов KIPI (KDE Image Plugins Interface) для работы с изображениями;
- разные режимы просмотра изображений;
- возможность вызова внешних программ.

Далее рассмотри основные принципы работы приложения.

Стартовый экран приложения (Рисунок 58) представляет собой файловый менеджер позволяющий открыть необходимые файлы с ПК и открытие последних файлов.

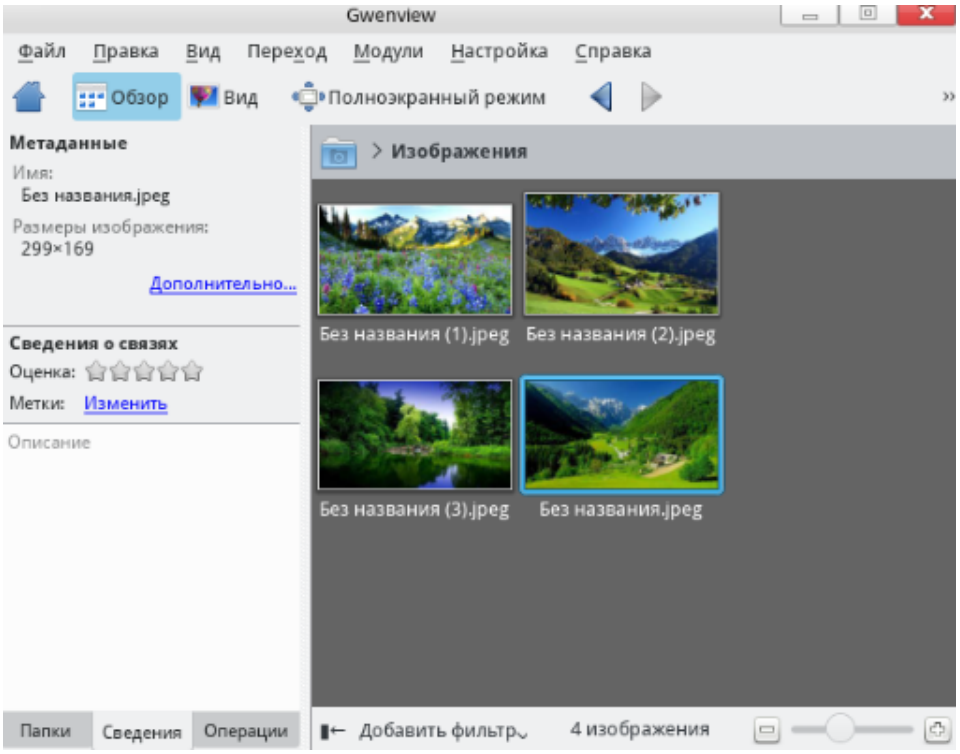


Рисунок 58

Операции с изображениями

Для просмотра содержимого выбранного каталога Gwenview предоставляет несколько вариантов отображения файлов: Обзор, Вид и Полноэкранный режим.

Для просмотра изображений также доступен режим слайд-шоу, для этого перейдите во вкладку [Вид] → [Запустить слайд-шоу].

Программа также может выполнять следующие базовые манипуляции с изображениями:

– Поворот (влево или вправо) на 90 градусов. Для этого перейдите из панели меню во вкладку [Правка] → [Поворот вправо] (или воспользуйтесь сочетанием клавиш Ctrl + R) или [Правка] → [Поворот влево] <Ctrl + L>.

– Зеркальное отражение изображения по вертикальной оси. Для этого перейдите во вкладку [Правка] → [Зеркало].

– Отражение изображения по горизонтальной оси. Для этого перейдите из меню [Правка] → [Отразить].

– Уменьшение или увеличение изображения. Для этого перейдите во вкладку [Правка] → [Изменить размер] <Shift + R>.

– Обрезка изображения. При необходимости обрезки лишних частей изображения из панели меню перейдите во вкладку [Правка] → [Обрезать] <Shift + C>. Также можно настроить дополнительные параметры, перейдя в раздел Расширенные настройки в нижней всплывающей панели.

– Устранение эффекта красных глаз на фотографиях. Для проведения этой операции перейдите во вкладку [Правка] → [Уменьшение эффекта красных глаз].

– Изменение масштаба изображений, для этого перейдите во вкладку [Вид] → [Фактический размер/ Масштабировать по размеру/ Увеличить/ Уменьшить].

– Печать изображений, для того чтобы выполнить печать необходимо перейти во вкладку [Файл] → [Печать] <Ctrl + P>.

Для получения более подробной информации по использованию приложения перейдите во вкладку [Справка].

3.4.7. Rosa Media Player — видеопроигрыватель

Встроенным видеопроигрывателем в ОС РОСА «НИКЕЛЬ» является Rosa Media Player. Функциональные возможности проигрывателя позволяют воспроизводить следующие форматы видео файлов: MKV, MPEG-1/2 (ES/PS/PES/VOB), AVI, ASF/WMV/WMA, QT/MOV/MP4, RealAudio/RealVideo, Ogg/OGM files, Matroska, NSV (Nullsoft Streaming Video), VIVO, FLI.

Rosa Media Player предоставляет пользователю простой в использовании интерфейс (Рисунок 59).

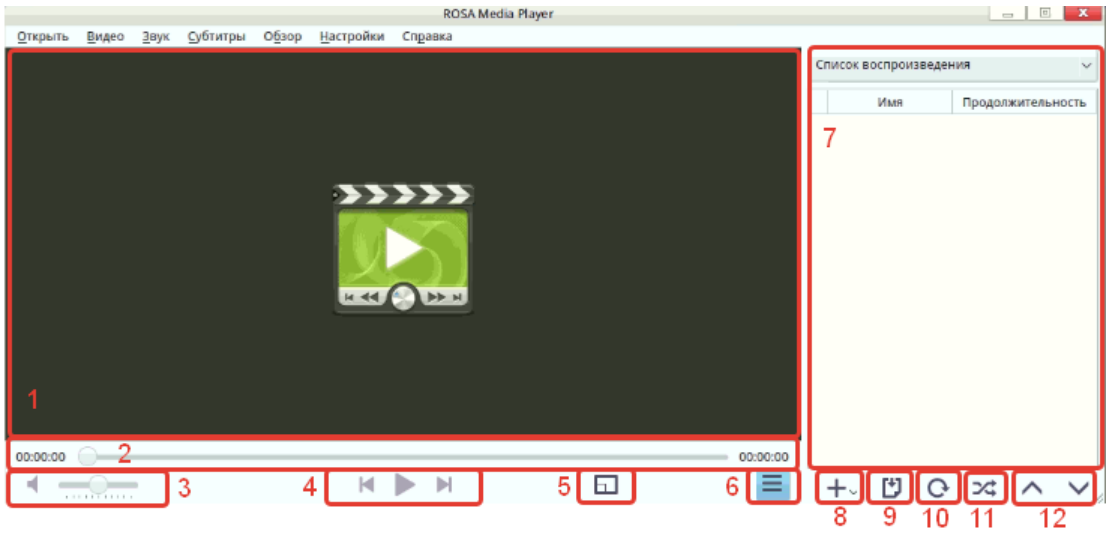


Рисунок 59

Рассмотрим рабочую область Rosa Media Player подробнее:

1 – область воспроизведения видео файла;

2 – шкала времени воспроизведения файла;

3 – шкала звука;

4 – кнопки управления воспроизведением (предыдущий файл/ воспроизведение (пауза)/ следующий файл);

5 – переход в полноэкранный режим;

6 – отобразить/скрыть список воспроизведения;

7 – список воспроизводимых файлов;

8 – добавить файл к текущему списку воспроизведения;

9 – сохранить плейлист;

10 – повторить воспроизведение текущего файла;

10 – перемешать файлы из списка воспроизведения;

11 – переход к предыдущему/ следующему файлу.

Также с помощью Rosa Media Player можно обрезать видео и извлечь аудиодорожку из видео файла. Для доступа к данным функциям нажмите на раскрывающееся меню над списком воспроизведения.

При выборе параметра [Обрезать видео] в открывшемся окне (Рисунок 60) необходимо указать временной интервал для выполнения действия.

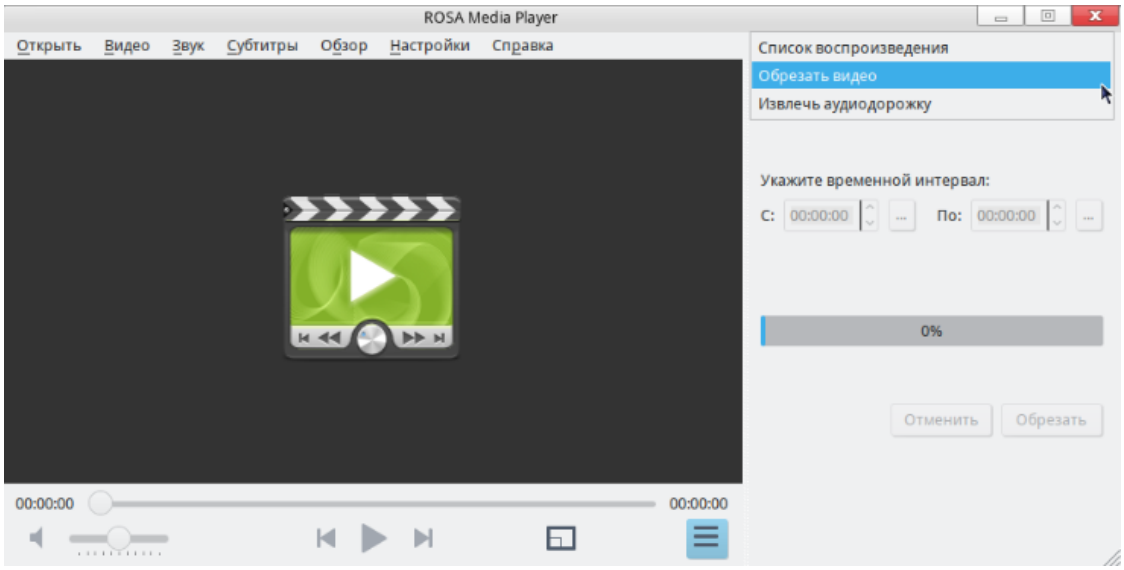


Рисунок 60

При необходимости извлечения аудиодорожки из файла выберете желаемый формат итогового файла (mp3/ogg) (Рисунок 61).

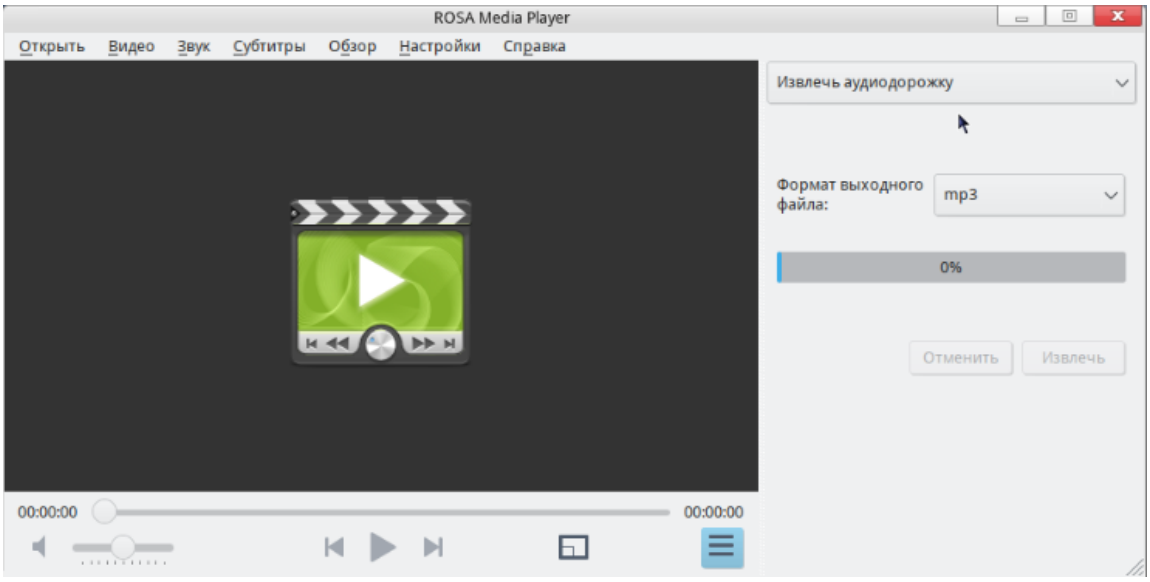


Рисунок 61

Rosa Media Player предоставляет разные возможности по настройке параметров видео, которые представлены во вкладке [Видео] на панели меню (Рисунок 62).

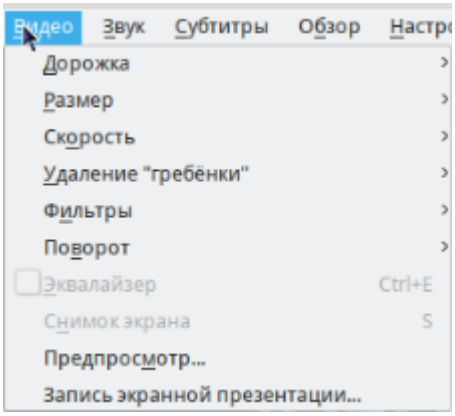


Рисунок 62

Параметры вкладки позволяют регулировать размер (масштаб) отображения видео в области воспроизведения, скорость воспроизведения, выбрать опцию для удаления эффекта «гребенки» в видеофайле, наложить фильтр на видео (постобработка, «смазывание» границ квадратов, удаление краевых эффектов, а также несколько режимов борьбы с шумами), повернуть видео, открыть эквалайзер, сделать снимок экрана или произвести запись экрана.

Для настройки параметров звука воспользуйтесь вкладкой [Звук], где возможно установить задержку на воспроизведение аудиодорожки, открыть эквалайзер или установить эффекты для аудиодорожек.

3.4.8. Офисный пакет LibreOffice

LibreOffice — офисный пакет, включающий в себя все необходимые компоненты для организации работы с документами и файлами любой сложности (Рисунок 63).

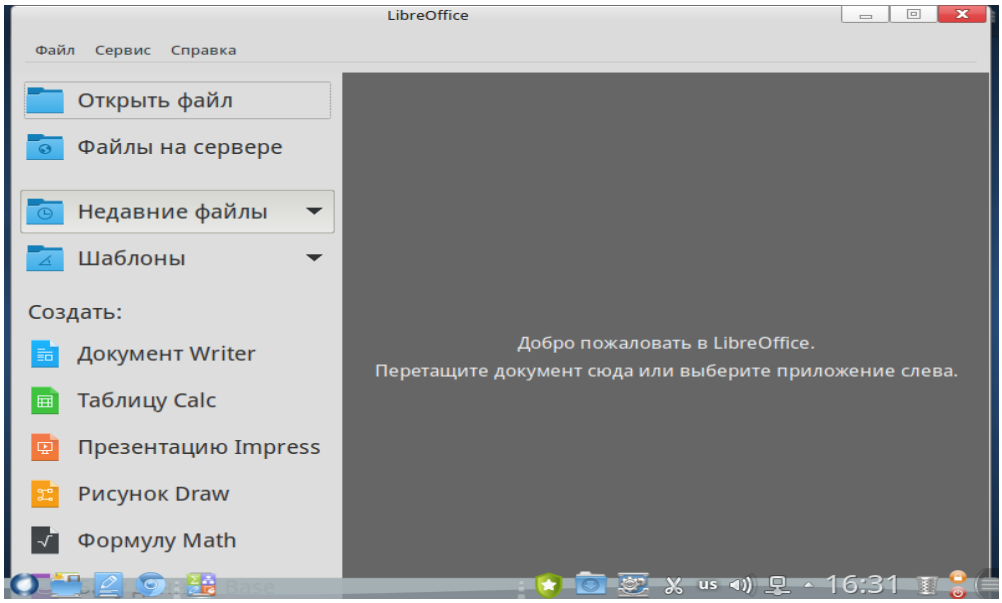


Рисунок 63

Компоненты офисного пакета предоставляют пользователю следующие возможности:

Текстовый процессор обеспечивает:

– работу с текстовыми документами формата ODT (Open Document Format);

– работу с текстовыми документами формата DOC, DOCX, TXT, RTF;

– работу полнотекстового поиска;

– экспорт документов в формат HTML и формат переносимого документа PDF;

– возможность вставки и редактирования таблиц и диаграмм;

– возможность вставки изображений из файлов формата PNG, JPEG;

– возможность изменения размера шрифта произвольно выделенного фрагмента текста, цвета произвольно выделенного фрагмента текста;

– возможность выравнивания текста по левому краю, по правому краю, по ширине, по центру;

– возможность редактирования математических формул.

Приложение для работы с электронными таблицами обеспечивает:

– редактирование таблиц формата CSV, ODS (Open Document Format);

– работу с электронными таблицами формата XLS, XLSX;

– работу полнотекстового поиска;

– экспорт документов в формат HTML, CSV и формат переносимого документа PDF;

– вставку диаграмм на основе таблиц;

– возможность вставки изображений из файлов формата PNG, JPG;

– возможность изменения размера шрифта произвольно выделенного фрагмента;

– текста, цвета произвольно выделенного фрагмента текста;

– возможность выравнивания текста в ячейке по левому краю, по правому краю, по ширине, по центру;

– выполнение математических операций в ячейках таблицы;

– возможность изменения габаритов столбцов, строк и ячеек таблицы;

– возможность изменения размера и цвета шрифта для ячейки таблицы.

Средства для работы с презентациями обеспечивает:

– редактирование презентаций формата ODP (Open Document Format);

– работу с презентациями формата PPT, PPTX;

– работу полнотекстового поиска;

– возможность создания и упорядочивания слайдов презентации;

– изменение стиля и фона презентации;

– макеты для создания типовых слайдов;

– просмотр структуры презентации;

– показ слайдов (презентации) в полноэкранном режиме;

– рисование и редактирование векторных примитивов: линий, стрелок, прямоугольников, эллипсов, кривых, замкнутых и др. фигур;

– вращение и масштабирование графических фигур;

– изменение толщины линии и цвета заливки графических фигур;

– изменение стиля линии и стиля стрелок для линии;

– возможность заливки фигуры текстурой или градиентом;

– вставку и редактирование таблиц;

– вставку текста с возможностью изменения начертания шрифта, размера и цвета текста;

– вставку текста с возможностью выравнивания текста по левому краю, по правому краю, по ширине, по центру;

– возможность вставки растровых изображений из файлов формата PNG, JPG;

– экспорт документов в формат переносимого документа PDF.

С подробным руководством пользователя можно ознакомиться, нажав клавишу F1 в открытом окне компонента приложения, после чего откроется раздел [Справка LibreOffice].

Далее кратко рассмотрим основные возможности каждого из компонентов

LibreOffice.

Writer

Текстовый процессор Writer содержит все необходимые функции современного полнофункционального редактора, а также инструмента публикаций. Он достаточно прост для создания быстрых заметок, достаточно мощный, чтобы создавать сложные документы с содержанием, диаграммами, индексами, примечаниями нескольких авторов и т.д.

Встроенные «мастера» автоматизируют процесс создания стандартных документов, таких как письма, факсы, повестки дня, протоколы, а также могут выполнить более сложные задачи, например, создавать множества документов из одного шаблона и источника данных для рассылки разным адресатам.

Writer может отображать во время редактирования одновременно несколько страниц, тем самым он идеально подходит для сложных документов и больших мониторов (или мультимониторных систем).

Документы Write поддерживают открытие и сохранение документов для Microsoft Word и MacOS X.

Calc

Calc - компонент для работы с электронными таблицами. При работе с приложением в электронную таблицу можно вводить данные (обычно числа) и манипулировать этими данными для получения определенного результата.

Кроме того, можно ввести данные, а затем изменить только некоторые из этих данных и наблюдать результат без необходимости полного повторного ввода таблиц или листа.

Другие возможности, представленные в Calc, включают в себя:

– Функции, которые могут быть использованы при создании формул, для выполнения сложных вычислений на основе данных.

– Функции баз данных, чтобы организовывать, хранить и фильтровать данные.

– Динамические диаграммы; широкий спектр 2D и 3D диаграмм.

– Макросы для записи и исполнения повторяющихся задач. В компонент включена поддержка для языков программирования Basic, Python, BeanShell и JavaScript.

– Возможность открывать, редактировать и сохранять файлы в формате Microsoft Excel.

– Импорт и экспорт электронных таблиц во множество форматов, включая HTML, CSV, PDF и PostScript.

Impress

Impress - программа для создания, редактирования и просмотра презентаций.

С помощью Impress презентации могут быть дополнены 2D и 3D клипартами, спецэффектами, сменой стиля, анимацией и высококачественными инструментами рисования.

В приложении имеется широкий выбор шаблонов для создания презентаций.

В рабочей области программы доступны различные режимы просмотра работы, для соответствия вашей текущей задаче:

- Normal (для общего редактирования);
- Outline (для организации и изложения содержания текста в общих чертах);
- Notes (для просмотра и редактирования примечаний к слайду);
- Handout (для представления бумажных материалов);
- Slide Sorter (для просмотра миниатюрных эскизов листа, что позволяет быстро находить и упорядочивать ваши слайды).

Impress имеет широкий ассортимент легких в использовании инструментов по созданию чертежей и диаграмм для добавления в презентацию.

Вы можете настроить ваше рабочее пространство таким образом, чтобы иметь мгновенный доступ к часто используемым инструментам рисования, и воспользоваться блоком «Стили и форматирование» чтобы применять графические стили одним кликом.

Вы можете открыть файлы Microsoft PowerPoint, а также сохранить свою работу в этом формате для тех пользователей, которые пользуются продуктами Microsoft. Кроме того, в приложении есть встроенный экспортер для создания Flash (.swf) версий ваших презентаций.

Draw

Draw - векторный графический редактор, который также может выполнять некоторые операции и с растровой графикой, используя Draw, можно быстро создавать большое разнообразие графических изображений.

Векторная графика хранит и отображает изображения в виде простых геометрических элементов, таких как линии, окружности и многоугольники, а не как наборы пикселей (точек на экране), как растровая.

Функциональность LibreOffice Draw обладает более обширной функциональностью, чем инструменты рисования, интегрированные в большинство иных офисных пакетов. В приложении доступны такие функции как: управление слоями, система привязок, отображение размеров, соединители для создания диаграмм, 3D функции, которые позволяют создавать небольшие трехмерные рисунки (с текстурированием и световыми эффектами), рисование и интеграция в стиль страницы,

кривые Безье.

Math

Модуль Math предназначен для написания математических и химических формул. Math обычно используется как редактор формул для текстовых документов, но также может быть использован в других типах документов (презентациях, таблицах, рисунках) или автономно. При использовании внутри Writer, формула обрабатывается как объект в текстовом документе.

Math используется для записи формул в символическом виде, и не предназначен для расчетов. Для расчета числовых значений используйте модуль Calc.

3.4.9. Okular

Okular (Рисунок 64) - универсальное приложение для просмотра документов формата PDF из окружения рабочего стола KDE.

Кроме возможности просматривать PDF-файлы в Okular есть и дополнительные функции. Функция заметок Okular позволяет добавлять комментарии в PDF-документы, подсвечивать текст и рисовать линии, геометрические фигуры, добавлять надписи и штампы. Заметки могут храниться отдельно от неизмененного PDF-файла либо могут быть сохранены в документ как стандартные PDF-заметки.

Текст может быть извлечен в текстовый файл. Возможно выделить часть документа и скопировать текст или изображения в буфер обмена.

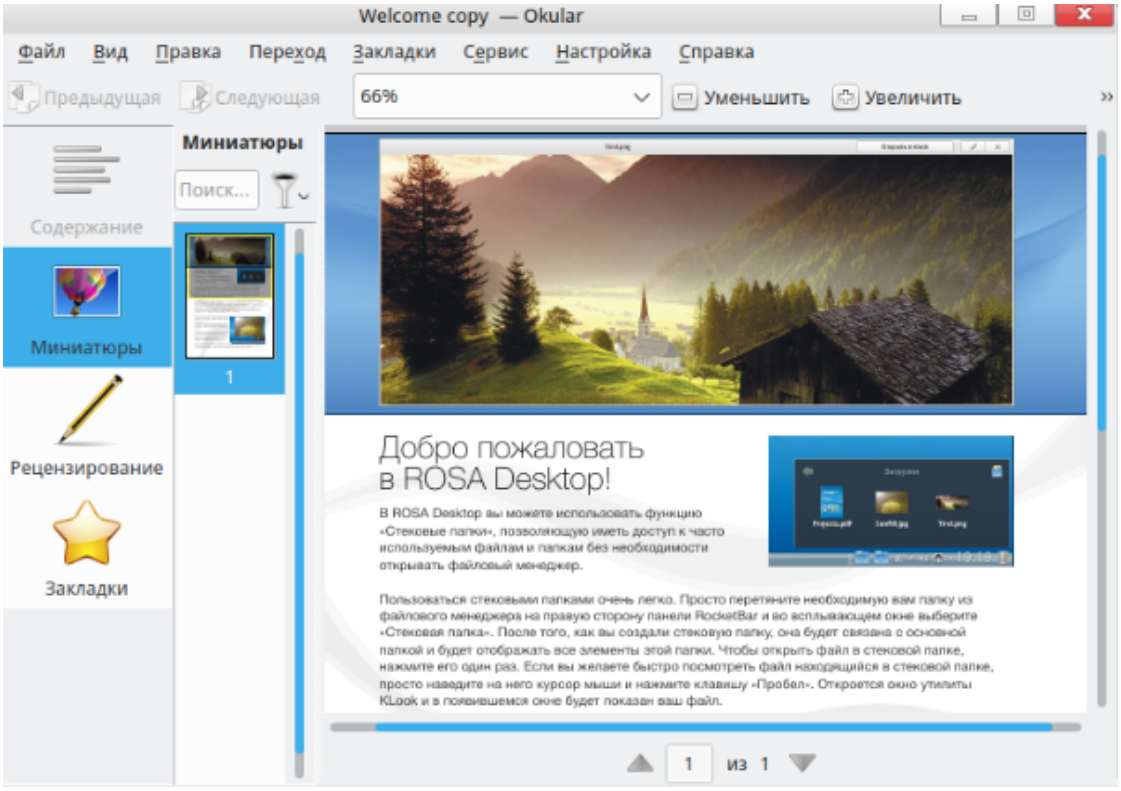


Рисунок 64

Рассмотрим основные функциональные возможности Okular, полное руководство пользователя доступно при переходе во вкладку [Справка] → [Руководство пользователя Okular] <F1> из панели меню.

Для того что бы открыть файл воспользуйтесь вкладкой [Файл] → [Открыть] <Ctrl+O> или [Последние файлы] для доступа к последним открытым файлам в программе.

Для того чтобы сохранить текущий файл перейдите во вкладку [Файл] → [Сохранить] <Ctrl+S> или [Сохранить как] <Ctrl+Shift+S>, для того чтобы сохранить документ в новом файле с новым именем.

Для печати текущего документа перейдете во вкладку [Файл] → [Печать] <Ctrl+P> или [Предварительный просмотр], для демонстрации печати текущей версии документа с настройками печати по умолчанию.

Для просмотра параметров файла перейдите во вкладку [Файл] → [Свойства], после чего откроется новое окно с информацией о файле.

Для некоторых фалов программа предоставляет возможность экспорта файла в текстовый форма, для этого перейдите во вкладку [Файл] → [Экспорт в…].

Приложение Okular предоставляет возможность просматривать файл в полноэкранном режиме или в режиме презентации, для изменения типа отображения файла перейдите во вкладку [Вид] и выберете соответствующий параметр. Также во вкладке [Вид] представлены инструменты по настройке масштабирования отображаемого документа.

Для навигации по страницам текущего файла воспользуйтесь вкладкой [Переход], которая предоставляет возможность перемещения к следующей/предыдущей странице, в начало/конец документа, перейти к конкретной странице.

Для удобства работы с документом имеется возможность добавления закладок в документ, для этого перейдите во вкладку [Закладки] → [Добавить закладку] <Ctrl+B>.

3.4.10. Управление разделами KDE

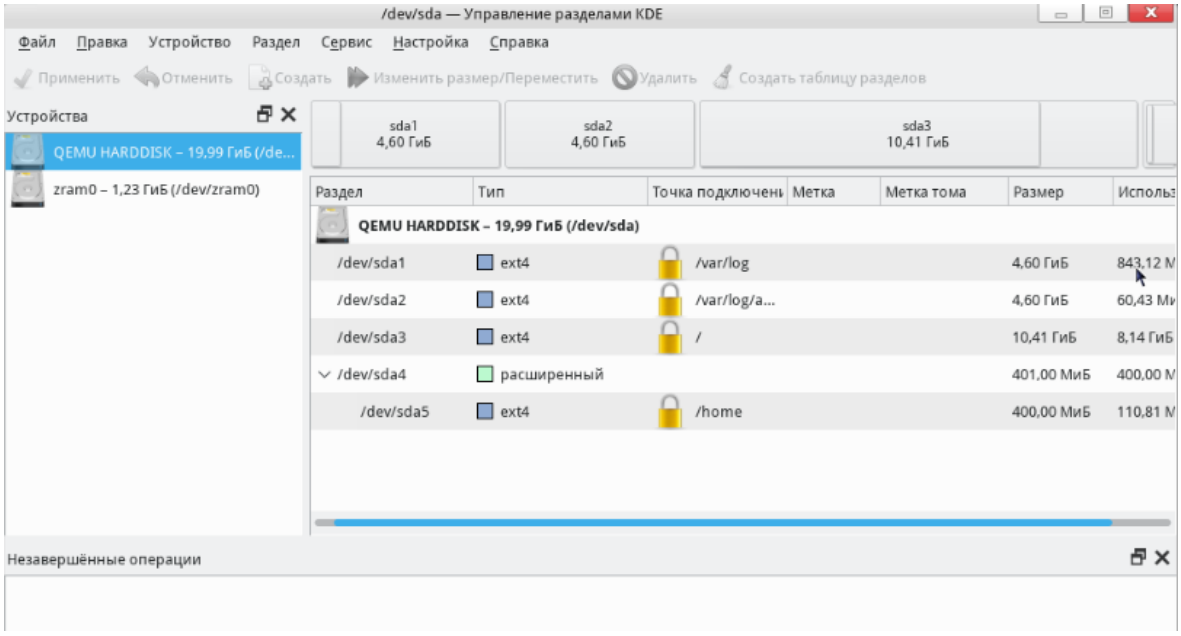


Рисунок 65

Утилита Управление разделами KDE (Рисунок 65) дает возможность пользователю с правами администратора управления дисковыми разделами и носителями данных в графическом режиме. ПО имеет простой и понятный интерфейс, что позволяет работать с ней пользователю любого уровня подготовки. С помощью утилиты можно разбить пространство жесткого диска ПК на несколько отдельных разделов, на усмотрение пользователя.

Для получения подробной информации о диске, выполните двойное нажатие левой кнопкой мыши по необходимому диску, после чего откроется новое окно с со свойствами выбранного раздела. В открывшимся окне доступна информация о ФС раздела, имеющихся метках, типе и состоянии раздела, размере и доступном объеме хранилища и прочие параметры (Рисунок 66).

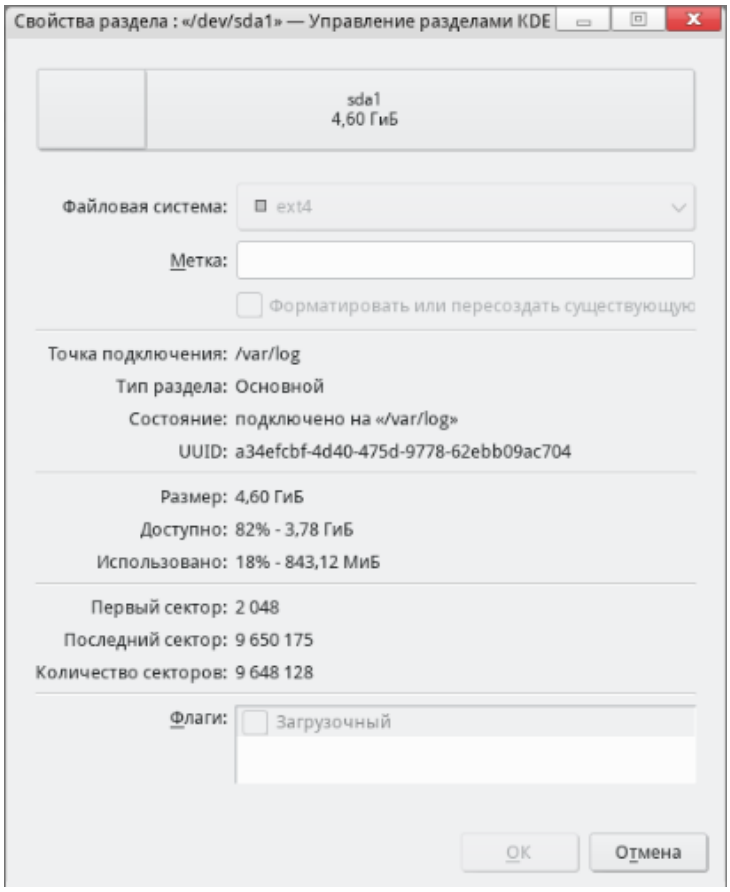


Рисунок 66

Создать новый раздел

Для создания нового раздела воспользуйтесь кнопкой [Создать] на панели инструментов или перейдите из панели меню [Разделы] - [Создать]. В открывшемся окне установите величину, для первоначального, расширенного или логического раздела, и ФС. Если допущена ошибка, можно удалить раздел, или, если еще не нажата кнопка [Применить все операции], можно использовать [Отменить последнюю операцию].

Изменить размер или переместить раздел

Если вы хотите изменить размер или сдвинуть выбранный раздел, нажмите на кнопку [Изменить или переместить] на панели инструментов (выделив необходимый раздел нажатием левой кнопкой мыши), после чего появляется новое окно (Рисунок 67). В открывшимся окне введите необходимые параметры.

После того, как все правильно установлено, нажмите [Применить все операции], только тогда запланированные изменения будут применены.

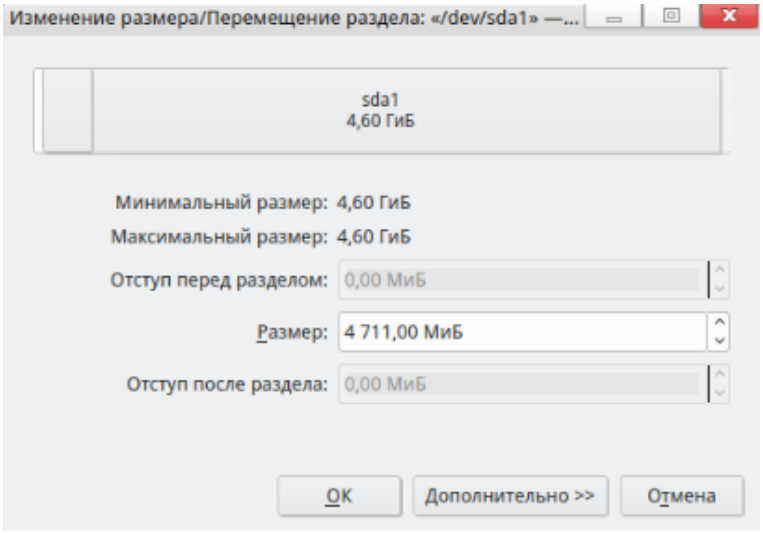


Рисунок 67

3.4.11. Калькулятор KCalc

KCalc - это свободная программа-калькулятор для арифметических расчетов, входящая в проект KDE.

В калькуляторе KCalc кроме стандартных математических операций присутствуют дополнительные функции, такие как:

– Тригонометрические функции, логические операции и статистические расчеты;

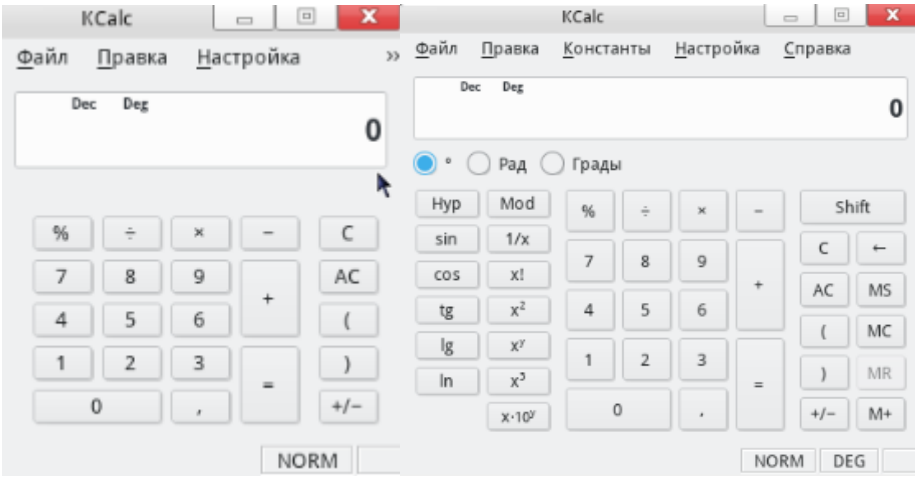
– Стек результатов, который позволяет легко получать доступ к предыдущим результатам;

– Задаваемая пользователем точность вычислений;

– Копирование и вставка чисел;

– Настраиваемые цвета и шрифты;

– Поддержка сочетаний клавиш для облечения работы без использования мыши.



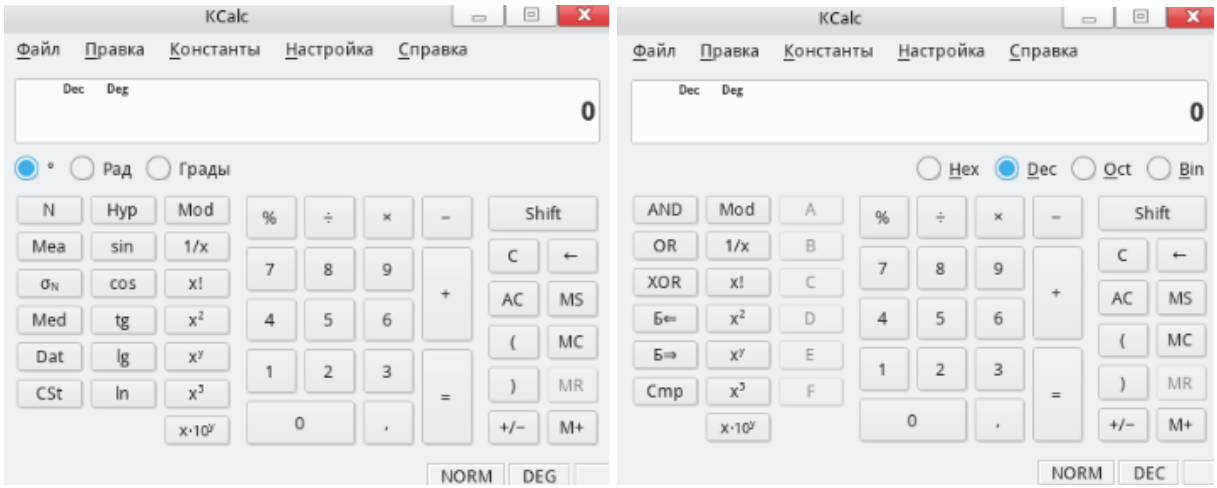


Рисунок 68

В приложении доступны 4 режима работы калькулятора: простой, инженерный, статистический и режим систем счисления (Рисунок 68).

3.4.12. Другие предустановленные пакеты

Сборка Wildfly 10.1

В серверную часть ОС включена сборка пакетов WildFly (JBoss Application Server) – сервер приложений Java EE, полностью разработанный на Java.

Для активации модуля и проверки его статуса воспользуйтесь командами в консоли (с командой sudo -i):

```
systemctl start wildfly
systemctl status wildfly
```

После чего выведется сообщение о том, что сервис активирован:

```
Active: active(running)
```

Сборка MQTT (Mosquitto)

Протокол передачи сообщений MQTT (Message Queue Telemetry Transport) – это легкий, компактный и открытый протокол обмена данными, созданный для передачи данных на удаленных локациях, где требуется небольшой размер кода и есть ограничения по пропускной способности канала.

Для активации и проверки статуса сервиса пакетов перейдите в консоль и воспользуйтесь следующими командами (с командой sudo -i):

```
systemctl start mosquitto.service
systemctl status mosquitto.service
```

После чего на экране высветится о том что сервис активирован:

```
Active: active (running)
```

Для реализации процесса пересылки сообщений, следуйте следующей

инструкции:

1. Откройте первую консоль, запустите клиент подписки сообщений, например на топик "test/topic" и порт 1883:

```
mosquitto_sub -p 1883 -t 'test/topic' -v
```

2. Откройте вторую консоль, опубликуйте сообщение в этот топик:

```
mosquitto_pub -p 1883 -t 'test/topic' -m 'test send message'
```

3. После чего в первой консоли должно отобразиться сообщение 'test send message'.

MongoDB

В серверную часть сборки ОС РОСА «НИКЕЛЬ» входит система управления базами данных MongoDB.

Для активации и проверки статуса службы воспользуйтесь следующими командами в консоли (с командой sudo -i):

```
systemctl start mongod.service
systemctl status mongod.service
```

Далее при успешной активации на экране высветится сообщение о том, что сервис запущен:

```
Active: active (running)
```

Для обращения к тестовой базе данных выполните следующие действия:

1. Установить тестовую коллекцию, командой:

```
dnf install mongodb-primer
```

2. Войти в оболочку, выполнив команду:

```
mongo
```

3. Сделать запрос к коллекции командой:

```
db.restaurants.find().limit(1).pretty()
```

На экране будут выведены данные из коллекции. Для выхода из оболочки нажмите Ctrl + D.

Сборка RabbitMQ-server

В серверной части ОС РОСА «НИКЕЛЬ» предустановлен программный брокер сообщений на основе стандарта AMQP (тиражируемое связующее программное обеспечение, ориентированное на обработку сообщений).

Сборка состоит из сервера, библиотек поддержки протоколов HTTP, XMPP и STOMP, клиентских библиотек AMQP для Java и .NET Framework и различных плагинов.

Для работы с RabbitMQ необходимо настроить утилиту и провести ее запуск и

подключение:

1. Проведение настройки

Для настройки утилиты откройте файл конфигурационный файл, утилитой mc или командой в консоли (с командой sudo -i):

```
nano /etc/rabbitmq/rabbitmq.conf
```

В начале файла найдите строку и раскомментируйте ее (уберите символ #):

```
# listeners.tcp.default = 5672
```

Далее находим строки:

```
# default_user = guest
# default_pass = guest
```

Меняем их на свои, например:

```
# default_user = rabbitadmin
# default_pass = rabbitadmin
```

В утилите установлен временный пароль, который необходимо поменять после запуска RabbitMQ. Раскомментируйте данные строки (уберите символ #).

Далее находим строку и также раскомментируйте ее:

```
default_user_tags.administrator = true
```

Сохраните файл и выйдите из него.

2. Для запуска сервиса воспользуйтесь следующей командой:

```
systemctl start rabbitmq-server.service
```

3. Включить плагин управления RabbitMQ, командами:

```
sudo -u rabbitmq rabbitmq-plugins enable rabbitmq_management
chown -R rabbitmq:rabbitmq /etc/rabbitmq/
sudo -u rabbitmq rabbitmqctl change_password rabbitadmin 12345
systemctl restart rabbitmq-server.service
```

4. Для просмотра открытых портов воспользуйтесь командой:

```
sudo ss -an | grep 5672
```

Должны быть открыты следующие порты: 5672/25672/15672

5. Запустить браузер, и зайти в web интерфейс по адресу:

```
http://localhost:15672/
```

Введите указанный выше логин и пароль: rabbitadmin/12345.

Сборка Redis

Redis (REmote DIctionary Server) — это не реляционная структура данных в памяти, используемая в качестве базы данных.

Для проверки статуса Redis необходимо запустить сервис, введя команды:

```
systemctl start redis.service
systemctl status redis.service
```

Далее на экране высветится сообщение о том, что сервис запущен:

```
Active: active (running)
```

Для создания и чтения ключей базы данных выполните следующую инструкцию:

1. Проверьте что сервис находиться на хосте localhost:6379, командой:

```
netstat -tlnp | grep 6379
```

2. От пользовательской (не sudo -i) учетной записи выполнить команды:

```
redis-cli
set mykey 2000
get mykey
```

Если на экране появится значение ключа «2000», то сервис работает успешно.

По окончании проверки необходимо ввести команду для выхода:

```
quit
```

Проверка fuzzystrmatch

Fuzzystrmatch – расширение для СУБД PostgreSQL. Для запуска расширения необходимо создать расширение и проверить одну или несколько из его команд:

1. Запустите PostgreSQL командой:

```
systemctl start postgresql12.service
```

2. Зайдите в командный интерфейс:

```
sudo -u postgres psql
```

3. Выполните команду:

```
CREATE EXTENSION fuzzystrmatch;
```

4. Для примера проверьте команду soundex, выполнив:

```
SELECT soundex('hello world!');
```

Проверка считается выполненной успешно, если на экране появится результат команды, в такой форме:

```
 soundex
---------
 H464
(1 row)
```

Для выхода нажать сочетание клавиш <Ctrl + D>.

TRIPSO-CIPSO конвертер

Для проверки и настройки сервиса необходимо выполнить последовательность действий, описанных в руководстве от разработчика:

https://abf.io/kpl/help/raw/master/Instructions/network_compatibility.html

Проверка сборки пакета Контроля носителей USBguard

USBGuard — программная среда, которая предназначена для сличения атрибутов устройств с «белым» и «черным» списками подключения устройств, что позволяет ей блокировать любые подключения внешних устройств.

После установки USBGuard потребуется провести настройку конфигурационного файла usbguard-daemon.conf. Подключившись затем к ОС, программа сканирует подключенные к системе USB-устройства или хабы и последовательно применяет прописанные настройки сетевой защиты. По итогам сканирования она может разрешить (активировать) работу накопителя, запретить (деактивировать) его либо заблокировать (выключить).

Полную справку по работе с утилитой можно получить по команде `man usbguard`.

Проверка интеграции fapolicyd

fapolicyd – фреймворк, реализующий возможность создания белого и черного списков приложений, которые позволяют разграничить какие из программ можно запускать пользователю, а какие нет (например, для блокировки запуска непроверенных внешних исполняемых файлов).

Для проверки запуска сервиса fapolicyd необходимо и проверки статус, введите команды:

```
systemctl start fapolicyd.service
systemctl status fapolicyd.service
```

Проверка по пункту считается успешной если на экране высветится сообщение о том что сервис запущен:

```
Active: active (running)
```

Полную справку по работе с утилитой можно получить по команде `man fapolicy`.

4. РОЛИ И ПРИВИЛЕГИИ

4.1. Пользователь и администратор

В системе Никель присутствуют две роли — пользователь и администратор, у них есть несколько атрибутов, дающим им дополнительные привилегии по доступу к функциям системы.

Административные действия всегда выполняются из-под суперпользователя linux (root) с ID=0, но в современной концепции безопасности прямая работа с неограниченными полными правами, под root настоятельно не рекомендуется. Поэтому по-умолчанию непосредственный вход под root отключен и административные задачи должны выполняться с помощью механизма запроса привилегий, необходимых на время выполнения таких задач.

Таким образом **администратором** в системе Никель называется пользователь с учетной записью linux, которому присвоены атрибуты безопасности, дающие право запроса привилегий на временное «переключение в root» для совершения административных действий.

Атрибуты безопасности администратора системы:

1. Пользователь linux должен быть включен в группу **wheel**, дающую доступ к стандартному для linux механизму поднятия привилегий пользователя до **root** командой *sudo*

2. Пользователю linux должны быть присвоены посредством сопоставленного SELinux-пользователя SELinux-роли **sysadm_r** и/или **secadm_r**, которые дают дополнительные привилегии для управления атрибутами конфиденциальности SELinux. Также администратору системы присваивается Selinux-роль **auditadm_r** для доступа к логам аудита.

Роль **пользователя** системы выполняет любой пользователь linux, НЕ включенный в группу wheel, которому присвоены посредством сопоставленного SELinux-пользователя SELinux-роли **user_r** и/или **auditadm_r**, дающие возможность соответственно к работе с конфиденциальными документами и к мониторингу логов аудита системы.

4.2. Пользователи, пользователи selinux и их роли

В ОС РОСА «НИКЕЛЬ» реализованы две системы разграничения контроля

доступа: учетные записи пользователей Linux и SELinux-пользователи (Рисунок 69). С каждой учетной записью Linux сопоставляются доступные для нее SELinux-пользователи и далее определяется роль/роли SELinux-пользователя.

При установке ОС РОСА «НИКЕЛЬ» в системе создается первый пользователь, который по умолчанию настроен как администратор системы, обладающий доступом к максимальному количеству привилегий.

В дальнейшем администратором системы будет называться Linux-пользователь, включенный в группу *wheel* для доступа к команде *sudo* и сопоставленный с SELinux-пользователями aib_u или sysadm_u, и, соответственно имеющий доступ к ролям SELinux **sysadm_r | secadm_r | auditadm_r**. При установке по-умолчанию администратор это первый пользователь системы, сопоставленный с selinux-пользователем aib_u.

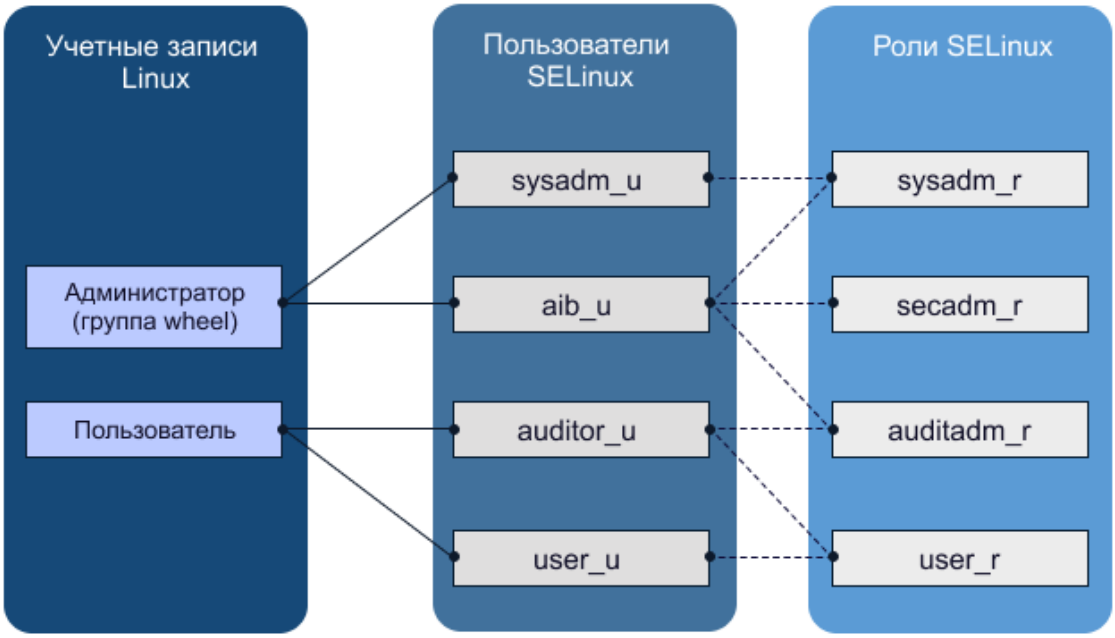


Рисунок 69

В ОС РОСА «НИКЕЛЬ» определено четыре пользователя SELinux:

- администратор системы (**sysadm_u,** доступна роль **sysadm_r**);
- администратор безопасности (**aib_u**, доступны проли **sysadm_r**, **secadm_r, auditadm_r**);
- оператор аудита (**auditor_u**, доступны роли **user_r**, **auditadm_r**);
- пользователь (**user_u**, доступна роль **user_r**).

Selinux-пользователь *user_u* – сопоставленный с ним linux-пользователь выполняет обработку защищаемой информации с помощью установленного в системе ПО. У него доступна одна роль — *user_r*, по-умолчанию он входит именно под ней.

Selinux-пользователь оператор аудита *auditor_u* – сопоставленный с ним linux-

пользователь выполняет расследования инцидентов и событий безопасности, ему предоставляется доступ к журналам аудита и, кроме умолчательной для пользователя SELinux-роли *user_r*, ему доступна SELinux-роль *auditadm_r.* Переключиться на SELinux роль *auditadm_r* с целью доступа к журналам аудита можно командой в консоли:

```
newrole -r auditadm_r
```

Для запуска графической программы с доступом к роли аудитора применяется команда:

```
newrole-gui -r auditadm_r -c <КомандаЗапускаПрограммы>
```

Selinux-администратор системы *sysadm_u* – сопоставленный с ним linux-пользователь, выполняет настройку и восстановление работоспособности ОС, установки и удаления ПО. Ему доступна роль *sysadm_r,* под ней и совершается вход.

Selinux-администратор безопасности *aib_u* – сопоставленный с ним пользователь linux, выполняет администрирование безопасности ОС. Данный пользователь наделен максимальными привилегиями: управление другими пользователями и их атрибутами безопасности, управление параметрами механизмов безопасности, настройка и восстановление работоспособности ОС, установка, удаление ПО и др. Этому пользователю selinux доступны роли *auditadm_r*, *sysadm_r*, *secadm_r.* Для переключения на эти роли используются, соответственно, команды в консоли:

```
newrole -r auditadm_r
newrole -r sysadm_r
newrole -r secadm_r
```

Для запуска графической программы с доступом к ролям применяются команды:

```
newrole-gui -r auditadm_r -c <КомандаЗапускаПрограммы>
newrole-gui -r sysadm_r -c <КомандаЗапускаПрограммы>
newrole-gui -r secadm_r -c <КомандаЗапускаПрограммы>
```

Для просмотра функциональных возможностей SELinux пользователей, перейдите к следующим разделам документа:

- для администратора безопасности – к разделу 3.1. Администратор безопасности (aib_u, доступна роль secadm_r);
- для администратора – к разделу 3.2. Администратор системы (sysadm_u, доступна роль sysadm_r);
- для оператора аудита – к разделу 3.3. Оператор аудита (auditor_u, доступ к роли auditadm_r);
- для пользователя – к разделу 3.4. Пользователь (user_u, доступ к роли

user_r).

Сопоставление учетных записей Linux с пользователями SELinux определена в файле **/etc/selinux/mls/seusers**.

В графическом интерфейсе пользователя сопоставление пользователей linux и пользователей selinux (Рисунок 70), а также назначение ролей доступно в программе «Администрирование selinux»

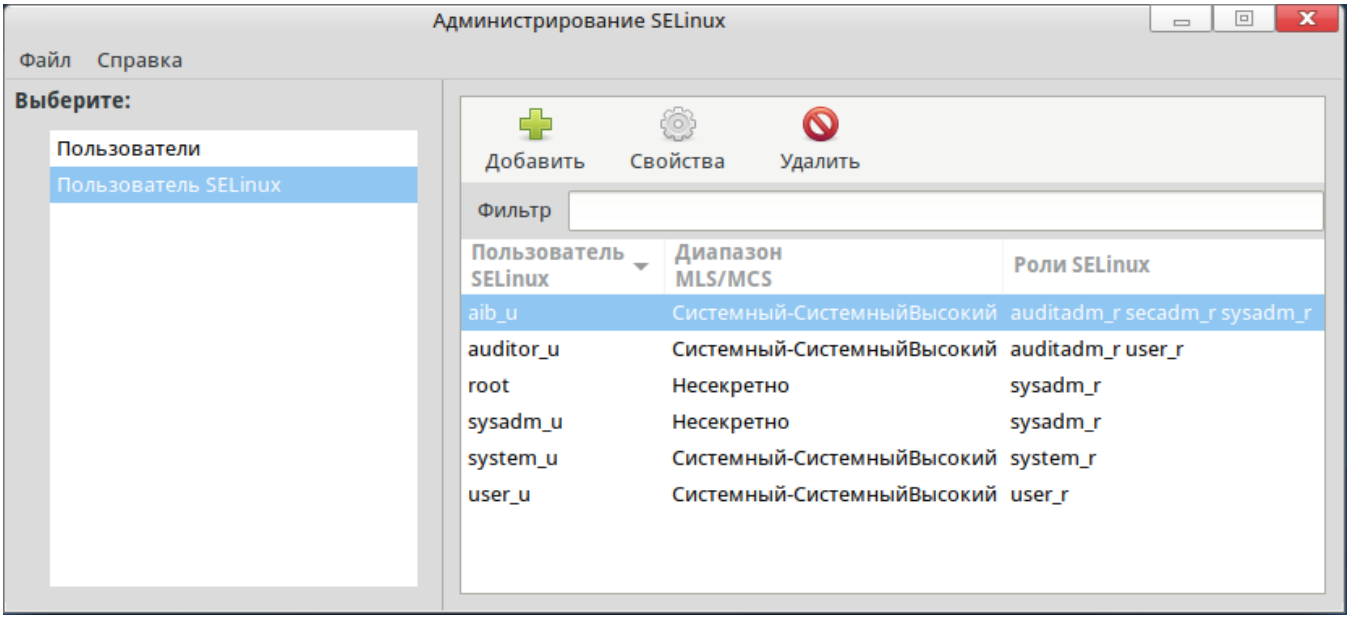


Рисунок 70

Далее описаны функциональные возможности по минимальному доступу SELinux-пользователя (т.е. если функция описана для auditor_u, она также доступна и более привилегированным пользователям sysadm_u и aib_u).

4.3. Администратор безопасности (aib_u, доступна роль secadm_r)

4.3.1. Обязанности (Права и обязанности)

Пользователь «Администратор безопасности» является самым привилегированным пользователем ОС. Убедитесь, что пользователь с правами администратора безопасности систем – опытный пользователь ОС, поскольку администратор безопасности обладает неограниченными правами в ОС. Только пользователь aib_u может назначать другим пользователям системы уровень доступа к защищенной информации и также обладает доступом к защищаемой информации в пределах выделенного диапазона. Администратору безопасности также доступны действия по изменению системного времени в ОС.

Идентификация и аутентификация пользователей /Управление учетными записями

Со стороны администратора безопасности выполняются задачи по выдаче доступа к защищаемой информации разным категориям пользователей. Операции, не требующие для работы доступа к защищаемой информацией, может выполнять и администратор системы.

Управление доступом

ОС РОСА «НИКЕЛЬ» является многопользовательской системой, в которой доступ к файлам и каталогам разграничен для разных пользователей и групп пользователей. Администратор безопасности системы задает и управляет параметрами доступа к файлам, назначая разным пользователям/группам пользователей разный контекст безопасности SELinux (назначение SELinux-пользователей учетным записям Linux). Подробнее об управлении доступом Selinux см. в разделе 6.

Ограничение программной среды

Пользователь с правами администратора безопасности может ограничивать работу других пользователей системы, посредством использования режима киоска, с помощью которого возможно наложение ограничений программной среды. Подробнее о работе с режимом киоск см. в разделе 8.1. Киоск.

4.3.2. Сообщения

В ходе работы с ОС SELinux-пользователь aib_u может получать сообщения, свидетельствующие о следующих изменениях в системе:

- ошибки авторизации (неверный идентификатор или пароль);
- блокирования учетной записи;
- безуспешное связывание атрибутов безопасности пользователя с субъектом;
- сбой механизма безопасности;
- изменение системного времени;
- использование механизма восстановления информации;
- изменение настроек механизмов уничтожения (стирания) данных.

4.4. Администратор системы (sysadm_u, доступна роль sysadm_r)

4.4.1. Обязанности (Права и обязанности)

SELinux-пользователь sysadm_u с доступом к роли sysadm_r и возможностью переключения в режим root также является привилегированным пользователем ОС. Таким пользователем должен являться опытный пользователь ОС, поскольку права администратора предполагают реализацию процедур по настройке и восстановлению работоспособности ОС. Пользователь sysadm_u по-умолчанию не имеет доступа к

защищаемой информации.

Идентификация и аутентификация пользователей /Управление учетными записями

В обязанности sysadm_u входит контроль и выполнение операций по идентификации и аутентификации пользователей системы, управление учетными записями и паролями.

Процесс управления учетными записями может быть частично автоматизирован, но многие задачи должны быть исполнены администратором системы, такие как: подключение нового пользователя к системе, задание места размещения его начального каталога на СВТ, где будет создана учетная запись, создание определенных групп пользователей, добавление пользователя к группе, удаление пользователя из системы с очищением всех файлов пользователя.

Добавляя новых пользователей в систему, стоит учесть, что каждый из них должен обладать уникальным именем. Для каждого из пользователей должен быть назначен временный пароль, который в последствии меняется самим пользователем.

Подробнее о создании учетных записей см. раздел 5.

Настройка SSH-соединений

Для обеспечения удаленного управления ОС используется протокол SSH-соединений. Организация удаленного подключения к системе, настройка такого подключения, а также работы, связанные с защитой SSH-соединения доступны только пользователям с правами администратора. Инструкции по настройке SSH-соединения приведены в разделе 19.

Обеспечение надежного функционирования

Администратор системы также должен реализовывать и такую важную функцию средств защиты информации как резервное копирование системы. Проведение резервного копирования необходимо с целью возможности восстановления системы или ее части после возможных системных ошибок до того состояния, в каком она находилась на момент последнего копирования. Резервное копирование необходимо проводить на выделенные средства хранения данных, где будут храниться архивы с резервными копиями ОС.

Инструкция по созданию и восстановлению резервных копий системы рассмотрена в разделе 12.3. Создание и восстановление резервных копий.

При работе системы в аварийном режиме, задачей администратора является восстановление ОС в ручном режиме, порядок действий для восстановления приведен в разделе 12.4. Ручное восстановление системы.

Аудит

Администратор системы может задавать правила аудита, подробные инструкции приведены в разделе 8.2.Правила аудита, а также изменять правила ротации журналов (см. 8.3. Ротация журналов), а также настраивает оповещения.

Установка и удаление ПО

Для того, чтобы избежать установки нежелательных компонентов в систему, а также компонентов, которые могут нанести вред системе, права на установку, как и на удаление ПО есть только у администраторов системы (sysadm_u и aib_u). Стоит отметить, что для установки стороннего ПО в ОС РОСА «НИКЕЛЬ» необходимо выполнить процедуру подписи дистрибутива сертификатом ЭП разработчика ОС, об этом подробнее см. раздел 8.2. Проверка подписей исполняемых файлов.

Для выполнения процедур по установке, удалению и обновлению ПО в ОС РОСА «НИКЕЛЬ» пользователь с правами администратора может использовать командную строку. Подробнее об использовании менеджера пакетов см. в разделе 8.5. Менеджер пакетов.

Ограничение программной среды

Пользователю с правами администратора доступен просмотр, настройка, создание новых и управление предустановленными юнитами в системном менеджере systemd. Также с помощью systemd администратор может установить параметры восстановления системы и аварийного режима работы. Подробнее об этом см. в разделе 8.3. Системный менеджер systemd.

Ограничение ресурсов СВТ для пользователей системы

SELinux-пользователю sysadm_u доступны управление и настройка доступа других пользователей системы к ресурсам СВТ для обеспечения полноценной работы каждого из них. Для этого администратор должен устанавливать ограничение на использование оперативной памяти и дискового пространства для каждого из пользователей в зависимости от выполняемых задач. Подробнее об алгоритме установки таких ограничений см. раздел 12.2. Ограничение ресурсов для пользователя.

Планировщик заданий

SELinux-пользователь sysadm_u может выполнять настройки выполнения команд по расписанию с помощью службы crond, создавая конфигурационные файлы расписаний. Подробнее с механизмами работы службы можно ознакомиться в разделе 8.4 Планировщик заданий.

Защита памяти

Для обеспечения корректной работы системы и доступа пользователей к

свободному месту на СВТ, администратор системы должен проводить профилактическую очистку памяти СВТ с помощью утилиты ROSA Memory Clean. Механизм работы утилиты рассмотрен в разделе 10.1. Очистка памяти с помощью утилиты ROSA Memory Clean.

Контроль целостности

SELinux-пользователь sysadm_u также ответственен за проведение мониторинга целостности и правильной работы системы и компонентов системы на предмет выявления ранних признаков неисправностей. Контроль целостности компонентов ОС предполагает, что информация должна быть защищена от несанкционированного изменения. Неавторизованные пользователи должны быть ограничены в возможностях модифицировать или удалять уязвимую информацию. Подробнее о механизмах контроля целостности см. в разделе 11. Контроль целостности.

Управление доступом

Администратору доступен просмотр и модификации списков доступа ACL к файлам и каталогам, а также использование утилиты umask для наложения маски прав доступа. Об этом подробнее см. разделы 7.4.Управление маской прав доступа и 7.5. Управление списками доступа ACL.

Настройка сетевых служб

Администратор системы должен организовать подключение и работу следующих сетевых служб:

— Настройка веб-сервера Apache;

— Настройка сетевого доступа к ФС NFS;

— Настройка служб доступа по протоколу Samba.

Настройка и управление сетевыми службами доступны только пользователям с правами администратора, подробные инструкции по работе с данными службами рассмотрены в разделе Настройка сетевых служб.

Администратор также должен обеспечить подключение системы и корректную работу системы с сервером FreeIPA, который позволяет создать централизованную систему по управлению идентификацией пользователей, задать политику доступа и аудита, об этом подробнее см. в разделе 14.

Управление печатью

Для реализации функции печати документов администратор системы должен выполнить подключение к серверу печати CUPS, а также произвести процедуру настройки маркировки документов для печати документации, содержащей конфиденциальную информацию.

Пользователи с правами администратора задают правила маркировки документов

и настраивают режимы маркировки. Подробнее об управлении печатью в ОС см. раздел 16.

Добавление и настройка внешнего оборудования

Для установки, настройки и удаления аппаратных средств необходимо обладать правами администратора системы. В случае подключения новых аппаратных средств необходимо произвести соответствующую настройку оборудования для дальнейшей корректной работы с ним, подробнее об этом см. раздел 17.Настройка оборудования.

Отказоустойчивый кластер

Инструкции по созданию и настройке отказоустойчивого кластера приведены в разделе 12.5. Отказоустойчивый кластер.

Фильтрация сетевого потока

Блокирование нежелательного входящего трафика на сервере – важный инструмент повышения уровня защищенности системы. Фильтрация трафика предотвращает различные типы вторжений, особенно из-за пределов локальной сети. Для проведения фильтрации сетевого потока администратор безопасности системы должен проводить настройку firewall, iptables и nftables, в ходе которой пользователям будет разрешен только действительно необходимый и безопасный трафик и блокирован остальной. Подробнее о настройке межсетевого экрана см. в разделе 13.2. Фильтрация сетевого потока.

4.4.2. Сообщения

В ходе работы с ОС SELinux-пользователь sysadm_u может получать сообщения, свидетельствующие о следующих изменениях в системе:

- ошибки авторизации (неверный идентификатор или пароль);
- блокирования учетной записи;
- безуспешное связывание атрибутов безопасности пользователя с субъектом;
- сбой механизма безопасности;
- изменение системного времени;
- использование механизма восстановления информации;
- изменение настроек механизмов уничтожения (стирания) данных.

4.5. Оператор аудита (auditor_u, доступ к роли auditadm_r)

4.5.1. Обязанности (Права и обязанности)

Оператор аудита – специализированный пользователь SELinux, задачами которого является контроль аудита ОС. В обязанности оператора аудита входит работа

по расследованию инцидентов и событий безопасности, такой пользователь имеет доступ к логам аудита, имеет право работать с журналами аудита и просматривать их. Оператор аудита имеет доступа к защищаемой информации.

Аудит

Оператору аудита доступна работа с утилитой ROSA Central Panel, в частности с приложением Аудит (кроме него это доступно только SELinux-пользователю администратор безопасности aib_u). С помощью утилиты просматриваются события безопасности системы. Подробнее о работе с приложением см. 7.1.4. Rosa-central-panel-logviewer

У пользователя auditor_u ограничен доступ к эмулятору терминала.

4.5.2. Сообщения

В ходе работы с ОС пользователь auditor_u может получать сообщения, свидетельствующие о следующих изменениях в системе:

- ошибки авторизации (неверный идентификатор или пароль);
- блокирования учетной записи;
- безуспешное связывание атрибутов безопасности пользователя с субъектом;
- сбой механизма безопасности;
- изменение системного времени;
- использование механизма восстановления информации;
- изменение настроек механизмов уничтожения (стирания) данных.

4.6. Пользователь (user_u, доступ к роли user_r)

4.6.1. Обязанности (Права и обязанности)

Пользователь user_u – SELinux пользователь, выполняющий обработку защищаемой информации с помощью установленного в системе ПО**.** У пользователя user_u имеется доступ к защищаемой информации в пределах выделенного диапазона.

Пользователь имеет право хранить и обрабатывать информацию в рамках выделенного для него домашнего каталога.

У пользователя user_u ограничен доступ к эмулятору терминала.

Настройка пароля

Пользователю user_u доступны действия по изменению собственного пароля в соответствии с требованиями, предъявляемыми к безопасности паролей в ОС. Параметры сложности пароля представлены в разделе 4.1.3. Назначение пароля и его

временных характеристик, а также 4.1.4. Сложность паролей.

Работа с ПО

Для обработки информации пользователь может использовать любое ПО, установленное администратором системы.

Таже в ОС РОСА «НИКЕЛЬ» имеется ряд предустановленного ПО, с помощью которого возможен просмотр, редактирование и работа с файлами и документами различного рода, организация работы с электронной почтой и в сети. Полный список предустановленного ПО и краткие инструкции по работе с ним приведены в разделе 2.4. Встроенное программное обеспечение.

Пользователи могут самостоятельно задавать атрибуты собственных файлов.

Тестирование

Также пользователю доступно тестирования ОС с помощью утилиты Rosa Security Test, подробнее о процедуре тестирования см. в разделе 11.2 Тестирование ROSA Security Test.

Защита памяти

Для обеспечения защиты конфиденциальной информации, при ее удалении с внешних носителей пользователю доступно использование специализированной утилиты Rosa Shred. Об этом см. подробнее в разделе 11.3. Удаление файлов с носителей с помощью утилиты ROSA Shred.

4.6.2. Сообщения

В ходе работы с ОС SELinux-пользователь user_u может получать сообщения, свидетельствующие о следующих изменениях в системе:

- ошибки авторизации (неверный идентификатор или пароль);
- блокирования учетной записи;
- безуспешное связывание атрибутов безопасности пользователя с субъектом;
- сбой механизма безопасности;
- изменение системного времени;
- использование механизма восстановления информации;
- изменение настроек механизмов уничтожения (стирания) данных.

4.7. SELinux-пользователи их роли и функциональности

SELinux-пользователи, их роли и их функциональности (Таблица 2).

Таблица 2

Функциональность	**aib_u (secadm_r)**	**sysadm_u (sysadm_r)**	**auditor_u (auditadm_r)**	**user_u (user_r)**
Идентификация и аутентификация				
Управление локальными учетными записями: создание, модификация, удаление учетных записей	+	+	-	-
Назначение SELinux-пользователей учетным записям	+	-	-	-
Возможность удаленного входа по SSH	+	+	-	-
Назначение пароля другим пользователям	+	+	-	-
Изменение собственного пароля	+	+	+	+
Управление доступом				
Задание уровней конфиденциальности и категорий доступа SELinux-пользователям	+	-	-	-
Повышение привилегий (дискреционная политика управления доступом; с помощью команды sudo)	+	+	-	-
Повышение привилегий (мандатная и ролевая политика управления доступом; с помощью команды sudo)	+	+	-	-
Изменение дискреционных атрибутов файлов	+	+	+	+
Управление маской прав доступа	+	+	-	-
Управление списками доступа ACL	+	+	-	-
Настройка блокировки сеанса пользователя по таймеру	+	+	+	+
Настройка таймера завершения сеанса после времени бездействия	+	+	+	+
Регистрация событий безопасности (аудит)				
Работа с приложением Аудит (работа с журналом)	+	-	+	-
Задание правил аудита	+	+	-	-
Ротация журналов	+	+	-	-
Настройка оповещения администратора	+	+	-	-
Ограничение программной среды				
Киоск	+	-	-	-
Проверка подписей исполняемых файлов	+	+	-	-
Системный менеджер systemd	+	+	-	-
Планировщик заданий	+	+	-	-
Работа с менеджером пакетов	+	+	-	-

Функциональность	aib_u (secadm_r)	sysadm_u (sysadm_r)	auditor_u (auditadm_r)	user_u (user_r)
Установка ПО	+	+	-	-
Удаление ПО	+	+	-	-
Защита памяти				
Очистка памяти Rosa Memory Clean	+	+	-	-
Очистка памяти носителей с Rosa Shred	+	+	+	+
Удаление файлов	+	+	+	+
Контроль целостности				
Тестирование Rosa Security Test	+	+	+	+
Проверка целостности aide	+	+	-	-
Обеспечение надежного функционирования				
Настройка системного времени	+	+	-	-
Ограничение ресурсов для пользователя	+	+	-	-
Создание и восстановление резервных копий	+	+	-	-
Ручное восстановление системы	+	+	-	-
Настройка отказоустойчивого кластера	+	+	-	-
Фильтрация сетевого потока				
Настройка firewall	+	+	-	-
Использование службы iptables	+	+	-	-
Настройка nftables	+	+	-	-
Подключение к домену FreeIPA				
Настройка сети	+	+	-	-
Установка и подключение клиента	+	+	-	-
Настройка сетевых служб	+	+	-	-
Управление печатью				
Настройка службы CUPS	+	+	-	-
Настройка маркировки документов	+	+	-	-
Добавление и настройка внешнего оборудования	+	+	-	-
Настройка SSH-СОЕДИНЕНИЙ	+	+	-	-
Работа с СУБД PostgreSQL	+	+	-	-

Полный список графических, текстовых и командных интерфейсов безопасности с доступностью по ролям selunux см в настоящем документе.

4.7.1. Реагирование на ошибки эксплуатации

При ошибках эксплуатации ОС сама переводится в режим обслуживания. Если этого не произошло, необходимо прекратить обработку информации.

После этого нужно уведомить административно-технический персонал,

отвечающий за обслуживание и ждать, пока проблема будет устранена.

5. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

5.1. Управление локальными учетными записями

Управление локальными учетными записями осуществляется с помощью графического приложения «Управление пользователями» или с помощью утилит командной строки, описание которых приведено далее.

Приложение «Управление пользователями» предоставляет возможность создания, модификации, удаления учетных записей пользователей и групп пользователей. Оно имеет интуитивно понятный интерфейс управления. Приложение можно запустить, выбрав пункт меню [Параметры системы] → [Управление пользователями], или используя команду userdrake.

5.1.1. Создание, модификация, удаление учетных записей

Имена учетных записей пользователей и их идентификаторы хранятся в файле /etc/passwd. Каждая запись в файле состоит из полей (Таблица 3).

Таблица 3

Поле	**Описание**
Имя пользователя	Системное имя пользователя
Признак пароля	Символ «x» обозначает наличие пароля
Идентификатор пользователя (UID)	Каждый пользователь имеет свой уникальный идентификационный номер
Идентификатор основной группы пользователя (GID)	В этом поле указывается идентификационный номер группы, к которой принадлежит пользователь
Дополнительная информация (GECOS)	Используется опционально для хранения дополнительной информации о пользователе
Домашний каталог пользователя	Поле содержит путь к домашнему каталогу пользователя
Путь к командной оболочке	Поле содержит путь к файлу командной оболочки

Для управления учетными записями рекомендуется использовать следующие утилиты.

Утилита useradd предназначена для создания учетной записи пользователя. Часто используемые опции утилиты useradd. Подробное описание приведено в man useradd (Таблица 4).

Синтаксис:

```
useradd <опции> <имя учетной записи>
```

Таблица 4

Опция	Описание
-g, --gid GROUP	Указание первичной группы пользователя
-G, --groups GROUP1[,GROUP2,...[,GROUPN]]]	Указание дополнительных групп пользователя
-m, --create-home	Создание домашнего каталога пользователя
-s, --shell SHELL	Указание командной оболочки пользователя
-u, --uid UID	Указание идентификатора пользователя

В результате выполнения данной команды произойдет создание учетной записи пользователя user1 и его домашнего каталога:

```
# useradd -m user1
```

Утилита usermod предназначена для изменения параметров учетной записи пользователя. Часто используемые опции утилиты usermod. Подробное описание приведено в man usermod (Таблица 5).

Синтаксис:

```
usermod <опции> <имя учетной записи>
```

Таблица 5

Опция	Описание
-e, --expiredate EXPIRE_DATE	Указание даты блокировки в формате ГГГГ-ММ-ДД (дней, после которых учетная запись будет заблокирована, начиная с 1 января 1970 года)
-f, --inactive DAYS	Указание числа дней с даты обязательной смены пароля до блокировки учетной записи
-g, --gid GROUP	Указание новой первичной группы пользователя
-G, --groups GROUP1[,GROUP2,...[,GROUPN]]]	Указание дополнительных групп пользователя
-l, --login LOGIN	Указание нового имени учетной записи пользователя
-L, --lock	Блокирование учетной записи пользователя
-s, --shell SHELL	Указание командной оболочки пользователя
-u, --uid UID	Указание нового идентификатора пользователя
-U, --unlock	Разблокирование учетной записи пользователя

В результате выполнения следующей команды произойдет смена идентификатора пользователя user1:

```
# usermod -u 1050 user1
```

Утилита userdel предназначена для удаления учетной записи пользователя. В Часто используемые опции утилиты userdel. Подробное описание приведено в man userdel (Таблица 6).

Синтаксис:

```
userdel <опции> <имя учетной записи>
```

Таблица 6

Опция	Описание
-r, --remove	Удаление файлов пользователя (домашний каталог, почта)

В результате выполнения следующей команды произойдет удаление учетной записи пользователя user1 и его пользовательских файлов:

```
# userdel -r user1
```

Управления пользователями в графическом режиме осуществляется с помощью утилиты [Управление пользователями], которая находится в меню [Параметры системы].

Для добавления нового пользователя или удаления одного из имеющихся пользователей системы воспользуйтесь соответствующими кнопками в верхней части окна или выделите необходимого пользователя и выберете необходимый параметр вкладки [Действия].

Для редактирования параметров пользователя выберете необходимого пользователя двойным нажатием левой кнопки мыши или перейдите во вкладки [Действия] → [Редактировать].

В открывшемся окне (Рисунок 71) доступны настройки данных пользователя, в том числе идентификационных и аутентификационных, а также установка срока действия учетной записи, блокировка и установка изображения для учетной записи во вкладке [Информация об учетной записи].

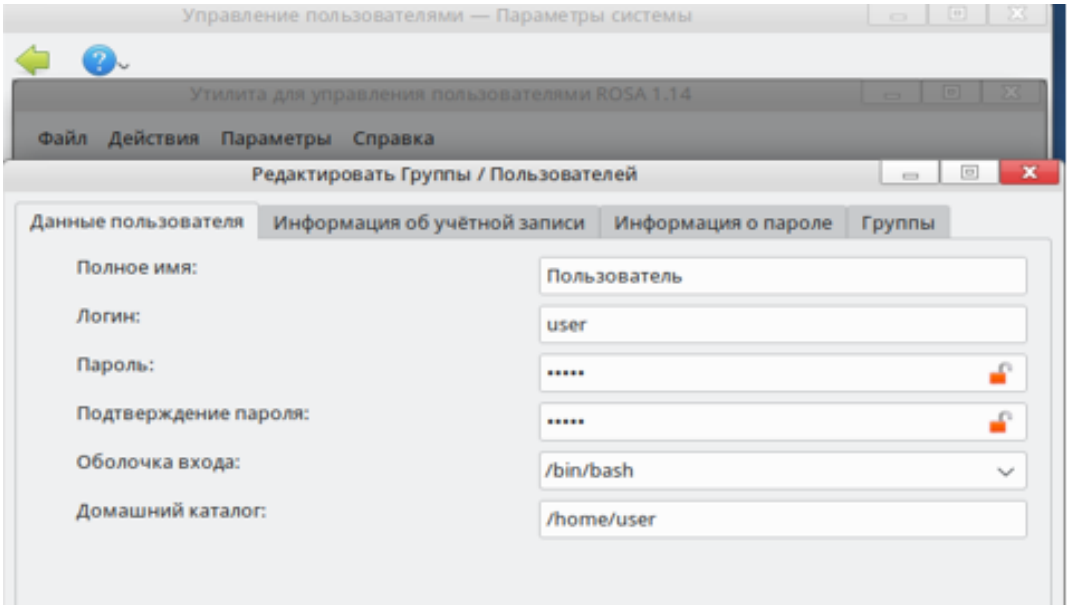


Рисунок 71

5.1.2. Создание, модификация, удаление групповых учетных записей

Имена групповых учетных записей (далее – имена групп) и их идентификаторы

хранятся в файле /etc/group. Каждая запись в файле состоит из полей (Таблица 7).

Таблица 7

Поле	Описание
Имя группы	Системное имя группы
Признак пароля	Символ «x» обозначает наличие пароля (обычно не используется)
Идентификатор группы (GID)	Уникальный идентификатор группы
Члены группы	В этом поле перечисляются пользователи, для которых группа является дополнительной

Для управления группами рекомендуется использовать следующие утилиты.

Утилита groupadd предназначена для создания группы. Часто используемые опции утилиты groupadd. Подробное описание приведено в man groupadd (Таблица 8).

Синтаксис:

```
groupadd <опции> <имя группы>
```

Таблица 8

Опция	Описание
-g, --gid GID	Указание идентификатора группы

Пример использования: в результате выполнения следующей команды будет создана группа group1:

```
# groupadd -g 1030 group1
```

Утилита groupmod предназначена для изменения параметров группы. используемые опции утилиты groupmod. Подробное описание приведено в man groupmod (Таблица 9).

Синтаксис:

```
groupmod <опции> <имя группы>
```

Таблица 9

Опция	Описание
-g, --gid GID	Указание нового идентификатора группы
-n, --new-name NEW_NAME	Указание нового имени группы

В результате выполнения следующей команды произойдет смена идентификатора группы group1:

```
# groupmod -g 1031 group1
```

Утилита groupdel предназначена для удаления группы. Подробное описание приведено в man groupdel.

Синтаксис:

```
groupdel <опции> <имя группы>
```

Пример использования: в результате выполнения следующей команды произойдет удаление группы group1:

```
# groupdel <имя группы>
```

Также доступно управление группами пользователей в графическом режиме через меню [Управление пользователями].

Для добавления группы пользователей в систему воспользуйтесь кнопкой [Добавить группу в систему]. В открывшимся окне введите все необходимые параметры (Рисунок 72).

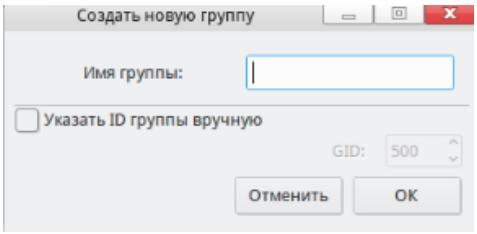


Рисунок 72

Для редактирования групп, в которые входит тот или иной пользователь войдите в режим редактирования пользователя (двойным нажатием левой кнопки мыши или выберете параметр [Редактировать] вкладки [Действия]) и отметься группы, в которые будет входить данный пользователь (Рисунок Рисунок 73).

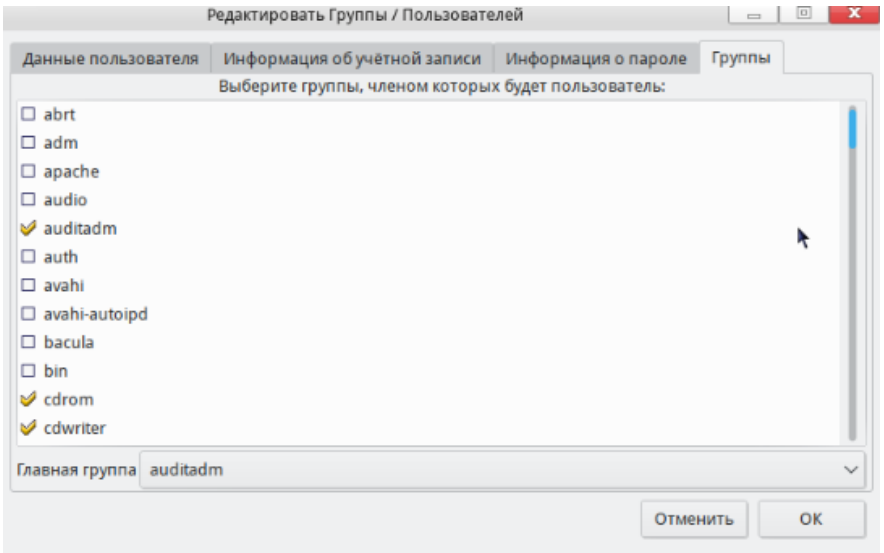


Рисунок 73

5.1.3. Назначение пароля и его временных характеристик

Пароли пользователей в неявном виде и временные параметры учетных записей хранятся в файле /etc/shadow. Каждая запись в файле состоит из полей (

Таблица 10).

Таблица 10

Поле	Описание
Имя пользователя	Это поле дублируется из файла /etc/passwd
Хэш пароля	Пароль хранится в неявном виде: хэш формируется по алгоритму SHA512. Если данное поле содержит знак «!!», это означает, что учетная запись заблокирована и пользователь не сможет осуществить вход
Дата последней смены пароля	В этом поле записывается число дней, прошедших с 1 января 1970 года до даты, когда пользователь сменил пароль в последний раз. Эта информация вместе используется со следующими полями, управляющими сроком действия пароля
Минимальное число дней действия пароля	Минимальный срок (в днях), который должен истечь, прежде чем пользователь сможет сменить пароль
Максимальное число дней действия пароля	Максимальный срок (в днях), по истечении которого необходимо сменить пароль
Число дней до вывода предупреждения о необходимости смены пароля	Число дней до истечения срока действия пароля, в течение которых пользователь будет получать предупреждения о скором окончании срока действия пароля
Число дней с даты обязательной смены пароля до блокировки учетной записи	Число дней, которое должно пройти с момента окончания срока действия пароля до отключения учетной записи
Дата блокировки	Число дней, после которых учетная запись будет заблокирована, начиная с 1 января 1970 года
Пустое поле	Поле игнорируется

Для установки, изменения паролей и временных параметров рекомендуется использовать следующие утилиты.

Утилита passwd предназначена для задания пароля пользователя и изменения временных параметров учетной записи. Новая учетная запись пользователя будет заблокирована, пока не будет установлен начальный пароль. Часто используемые опции утилиты passwd. Подробное описание приведено в man passwd (Таблица 11).

Синтаксис:

```
passwd <опции> <имя учетной записи>
```

Таблица 11

Опция	Описание
-l, --lock	Блокирование учетной записи пользователя
-u, --unlock	Разблокирование учетной записи пользователя
-e, --expire	Сделать пароль устаревшим. В результате этого система заставит пользователя изменить пароль при следующем входе в систему
-n, --minimum DAYS	Указание минимального числа дней действия пароля
-x, --maximum DAYS	Указание максимального числа дней действия пароля

Опция	Описание
-w, --warning DAYS	Указание числа дней до вывода предупреждения о необходимости смены пароля
-i, --inactive DAYS	Указание числа дней с даты обязательной смены пароля до блокировки учетной записи
-S, --status	Вывод информации о пароле и временных параметрах учетной записи

Пример использования: в результате выполнения команды будет предложено установить новый пароль для пользователя user1:

```
# passwd user1
```

Утилита chage предназначена для изменения временных параметров учетной записи. Часто используемые опции утилиты chage. Подробное описание приведено в man chage (Таблица 12).

Синтаксис:

```
chage <опции> <имя учетной записи>
```

Таблица 12

Опция	Описание
-d, --lastday LAST_DAY	Дата последней смены пароля в формате ГГГГ-ММ-ДД
-E, --expiredate EXPIRE_DATE	Указание даты блокировки в формате ГГГГ-ММ-ДД (дней, после которых учетная запись будет заблокирована, начиная с 1 января 1970 года)
-I, --inactive DAYS	Указание числа дней с даты обязательной смены пароля до блокировки учетной записи
-l, --list	Вывод временных параметров учетной записи
-m, --mindays DAYS	Указание минимального числа дней действия пароля
-M, --maxdays DAYS	Указание максимального числа дней действия пароля
-W, --warndays DAYS	Указание числа дней до вывода предупреждения о необходимости смены пароля

Пример использования: в результате выполнения следующей этой команды будет предложено изменение всех временных полей учетной записи user1:

```
# chage user1
```

Утилита usermod, также предназначена для изменения некоторых временных параметров учетной записи.

Для редактирования пароля в графическом режиме перейдите в меню [Параметры системы] → [Управление пользователями], далее в открывшемся окне выберете необходимого пользователя (двойным нажатием левой кнопки мыши на строчку пользователя или выберете параметр [Редактировать] вкладки [Действия]). В открывшимся окне (Рисунок 185) в соответствующих полях введите пароль.

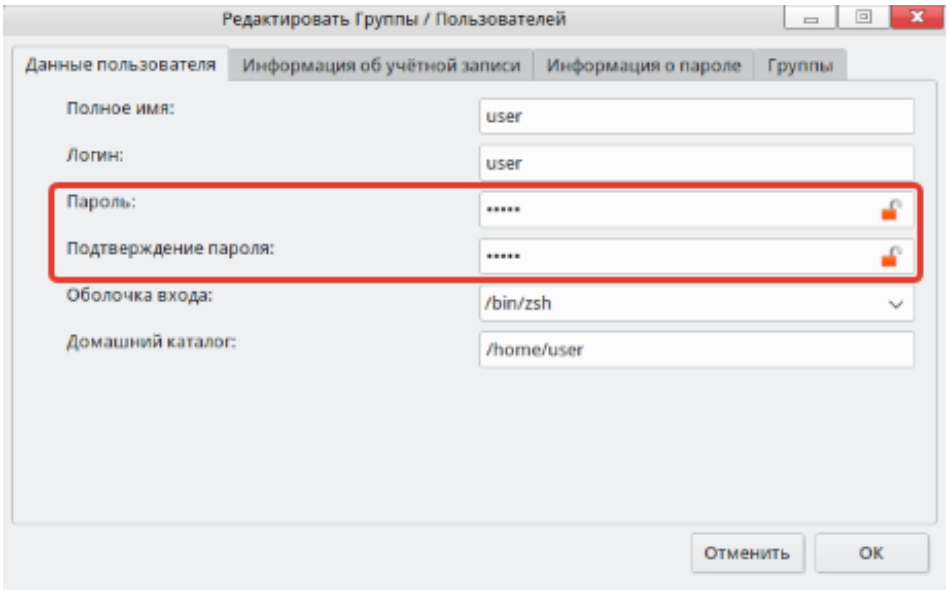


Рисунок 74

Также доступна установка срока действия пароля для пользователя во вкладке [Информация о пароле] (Рисунок 75).

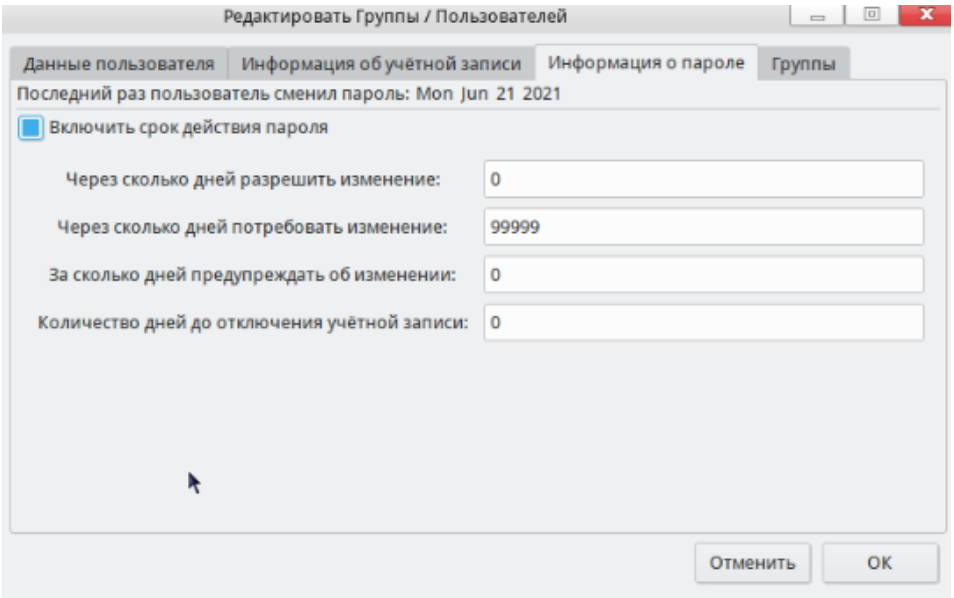


Рисунок 75

Для изменения собственного пароля (Рисунок 75) в графическом режиме откройте параметры настройки «Профиль пользователя – Модуль настройки KDE», а далее нажмите на кнопку «Изменить пароль», после чего после введения текущего пароля пользователя станет доступно назначение нового пароля.

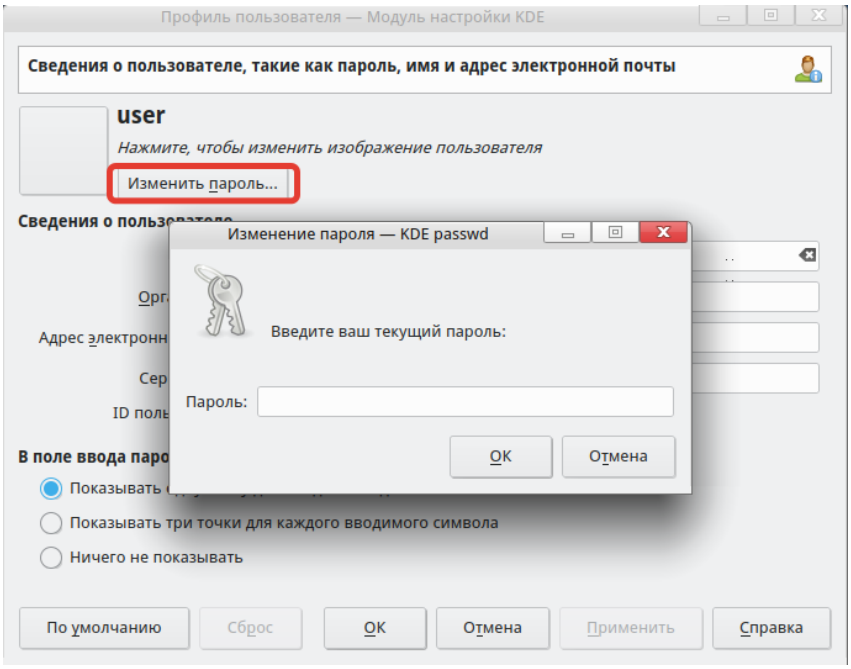


Рисунок 76

5.1.4. Сложность паролей

К паролям пользователей задаются следующие требования:

— длина пароля не менее 8 символов;

— пароль не основан на слове из словаря;

— пароль не должен повторять текущий пароль;

— пароль должен содержать комбинацию минимум трех категорий из перечисленных ниже:

а) символы верхнего регистра английского алфавита от A до Z;

б) символы нижнего регистра английского алфавита от A до Z;

в) цифры от 0 до 9;

г) знаки препинания или спецсимволы.

Модуль pam_pwquality предназначен для проверки паролей на соответствие правилам сложности паролей.

Для установки сложности пароля через модуль pam_pwquality используется файл /etc/security/pwquality.conf. В нем задается сложность паролей. Параметры, которые необходимо установить в соответствии с требованиями к паролям (Таблица 13).

Таблица 13

Параметр	Описание
difok	Параметр, указывающий какое количество символов нового пароля не должно совпадать с количеством символов старого пароля
minlen	Минимальное количество символов в пароле

Параметр	Описание
dcredit	Класс устойчивости пароля 1: минимальное количество цифр в пароле
ucredit	Класс устойчивости пароля 2: минимальное количество заглавных букв в пароле
lcredit	Класс устойчивости пароля 3: минимальное количество строчных букв в пароле
ocredit	Класс устойчивости пароля 4: минимальное количество спецсимволов в пароле
minclass	Количество учитываемых классов для качества пароля (число от 1 до 4)

Подробное описание всех параметров приведено в файле pwquality.conf. Подробное описание модуля приведено в man pam_pwquality.

5.2. Управление доменными учетными записями

Утилита ipa предназначена для управления доменом, учетными данными домена и пр. Утилита имеет большой функционал, описание которого приведено в man ipa, ipa help commands. Основные команды для управления учетными записями пользователя приведены далее.

Отображение всех учетных записей домена и их характеристик происходит с помощью команды:

```
# ipa user-find
```

Отображение учетной записи user происходит с помощью команды:

```
# ipa user-find user
```

Команда ipa user-add предназначена для создания учетной записи пользователя. Часто используемые опции команды ipa user-add. Подробное описание приведено в ipa user-add –help (Таблица 14).

Синтаксис:

```
ipa user-add <имя учетной записи> <опции>
```

Таблица 14

Опция	Описание
--gidnumber=INT	Указание первичной группы пользователя
--homedir=STR	Создание домашнего каталога пользователя
--shell=STR	Указание командной оболочки пользователя
--uid=INT	Указание идентификатора пользователя

Пример использования: в результате выполнения этой команды будет создана учетная запись пользователя user93 с идентификатором 200000001:

```
# ipa user-add user93 –uid=200000001
```

Команда ipa user-mod предназначена для изменения параметров учетной записи пользователя. Часто используемые опции команды ipa user-mod. Подробное описание приведено в ipa user-mod –help (Таблица 15).

Синтаксис:

```
ipa user-mod <имя учетной записи> <опции>
```

Таблица 15

Опция	Описание
--gidnumber=INT	Указание новой первичной группы пользователя
--homedir=STR	Указание нового домашнего каталога пользователя
--shell=STR	Указание командной оболочки пользователя
--uid=INT	Указание нового идентификатора пользователя

Пример использования: в результате выполнения этой команды произойдет смена идентификатора пользователя user93:

```
# ipa user-mod user93 --uid=1785800015
```

Для добавления пользователя user93 в группу business используется команда:

```
# ipa group-add-member business --users=user93
```

Для удаления пользователя user93 из группы business используется команда:

```
# ipa group-remove-member business --users=user93
```

Команда ipa user-del предназначена для удаления учетной записи пользователя. Часто используемые опции команды ipa user-del. Подробное описание приведено в `ipa user-del –help` (Таблица 16).

Синтаксис:

```
ipa user-del <имя учетной записи> <опции>
```

Таблица 16

Опция	Описание
--preserve	Удаление учетной записи, оставив запись доступной для использования в будущем
--no-preserve	Удаление учетной записи

Пример использования: в результате выполнения этой команды произойдет удаление пользователя user93:

```
# ipa user-del user93
```

5.2.1. Создание, модификация, удаление групповых учетных записей

Утилита ipa group-add предназначена для создания группы. Часто используемые опции утилиты ipa group-add. Подробное описание приведено в `ipa group-add –help` (Таблица 17).

Синтаксис:

```
ipa group-add <имя группы> <опции>
```

Таблица 17

Опция	Описание

Опция	Описание
--gid=GID	Указание идентификатора группы

Пример использования: в результате выполнения команды будет создана группа business с идентификатором 14475445:

```
# ipa group-add business --gid=14475445
```

Утилита ipa group-mod предназначена для изменения параметров группы. Часто используемые опции утилиты ipa group-mod. Подробное описание приведено в `ipa group-mod –help` (Таблица 18).

Синтаксис:

```
ipa group-mod <имя группы> <Опции>
```

Таблица 18

Опция	Описание
--gid=GID	Указание нового идентификатора группы
--rename=STR	Переименование группы

Пример использования: в результате выполнения команды произойдет переименование группы business на traders:

```
# ipa group-mod business --rename=traders
```

Утилита ipa group-del предназначена удаления группы. Подробное описание приведено в ipa group-del --help.

Синтаксис:

```
ipa group-del <имя группы> <опции>
```

Пример использования: в результате выполнения команды произойдет удаление группы business:

```
# ipa group-del business
```

5.2.2. Назначение пароля и его временных характеристик

Команда ipa passwd предназначена для изменения пароля учетной записи пользователя. Часто используемые опции команды ipa passwd. Подробное описание приведено в ipa passwd –help (Таблица 19).

Синтаксис:

```
ipa passwd <имя учетной записи> <опции>
```

Таблица 19

Опция	Описание
--otp	Указание одноразового пароля

Пример использования: в результате выполнения этой команды произойдет процедура смены пароля пользователя user93:

```
# ipa passwd user93
```

5.2.3. Сложность паролей (утилита ipa pwpolicy-mod)

Утилита ipa pwpolicy-mod предназначена для изменения параметров групповой политики паролей в домене. Часто используемые опции команды ipa pwpolicy-mod. Подробное описание приведено в `ipa pwpolicy-mod –help` (Таблица 20).

Синтаксис:

```
ipa pwpolicy-mod <имя группы> <опции>
```

Таблица 20

Опция	Описание
–-maxlife=INT	Указание максимального времени жизни пароля (в днях)
--minlife=INT	Указание минимального времени жизни пароля (в часах)
--history=INT	Указание запоминать прошлые пароли
--minclasses=INT	Указание минимального числа классов символов
--minlenght=INT	Указание минимальной длины пароля
--priority=INT	Указание приоритета политики (чем больше номер, тем ниже приоритет)
--maxfail=INT	Указание числа неправильных введенных подряд паролей для блокировки
--failinterval=INT	Интервал, после которого отсчет неправильно введенных паролей начинается заново
--lockouttime=INT	Период, во время которого удерживается блокировка (сек)

```
# ipa pwpolicy-mod business --minleght=8
```

в результате выполнения этой команды произойдет установка требования минимальной длины, равной восьми символам, для паролей пользователей группы business:

5.3. Параметры аутентификации

Механизм PAM (Pluggable Authentication Modules — подключаемые модули аутентификации) позволяет интегрировать различные низкоуровневые методы аутентификации и предоставить единые механизмы для использования прикладных программ в процессе аутентификации. Механизм состоит из набора разделяемых библиотек и конфигурационных файлов — сценариев процедур аутентификации.

В каталоге /etc/pam.d расположены конфигурационные файлы PAM для соответствующих сервисов, в т.ч. и для login (авторизованный вход в систему). В конфигурационном файле сервиса дана информация по проведению аутентификации.

Модули PAM вызываются при выполнении следующих функций:

- auth — аутентификация;
- account — получение привилегий доступа;
- password — управление паролями;
- session — сопровождение сессий.

Для выполнения каждой функции может быть перечислено несколько модулей PAM, которые будут вызываться последовательно, образуя стек PAM для данной задачи. Каждый вызываемый модуль возвращает в стек результат своей работы: успешный (PAM_SUCCESS), неуспешный (PAM_AUTH_ERR), игнорирующий (PAM_IGNORE) или иной. Для каждого вызова может быть указан набор управляющих флагов в виде соответствия кода возврата и того, как результат работы модуля скажется на обработке всей сервисной задачи, например, ignore, ok, die. Для управления аутентификацией используются следующие флаги:

- requisite — немедленное прекращение дальнейшего выполнения сервисной задачи с общим неуспешным результатом в случае неуспешного результата выполнения данного модуля;
- required — требование удачного выполнения этого модуля одновременно с выполнением всех остальных, перечисленных в данной сервисной задаче;
- sufficient — немедленное прекращение дальнейшего выполнения сервисной задачи с общим позитивным результатом, в случае позитивного результата выполнения данного модуля и всех предыдущих с флагом required в стеке задачи, если же модуль вернул негативный результат, то его значение игнорируется;
- optional — выполнение данного модуля никак не сказывается на результате всей задачи, но играет дополнительную информационную роль.

5.3.1. Блокирование неудачных попыток ввода аутентификационной информации

Модуль аутентификации pam_tally2 предназначен для блокирования учетной записи пользователя после нескольких неудачных попыток авторизации.

Для настройки модуля аутентификации pam_tally2 выполнить следующие действия. В конфигурационные файлы /etc/pam.d/system-auth и /etc/pam.d/password-auth добавить строки:

- в секцию auth (установить первой строкой):

```
auth required pam_tally2.so file=/var/log/tallylog deny=3 even_deny_root unlock_time=4800
```

где deny=3 задает количество неуспешных попыток входа пользователя до его

блокировки, unlock_time=4800 задает время блокирования пользователя;

– в секцию account (после строки «account required pam_unix.so»):

```
account required pam_tally2.so
```

Посмотреть данные по неуспешным входам пользователей можно с помощью утилиты pam_tally2. Подробное описание утилиты pam_tally2 приведено в man pam_tally2.

5.3.2. Ограниченная по времени авторизация

Модуль аутентификации pam_time предназначен для ограничения входа в систему. Подробное описание модуля pam_time приведено в man pam_time. Для реализации отказа в открытии сеанса пользователя, основанного на времени доступа, нужно сделать следующее.

Создать правило в файле /etc/security/time.conf, задающее разрешенное или запрещенное время доступа. Формат файла:

```
<services> <ttys> <users> <times>
```

Описание полей (Таблица 21). Более подробное описание полей и их параметров приведено в файле /etc/security/time.conf.

Таблица 21

Поле	Описание
<services>	Программы, на которые распространяется действие правила
<ttys>	Терминалы, на которых будет действовать правило
<users>	Пользователи, к которым относится правило
<times>	Время, к которому относится правило

Следующее правило запретит использование любых программ (включая вход в ОС) всеми пользователями в будние дни после 18-00 и до 9-00:

```
*;*;*;!Al1800-2400|Al0000-9000
```

После создания правила необходимо включить модуль pam_time. Для этого нужно добавить в файл /etc/pam.d/system-auth (первой строкой в секцию account):

```
account required pam_time.so
```

5.3.3. Ограничение числа параллельных сеансов пользователей и других ресурсов

В файле /etc/security/limits.conf определяются ограничения ресурсов системы для пользователя или группы пользователей. Формат файла:

```
<domain> <type> <item> <value>
```

Описание полей (Таблица 22). Более подробное описание полей приведено в файле /etc/security/limits.conf.

Таблица 22

<domain>	Поле может содержать: - имя пользователя; - имя группы. Перед именем группы нужно указать символ «@»; - символ «*» (данное ограничение будет ограничением по умолчанию)
<type>	Тип ограничения: мягкое (soft) или жесткое (hard). Мягкое ограничение определяет число системных ресурсов, которое пользователь все еще может превысить, жесткое ограничение превысить невозможно. При попытке сделать это, пользователь получит сообщение об ошибке
<item>	Параметром ограничения может быть: - core – ограничение размера файла core (Кб); - data – максимальный размер данных (Кб); - fsize – максимальный размер файла (Кб); - memlock – максимальное заблокированное адресное пространство (Кб); - nofile – максимальное число открытых файлов; - stack – максимальный размер стека (Кб); - cpu – максимальное время процессора (минуты); - nproc – максимальное число процессов; - as – ограничение адресного пространства; - priority – приоритет для процессов по умолчанию; - nice – максимальный приоритет, который можно назначить процессам; - maxlogins – максимальное число одновременных регистраций в системе; - locks – максимальное число файлов блокировки; и др.
<value>	Ограничительное значение параметра

Следующая запись ограничит число параллельных сеансов доступа для каждой учетной записи пользователей:

```
* - maxlogins 5
```

При регистрации в шестом сеансе пользователь user увидит сообщение:

```
Too many logins for 'user'
```

5.3.4. Двухфакторная аутентификация

Повышение надежности аутентификации возможно путем применения многофакторной аутентификации, т. е. аутентификации, в процессе которой используются аутентификационные факторы нескольких типов.

К факторам, которые могут быть использованы, относятся:

— ввод пароля или PIN-кода;

— ввод одноразовых паролей (скрэтч-карты);

— предоставление физического устройства или носителя, содержащего аутентификационную информацию (смарт-карта, USB-токен и т. п.);

— предоставление биометрической информации (отпечатки пальцев,

изображение сетчатки глаза и т. п.).

На практике в большинстве случаев используется двухфакторная аутентификация на основе ввода пароля с одновременным предоставлением пользователем физического устройства или носителя, содержащего дополнительную аутентификационную информацию. Дополнительной аутентификационной информацией в этом случае обычно является размещенный на устройстве сертификат пользователя.

Для обеспечения двухфакторной аутентификации с помощью внешнего носителя используются следующие средства и технологии:

— PKCS (Public-Key Cryptography Standard) — группа стандартов криптографии с открытым ключом, в частности, стандарты PKCS-11, PKCS-12, PKCS-15, относящиеся к работе с криптографическими токенами;

— X.509 — стандарт, определяющий форматы данных и процедуры распределения открытых ключей с помощью сертификатов с цифровыми подписями, которые предоставляются удостоверяющими центрами сертификации (Certification Authority (CA));

— OpenSC — набор программных утилит и библиотек для работы с носителями аутентификационной информации пользователя (смарт-карты, USB-токены), содержащие функции аутентификации, шифрования и цифровой подписи. Поддерживает стандарты PKCS-11, PKCS-15;

— OpenSSL — программное средство для работы с криптографическим протоколом SSL/TLS. Позволяет создавать ключи RSA, DH, DSA и сертификаты X.509, подписывать их, формировать файлы сертификатов CSR и CRT. Также имеется возможность тестирования SSL/TLS соединений;

— PC/SC — набор спецификаций для доступа к смарт-картам;

— PKINIT (Public Key Cryptography for Initial Authentication in Kerberos) — стандарт использования криптографии с открытым ключом в качестве фактора аутентификации в протоколе аутентификации Kerberos.

Двухфакторная аутентификация может применяться как в случае использования локальной аутентификации, так и в случае использования ЕПП.

Состав средств поддержки двухфакторной аутентификации

В состав ОС входят необходимые программные инструменты и библиотеки, реализующие перечисленные средства и технологии. Сведения о содержащих их программных пакетах (Таблица 23).

Таблица 23

Наименование	Описание
opensc	Набор программных утилит и библиотек OpenSC
pcscd	Служба доступа к смарт-картам через PC/SC
libpcsclite1	Библиотека доступа к смарт-картам через PC/SC
openct	Набор драйверов устройств работы с носителями аутентификационной информации (OpenCT)
libopenct1	Библиотека драйверов устройств работы с носителями аутентификационной информации (OpenCT)
libccid	PC/SC драйвер для CCID совместимых USB устройств работы с носителями аутентификационной информации
openssl	Программное средство генерации ключей и сертификатов OpenSSL
libengine-pkcs11-openssl	Расширение OpenSSL для поддержки модулей PKCS-11
libp11	Библиотека поддержки PKCS-11
libpam-p11	Подгружаемый модуль аутентификации с помощью смарткарт PKCS-11
libpam-pkcs11	Полнофункциональный подгружаемый модуль аутентификации с помощью смарт-карт PKCS-11
krb5-pkinit	Расширение MIT Kerberos V5 для поддержки PKINIT

Перед использованием средств двухфакторной аутентификации должны быть установлены перечисленные пакеты. Из последних трех пакетов должны быть выбраны именно те, которые будут применяться для организации локального входа пользователя (`libpam-p11` или `libpam-pkcs11`) или доменного входа пользователя в случае использования ЕПП (`krb5-pkinit`).

5.3.5. Локальная двухфакторная аутентификация с помощью смарт-карт Rutoken ЭЦП

Перед настройкой рекомендуется ознакомиться с актуальными материалами от производителя Rutoken (Портал документации Рутокен - Портал документации Рутокен - Сервер документации Рутокен (с официального сайта rutoken.ru)).

Установка Rutoken

Установите требуемые утилиты, для чего требуются права администратора:

```
sudo dnf install ccid opensc pam_pkcs11 pam_pkcs11-tools p11-kit-trust
```

Установите библиотеку PKCS#11 для Rutoken. Обратите внимание на то, что необходимо устанавливать библиотеку после установки утилит (Рисунок 77):

1. Для загрузки библиотек перейдите на сайт Rutoken: Библиотека PKCS#11 /

Центр загрузки / Поддержка / Рутокен (rutoken.ru).

2. На сайте Rutoken откройте вкладку «Пользователям GNU/Linux» и нажмите на ссылку «Библиотека rtPKCS11ecp для GNU/Linux RPM 64-bit (x64)».

3. Скачайте и установите пакет (требуется пароль администратора системы).

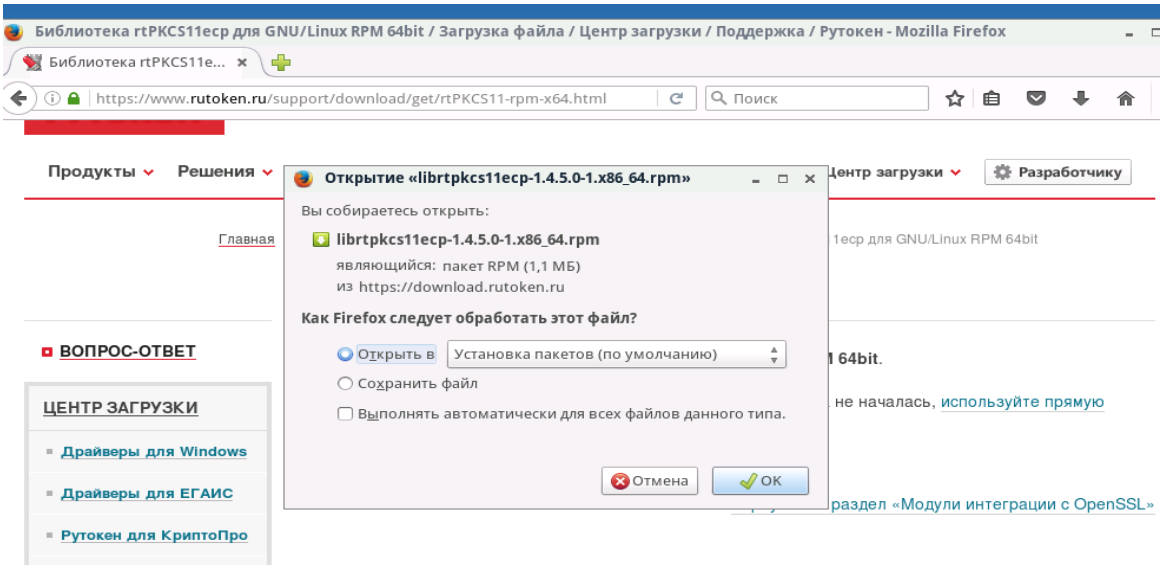


Рисунок 77

Настройка Rutoken

Для проверки отображения устройства в системе и наличия на нем нужной информации воспользуйтесь командой (требуются права администратора):

```
sudo pcsc_scan
```

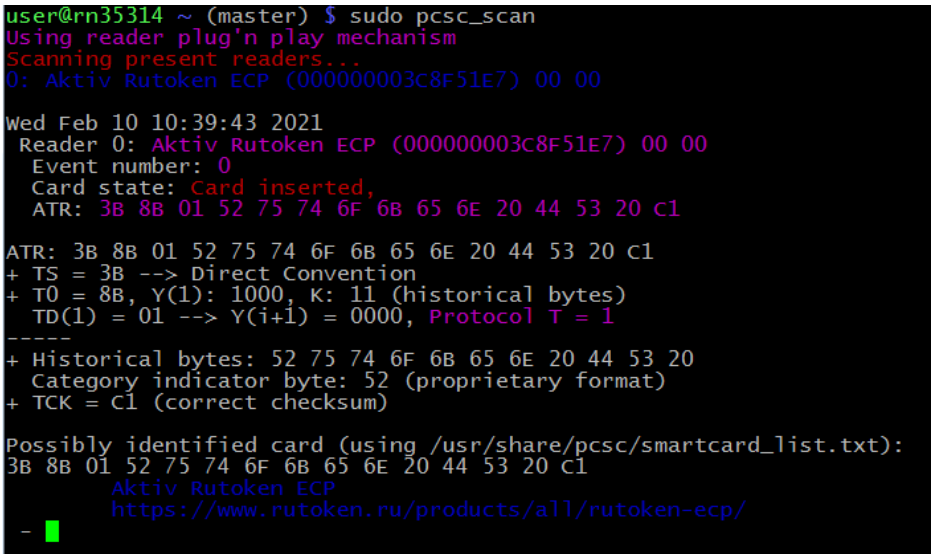


Рисунок 78

Запустите `pcscd` (требуются права администратора):

```
su
```

Завершите существующий процесс `pcscd`, если таковой имелся:

```
killall pcscd
```

С этого момента токен должен быть вставлен в соответствующий разъем.

Выполните:

```
pcscd -adfffff
```

Откройте отдельную вкладку или окно терминала и выполните в ней следующую команду:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -T
```

В выводе должны быть видны параметры и название устройства.

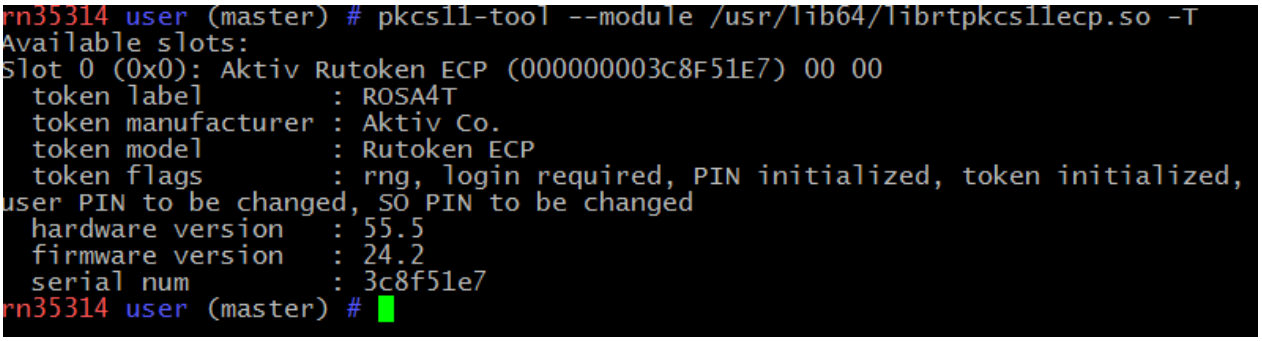


Рисунок 79

Для проверки наличия необходимой информации на токене воспользуйтесь следующей командой (требуется пароль от токена):

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -O -l
```

В выводе обязан присутствовать `Certificate Object`. Такие параметры, как `ID` и `label`, могут отличаться от Рисунок Рисунок 80.

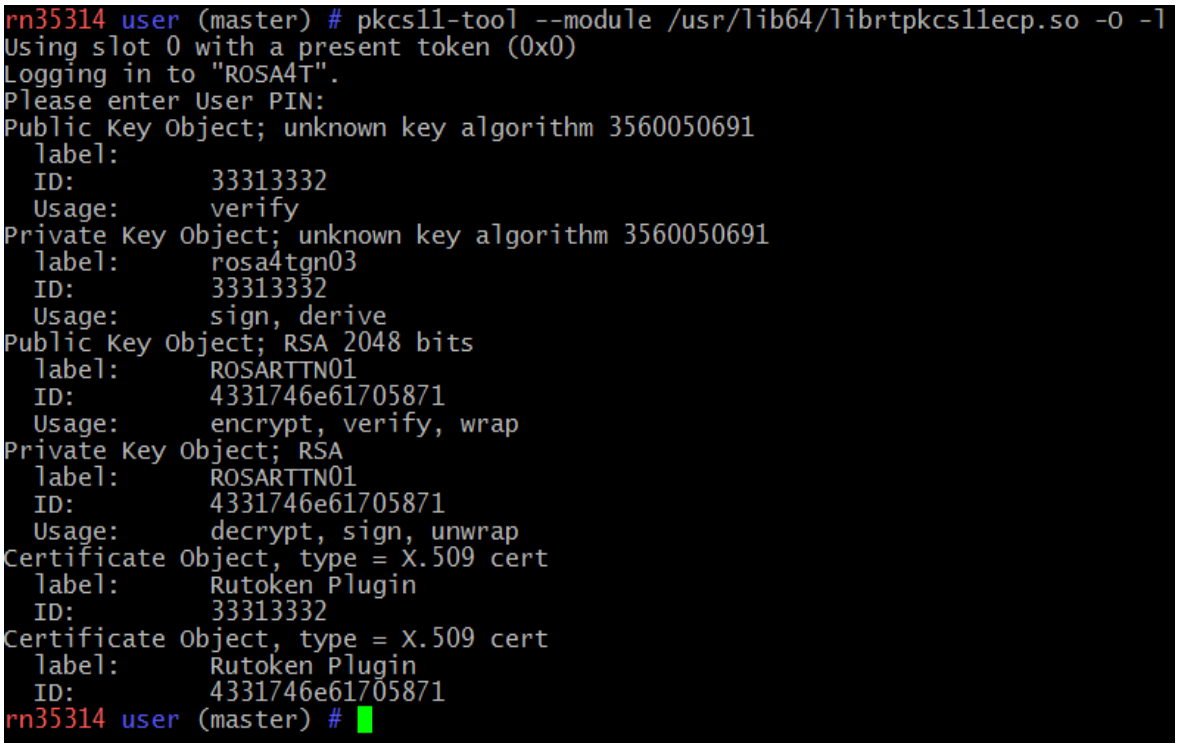


Рисунок 80

Создание ключей и сертификатов RSA

Для генерации ключевой пары в терминале введите следующую команду:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so --label "название_ключа" --keypairgen --key-type rsa:2048 -l --id 45
```

Далее создайте самоподписанный сертификат следующими командами:

```
openssl
 OpenSSL> engine dynamic -pre SO_PATH:/usr/lib64/openssl-1.0.0/engines/libpkcs11.so -pre ID:pkcs11 -pre LIST_ADD:1 -pre LOAD -pre MODULE_PATH:/usr/lib64/librtpkcs11ecp.so
 OpenSSL> req -engine pkcs11 -new -key 0:45 -keyform engine -x509 -out cert.crt -outform DER
```

Поместите сертификат на токен

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l -y cert -w cert.crt -a "Имя_сертификата_в_токене" --id 45
```

Проверьте, что токен подключен и на нем имеются сертификаты с ключами:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -O -l
```

Создание ключей и сертификатов ГОСТ-2012

Для генерации ключевой пары в терминале введите команду:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so --keypairgen --key-type GOSTR3410-2012-512:A -l --id 4142
```

Далее создайте самоподписанный сертификат:

Чтобы использовать id ключевой пары, созданной через утилиту pkcs11-tool, в OpenSSL – необходимо использовать hex-символы из таблицы ASCII, соответствующие этим кодам. Например: для `--id 3132` в OpenSSL надо указывать `pkcs11:id=12`. (Для удобства можно воспользоваться удобными онлайн-сервисами конвертации строк в ASCII-коды, например: https://www.rapidtables.com/convert/number/ascii-to-hex.html)

```
openssl req -utf8 -x509 -keyform engine -key "pkcs11:id=12" -engine rtengine -out cert.cer
```

Поместите сертификат на токен с помощью команды:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l -y cert -w cert.crt -a "Имя_сертификата_в_токене" --id 3132
```

Проверьте, что токен подключен и на нем имеются сертификаты с ключами:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -O -l
```

Добавление сертификата в доверенные

Для добавления сертификата в доверенные создайте базу данных доверенных сертификатов, используя следующие команды (для данного действия требуются права

администратора) (Рисунок 81):

```
sudo -i
mkdir /etc/pam_pkcs11/nssdb
chmod 0644 /etc/pam_pkcs11/nssdb
certutil -d /etc/pam_pkcs11/nssdb -N (создание базы данных)
modutil -dbdir /etc/pam_pkcs11/nssdb/ -add p11-kit-trust -libfile /usr/lib64/pkcs11/p11-kit-trust.so (утилита потребует отключить браузер)
```

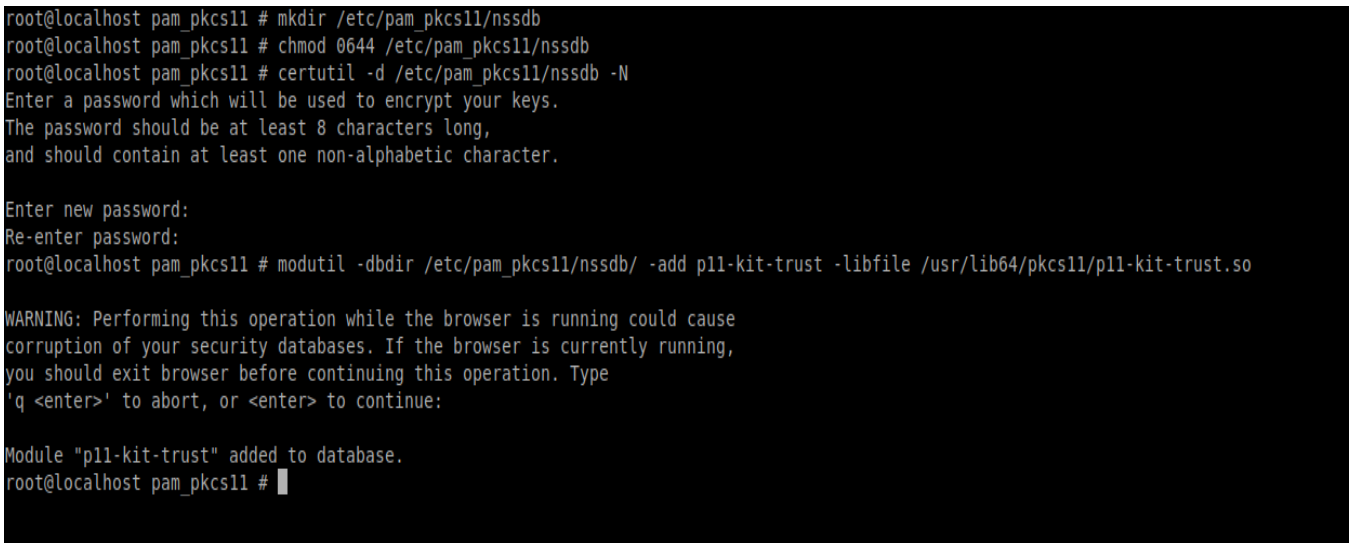


Рисунок 81

Скопируйте сертификат с токена (требуется пароль токена. Параметр `ID` можно взять из вывода команды `pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -O -l`):

```
pkcs11-tool --module=/usr/lib64/librtpkcs11ecp.so -l -r -y cert -d <ID> -o cert.crt
```

Данная команда запишет сертификат в текущую директорию как cert.crt (Рисунок Рисунок 82):

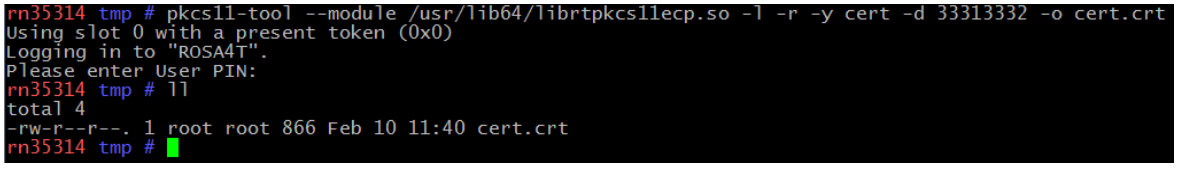


Рисунок 82

Далее добавьте сертификат в доверенные (требуются права администратора):

```
sudo -i
cp cert.crt /etc/pki/ca-trust/source/anchors/ (команда вводится из директории, в которую был помещен сертификат)
update-ca-trust force-enable
```

```
update-ca-trust extract (может занять некоторое время)
```

Изменение конфигурационных файлов

Для изменения конфигурационных файлов потребуются права администратора.

pam_pkcs11.conf

1. Создайте (например, на рабочем столе) текстовый файл `pam_pkcs11.conf` со следующим содержимым:

```
pam_pkcs11 {
 nullok = false;
 debug = true;
 use_first_pass = false;
 use_authtok = false;
 card_only = false;
 wait_for_card = false;
 use_pkcs11_module = rutokenecp;

 # Aktiv Rutoken ECP
 pkcs11_module rutoken{
  module = /usr/lib64/librtpkcs11ecp.so;
  slot_num = 0;
  support_thread = true;
  ca_dir = /etc/pam_pkcs11/cacerts;
  crl_dir = /etc/pam_pkcs11/crls;
  cert_policy = signature;
 }

 use_mappers = subject;

 mapper_sex86_64_path = /usr/lib64/pam_pkcs11;

 mapper subject {
    debug = true;
    module = internal;
    ignorecase = false;
    mapfile = file:///etc/pam_pkcs11/subject_mapping;
 }
```

```
}
```

2. Поместите файл в каталог `/etc/pam_pkcs11/`:

```
cd /etc/pam_pkcs11/
sudo -i (получение прав администратора)
mv pam_pkcs11.conf pam_pkcs11.conf.default (резервное копирование)
mkdir cacerts crls
cp /home/<имя_пользователя>/Desktop/pam_pkcs11.conf /etc/pam_pkcs11/
system-auth
```

3. Подключите модуль к системе авторизации PAM, получите права администратора:

```
sudo -i
```

4. Откройте файл system-auth в текстовом редакторе:

```
nano /etc/pam.d/system-auth
```

5. Добавьте в открывшемся файле вверху следующую строку:

```
auth sufficient pam_pkcs11.so pkcs11_module=/usr/lib64/librtpkcs11ecp.so debug
```

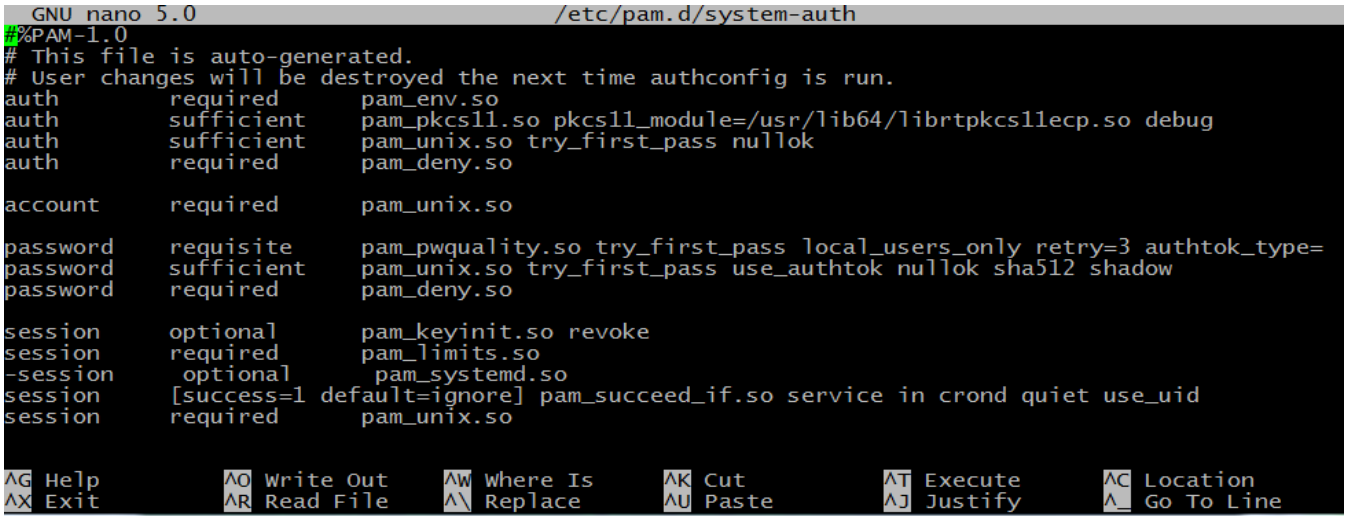


Рисунок 83

6. Сохраните файл (<Ctrl+O>) и закройте редактор (<Ctrl+X>).

subject_mapping

Выполните команды:

```
su
pkcs11_inspect
```

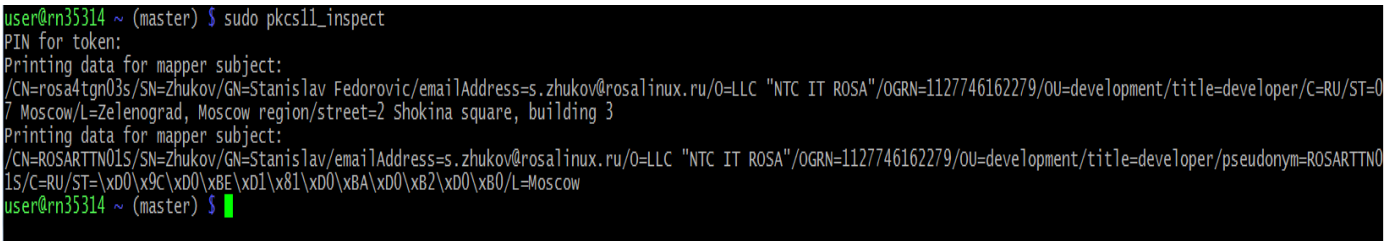


Рисунок 84

Скопируйте вывод предыдущей команды в файл /etc/pam_pkcs11/subject_mapping и укажите, какому пользователю принадлежит сертификат.

Строка конфигурации имеет вид:

`Вывод команды pkcs11_inspect -> <имя_пользователя>`

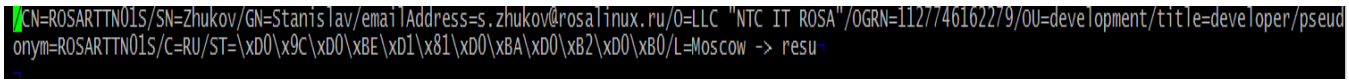


Рисунок 85

Проверка аутентификации через консоль

1. Откройте новое окно или вкладку консоли.
2. Выполните команду

`su <имя_пользователя>`

Имя пользователя указано в файле subject_mapping.

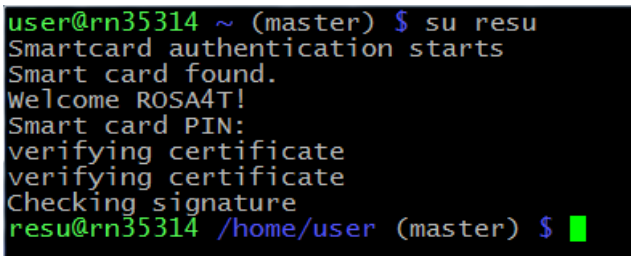


Рисунок 86

После проверки работы аутентификации через консоль можно убрать режим отладки. Для этого в файле /etc/pam.d/sysauth в добавленной строке уберите слово `debug`, а в файле /etc/pam_pkcs11/pam_pkcs11.conf поставьте напротив `debug` параметр `false` вместо `true`.

Для получения дополнительной информации по устройствам Rutoken обратитесь к официальному сайту https://rutoken.ru, который содержит большой объем справочной информации об устройствах, а также к сайту https://dev.rutoken.ru - порталу разработчиков Rutoken, который содержит техническую информацию об устройствах Rutoken и руководства по их интеграции.

5.3.6. Локальная двухфакторная аутентификация с помощью смарт-карт JaCarta ЭЦП

Перед настройкой рекомендуется ознакомиться с актуальными материалами от производителя JaCarta (Компания "Аладдин Р.Д." (с официального сайта www.aladdin-rd.ru)).

Установка компонентов

Установите требуемые утилиты, для этого требуются права администратора:

```
sudo -i
dnf install ccid opensc pam_pkcs11 pam_pkcs11-tools p11-kit-trust
```

Установите библиотеку PKCS#11 для JaCarta (важно устанавливать библиотеку после установки утилит):

1. Перейдите на сайт JaCarta (www.aladdin-rd.ru), далее перейдите во вкладку Центр загрузки.
2. Откройте вкладку из списка «Linux» и перейдите по ссылке ПК "Единый Клиент JaCarta" 2.13 Beta (версия для AlterOS, CentOS 7/8, РОСА "КОБАЛЬТ" 7.3, ROSA ENTERPRISE LINUX 7.3) | Центр загрузки (aladdin-rd.ru).
3. Скачайте и установите пакет (требуется пароль администратора). Текущая версия архива (2021-02-09 jacartauc_2.13.0.3084_centOS_x64_ru.zip) содержит скрипт уставки (install.sh) с импортом ключа RPM-GPG-KEY-ALADDIN_RD-ZAO.public, который нужно отредактировать, добавив инструкцию --skip-broken в строку установки пакетов.

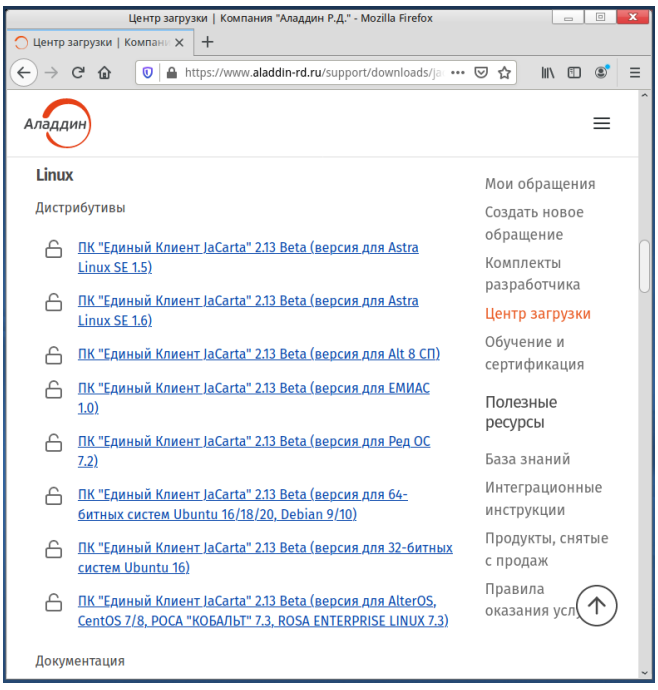


Рисунок 87

Настройка JaCarta

Для проверки отображения устройства в системе и наличия на нем необходимой информации используйте команду (требуются права администратора) (Рисунок Рисунок 88)

```
sudo pcsc_scan
```

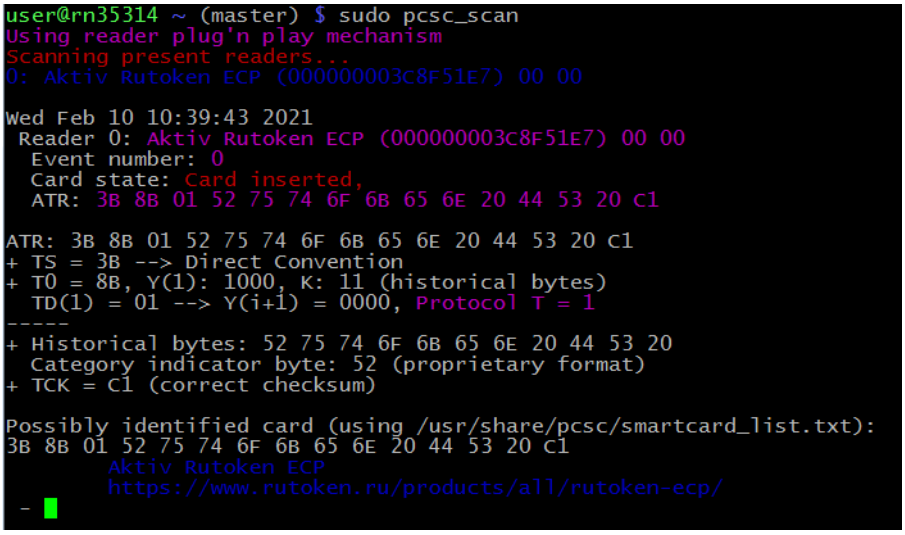


Рисунок 88

Запустите `pcscd` (требуются права администратора):

```
sudo -i
```

Завершите существующий процесс `pcscd`, если таковой имелся:

```
killall pcscd
```

С этого момента токен должен быть вставлен в соответствующий разъем.

Далее выполните:

```
pcscd -adfffff
```

Откройте отдельную вкладку или окно терминала и выполните в ней следующую команду:

```
pkcs11-tool --module /usr/lib64/libjcPKCS11-2.so -T
```

В выводе (Рисунок 89) должны быть видны параметры и название устройства.

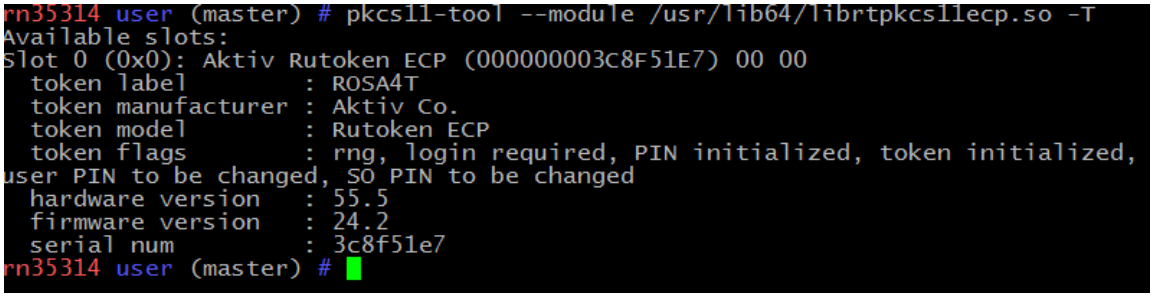


Рисунок 89

Проверьте наличие необходимой информации на токене при помощи следующей

команды (требуется пароль от токена):

```
pkcs11-tool --module /usr/lib64/libjcPKCS11-2.so -O -l
```

В выводе обязан присутствовать `Certificate Object`. Такие параметры, как `ID` и `label`, могут отличаться от Рисунок 90.

```
rn35314 user (master) # pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -O -l
Using slot 0 with a present token (0x0)
Logging in to "ROSA4T".
Please enter User PIN:
Public Key Object; unknown key algorithm 3560050691
  label:
  ID:         33313332
  Usage:      verify
Private Key Object; unknown key algorithm 3560050691
  label:      rosa4tgn03
  ID:         33313332
  Usage:      sign, derive
Public Key Object; RSA 2048 bits
  label:      ROSARTTN01
  ID:         4331746e61705871
  Usage:      encrypt, verify, wrap
Private Key Object; RSA
  label:      ROSARTTN01
  ID:         4331746e61705871
  Usage:      decrypt, sign, unwrap
Certificate Object, type = X.509 cert
  label:      Rutoken Plugin
  ID:         33313332
Certificate Object, type = X.509 cert
  label:      Rutoken Plugin
  ID:         4331746e61705871
rn35314 user (master) #
```

Рисунок 90

Добавление сертификата в доверенные

Для добавления сертификата в доверенные создайте базу данных доверенных сертификатов (требуются права администратора):

```
sudo -i
mkdir /etc/pam_pkcs11/nssdb
chmod 0644 /etc/pam_pkcs11/nssdb
certutil -d /etc/pam_pkcs11/nssdb -N (создание базы данных)
modutil -dbdir /etc/pam_pkcs11/nssdb/ -add p11-kit-trust -libfile /usr/lib64/pkcs11/p11-kit-trust.so (утилита потребует отключить браузер)
```

```
root@localhost pam_pkcs11 # mkdir /etc/pam_pkcs11/nssdb
root@localhost pam_pkcs11 # chmod 0644 /etc/pam_pkcs11/nssdb
root@localhost pam_pkcs11 # certutil -d /etc/pam_pkcs11/nssdb -N
Enter a password which will be used to encrypt your keys.
The password should be at least 8 characters long,
and should contain at least one non-alphabetic character.

Enter new password:
Re-enter password:
root@localhost pam_pkcs11 # modutil -dbdir /etc/pam_pkcs11/nssdb/ -add p11-kit-trust -libfile /usr/lib64/pkcs11/p11-kit-trust.so

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

Module "p11-kit-trust" added to database.
root@localhost pam_pkcs11 #
```

Рисунок 91

Скопируйте сертификат с токена (требуется пароль токена). Параметр ID можно взять из вывода команды:

`pkcs11-tool --module /usr/lib64/libjcPKCS11-2.so -O -l):`

`pkcs11-tool --module=/usr/lib64/libjcPKCS11-2.so -l -r -y cert -d <ID> -o cert.crt`

Данная команда запишет сертификат в текущую директорию как cert.crt (Рисунок 92)

```
rn35314 tmp # pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l -r -y cert -d 33313332 -o cert.crt
Using slot 0 with a present token (0x0)
Logging in to "ROSA4T".
Please enter User PIN:
rn35314 tmp # ll
total 4
-rw-r--r--. 1 root root 866 Feb 10 11:40 cert.crt
rn35314 tmp #
```

Рисунок 92

Далее добавьте сертификат в доверенные (требуются права администратора):

`su`

`cp cert.crt /etc/pki/ca-trust/source/anchors/` (команда вводится из директории, в которую был помещен сертификат)

`update-ca-trust force-enable`

`update-ca-trust extract` (может занять некоторое время)

Изменение конфигурационных файлов

Для изменения конфигурационных файлов потребуются права администратора.

pam_pkcs11.conf

1. Создайте (например, на рабочем столе) текстовый файл pam_pkcs11.conf со следующим содержимым:

```
pam_pkcs11 {
 nullok = false;
```

```
 debug = true;
 use_first_pass = false;
 use_authtok = false;
 card_only = false;
 wait_for_card = false;
 use_pkcs11_module = jacartaecp;

 # Aktiv JaCarta ECP
 pkcs11_module jacartaecp {
  module = /usr/lib64/libjcPKCS11-2.so;
  slot_num = 0;
  support_thread = true;
  ca_dir = /etc/pam_pkcs11/cacerts;
  crl_dir = /etc/pam_pkcs11/crls;
  cert_policy = signature;
 }

 use_mappers = subject;

 mapper_sex86_64_path = /usr/lib64/pam_pkcs11;

 mapper subject {
    debug = true;
    module = internal;
    ignorecase = false;
    mapfile = file:///etc/pam_pkcs11/subject_mapping;
 }
}
```

2. Поместите файл в каталог /etc/pam_pkcs11/:

```
cd /etc/pam_pkcs11/
sudo -i (получение прав администратора)
mv pam_pkcs11.conf pam_pkcs11.conf.default (резервное копирование)
mkdir cacerts crls
cp /home/<имя_пользователя>/Desktop/pam_pkcs11.conf /etc/pam_pkcs11/
```

system-auth

1. Подключите модуль к системе авторизации PAM и получите права администратора командой:

```
su <имя_пользователя>
```

2. Откройте файл `system-auth` в текстовом редакторе (например mcedit или nano):

```
nano /etc/pam.d/system-auth
```

3. Добавьте в открывшийся файл вверху следующую строку:

```
auth      sufficient                                pam_pkcs11.so
pkcs11_module=/usr/lib64/libjcPKCS11-2.so debug
```

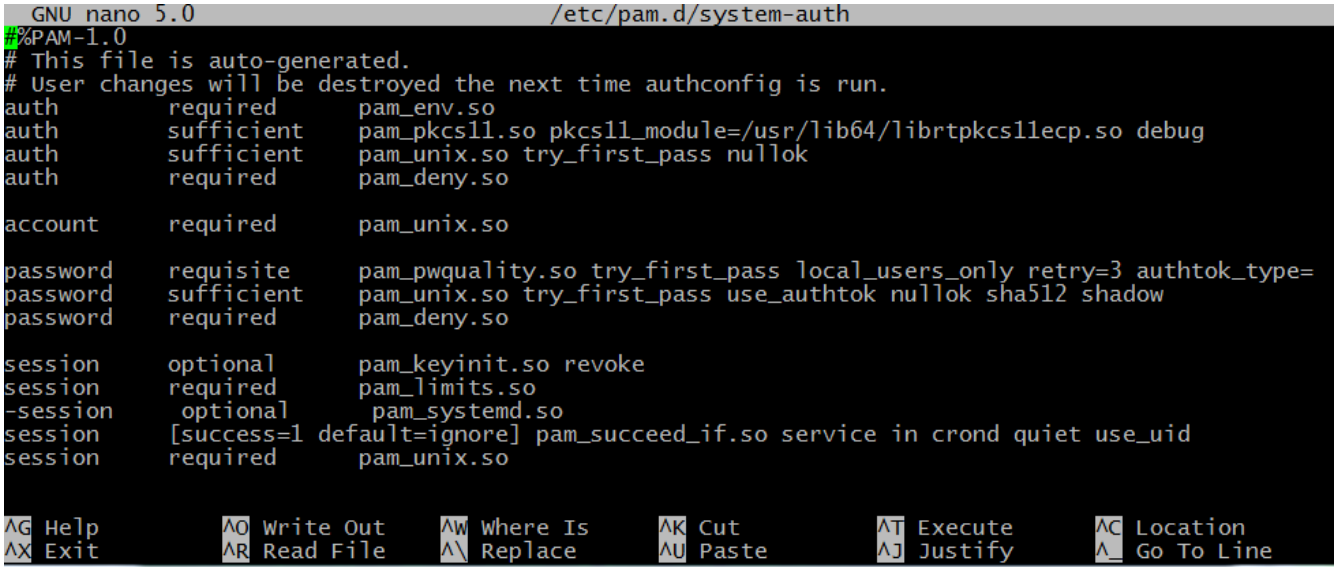


Рисунок 93

4. Сохраните файл (<Ctrl+O>) и закройте редактор (<Ctrl+X>).

subject_mapping

Выполните команды:

```
sudo -i
pkcs11_inspect
```

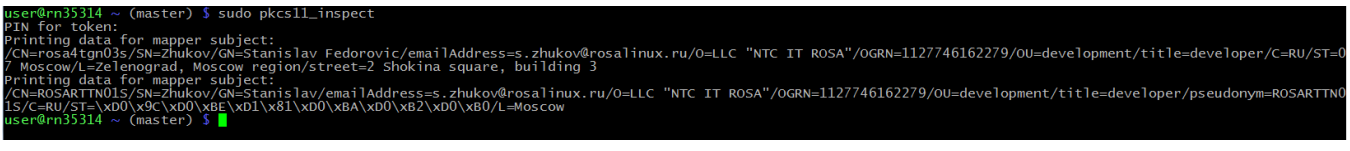


Рисунок 94

Скопируйте вывод предыдущей команды в файл /etc/pam_pkcs11/subject_mapping и укажите, какому пользователю принадлежит сертификат.

Строка конфигурации имеет следующий вид:

```
Вывод команды pkcs11_inspect -> <имя_пользователя>
```

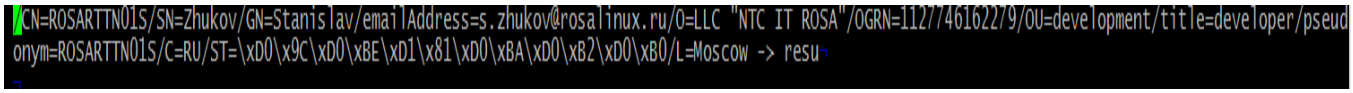


Рисунок 95

Для проведения проверки аутентификации через консоль откройте новое окно или вкладку консоли. Далее выполните команду:

```
su <имя_пользователя>
```

Имя пользователя указано в файле subject_mapping.

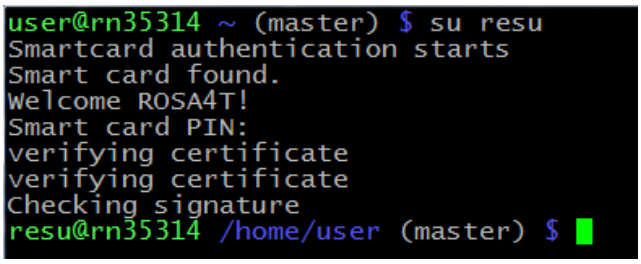


Рисунок 96

После проверки работы аутентификации через консоль можно убрать режим отладки. Для этого в файле `/etc/pam.d/sysauth` в добавленной строке уберите слово `debug`, а в файле /etc/pam_pkcs11/pam_pkcs11.conf поставьте напротив `debug` параметр `false` вместо `true`.

Создание ключей и сертификатов RSA

Для генерации ключевой пары в терминале следует ввести команду:

```
pkcs11-tool --module /usr/lib64/libjcPKCS11-2.so --label "название_ключа" --keypairgen --key-type rsa:2048 -l --id 45
```

Далее создаем самоподписанный сертификат:

```
openssl
OpenSSL> engine dynamic -pre SO_PATH:/usr/lib64/openssl-1.0.0/engines/libpkcs11.so -pre ID:pkcs11 -pre LIST_ADD:1 -pre LOAD -pre MODULE_PATH:/usr/lib64/libjcPKCS11-2.so

OpenSSL> req -engine pkcs11 -new -key 131071:45 -keyform engine -x509 -out cert.crt -outform DER
```

Номер слота указывается в десятичной системе счисления. Число 131071 в шестнадцатеричной системе = 0x1ffff.

Для того чтобы поместить слот на токен воспользуйтесь следующими командами:

```
pkcs11-tool --module /usr/lib64/libjcPKCS11-2.so -l -y cert -w cert.crt -a "Имя_сертификата_в_токене" --id 45
```

Проверьте, что токен подключен и сертификаты с ключами на нем имеются.

```
pkcs11-tool --module /usr/lib64/libjcPKCS11-2.so -O -l
```

Создание ключей и сертификатов ГОСТ-2012

Для генерации ключевой пары в терминале следует ввести команду:

```
pkcs11-tool --module /usr/lib/ libjcPKCS11-2.so --keypairgen --key-type GOSTR3410-2012-512:A -l --id 3132
```

Теперь создайте самоподписанный сертификат:

Чтобы использовать этот id ключевой пары, созданной через pkcs11-tool, в OpenSSL – надо использовать hex-символы из таблицы ASCII, соответствующие этим кодам. Например: для `--id 3132` в OpenSSL надо указывать `pkcs11:id=12`.

```
openssl req -utf8 -x509 -keyform engine -key "pkcs11:id=12" -engine (libjckt2) -out cert.cer
```

Далее поместите его на токен:

```
pkcs11-tool --module /usr/lib64/libjcPKCS11-2.so -l -y cert -w cert.crt -a "Имя_сертификата_в_токене" --id 3132
```

Проверьте, что токен подключен и на нем имеются сертификаты с ключами с помощью команды:

```
pkcs11-tool --module /usr/lib64/libjcPKCS11-2.so -O -l
```

Для получения дополнительных источников информации обратитесь к официальному сайту JaCarta.

6. РАБОТА В ТЕРМИНАЛЬНОМ РЕЖИМЕ

6.1. Графический и текстовый режимы

В ОС РОСА «НИКЕЛЬ» (и любом другом дистрибутиве Linux) пользователю доступны два режима работы — графический и текстовый (консольный). В текстовом режиме работа осуществляется путем выполнения вводимых с клавиатуры команд, а графика в привычном смысле этого слова недоступна. В вашем распоряжении будут только текстовые и псевдографические символы и несколько десятков базовых цветов. Тем не менее, в текстовом режиме можно выполнять практически любые действия, в том числе и те, которые нельзя осуществить через графический интерфейс. Текстовый режим — это мощный и гибкий инструмент управления системой.

Бывают ситуации, когда графический режим недоступен или неработоспособен (удаленный доступ по сети, проблемы с поддержкой видеокарты, сбои системы и т. п.). В таких случаях всегда остается возможность работать в текстовом режиме, поскольку он не требует специальных драйверов или настройки.

Предположим, что загрузка системы по каким-либо причинам не дошла до графического режима и завершилась вот таким приглашением к регистрации:

```
login:
```

В этом случае можно попробовать запустить графический режим вручную. Для этого следует ввести имя пользователя и пароль, а затем выполнить команду

```
startx
```

Для ввода информации и выполнения набранной команды используется клавиша <Enter>.

Если после того, как вы это проделали, на экране появилась привычная графическая оболочка, знайте: до этого момента вы работали в терминале с командной строкой.

6.2. Терминал

Слово «терминал» даже в компьютерном мире имеет множество значений. Изначально так называли рабочее место, состоящее из монитора и клавиатуры, соединенных с центральным сервером (мейнфреймом). В ОС семейства Linux под терминалом теперь чаще всего подразумевают окно, в котором можно взаимодействовать с системой и приложениями, набирая те или иные команды.

Если система запущена в текстовом режиме, таким «окном» будет весь экран монитора. В графическом режиме открыть терминал можно, например, щелкнув по значку *Konsole* на панели приложений SimpleWelcome. Такой терминал будет виртуальным, созданным в рамках графического режима эмулятором терминала, но это не имеет значения —будут доступны все возможности консольного режима.

Приглашение командной строки

Приглашение представляет собой фрагмент текста в начале строки. По умолчанию он включает имена пользователя и ПК, например, так:

```
[user@computer- ~]$
```

Приглашение может быть оформлено по-разному, но обычно оно заканчивается символом `$`. Пока не нажата клавиша <Enter>, набранную команду можно редактировать. Если для выполнения команды требуются полномочия системного администратора, для разграничения приветствия и команды вместо `$` используется символ `#`.

Выполнение команд

Команда чаще всего является именем исполняемого файла — программы, которую требуется вызвать. Далее могут быть указаны дополнительные параметры.

Вызовите терминал и попробуйте выполнить команду date просто так и с параметром `-u`, предписывающим выводить время по Гринвичу (UTC). В процессе выполнения команды система может отображать те или иные сообщения; в данном случае на экране должны появиться текущие дата и время. Когда выполнение завершено, вновь выводится приглашение командной строки.

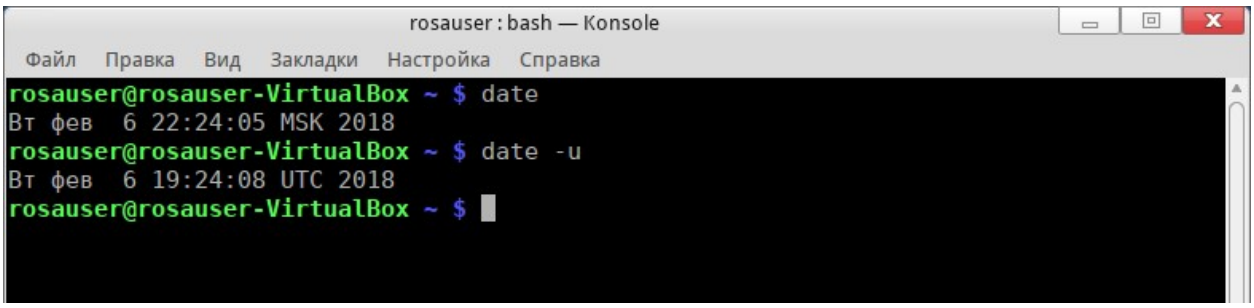


Рисунок 97. Выполнение команды date

Команда `clear` («очистить») сотрет предыдущие команды и результаты их выполнения, а `exit` («выйти») закроет окно терминала. При работе в текстовом режиме команда `exit` завершает сеанс работы текущего пользователя, и другой пользователь может зарегистрироваться в системе. Конечно, эмулятор терминала, как и любое окно, можно закрыть с помощью графического интерфейса, щелкнув мышью по крестику в правом верхнем углу окна.

Обычно работать в графической среде удобнее, но знание команд текстового

режима никогда не будет лишним.

Нередко к командной строке обращаются, например, инженеры службы поддержки. Указать команду, которая даст нужный результат, гораздо проще и надежнее, чем описывать действия, которые нужно произвести для достижения того же эффекта в графическом интерфейсе.

6.3. Команды для работы с файлами

ls — вывести содержимое каталога

```
ls [ключ] ... [файл]
```

Команда `ls` выводит информацию о файлах. Если в параметрах указан конкретный файл — только об этом файле, если указан каталог — о файлах этого каталога, если ничего не указано — о файлах текущего каталога.

Команду можно выполнять с множеством разных ключей, некоторые из которых рассматриваются ниже. Полный их список и справку по команде (не только ls) можно получить с помощью ключа `–help`.

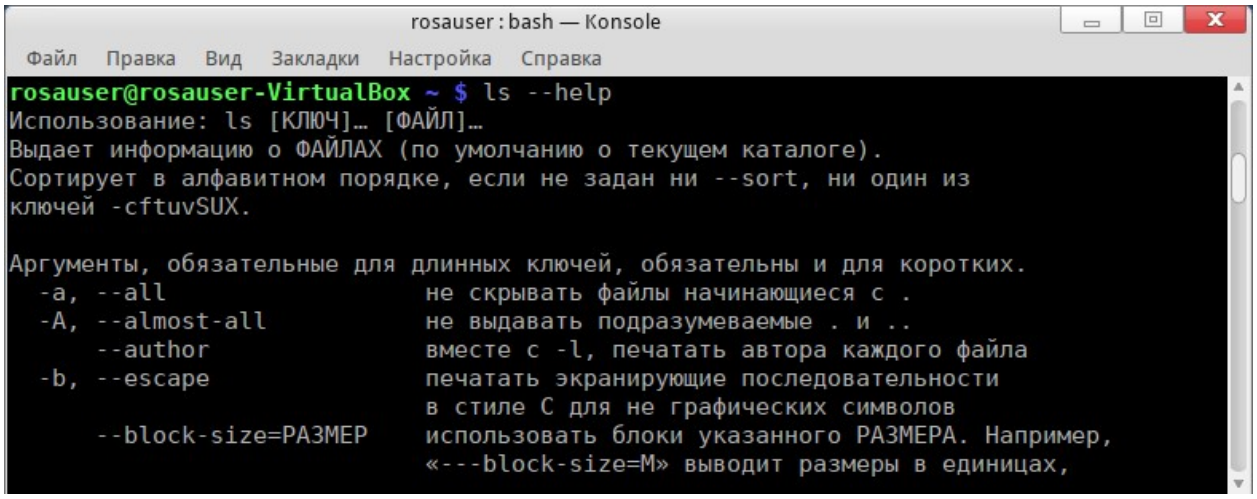


Рисунок 98. Использование ключа –help

- `-R` — выводить содержимое каталога и всех его подкаталогов рекурсивно. Обратите внимание, что перед отображением содержимого каталога выводится имя самого каталога;
- `-l` — использовать подробный формат вывода. Отображается детальная информация о файле: тип файла, права доступа, владелец и размер;
- `-a` — показывать скрытые файлы. В UNIX-подобных системах файлы с именами, начинающимися с точки (.), являются скрытыми. Ключ используется, чтобы показать такие файлы при отображении содержимого каталога. Если вы не хотите, чтобы выводились ссылки на текущий и родительский каталоги (. и .., соответственно),

пользуйтесь опцией -A (как видите, регистр имеет значение).

Примеры:

```
ls -lA /tmp/movies /tmp/images
```

В результате выполнения этой команды в окно терминала будет выведено содержимое подкаталогов `movies` и `images`, находящихся в каталоге `/tmp`, с отображением скрытых файлов и детальной информации, но без показа каталогов . и ..;

```
ls -R ~/
```

В окно терминала будут рекурсивно выведены все файлы и каталоги, которые располагаются внутри вашего домашнего каталога.

cp — копировать

```
cp [ключ] ... <источник> <назначение>
```

Часто используемые ключи:

- `-R`: рекурсивное копирование; ключ обязателен для копирования каталога, даже если он пуст;
- `-f`: заменять имеющиеся файлы без запроса подтверждения. Пользуйтесь с осторожностью;
- `-a`: архивный режим. Сохраняет все атрибуты файлов для копии и производит рекурсивное копирование;
- `-v`: подробный режим. В терминал выводится информация обо всех действиях, совершаемых командой `cp`.

Примеры:

```
cp -f /tmp/images/* images/
```

Эта команда копирует все файлы каталога `/tmp/images` в каталог images, расположенный в текущем каталоге. Если какой-то файл при этом должен быть перезаписан, запрос не выдается.

```
cp -vR docs/ /shared/mp3s/* mystuff/
```

Эта команда копирует весь каталог `docs` и все файлы из каталога `/shared/mp3s` в каталог `mystuff`, выводя информацию обо всех производимых действиях.

```
cp foo bar
```

Эта команда создает в текущем каталоге копию файла `foo` под именем `bar`.

mv — переместить

```
mv [ключ] ... <источник> <назначение>
```

Обратите внимание, что при перемещении нескольких файлов место назначения должно быть каталогом. Также эта команда используется для переименования файлов; технически они перемещаются, получая новое имя в текущем каталоге.

Часто используемые ключи:

- `-f`: не предупреждать при перезаписи файлов. Пользуйтесь с осторожностью;
- `-v`: выводить сообщения обо всех изменениях и действиях.

Примеры:

```
mv /tmp/pics/*.png
```

Эта команда перемещает все файлы из каталога `/tmp/pics`, чьи имена заканчиваются на `.png`, в текущий каталог.

```
mv foo bar
```

Эта команда переименовывает файл `foo` в `bar`. Если при этом существует каталог `bar`, в результате выполнения этой команды файл `foo` или весь каталог `foo` (сам каталог, а также все файлы и каталоги внутри него, рекурсивно) переместятся в каталог `bar`.

```
mv -vf file* images/ trash/
```

Эта команда перемещает без запроса на перезапись все файлы из текущего каталога, чьи имена начинаются на `file`, вместе со всем каталогом `images` в каталог trash, выводя информацию обо всех производимых действиях.

rm — удалить

```
rm [ключ]... <файл|каталог>...
```

Часто используемые ключи:

- `-r` или `-R` — удалять рекурсивно. Ключ необходим при удалении каталогов, как пустых, так и непустых (для удаления пустых каталогов можно пользоваться и командой `rmdir`);
- `-f` — принудительное удаление файлов или каталогов. Используйте эту опцию с осторожностью.

Примеры:

```
rm images/*.jpg file1
```

Эта команда удаляет все файлы с именами, заканчивающимися на `.jpg`, из каталога `images` и удаляет файл `file1` из текущего каталога.

```
rm -Rf images/misc/ file*
```

Эта команда удаляет, не спрашивая подтверждения, весь каталог `misc` из каталога `images`, вместе со всеми файлами текущего каталога, чьи имена начинаются на `file`.

Команда `rm` удаляет файлы не в корзину, а безвозвратно. Будьте особенно

внимательны при использовании опции `-f`, при которой пропускается запрос на удаление.

mkdir — создать каталог

```
mkdir [ключ] ... <каталог> ...
```

Отметим ключ `-p`, который при необходимости создает сразу всю цепочку родительских каталогов (если их еще нет). Кроме того, ключ убирает сообщение об ошибке при попытке создать уже существующий каталог.

Примеры:

```
mkdir foo
```

Эта команда создает каталог `foo` в текущем каталоге.

```
mkdir -p images/misc
```

Эта команда создает каталог `misc` в каталоге `images`. В случае отсутствия последнего он тоже будет создан.

cd — сменить текущий каталог

```
cd [ключ] <каталог>
```

Текущий каталог, обозначаемый точкой (.), это место ФС, где вы «находитесь». Если не указано иное, команды выполняют свои действия применительно к текущему каталогу.

Двойная точка (..) обозначает каталог, родительский для текущего, который расположен одним уровнем выше в иерархии ФС.

Примеры:

```
cd /tmp/images
```

Эта команда выполнит переход в каталог images, расположенный внутри каталога `/tmp`.

```
cd -
```

Эта команда сменит текущий каталог на предыдущий рабочий каталог.

```
cd
```

Эта команда сменит текущий каталог на домашний каталог.

```
cd ~/images
```

Эта команда сменит текущий каталог на каталог images, расположенный внутри вашего домашнего каталога.

6.4. Команды для управления процессами

С точки зрения системы приложения выполняются в одном или нескольких

процессах, которые потребляют системные ресурсы — память и процессорное время. Опишем некоторые команды для отслеживания процессов и управления ими, а следовательно, и приложениями, которым они принадлежат.

ps — получить информацию о процессах

Команда `ps` выдает, согласно указанному критерию, список процессов, которые выполняются в системе в настоящий момент.

Запуск `ps` без аргументов покажет только те процессы, которые были запущены и привязаны к используемому терминалу.

Часто используемые ключи:

- `-a` — отображает процессы, запущенные всеми пользователями;
- `-x` — отображает процессы, запущенные со всех терминалов (и даже те, что не имеют терминала), а не только с вашего;
- `-u` — для каждого процесса отображается имя пользователя, запустившего процесс, и время, когда он был запущен.

kill, killall — остановить процессы

Процессы управляются сигналами. Команды `kill` и `killall` используются для того, чтобы посылать эти сигналы процессам. Разные процессы по-разному реагируют на одни и те же сигналы.

```
kill <номер_процесса>
killall <имя_процесса>
```

Команда `kill` требует в качестве аргумента номер процесса, а команда `killall` — его имя.

Сигналы можно указывать по имени или по номеру. Чтобы увидеть список доступных сигналов, используйте команду `kill -l`. Наиболее употребляемые сигналы и их номера:

`TERM` или `15`

Этот сигнал посылается по умолчанию, если имя или номер сигнала не заданы. Используется для остановки процесса.

`STOP` или `19`

Этот сигнал используется для временной приостановки процесса. Для возобновления работы следует послать сигнал `CONT` или 18.

`KILL` или `9`

Этот сигнал используется для принудительного прерывания процесса. Его часто используют, когда процесс больше ни на что не отвечает («заморожен»). Прекращение

работы происходит мгновенно.

Примеры:

```
kill 785
```

Эта команда просит процесс под номером 785 завершить работу, дав ему шанс произвести все требуемые завершающие действия.

```
kill -KILL 785
```

Эта команда вынуждает процесс под номером 785 завершиться, не предоставляя ему никаких возможностей произвести завершающие операции. Процесс прекращает работу немедленно.

```
killall -TERM make
```

Эта команда просит прекратить работу все процессы по имени make, запущенные текущим пользователем.

Пользователь может контролировать только свои процессы и не способен повлиять на выполнение процессов других пользователей. Такой способностью обладают только администраторы системы.

top — утилита для управления процессами

Работа с утилитой `top` отличается от простого выполнения команд в терминале. Она запускается как программа и далее управляется с клавиатуры. Работает она исключительно в текстовом режиме.

Утилита `top` используется как для отслеживания процессов в реальном времени, так и для управления ими. Она умеет выдавать информацию об использовании ресурсов процессора и памяти, времени выполнения процессов и др.

При нажатии клавиш обращайте внимание на регистр. Наиболее востребованные клавиши:

- `<h>` — вызвать справку;
- `<k>` — послать сигнал процессу. Будет запрошен PID процесса, после которого следует ввести номер или имя посылаемого сигнала (по умолчанию это `TERM` или `15`);
- `<M>` — упорядочить вывод процессов по объему потребляемой памяти (поле `%MEM`);
- `<P>` — упорядочить вывод процессов по потребляемому процессорному времени (поле `%CPU`).
- `<u>` — вывести процессы конкретного пользователя. Нужно будет ввести имя пользователя (не UID). Если имя не введено, будут показаны все процессы;

- `<i>` — вывести только выполняющиеся процессы (процессы, поле STAT которых показывает `R, Running`). Повторное нажатие этой клавиши возвращает к отображению всех процессов, включая «спящие».

7. УПРАВЛЕНИЕ ДОСТУПОМ

Дистрибутив РОСА «НИКЕЛЬ» поставляется с встроенными средствами разграничения доступа на основе модели SELinux MLS (многоуровневый доступ) с поддержкой модели Белла-Ла-Падулы (мандатный доступ) и набором утилит администратора безопасности, дающих средства для управления режимами и правами как в графическом режиме, так и в режиме терминала.

Субъект-Объектная модель Белла-Ла-Падулы

1) Субъекты: пользователи ОС, процессы, запускаемые от имени пользователей ОС.

2) Объекты: объекты ФС (файлы, каталоги), устройства, сетевые пакеты, сокеты. В роли объектов могут быть и процессы, управляемые другими процессами.

Пусть контекст безопасности субъекта содержит уровень конфиденциальности Ls и категории Cs, а мандатная метка объекта содержит уровень конфиденциальности Lo и категории Co.

Операции сравнения уровней и категорий и доступа субъектов к объектам определяются следующим образом:

1) уровень субъекта Ls меньше уровня объекта Lo (Ls<Lo), если численное значение Ls меньше численного значения Lo;

2) уровень субъекта Ls равен уровню объекта Lo (Ls=Lo), если численные значения Ls и Lo совпадают;

3) категории субъекта Cs включают категории объекта Co (Cs>=Co), если все биты набора категорий Co являются подмножеством набора бит категорий Cs;

4) операция чтения разрешена, если Ls>=Lo и Cs>=Co;

5) операция записи разрешена, если Ls=Lo и Cs>=Co.

В отношении атрибутов доступа действуют следующие правила наследования:

- если в сессии порождаются другие процессы, то они наследуют уровень конфиденциальности и категорию;
- процесс создает объекты только полностью наследуя свой уровень конфиденциальности и категорию.

SELinux

SELinux — это система принудительного контроля доступа, реализованная на уровне ядра.

Сущности SELinux

Домен — список действий, которые может выполнять процесс. Определяется минимально-возможный набор действий, при помощи которых процесс способен функционировать.

Роль — список доменов, которые могут быть применены. Если какого-то домена нет в списке доменов роли, то действия из этого домена не могут быть применены.

Тип — набор действий, которые допустимы по отношения к объекту.

Контекст безопасности — все атрибуты SELinux — роли, типы и домены.

Режимы работы SELinux

Enforcing: Режим по умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.

Permissive: В случае использования этого режима, информация обо всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.

Для отключения принудительного режима работы системы можно воспользоваться одним из следующих способов:

1) В начальном меню загрузки системы войдите в режим редактирования параметров загрузчика grub (для чего при загрузке системы нажмите клавишу E), далее укажите имя пользователя root и пароль root, нажать клавишу F10, далее дописать в параметры ядра параметр enforcing=0 и загрузить систему.

2) Если в системе включен root, необходимо войти под пользователем root в консоль и используя команду

```
# nano /etc/selinux/config
```

отредактировать файл настройки SElinux `/etc/selinux/config`, сменив режим с enforcing на permissive и перезагрузить ОС.

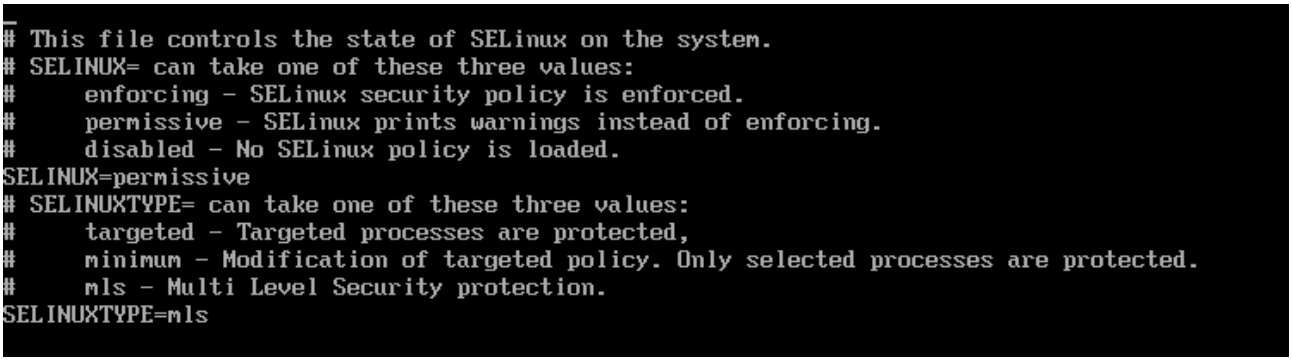


Рисунок 99. Смена режима SELinux

7.1. Назначение контекста безопасности пользователям

В ОС РОСА «НИКЕЛЬ» предусмотрены несколько уровней конфиденциальности для пользователей системы.

Настройка уровня возможна при помощи графических утилит и командами в консоли, после входа в систему с правами администратора и дополнительного ввода его пароля.

Применяемые в системе уровни конфиденциальности при работе с документами и их псевдонимы:

— s0 [Несекретно, Системный, Unclassified, SystemLow]

— s1 [ДСП, Конфиденциально, Classified)]

— s2 [Секретно, Secret]

— s3 [СовершенноСекретно, TopSecret, Полный]

Также могут использоваться другие варианты записей уровней доступа:

— s3:c0.c1023 [СистемныйВысокий, SystemHigh]

— s0-s1 [Несекретно-ДСП, Unclassified-Classified]

— s0-s2 [Несекретно-Секретно, Unclassified-Secret]

— s0-s3 [Несекретно-Сов.Секретно, Unclassified-TopSecret]

— s0-s3:c0.c1023 [Системный-СистемныйВысокий, SystemLow-SystemHigh, Системный-Полный]

В данном случае для отображения будет использоваться только первый псевдоним из списка. Остальные псевдонимы сработают только при их использовании вместо других вариантов, однако, отображаться все равно будет или кодировка, или первый псевдоним из списка.

Пользователь может просматривать документы своего или более низкого уровня, а записывать — свой уровень или уровень выше.

Текущий уровень доступа для каждого пользователя можно посмотреть с помощью значка около системного лотка (Рисунок 100. Просмотр контекста

безопасности). Например, для роли Администратора (sysadm_r) по умолчанию установлен нулевой уровень доступа, также видно, что ему сопоставлен SELinux-пользователь aib_u.

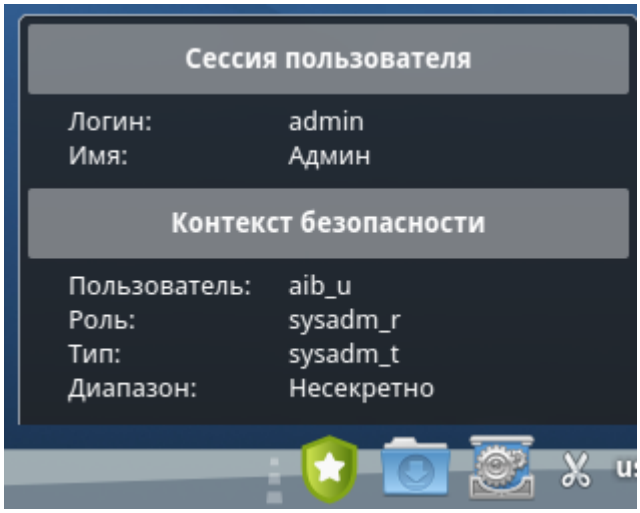


Рисунок 100. Просмотр контекста безопасности

Сопоставление Linux-пользователей с пользователями SELinux, установка для них уровней доступа и другие операции доступны в консоли (с помощью команды `semanage`, а по команде `man` доступно локализованное руководство) и в графической программе [Администрирование SELinux] (Рисунок 101).

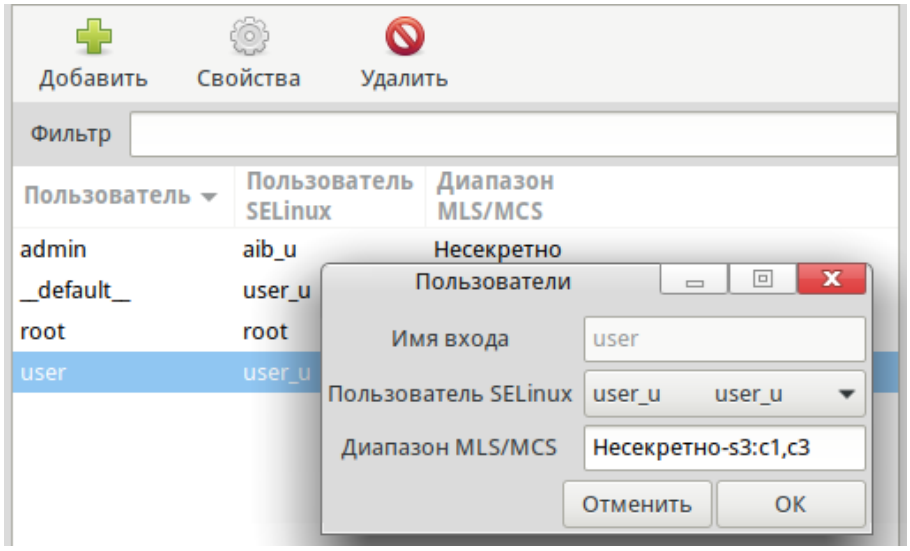


Рисунок 101. Назначение контекста безопасности

Для назначения контекста безопасности в консоли используйте следующую команду:

```
newrole -r secadm_r
sudo semanage login -m -s user_u -r s0-s3:c1,c3 user
```

Здесь для пользователя user установлен полный доступ к документам любой секретности, также указано две категории — c1 и c3.

Проверим результат командой (Рисунок 102. Проверка контекста безопасности):

```
sudo semanage login -l
```

```
admin@localhost ~ $ sudo semanage login -m -s user_u -r s0-s3:c1,c3  user
admin@localhost ~ $ sudo semanage login -l

Имя входа           Пользователь SELinux Диапазон MLS/MCS     Служба

__default__         user_u               Несекретно           *
admin               aib_u                Несекретно           *
root                root                 Несекретно           *
user                user_u               Несекретно-s3:c1,c3  *
admin@localhost ~ $
```

Рисунок 102. Проверка контекста безопасности

После задания контекста безопасности при входе в систему пользователь user сможет выбрать один из доступных ему уровней секретности, включая или исключая категории (Рисунок 103. Выбор контекста безопасности при входе в систему).

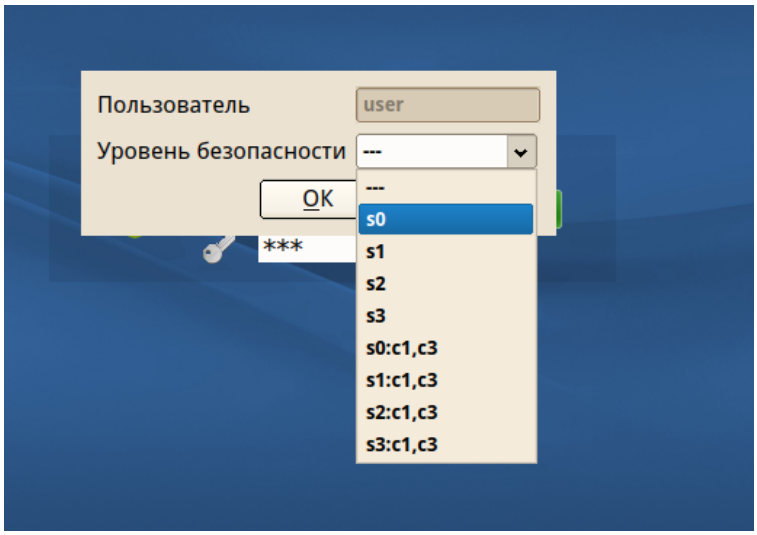


Рисунок 103. Выбор контекста безопасности при входе в систему

1.1.1. Дискреционное управление доступом

Избирательное управление доступом (discretionary access control, DAC) — управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа. Также используются названия дискреционное управление доступом, контролируемое управление доступом и разграничительное управление доступом.

Субъект доступа «Пользователь № 1» имеет право доступа только к объекту доступа № 3, поэтому его запрос к объекту доступа № 2 отклоняется. Субъект «Пользователь № 2» имеет право доступа как к объекту доступа № 1, так и к объекту доступа № 2, поэтому его запросы к данным объектам не отклоняются.

Для каждой пары (субъект — объект) должно быть задано явное и

недвусмысленное перечисление допустимых типов доступа (читать, писать и т. д.), то есть тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу (объекту).

Возможны несколько подходов к построению дискреционного управления доступом:

- Каждый объект системы имеет привязанного к нему субъекта, называемого владельцем. Именно владелец устанавливает права доступа к объекту.
- Система имеет одного выделенного субъекта — суперпользователя, который имеет право устанавливать права владения для всех остальных субъектов системы.
- Субъект с определенным правом доступа может передать это право любому другому субъекту.

1.1.1. Мандатное управление доступом

Мандатное управление доступом (Mandatory access control, MAC) — разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности. Это способ, сочетающий защиту и ограничение прав, применяемый по отношению к компьютерным процессам, данным и системным устройствам и предназначенный для предотвращения их нежелательного использования.

Пример: субъект «Пользователь № 2», имеющий допуск уровня «не секретно», не может получить доступ к объекту, имеющему метку «для служебного пользования». В то же время субъект «Пользователь № 1» с допуском уровня «секретно» право доступа к объекту с меткой «для служебного пользования» имеет.

Мандатная модель управления доступом, помимо дискреционной и ролевой, является основой реализации разграничительной политики доступа к ресурсам при защите информации ограниченного доступа. При этом данная модель доступа практически не используется «в чистом виде», обычно на практике она дополняется элементами других моделей доступа.

Для ФС оно может расширять или заменять дискреционный контроль доступа и концепцию пользователей и групп.

Самое важное достоинство заключается в том, что пользователь не может полностью управлять доступом к ресурсам, которые он создает.

Политика безопасности системы, установленная администратором, полностью определяет доступ, и обычно пользователю не разрешается устанавливать более

свободный доступ к его ресурсам чем тот, который установлен администратором пользователю. Системы с дискреционным контролем доступа разрешают пользователям полностью определять доступность их ресурсов, что означает, что они могут случайно или преднамеренно передать доступ неавторизованным пользователям. Такая система запрещает пользователю или процессу, обладающему определенным уровнем доверия, получать доступ к информации, процессам или устройствам более защищенного уровня. Тем самым обеспечивается изоляция пользователей и процессов, как известных, так и неизвестных системе (неизвестная программа должна быть максимально лишена доверия, и ее доступ к устройствам и файлам должен ограничиваться сильнее).

Очевидно, что система, которая обеспечивает разделение данных и операций в ПК, должна быть построена таким образом, чтобы ее нельзя было «обойти». Она также должна давать возможность оценивать полезность и эффективность используемых правил и быть защищенной от постороннего вмешательства.

7.2. Повышение привилегий (дискреционная политика управления доступом)

Утилита sudo предназначена для выполнения команды от другой учетной записи. Обычно утилита используется для выполнения административных команд с правами администратора (sudo -i). В Таблица 24 приведены часто используемые опции утилиты sudo. Подробное описание приведено в man sudo.

Синтаксис:

```
sudo <опции> <команда>
```

Таблица 24 – Опции утилиты sudo

Опция	Описание
-l	Отображение доступных пользователю команд
-u user	Выполнение команды от имени пользователя, отличного от суперпользователя

Пример использования:

в результате выполнения этой команды произойдет просмотр каталога root с правами администратора:

```
sudo ls /root
```

Утилита su предназначена для выполнения команды от имени другого пользователя. В Таблица 25 приведены часто используемые опции утилиты su. Подробное описание приведено в man su.

Синтаксис:

```
su <опции> <имя учетной записи>
```

Таблица 25 — Опции утилиты su

Опция	Описание
-c command, --command=command	Указание команды, которую необходимо выполнить

Примеры использования:

В результате выполнения этой команды при условии ввода пароля пользователя user1 произойдет вывод содержимого каталога /home/user1 с правами пользователя user1:

```
su -c "ls /home/user1" user1
```

В результате выполнения этой команды при условии ввода пароля пользователя user1 произойдет запуск командной оболочки с правами пользователя user1:

```
su -c "ls /home/user1" user1
```

В результате выполнения этой команды при условии ввода пароля пользователя, выполняющего данную команду, произойдет запуск командной оболочки с правами пользователя user1:

```
sudo su user1
```

В результате выполнения этой команды при условии ввода пароля пользователя, выполняющего данную команду, произойдет запуск командной оболочки с правами суперпользователя:

```
sudo su
```

7.3. Изменение дискреционных атрибутов файлов

7.3.1. Управление правами владения

Управление правами владения файлов и каталогов осуществляется с помощью графического приложения «Dolphin» или с помощью утилит командной строки, описание которых приведено далее.

Приложение «Dolphin» представляет возможность отображения и модификации прав доступа. Полный набор возможностей и описание графического интерфейса приведены в справке приложения. Приложение можно запустить, выбрав пункт меню «Утилиты» → «Dolphin», или используя команду `dolphin`.

Утилита ls для каталога выводит список входящих в этом каталог файлов; для файлов – выводит дополнительную информацию в соответствии с указанными ключами. В приведены часто используемые опции утилиты ls. Подробное описание приведено в

man ls. По умолчанию имена файлов выводятся в алфавитном порядке. Если имена не заданы, выдается содержимое текущего каталога.

Синтаксис:

```
ls <опции> <путь к файлу>
```

Таблица 26 – Опции утилиты ls

Опция	Описание
-a, --all	Вывод файлов, включая скрытые файлы
-l	Вывод полной информации о файлах и каталогах (владелец, группа, права доступа и др.)
-R, --recursive	Вывод информации каталога и его содержимого

Примеры использования: в результате выполнения этой команды произойдет вывод полной информации о файлах и каталогах в каталоге /home:

```
ls -l /home
```

Утилита chown предназначена для изменения владельца и группы файла, каталога. В приведены часто используемые опции утилиты chown. Подробное описание приведено в man chown.

Синтаксис:

```
chown <опции> <владелец:группа> <путь к файлу>
```

Таблица 27 – Опции утилиты chown

Опция	Описание
--reference=RFILE	Указание владельца и/или группы из указанного файла
-R, --recursive	Рекурсивное изменение владельца и/или группы для каталогов и их содержимого

Примеры использования:

В результате выполнения этой команды владельцем файла file1 станет пользователь user1, а группой – группа пользователя user1:

```
# chown user1:user1 file1
```

В результате выполнения этой команды владельцем файла file2 станет пользователь user2:

```
# chown user2 file2
```

В результате выполнения этой команды группой каталога catalog и его файлов станет группа пользователя user2:

```
# chown -R :user2 catalog
```

Утилита chgrp предназначена для изменения группы файла, каталога. В приведены часто используемые опции утилиты chgrp. Подробное описание приведено в man chgrp.

Синтаксис:

```
chgrp <опции> <группа> <путь к файлу>
```

Таблица 28 – Опции утилиты chgrp

Опция	Описание
--reference=RFILE	Указание группы из указанного файла
-R, --recursive	Рекурсивное изменение группы для каталогов и их содержимого

Пример использования: в результате выполнения этой команды группой файла file1 станет группа пользователя user1:

```
# chgrp user1 file1
```

7.3.2. Управление правами доступа

Управление правами доступа осуществляется с помощью графического приложения «Dolphin» или с помощью утилиты командной строки, описание которой приведено далее.

Приложение «Dolphin» представляет возможность отображения и модификации прав доступа. Полный набор возможностей и описание графического интерфейса приведены в справке приложения. Приложение можно запустить, выбрав пункт меню «Утилиты» → «Dolphin», или используя команду dolphin.

Для отображения прав доступа используется утилита ls. Ее описание приведено в 7.3.Изменение дискреционных атрибутов файлов.

Утилита chmod предназначена для изменения режима доступа (прав доступа) к файлам. В приведены часто используемые опции утилиты chmod. Подробное описание приведено в man chmod.

Синтаксис:

```
chmod <опции> <режим> <путь к файлу>
```

Таблица 29 – Опции утилиты chmod

Опция	Описание
--reference=RFILE	Указание маски прав из указанного файла
-R, --recursive	Изменение прав доступа для каталога и его содержимого

Права доступа к указанным файлам, среди которых могут быть и каталоги, изменятся в соответствии с указанным режимом. Режим может быть задан в абсолютном или символьном виде.

Абсолютный вид – восьмеричное число, являющееся результатом поразрядного выполнения логического «или» для следующих режимов:

— «4000» – SUID бит;

- «1000» – sticky бит;
- «0400» – доступен для чтения владельцу;
- «0200» – доступен для записи владельцу;
- «0100» – доступен для выполнения (просмотра каталогов) владельцу;
- «0040» – доступен для чтения членам группы;
- «0020» – доступен для записи членам группы;
- «0010» – доступен для выполнения (просмотра каталогов) членам группы;
- «0004» – доступен для чтения прочим пользователям;
- «0002» – доступен для записи прочим пользователям;
- «0001» – доступен для выполнения (просмотра каталогов) прочим пользователям; и др.

Для задания режима доступа в символьном виде используется следующий синтаксис:

```
chmod [объект] <операция> <права доступа> <путь к файлу>
```

Необязательное поле [объект] может представлять собой комбинацию букв «u», «g» и «o» (владелец, члены группы и прочие пользователи соответственно). Если данное поле пропущено или в нем стоит «a», это эквивалентно «ugo» (для всех). В поле <операция> может стоять «+» (добавить право), «–» (лишить права) или «=» (присвоить права абсолютно, то есть добавить указанные права и отнять неуказанные). В поле <права доступа> может быть указана любая комбинация следующих символов:

- «r» – право на чтение;
- «w» – право на запись;
- «x» – право на выполнение (просмотр каталога);
- «s» – SUID бит;
- «t» – sticky бит.

Если поле <Права_доступа> отсутствует, может быть выполнена только операция «=» – это будет эквивалентно лишению всех прав доступа.

SUID бит или GUID бит устанавливается на месте соответствующей буквы «x»: малой «s», если соответствующая категория пользователей имеет право «x», и большой «S», если не имеет. Sticky бит указывается на месте последней буквы «x»: малой «t», если прочие пользователи имеют право выполнять файл, и большой «T», если не имеют.

Примеры использования:

В результате выполнения этой команды владелец получит полный доступ к файлу file1, а члены группы и прочие пользователи – право только на чтение:

```
# chmod 744 file1
```

В результате выполнения этой команды владелец получит право писать в файл file2, а члены группы и прочие пользователи – право исполнять данный файл:

```
# chmod u+w,go+x file2
```

7.4. Управление маской прав доступа

Утилита umask предназначена для установки маски создания файлов. Подробное описание приведено в man umask.

Синтаксис:

```
umask <маска>
```

Поле <Маска> представляет из себя восьмеричное значение, определяющее права на чтение, запись и выполнение для владельца, группы и прочих пользователей соответственно. Значение каждой указанной в маске цифры вычитается из значения соответствующей цифры, определенной ОС при создании файла.

Примеры использования:

В результате выполнения этой команды будет показано текущее значение маски:

```
# umask
```

В результате выполнения этой команды произойдет назначение маски 002:

```
# umask 002
```

Утилита umask изменяет маску создания файлов на текущий сеанс. Для задания маски по умолчанию необходимо редактировать файлы /etc/profile и /etc/bashrc: найти строчки, начинающиеся с «umask», и изменить значение маски.

Если при этом в домашнем каталоге пользователя в файле .bashrc пользователем задана иная маска – она будет использоваться по умолчанию для объектов, создаваемых с помощью приложения «Konsole» в графическом режиме.

7.5. Управление списками доступа ACL

Утилита getfacl предназначена для отображения текущих списков доступа ACL файла, каталога. В приведены часто используемые опции утилиты getfacl. Подробное описание приведено в man getfacl.

Синтаксис:

```
getfacl <опции> <путь к файлу>
```

Таблица 30 – Опции утилиты getfacl

Опция	Описание
-R, --recursive	Вывод списков доступа ACL каталога и его содержимого

Пример использования:

В результате выполнения этой команды произойдет вывод списков доступа ACL файла file1:

```
# getfacl file1
```

Утилита setfacl предназначена для модификации списков доступа ACL файлов, каталогов. В приведены часто используемые опции утилиты setfacl. Подробное описание приведено в man setfacl.

Синтаксис:

```
setfacl <опции> <ключ> <список правил> <путь к файлу>
```

Таблица 31 – Опции утилиты setfacl

Опция	Описание
-b, --remove-all	Удаление списков доступа ACL
-k, --remove-default	Удаление списков доступа ACL по умолчанию
-d, --default	Установка списков доступа ACL по умолчанию
--restore=file	Восстановление списков доступа ACL на объекты из ранее созданного файла с правами
-R, --recursive	Указание списков доступа ACL для каталога и его содержимого

Поле <Ключ> обычно задает один из следующих режимов работы, указанных в таблице Таблица 32. Подробное описание приведено в man setfacl.

Таблица 32 – Ключи утилиты setfacl

Ключ	Описание
--set	Указание новых списков доступа ACL, удаляя все существующие
-m	Модификация списков доступа ACL
-x	Удаление списков доступа ACL

Поле <Список правил> определятся синтаксисом, описанным в Таблица 33.

Таблица 33 – Синтаксис правил setfacl

Синтаксис	Описание
u:<пользователь>:<права>	Назначение прав для пользователя. Права определяются значениями r, w, x или сочетанием значений
g:<группа>:<права>	Назначение прав для группы. Права определяются значениями r, w, x или сочетанием значений
m:<права>	Назначение маски эффективных прав. Права определяются значениями r, w, x или сочетанием значений
o:<права>	Назначение прав для прочих пользователей. Права определяются значениями r, w, x или сочетанием значений

Примеры использования:

В результате выполнения этой команды произойдет модификация списков доступа ACL файла file1 – пользователь user1 будет иметь полный доступ к файлу file1:

```
# setfacl -m u:user1:rwx file1
```

В результате выполнения этой команды произойдет удаление списков доступа ACL файла file1 – пользователь user1 не будет иметь доступ к файлу file1:

```
# setfacl -x u:user1 file1
```

7.6. Блокирование сеанса пользователя

7.6.1. Блокирование сеанса в графическом режиме

Блокирование сеанса пользователя в графическом режиме после установленного времени бездействия можно настроить двумя способами. Для этого необходимо выполнить действия описанные в следующих 2 подразделах.

Блокировка сеанса по таймеру

Выбрать пункт меню «Блокировщик экрана» (Рисунок 104) или выполнить команду

```
/usr/bin/kcmshell4 screensaver
```

Для установки блокирования сеанса по таймеру необходимо обладать правами администратора. В окне «Блокировщик экрана – Модуль настройки KDE» установить опцию «Запускать автоматически после» и задать значение, а также задать параметры запроса пароля в окне «Требовать пароль после». При задании параметров через настройку «Блокировщик экрана» в домашнем каталоге пользователя автоматически обновляется файл конфигурации ~/.config/.kde4/share/config/kscreensaverrc, содержащий установленные параметры.

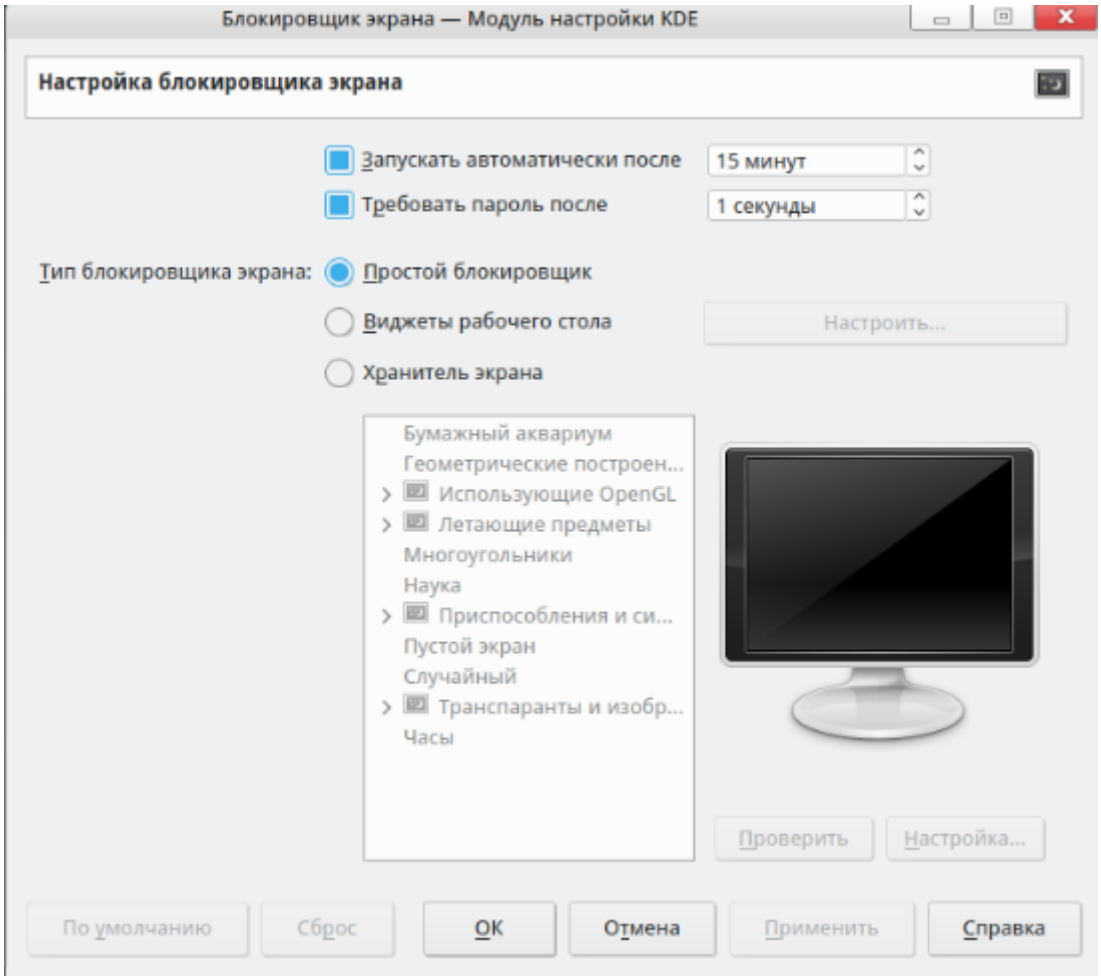


Рисунок 104. Блокировщик экрана

Выбрать пункт меню «Энергосбережение» или выполнить команду kcmshell4 powerdevilprofilesconfig. В окне «Энергосбережение – Модуль настройки KDE» перейти к настройке «Приостановить сеанс», установить опцию «Заблокировать экран» и задать значение. При задании параметров через пункт «Энергосбережение» в домашнем каталоге пользователя автоматически обновляется файл конфигурации ~/.config/.kde4/share/config/powermanagementprofilesrc, содержащий установленные параметры.

Принудительная блокировка сеанса пользователем

Для принудительного блокирования сеанса пользователя в графическом режиме необходимо нажать на значок в правой части панели задач «Заблокировать экран» (Рисунок 105), также кнопка доступна при открытии панели меню (в правом верхнем углу крана). Для разблокирования сеанса необходимо пройти процедуру аутентификации пользователя.

Рисунок 105. Кнопка принудительной блокировки сеанса пользователем

7.6.2. Блокирование сеанса в консольном режиме

Для блокирования консольной сессии пользователя и интерфейса консоли применяется утилита `vlock`. Она может работать в ручном или автоматическом режимах (режим по таймеру).

Для ручного блокирования консольного интерфейса в tty или эмуляторе консоли введите команду

```
vlock
```

После чего на экран выведется сообщение о том, что консоль заблокирована (Рисунок 106).

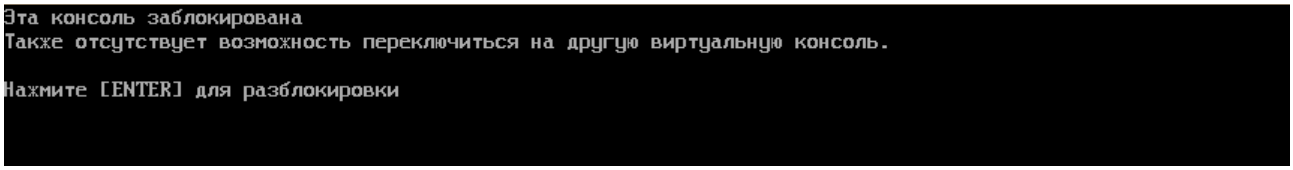


Рисунок 106.Сообщение о блокировки консоли

После нажатия на клавишу [ENTER] и ввода пароля пользователя интерфейс консоли будет разблокирован.

Также консольный интерфейс TTY блокируется по таймеру. Для изменения значения таймера введите команду:

```
sudo nano /etc/tmux.conf
```

По умолчанию таймер установлен на 15 минут.

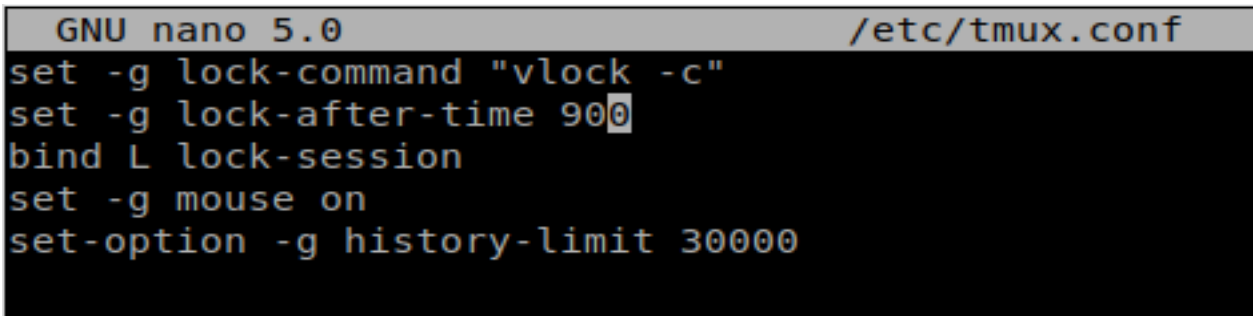


Рисунок 107. Таймер блокировки консоли

Для блокировки открытого эмулятора консоли `vlock` не применяется, эмулятор блокируется с помощью обычного блокировщика графических приложений. Эта настройка

произведена в файле `/etc/bashrc`.

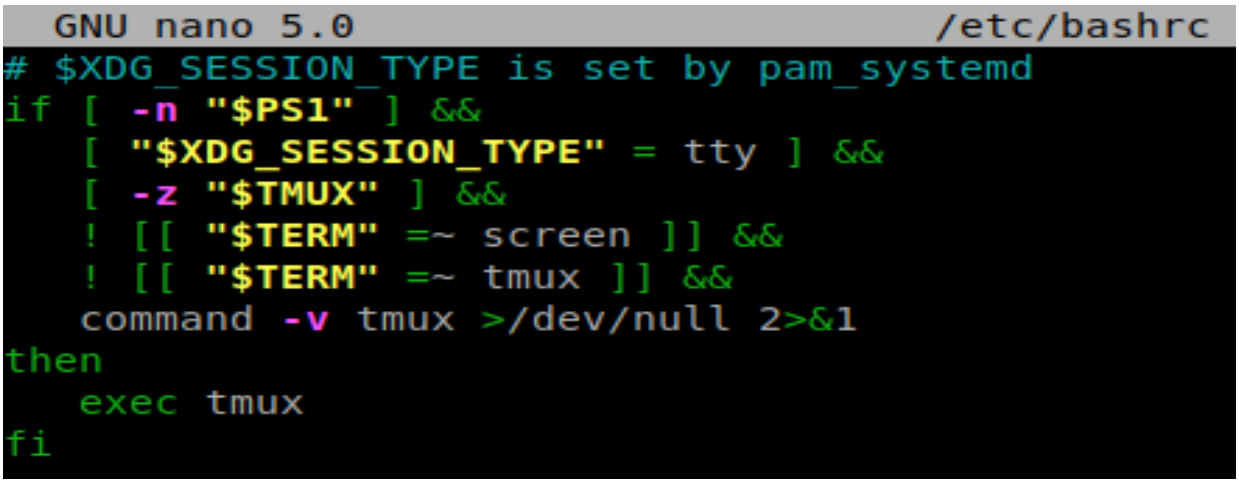


Рисунок 108. Исключение блокировки эмулятора консоли

7.7. Завершение сеанса после времени бездействия

7.7.1. Завершение сеанса после времени бездействия в графическом режиме

Для завершения сеанса пользователя в графическом режиме после установленного времени бездействия необходимо выполнить следующие действия.

Выбрать пункт меню «Энергосбережение» или выполнить команду

```
kcmshell4 powerdevilprofilesconfig
```

В окне «Энергосбережение – Модуль настройки KDE» перейти к настройке «Приостановить сеанс», установить опцию «Диалог подтверждения выхода» и задать значение. При задании параметров через пункт «Энергосбережение» в домашнем каталоге пользователя автоматически обновляется файл конфигурации ~/.config/.kde4/share/config/powermanagementprofilesrc, содержащий установленные параметры.

7.7.2. Завершение сеанса после времени бездействия в консольном режиме

Для каждого пользователя можно настроить автоматическое завершение сеанса, после установленного времени бездействия (неактивности) пользователя. По-умолчанию это время установлено в 60 минут настройками в файле /etc/bashrc

```
readonly TMOUT=3600
export TMOUT
```

7.8. Использование утилиты ROSA Chattr

Для работы с программой требуются привилегии администратора системы.

Утилита ROSA Chattr предназначена для назначения и модификации

дополнительных атрибутов файлов и каталогов. Чтобы запустить утилиту, выберите пункт меню «Приложения» → «Утилиты СЗИ ОС РОСА «НИКЕЛЬ» → «ROSA Chattr» или выполните команду rosachattr.

Интерфейс программы выглядит следующим образом (Рисунок 109):

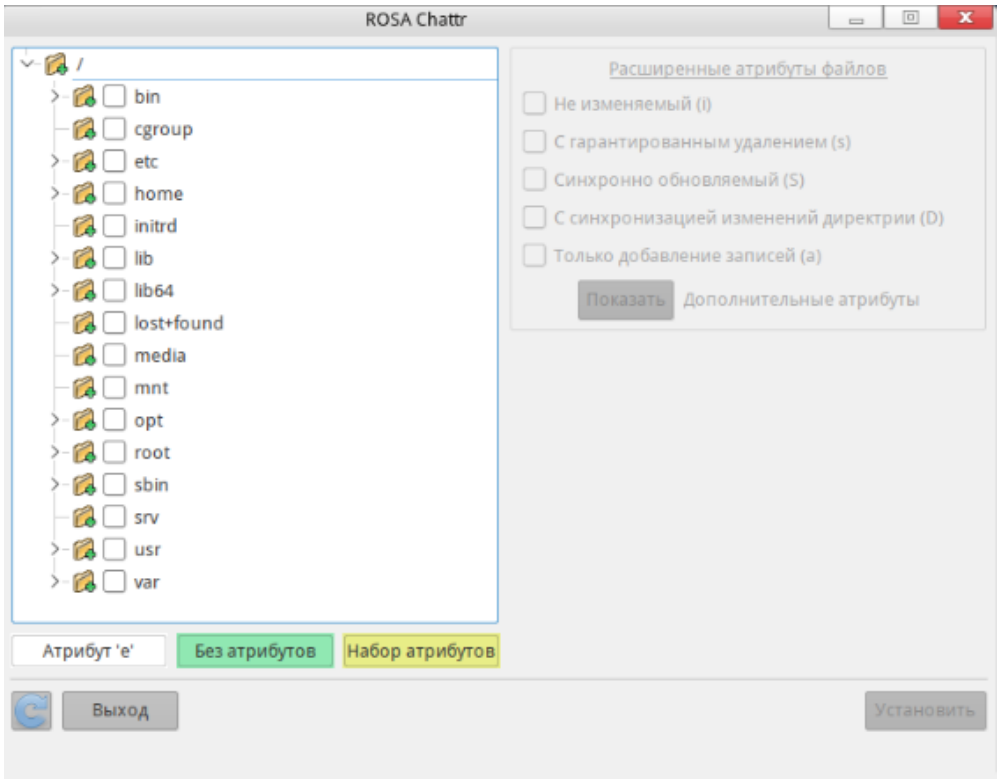


Рисунок 109. Интерфейс ROSA Chattr

В окне слева представлена корневая ФС ОС. Файлы и каталоги снабжены цветовой подсказкой в зависимости от наличия тех или иных атрибутов. Справа представлены атрибуты, которые можно установить. Слева внизу есть подсказка по цветовому обозначению.

Пока не выбрано ни одного файла или каталога слева, выбор атрибутов будет невозможен.

Чтобы назначить расширенные права файлу или каталогу, выберите его, а затем установите для него необходимые атрибуты справа и нажмите на кнопку [Установить].

Атрибуты устанавливаются нерекурсивно.

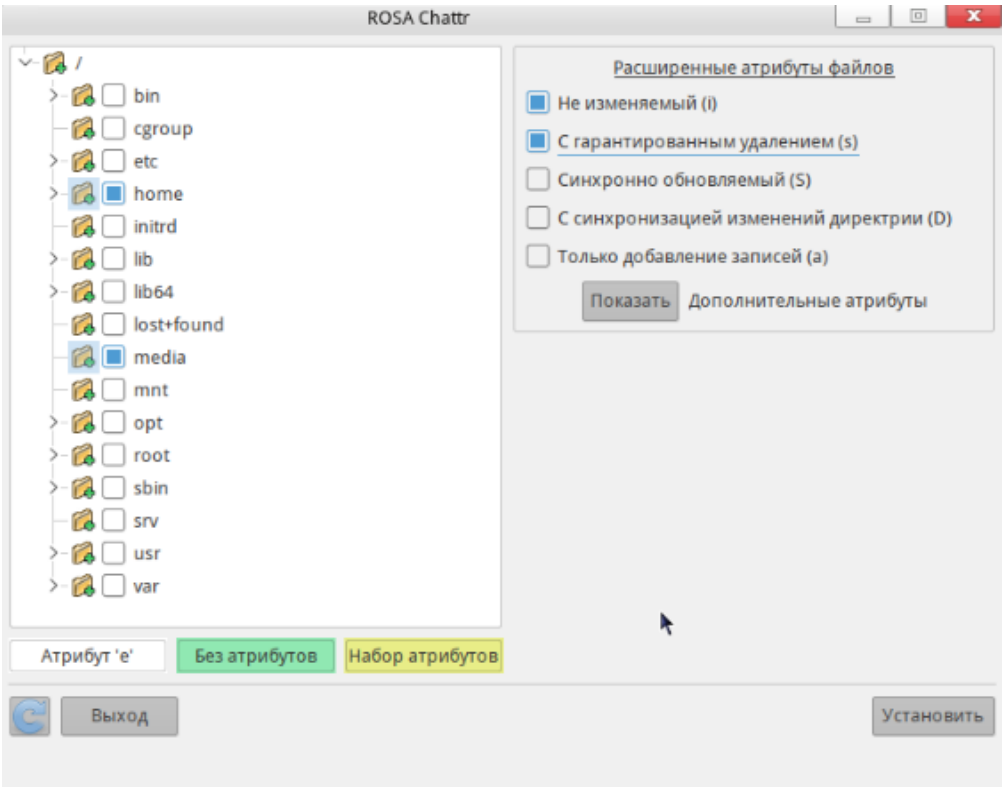


Рисунок 110. Установка атрибутов

Если нажать на кнопку [Показать], будет доступен список дополнительных атрибутов (Рисунок 111):

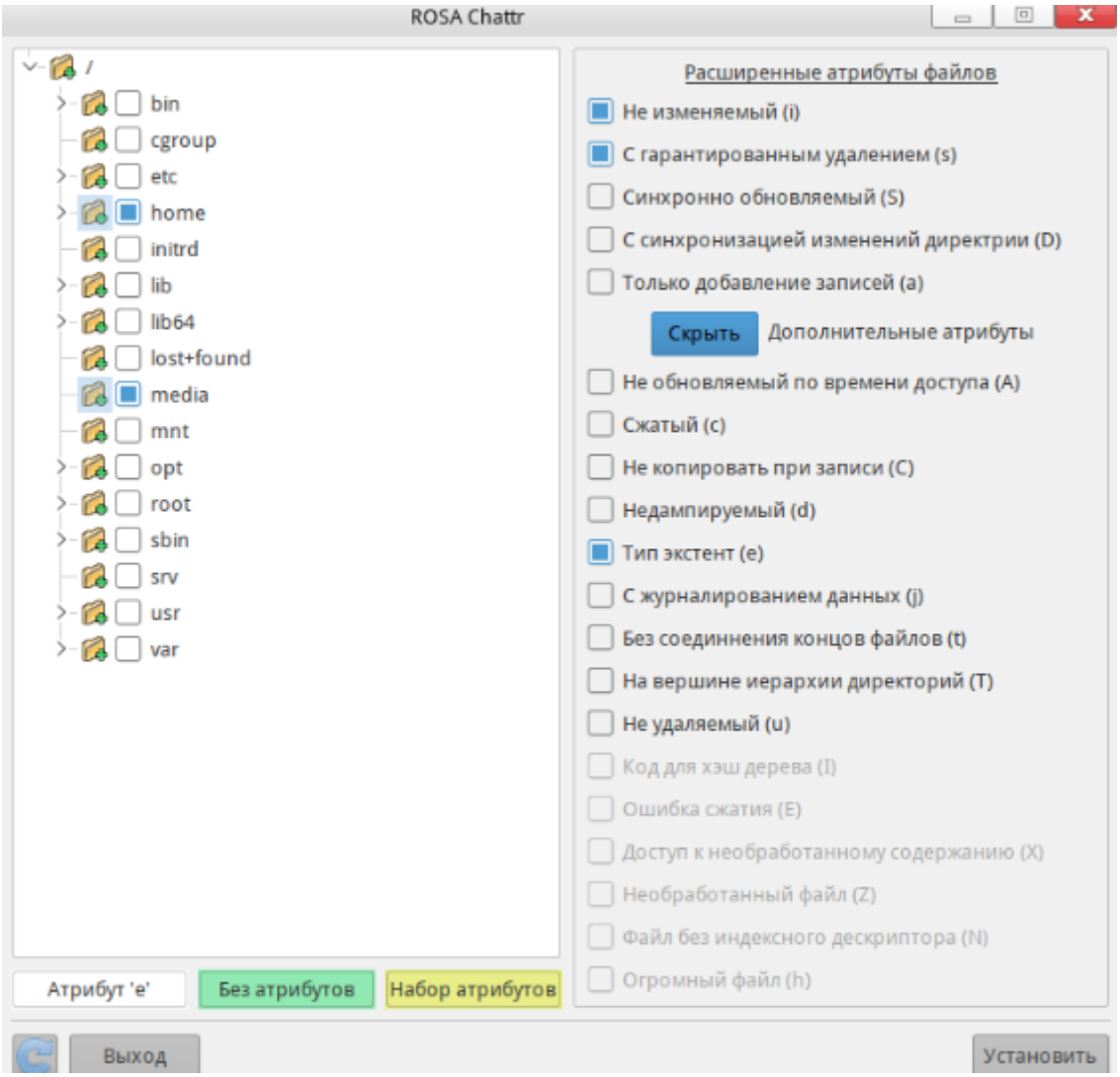


Рисунок 111. Дополнительные атрибуты

7.8.1. Перечень атрибутов

1) Если для файла установлен атрибут «A», обновление (модификация) записи atime (времени доступа к файлу) не происходит. Это позволяет избежать дополнительных дисковых операций ввода/вывода.

2) Для файла с установленным атрибутом «a» разрешено лишь добавлять записи. Только суперпользователь или процесс, обладающий возможностью CAP_LINUX_IMMUTABLE, может установить или очистить этот атрибут.

3) Информация файла с установленным атрибутом «c» автоматически упаковывается (сжимается) на диске ядром ОС. Операция чтения информации из этого файла возвращает несжатые данные. Запись информации в такой файл сопровождается предварительной ее упаковкой и, наконец, последующим сохранением на диск.

4) При модификации файла с атрибутом «D» внесенные изменения синхронно записываются на диск; использование этого атрибута эквивалентно применению опции монтирования «dirsync» к подмножеству файлов.

5) Для файла с установленным атрибутом «d» не выполняется резервное копирование, когда запущена программа dump(8).

6) Атрибут «E» используется экспериментальными заплатками сжатия для определения того, что сжатый файл имеет ошибку сжатия. Это состояние может быть установлено или сброшено с помощью chattr(1), а отображено — с помощью lsattr(1).

7) Атрибут «I» используется кодом для хеш-деревьев (htree), чтобы указать, что каталог находится позади индексированных хешированных деревьев. Это состояние может быть установлено или сброшено с помощью chattr(1), а отображено — с помощью lsattr(1).

8) Файл с установленным атрибутом «i» становится не модифицируемым (недосягаемым): он не может быть удален или переименован, на этот файл не могут быть созданы никакие ссылки и никакие данные не могут быть записаны в него. Только суперпользователь или процесс, обладающий возможностью CAP_LINUX_IMMUTABLE, может установить или очистить этот атрибут.

9) Для файла с установленным атрибутом «j» все его данные, прежде чем быть записанными непосредственно в файл, сохраняются в журнал ext3. Правда, это происходит лишь в том случае, если ФС была смонтирована с опциями «data=ordered» или «data=writeback». Когда ФС смонтирована с опцией «data=journal», все данные файла уже журналируются, и этот атрибут не имеет никакого эффекта. Только суперпользователь или процесс, обладающий возможностью CAP_SYS_RESOURCE, может установить или очистить этот атрибут.

10) При удалении файла с установленным атрибутом «s» выполняется обнуление его блоков и запись их обратно на диск.

11) При модификации файла с атрибутом «S» внесенные изменения синхронно записываются на диск; использование этого атрибута эквивалентно применению опции монтирования «sync» к подмножеству расположенных файлов.

12) Каталог с установленным атрибутом «T» будет считаться расположенным на вершине иерархии каталогов с целью использования метода распределения блоков по Orlov.

13) Файл с установленным атрибутом «t» не будет иметь в завершающем блоке на диске дописанных («склеенных» с ним) фрагментов других файлов (для тех ФС, которые поддерживают «склеивание хвостов» файлов.

14) При удалении файла с атрибутом «u» его содержимое сохраняется (остается нетронутым) на диске. Это позволяет пользователю в дальнейшем восстановить такой файл.

15) Атрибут «X» используется экспериментальными заплатками сжатия для определения того, что к необработанному содержанию сжатого файла можно получить непосредственный доступ. Это состояние может быть установлено или сброшено с помощью chattr(1), а отображено — с помощью lsattr(1).

16) Атрибут «Z» используется экспериментальными средствами сжатия для определения того, что сжатый файл является необработанным. Это состояние может быть установлено или сброшено с помощью chattr(1), а отображено — с помощью lsattr(1).

8. РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ (АУДИТ)

8.1. Rosa-central-panel

Rosa-central-panel – комплекс программ, реализующих централизованный сбор, хранение и просмотр событий аудита. В составе комплекса 4 программных решения:

1. Rosa-audisp-sender
2. Rosa-central-panel-serverd
3. Rosa-central-panel-logviewer
4. Rosa-central-panel-ui

В ОС существует механизм аудита событий, реализуемый службой аудита auditd. Для того, чтобы отследить любое событие в системе, служба аудита перехватывает обращения к системным вызовам. Данные из auditd перенаправляются в rsyslog, объединяются с системным журналом syslog и передаются приложению rosa-central-panel-serverd. Приложение rosa-central-panel-serverd обрабатывает данные и при наличии подключения через rosa-audisp-sender отправляет эти данные на хранение.

8.1.1. Общие сведения

Работа комплекса возможна как в распределенном режиме, так и локально.

Для локальной работы системы необходим запуск сервиса rosa-central-panel-serverd.service (запущен по-умолчанию), для передачи сообщений на сервер необходим запуск сервиса rosa-audisp-sender.

Сервис rosa-central-panel-serverd.service имеет функционал проверки свободного места на диске. Например, файл конфигурации может выглядеть следующим образом (Рисунок 112).

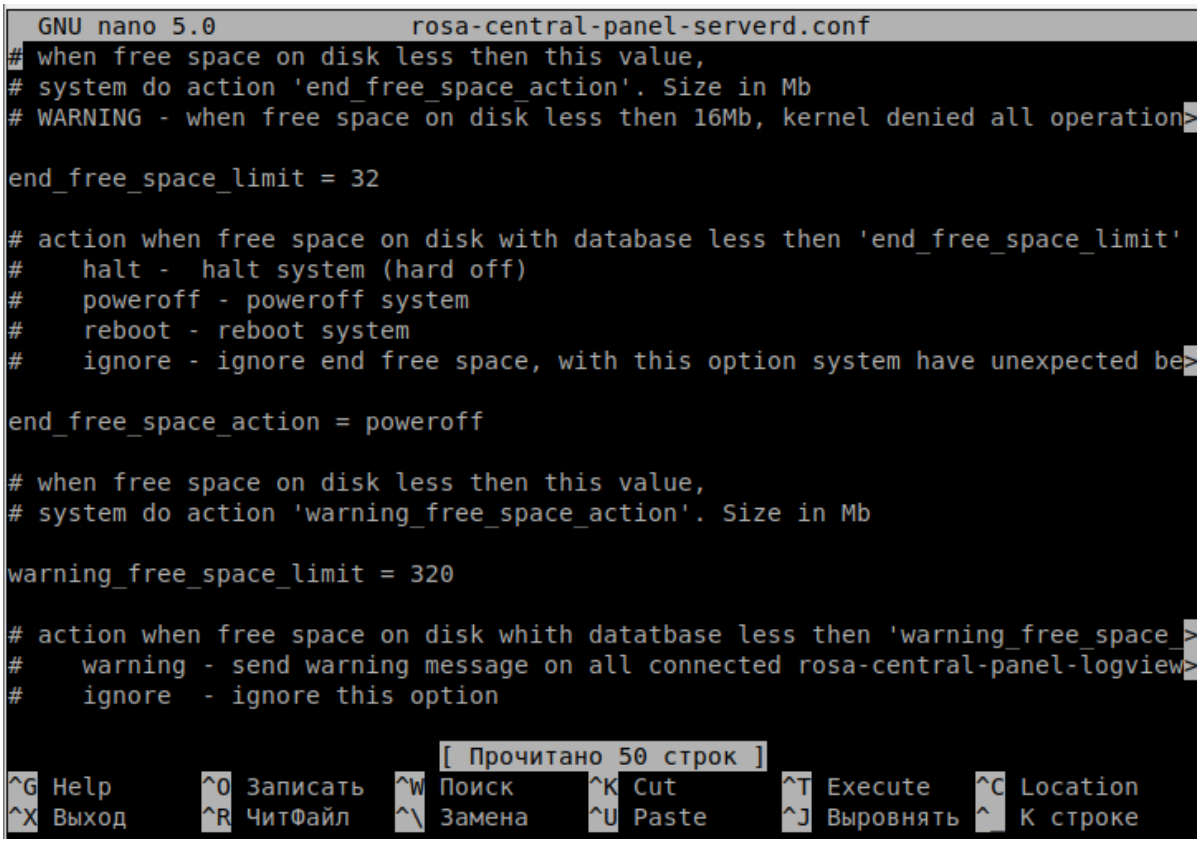


Рисунок 112. Проверка свободного места на диске

В настройках `/etc/rosa-central-panel-serverd.conf` строки `end_free_space_action` и `warning_free_space_action` установлены в значение отличные от `ignore`.

Для распределенной работы необходимо по меньшей мере 2 ПК – сервер и клиент.

На сервере необходимо установить статический ip. Для этого (Рисунок 113):

1. Щелкаем на значке сетевого соединения левой кнопкой мыши.
2. Нажимаем на значок настроек.
3. В появившемся окне «Редактор соединений» выбираем соединение, которое хотим настроить.
4. Нажимаем на значок настроек.
5. В появившемся окне «Изменение соединения» переходим во вкладку «IPv4».
6. Выбираем метод: вручную.
7. Нажимаем добавить.
8. Вводим следующие параметры: адрес, маску сети и шлюз.
9. Нажимаем кнопку «Ок»

Далее после установки необходимо перезагрузить машину.

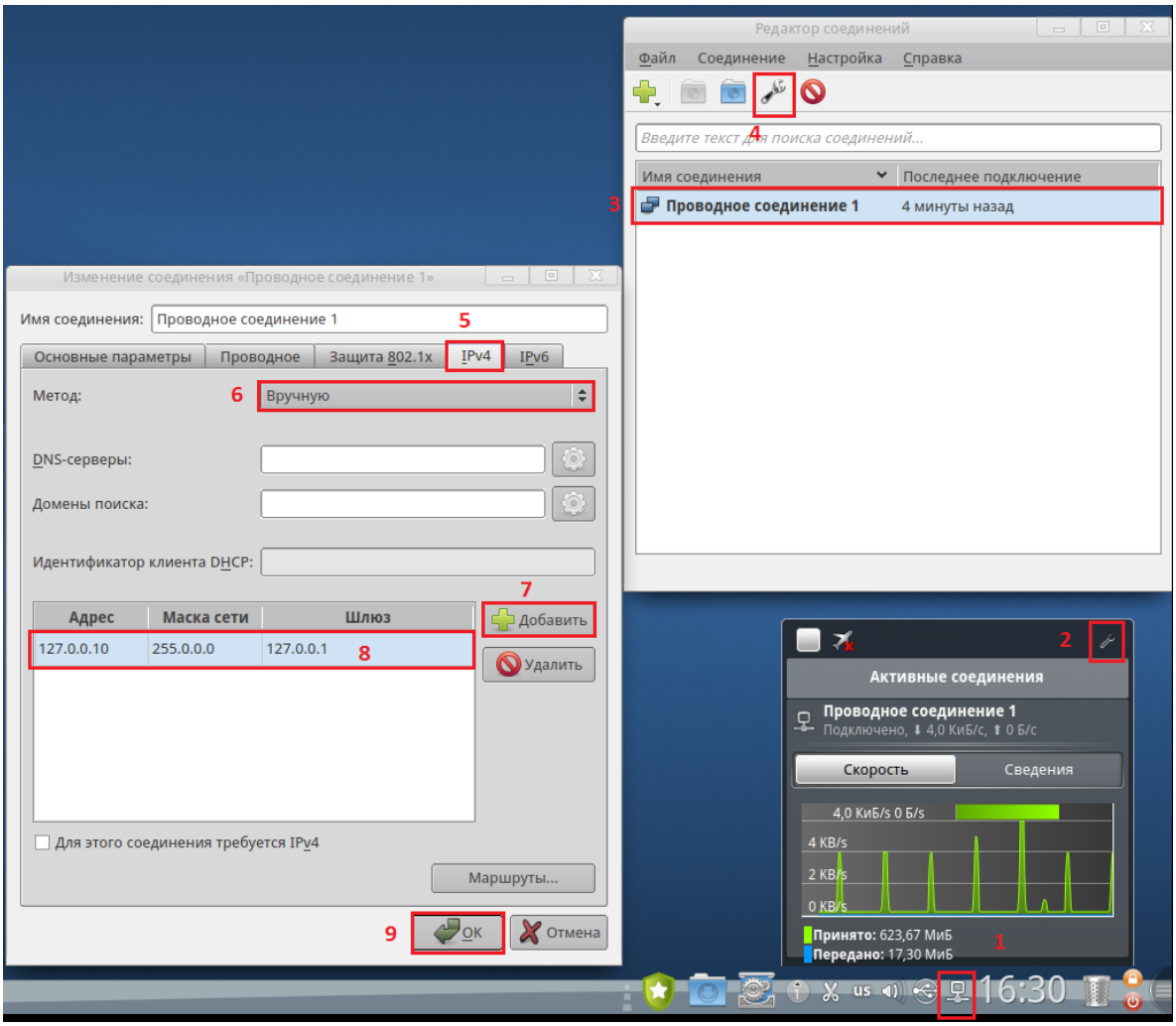


Рисунок 113. Порядок настройки статического ip

Можно оставить метод получения адреса автоматическим, для этого на сетевом оборудовании необходимо настроить резервацию статических адресов на вашем DHCP-сервере. Подробнее смотрите соответствующую документацию к вашему оборудованию/DHCP-серверу.

На сервере необходима работа сервиса rosa-central-panel-serverd.service а также проверить, что в файле /etc/rosa-audisp-sender.conf установлен локальный адрес отправки сообщений 127.0.0.1 .

При необходимости изменить поведение и лимиты свободного места на жестком диске отредактируйте файл /etc/rosa-central-panel-serverd.conf.

Подробнее о том, как это сделать можно посмотреть в выше в данном разделе.

Далее на клиенте необходимо отредактировать файл /etc/rosa-audisp-sender.conf установив адрес сервера (например: 192.168.0.101).

Для корректной работы необходим запуск сервиса rsyslog (запущен по-:

Проверить статус сервиса следующей командой:

```
#systemctl status rsyslog.service
```

Если статус сервера неактивен, как указано на Рисунок 114 (`Active: inactive (dead)`) выполните следующие действия.

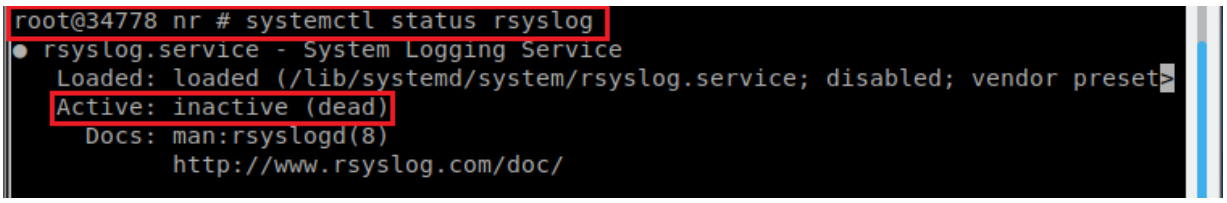


Рисунок 114. Неактивный статус сервера

Активируйте сервис следующей командой:

```
#systemctl enable rsyslog.service
```

А затем запустите командой:

```
#systemctl start rsyslog.service
```

Проверить статус работы можно командой:

```
#systemctl status rsyslog.service
```

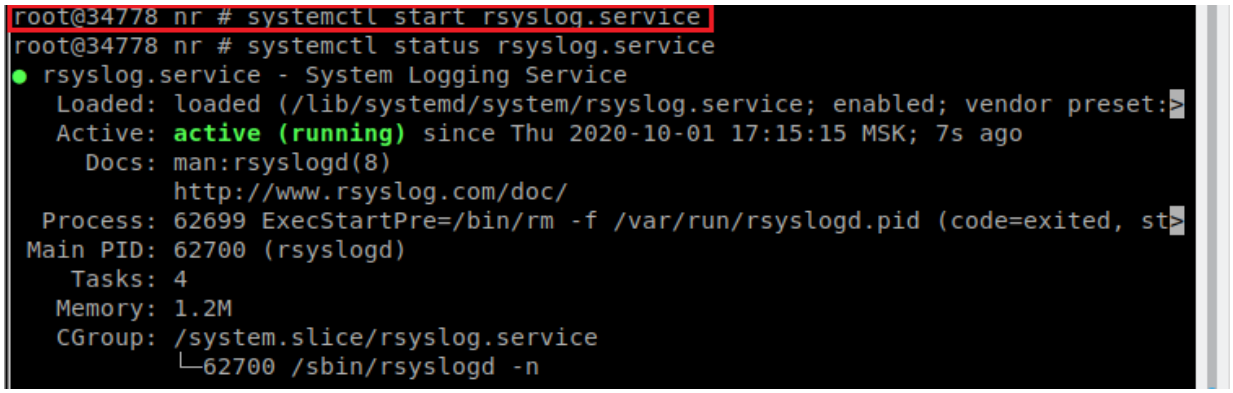


Рисунок 115. Запуск сервиса

8.1.2. Rosa-audisp-sender

Audisp-sender — сервис, отвечающий за отправку данных аудита по протокол SYSLOG с использованием шифрования TLS1.2 Использует для работы сервисы auditd и rsyslog.

Принцип работы

Сервис auditd регистрирует события и отправляет данные сервису rsyslog. Сервис rsyslog отправляет данные от auditd и из системного журнала syslog данные в сервис audisp-sender. Audisp-sender получает данные от rsyslog, шифрует данные и пересылает по указанному ip-удресу сервису serverd. Если сервис serverd недоступен, audisp-sender сохраняет данные, до возможности отправить их сервису serverd. При остановке сервисе audisp-sender и наличии не отправленных сообщений, все сообщения сохраняются локально, в файл /var/spool/logs_queue.txt

Как только сервер станет доступен для отправки, данные будут считаны с жесткого диска и отправлены на сервер.

Настройка

Настройки сервиса хранятся в файле конфигурации /etc/rosa-audisp-sender.conf и имеют следующий вид:

- `ip` — ip-адресс хоста, на котором работает serverd;
- `port` — порт сервиса serverd;
- `local` — порт сервиса rsyslog;
- `log_level` — уровень логирования.

Параметр `log_level` может принимать одно из значений:

- `LOG_TRACE` — максимально подробное логирование;
- `LOG_DEBUG` — логирование ошибок, предупреждений, информационных и отладочных сообщений;
- `LOG_INFO` — логирование ошибок, предупреждений и информационных сообщений;
- `LOG_WARNING` — логирование только ошибок и предупреждений;
- `LOG_ERROR` — логирование только ошибок.

8.1.3. Rosa-central-panel-serverd

Serverd – серверный сервис, отвечающий за прием, хранение данных аудита и ответ на запросы от приложений для просмотра данных аудита. (rosa-central-panel-logviewer и rosa-central-panel-ui)

Принцип работы

Сервис принимает входящие соединения от сервисов audisp (порт 3427) и запросы от интерфейсов администратора (порт 3428) При получении входящего сообщения от сервиса audisp, происходит его обработка и запись в базу данных sqilte3. Так же, если в момент получения хотя бы один интерфейс администратора был подключен к serverd, происходит отправка этого сообщения всем подключенным интерфейсам. При получении входящего запроса от интерфейса администратора, происходит его обработка и отправка запрошенных данных.

Настройка

Настройки сервиса хранятся в файле конфигурации /etc/rosa-central-panel-serverd.conf и имееют следующий вид (Рисунок 116):

```
# when free space on disk less then this value,
# system do action 'end_free_space_action'. Size in Mb
# WARNING - when free space on disk less then 16Mb, kernel denied all operation whith disk!
end_free_space_limit = 32

# action when free space on disk with database less then 'end_free_space_limit'
#    halt -  halt system (hard off)
#    poweroff - poweroff system
#    reboot - reboot system
#    ignore - ignore end free space, with this option system have unexpected behavior
end_free_space_action = poweroff

# when free space on disk less then this value,
# system do action 'warning_free_space_action'. Size in Mb
warning_free_space_limit = 320

# action when free space on disk whith datatbase less then 'warning_free_space_limit'
#    warning - send warning message on all connected rosa-central-panel-logviewers
#    ignore  - ignore this option
warning_free_space_action = warning
~
~
~
~
```

Рисунок 116. Настройка сервера

Параметр `end_free_space_limit` – задает порог свободного места на диске, на котором расположен файл базы данных. Указывается в MiB. По умолчанию установлен уровень в 32 Мб свободного места, при достижении этого порога выполняется действие, заданное опцией end_free_space_action.

`warning_free_space_limit` – задает порог свободного места на диске, на котором расположен файл базы данных. Указывается в MiB. По умолчанию установлен уровень в 320 Мб свободного места, при достижении этого порога выполняется действие, заданное опцией warning_free_space_action.

`end_free_space_action` – действие, выполняемое при достижении критически низкого уровня свободного места на диске, на котором расположен файл базы данных. Возможные варианты действий:

- `reboot` – выполняется перезагрузка системы;
- `poweroff` – выполняется обычное выключение системы;
- `halt` – выполняется экстренная остановка системы;
- `ignore` – игнорирование критического уровня свободного места, данная опция не рекомендуется для использования, так как возможно потеря данных аудита, оставлена для возможности тестирования

`warning_space_action` – действие, выполняемое при достижении уровня свободного места на диске, на котором расположен файл базы данных, указанного в опции warning_free_space_limit. Возможные варианты действий:

`warning` – генерируется сообщение о достижении порога свободного места, и отправляется в очередь обработки сообщений, тем самым попадая в базу

данных и оповещая администратора.

`ignore` – сообщение не генерируется, производится только запись в лог (/var/log/rosa-central-panel-serverd.log).

Так же имеется раздел, посвященный ротации базы данных:

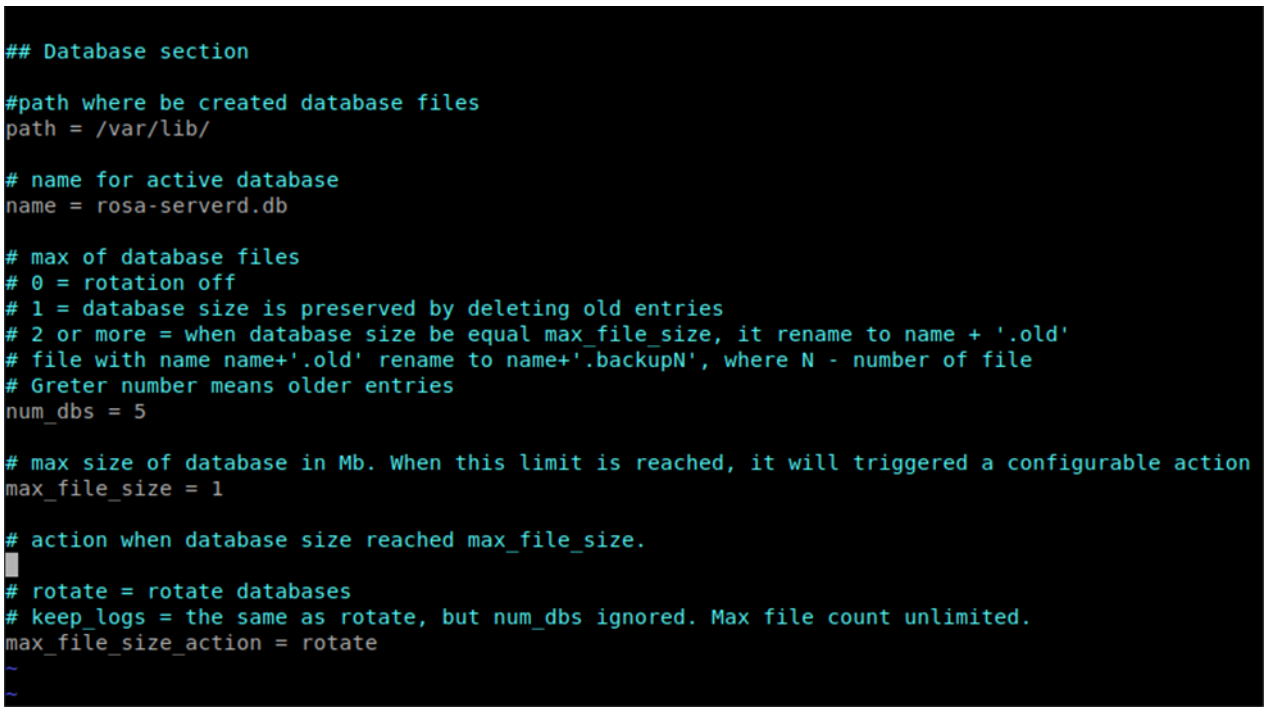


Рисунок 117. Ротация базы данных

— `path` — полный путь к дериктории, где будут храниться базы данных. Путь должен существовать на момент запуска сервера.

— `name` — имя активной базы данных.

— `num_dbs` — максимально количество файлов баз данных. Если установлен 0 - ротация отключена. Если установлен 1 - ротация отключена, но размер базы данных не будет превышать установленный лимит за счет удаления наиболее старых записей. Если установлено 2 или больше ротация файлов включена. При достижении максимального размера активной базы данных она будет переименована в *name*.old — это база так же будет использоваться для чтения. При следующей ротации *name*.old будет переименована в *name*.backup1, далее *name*.backup2 и т. д.

— `max_file_size` — предельный размер одного файла база данных в мегабайтах. (1Мб = 1048576 байт). Если `num_dbs > 1`, при достижении этого лимита поведение будет определятся следующей опцией `max_file_size_action`

— `max_file_size_action` — действие выполняемое при достижении размера базы данных заданного лимита.

— `rotate` - ротация базы данных, не будет выполняться если `num_dbs` меньше 2. иначе файлы будут переименовываться при этом индекс растет вверх со временем. Более старые файлы будут иметь больший индекс.

— `keep_logs` — тоже самое что и `rotate`, но без удаления более старых записей, `num_logs` игнорируется.

— `Ignore` — никакие действия не предпринимаются, игнорируются `num_dbs` и `max_file_size`

Файл логов находится по адресу /var/log/rosa-serverd.log.

Параметры запуска можно изменить, отредактировав файл rosa-central-panel-serverd.service расположенный в каталоге /lib/systemd/system/.

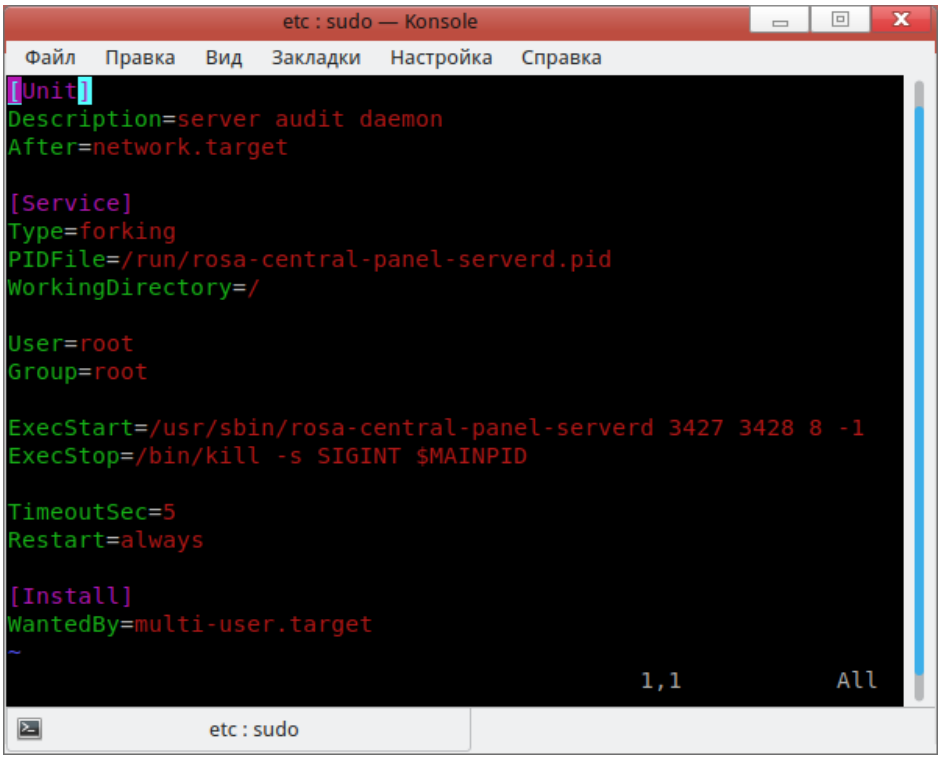


Рисунок 118. Параметры запуска сервиса

Здесь ExecStart содержит параметры запуска сервиса. Всего сервис serverd принимает 4 параметра.

1) 3427 - порт для подключения сервисов audisp-sender (Внимание! Замена этого значения приведет к невозможности подключения сервисов audisp, пока не будет отредактированы файлы конфигурации сервисов audisp)

2) 3428 - порт для подключения интерфейсов администратора.

3) 8 - максимальное количество соединений.

4) -1 - уровень логирования. Имеется 5 уровней логирования:

-1 — Максимально подробное логгирование.

0 — Логгирование ошибок, предупреждений, информационных и отладочных

сообщений.

1 — Логгирование ошибок, предупреждений и информационных сообщений.

2 — Логирование ошибок и предупреждений.

3 — Логгирование только ошибок.

Запуск

Для запуска сервиса используются стандартные команды systemctl.

Для проверки статуса сервера:

```
#systemctl status rosa-central-panel-serverd.service
```

Для запуска сервера:

```
#systemctl start rosa-central-panel-serverd.service
```

Для включения сервера в автозапуск:

```
#systemctl enable rosa-central-panel-serverd.service
```

8.1.4. Rosa-central-panel-logviewer

Приложение является графическим интерфейсом администратора для просмотра событий аудита, полученных сервисом rosa-central-panel-serverd.

Принцип работы

Приложение при запуске подключается к сервису serverd использую шифрованное соединение. В зависимости от действий администратора может отсылать серверу запросы. В процессе работы получает ответы на запросы от сервера.

Настройка

Настройка приложения производится путем редактирования конфигурационного файла /etc/rosa-central-panel-logviewer.conf.

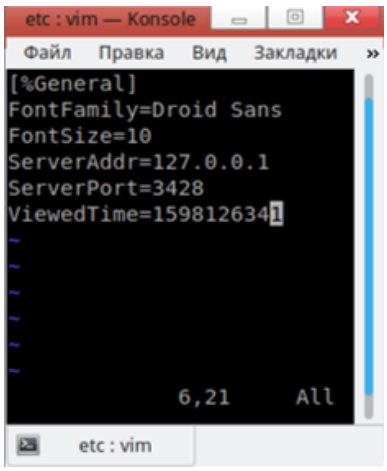


Рисунок 119. Настройка Rosa-central-panel-logviewer

Параметры Rosa-central-panel-logviewer:

— `FontFamaly` — семейство шрифтов;

— `FontSize` — размер шрифта;

— `ServerAddr` — адрес сервера (serverd);

— `ServerPort` — порт сервера (serverd);

— `ViewedTime` — время последнего просмотренного события красной категории.

Запуск

Для удаленного мониторинга состояния защиты запустить утилиту «Аудит». Иконка утилиты «Аудит» находится в приложениях в разделе «Утилиты СЗИ» (Рисунок 120).

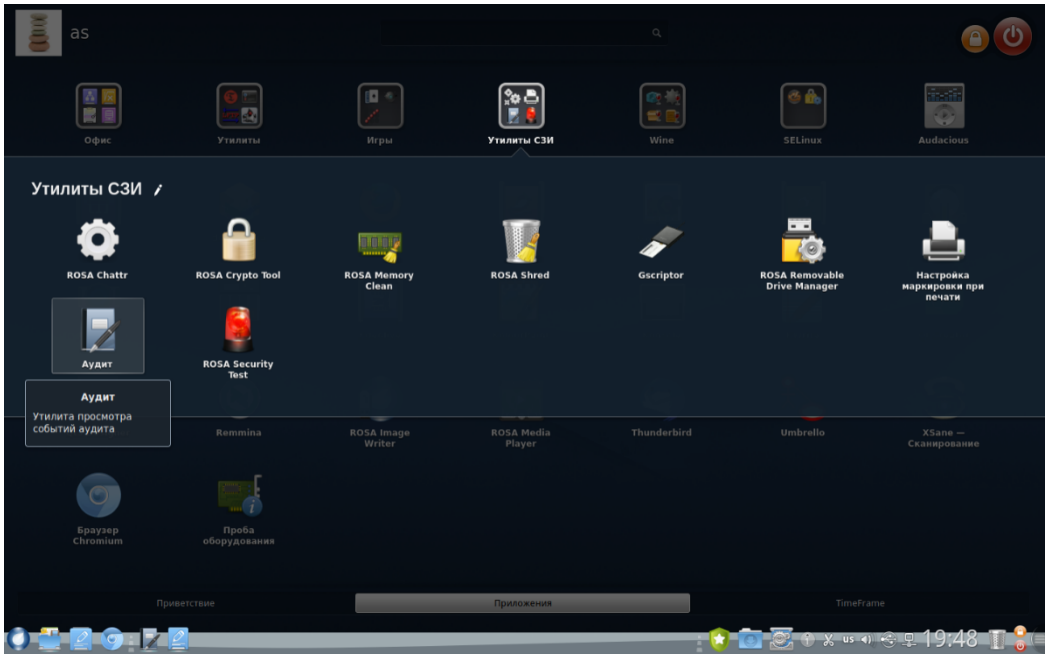


Рисунок 120. Доступ к утилите «Аудит»

Для доступа к приложению также необходимо ввести пароль администратора безопасности или оператора аудита в открывшимся окне (Рисунок 121).

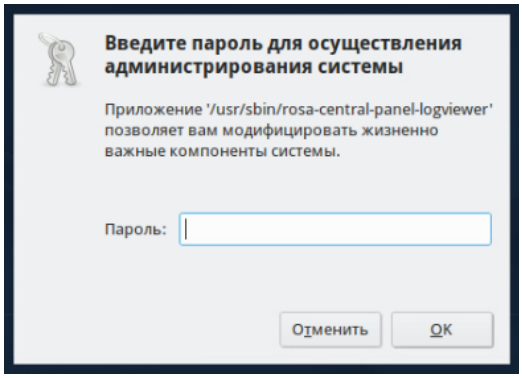


Рисунок 121. Ввод пароля

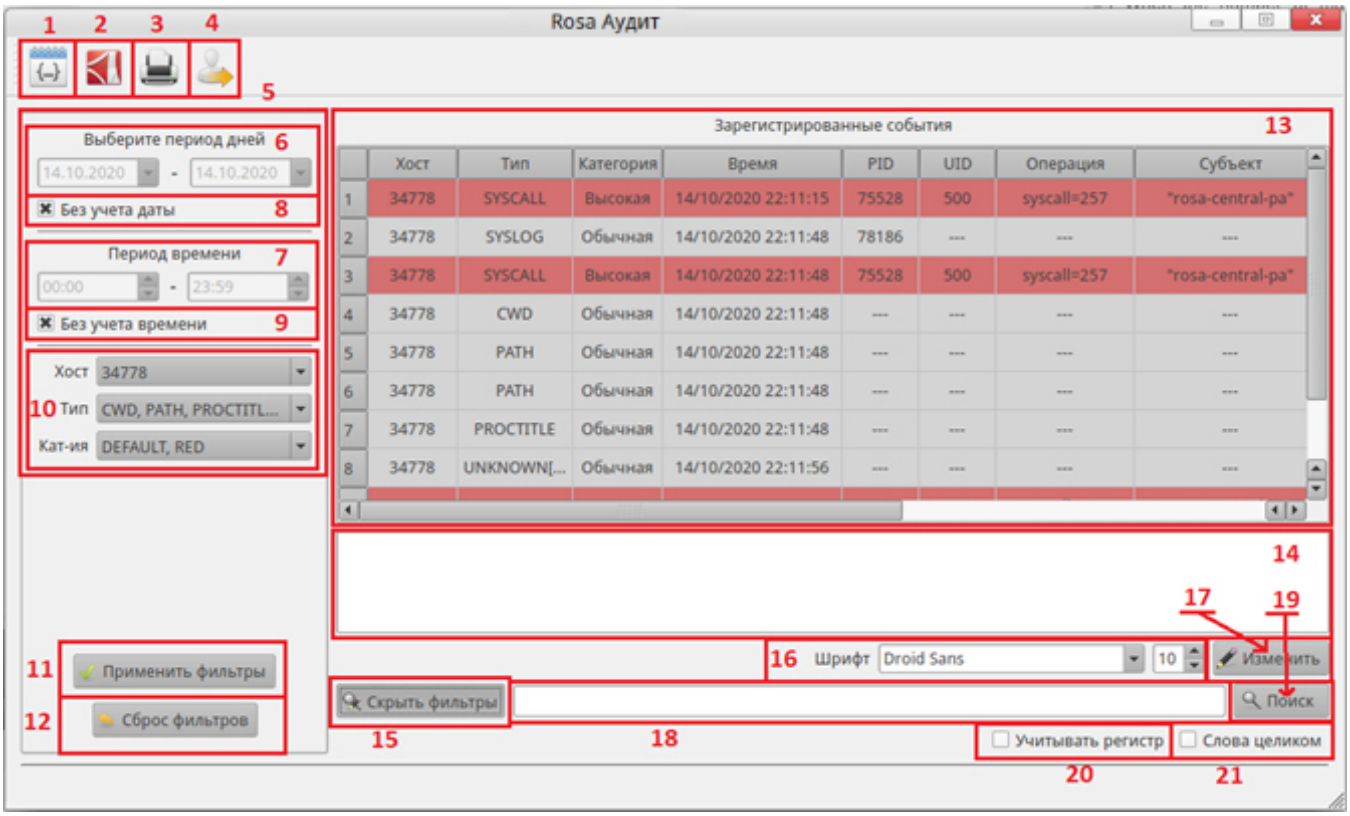


Рисунок 122. Интерфейс утилиты «Аудит»

Рассмотрим интерфейс программы:

1. Экспорт в CSV-файл.
2. Экспорт в PDF-файл.
3. Печать.
4. Выход.
5. Блок фильтров времени. Итоговый диапазон отображения зависит как от диапазона дат, так и от периода времени. По умолчанию, когда переключатели 8 и 9 активны, в полях дат установлено значение текущего дня, а в полях времени период от 00:00 до 23:59. Итоговый диапазон всегда непрерывен и вычисляется следующим образом: от значения первого поля дней – значение первого поля времени до значение второго поля дней – значение второго поля времени. Это значит, что если будет установлены даты 01.10.20 и 03.10.20, а в полях времени будут указано 15:00 и 16:00, то итоговый диапазон будет от 15:00 01.10.20 до 16:00 03.10.20.
6. Поля для установки диапазона дат. Не активны, когда выбрана опция «Текущий день».
7. Поля для установки диапазона времени. Не активна, когда выбрана опция «Текущий час».
8. Переключатель «Текущий день». Когда активирован, диапазон дат равен текущему дню. Когда не активен, можно установить диапазон дат для отображения.

9. Переключатель «Текущий час». Когда активирован, диапазон времени равен последнему часу от текущего времени.

10. Остальные фильтры. Здесь используется выпадающий список со множественным выбором. Заполняется при получении данных. Для исключения из результатов какого-нибудь значения, достаточно снять галочку напротив этого значения в соответствующем списке, и нажать на кнопку «Применить фильтр».

11. Кнопка «Применить фильтры». При нажатии на данную кнопку происходит отображение только тех данных, которые соответствуют заданным фильтрам. При отсутствии необходимых данных в памяти, формируется запрос к серверу, для получения недостающих данных.

12. Кнопка «Сбросить фильтры». Возвращает состояние фильтров в исходное состояние.

13. Таблица, предоставляющая события аудита. События можно фильтровать с помощью блока фильтров, расположенного слева. Если этот блок не отображается, нужно нажать на кнопку «Показать фильтры» (15). Если блок отображается, данная кнопка меняет свое название на «Скрыть фильтры». Так же уже отображенные данные можно сортировать по любому столбцу. Для этого необходимо щелкнуть на заголовке столбца. Повторный клик приведет к сортировке в обратном порядке. Важно! Сортировка происходит лексикографически.

14. Поле для отображение дополнительной информации о событии. При выборе события левым щелчком мыши в таблице (13), в этом поле отобразиться не форматированная информации о событии.

15. Кнопка «Показать фильтры» / «Скрыть фильтры» показывает или скрывает блок фильтров.

16. Поле установки шрифта для таблицы зарегистрированных событий и поля дополнительной информации под ним. Здесь можно будет выбрать семейство шрифтов и размер.

17. Кнопка «Изменить». Применяет изменения для шрифта.

18. Поля для ввода искомой фразы.

19. При нажатии на кнопку происходит поиск текста, введенного в поле левее (18). Учитываются флаги ниже (20,21). Если где-то в таблице найдено соответствие, ячейка меняет свое оформление. Шрифт меняет начертание на жирное, а цвет меняется на зеленый. В поиске не учитываются поле дополнительной информации, и строки, которые были скрыты фильтром.

20. Переключатель «Учитывать регистр». По умолчанию поиск происходит без

учета регистра. Если нужно, чтобы при поиске учитывался регистр, необходимо установить этот переключатель.

21. Переключатель «Слова целиком». Если установить этот переключатель, поиск будет производиться по другим правилам. Например, если переключатель выключен поиск по фразе «sys» найдет как «syslog», так и «syscall». Если переключатель включен, то поиск будет идти только целых слов, соответствующих заданному поисковому запросу, а не их части. Например, при поиске по фразе «run» не будут отмечены слова «runnig» или «unrun», то будет найдены строки с отдельно стоящим словом «run». Искомое слово может быть окружено любыми знаками препинания или пробелом, но не буквенными символами.

Работа сигнализации логов

В процессе работы программы, при наличии активного подключения к серверу, все новые события, попадающие на сервер, сразу отправляются на все подключенные интерфейсы администратора. При этом они будут отображаться только если это не противоречит настройкам фильтров. Однако, события красной категории все равно будут отображаться в системном трее в виде всплывающего сообщения.

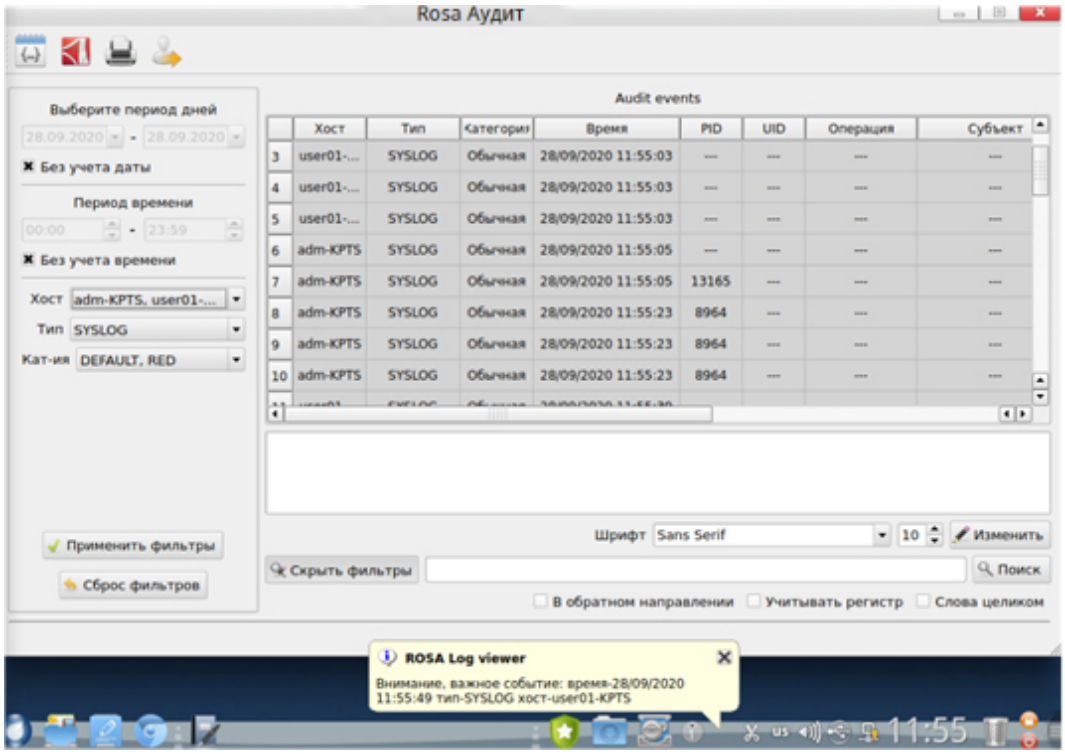


Рисунок 123. Интерфейс программы и всплывающее сообщение LogViewer

8.1.5. Rosa-central-panel-ui

Приложение является консольным интерфейсом администратора, с помощью

которого можно просматривать события аудита, хранящиеся в базе данных сервиса serverd.

Принцип работы

Приложение подключается к серверу при старте. В зависимости от действий администратора может отсылать запросы к серверу и получать данные по зашифрованному каналу.

Настройка

Настройка производится путем редактирования файла /etc/rosa-central-panel-ui.conf.

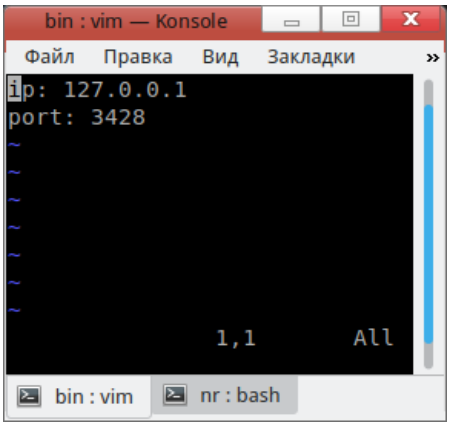


Рисунок 124. Параметры Rosa-central-panel-ui

Параметры утилиты:

— `ip` - адрес сервера;

— `port` - порт сервера.

1.1.1.1. Работа с программой

Работа с программой производится путем ввода команд, после успешного подключения. Первое слово расценивается как команда. Порядок флагов и фильтров не имеет значения.

Список команд:

— `exit` - выйти из программы;

— `help` - показать справочную информацию;

— `clear` - отчистить экран;

— `reset` - отчистить локальное хранилище;

— `get` - отправить запрос к серверу. В запросе можно указывать фильтры. Фильтр времени значительно ускорит время получения данных. Полученные данные фильтруются и сохраняются в локальном хранилище для последующего вывода или других действий;

— `find` - найти в локальном хранилище. Фраза для поиска указывается после команды. Сразу выводит данные. Поддерживаемые опции -insensetive, -full, -file, -sort;

— `show` - вывести данные из локального хранилища. Фильтры не удаляют данные, а только фильтуют вывод. Поддерживаемые флаги -full, -file, -sort;

— `filter` - удалить данные из локального хранилища согласно фильтрам.

Фильтры

Фильтры применяются в командах `get, show, filter`. Общий вид фильтра:

```
поле знак значение
```

Разные поля поддерживают разные знаки. Поля `id, grade, date` поддерживают три знака сравнения `> < =` .

Их можно комбинировать для получения диапазона. Например:

```
date > 10/12/2020-15:00 date < 10/12/2020-16:00
```

Команда задает диапазон времени от 15:00 до 16:00 включительно (секунды не учитываются).

Поля `subj, host, type, result` поддерживают только знак `=` и используют полное совпадение. Например `host = localhost.local` не совпадет с сообщениями в которых поле `host = localhost.localdomain`.

Флаги

`-sort` - сортирует вывод по указанному полю. Если название поля указанно со знаком минус, сортировка будет происходить в обратном порядке. Сортировка доступна по полям `id, type, date, subj, host, result, grade`. Сортировка по полю `grade` численная (default=0, green=1, yellow=2, red=3) Флаг учитывается в командах вывода: `show` и `find`.

`-file` - перенаправляет вывод в файл, имя которого указано сразу после флага. Вывод происходит в развернутом виде, считается что установлен флаг `-full`. Флаг учитывается в командах вывода: `show` и `find`.

`-full` - выводить данные в развернутом виде. По умолчанию вывод сообщения упаковывается в 4 строки. По несколько значений в каждой. Используется фиксированный размер каждого поля. Если значение не помещается в поле, оно обрезается и в конце добавляются … В развернутом виде на каждое поле сообщения - одна строка неограниченная размером. Флаг учитывается в командах вывода: `show` и `find`.

`-insensitive` - не учитывать регистр. Флаг учитывается в команде поиска find.

8.2. Правила аудита

Утилита auditctl предназначена для контроля службы и управления правилами правил аудита. В Таблица 34 приведены часто используемые опции утилиты auditctl. Подробное описание приведено в man auditctl.

Синтаксис:

```
auditctl <опции>
```

Таблица 34 – Опции утилиты auditctl

Опции	Описание
-a list,action	Добавление правила. В качестве параметра list указывают: - task – события, связанные с созданием процессов; - entry – события, происходящие при входе в системный вызов; - exit – события, происходящие во время выхода из системного вызова; - user – события с определенными UID, PID и GID; - exclude – используется для исключения событий. В качестве параметра action указывают: - never – события не записываются в журнал; - always – события записываются в журнал
-d list,action	Удаление правила
-D	Удаление всех правил
-l	Вывод списка текущих правил
-S SYSCALL NAME ИЛИ NUMBER	Указание системного вызова, на основании которого будет работать правило
-F	Дополнительные фильтры
-W PATH	Аудит файла
-R file	Чтение правил из файла

Примеры использования:

В результате выполнения этого правила будут записываться все файлы, открытые пользователем с идентификатором 1001:

```
# auditctl -a exit,always -S open -F auid=1001
```

В результате выполнения этого правила будут записываться события, связанные с файлом /etc/passwd:

```
# auditctl -w /etc/passwd -p wa
```

Утилита auditctl устанавливает временные правила. Для того, чтобы они стали

постоянными их необходимо прописать их в файл /etc/audit/audit.rules или в файлы каталога /etc/audit/rules.d. Для указания правил используется синтаксис утилиты auditctl. Подробное описание файлов приведено в man audit.rules. После добавления правил необходимо перезапустить службу аудита одной из следующих команд:

```
# systemctl restart auditd.service
```

8.3. Ротация журналов

За ротацию журналов отвечают параметры конфигурационного файла /etc/audit/auditd.conf:

```
num_logs = 5
max_log_file = 8
max_log_file_action = ROTATE
```

где

- `num_logs` – число журналов аудита, хранимых на диске;
- `max_log_file` – максимальный размер одного файла журнала (в МБ), по достижении которого будет выполнено действие, определенное параметром max_log_file_action;
- `max_log_file_action` – действие, выполняемое по достижении максимального размера журнала.

Подробное описание конфигурационного файла и его параметров приведено в man auditd.conf.

8.4. Настройка оповещения администратора

В ходе работы с ОС пользователь с ролью администратора может получать сообщения, свидетельствующие о критических изменениях в системе.

Создаем службу для оповещений об аварийном завершении других служб:

/etc/systemd/system/notify-admin@.service
с текстом:

```
[Unit]
Description=Notify about failures of %i
After=systemd-journald.service
[Service]
Type=oneshot
```

```
RemainAfterExit=no
ExecStart=/usr/bin/logger "FIA_SOS: service %i failed"

[Install]
WantedBy=multi-user.target
```

Делаем так, чтобы эта служба запускалась один раз при возникновении проблем в другой службе.

Делаем другую службу:

```
/etc/systemd/system/test-notify.service
```

с текстом:

```
[Unit]
Description=Test fail or success
OnFailure=notify-admin@test-notify.servic
[Service]
Type=oneshot
RemainAfterExit=no
ExecStart=/bin/sh -x -c 'exit 0'
[Install]
WantedBy=multi-user.target
```

Запускаем ее:

```
sudo systemctl start test-notify.service
```

читаем лог:

```
sudo systemctl status test-notify.service
```

Видим, что служба была завершена успешно.

В файле /etc/systemd/system/test-notify.service заменяем "exit 0" на "exit 1", тем самым эмулируя неуспешное завершение службы.

Перезапускаем тестовую службу:

```
sudo systemctl restart test-notify.service
```

При ее неуспешном завершении запускается служба notify-admin@ с подстановкой имени нашей тестовой службы. Смотрим лог:

```
sudo systemctl status notify-admin@test-notify.service
```

Убеждаемся, что в syslog была внесена соответствующая запись:

```
sudo journalctl -xb | grep FIA_SOS
```

Если при этом был открыт графический интерфейс rosa-central-panel "Аудит", то он

покажет всплывающее уведомление в трее о поступлении тревоги красного уровня, тем самым уведомив администратора о проблеме недоступности сервиса.

```
[user@rosa2019 Finale 2009]$ sudo journalctl -xb | grep SOS
янв 20 17:51:14 rosa2019.1 root[25567]: FIA_SOS: service test failed
янв 20 17:51:45 rosa2019.1 root[25591]: FIA_SOS: service test failed
янв 20 17:58:22 rosa2019.1 root[25855]: FIA_SOS: service test-notify failed
[user@rosa2019 Finale 2009]$ cat /etc/systemd/system/test-notify.service^C
[user@rosa2019 Finale 2009]$ sudo systemctl status notify-admin@test-notify.service
○ notify-admin@test-notify.service - Notify about failures of test-notify
     Loaded: loaded (/etc/systemd/system/notify-admin@.service; disabled; vendor preset: disabled)
     Active: inactive (dead) since Thu 2022-01-20 17:58:22 MSK; 1min 15s ago
    Process: 25855 ExecStart=/usr/bin/logger FIA_SOS: service test-notify failed (code=exited, status=0/SUCCESS)
   Main PID: 25855 (code=exited, status=0/SUCCESS)
        CPU: 15ms

янв 20 17:58:22 rosa2019.1 systemd[1]: Starting Notify about failures of test-notify...
янв 20 17:58:22 rosa2019.1 root[25855]: FIA_SOS: service test-notify failed
янв 20 17:58:22 rosa2019.1 systemd[1]: notify-admin@test-notify.service: Deactivated successfully.
янв 20 17:58:22 rosa2019.1 systemd[1]: Finished Notify about failures of test-notify.
[user@rosa2019 Finale 2009]$
```

Рисунок 125. Лог сообщений аудита

9. ОГРАНИЧЕНИЕ ПРОГРАММНОЙ СРЕДЫ

9.1. Киоск

Утилита ROSA-KIOSK предназначена для запуска системы в режиме киоска, т. е. в режиме доступности только выбранного функционала. Например, создадим профиль, в котором пользователю будет разрешено пользоваться только текстовым редактором KWrite (Рисунок 126).

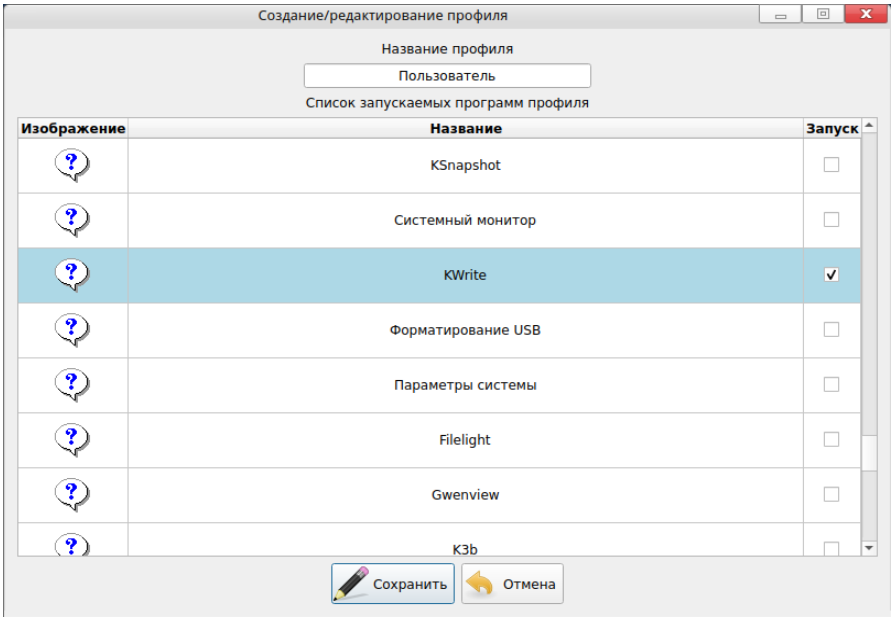


Рисунок 126. Создание профиля в ROSA-KIOSK

После входа пользователя в систему он увидит черный экран и только одну доступную для него программу, она и будет запущена (Рисунок 127).

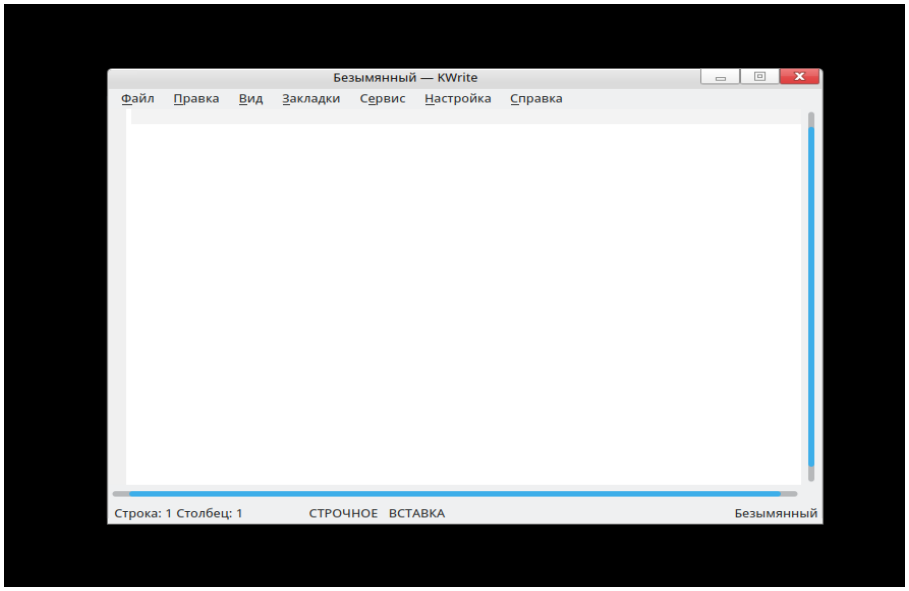


Рисунок 127. Работа в режиме Киоск

9.2. Проверка подписей исполняемых файлов

В ОС РОСА «НИКЕЛЬ» реализован запрет запуска исполняемых файлов не доверенного происхождения. Администратор сам управляет списком доверенных ключей.

Фиксируется состояние системы путем подписывания имеющихся в ней файлов, а иные файлы не могут быть запущены.

Описанные команды следует запускать от пользователя, где указано sudo — от пользователя с правами sudoers или от root без sudo.

При использовании системы со включенным SELinux загрузитесь в режиме permissive (enforcing=0).

Подготовка

Установите необходимые пакеты:

```
sudo dnf install ima-evm-utils libressl audit ima-inspect
```

Создание ключей

Создается пара ключей: закрытый и открытый ключи.

Закрытым ключом подписываются файлы, следовательно, к нему не должно быть доступа у тех, кто не должен иметь возможности подписать файлы, и рекомендуется хранить его отдельно, а не на машине, где выполняется запуск подписанных исполняемых файлов.

Открытый ключ должен быть установлен на каждой системе, на которой производится запуск подписанных исполняемых файлов, он используется для проверки валидности подписи. Открытый ключ хранится на диске и загружается в ключницу ядра в initrd.

Ниже описано создание ключевой пары по ГОСТ. Возможно применение RSA.

В текущей рабочей папке терминала создайте файл x509.conf со следующим текстом:

```
[ req ]
distinguished_name = req_distinguished_name
prompt = no
string_mask = utf8only
x509_extensions = myexts

[ req_distinguished_name ]
O = IMA
```

```
CN = Executable Signing Key
emailAddress = ivan@petrov.tld

[ myexts ]
basicConstraints=critical,CA:FALSE
keyUsage=digitalSignature
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid
```

Значения полей `O`, `CN`, `emailAddress` являются произвольными, можно заменить их на свои. Месторасположение файла не играет роли, он нужен только для создания пары ключей один раз.

Далее создайте пару ключей:

```
libressl req -new -nodes -utf8 -batch -newkey gost2001 -pkeyopt dgst:streebog512 -pkeyopt paramset:A -streebog512 -days 109500 -x509 -config x509.conf -outform DER -out ima_cert.der -keyout ima_priv.pem
```

где `ima_cert.der` — открытый ключ, `ima_priv.pem` — закрытый.

Создайте каталог с открытыми ключами:

```
sudo mkdir -p /etc/keys/ima
```

Все ключи из этого каталога будут импортированы в ядро на этапе initrd.

Скопируйте созданный открытый ключ в этот каталог:

```
sudo cp -v ima_cert.der /etc/keys/ima/ima_cert.der
```

Создание политики IMA

Создайте файл /etc/sysconfig/ima-policy (запуская текстовый редактор) со следующим содержимым:

```
# PROC_SUPER_MAGIC
dont_measure fsmagic=0x9fa0
dont_appraise fsmagic=0x9fa0
# SYSFS_MAGIC
dont_measure fsmagic=0x62656572
dont_appraise fsmagic=0x62656572
# DEBUGFS_MAGIC
dont_measure fsmagic=0x64626720
dont_appraise fsmagic=0x64626720
# TMPFS_MAGIC
dont_measure fsmagic=0x01021994
```

```
dont_appraise fsmagic=0x01021994
# RAMFS_MAGIC
dont_appraise fsmagic=0x858458f6
# DEVPTS_SUPER_MAGIC
dont_measure fsmagic=0x1cd1
dont_appraise fsmagic=0x1cd1
# BINFMTFS_MAGIC
dont_measure fsmagic=0x42494e4d
dont_appraise fsmagic=0x42494e4d
# SECURITYFS_MAGIC
dont_measure fsmagic=0x73636673
dont_appraise fsmagic=0x73636673
# SELINUX_MAGIC
dont_measure fsmagic=0xf97cff8c
dont_appraise fsmagic=0xf97cff8c
# CGROUP_SUPER_MAGIC
dont_measure fsmagic=0x27e0eb
dont_appraise fsmagic=0x27e0eb
# CGROUP2_SUPER_MAGIC
dont_measure fsmagic=0x63677270
dont_appraise fsmagic=0x63677270
# NSFS_MAGIC
dont_measure fsmagic=0x6e736673
dont_appraise fsmagic=0x6e736673

appraise func=BPRM_CHECK appraise_type=imasig
appraise func=BPRM_CHECK appraise_type=imasig
appraise func=FILE_MMAP mask=MAY_EXEC appraise_type=imasig
appraise func=FILE_MMAP mask=MAY_EXEC appraise_type=imasig
#appraise func=MODULE_CHECK appraise_type=imasig
#appraise func=FIRMWARE_CHECK appraise_type=imasig
# this is only for newer kernels that support loading policies
# from file by writing the file path to the ima sysfs node
#appraise func=POLICY_CHECK appraise_type=imasig
```

Выставьте права на этот файл:

```
sudo chmod 0400 /etc/sysconfig/ima-policy
```

В процессе работы системы содержимое политики доступно по адресу /sys/kernel/security/ima/policy с правами 0400, поэтому для единообразия запретим всем, кроме root, читать этот файл. Так нельзя будет узнать применяемую политику IMA без root-прав.

Подписывание файлов в системе

Теперь необходимо подписать все исполняемые файлы, в т.ч. скрипты, иные файлы, которые mmap()-ятся с PROT_EXEC, в т.ч. разделяемые библиотеки *.so*.

Для подписывания выполните следующие действия:

```
FS="$(findmnt --output FSTYPE / | tail -n1)"
echo "$FS"
touch failed.log

set -x; find / -fstype "$FS" -type f -executable | sort -u | while read -r line ; do if ! evmctl ima_sign --hashalgo streebog512 --key ima_priv.pem "$line" ; then echo "$line" >> failed.log; fi; done ; set +x

set -x; for D in /lib /lib64 /usr/lib /usr/lib64; do find "$D" -fstype $FS -\! -executable -type f -name "*.so*" | sort -u | while read -r line ; do if ! evmctl ima_sign --hashalgo streebog512 --key ima_priv.pem "$line"; then echo "$line" >> failed.log; fi; done; done; set +x
```

Выполните

```
cat failed.log
```

и убедитесь, что этот файл пуст, а значит в процессе подписывания не возникло ошибок.

Сборка initrd с поддержкой IMA

Создайте файл /etc/dracut.conf.d/10-ima.conf (запуская текстовый редактор) со следующим содержимым:

```
add_dracutmodules+=" integrity "
```

Следующая команда пересобериет initrd:

```
sudo systemd-initramfs-gen
```

Обратите внимание, что в initrd должны попасть уже подписанные файлы.

Пробный запуск подписанной системы

Запустите систему с добавлением

```
ima_appraise=log
```

в cmdline ядра, добавив это непосредственно в загрузчике Grub или в /etc/default/grub в переменной GRUB_CMDLINE_LINUX_DEFAULT и выполнив команду `sudo update-grub2`.

В этом режиме система не будет запрещать запуск неподписанных файлов, но будет записывать попытки их запуска. Посмотрите, нет ли в логе событий безопасности сообщений от IMA:

```
sudo grep -i ima /var/log/audit/audit.log
```

В логе аудита не должно быть записей.

Проверьте наличие подписи у файлов:

```
[root@rosa2019 ~]# ima_inspect /bin/bash
/bin/bash

security.ima
------------
digital signature version 2
digest algorithm: streebog512
key-id v2 (gpg compatible): 5ac982c4
signature length: 1024 bits
signature data:

afbe5f078a9a052c        eda2683037c92b40        dab77e6f7fcf2d42
bdce159ef64097ad  9db7b39124fa9f5c  ea04c010248e65d4  6ce4d8dcf692d124
62447ccdf53e979c
16ca24090c175f55        81218c5e024a5d6e        57c81d2511bc1311
0b9479aaa04605a5  cbf0b5c1f64aca04  47ab95abd392de8c  08d2683bc1f3c4a4
e6355635c1608671



security.evm
------------
no such attribute
[root@rosa2019      ~]#      evmctl      ima_verify      --key
/etc/keys/ima/ima_cert.der /bin/bash
key 1: 5ac982c4 /etc/keys/x509_evm.der
```

```
/bin/bash: verification is OK
[root@rosa2019 ~]#
```

Запуск и проверка работы

Запустите без `ima_appraise=log`. Система должна запуститься и работать штатно.

Теперь проверим работу защиты от запуска неподписанных исполняемых файлов.

Создайте копию существующего исполняемого файла:

```
cp -v /bin/cat cat.copy
```

Дайте ему права на исполнение:

```
chmod +x cat.copy
```

Попробуйте его запустить и получите ошибку:

```
$ ./cat.copy
-bash: ./cat.copy: Отказано в доступе
```

При этом в логе аудита появляется запись о запрете запуска неподписанного файла:

```
# grep -i ima /var/log/audit/audit.log | tail -n 1
type=INTEGRITY_DATA msg=audit(1610966070.898:250): pid=7021 uid=0 auid=1000 ses=2 op=appraise_data cause=IMA-signature-required comm="bash" name="/root/cat.copy" dev="sda2" ino=2759743 res=0 errno=0
```

9.3. Системный менеджер systemd

Для управления системой применяется системный менеджер systemd. Systemd был разработан с учетом обратной совместимости со сценариями, инициализации SysV, и предлагает такие возможности, как параллельный запуск системных служб во время загрузки системы, активация демонов по требованию, поддержка снимков ОС, а также логику управления службами на основе зависимостей.

Системный менеджер оперирует специальными файлами конфигурации – юнитами. Каждый юнит представляет из себя конфигурационный файл и отвечает за отдельно взятую службу, точку монтирования, подключаемое устройство, файл подкачки, виртуальную машину и т.п.

Таблица 35 – Юниты system

Юнит	Описание
service	Конфигурация служб или ПО
target	Конфигурация группы юнитов systemd

Юнит	Описание
automount	Конфигурация точек автоматического монтирования ФС
device	Конфигурация устройств
mount	Конфигурация точек монтирования ФС
path	Описание файлов или каталогов ФС
scope	Конфигурация наборов системных процессов, созданных извне systemd
slice	Конфигурация группы иерархически организованных юнитов, управляющих системными процессами
snapshot	Сохраненное состояние менеджера systemd
socket	Описание сокета для обмена информацией между процессами
swap	Описание устройства или файла подкачки
timer	Описание таймеров systemd

Системные юниты хранятся в каталогах:

- /etc/systemd/system – каталог для юнитов администраторов системы;
- /run/systemd/system – каталог для динамически создаваемых юнитов;
- /lib/systemd/system – каталог для юнитов, которые поставляются с установленным ПО.

Конфигурация systemd по умолчанию определяется в файле /etc/systemd/system.conf, где ее можно просмотреть. При необходимости изменить параметры по умолчанию и глобально переопределить отдельные значения юнитов systemd, используйте этот файл.

Юниты служб имеют расширение .service и служат для тех же самых целей, что и сценарии инициализации. Чтобы просмотреть, запустить, остановить, перезапустить, включить или отключить системные службы, используйте команду `systemctl`. . Подробное описание приведено в man systemctl.

Синтаксис:

```
systemctl <опции> <команда> <юнит>
```

В ОС предусмотрено несколько режимов работы, которые соответствуют целям (юнитам типа target) системного менеджера systemd. Основные режимы работы представлены в Таблица 36.

Таблица 36 – Режимы работы ОС

Цель systemd	Режим
poweroff.target	Завершение работы и выключение системы
rescue.target	Режим восстановления (консольный однопользовательский режим работы)

Цель systemd	Режим
emergency.target	Аварийный режим (консольный однопользовательский режим работы)
multi-user.target	Консольный режим (консольный многопользовательский режим работы)
graphical.target	Графический режим (графический многопользовательский режим работы)
reboot.target	Перезагрузка системы

Эксплуатация ОС пользователем осуществляется в консольном и графическом режимах. Аварийным режим предназначен для восстановления системы после сбоев или ошибок, возникших в процессе эксплуатации. Выполнение действий в аварийном режиме доступно только администратору безопасности (владельцу учетной записи суперпользователя).

9.3.1. Юниты типа target

Режимы работы ОС описываются юнитами типа target (юниты цели). Для запуска юнита типа target используется значение «isolate» в поле <команда>. Следующие команды можно использовать для смены режима работы ОС:

```
# systemctl isolate TARGET.target
# systemctl TARGET
```

где

- «`TARGET.target`» – полное наименование юнита типа target или полное наименование режима работы ОС; полные наименования режима работы ОС (см.) ;
- «`TARGET`» – сокращенное наименование юнита типа target или сокращенное наименование режима работы (без конструкции «.target»).

Например, юнит graphical.target, используемый для запуска графического сеанса работы, запускает системные службы, такие как менеджер графического входа в систему GNOME Display Manager (gdm.service) или служба учетных записей (accounts-daemon.service), а также включает юнит multi-user.target. Далее юнит multiuser.target запускает другие важные службы.

В состав ОС РОСА «НИКЕЛЬ» входит несколько предварительно настроенных юнитов типа target, которые представлены в таблице ниже.

Таблица 37 – Юниты типа target

Юниты .target	Описание
runlevel0.target, poweroff.target	Завершение работы и выключение ОС
runlevel1.target, rescue.target	Аварийный командный интерпретатор
runlevel2.target, multi-user.target	Многопользовательская ОС без графического режима

runlevel3.target, multi-user.target	Многопользовательская ОС без графического режима
runlevel4.target, multi-user.target	Многопользовательская ОС без графического режима
runlevel5.target, graphical.target	Многопользовательская ОС с графическим режимом
runlevel6.target, reboot.target	Выключение и перезагрузка ОС

Чтобы просмотреть, изменить или настроить target systemd, используйте утилиту `systemctl`.

Чтобы узнать, какая из целей используется по умолчанию, выполните следующую команду:

```
$ systemctl get-default
```

Чтобы получить список всех юнитов цели, загруженных на данный момент, выполните следующую команду:

```
$ systemctl list-units --type target
```

Для каждого юнита цели данная команда показывает его полное имя (`UNIT`), примечание, был ли юнит загружен (`LOAD`), статус его высокоуровневой (`ACTIVE`) и низкоуровневой (`SUB`) активаций, а также короткое описание (`DESCRIPTION`). По умолчанию команда `systemctl list-units` показывает только активные юниты. Чтобы просмотреть список всех загруженных юнитов вне зависимости от их статуса, выполните эту команду с ключом `--all` или `-a`:

```
systemctl list-units --type target --all
```

Чтобы установить другую цель в текущем сеансе, выполните следующую команду:

```
# systemctl isolate <имя>.target
```

Замените параметр `<имя>` на имя юнита цели, который нужно использовать, например, `multiuser`. Данная команда запускает юнит цели с указанным именем со всеми юнитами-зависимостями и немедленно останавливает все остальные.

9.3.2. Управление системными службами

Управление службами или ПО описывается юнитами типа service. Для управления юнитами типа service в основном используются значения «start», «stop», «restart», «try-restart», «kill», «status», «enable», «disable», «mask», «unmask» в поле <Команда>. В Таблица 38 приведены команды для управления юнитами типа service. Юнит «SERVICE.service» – это полное наименование юнита типа service.

Таблица 38 – Управление юнитами типа service с помощью утилиты systemctl

Команда	Описание
systemctl start SERVICE.service	Запуск юнита

Команда	Описание
systemctl stop SERVICE.service	Остановка юнита
systemctl restart SERVICE.service	Перезапуск юнита
systemctl try-restart SERVICE.service	Перезапуск юнита, если он запущен
systemctl kill SERVICE.service	Принудительная остановка юнита
systemctl status SERVICE.service	Отображение состояния юнита
systemctl enable SERVICE.service	Включение юнита в автозагрузку
systemctl disable SERVICE.service	Выключение юнита из автозагрузки
systemctl mask SERVICE.service	Запрет запуска юнита
systemctl unmask SERVICE.service	Разрешение запуска юнита

Пример использования:

В результате выполнения этой команды произойдет перезапуск службы (сервиса) auditd:

```
# systemctl restart auditd.service
```

Для управления состоянием юнитов типа service также предназначена утилита service. Подробное описание приведено в man service.

Синтаксис:

```
service <юнит типа service> <команда>
```

Чтобы получить список загруженных на данный момент служб, выполните следующую команду:

```
$ systemctl list-units --type service
```

Для каждого файла юнита службы эта команда покажет его полное имя `(UNIT)`, примечание о том, был ли файл юнита загружен `(LOAD)`, статус активации файла юнита высокого `(ACTIVE)` и низкого уровня `(SUB)`, а также короткое описание `(DESCRIPTION)`.

По умолчанию команда systemctl list-units отображает только активные юниты. Чтобы просмотреть все загруженные юниты независимо от их статуса, выполните эту команду с ключом `--all` или `-a`:

```
$ systemctl list-units --type service --all
```

Также можно получить список всех доступных юнитов служб, чтобы узнать, включены ли они. Для этого выполните:

```
$ systemctl list-unit-files --type service
```

Для каждого юнита службы эта команда показывает его полное имя `(UNIT FILE)` и данные о том, включен ли юнит службы или нет `(STATE)`.

Чтобы просмотреть подробную информацию о юните службы, соответствующем системной службе, выполните следующую команду:

```
$ systemctl status <имя>.service
```

Замените <имя> именем юнита службы, которую нужно просмотреть (например, gdm). Данная команда отобразит имя выбранной службы, ее короткое описание, одно или несколько полей, указанных ниже в «Доступная информация о юнитах служб», и, в случае запуска команды с правами администратора (sudo -i), также недавние записи в журнале службы.

Таблица 39 – Доступная информация о юнитах служб

Поле	Описание
loaded	Была ли загружена служба, абсолютный путь до файла юнита, а также примечание о том, включен ли юнит.
active	Выполняется ли юнит службы, а также указывается метка времени
main pid	PID соответствующей системной службы, а также указывается имя службы
status	Дополнительная информация о соответствующей системной службе
process	Дополнительная информация о связанных процессах
cgroup	Дополнительная информация о связанных контрольных группах (cgroups).

Чтобы только проверить, выполняется ли конкретная служба, выполните:

```
$ systemctl is-active <имя>.service
```

Чтобы определить, включен ли юнит конкретной службы, выполните:

```
$ systemctl is-enabled <имя>.service
```

Для управления состоянием юнитов юнитами типа service обычно используются значения «start», «stop», «restart», «try-restart», «status» в поле <Команда>. В приведены команды для управления юнитами типа service. Юнит «SERVICE» - это сокращенное наименование юнита типа service (без конструкции «.service»).

Таблица 40 – Управление юнитами типа service с помощью утилиты service

Команда	Описание
service SERVICE start	Запуск юнита
service SERVICE stop	Остановка юнита
service SERVICE restart	Перезапуск юнита
service SERVICE try-restart	Перезапуск юнита, если он запущен
service SERVICE status	Отображение состояния юнита

Пример использования:

В результате выполнения этой команды произойдет перезапуск службы (сервиса) auditd:

```
# service auditd restart
```

Чтобы завершить работу ОС и выключить питание ПК, выполните следующую команду:

```
# systemctl poweroff
```

Чтобы завершить работу ОС без отключения питания, выполните:

```
# systemctl halt
```

По умолчанию при запуске одной из этих команд systemd посылает информационное сообщение всем пользователям, на данный момент выполнившим вход в систему. Чтобы systemd не посылал этого сообщения, выполните указанную команду с ключом `--no-wall`, например:

```
systemctl --no-wall poweroff
```

Также для выключения системы и для обесточивания машины в определенное время, выполните следующую команду:

```
# shutdown --poweroff чч:мм
```

Здесь `чч:мм` — это время в 24-часовом формате. За 5 минут до выключения системы создается файл /run/nologin, запрещающий пользователям вход в систему. При использовании аргумента времени к команде можно добавить необязательное сообщение `wall`.

Чтобы выключить и остановить систему после некоторой задержки без отключения питания ПК, выполните:

```
# shutdown --halt +<m>
```

Здесь `+<m>` — время задержки в минутах. Ключевое слово `now` является псевдонимом для `+0`.

Пользовательможет отменить ожидаемое выключение следующим образом:

```
# shutdown -c
```

Дополнительные возможности и параметры см. на странице руководства shutdown(8).

Чтобы перевести систему в спящий режим, выполните следующую команду:

```
# systemctl hibernate
```

Данная команда сохраняет состояние системы на жесткий диск и выключает питание. Далее при повторном включении ПК система восстанавливает свое состояние из сохраненных данных без необходимости в полной загрузке. Поскольку состояние системы сохраняется на жестком диске, а не в оперативной памяти, отпадает необходимость поддерживать электропитание для модулей ОЗУ, но, соответственно, процесс восстановления системы из спящего режима происходит значительно

медленнее, чем из режима ожидания. Чтобы перевести систему в гибридный спящий режим, выполните:

```
# systemctl hybrid-sleep
```

9.3.3. Управление systemd на удаленной машине

Помимо локального управления systemd и service manager, утилита systemctl также предоставляет возможность взаимодействия с systemd на удаленной машине с использованием протокола SSH. При условии, что на удаленной машине служба выполняется sshd, подключиться к этой машине можно, выполнив команду systemctl с ключом --host или -H:

```
systemctl --host <имя_пользователя>@<имя_хоста> <команда>
```

Замените <имя_пользователя> именем удаленного пользователя, <имя_хоста> — именем хоста машины, а <команду> — одной из команд systemctl, описанных выше. Обратите внимание, что для того, чтобы указанный пользователь смог получить удаленный доступ с использованием протокола SHH, удаленная машина должна быть настроена так, чтобы разрешить ему сделать это.

9.3.4. Установка режима восстановления и аварийного режима

Режим восстановления (rescue) предоставляет удобное однопользовательское окружение, в котором администратор имеет возможность исправить ошибки в системе, препятствующие ее нормальной загрузке. В режиме восстановления система пытается смонтировать все локальные ФС и запустить некоторые важные системные службы, но не активирует сетевые интерфейсы и не позволит другим пользователям выполнить одновременный вход. В ОС РОСА «НИКЕЛЬ» режим восстановления равноценен однопользовательскому режиму и требует пароля root а также включенного входа под пользователем root (по-умолчанию выключено).

Чтобы сменить текущую цель и войти в режим восстановления в текущем сеансе, выполните следующую команду:

```
# systemctl rescue
```

Данная команда аналогична команде `systemctl isolate rescue.target`, но помимо прочего также посылает информационное сообщение всем пользователям, выполнившим на данный момент вход в систему. Чтобы systemd не посылал этого сообщения, выполните данную команду с ключом `--no-wall`:

```
systemctl --no-wall rescue
```

Аварийный режим (emergency) предоставляет самое минимальное окружение из всех возможных, которое позволяет исправить ошибки системы даже в тех ситуациях, когда она не в состоянии войти в режим восстановления. В аварийном режиме ОС монтирует корневую ФС только для чтения, не пытается смонтировать никаких других локальных ФС, не активирует сетевые интерфейсы и запускает только несколько самых важных служб. В ОС РОСА «НИКЕЛЬ» аварийный режим требует пароля root.

Чтобы сменить текущую цель и войти в аварийный режим, выполните следующую команду с привилегиями суперпользователя:

```
# systemctl emergency
```

Данная команда аналогична команде `systemctl isolate emergency.target`, но помимо прочего также посылает информационное сообщение всем пользователям, выполнившим на данный момент вход в систему. Чтобы systemd не посылал этого сообщения, выполните данную команду с ключом `--no-wall`:

```
# systemctl --no-wall emergency
```

9.3.5. Создание и изменение файлов юнитов systemd

Файл юнита содержит конфигурационные директивы, описывающие юнит и определяющие его поведение. Несколько команд systemctl работают с файлами юнита в фоновом режиме. Чтобы более тонко отрегулировать поведение юнита, системный администратор должен отредактировать файл вручную. В таблице «Местоположение файлов юнитов systemd» приводятся три основных каталога, в которых располагаются файлы юнитов. Каталог /etc/systemd/system/ зарезервирован для файлов юнитов, созданных или измененных системным администратором.

Имена файлов юнитов имеют формат «<имя_юнита>.<тип_расширение>». Полный список типов юнитов см. в В системе обычно присутствуют юниты sshd.service и sshd.socket.

Файлы юнитов могут быть дополнены каталогом для дополнительных конфигурационных файлов. Чтобы, например, добавить пользовательские параметры в sshd.service, создайте файл sshd.service.d/custom.conf и поместите в него дополнительные директивы.

Также можно создать каталоги sshd.service.wants/ и sshd.service.requires/, содержащие символьные ссылки на файлы юнитов, которые являются зависимостями службы sshd. Эти символьные ссылки автоматически создаются либо во время процесса установки согласно параметрам для файлов юнитов, указанным в разделе [Install, либо в

процессе работы, согласно параметрам, раздела [Unit]. Также можно создать эти каталоги и символьные ссылки вручную.

Многие параметры файлов юнитов можно настроить с помощью так называемых спецификаторов юнитов — записей с символами замены, динамически заменяемых параметрами юнитов при загрузке файлов юнитов. Это дает возможность создавать универсальные файлы юнитов, служащие шаблонами для создаваемых экземпляров.

Структура файла юнита

Файл юнита обычно состоит из трех разделов:

1) `[Unit]` — содержит общие параметры, не зависящие от типа юнита. Эти параметры предоставляют описание юнита, определяют его поведение и настраивают зависимости для других юнитов. Список наиболее часто используемых параметров `[Unit]` см. в .

2) `[unit type]` — если у юнита есть директивы, характерные для данного типа юнита, они собраны в разделе, названном по типу юнита. Файлы юнитов служб, например, содержат раздел `[Service]`. Список наиболее часто используемых параметров `[Service]` см. Таблица 42.

3) `[Install]` — содержит информацию об установке юнитов, которая используется командами `systemctl enable` и `disable`. Список параметров `[Install]` см. .

Таблица 41 – Важные параметры раздела [Unit]

Параметр	Описание
description	Значимое описание юнита. Этот текст показывается, например, в выводе команды `systemctl status`
documentation	Список адресов URI, ссылающихся на документацию для данного юнита
after	Определяет порядок, в котором запускаются юниты. Юнит начинает работу только после того, как становятся активными юниты, указанные параметром `After`. В отличие от параметра `Requires`, параметр `After` не выполняет явную активацию указанных юнитов. Параметр `Before` имеет действие, противоположное параметру `After`
requires	Настраивает зависимости от других юнитов. Юниты, перечисленные в параметре `Requires`, активируются вместе с изначальным юнитом. Если запуск какого-то из перечисленных юнитов окончится неудачей, изначальный юнит не будет активирован

wants	Настраивает более слабые зависимости, чем `Requires`. Если запуск какого-то из перечисленных юнитов окончится неудачей, это не повлияет на запуск исходного юнита. Это рекомендованный способ настройки пользовательских зависимостей юнитов
conflicts	Настраивает отрицательные зависимости, в противоположность `Requires`

Таблица 42– Важные параметры раздела [Service]

Параметр	Описание
Type	Настраивает тип запуска процесса юнита, влияющий на функционал `ExecStart` и связанные с ним параметры. Может быть одним из: • `simple` — значение по умолчанию. Процесс, запущенный с помощью ExecStart, является главным процессом службы; • `forking` — процесс, запущенный с помощью ExecStart, порождает другой процесс, который становится главным процессом службы. После завершения запуска родительский процесс завершается; • `oneshot` — этот тип аналогичен типу `simple`, но процесс завершается до запуска последующих юнитов; • `dbus` — этот тип аналогичен типу `simple`, но последующие юниты запускаются только после того, как главный процесс получает имя D-Bus; • `notify` — этот тип аналогичен типу `simple`, но последующие юниты запускаются только после того, как будет послано уведомительное сообщение с помощью функции sd_notify(); • `idle` — аналогичен `simple`. Фактическое выполнение бинарного файла службы откладывается до окончания выполнения всех задач, что помогает избежать смешения вывода сообщений статуса с выводом сообщений служб из командного интерпретатора
ExecStart	Указывает команды или сценарии, которые должны выполняться при запуске юнита. `ExecStartPre` и `ExecStartPost` указывают на пользовательские команды, которые должны запуститься до и после `ExecStart`. `Type=oneshot` включает возможность указать несколько пользовательских команд, которые затем выполняются последовательно
ExecStop	Указывает команды или сценарии, которые должны выполняться при остановке юнита
ExecReload	Указывает команды или сценарии, которые должны выполняться при перезагрузке юнита

Restart	Если этот параметр включен, после завершения ее процесса служба перезапускается, за исключением «чистой остановки» (clean stop), выполненной с помощью команды systemctl
RemainAfterExit	Если значение установлено как истинное, служба считается активной даже после завершения всех ее процессов. Значение по умолчанию — неверно. Этот параметр особенно полезен при настроенном параметре `Type=oneshot`

Таблица 43 – Важные параметры раздела [Install]

Параметр	Описание
Alias	Предоставляет список дополнительных имен юнита, разделенных пробелами. Большинство команд systemctl, исключая `systemctl enable`, вместо фактических имен юнитов могут использовать псевдонимы
RequiredBy	Список юнитов, зависящих от данного юнита. При включении данного юнита юниты, перечисленные в `RequiredBy`, получают зависимость `Require` относительно данного юнита
WantedBy	Список юнитов со слабой зависимостью от данного юнита. При включении данного юнита юниты, перечисленные в `WantedBy`, получают зависимость Want относительно данного юнита
Also	Указывает список юнитов, которые должны быть установлены или удалены вместе с данным юнитом
DefaultInstance	Этот параметр ограничен создаваемыми экземплярами юнитов и указывает экземпляр по умолчанию, для которого включается юнит

9.4. Планировщик заданий

Служба crond предназначена для выполнения программ по расписанию. Подробное описание работы службы приведено в man crond. Служба постоянно проверяет свои конфигурационные файлы (файлы расписаний) и выполняет программы согласно временным параметрам их запуска. К конфигурационным файлам относятся:

- файлы пользователей в каталоге /var/spool/cron;
- общесистемные файлы: /etc/crontab, файлы каталога/etc/cron.d, /etc/cron.minutely, /etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly, /etc/cron.monthly.

Утилита crontab предназначена для создания расписания выполнения программ. В Таблица 44 приведены часто используемые опции утилиты crontab. Подробное

описание приведено в man crontab.

Синтаксис:

```
crontab <опции>
```

Таблица 44 – Опции утилиты crontab

Опции	Описание
-e	Редактирование расписание пользователя
-l	Вывод расписания пользователя
-r	Удаление расписания пользователя
-u user	Указание пользователя, с расписанием которого планируется работа

Примеры использования:

В результате выполнения этой команды откроется окно редактирования расписания администратора:

```
# crontab -e
```

В результате выполнения этой команды откроется окно редактирования расписания для пользователя user1:

```
# crontab -u user1 -e
```

Форматы записей расписания:

```
<минута> <час> <день> <месяц> <день недели> <команда>
<переменная cron> <команда>
```

Описание полей записи расписания приведено в Таблица 45.

Таблица 45 – Поля записей crontab

Поля	Описание
<минута>	Значение в диапазоне от 0 до 59
<час>	Значение в диапазоне от 0 до 23
<день>	Значение в диапазоне от 1 до 31
<месяц>	Значение в диапазоне от 1 до 12 или в буквенном варианте: jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec
<день недели>	Значение в диапазоне от 0 до 6 (0 – это воскресенье) или в буквенном варианте: sun, mon, tue, wed, thu, fri, sat
<переменная cron>	@reboot – Запуск при загрузке; @yearly – Раз в год (эквивалентно 0 0 1 1 *); @annually – Раз в год (эквивалентно 0 0 1 1 *); @monthly – Раз в месяц (эквивалентно 0 0 1 * *); @weekly – Раз в неделю (эквивалентно 0 0 * * 0); @daily – Раз в день (эквивалентно 0 0 * * *); @midnight – В полночь (00:00); @hourly – Каждый час (эквивалентно 0 * * * *)

Поля	Описание
<команда>	Описание действий, которые необходимо выполнить

После завершения работы утилиты crontab все правила будут добавлены в файл пользователя в каталоге /var/spool/cron/crontabs; добавленные команды будут запускаться от того пользователя, от которого они были добавлены.

9.5. Менеджер пакетов

Управление программными пакетами осуществляется с помощью утилит командной строки rpm, dnf.

9.5.1. Управление с помощью командной строки

Утилита dnf предназначена для работы с программными пакетами. Подробное описание опций утилиты приведено в man dnf.

Синтаксис:

```
sudo dnf <опции> <команда> <пакет>
```

Поле <Команда> определяет одно из действий, представленных в Таблица 46. Дополнительные команды приведены в man dnf.

Таблица 46 – Значение поля <Команда> утилиты dnf

Команда	Описание
install	Установка пакета
reinstall	Переустановка пакета
check-update	Проверка наличия обновлений
update	Обновление пакета
remove	Удаление пакета
list	Вывод имен всех доступных и установленных пакетов
search	Поиск пакета
info	Вывод информации о пакете
groupinstall	Установка группы пакетов
groupupdate	Обновление группы пакетов
groupremove	Удаление группы пакетов
grouplist	Вывод информации о группах
repolist	Вывод списка подключенных репозиториев
repolist all	Вывод списка репозиториев
history	Дает информацию о выполненных командах, о датах и времени их выполнения, о числе затронутых пакетов, о том, были ли эти транзакции успешными или же были прерваны, и была ли изменена база данных RPM в промежуток между транзакциями.

Все команды поиска предоставляют пользователю возможность фильтрации результата с помощью добавления одного или более шаблонов выражений в качестве аргумента. Шаблоны выражений — это обычные строки символов, содержащие один или несколько символов подстановки «*» (который расширяется до соответствия любому поднабору знаков) и символа «?» (который расширяется до соответствия любому одиночному символу).

Не забывайте об экранировании шаблонов выражений, указывая их в качестве аргументов для команды. В противном случае командный интерпретатор обработает эти выражения как расширения имени пути и может передать все файлы в текущем каталоге, совпадающие с шаблоном. Чтобы корректно передать все шаблоны выражений, используйте один из следующих приемов:

— Экранируйте символы подстановки, поставив перед ними символ косой черты.

— Заключите все выражение-шаблон в одинарные или двойные кавычки.

Примеры использования:

1. В результате выполнения этой команды произойдет установка пакета mc:

```
dnf install mc
```

Отметим, что команде `install` не требуются четкие аргументы. Она может обрабатывать различные форматы имен пакетов и шаблонов выражений, что облегчает пользователям установку. С другой стороны, на корректную обработку команды менеджеру пакетов требуется время, особенно если было указано большое число пакетов. Для оптимизации поиска пакетов можно использовать следующие команды, явным образом указывающие, как именно необходимо обрабатывать аргументы:

```
sudo dnf install-n <имя>
sudo dnf install-na <имя.архитектура>
sudo dnf install-nevra <имя-epoch:версия-релиз.архитектура>
```

При использовании аргумента `install-n` команда `dnf` воспринимает имя как точное имя пакета. Команда `install-na` указывает, что последующий аргумент содержит имя пакета и архитектуру, разделенные символом точки. С аргументом `installnevra` команда ожидает аргумента в виде `<имя-epoch:версиярелиз.архитектура>`. Точно так же при поиске пакетов для удаления можно использовать команды:

```
sudo dnf remove-n
sudo dnf remove-na
sudo dnf remove-nevra
```

2. В результате выполнения этой команды произойдет обновление пакета mc:

```
dnf update mc
```

3. В результате выполнения этой команды произойдет удаление пакета mc:

```
dnf remove mc
```

9.6. Установка стороннего ПО

Установка Стороннего ПО происходит согласно процедуре проверки подписей исполняемых файлов и рассмотрена выше в разделе 9.2. Проверка подписей исполняемых файлов данного руководства.

10. ИДЕНТИФИКАЦИЯ И КОНТРОЛЬ ДОСТУПА УСТРОЙСТВ

10.1. ROSA Removable Drive Manager

Приложение ROSA Removable Drive Manager предназначено для разграничения доступа к съемным носителям памяти, таким как usb-накопители, жесткие диски, приводы оптических дисков.

Далее рассмотрим основные принципы работы приложения.

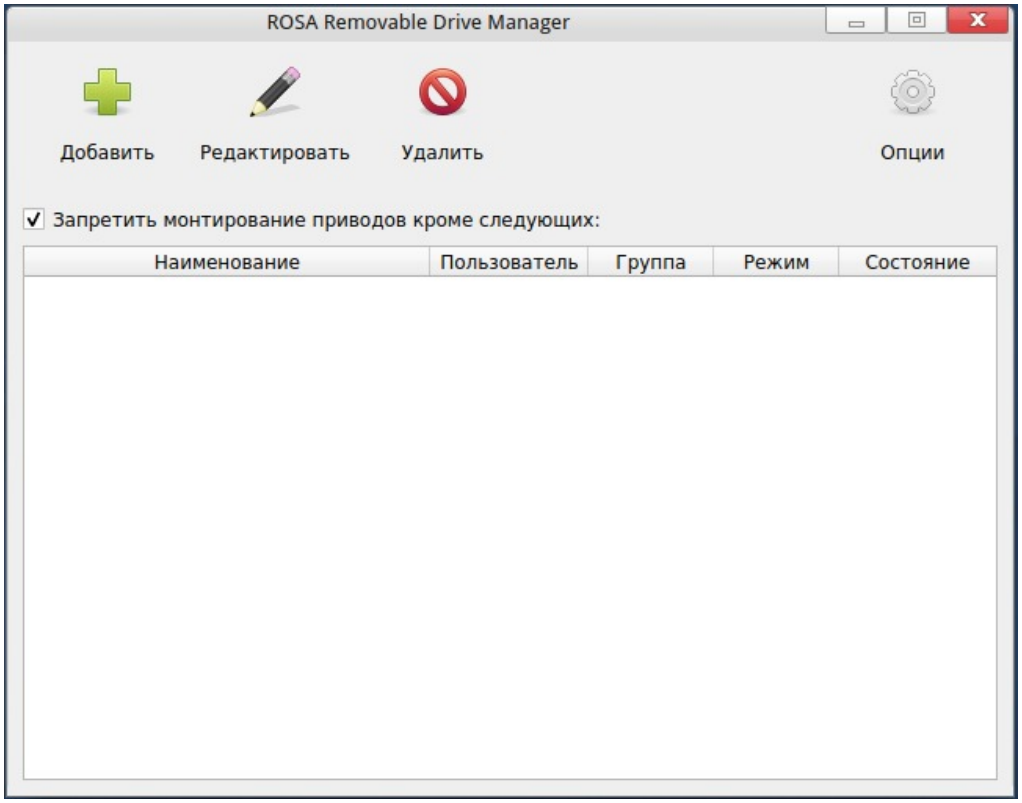


Рисунок 128. Интерфейс ROSA Removable Drive Manager

Для добавления устройства и назначения ему права доступа необходимо кликнуть на кнопку [Добавить] на панели инструментов. Далее в появившемся диалоговом окне необходимо задать права доступа (Рисунок 129). После этого устройство появится в списке контролируемых устройств.

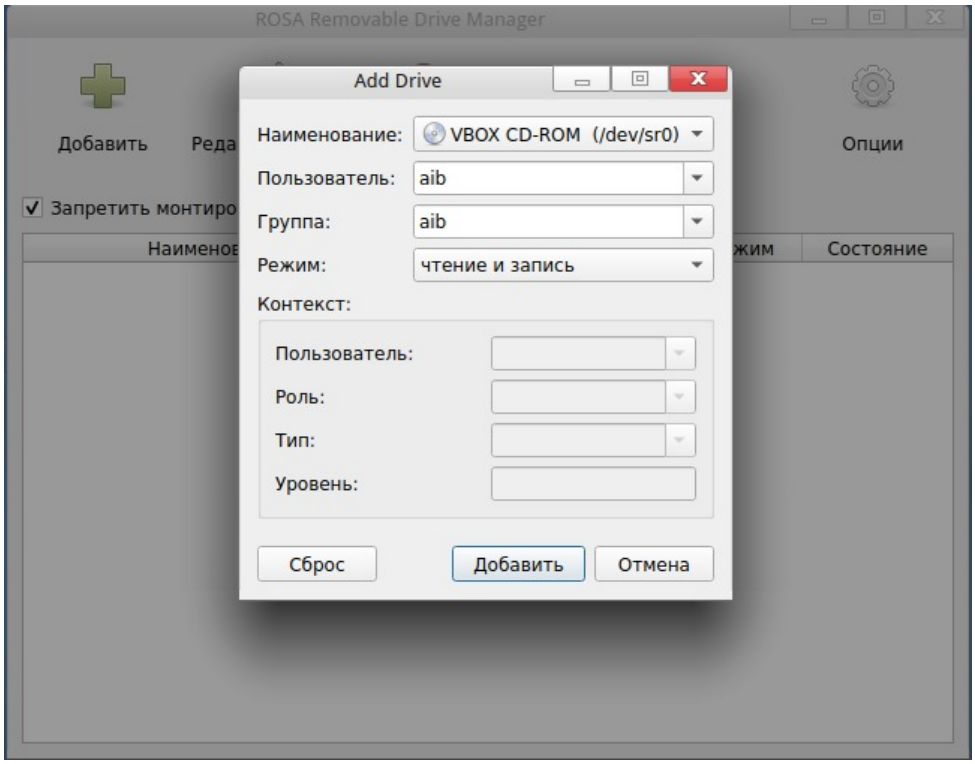


Рисунок 129. Добавление нового устройства

Чтобы изменить настройки доступа к устройству достаточно кликнуть по нему двойным щелчком мыши в таблице контролируемых устройств.

По умолчанию, контроль устройств в системе отключен, для его включения необходимо отметить опцию [Запретить монтирование приводов кроме следующих:], которая расположена над таблицей со списком контролируемых устройств. После активации этой опции создаются правила `udev` (файл /etc/udev/rules.d/80-rosa-removable-drive-manager.rules), которые делают доступными в системе только заданные устройства. Также создаются правила `polkit`, которые разграничивают доступ на уровне пользователей и групп (файл /usr/share/polkit-1/rules.d/00-rosa-removable-drive-manager.rules). И добавляется правило в `fstab` (файл /etc/fstab), задающее опциями монтирования режим доступа к устройству (чтение/запись) и задающее точке монтирования устройства контекст безопасности SElinux.

10.2. ROSA Device Manager

Приложение ROSA Device Manager предназначено для идентификации подключаемых устройств во время загрузки системы, а также вновь добавленных устройств в процессе работы ОС. Приложение работает в терминальном режиме и блокирует неидентифицированные устройства, ограничивая к ним доступ. Доступ к ROSA Device Manager разрешен только пользователям с правами администратора.

Запуск приложения осуществляется следующей командой:

```
#rosa-device-manager
```

При запуске с ключом `-h (--help)` отображается справочная информация со списком всех доступных ключей (опций).

При первом запуске системы после установки приложение запустится с ключом `-c (--create)` – специальным скриптом автозапуска, после чего будут созданы правила `udev` для идентификации устройств (файл /etc/udev/rules.d/00-rosa-device-manager.rules), а в системном логе будет создана следующая запись:

```
"Device identification rules is created"
```

С этого момента любые добавления новых устройств будут идентифицироваться. В случае обнаружения нового устройства в системный лог будет совершена следующая запись:

```
"Unidentified device is detected"
```

Затем системой будет совершена попытка удаления устройства, блокировка порта на шине устройства, либо отвязывание устройства от драйвера, а в системный лог будет совершена запись о блокировании подключенного устройства:

```
"Unidentified device is blocked"
```

Идентификацию устройств приложением можно отключить запуском с ключом `-d (-disable)`. В системный лог будет совершена запись:

```
"Device identification is disabled"
```

Затем идентификацию устройств приложением можно включить запуском с ключом `-e (-enable)`. В системный лог будет совершена запись:

```
"Device identification is enabled"
```

Для того, чтобы система не производила блокировку неидентифицированных устройств необходимо воспользоваться ключом `-n (--non-blocking)`. В системный лог будет совершена следующая запись:

```
"Non-blocking mode is set"
```

Включение режима блокировки неидентифицированных устройств производиться с помощью ключа `-b (--blocking)`. В системный лог будет совершена запись:

```
"Blocking mode is set"
```

Чтобы добавить устройство в правила идентификации устройств, необходимо запустить приложение с ключом `-u (--update)`, после чего выключить ПК и подключить новое устройство. Во время следующего запуска системы правила идентификации обновятся, и в системный лог будет совершена запись:

```
"Device identification rules update is requested"
```

```
"Device identification rules is created".
```

В случае непредвиденного выхода устройства из строя или замены его новым, система заблокирует данное устройство. В данной ситуации необходимо произвести загрузку системы с компакт-диска в live-режиме, примонтировать корневой раздел с системой и удалить правила `udev` (файл /etc/udev/rules.d/00-rosa-device-manager.rules), после чего перезагрузить систему и запустить приложение с ключом `-c(--create)`.

Для включения записи в системный лог всех проходящих идентификацию устройств, следует запустить приложение с ключом `-l (--log)`.

Для отключения записи в системный лог всех проходящих идентификацию устройств, следует запустить приложение с ключом `-q (--quiet)`.

11. ЗАЩИТА ПАМЯТИ

11.1. Очистка памяти с помощью утилиты ROSA Memory Clean

Утилита ROSA Memory Clean предназначена для освобождения памяти ОС. Для работы с программой требуются привилегии суперпользователя.

Имеется возможность освобождения различных участков памяти по расписанию. Интерфейс программы выглядит следующим образом:

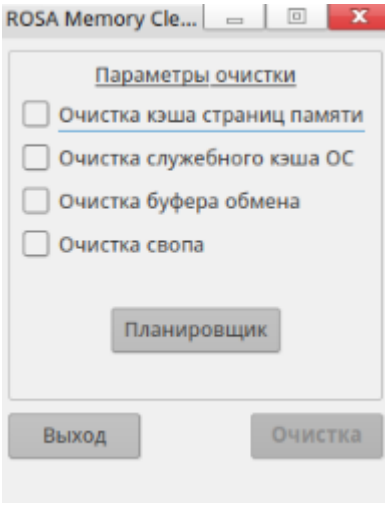


Рисунок 130. Интерфейс ROSA Memory Clean

11.1.1. Описание элементов интерфейса

В верхней части окна перечислены различные варианты очистки памяти:

1) Очистка кэша страниц памяти. Соответствующие страницы памяти получаются в результате чтения и записи обычных файлов на ФС, специальных файлов блочных устройств и файлов, отображаемых в память. Таким образом, в страничном кэше содержатся страницы памяти, полностью заполненные данными из файлов, к которым только что производился доступ.

2) Очистка служебного кэша ОС — удаление различных служебных элементов работы ОС, например, так называемых элементов каталога. Данные объекты создаются «на лету» на основании строкового представления имени пути к конкретному файлу в результате внутреннего перевода системой элементов пути. Также удаляются индексные дескрипторы. Это структуры, хранящие метаинформацию о файлах, каталогах или других объектах ФС.

3) Очистка буфера обмена — освобождение промежуточного хранилища данных, служащего для их переноса между приложениями или в рамках одного приложения.

4) Очистка свопа — перезапуск механизма виртуальной памяти, перемещающего фрагменты данных из оперативной памяти в хранилище (например, жесткий диск или внешний флеш-накопитель).

Кнопка [Планировщик] позволяет перейти в режим планирования очистки по расписанию. Внешний вид окна при нажатии на кнопку меняется:

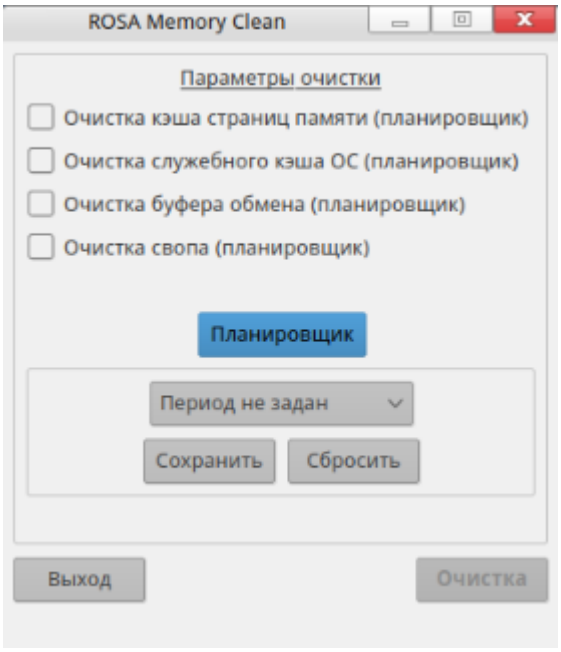


Рисунок 131. Внешний вид ROSA Memory Clean при переходе в режим планировщика

При нажатой кнопке [Планировщик] появятся несколько новых элементов интерфейса — кнопки [Сохранить], [Сбросить] и выпадающий список с выбором периода очистки:

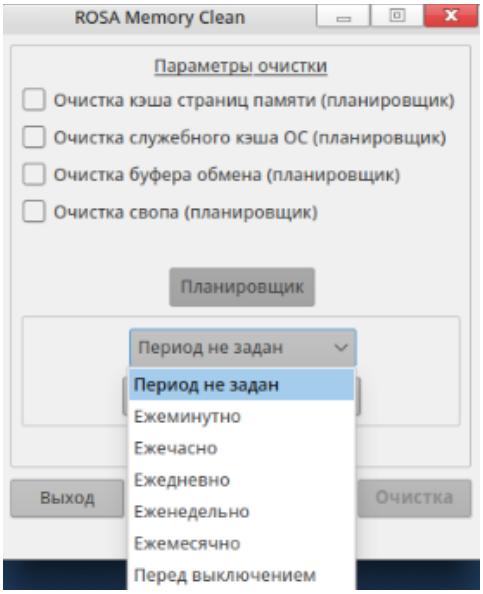


Рисунок 132. Выбор периода очистки

Повторное нажатие кнопки [Планировщик] скроет окошко с периодами и кнопками управления планированием очистки. Кнопка [Помощь] открывает данный документ. По

кнопке [Выход] происходит выход из программы. Нажатие кнопки [Очистка] при выбранных параметрах после подтверждения запустит процесс очистки.

11.1.2. Работа с утилитой

Для запуска процесса очистки памяти необходимо выбрать один или несколько из представленных параметров, после чего нажать на кнопку [Очистка].

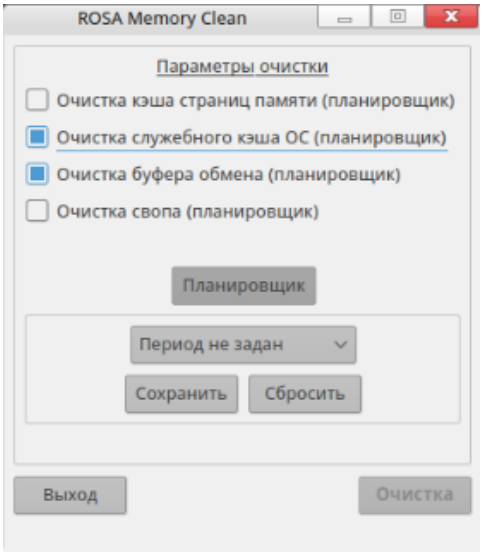


Рисунок 133. Выбор областей памяти для очистки

После нажатия на кнопку [Очистка] нужно будет подтвердить выбранные действия. При положительном ответе запустится процесс очистки и появится окно ожидания операции. Необходимо дождаться ее окончания. По окончании окно ожидания исчезнет, и в нижней части появится сообщение «Операция завершена».

Очистку памяти можно сделать периодической, чтобы не запускать программу каждый раз вручную. Для этого нужно нажать на кнопку [Планировщик]. Выбрав период очистки, нажмите на кнопку [Сохранить], чтобы записать период в конфигурационный файл программы. Теперь очистка памяти будет запускаться автоматически без дополнительных действий пользователя. Нажатие кнопки [Сбросить] удалит выбранные ранее период и параметры очистки.

11.2. Очистка памяти ядра

Для очистки памяти ядра ОС также используются следующие параметры. Для установки shredder используйте команду:

```
make && sudo ./install.sh
```

Для удаления shredder используйте команду:

```
sudo ./uninstall.sh
```

Параметры команды:

`mode` – `random` или `zeroone` – параметры очистки ядра;

`loops` – количество кругов очистки.

Синтаксис использования команды:

```
insmod ./kernelspace/shredder-kernel.ko mode="random" loops=1
```

11.3. Удаление файлов с носителей с помощью утилиты ROSA Shred

Удаление файлов на внешних носителях, содержащих конфиденциальную информацию, должно происходить с помощью графического приложения «ROSA Shred» или с помощью утилит shred и wipe, описанных далее.

Приложение «ROSA Shred» предназначено для удаления файлов методом многократной перезаписи уничтожаемых объектов ФС специальными битовыми последовательностями. Описание графического интерфейса приведено в справке приложения. Приложение можно запустить, выбрав пункт меню «Утилиты СЗИ» → «ROSA Shred», или используя команду rosa-shred.

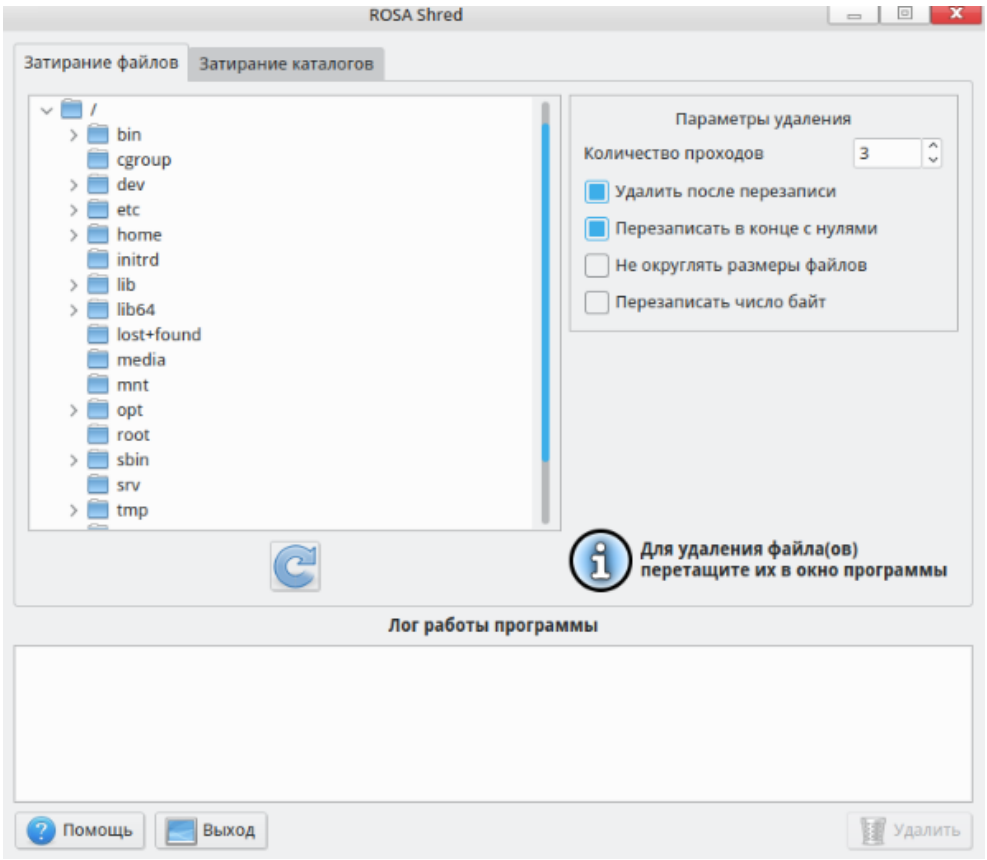


Рисунок 134. Графический интерфейс утилиты ROSA Shred

В приведены часто используемые опции утилиты ROSA Shred. Подробное описание приведено в man shred.

Синтаксис:

```
shred <опции> <путь к файлу>
```

Таблица 47 – Опции утилиты shred

Опция	Описание
-n, --iterations=N	Указание N проходов перезаписи
-u, --remove	Удаление файла после перезаписи
-z, --zero	Перезаписать в конце с нулями, чтобы скрыть перемешивание
-x, --exact	Округление размера файлов до следующего целого блока не производится (по умолчанию для файлов устройств)
-s, --size=N	Очищение N байт (возможны суффиксы вида K, M, G)
-v, --verbose	Вывод индикатора прогресса

Пример использования:

В результате выполнения этой команды произойдет удаление файла file1 методом двукратной перезаписи уничтожаемых объектов ФС специальными битовыми последовательностями:

```
# shred -uv -n 2 file1
```

Утилита wipe предназначена для удаления каталогов методом многократной перезаписи уничтожаемых объектов ФС специальными битовыми последовательностями. В приведены часто используемые опции утилиты wipe. Подробное описание приведено в man wipe.

Синтаксис:

```
wipe <опции> <каталог>
```

Таблица 48 – Опции утилиты wipe

Опция	Описание
-r	Удаление каталога и его содержимого
-pX	Указание X проходов перезаписи

Пример использования:

В результате выполнения этой команды произойдет удаление каталога cat1 методом двукратной перезаписи уничтожаемых объектов ФС специальными битовыми последовательностями:

```
# wipe -r -p2 cat1
```

Рекомендации: удаление файлов необходимо производить только с использованием приложения «ROSA shred» или утилит shred и wipe (количество итераций перезаписи – не менее двух раз).

12. КОНТРОЛЬ ЦЕЛОСТНОСТИ

Для реализации неизменности политик безопасности в ОС РОСА «НИКЕЛЬ» необходимо проводить контроль целостности системных файлов и директорий ОС (с помощью электронных замков ПАК «Соболь», Аккорд-АМДЗ и др.).

Контроль производится путем сравнения значений контрольных сумм файлов и директорий с контрольными суммами, приведенными в документе «polkit_sum», размещенном на оптическом диске с комплектом документации ОС.

Список директорий, необходимых для проверки:

- `/etc/selinux/config`
- `/usr/share/selinux/mls/base.lst`
- `/usr/share/selinux/mls/modules-base.lst`
- `/usr/share/selinux/mls/modules-contrib.lst`
- `/usr/share/selinux/mls/default/active/modules/100/`
- `/var/lib/selinux/mls/active/modules/`

Внимание! Запрещается эксплуатация ОС при несовпадении полученных контрольных сумм средством доверенной загрузки со значениями, указанными в документе «polkit_sum».

После установки ОС необходимо настроить проверку контроля целостности системных файлов ОС, указанных в документах «desktop_install_sum» или «server_install_sum», в зависимости от установленного типа ОС – Рабочая станция или Сервер, соответственно, с помощью утилиты проверки целостности aide.

12.1. Проверка целостности aide

Утилита aide (Advanced Intrusion Detection Environment) предназначена для проверки целостности файлов. Утилита aide позволяет делать снимки всех основных конфигурационных и исполняемых файлов, состояния библиотек и в случае компрометации системы позволяет определить, какие файлы были изменены.

В приведены часто используемые опции утилиты aide. Подробное описание приведено в man aide.

Синтаксис:

```
aide <опции>
```

Таблица 49 – Опции утилиты aide

Опция	Описание
--check, -C	Проверка целостности файлов
--init, -i	Инициализация базы файлов
--update, -u	Обновление базы файлов (проверка целостности файлов и инициализация базы файлов)
--compare	Сравнение двух баз файлов

Пример инициализации базы данных и проверки целостности:

```
# aideinit
```

12.2. Тестирование ROSA Security Test

Утилита rst включает в себя тесты, выполняющиеся при загрузке ОС. Доступ к интерфейсу приложения осуществляется из панели приложений через ярлык «ROSA Security Test».

Утилита запускается автоматически при входе любого пользователя в систему.

Рисунок 135. Ярлык ROSA Security Test

Тесты, выполняемые утилитой (Рисунок 136):

1) Проверка ограничений пользователя на доступ к файлам и директориям:
   - Осуществляет проверку всех файлов и директорий /home и /tmp, проверяя при этом права доступа и контекстные метки selinux для файлов, ссылок и сокетов, а также пытается осуществить нарушение модели безопасности по отношению к каждому найденному файлу;
   - Осуществляет проверку всех корневых директорий (кроме /tmp), пытаясь осуществить в них запись
3) Общая проверка режима безопасности:

— Утилита проверяет включен ли selinux;

— Утилита проверяет включена ли поддержка mls.

3) Проверка ограничения возможности пользователя по созданию файлов без контекста безопасности:

— В ходе проведения теста утилита пытается создать файл в директориях /tmp и /home и проверяет, чтобы у каждого была контекстная метка.

4) Проверка ограничений пользователя на установку программного обеспечения:

— В ходе выполнения теста утилита проверяет возможность установки, а затем удаления пакета dos2unix (бесполезный пакет).

5) Проверка идентификации пользователея

6) Проверка ограничений пользователя на изменение системного времени:

— В ходе выполнения теста утилита проверяет возможность изменения текущего времени командой date -s.

7) Проверка виртуализации служебных фалов.

8) Проверка сервисов аудита

9) Поддержка MLS при операциях над файлами

10) Проверка границ пользовательского пространства

11) Проверка механизмов подписей

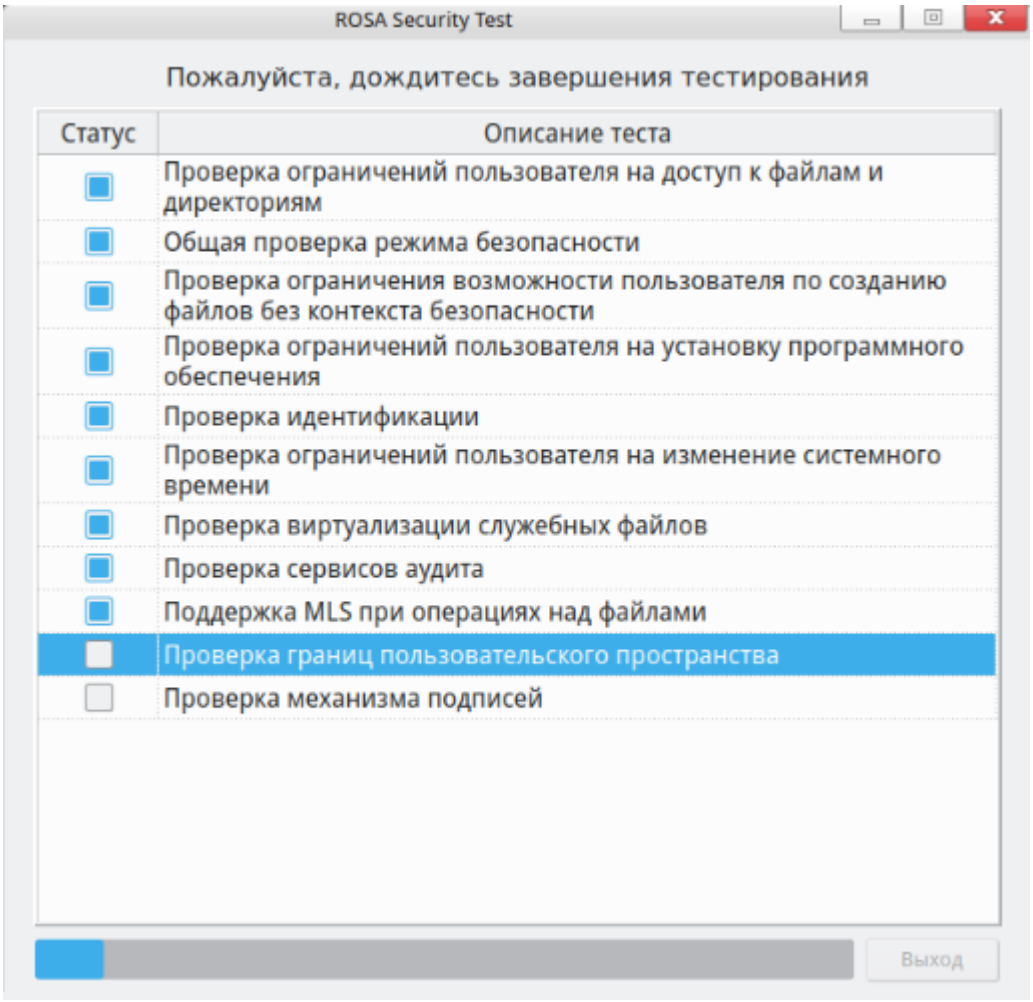


Рисунок 136. Тесты ROSA Security Test

Все тесты кроме: [Тест на виртуализацию служебных файлов], [Общая проверка режима безопасности], пытаются осуществить атаку на ОС. Если хотя бы одно действие будет пропущено (исключение – об отказе доступа) – весь процесс тестирования будет провален.

Если запустить Rosa Security Test с параметром `--ultimate`, то при не прохождении хотя бы одного теста, блокируются любые действия пользователя, кроме выхода из сессии. Если Rosa Security Test запущен без этого параметра, пользователь имеет возможность закрыть программу и продолжить работу, даже если какой-то тест не пройден.

13. РУКОВОДСТВО ПО ПОДГОТОВИТЕЛЬНЫМ ПРОЦЕДУРАМ

13.1. Общесистемные настройки

Для реализации неизменности политик безопасности в ОС РОСА «НИКЕЛЬ» необходимо проводить контроль целостности системных файлов и директорий ОС (с помощью электронных замков ПАК «Соболь», Аккорд-АМДЗ и др.).

В данном разделе приведены рекомендации по настройке ряда системных характеристик, влияющих на безопасность системы в целом. Правильная настройка системных разделов и ФС, настройки возможности использования механизмов защиты от переполнения буфера, настройки правильного использования изоляции процессов, настройки, предотвращающие появление системной избыточности, и другие — все это необходимо применять для того, чтобы снизить площадь атаки на систему и препятствовать нарушителю осуществлять угрозы безопасности.

13.1.1. Отключение создания отладочных файлов (core dumps)

13.1.1.1. Аннотация угрозы

Отладочные файлы, образующиеся при крахе приложений (core dumps).

13.1.1.2. Описание угрозы

Отладочные файлы программ после краха (core dumps) могут содержать информацию о состоянии системы (данные страниц памяти ОЗУ, включающие, например, ключи шифрования, хэши паролей, другие входные и выходные данные программ), параметры конфигурации программ и приложений, состояния среды функционирования (параметры системного окружения, переменные среды, идентификаторы субъектов и объектов) и т.п.

Следовательно, в случае если потенциальный нарушитель получит доступ к такого рода файлам и сможет подвергнуть их анализу, это может привести к раскрытию информации и последующей реализации угроз безопасности информации (УБИ).

13.1.1.3. Идентификаторы угрозы

По БДУ ФСТЭК России:

– УБИ.012: Угроза деструктивного изменения конфигурации/среды окружения программ;

– УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией;

– УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением.

Потенциальные уязвимости согласно MITRE Common Weakness Enumeration:

- CWE-201: Insertion of Sensitive Information Into Sent Data;
- CWE-209: Generation of Error Message Containing Sensitive Information;
- CWE-213: Exposure of Sensitive Information Due to Incompatible Policies;
- CWE-215: Insertion of Sensitive Information Into Debugging Code;
- CWE-532: Insertion of Sensitive Information into Log File.

По ИТ.ОС.А2.ПЗ:

- Угроза-1 — несанкционированный доступ к объектам доступа со стороны субъектов доступа, для которых запрашиваемый доступ не разрешен;
- Угроза-2 — получение нарушителем несанкционированного доступа к информации, обрабатываемой средством вычислительной техники (СВТ), в период, когда пользователь ОС покинул АРМ, не завершив сеанс работы в ОС;
- Угроза-5 — утечка или несанкционированное изменение информации в оперативной памяти, используемой различными процессами и формируемыми ими потоками данных;
- Угроза-7 — осуществление нарушителем восстановления (подбора) аутентификационной информации пользователей ОС;
- Угроза-8 — использование нарушителем идентификационной и начальной аутентификационной информации, соответствующей учетной записи пользователя ОС;
- Угроза-11 — несанкционированный доступ субъектов доступа к информации, обработка которой осуществлялась в рамках сеансов (сессий) других субъектов доступа.

Матрица MITRE ATT&CK:

- T1003 OS Credential Dumping;
- T1005 Data from Local System;
- T1413 Access Sensitive Data in Device Logs.

13.1.1.4. Способ противостояния угрозе

Реализация конфигурации системы, не предусматривающая разрешений на создание файлов отладочной информации, образующихся при крахе приложений и системных программ.

MITRE ATT&CK Mitigations:

- M1022 Restrict File and Directory Permissions;
- M1013 Application Developer Guidance;
- M1028 Operating System Configuration;
- M1042 Disable or Remove Feature or Program.

13.1.1.5. Проекция ИФБО к ФТБ

Настройка перечисленных ИФБО способствует реализации ФТБ, мер защиты или контроля.

Проекция ИФБО к ФТБ для интерфейсов, отключающих создание файлов core dumps приведена в таблице (Таблица 50).

Таблица 50

ИФБО	ФТБ ГОСТ 15408-2	Мера защиты 17-ого приказа ФСТЭК России	Контроль ГОСТ 27002
/etc/security/limits.conf	FRU_PRS.1 FRU_RSA.1	ОПС.4	11.2.2. а) 11.3.3
/etc/sysctl.conf			
/etc/profile			
/etc/systemd/coredump.conf			

13.1.1.6. Проверки и действия

Все проверки и действия выполняются в контексте учетной записи суперпользователя, если специально не определено иное.

Необходимые действия описаны ниже.

Лимиты для субъектов при создании отладочных файлов

В файле /etc/security/limits.conf указать (проверить что указаны) следующие значения:

```
*   hard core 0
root     hard core 0
```

Переменная ядра, воспрещающая создание файлов отладки

В файле /etc/sysctl.conf проверить, что установлена следующая переменная ядра, воспрещающая создание дампов памяти от имени процессов с установленным биты смены идентификатора суперпользователя (SUID bit):

```
# cat /etc/sysctl.conf | grep fs.suid_dumpable
fs.suid_dumpable = 0
```

иначе установить таковую переменную и выполнить команду, переинициализирующую пространство переменных ядра ОС:

```
#echo 'fs.suid_dumpable = 0' >> /etc/sysctl.conf
#sysctl -p
```

Определение лимитов для core dumps

Установить (проверить, что установлено) ограничение (лимит) в файле /etc/profile для всех интерактивных пользователей системы, принудительно ограничивающий системное окружение (действует после переинициализации интерактивного сеанса):

```
#echo 'ulimit -S -c 0 > /dev/null 2>&1' >> /etc/profile
```

Ограничения для systemd-coredump

В том случае, если компонент systemd-coredump установлен, то требуется проверить и при наличии ИФБО выполнить в файле /etc/systemd/coredump.conf соответствующие изменения:

```
Storage=none
ProcessSizeMax=0
```

Выполнить переинициализацию конфигурации служб с помощью команды:

```
#systemctl daemon-reload
```

Отключение сброса страниц памяти с помощью клавиш SysRq

Для отладки ОС РОСА «НИКЕЛЬ» поддерживает обработку т. н. клавиш SysRq — это сокращение от System Request (системный запрос).

В защищенной системе недопустимо использовать комбинации SysRq, так как это приводит к возникновению угроз безопасности информации.

Описание SysRq:

- Alt + SysRq + B — немедленно перезагрузить систему без синхронизации и размонтирования дисков;
- Alt+SysRq+C — выполнить крах со сбросом на диск состояния страниц памяти;
- Alt+SysRq+E — послать сигнал SIGTERM всем процессам кроме Init (systemd);
- Alt+SysRq+I — послать сигнал SIGKILL всем процессам кроме Init (systemd);
- Alt+SysRq+O — выключить ПК;
- Alt+SysRq+R — вернуть управление клавиатурой в случае сбора X-сервера;
- Alt+SysRq+U — перемонтирует ФС в режиме «только для чтения»;
- Alt+SysRq+S — записать весь имеющийся кеш из памяти данные на диск;
- Alt+SysRq+K — уничтожить все процессы в текущем терминале;
- Alt+SysRq+N — сбросить приоритет всех высоко приоритетных процессов;
- Alt+SysRq+F — запустить механизм oom_kill, который уничтожит процесс, занимающий много памяти;
- Alt+SysRq+T — вывести всю информацию о запущенных процессах на текущую консоль;
- Alt+SysRq+L — послать сигнал SIGKILL всем процессам включая Init (systemd);
- Alt+SysRq+P — выдать сброс текущего состояния регистров процессора в текущий терминал.

Для проверки текущей конфигурации SysRq выполнить:

```
# cat /proc/sys/kernel/sysrq
```

```
0
```

Если значение вывода отлично от нуля, выполнить:

```
#echo "0" > /proc/sys/kernel/sysrq
#echo "kernel.sysrq = 0" >> /etc/sysctl.conf
```

13.1.2. Отключение редко используемых ФС

13.1.2.1. Аннотация угрозы

Поддержка редких ФС, в которых не поддерживаются атрибуты безопасности, а также ФС, предполагающих наличие избыточных прав доступа (возможность создания файлов устройств, исполнения загрузочных модулей, установки бита смены идентификатора).

13.1.2.2. Описание угрозы

В составе ОС РОСА «НИКЕЛЬ» может поддерживаться несколько редко используемых, мало распространенных или не требуемых в конкретной ИС ФС. Такие ФС могут полностью или частично не иметь поддержки атрибутов безопасности. Драйверы (модули) таких ФС могут иметь устаревшую, не поддерживаемую или плохо поддерживаемую реализацию. Поддержка таких ФС должна быть предусмотрена только в случае исключительной значимости и полностью аргументированной. Иначе такая поддержка существенно увеличивает площадь атаки как на отдельный экземпляр ОС, так и на всю ИС.

13.1.2.3. Идентификаторы угрозы

По БДУ ФСТЭК России:

– УБИ.012: Угроза деструктивного изменения конфигурации/среды окружения программ;

– УБИ.015: Угроза доступа к защищаемым файлам с использованием обходного пути;

– УБИ.028: Угроза использования альтернативных путей доступа к ресурсам;

– УБИ.166: Угроза внедрения системной избыточности.

Потенциальные уязвимости согласно MITRE Common Weakness Enumeration:

– CWE-178: Improper Handling of Case Sensitivity;

– CWE-250: Execution with Unnecessary Privileges;

– CWE-276: Incorrect Default Permissions;

– CWE-278: Insecure Preserved Inherited Permissions;

– CWE-281: Improper Preservation of Permissions;

– CWE-610: Externally Controlled Reference to a Resource in Another Sphere;

– CWE-732: Incorrect Permission Assignment for Critical Resource;

- CWE-766: Critical Data Element Declared Public;
- CWE-843: Access of Resource Using Incompatible Type ('Type Confusion');
- CWE-1104: Use of Unmaintained Third Party Components.

По ИТ.ОС.А2.ПЗ:

- Угроза-3 — ограничение нарушителем доступа пользователей ОС к ресурсам СВТ, на котором установлена ОС за счет длительного удержания вычислительного ресурса в загруженном состоянии путем осуществления нарушителем многократных запросов, требующих большого количества ресурсов на их обработку;
- Угроза-10 — несанкционированный доступ к информации вследствие использования пользователями ОС неразрешенного ПО.

Матрица MITRE ATT&CK:

- T1565.001 Data Manipulation: Stored Data Manipulation;
- T1005 Data from Local System;
- TA0005 Defense Evasion;
- T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control;
- T1037 Boot or Logon Initialization Scripts;
- T1211 Exploitation for Defense Evasion.

13.1.2.4. Способ противостояния угрозе

Реализация конфигурации системы, не предусматривающая избыточную (не требуемых для использования) поддержку ФС.

MITRE ATT&CK Mitigations:

- M1046 Boot Integrity;
- M1022 Restrict File and Directory Permissions;
- M1038 Execution Prevention;
- M1026 Privileged Account Management;
- M1028 Operating System Configuration;
- M1042 Disable or Remove Feature or Program.

13.1.2.5. Проекция ИФБО к ФТБ

Настройка перечисленных ИФБО способствует реализации ФТБ, мер защиты или контроля.

Проекция ИФБО к ФТБ для интерфейсов, отключающих использование ФС приведена в Таблица 51.

Таблица 51

ИФБО	ФТБ ГОСТ 15408-2	Мера защиты 17-ого приказа ФСТЭК России	Контроль ГОСТ 27002
/sbin/modprobe	FPT_ACF_EXT.1, FDP_RSP_EXT.1, FDP_RSP_EXT.2	ИАФ.7, УПД.2, ОПС.1	11.2.2. а) 11.3.3
/etc/modprobe.d/*.conf			

13.1.2.6. Проверки и действия

Все проверки и действия выполняются в контексте учетной записи суперпользователя, если специально не определено иное.

Необходимые действия описаны ниже.

Отключение ФС cramfs

Выполнить команды проверки доступности модуля ядра, поддерживающего ФС cramfs:

```
#modprobe -n -v cramfs | grep -E 'cramfs|install'
#lsmod | grep cramfs
```

Отключить поддержку этой ФС:

```
#echo 'install cramfs /bin/true' >> /etc/modprobe.d/restrict_fs_modules.conf
#rmmod cramfs
```

Отключение ФС freevxfs

Выполнить команды проверки доступности модуля ядра, поддерживающего ФС freevxfs:

```
#modprobe -n -v freevxfs | grep -E 'freevxfs|install'
#lsmod | grep freevxfs
```

Отключить поддержку этой ФС:

```
#echo 'install freevxfs /bin/true' >> /etc/modprobe.d/restrict_fs_modules.conf
#rmmod freevxfs
```

Отключение ФС jffs2

Выполнить команды проверки доступности модуля ядра, поддерживающего ФС jffs2:

```
#modprobe -n -v jffs2 | grep -E 'jffs2|install'
#lsmod | grep jffs2
```

Отключить поддержку этой ФС:

```
#echo 'install jffs2 /bin/true' >>
```

```
/etc/modprobe.d/restrict_fs_modules.conf
```

```
#rmmod jffs2
```

Отключение ФС hfs

Выполнить команды проверки доступности модуля ядра, поддерживающего ФС hfs:

```
#modprobe -n -v hfs | grep -E 'hfs|install'
#lsmod | grep hfs
```

Отключить поддержку этой ФС:

```
#echo 'install hfs /bin/true' >>
/etc/modprobe.d/restrict_fs_modules.conf
#rmmod hfs
```

Отключение ФС hfsplus

Выполнить команды проверки доступности модуля ядра, поддерживающего ФС hfsplus:

```
#modprobe -n -v hfsplus | grep -E 'hfsplus|install'
#lsmod | grep hfsplus
```

Отключить поддержку этой ФС:

```
#echo 'install hfsplus /bin/true' >>
/etc/modprobe.d/restrict_fs_modules.conf
#rmmod hfsplus
```

Отключение ФС udf

ФС udf иногда может требоваться при работе в гетерогенной среде.

Выполнить команды проверки доступности модуля ядра, поддерживающего ФС udf:

```
#modprobe -n -v udf | grep -E 'udf|install'
#lsmod | grep udf
```

Отключить поддержку этой ФС:

```
#echo 'install udf /bin/true' >>
/etc/modprobe.d/restrict_fs_modules.conf
#rmmod udf
```

13.1.3. Использование безопасной конфигурации ФС

13.1.3.1. Аннотация угрозы

Конфигурация системы, при которой системные и пользовательские файлы расположены в пределах общего раздела. Либо конфигурация, при которой системные файлы расположены в пределах общего раздела или они недостаточно распределены.

13.1.3.2. Описание угрозы

Наличие в системе одного (не распределенного на части) раздела (тома) - делает возможным создание перекрестных ссылок, которые могут быть использованы нарушителем; файлов устройств, которые могут вести к возможности использования нарушителем недоверенного оборудования или применения нарушителем собственного исполняемого кода, снабженного битом смены идентификатора, и, как следствие может привести к эскалации привилегий или обходу механизмов безопасности иным способом.

Небезопасная конфигурация дисковых разделов существенно повышает площадь атаки на ОС и на ИС. Необходимо учитывать, что в составе ОС РОСА «НИКЕЛЬ» присутствуют каталоги, доступные на запись всем субъектам доступа. Например, каталог /tmp. В том случае, если каталог /tmp не выделен в отдельный раздел, потенциальный нарушитель может быстро и просто переполнить ФС. Это может привести к любым негативным последствиям (как минимум, будет реализована атака типа «отказ в обслуживании»).

13.1.3.3. Идентификаторы угрозы

По БДУ ФСТЭК России:

- УБИ.012: Угроза деструктивного изменения конфигурации/среды окружения программ;
- УБИ.015: Угроза доступа к защищаемым файлам с использованием обходного пути;
- УБИ.028: Угроза использования альтернативных путей доступа к ресурсам;
- УБИ.166: Угроза внедрения системной избыточности.

Потенциальные уязвимости согласно MITRE Common Weakness Enumeration:

- CWE-178: Improper Handling of Case Sensitivity;
- CWE-250: Execution with Unnecessary Privileges;
- CWE-276: Incorrect Default Permissions;
- CWE-278: Insecure Preserved Inherited Permissions;
- CWE-281: Improper Preservation of Permissions;
- CWE-610: Externally Controlled Reference to a Resource in Another Sphere;
- CWE-732: Incorrect Permission Assignment for Critical Resource;
- CWE-766: Critical Data Element Declared Public;
- CWE-843: Access of Resource Using Incompatible Type ('Type Confusion');
- CWE-1104: Use of Unmaintained Third Party Components.

По ИТ.ОС.А2.ПЗ:

– Угроза-3 — ограничение нарушителем доступа пользователей ОС к ресурсам СВТ, на котором установлена ОС за счет длительного удержания вычислительного ресурса в загруженном состоянии путем осуществления нарушителем многократных запросов, требующих большого количества ресурсов на их обработку;

– Угроза-5 — утечка или несанкционированное изменение информации в оперативной памяти, используемой различными процессами и формируемыми ими потоками данных;

– Угроза-10 — несанкционированный доступ к информации вследствие использования пользователями ОС неразрешенного ПО.

Матрица MITRE ATT&CK:

– T1565.001 Data Manipulation: Stored Data Manipulation;

– T1005 Data from Local System;

– TA0005 Defense Evasion;

– T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control;

– T1037 Boot or Logon Initialization Scripts;

– T1211 Exploitation for Defense Evasion;

– T1055.009 Process Injection: Proc Memory.

13.1.3.4. Способ противостояния угрозе

Реализация конфигурации системы, предусматривающая совершение только требуемых операций с файлами.

Реализация конфигурации системы, предусматривающая создание и использование отдельных логических томов (разделов) для ФС. Следует обязательно разделять (сегментировать) дисковое пространство на несколько перечисленных ниже ФС, чтобы обеспечить изоляцию механизмов защиты, вынося системные файлы (включающие средства защиты информации (СЗИ) ОС) за пределы пространства, доступного пользователям. Дополнительно требуется обязательно учитывать назначение каждой из указанных ниже ФС с тем, чтобы предоставлять субъектам доступа только необходимый для выполнения задач минимальный набор привилегий при работе в них. Все каталоги, имеющие права, позволяющие запись всех субъектам, должны быть ограничены по объему, вынесены в отдельные ФС и снабжены соответствующим битом разрешений (sticky). Реализация этих мер будет способствовать невозможности преодоления механизмов безопасности потенциальным нарушителем. Необходимо предусмотреть сегментирование для:

– корневой ФС </>;

- раздела подкачки <swap>;
- раздела хранения ядра и загрузчика </boot>;
- раздела поддержки UEFI SecureBoot </boot/efi> (при необходимости);
- домашней ФС </home>;
- для хранения временных файлов </tmp>;
- для служебных нужд </var>;
- для нужд служб регистрации событий </var/log>;
- для нужд служб регистрации событий системы и ядра </var/log/audit>.

MITRE ATT&CK Mitigations:

- M1046 Boot Integrity;
- M1022 Restrict File and Directory Permissions;
- M1038 Execution Prevention;
- M1026 Privileged Account Management;
- M1028 Operating System Configuration;
- M1040 Behavior Prevention on Endpoint;
- M1042 Disable or Remove Feature or Program.

13.1.3.5. Проекция ИФБО к ФТБ

Настройка перечисленных ИФБО способствует реализации ФТБ, мер защиты или контроля.

Проекция ИФБО к ФТБ для интерфейса определения приведена в таблице (Таблица 52).

Таблица 52

ИФБО	ФТБ ГОСТ 15408-2	Мера защиты 17-ого приказа ФСТЭК России	Контроль ГОСТ 27002
/etc/fstab	FRU_RSA.1, FMT_MSA.3, FIA_OID_EXT.1	ИАФ.7, УПД.2, ОПС.1	11.2.2. а) 11.3.3

13.1.3.6. Проверки и действия

Все проверки и действия выполняются в контексте учетной записи суперпользователя, если специально не определено иное.

Необходимые действия описаны ниже.

Конфигурация корневой ФС

При установке ОС требуется выделить отдельный раздел для корневой ФС.

Проверка выделения отдельного раздела для корневой ФС не производится.

Выделение отдельного раздела подкачки

При установке ОС требуется выделить отдельный раздел для подкачки (swap).

Для проверки выполнить команды:

```
#lsblk | grep SWAP
#cat /etc/fstab | grep swap
#swapon –show
```

Выделение отдельного раздела для /boot

При установке ОС требуется выделить отдельный раздел для файлов ядра и загрузчика /boot. Для проверки выполнить команды:

```
#lsblk | grep boot
#cat /etc/fstab | grep boot
#mount | grep '/boot'
```

Настройка безопасных опций монтирования /boot

Проверка на ФС /boot специальных опций монтирования (nodev,noexec,nosuid). Выполнить команды:

```
#mount | grep -E '\s/boot\s' | grep -v nodev
#mount | grep -E '\s/boot\s' | grep -v noexec
#mount | grep -E '\s/boot\s' | grep -v nosuid
```

Для установки на ФС /boot специальных опций монтирования (nodev,noexec,nosuid) — внести изменения в четвертое поле файла /etc/fstab вместо defaults:

```
<раздел> /boot ext4 nodev,noexec,nosuid
```

Перемонтировать ФС:

```
#mount -o remount /boot
```

Выделение отдельного раздела /boot/efi

При установке ОС требуется выделить отдельный раздел для поддержки UEFI SecureBoot (/boot/efi, при необходимости). Для проверки выполнить команды:

```
#lsblk | grep efi
#cat /etc/fstab | grep efi
#mount | grep efi
```

Выделение отдельного раздела /home

При установке ОС требуется выделить отдельный раздел для хранения данных пользователей — домашней ФС /home. Для проверки выполнить команды:

```
#lsblk | grep home
#cat /etc/fstab | grep home
#mount | grep home
```

Настройка безопасных опций монтирования /home

Для проверки того, установлены ли на ФС /home безопасные опции монтирования (nodev,nosuid,noexec) выполнить команды:

```
#mount | grep -E '\s/home\s' | grep -v nodev
#mount | grep -E '\s/home\s' | grep -v nosuid
#mount | grep -E '\s/home\s' | grep -v noexec
```

Для установки на ФС /home специальных опций монтирования (nodev,noexec,nosuid) — внести изменения в четвертое поле файла /etc/fstab вместо defaults:

```
<раздел> /home ext4 nodev,noexec,nosuid
```

Перемонтировать ФС:

```
#mount -o remount /home
```

Выделение отдельного раздела /tmp

При установке ОС требуется выделить отдельный раздел хранения временных файлов /tmp. Для проверки выполнить команды:

```
#lsblk | grep tmp
#cat /etc/fstab | grep tmp
#mount | grep tmp
```

Настройка безопасных опций монтирования /tmp

Для проверки того, установлены ли на ФС /tmp безопасные опции монтирования (nodev,nosuid,noexec) выполнить команды:

```
#mount | grep -E '\s/tmp\s' | grep -v nodev
#mount | grep -E '\s/tmp\s' | grep -v nosuid
#mount | grep -E '\s/tmp\s' | grep -v noexec
```

Для установки на ФС /tmp специальных опций монтирования (nodev,noexec,nosuid) — внести изменения в четвертое поле файла /etc/fstab вместо defaults:

```
<раздел> /tmp ext4 nodev,noexec,nosuid
```

Перемонтировать ФС:

```
#mount -o remount /tmp
```

Удалить каталог /var/tmp и создать символическую ссылку на /tmp в /var/tmp:

```
#rmdir /var/tmp
#ln -s /tmp /var/tmp
```

Примечание по использованию опции noexec для /tmp

Требуется учитывать, что в некоторых случаях устанавливаемое в ОС ПО устанавливается таким образом, что сначала разворачивается в каталоге /tmp, откуда

затем запускается установщик. Такое ПО при эксплуатации требуется отслеживать и классифицировать. А для обеспечения его установки требуется временно отключать опцию монтирования noexec и затем, после успешной установки ПО, заново активизировать, вместе со своевременным перемонтированием ФС.

Выделение отдельного раздела /var

При установке ОС требуется выделить отдельный том для служебных нужд /var. Для проверки выполнить команды:

```
#lsblk | grep var
#cat /etc/fstab | grep var
#mount | grep var
```

Настройка безопасных опций монтирования /var

Для проверки того, установлены ли на ФС /var безопасные опции монтирования (nodev,nosuid) выполнить команды:

```
#mount | grep -E '\s/var\s' | grep -v nodev
#mount | grep -E '\s/var\s' | grep -v nosuid
```

Для установки на ФС /var специальных опций монтирования (nodev,nosuid) — внести изменения в четвертое поле файла /etc/fstab вместо defaults:

```
<раздел> /var ext4 nodev,nosuid
```

Перемонтировать ФС:

```
#mount -o remount /var
```

Выделение отдельного раздела /var/log

При установке ОС требуется выделить отдельный том для нужд служб регистрации событий /var/log. Для проверки выполнить команды:

```
#lsblk | grep log
#cat /etc/fstab | grep log
#mount | grep log
```

Настройка безопасных опций монтирования /var/log

Для проверки того, установлены ли на ФС /var/log безопасные опции монтирования (nodev,noexec,nosuid) выполнить команды:

```
#mount | grep -E '\s/log\s' | grep -v nodev
#mount | grep -E '\s/log\s' | grep -v nosuid
#mount | grep -E '\s/log\s' | grep -v noexec
```

Для установки на ФС /var/log специальных опций монтирования (nodev,noexec,nosuid) — внести изменения в четвертое поле файла /etc/fstab вместо defaults:

```
<раздел> /var/log ext4 nodev,noexec,nosuid
```

Перемонтировать ФС:

```
#mount -o remount /var/log
```

Выделение отдельного раздела /var/log/audit

При установке ОС требуется выделить отдельный том для нужд служб регистрации событий /var/log/audit. Для проверки выполнить команды:

```
#lsblk | grep audit
#cat /etc/fstab | grep audit
#mount | grep audit
```

Настройка безопасных опций монтирования /var/log/audit

Для проверки того, установлены ли на ФС /var/log/audit безопасные опции монтирования (nodev,nosuid,noexec) выполнить команды:

```
#mount | grep -E '\s/audit\s' | grep -v nodev
#mount | grep -E '\s/audit\s' | grep -v nosuid
#mount | grep -E '\s/audit\s' | grep -v noexec
```

Для установки на ФС /var/log/audit специальных опций монтирования (nodev,noexec,nosuid) — внести изменения в четвертое поле файла /etc/fstab вместо defaults:

```
<раздел> /var/log/audit ext4 nodev,noexec,nosuid
```

Перемонтировать ФС:

```
#mount -o remount /var/log/audit
```

Настройка ФС /dev/shm

В составе ОС РОСА «НИКЕЛЬ» обычно содержится ФС /dev/shm, доступная для всех пользователей, в том числе на запись, так же, как и /tmp. Эта ФС является одним из интерфейсов к памяти ОС, и предназначена для обеспечения обмена данными между процессами. Она представляет собой временную ФС. Эта ФС существует в ОЗУ до перезагрузки ОС. Потенциальный нарушитель может разместить в этой ФС исполняемый файл и/или файл, снабженный битом смены идентификатора с целью воздействовать на обмен данными между процессами и попытаться нарушить целостность, конфиденциальность или доступность обрабатываемой информации.

Следует препятствовать указанным выше действиям нарушителя, ограничив объем и параметры монтирования для этой ФС.

Для проверки текущего состояния монтирования /dev/shm и опций монтирования ее, выполните команду:

```
#mount | grep -E '\s/dev/shm\s'
```

```
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,noexec)
```

Если вывод отличается от приведенного выше, следует задать безопасную конфигурацию для ФС /dev/shm. Для установки на ФС /dev/shm специальных опций монтирования (nodev,noexec,nosuid) — внести изменения в четвертое поле файла /etc/fstab вместо defaults:

```
tmpfs /dev/shm tmpfs nodev,noexec,nosuid 0 0
```

Перемонтировать ФС:

```
#mount -o remount /dev/shm
```

Настройка политики использования ссылок

Возможности ОС РОСА «НИКЕЛЬ» могут позволять пользователю работать со ссылками. Потенциальный нарушитель может использовать эти возможности для:

– создания ссылок на объекты ФС, которые подготовлены заранее (включая файлы устройств, файлы, снабженные битом смены идентификатора, исполняемые файлы и т.п.);

– создания ссылок на удаленные ресурсы нарушителя (включая подготовленные заранее сетевые ресурсы и т.п.);

– реализации атак типа «гонки состояний» (Race Conditions), при которой ссылки будут создаваться друг на друга в некоем конечном (но очень большом) множестве;

– реализации атак типа «отказ в обслуживании» (DOS — Denial Of Service), приводящих к переполнению метаданных (i-node) в ФС большим количеством ссылок и/или их высокой иерархической вложенностью.

Для предотвращения указанных выше возможностей нарушителя, в защищенной системе следует использовать политику ужесточения при разграничении доступа к ссылкам, базирующуюся на следующих перечисленных ниже принципах для «жестких» (hardlinks) и «символических» (softlinks) ссылок соответственно.

Субъекту доступа для создания «жесткой» ссылки необходимо выполнить одно из следующих условий.

– субъект может ссылаться только на файлы, которыми он владеет;

– субъект должен сначала иметь доступ на чтение и запись к файлу, к которому он хочет подключиться.

Субъекту разрешено следовать только по ссылкам, которые находятся за пределами доступных для публичной записи каталогов, или одно из следующего должно быть выполнено:

– процесс, следующий по символической ссылке, является владельцем

символической ссылки;

– владелец каталога также совпадает с владельцем символической ссылки.

Для проверки политики при работе со ссылками выполнить:

```
#sysctl -a | grep links
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
```

Если вывод отличается, то настроить политику. Для этого выполнить:

```
#sysctl -w fs.protected_hardlinks=1
#sysctl -w fs.protected_symlinks=1
#echo 'fs.protected_hardlinks = 1' >> /etc/sysctl.conf
#echo 'fs.protected_symlinks = 1' >> /etc/sysctl.conf
```

Настройка ФС /proc

Настройки ОС РОСА «НИКЕЛЬ» по умолчанию предусматривают возможность получения доступа к информации обо всех процессах в системе для любого пользователя. Такая возможность может помочь потенциальному нарушителю собрать информацию о системе, включая сведения о СЗИ и их настройках, используемых в ОС.

В защищенной системе необходимо противодействовать действиям нарушителя, направленным на получение информации. Для этого следует использовать настройку политики доступа к служебной ФС /proc, при которой пользователям системы будет разрешено просматривать информацию только о собственных процессах, но ни о процессах, принадлежащих другим пользователям.

Для проверки того, используется ли настройка скрытия информации о процессах других пользователей выполнить:

```
#mount | grep /proc
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime,hidepid=invisible)
```

В том случае, если настройка отличается, внести следующие изменения в файл /etc/fstab и выполнить перемонтирование ФС /proc:

```
proc /proc proc defaults,noexec,nodev,nosuid,hidepid=2 0 0
#mount -o remount /proc
```

Настройка каталогов, доступных к публичной записи

Все публично доступные на запись каталоги должны постоянно отслеживаться и снабжаться специальным битом sticky, чтобы предотвратить бесконтрольное удаление

файлов из них. Рекомендуется с помощью планировщика задач создать регулярное задание по поиску таких каталогов и осуществлять автоматизированное изменение прав для применения бита sticky. Для поиска таких каталогов требуется выполнить:

```
#df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null
```

Вывода на экран быть не должно. Иначе выполнить присвоение бита:

```
#df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null | xargs -I '{}' chmod a+t '{}'
```

13.1.4. Настройка изоляции процессов

13.1.4.1. Аннотация угрозы

Повторное использование или повторный доступ к информации, содержащейся в страницах оперативной памяти.

13.1.4.2. Описание угрозы

В страницах памяти виртуального адресного пространства, выделяемых процессу, содержится информация, необходимая для его функционирования, а также обрабатываемая информация, в том числе, подлежащая защите. В этих страницах могут храниться ключи шифрования, защищаемые данные, хэши паролей пользователей, идентификаторы субъектов и объектов и т.п. Повторное использование или доступ к информации, содержащейся в страницах оперативной памяти может способствовать раскрытию указанной информации потенциальным нарушителем, в случае выполнения соответствующего запроса к ней.

Поэтому требуется обеспечить невозможность или существенно затруднить доступ к предыдущему содержанию страниц памяти. Для этого в составе ядра ОС содержится поддержка соответствующей технологии, а именно — технология случайного выделения страниц памяти при их первичном распределении ASLR — Address Space Layout Randomization. Правильная настройка ASLR обеспечивает изоляцию процессов. Применение ASLR существенным образом затрудняет для потенциального нарушителя возможность эксплуатации уязвимостей, связанных с повторным получением доступа к использовавшимся страницам памяти процесса(ов).

13.1.4.3. Идентификаторы угрозы

По БДУ ФСТЭК России:

– УБИ.012: Угроза деструктивного изменения конфигурации/среды окружения программ;

– УБИ.022: Угроза избыточного выделения оперативной памяти;

– УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией;

– УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением.

Потенциальные уязвимости согласно MITRE Common Weakness Enumeration:

– CWE-203: Observable Discrepancy;

– CWE-213: Exposure of Sensitive Information Due to Incompatible Policies;

– CWE-226: Sensitive Information in Resource Not Removed Before Reuse;

– CWE-330: Use of Insufficiently Random Values;

– CWE-1303: Non-Transparent Sharing of Microarchitectural Resources.

По ИТ.ОС.А2.ПЗ:

– Угроза-5 — утечка или несанкционированное изменение информации в оперативной памяти, используемой различными процессами и формируемыми ими потоками данных.

Матрица MITRE ATT&CK:

– T1057 Process Discovery.

13.1.4.4. Способ противостояния угрозе

Реализация конфигурации системы, предусматривающая случайное выделение страниц памяти для процесса при каждом первичном распределении ресурса (ASLR), т.е. задействовать механизм изоляции процессов.

MITRE ATT&CK Mitigations:

– M1048 Application Isolation and Sandboxing;

– M1042 Disable or Remove Feature or Program.

13.1.4.5. Проекция ИФБО к ФТБ

Настройка перечисленных ИФБО способствует реализации ФТБ, мер защиты или контроля.

Проекция ИФБО к ФТБ для интерфейса управления ASLR приведена в таблице (Таблица 53).

Таблица 53

ИФБО	ФТБ ГОСТ 15408-2	Мера защиты 17-ого приказа ФСТЭК России	Контроль ГОСТ 27002
/etc/sysctl.conf	FPO_DFS_EXT.1	ЗИС.19	11.2.2. а)
/sbin/sysctl			11.3.3

13.1.4.6. Проверки и действия

Все проверки и действия выполняются в контексте учетной записи суперпользователя, если специально не определено иное.

Необходимые действия описаны ниже.

Настройка параметров изоляции процессов

Описанная ниже переменная ядра ОС может принимать значение «0», при котором нет рандомизации, и распределение страниц памяти происходит статично.

Значение «1» означает консервативную рандомизацию. Данные об общих библиотеках, стеке, mmap()VDSO рандомизированы. Значение «2» определяет полную рандомизацию. В дополнение к элементам, перечисленным в предыдущем пункте, управляемая память brk()также рандомизирована.

Для проверки механизма применения ASLR (изоляции процессов) необходимо использовать следующие команды:

```
#sysctl kernel.randomize_va_space
```

В ответ система должна сообщить текущее значение параметра ядра по изоляции процессов.

```
kernel.randomize_va_space = 2
```

В том случае, если выведенное на экран значение изоляции отлично от «2», требуется произвести настройку ASLR.

Для активизации поддержки механизма изоляции процессов ASLR требуется выполнить:

```
#echo "kernel.randomize_va_space = 2" >> /etc/sysctl.conf
#sysctl -w kernel.randomize_va_space=2
```

13.1.5. Отключение динамического связывания (prelink)

13.1.5.1. Аннотация угрозы

Использование предварительного динамического связывания (prelink), которое потенциально может привести к нарушению целостности элементов разделяемых библиотек и исполняемых файлов при их предварительном динамическом связывании с целью ускорения запуска.

13.1.5.2. Описание угрозы

Так называемое предварительное связывание (prelink) — наделяет исполняемые файлы и библиотеки формата ELF (ELF-файлы) наиболее выгодной с точки зрения производительности чертой формата a.out. Запускаемые файлы (заранее, до загрузки в память) модифицируются таким образом, чтобы уже включать в себя результат динамического связывания и, соответственно, заранее знать собственные адреса в памяти процесса и не тратить на их вычисление время в течение запуска, что может существенно ускорять запуск ПО.

Однако это приводит к изменениям в составе данных исполняемых файлов и

библиотек в момент их предварительного распределения, что делает возможным компрометацию их целостности и осуществлению атак, направленных на изменение в составе обрабатываемых данных как исполняемых файлов, так и разделяемых библиотек (атаки внедрения кода).

13.1.5.3. Идентификаторы угрозы

По БДУ ФСТЭК России:

- УБИ.006: Угроза внедрения кода или данных.

Потенциальные уязвимости согласно MITRE Common Weakness Enumeration:

- CWE-94: Improper Control of Generation of Code ('Code Injection');
- CWE-676: Use of Potentially Dangerous Function;
- CWE-913: Improper Control of Dynamically-Managed Code Resources.

По ИТ.ОС.А2.ПЗ:

- Угроза-11 — несанкционированный доступ субъектов доступа к информации, обработка которой осуществлялась в рамках сеансов (сессий) других субъектов доступа.

Матрица MITRE ATT&CK:

- T1055 Process Injection.

13.1.5.4. Способ противостояния угрозе

Реализация конфигурации системы, не предусматривающая использование механизма предварительного связывания исполняемых файлов и разделяемых библиотек (prelink)

MITRE ATT&CK Mitigations:

- M1040 Behavior Prevention on Endpoint;
- M1026 Privileged Account Management;
- M1042 Disable or Remove Feature or Program.

13.1.5.5. Проекция ИФБО к ФТБ

Настройка перечисленных ИФБО способствует реализации ФТБ, мер защиты или контроля.

Проекция ИФБО к ФТБ для интерфейсов управления динамическим связыванием приведена в таблице (Таблица 54).

Таблица 54

ИФБО	ФТБ ГОСТ 15408-2	Мера защиты 17-го приказа ФСТЭК России	Контроль ГОСТ 27002
/usr/bin/prelink	Не применимо	ОЦЛ.1, ОПС.1	11.2.2. а) 11.3.3
/usr/bin/rpm	FDP_RSP_EXT.2.2		

13.1.5.6. Проверки и действия

Все проверки и действия выполняются в контексте учетной записи суперпользователя, если специально не определено иное.

Необходимые действия описаны ниже.

Проверка наличия prelink

Для проверки наличия prelink требуется выполнить:

```
#rpm -qa| grep prelink
```

Отключение prelink

В случае, если prelink установлен, то требуется вернуть исполняемые файлы и библиотеки в исходное состояние, для чего необходимо выполнить:

```
#prelink -ua
```

Выполнить удаление prelink:

```
#rpm -e prelink
```

13.1.6. Контроль целостности с помощью AIDE

13.1.6.1. Аннотация угрозы

Отсутствие КЦ.

13.1.6.2. Описание угрозы

Отсутствие КЦ препятствует достижению критерия безопасности и приобретению доверия. Отсутствие КЦ делает возможным реализацию любых атак.

13.1.6.3. Идентификаторы угрозы

По БДУ ФСТЭК России:

– УБИ.012: Угроза деструктивного изменения конфигурации/среды окружения программ.

Потенциальные уязвимости согласно MITRE Common Weakness Enumeration:

– CWE-94: Improper Control of Generation of Code (‘Code Injection’);

– CWE-676: Use of Potentially Dangerous Function;

– CWE-913: Improper Control of Dynamically-Managed Code Resources.

По ИТ.ОС.А2.ПЗ:

– Угроза-6 – несанкционированное внесение нарушителем изменений в конфигурационные (и иные) данные, которые влияют на функционирование отдельных сервисов, приложений или ОС в целом;

– Угроза-9 – несанкционированное внесение изменений в журналы регистрации событий безопасности ОС;

– Угроза-10 – несанкционированный доступ к информации вследствие использования пользователями ОС неразрешенного ПО.

Матрица MITRE ATT&CK:

- TA0004 Privilege Escalation;
- TA0005 Defense Evasion;
- TA0040 Impact;
- T1547 Boot or Logon Autostart Execution.

13.1.6.4. Способ противостояния угрозе

Реализация конфигурации проверки КЦ с помощью AIDE.

AIDE — это система обнаружения атак, основанная на узле (Host-Based Intrusion Detection System, HIDS). Программа используется для обнаружения изменений в заранее определенных объектах с помощью сверки уникальных значений контрольных сумм, созданных для каждого из объектов и сохраненных в базе КЦ.

Принцип действия: заранее сохраненное значение хэш-суммы объекта и его метаданных сравнивается с вычисленным текущим значением, чтобы определить какой из объектов был изменен.

MITRE ATT&CK Mitigations:

- M1004 System Partition Integrity;
- M1025 Privileged Process Integrity;
- M1045 Code Signing;
- M1046 Boot Integrity.

13.1.6.5. Проекция ИФБО к ФТБ

Настройка перечисленных ИФБО способствует реализации ФТБ, мер защиты или контроля.

Проекция ИФБО к ФТБ для интерфейсов КЦ приведена в таблице (Таблица 55).

Таблица 55

ИФБО	ФТБ ГОСТ 15408-2	Мера защиты 17-го приказа ФСТЭК России	Контроль ГОСТ 27002
/usr/bin/aide	FDP_RSP_EXT.2	УПД.17, ОПС.1, РСБ.1, ОЦЛ.1	
/etc/aide/aide.conf*	FDP_RSP_EXT.2	УПД.17, ОПС.1, РСБ.1, ОЦЛ.1	

13.1.6.6. Проверки и действия

Все указанные ниже проверки и действия выполняются в контексте учетной записи суперпользователя (root).

Необходимые действия описаны ниже.

Проверка наличия ПО КЦ AIDE

Для проверки наличия AIDE выполнить команду:

```
# rpm -aq | grep aide
aide-0.16.2-4.x86_64
```

Иначе, произвести установку и настройку ПО КЦ.

Настройка AIDE

Для настройки ПО КЦ выполнить:

```
#aideinit
```

Проверить, что КЦ регулярно производится в системе:

```
#systemctl status aidecheck.timer
```

Иначе, произвести настройку планировщика задач на регулярный запуск КЦ ежедневно в 05 часов 00 минут.

```
#crontab -u root -e
#0 5 * * * /usr/sbin/aidecheck
```

13.1.7. Установка предупреждающих сообщений

13.1.7.1. Аннотация угрозы

Отсутствие сообщений для пользователя, совершающего вход (попытку входа) в систему о том, что в системе активизированы механизмы безопасности.

13.1.7.2. Описание угрозы

Отсутствие сообщений для пользователя, совершающего вход (попытку входа) в систему о том, что в системе активизированы механизмы безопасности существенно усложняет привлечение пользователя к ответственности в случае наступления инцидента безопасности. Кроме того, в ОС РОСА «НИКЕЛЬ» по умолчанию нередко используются сообщения, с указанием версии используемой ОС, версии ядра ОС и т.п., которые при их наличии могут способствовать раскрытию информации о состоянии СЗИ в системе.

13.1.7.3. Идентификаторы угрозы

По БДУ ФСТЭК России:

- УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией.

Потенциальные уязвимости согласно MITRE Common Weakness Enumeration:

- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor;
- CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer;
- CWE-862: Missing Authorization.

Матрица MITRE ATT&CK:

- T1119 Automated Collection;
- T1213 Data from Information Repositories.

13.1.7.4. Способ противостояния угрозе

В ОС РОСА «НИКЕЛЬ» есть несколько интерфейсов, отображающих

предупреждающие сообщения для пользователя перед входом. Требуется настроить предупреждающие сообщения с целью уведомления пользователя о том, что он совершает вход в систему, где может обрабатываться информация, подлежащая защите. А сообщения ОС, сконфигурированные по умолчанию (обычно предоставляющие информацию о версии ОС, версии ядра ОС, идентификаторе терминала и т.п.) - должны быть отключены с целью воспрепятствования раскрытию информации о характеристиках системы.

Такие настройки должны быть применены для каждого интерфейса входа.

MITRE ATT&CK Mitigations:

– M1017 User Training.

13.1.7.5. Проекция ИФБО к ФТБ

Настройка перечисленных ИФБО способствует реализации ФТБ, мер защиты или контроля.

Проекция ИФБО к ФТБ для интерфейсов, устанавливающих предупреждающие сообщения приведена в таблице (Таблица 56).

Таблица 56

ИФБО	ФТБ ГОСТ 15408-2	Мера защиты 17-го приказа ФСТЭК России	Контроль ГОСТ 27002
/etc/motd	FTA_TAB.1	УПД.7	
/etc/issue*	FTA_TAB.1	УПД.7	
/etc/issue.net	FTA_TAB.1	УПД.7	
/etc/gdm3/greeter.dconf-defaults (настраивается только при наличии Gnome3 и службы GDM)	FTA_TAB.1	УПД.7	

13.1.7.6. Проверки и действия

Действия выполняются в контексте учетной записи суперпользователя. Необходимые действия описаны ниже.

Проверка предупреждающих сообщений не требуется.

Установка предупреждающих сообщений.

Сообщения устанавливаются в файлы /etc/motd, /etc/issue, /etc/issue.net.

Для установки сообщений для пользователей, осуществляющих локальный или удаленный вход и получение оболочки, выполнить команды:

```
#echo 'Unauthorized access to this system is forbidden and will be prosecuted.' > /etc/motd
#echo 'By accessing this system, you agree that your actions may
```

```
be monitored.' >> /etc/motd
      #echo ' ' >> /etc/motd
      #echo 'Данная система предназначена для использования только полномочными пользователями.' >> /etc/motd
      #echo 'Любой неправомерный доступ или попытки доступа могут быть автоматически прерваны.' >> /etc/motd
      #echo 'Получая доступ к системе вы соглашаетесь с тем, что все действия могут быть зафиксированы.' >> /etc/motd
      #cat /etc/motd > /etc/issue
      #cat /etc/motd > /etc/issue.net
      #chown root:root /etc/motd
      #chown root:root /etc/issue
      #chown root:root /etc/issue.net
```

Установить права доступа на файлы /etc/motd, /etc/issue, /etc/issue.net:

```
      #chmod 0644 /etc/motd
      #chmod 0644 /etc/issue
      #chmod 0644 /etc/issue.net
```

Некоторые современные продолжают отображать пользователю различные сообщения при входе, кроме заданных. Это происходит из-за подключенного расширения к модулю авторизации PAM. Для того, чтобы отключить все сообщения, помимо описанных выше, требуется произвести поиск и удаление (или закомментировать с помощью знака решетки «#») следующие строки в файлах /etc/pam.d/login и /etc/pam.d/sshd (при наличии):

```
      #session   optional   pam_motd.so motd=/run/motd.dynamic
      #session   optional   pam_motd.so noupdate
```

Настройка аутентификации для режима обслуживания

При необходимости можно проверить и установить аутентификацию для суперпользователя root, в том случае, если ОС переводится в режим обслуживания (Single User Mode).

Для проверки того, задан ли в ОС пароль для суперпользователя root, необходимо выполнить следующую команду:

```
      #grep ^root:[*\!]: /etc/shadow
```

Вывода на экран быть не должно. Иначе выполнить установку пароля:

```
      #passwd root
```

13.1.8. Дополнительные меры общесистемной защиты

13.1.8.1. Общие сведения по дополнительным мерам

Далее описаны дополнительные меры защиты, которые настоятельно рекомендуется предпринять при реализации безопасной конфигурации ОС, а также среды ее выполнения.

В данном случае будет выполнена идентификация угроз, не предусматривающая проекцию к стандартам или БДУ. Предполагается, что для данных мер, перечень формальных угроз может быть выполнен (спроецирован) самостоятельно органом, осуществляющим эксплуатацию ИС. Это обусловлено следующим соображением: меры, реализация которых позволяет угрозам противостоять, не могут рассматриваться в отрыве от среды выполнения. И эти меры настоятельно рекомендуются к реализации, как на уровне ОС, так и на более низком уровне (BIOS, UEFI).

13.1.8.2. Аннотация угроз

Угроза несанкционированного выполнения кода в пространстве ядра.

Угроза использования ошибочного контроля доступа к памяти при спекулятивном выполнении инструкций процессора (уязвимости типа Meltdown), и/или связанные с особенностями функционирования модуля прогнозирования ветвлений (уязвимости типа Spectre).

13.1.8.3. Описание угроз

Современные процессоры семейства x86 (производства компаний Intel и AMD) предоставляют возможность запрета выполнения кода в некоторых страницах памяти. У процессоров AMD такая возможность называется No Execute Bit (NX bit), у Intel – Execute Disable Bit (XD bit). Задействование данных технологий способствует предотвращению атак, связанных с уязвимостями, вызванными переполнением буфера. Поэтому такие возможности должны быть задействованы в ядре ОС. Иначе потенциальный нарушитель может использовать атаки, вызванные переполнением буфера для воздействия на целостность, конфиденциальность или доступность обрабатываемой информации.

Также рекомендуется включать поддержку NX/XD битов еще и потому, что бинарные модули, выполняющиеся в системе, могут быть скомпилированы без использования техник защиты от переполнения буфера при компиляции (например, опции компилятора GCC типа «fstack-protection» не задействовались).

Современные процессоры семейства x86 предоставляют возможность параллельного использования нескольких «нитей» или «потоков» на каждом процессорном ядре. Такая опция называется SMT (Symmetric Multi-Threading). Поскольку «нити» или «потоки» (исходя из конструктивных особенностей ЦП) сохраняют

возможности обмена информацией между собой, то это потенциально может привести к несанкционированному обмену информацией между процессами, выполняющимися в разных потоках, но на одном ядре ЦП. Либо может привести к нежелательному раскрытию информации в памяти и т.п. Поэтому в защищенной системе опции процессора, отвечающие за SMT требуется отключить. При этом настоятельно рекомендуется использовать комплексный подход — отключать поддержку SMT как на уровне системы ввода-вывода (в BIOS или UEFI, если такая возможность поддерживается производителем оборудования), так и на уровне ОС. Уязвимости, связанные с недостатками SMT не будут проэксплуатированы, например в том случае, если производитель оборудования предоставит ошибочное обновление системы ввода-вывода, повторно включающее SMT после отключения.

13.1.8.4. Способ противостояния угрозам

Способы противостояния угрозам, следующие:

- включение для процессоров Intel бита XD (защиты от переполнения буфера), используя функции BIOS/UEFI;
- включение для процессоров AMD бита NX (защиты от переполнения буфера), используя функции BIOS/UEFI;
- отключение поддержки SMT, используя функции BIOS/UEFI, обеспечивающее противостояние атакам типа Meltdown/Spectre;
- отключение поддержки SMT, используя интерфейсы ОС, обеспечивающее противостояние атакам типа Meltdown/Spectre.

MITRE ATT&CK Mitigations:

- M1048 Application Isolation and Sandboxing;
- M1040 Behavior Prevention on Endpoint;
- M1042 Disable or Remove Feature or Program.

13.1.8.5. Проверка поддержки битов NX/XD

Для проверки того, задействованы ли в BIOS или UEFI функции аппаратной защиты от переполнения буфера, требуется от имени пользователя (суперпользователя) выполнить следующие команды.

Способ №1:

```
$journalctl | grep “protection: active”
kernel: NX (Execute Disable) protection: active
```

В том случае, если вывод отличается от приведенного выше, то требуется включить соответствующие опции в BIOS/UEFI (при наличии таковых) и перепроверить.

Способ №2:

```
$[[ -n $(grep noexec[0-9]*=off /proc/cmdline) || -z $(grep -E -i ‘ (pae|nx) ‘ /proc/cpuinfo) || -n $(grep ‘\sNX\s.*\sprotection:\s’ /var/log/dmesg | grep -v active) ]] && echo “NX Protection is not active”
```

В случае поддержки защиты от переполнения буфера — вывода не будет.

Иначе, требуется включить соответствующие опции в BIOS/UEFI (при наличии таковых) и перепроверить.

13.1.8.6. **Отключение SMT**

Для проверки того, используется ли технология SMT, требуется от имени пользователя (суперпользователя) выполнить следующую команду:

```
$ cat /sys/devices/system/cpu/smt/active
0
```

где «0» свидетельствует об отсутствии поддержки.

Иначе, если вывод не «0», а «1», то требуется отключить поддержку SMT, сначала в BIOS/UEFI. А затем выключить на уровне ОС. Для отключения поддержки SMT в ОС, требуется от имени суперпользователя выполнить изменение строки «GRUB_CMDLINE_LINUX=» конфигурационного файла /etc/default/grub, дописав в ее конец следующие директивы:

```
mitigations=auto,nosmt
```

После этого переинициализировать загрузчик:

```
#update-grub2
Sourcing file `/etc/default/grub’
Sourcing file `/etc/default/grub.d/init-select.cfg’
Генерируется файл настройки grub …
…
Adding boot menu entry for UEFI Firmware Settings
завершено
```

Далее выполнить перезагрузку и перепроверить.

13.1.9. Настройка синхронизации единого времени

13.1.9.1. Аннотация угрозы

Неверная конфигурация при синхронизации времени или отсутствие синхронизации времени.

13.1.9.2. Описание угрозы

Единое время, исчисляемое в рамках одной ИС (или среды), имеет критическое значение для безопасности. При отсутствии синхронизации времени или неверной

синхронизации, допускающей расхождения, невозможна корректная работа других служб и сервисов, предназначенных для безопасной эксплуатации ИС.

Например, использование служб аутентификации, таких как Kerberos, предполагает наличие единого времени для информации, хранящейся в билете. Без единого времени система безопасности не в состоянии принять верное решение при принятии авторизационных решений. Надежная работа механизмов TOTP, обеспечивающих многошаговую проверку при аутентификации, становится также невозможной. Службы аудита, фиксирующие системные события (в том числе события безопасности), будут записывать в сообщения аудита неверное время, что сделает невозможным достоверное расследование инцидентов безопасности. Службы планировщиков, службы для создания или восстановления резервных копий — все они будут не в состоянии надежно работать.

Требуется наличие надежного общего источника единого времени, действующего в рамках ИС. Каждая ОС должна быть сконфигурирована на использование временных меток, получаемых от такого источника.

13.1.9.3. Идентификаторы угрозы

По БДУ ФСТЭК России:

– УБИ.012: Угроза деструктивного изменения конфигурации/среды окружения программ;

– УБИ.214: Угроза несвоевременного выявления и реагирования компонентами ИС и АС (в том числе СЗИ) на события безопасности информации.

По MITRE Comon Weakness Enumeration:

– CWE VIEW: Architectural Concepts (семейство архитектурных уязвимостей).

По ИТ.ОС.А2.ПЗ:

– Угроза-6 – несанкционированное внесение нарушителем изменений в конфигурационные (и иные) данные, которые влияют на функционирование отдельных сервисов, приложений или ОС в целом.

Матрица MITRE ATT&CK:

– T1070.006 Indicator Removal on Host: Timestomp;

– T1556 Modify Authentication Process;

– T1547 Boot or Logon Autostart Execution.

13.1.9.4. Способ противостояния угрозе

Настройка синхронизации времени в ОС.

В ОС должна быть настроена только одна служба, а остальные должны быть недоступны.

В составе современных ОС РОСА «НИКЕЛЬ» обычно присутствует несколько служб, реализующих функции синхронизации времени, а именно:

- служба systemd-timesyncd (из состава службы инициализации systemd);
- служба chrony;
- служба ntp.

В настоящем документе описывается реализация настройки службы ntp (из соображений универсальности).

Необходимо учитывать, что выбрав любой удобный вариант настройки, остальные службы необходимо выключить и удалить.

MITRE ATT&CK Mitigations:

- M1028 Operating System Configuration.

13.1.9.5. Проекция ИФБО к ФТБ

Настройка или использование перечисленных ИФБО способствует реализации ФТБ, мер защиты или контроля.

Проекция ИФБО к ФТБ для интерфейсов, управляющих конфигурацией службы времени приведена в Таблица 57.

Таблица 57

ИФБО	ФТБ ГОСТ 15408-2	Мера защиты 17-го приказа ФСТЭК России	Контроль ГОСТ 27002
/etc/ntp.conf /etc/init.d/ntp	FPT_STM.1	РСБ.6	

13.1.9.6. Проверки и действия

Проверки и действия выполняются в контексте учетной записи суперпользователя.

Необходимые действия описаны ниже.

Проверка использования ntp для синхронизации времени

Для проверки того, используется ли служба ntp, выполнить следующие команды:

```
#rpm -aq | grep chrony
chrony-4.0.2.x86_64
```

В том случае, если вывод отличается и свидетельствует о том, что используется chrony, то требуется удалить этот компонент.

Затем проверить, не используется ли systemd-timesyncd:

```
# systemctl is-enabled systemd-timesyncd
disabled
```

В том случае, если вывод отличается и свидетельствует о том, что используется systemd-timesyncd, то требуется отключить этот компонент (0).

```
# grep "^restrict" /etc/ntp.conf
restrict -4 default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
```

Строка, начинающаяся с «- 4», может отсутствовать в выводе, а опции, следующие после «default» могут располагаться в произвольном порядке.

```
# grep -E "^(server|pool)" /etc/ntp.conf
server <remote-server>
```

В выводе может присутствовать несколько адресов для нескольких серверов NTP.

```
# grep "RUNASUSER=ntp" /etc/init.d/ntp
RUNASUSER=ntp
```

Вывод должен свидетельствовать о том, что служба ntp работает от имени (в контексте полномочий) системного пользователя ntp.

Настройка использования ntp

Для настройки ntp выполнить следующее. Произвести удаление chrony:

```
#rpm -e chrony
```

Отключить использование systemd-timesyncd:

```
#systemctl --now mask systemd-timesyncd
```

Сконфигурировать ntp, для чего внести соответствующие строки в файл /etc/ntp.conf:

```
restrict -4 default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
```

Указать адрес необходимого (определенного в ИС) сервера NTP для синхронизации. Допускается указывать адреса нескольких серверов, повторяя директиву server с новой строки.

```
server <IP_адрес_сервера_NTP>
```

Указать, что служба будет выполняться от имени (в контексте полномочий) системного пользователя ntp. Для чего отредактировать файл /etc/init.d/ntp:

```
RUNASUSER=ntp
```

Затем выполнить перезагрузку, после чего повторно выполнить проверку функционирования службы NTP (см. 0).

13.1.10. Конфигурация сервисов и их клиентов

13.1.10.1. Аннотация угрозы

Неверная конфигурация ОС, предусматривающая выполнение избыточного количества сервисов (служб).

13.1.10.2. Описание угрозы

В составе ОС РОСА «НИКЕЛЬ» может выполняться большое количество служб и сервисов, выполняющих разные задачи. Также в системе могут присутствовать ненужные клиенты служб. В защищенной системе должны выполняться только необходимые из них. Кроме того, некоторые службы и сервисы по своим характеристикам могут передавать данные, не подвергая их шифрованию или маскировке (т.е. «открытым текстом»). А некоторые службы (клиенты) могут иметь устаревшую, неподдерживаемую или плохую реализацию.

Все эти факторы крайне отрицательно влияют на безопасность системы и значительно увеличивают площадь атаки, как на ОС, так и на ИС в целом. Чтобы избежать отрицательного влияния такой избыточности, не используемые службы (сервисы), а также их клиентские приложения, необходимо отключить. Для использования требуемых служб и клиентов, необходимо подготовить четкую и непротиворечивую аргументацию, а также необходимо подвергать используемые службы постоянному наблюдению (отслеживанию).

13.1.10.3. Идентификаторы угрозы

По БДУ ФСТЭК России:

– УБИ.012: Угроза деструктивного изменения конфигурации/среды окружения программ;

– УБИ.012: Угроза деструктивного изменения конфигурации/среды окружения программ;

– УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными;

– УБИ.069: Угроза неправомерных действий в каналах связи;

– УБИ.166: Угроза внедрения системной избыточности;

– УБИ.178: Угроза несанкционированного использования системных и сетевых утилит;

– УБИ.214: Угроза несвоевременного выявления и реагирования компонентами ИС иАС (в том числе СЗИ) на события безопасности информации.

Потенциальные уязвимости согласно MITRE Common Weakness Enumeration:

– CWE-250: Execution with Unnecessary Privileges;

– CWE-657: Violation of Secure Design Principles;

– CWE-671: Lack of Administrator Control over Security;

– CWE-841: Improper Enforcement of Behavioral Workflow;

– CWE-1244: Improper Access to Sensitive Information Using Debug and Test

Interfaces.

По ИТ.ОС.А2.ПЗ:

– Угроза-10 — несанкционированный доступ к информации вследствие использования пользователями ОС неразрешенного ПО.

Матрица MITRE ATT&CK:

– TA0038 Network Effects;

– T1119 Automated Collection;

– T1213 Data from Information Repositories;

– T1498 Network Denial of Service;

– T1135 Network Share Discovery;

– T1046 Network Service Scanning;

– T1040 Network Sniffing;

– T1039 Data from Network Shared Drive.

13.1.10.4. Способ противостояния угрозе

Привести конфигурацию системы в состояние, при котором будут выполняться только необходимые службы и сервисы.

MITRE ATT&CK Mitigations:

– M1042 Disable or Remove Feature or Program;

– M1022 Restrict File and Directory Permissions;

– M1038 Execution Prevention;

– M1028 Operating System Configuration;

– M1031 Network Intrusion Prevention.

13.1.10.5.

Проверки и действия выполняются в контексте учетной записи суперпользователя.

Необходимые действия описаны ниже.

Сервис avahi

Сервис avahi представляет собой реализацию zeroconf (DNS-SD, APIPA, mDNS, SSDP, UPnP, LLMNR, SLP RFC 2608) — поддержку набора протоколов, служащих для автоматического обнаружения других устройств, услуг, сервисов и служб. Он позволяет программам опубликовывать (анонсировать) в сети свои сервисы, и искать соседние узлы, службы и сервисы. И все это происходит автоматически. Например, если пользователь соединит свой ПК в сеть, то avahi постарается автоматически обнаружить соседних абонентов, в виде узлов сети, их служб, принтеров, сетевых ресурсов и т.п. Рекомендуется использовать этот сервис только в случае реальной необходимости.

Иначе требуется его отключить.

Для проверки того, присутствует ли в системе сервис avahi, требуется выполнить:

```
#rpm -qa avahi-daemon
```

Если вывод отличается, то нужно остановить и удалить сервис. Для отключения и удаления сервиса требуется выполнить:

```
# systemctl stop avahi-daaemon.service
# systemctl stop avahi-daemon.socket
# rpm -e avahi-daemon
```

Сервис CUPS

Common UNIX Print System (CUPS) — основная и самая распространенная реализация службы печати для UNIX/Linux с открытым исходным кодом. Создана и поддерживается компанией Apple Inc. Предназначена для организации печати, как сетевой, так и локальной. Поскольку сервис (служба) CUPS, имея соответствующий интерфейс, принимает задания на печать (в т. ч. по сети), а также так как она поддерживает Web-панель для управления (порт 651 на интерфейсе обратной петли), то она может стать объектом сетевых атак. Рекомендуется применять CUPS только там, где действительно есть потребность в печати. Иначе требуется исключить данный сервис из состава выполняемого ПО.

Для проверки того, присутствует ли в системе CUPS выполнить:

```
# rpm -qa cups
```

Иного вывода быть не должно. Иначе, удалите систему печати. Естественно, удаление CUPS сделает невозможной печать на АРМ.

```
# rpm -e –nodeps cups-*
```

Сервис DHCP

Dynamic Host Configuration Protocol (DHCP) — сервис (служба), предоставляющий возможность назначения адресов IP для других АРМ. Как правило, такая служба используется на сервере. Использование этой службы на АРМ не должно быть предусмотрено.

Для проверки того, присутствует ли в системе DHCP выполнить:

```
# rpm -qa isc_dhcp_server
```

Если вывод отличается, то удалите службу DHCP и выполните перезагрузку.

```
# rpm -e --nodeps isc-dhcp-server
```

Сервис LDAP

Lightweight Directory Access Protocol (LDAP) — сервис (служба), предоставляющий возможность использования службы каталогов. Как правило, такая служба используется

на сервере. Использование этой службы на АРМ не должно быть предусмотрено.

Для проверки того, присутствует ли в системе LDAP выполнить:

```
# rpm -qa slapd
```

Иного вывода быть не должно. Иначе, удалите службу LDAP.

```
# rpm -e --nodeps slapd
```

Сервис NFS

Network File System (NFS) — сервис (служба), предоставляющий возможность использования сетевых ресурсов. Использование этой службы на АРМ должно быть предусмотрено только для тех АРМ, на которых она действительно нужна. Иначе, она должна быть удалена из системы. Уязвимым местом данной службы можно считать то, что обмен данными в NFS производится в открытом виде.

Для проверки того, присутствует ли в системе NFS выполнить:

```
# rpm -qa nfs-kernel-server
```

Иного вывода быть не должно. Иначе, удалите службу NFS.

```
# rpm -e --nodeps rpcbind
```

Сервис DNS

Domain Name System (DNS)— сервис (служба), предоставляющий возможность преобразования сетевых имен в адреса и наоборот. Использование этой службы на АРМ не должно быть предусмотрено. Обычно она используется на сервере. Служба DNS должна быть удалена из системы.

Для проверки того, присутствует ли в системе DNS выполнить:

```
# rpm -qa bind9
```

Иного вывода быть не должно. Иначе, удалите службу DNS.

```
# rpm -e --nodeps bind9
```

Сервис NIS

Network Information Service (NIS)— устаревший сервис (служба), ранее использовавшийся для управления доменной инфраструктурой. Поддерживается исключительно из соображений совместимости с устаревшими версиями ОС. Не рекомендуется его использовать.

Для проверки того, присутствует ли в системе NIS выполнить:

```
# rpm -qa nis
```

Иного вывода быть не должно. Иначе, удалите службу NIS.

```
# rpm -e --nodeps nis
```

Клиент службы rsh

Устаревший клиент службы rsh, использовавшийся до широкого появления ssh,

предполагает возможность удаленного выполнения команд. Шифрование не поддерживает и это клиентское приложение требуется удалить.

Для проверки того, присутствует ли в системе клиент rsh выполнить:

```
# rpm -qa rsh-client
```

Если вывод отличается, то удалите ПО rsh-client.

```
rpm -e --nodeps rsh-client
```

Клиент службы talk

Клиент службы talk (устанавливаемый по умолчанию), используется для обмена сообщениями между пользователями. Сообщения отправляются или принимаются прямо в сессию терминала. Поскольку данный протокол обмена данными не предусматривает никакое шифрование или иной способ сокрытия информации, то это несет потенциальный риск для безопасности. Данное клиентское приложение требуется удалить.

Для проверки того, присутствует ли в системе клиент talk выполнить:

```
# rpm -qa talk
```

Иного вывода быть не должно. Иначе, удалите ПО talk.

```
# rpm -e --nodeps talk
```

Клиент telnet

Устаревший клиент службы telnet, использовавшийся до широкого появления ssh, предполагает возможность удаленного выполнения команд. Шифрование не поддерживает. Данное клиентское приложение требуется удалить.

Для проверки того, присутствует ли в системе клиент telnet выполнить:

```
# rpm -qa telnet
```

Иного вывода быть не должно. Иначе, удалите ПО telnet .

```
# rpm -e --nodeps telnet
```

Клиент службы LDAP

Протокол LDAP требуется использовать только в случае совместного использования с Kerberos, для обеспечения безопасной аутентификации. Иначе, клиент LDAP требуется удалить.

Для проверки того, присутствует ли в системе клиент ldap выполнить:

```
# rpm -qa ldap-utils
```

Иного вывода быть не должно. Иначе, удалите ПО ldap-utils.

```
# rpm -e --nodeps ldap-utils
```

Клиент службы RPC

Клиент службы Remote Procedure Call (RPC), используется для создания

низкоуровневых клиент-серверных приложений в гетерогенной сетевой среде. Использование RPC должно быть строго необходимо и обосновано для ИС. В общем случае использовать RPC не рекомендуется. Данное клиентское приложение требуется удалить.

Для проверки того, присутствует ли в системе клиент rpcbind выполнить:

```
# rpm -qa rpcbind
```

Иного вывода быть не должно. Иначе, удалите ПО rpcbind.

```
# rpm -e --nodeps rpcbind
```

Отключение интерфейсов WLAN

В защищенной системе требуется ограничить или исключить использование беспроводных соединений WLAN. Для проверки того, используются ли на узле интерфейсы WLAN, выполнить сценарий:

```
#!/bin/bash
if command -v nmcli >/dev/null 2>&1 ; then
nmcli radio all | grep -Eq '\s*\S+\s+disabled\s+\S+\s+disabled\b' && echo "Беспроводная сеть отключена" || nmcli radio all
elif [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
t=0
drivers=$(for driverdir in $(find /sys/class/net/*/ -type d -name wireless
| xargs -0 dirname); do basename "$(readlink -f
"$driverdir"/device/driver)";done | sort -u)
for dm in $drivers; do
if grep -Eq "^\s*install\s+$dm\s+/bin/(true|false)"
/etc/modprobe.d/*.conf; then
/bin/true
else
echo "$dm не отключено"
t=1
fi
done
[[ $t -eq 0 ]] && echo "Беспроводная сеть отключена"
else
```

```
echo "Беспроводная сеть отключена"
fi
```

Пример выполнения сценария:

```
#./checkwifi.sh
WIFI-HW WIFI   WWAN-HW WWAN
включен отключен включен включен
```

Иначе, произвести отключение интерфейсов WLAN, для чего выполнить предлагаемый сценарий:

```
#!/bin/bash
if command -v nmcli >/dev/null 2>&1 ; then
nmcli radio all off
else
if [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
drivers=$(for driverdir in $(find /sys/class/net/*/ -type d -name
wireless | xargs -0 dirname); do basename "$(readlink -f
"$driverdir"/device/driver)";done | sort -u)
for dm in $drivers; do
echo "install $dm /bin/true" >> /etc/modprobe.d/disable_wireless.conf
done
fi
fi
```

Отключение интерфейсов Bluetooth

В защищенной системе требуется ограничить или исключить использование беспроводных соединений Bluetooth. Для проверки того, используются ли на узле интерфейсы Bluetooth, выполнить:

```
#cat /etc/bluetooth/main.conf | grep AutoEnable
AutoEnable=true
# bluetoothctl list
Controller 4C:1D:96:XX:XX:XX [default]
# bluetoothctl show
Controller 4C:1D:96:XX:XX:XX (public)
    Name: XXXX
```

```
        Alias: XXXX
        Class: 0x000XXXXX
        Powered: yes
        Discoverable: no
        DiscoverableTimeout: 0x000000XX
        Pairable: no
        UUID: A/V Remote Control      (0000110e-0000-1000-8000-
XXXXXXXXXXXX)
        UUID: Audio Source            (0000110a-0000-1000-8000-
XXXXXXXXXXXX)
        UUID: PnP Information         (00001200-0000-1000-8000-
XXXXXXXXXXXX)
        UUID: Headset AG              (00001112-0000-1000-8000-
XXXXXXXXXXXX)
        UUID: Audio Sink              (0000110b-0000-1000-8000-
XXXXXXXXXXXX)
        UUID: A/V Remote Control Target    (0000110c-0000-1000-8000-
XXXXXXXXXXXX)
        UUID: Generic Access Profile       (00001800-0000-1000-8000-
XXXXXXXXXXXX)
        UUID: Headset                 (00001108-0000-1000-8000-
XXXXXXXXXXXX)
        UUID: Generic Attribute Profile    (00001801-0000-1000-8000-
XXXXXXXXXXXX)
        Modalias: usb:XXXXXXXXXXXXXXX
        Discovering: no
    Advertising Features:
        ActiveInstances: XXXX
        SupportedInstances: XXXX
        SupportedIncludes: tx-power
     SupportedIncludes: appearance
     SupportedIncludes: local-name
     SupportedSecondaryChannels: 1M
     SupportedSecondaryChannels: 2M
     SupportedSecondaryChannels: Coded
     # bluetoothctl devices
```

```
Device F5:11:6C:XX:XX:XX MiMouse
```

Для отключения интерфейсов Bluetooth выполнить:

```
# echo 'rfkill block bluetooth' >> /etc/rc.local
# echo 'AutoEnable=false' >> /etc/bluetooth/main.conf
```

Отключение поддержки протокола IPv6

С целью снижения общей площади атаки на защищенную систему требуется отключить поддержку протокола IPv6, если необходимость в его использовании отсутствует. Для проверки того, поддерживает ли система работу по протоколу IPv6, выполнить:

```
# grep "^\s*linux" /boot/grub2/grub.cfg | grep -v "ipv6.disable=1"
```

Вывода быть не должно. Иначе, произвести отключение поддержки протокола Bluetooth, для чего отредактировать файл /etc/default/grub и переустановить загрузчик GRUB2:

```
GRUB_CMDLINE_LINUX="ipv6.disable=1"
#update-grub2
```

Настройка длины и алфавита пароля

В составе ОС РОСА «НИКЕЛЬ» присутствует модуль PAM pam_pwquality.so, настраиваемый с помощью файла /etc/security/pwquality.conf. Необходимо отредактировать политику паролей в соответствии с требованиями, действующими в конкретной ИС. В общем случае предполагается использовать следующие директивы и значения:

– minlen = 12 – определяет минимальную длину пароля, в символах;

– minclass = 4 – определяет сложность алфавита пароля, где:

«0» – нет требований к сложности алфавита;

«1» – пароль должен содержать хотя бы одну цифру;

«2» – пароль должен содержать хотя бы одну цифру и одну букву в верхнем регистре;

«3» – пароль должен содержать хотя бы одну цифру, одну букву в верхнем регистре и одну букву в нижнем регистре;

«4» – пароль должен содержать хотя бы одну цифру, одну букву в верхнем регистре, одну букву в нижнем регистре и один специсимвол.

retry=3 – определяет количество попыток повторного ввода пароля, прежде чем

аутентификация будет принята, в случае верного указания, или прежде, чем в аутентификации будет отказано. Например, три попытки.

Если нужно определять минимальное количество символов какого-то определенного класса (цифры, буквы в разных регистрах или спецсимволов), то требуется указывать каких именно символов и сколько минимум в пароле должно быть. Для этого можно указать, например:

- dcredit = -2 – не менее 2-х цифр;
- ucredit = -2 – не менее 2-х букв в верхнем регистре;
- ocredit = -2 – не менее 2-х спецсимволов;
- lcredit = -2 – не менее 2-х букв в нижнем регистре.

Проверить, установлена ли библиотека libpam-pwquality:

```
#rpm -aq | grep pam_pwquality
pam_pwquality-1.4.0-5.x86_64
```

Для проверки текущей политики длины пароля выполнить:

```
#grep '^\s*minlen\s*' /etc/security/pwquality.conf
minlen = 12
```

Для проверки текущей политики алфавита пароля выполнить:

```
# grep '^\s*minclass\s*' /etc/security/pwquality.conf
minclass = 4
```

или выполнить:

```
# grep -E '^\s*[duol]credit\s*' /etc/security/pwquality.conf
dcredit = -2
ucredit = -2
lcredit = -2
ocredit = -2
```

Для проверки текущей политики количества попыток ввода пароля выполнить:

```
# cat /etc/pam.d/system-auth | grep retry
password requisite          pam_pwquality.so retry=3
```

Для настройки политики паролей установить библиотеку ibpam-pwquality:

```
#rpm -ivh pam_pwquality
```

Установить политику длины пароля не менее чем 12 символов. Для этого в файл /etc/security/pwquality.conf внести соответствующее значение:

```
minlen = 12
```

Установить политику сложного алфавита (не менее одной цифры, одной буквы в верхнем регистре, одной буквы в нижнем регистре и не менее одного спецсимвола) или

более строгую. Для этого в файл /etc/security/pwquality.conf внести соответствующее значение:

```
minclass = 4
```

Или:

```
dcredit = -1
ucredit = -1
lcredit = -1
ocredit = -1
```

Установить политику попыток повторного ввода пароля не более 3-х раз. Для этого внести в файл /etc/pam.d/system-auth следующее значение:

```
password requisite pam_pwquality.so retry=3
```

Изменения в модулях аутентификации PAM применяются немедленно.

Настройка блокировки после исчерпания попыток ввода пароля

В защищенной системе требуется настраивать блокировку интерфейсов ввода пароля при достижении некоего максимального критерия попыток ввода. В предыдущем разделе лимит попыток ввода определял количество попыток, после которого принимается решение об отказе в аутентификации. Однако при этом у пользователя, осуществляющего попытки ввода, сохраняется возможность совершить еще три попытки, а потом еще и еще, и т. д. Описанная ниже настройка предусматривает блокирование интерфейсов ввода пароля на определенный срок, чтобы препятствовать потенциальному злоумышленнику постоянно подбирать пароль. Для этого используется модуль аутентификации PAM под названием pam_tally2.so и конфигурационный файл /etc/pam.d/system-auth.

Политика блокировки может принимать следующие значения:

- onerr=«fail|succeed» – продолжать ли обработку при возникновении ошибки;
- deny=«число» – количество попыток ввода пароля до наступления блокировки;
- unlock_time=«число» – требуемое время блокировки, в секундах;
- audit – создавать запись аудита о событии безопасности (если указано);
- silent – не выводить никаких информационных сообщений о блокировке (если указано).

Установить следующую политику: блокировка через 5 попыток ввода на 15 минут, создать запись аудита, не выводить информационных сообщений, или более строгую (в соответствии с требованиями, действующими в ИС). Для этого в файле /etc/pam.d/system-auth указать значения:

Выполнить модификацию файлов политики (/etc/pam.d/system-auth и

/etc/pam.d/password-auth, и добавить туда выше и ниже директивы

auth sufficient pam_unix.so nullok try_first_pass

следующие строки:

auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900

и

auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900

соответственно.

Generated by authselect on Thu May
5 06:33:53 2022
Do not modify this file manually.
auth required pam_env.so
auth required pam_faildelay.so delay=2000000
auth [default=1 ignore=ignore success=ok] pam_succeed_if.so uid >= 500 quiet
auth [default=1 ignore=ignore success=ok] pam_localuser.so
auth required pam_faillock.so preauth audit silent deny=5
unlock_time=900
auth sufficient
auth [default=die]
pam_unix.so nullok try_first_pass
pam_faillock.so authfail audit deny=5 unlock_time
=900
auth requisite pam_succeed_if.so uid >= 500 quiet_success
auth sufficient pam_sss.so forward_pass
auth required pam_deny.so

Рекомендации по настройке политики паролей

Для настройки политики паролей требуется руководствоваться действующей политикой в рамках определенной ИС, определенной в соответствующих документах.

В составе ОС РОСА «НИКЕЛЬ» предусмотрены широкие возможности определения политики паролей, допускающие гибкую настройку. В конфигурации по умолчанию ограничений по сроку действия паролей не предполагается.

В том случае, если требуется использовать настройку устаревания паролей, необходимо для проверки действующей политики выполнить:

```
# grep PASS_MAX_DAYS /etc/login.defs
```

```
PASS_MAX_DAYS 99999
```

Для того, чтобы вывести список пользователей, попадающих под ограничения, выполнить:

```
# grep -E '^[^:]+:[^!*]' /etc/shadow | cut -d: -f1,5
```

Для установления общесистемной политики пароля, ограничивающей срок его действия в один год, внести следующие изменения в файл /etc/login.defs:

```
PASS_MAX_DAYS 365
```

Если необходимо задать политику для отдельного пользователя, выполнить:

```
# chage --maxdays 365 <имя_пользователя>
```

В том случае, если требуется не допускать частой смены пароля пользователя, то возможно установить минимальный срок действия пароля, например сроком в одни сутки, и параметр уведомления для пользователя (в сутках), который определяет количество дней до истечения срока действия пароля, в течении которого пользователь будет получать уведомление о необходимости сменить его (например, за две недели).

Для этого нужно внести следующие изменения в файл /etc/login.defs:

```
PASS_MIN_DAYS  1
PASS_WARN_AGE  14
```

Для того, чтобы установить политику автоматической блокировки бюджетов пользователей после заданного периода неактивности (например, в 30 дней), выполнить:

```
# useradd -D -f 30
```

Если требуется использовать дифференцированную политику, выполнить:

```
# chage --inactive <количество дней> <пользователь>
```

Все пользователи системы должны иметь дату смены (назначения) пароля в прошлом. В том случае, если время системы переводилось назад, может возникнуть ситуация, когда дата смены (назначения) пароля у пользователя окажется в будущем. В такой ситуации для этого пользователя никакие ограничения писанных выше парольных политик действовать не будут. Требуется выявлять такие ситуации и своевременно на них реагировать. Для этого нужно заблокировать бюджет такого пользователя вручную или переназначить ему пароль. Выяснить дату последнего изменения аутентификационной информации можно с помощью следующей команды:

```
# for usr in $(cut -d: -f1 /etc/shadow); do [[ $(chage --list $usr | grep '^Last password change' | cut -d: -f2) > $(date) ]] && echo "$usr :$(chage --list $usr | grep '^Last password change' | cut -d: -f2)"; done
```

Вывода быть не должно.

13.1.11. Настройка разграничения доступа

13.1.11.1. Аннотация угрозы

Неверная конфигурация разграничения доступа.

Отсутствие разграничения доступа.

13.1.11.2. Описание угрозы

Правильное разграничение доступа имеет критическое значение для безопасности. Основной стратегией верного с точки зрения ИБ разграничения доступа, является предоставление минимального доступа. При необходимости доступ можно расширять в каждом нужном и аргументированном случае. Потенциальный нарушитель обязательно попытается использовать недочеты при разграничении доступа, чтобы получить доступ к данным.

13.1.11.3. Идентификаторы угрозы

По БДУ ФСТЭК России:

- УБИ.015: Угроза доступа к защищаемым файлам с использованием обходного пути;
- УБИ.028: Угроза использования альтернативных путей доступа к ресурсам;
- УБИ.074: Угроза несанкционированного доступа к аутентификационной информации;
- УБИ.168: Угроза «кражи» учетной записи доступа к сетевым сервисам;
- УБИ.215: Угроза несанкционированного доступа к системе при помощи сторонних сервисов.

Потенциальные уязвимости согласно MITRE Common Weakness Enumeration:

- CWE-266: Incorrect Privilege Assignment;
- CWE-268: Privilege Chaining;
- CWE-269: Improper Privilege Management;
- CWE-270: Privilege Context Switching Error;
- CWE-274: Improper Handling of Insufficient Privileges;
- CWE-282: Improper Ownership Management;
- CWE-284: Improper Access Control;
- CWE-286: Incorrect User Management;
- CWE-1220: Insufficient Granularity of Access Control;
- CWE-1280: Access Control Check Implemented After Asset is Accessed;
- CWE-1323: Improper Management of Sensitive Trace Data;
- CWE CATEGORY 264: Permissions, Privileges, and Access Controls.

По ИТ.ОС.А2.ПЗ:

– Угроза-2 – получение нарушителем несанкционированного доступа к информации, обрабатываемой СВТ, в период, когда пользователь ОС покинул АРМ, не завершив сеанс работы в ОС;

– Угроза среды-4 – несанкционированный доступ нарушителя к аутентификационной информации пользователей ОС.

Матрица MITRE ATT&CK:

– T1059 Command and Scripting Interpreter;

– T1059.004 Command and Scripting Interpreter: Unix Shell;

– T1078 Valid Accounts;

– T1078.001 Valid Accounts: Default Accounts;

– T1078.003 Valid Accounts: Local Accounts;

– T1204 User Execution;

– T1204.001 User Execution: Malicious Link;

– T1204.002 User Execution: Malicious File;

– T1211 Exploitation for Defense Evasion;

– T1222 File and Directory Permissions Modification;

– T1222.002 File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification;

– T1548 Abuse Elevation Control Mechanism;

– T1548.001 Abuse Elevation Control Mechanism: Setuid and Setgid;

– T1548.003 Abuse Elevation Control Mechanism: Sudo and Sudo Caching;

– T1589 Gather Victim Identity Information;

– T1592 Gather Victim Host Information;

– T1547 Boot or Logon Autostart Execution;

– T1550 Use Alternate Authentication Material;

– T1550.002 Use Alternate Authentication Material: Pass the Hash;

– T1556 Modify Authentication Process;

– T1556.003 Modify Authentication Process: Pluggable Authentication Modules;

– TA0001 Initial Access;

– TA0002 Execution;

– TA0003 Persistence.

13.1.11.4. Способ противостояния угрозе

Правильным образом сконфигурировать разграничение доступа.

MITRE ATT&CK Mitigations:

- M1017 User Training;
- M1022 Restrict File and Directory Permissions;
- M1026 Privileged Account Management;
- M1028 Operating System Configuration;
- M1047 Audit;
- M1052 User Account Control.

13.1.11.5. Проекция ИФБО к ФТБ

Настройка или использование перечисленных ИФБО способствует реализации ФТБ, мер защиты или контроля.

Проекция ИФБО к ФТБ для интерфейсов УПД приведена в таблице (Таблица 58).

Таблица 58

ИФБО	ФТБ ГОСТ 15408-2	Мера защиты 17-го приказа ФСТЭК России	Контроль ГОСТ 27002
/etc/login.defs /etc/profile /etc/bash.bashrc umask /etc/passwd /etc/pam.d/common-session	FDP_ACF.1	УПД.3	

13.1.11.6. Проверки и действия

Все действия производятся в контексте полномочий суперпользователя (root).

Необходимые действия описаны ниже.

Настройка системных пользователей

Крайне важно, чтобы всем системным пользователям (тем, которые нужны для запуска служб от их имени) была недоступна интерактивная оболочка (shell) и недоступен пароль. Для проверки той и другой настройки выполнить:

```
#awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $1!~/^\+/ && $3<'"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"' && $7!="'"$(which nologin)"'" && $7!="/bin/false") {print}' /etc/passwd
```

```
# awk -F: '($1!="root" && $1!~/^\+/ && $3<'"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' | awk '($2!="L" && $2!="LK") {print $1}'
```

Вывода быть не должно.

В том случае, если какая-то учетная запись отобразится как небезопасная (имеющая оболочку), то выполнить присвоение псевдооболочки nologin:

```
# usermod -s $(which nologin) <user>
```

А для блокировки любой требуемой учетной записи пользователя (включая системную), за исключением записи суперпользователя (root), выполнить:

```
# usermod -L <user>
```

Для установки для всех без исключения системных учетных записей, кроме суперпользователя (root) псевдооболочки nologin, выполнить:

```
#awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $1!~/^\+/ && $3<'"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"' && $7!="'"$(which nologin)"'" && $7!="/bin/false") {print $1}' /etc/passwd | while read -r user; do usermod -s "$(which nologin)" "$user"; done
```

Для установки блокировки для всех без исключения системных учетных записей, кроме суперпользователя (root), выполнить:

```
#awk -F: '($1!="root" && $1!~/^\+/ && $3<'"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' | awk '($2!="L" && $2!="LK") {print $1}' | while read -r user; do usermod -L "$user"; done
```

Для проверки того, назначена ли суперпользователю (root) основная группа с тем же идентификатором (root, 0) выполнить:

```
# grep "^root:" /etc/passwd | cut -f4 -d:
0
```

В случае, если вывод отличается, выполнить:

```
# usermod -g 0 root
```

Настройка автоматического назначения прав доступа (umask)

В процессе своей работы в системе, пользователи постоянно оперируют файлами, создают их, выполняют, удаляют, модифицируют и обмениваются ими. При создании файла или папки пользователь может, сам того не желая, ошибиться с разграничением прав доступа и скомпрометировать информацию. Для принятия мер, ограничивающих пользователей в совершении таких ошибок, требуется, чтобы ОС автоматически предусматривала невозможность доступа других пользователей к информации, созданной владельцем файла или папки. Эта настройка осуществляется с помощью интерфейса umask, который задает маску прав доступа, применяющуюся

автоматически после ее назначения. По умолчанию в большинстве версий ОС РОСА «НИКЕЛЬ» параметр mask равен 022, что недопустимо.

В защищенной системе параметр umask должен принимать значение 027, или более строгое. Это означает, что владельцу вновь создаваемого объекта (файла или папки) предоставляются полные права, основной группе предоставляются права на чтение и выполнение, а всем остальным никаких прав не предоставляется.

В данном разделе описан вариант настройки тайм-аута для оболочек, совместимых с bourne shell (sh, bash, zsh т.п.). Для оболочек синтаксиса BSD (csh, tcsh и т.п.) в данном разделе описание не предусмотрено. Для настройки оболочек синтаксиса BSD, требуется свериться с соответствующими руководствами.

Дополнительные сведения о блокировки консоли можно узнать в п.7.6.

Для проверки действия текущей политики для umask, выполнить:

```
# cat /etc/login.defs | grep UMASK | grep 027
UMASK         027
```

В том случае, если вывод отличается, то внести значение umask равное 027 в файл /etc/login.defs:

```
# echo 'UMASK 027' >> /etc/login.defs
```

Внести значение umask равное 027 в файлы /etc/profile и /etc/bash.bashrc:

```
# echo 'umask 027' >> /etc/profile
# echo 'umask 027' >> /etc/bash.bashrc
```

Новое значение umask будет применено после входа пользователя в систему.

Настройка тайм-аута времени сессии в shell

Для установки мультиплексора терминала tmux и программы блокировки vlock, выполнить (от имени суперпользователя root):

```
# rpm -ihv vlock tmux
```

Для конфигурации пользовательской сессии с учетом принудительного запуска tmux внести следующие директивы в файл /etc/bash.bashrc:

```
if
   command -v tmux &> /dev/null && [ -n "$PS1" ] && [[ ! "$TERM"
=~ screen ]] && [[ ! "$TERM" =~ tmux ]] && [ -z "$TMUX" ]; then
exec tmux
fi
```

Убрать (или закомментировать) переменную среды TMOUT из файла /etc/profile:

```
#readonly TMOUT=900 ; export TMOUT
```

Установить параметры tmux на отсчет времени истечения неактивности сессии

(рекомендуемое значение = 900 секунд, 15 минут) и принудительный запуск блокировки с помощью vlock в файле /etc/tmux.conf:

```
set -g lock-command vlock
set -g lock-after-time 900
bind L lock-session
set -g mouse on
set-option -g history-limit 30000
```

Об успешном запуске мультиплексора терминала будет свидетельствовать зеленая полоса внизу экрана. Помимо тайм-аута, можно ограничить количество строк для прокрутки в терминале (в примере – 30000). Для прокрутки настройка предусматривает использование мышки, либо Alt+b+[, после чего можно использовать стрелки вниз и вверх на клавиатуре, либо PgUp/PgDn.

Поиск файлов, доступных для записи любому пользователю

В защищенной системе в идеале не должно быть файлов, доступных для записи (значит, и для удаления) любому пользователю. Рекомендуется регулярно производить поиск таких файлов в каждой ФС и принимать необходимые меры (удалять или назначать новые права доступа) в том случае, если они будут обнаружены.

Также необходимо регулярно проверять каждую ФС на предмет появления «осиротевших» файлов, то есть тех, у кого нет корректного владельца (группы).

Появление файлов с полными правами доступа или не имеющих владельца (группы), помимо появления угроз безопасности, может быть признаком подозрительной активности.

В целом, при корректно и в полном объеме настроенном ПО КЦ AIDE (см. подраздел 13.1.6), данные рекомендации можно не применять.

Для поиска объектов, доступных для записи любому пользователю, выполнить (для каждой ФС):

```
# find <точка монтирования ФС> -xdev -type f -perm -0002
```

Для поиска «осиротевших» объектов выполнить:

```
# find <точка монтирования ФС> -xdev -nouser
# find <точка монтирования ФС> -xdev -nogroup
```

Убедиться, что вывод отсутствует.

Рекомендации по настройке переменных ядра ОС

Ядро ОС РОСА «НИКЕЛЬ» может принимать значительное количеств переменных (опций) настройки. Часть переменных уже рассматривались в настоящем руководстве. Остальная часть описана в данном разделе. Для удобства использования все они

сведены в таблицу с рекомендуемыми значениями и со ссылками, указывающими на описание их применения.

dev.tty.ldisc_autoload – переменная ядра ОС, отвечающая за автоматическое определение и назначение параметров терминала. Значение «0» запрещает автоматическое назначение параметров дисциплины линии (line discipline, ldisk). Потенциальный нарушитель может попытаться подключить к ОС внешнее устройство, такое как USB-COM переходник, эмулятор COM порта, и т.п., например, чтобы попробовать организовать скрытый канал передачи данных, провести атаку на ОС, получить отладочную информацию или каким-то иным образом воздействовать на нее. В защищенной системе при подключении таких устройств, ОС не должна автоматически определять их характеристики и назначать параметры протокола обмена данными. Для проверки текущего значения этой переменной выполнить:

```
# sysctl -a | grep tty | grep autoload
dev.tty.ldisc_autoload = 0
```

Если вывод отличается – выполнить соответствующую настройку:

```
# sysctl -w dev.tty.ldisc_autoload=0
# echo 'dev.tty.ldisc_autoload = 0' >> /etc/sysctl.conf
```

fs.protected_fifos – переменная ядра ОС, отвечающая за создание специальных файлов-сокетов FIFO в общедоступных каталогах. Потенциальный нарушитель может попытаться несанкционированно создать сокет в общедоступном каталоге, например, с целью создания попытки организации связи с оборудованиям или воздействия на механизмы обработки взаимодействия между процессами в системе. Рекомендуемое значение этой переменной «1», которое сигнализирует ядру о том, что ядру нельзя выполнять системный вызов open() или creat() с флагом O_CREAT (и, следовательно, нельзя создать файл) в общедоступном каталоге любому пользователю, за исключением владельца каталога. Значение «2» учитывает также группу. Значение «0» разрешает создавать сокеты без ограничений.

Для проверки текущего значения этой переменной выполнить:

```
# sysctl -a | grep fs.protected_fifos
fs.protected_fifos = 1
```

Если вывод отличается – выполнить соответствующую настройку:

```
# sysctl -w fs.protected_fifos=1
# echo 'fs.protected_fifos = 1' >> /etc/sysctl.conf
```

kernel.ctrl-alt-del – переменная ядра ОС, отвечающая за порядок обработки аппаратного прерывания, создающегося в результате нажатия кнопок «Alt+Crtl+Del». Может принимать значение «0» и «1». Если установлена в «0», то ядро производит перехват события, но не производит обработку прерывания. Вместо этого параметр «0» сигнализирует ядру, чтобы обработку события нажатия «Alt+Ctrl+Del» произвела служба инициализации (systemd, init, upstart и т.п.) в соответствии с ее настройками. Если задано значение «1», то ядро будет осуществлять немедленную и безусловную перезагрузку. Даже без синхронизации кеша буферов. В защищенной системе рекомендуется использовать значение «0» для этой переменной.

Для проверки текущего значения этой переменной выполнить:

```
# sysctl -a | grep alt
kernel.ctrl-alt-del = 0
```

Если вывод отличается – выполнить соответствующую настройку:

```
# sysctl -w kernel.ctrl-alt-del=0
# echo 'kernel.ctrl-alt-del = 0' >> /etc/sysctl.conf
```

kernel.dmesg_restrict – переменная ядра ОС, отвечающая за разграничение доступа к интерфейсу кольцевого буфера аудита ядра (файлу /dev/kmsg) для обычных пользователей (кроме root). В стандартной системе Linux, доступ пользователей к этому интерфейсу не запрещен. Соответственно любой пользователь ОС РОСА «НИКЕЛЬ» сможет или напрямую обратиться к этому файлу (cat /dev/kmsg), или использовать программы чтения аудита кольцевого буфера ядра, такие как dmesg или syslog. В защищенной системе требуется ограничивать пользователей в возможности получать сообщения аудита ядра. Рекомендуемое значение переменной «1», если установлено значение «0», то доступ пользователей к буферу аудита ядра не ограничивается.

Для проверки текущего значения этой переменной выполнить:

```
# sysctl -a | grep dmesg
kernel.dmesg_restrict = 1
```

Если вывод отличается – выполнить соответствующую настройку:

```
# sysctl -w kernel.dmesg_restrict=1
# echo 'kernel.dmesg_restrict = 1' >> /etc/sysctl.conf
```

kernel.kptr_restrict – переменная ядра ОС, отвечающая за разграничение доступа к интерфейсу ядра /proc/kallsyms и просмотру значений адресов в памяти для некоторых функций ядра. Может принимать значения «0», «1» и «2». Если определено значение «0», то просматривать значения адресов в памяти может любой пользователь ОС. Если

задано значение «1», то просматривать адресацию функций может только root. Если значение «2», то никто, кроме ядра не получит информацию об адресации функций. В защищенной системе рекомендуемое значение «2». При значении «1», адреса памяти заменяются на нули для всех пользователей, кроме root. При значении «2», адреса памяти заменяются на нули для всех пользователей, включая root.

Для проверки текущего значения этой переменной выполнить:

```
# sysctl -a | grep kptr
kernel.kptr_restrict = 2
```

Если вывод отличается – выполнить соответствующую настройку:

```
# sysctl -w kernel.kptr_restrict=2
# echo 'kernel.kptr_restrict = 2' >> /etc/sysctl.conf
```

kernel.modules_disabled – переменная ядра ОС, отвечающая за загрузку/выгрузку модулей ядра. Значение «0», означает, что модуль может быть загружен или выгружен. Значение «1» означает, что загрузка и выгрузка модулей невозможна. В защищенной системе должен быть четко определен состав технических и ПС. Следовательно, модули ядра, их количество и параметры загрузки также должны быть четко определены. Однако, требуется учитывать, что иногда загрузка модулей должна быть разрешена (например, при использовании ноутбуков или специфической периферии). В общем случае, рекомендуемое значение этой переменной: «1».

Для проверки текущего значения этой переменной выполнить:

```
# sysctl -a | grep modules
kernel.modules_disabled = 1
```

Если вывод отличается – выполнить соответствующую настройку:

```
# sysctl -w kernel.modules_disabled=1
# echo 'kernel.modules_disabled = 1' >> /etc/sysctl.conf
```

kernel.perf_event_paranoid – переменная ядра ОС, которая отвечает за возможности профилирования ядра и получения информации о производительности. Эта переменная может принимать значения «-1», «0», «1» и «2» и более. При этом, «-1» означает, что пользователь полномочен получать прямые необработанные данные трассировки ядра ОС. Значение «0» означает, что пользователь может получать трассировку о событиях процессора. Значение «1» означает, что пользователь может получать данные профилирования ядра (получать данные порядка обработки команд). Значение «2» препятствует получению данных профилировки ядра. В защищенной системе рекомендуется использовать значение «2» или выше для этой переменной.

Для проверки текущего значения этой переменной выполнить:

```
# sysctl -a | grep kernel.perf_event_paranoid
kernel.perf_event_paranoid = 2
```

Если вывод отличается – выполнить соответствующую настройку:

```
# sysctl -w kernel.perf_event_paranoid=2
# echo 'kernel.perf_event_paranoid = 2' >> /etc/sysctl.conf
```

kernel.unprivileged_bpf_disabled – переменная ядра ОС, которая разрешает непривелегированный доступ к подсистеме ядра BPF (Berkley Packet Filter). Может принимать значение «0» и «1». В значении «0» доступ предоставляется любому пользователю. В значении «1» доступ предоставляется только суперпользователю. В защищенной системе требуется устанавливать в значение «1».

Для проверки текущего значения этой переменной выполнить:

```
# sysctl -a | grep kernel.unprivileged_bpf_disabled
kernel.unprivileged_bpf_disabled = 1
```

Если вывод отличается – выполнить соответствующую настройку:

```
# sysctl -w kernel.unprivileged_bpf_disabled=1
# echo 'kernel.unprivileged_bpf_disabled = 1' >> /etc/sysctl.conf
```

net.core.bpf_jit_harden – переменная ядра ОС, регламентирующая доступ к JIT компилятору фильтра BPF. Значение «0» не препятствует доступу, значение «1» предоставлять доступ только суперпользователю, значение «2» никому не предоставлять доступ. В защищенной системе рекомендуется использовать значение «1» или более строгое.

Для проверки текущего значения этой переменной выполнить:

```
# sysctl -a | grep net.core.bpf_jit_harden
net.core.bpf_jit_harden = 2
```

Если вывод отличается – выполнить соответствующую настройку:

```
# sysctl -w net.core.bpf_jit_harden=2
# echo 'net.core.bpf_jit_harden = 2' >> /etc/sysctl.conf
```

13.1.11.7. **Контроль устройств USB**

Для контроля устройств USB в ОС РОСА «НИКЕЛЬ» можно рекомендовать использование ПС usbguard. Данное ПО взаимодействует с менеджером устройств ОС (device manager) через пространство служебной ФС ядра devfs, и является, по сути, высокоуровневым логическим интересом к функциям менеджера устройств ядра в части

обмена данными с устройствами USB. ПС usbguard позволяет назначать политики доступа ко всему спектру устройств USB, определяя политики по умолчанию для доверенных устройств. При установке usbguard все устройства USB, определенные программой в момент ее установки, автоматически добавляются в политику. Далее, после установки и автоматической настройки, программа usbguard функционирует в качестве службы. Основной конфигурационный файл службы — это /etc/usbguard/usbguard-daemon.conf. Основной файл, содержащий перечень устройств и политику — это /etc/usbguard/rules.conf. Файл аудита программы — это /var/log/usbguard/usbguard-audit.log.

Для запуска программы контроля USB устройств , выполнить (от имени суперпользователя root):

```
# systemctl start usbguard
# systemctl enable usbguard
```

Служба запустится автоматически, самостоятельно сформировав нужные конфигурационные файлы /etc/usbguard/usbguard-daemon.conf и /etc/usbguard/rules.conf. При этом, в конфигурационный файл политики автоматически будут занесены все обнаруженные на момент установки USB устройства и они в дальнейшем будут считаться доверенными. Для того, чтобы переделать политику целиком, в случае необходимости, требуется выполнить (от имени суперпользователя root):

```
# usbguard generate-policy > /etc/usbguard/rules.conf
```

В том случае, если необходимо разово разрешить подключение какого-то устройства USB, например, накопителя данных, требуется (от имени суперпользователя root) выполнить поиск устройства:

```
# usbguard list-devices
...
33: block id 01e9:63f0 serial "1234567XXX8" name "Portable SSD T5" hash "kKaIs6W/ZI3OnNWaCBHgmXh1234567/lfyBVVfy494YQ=" parent-hash "x9ceLltloDm7ceQyad6543210YVSX1Twdj/bnTelsH2c=" via-port "4-1.4" with-interface { 08:07:05 08:07:05 } with-connect-type "unknown"
```

В ответ система сообщит пронумерованные текущие идентификаторы устройств. Пример выше демонстрирует подключение SSD диска Samsung T5 на 512 Гбайт, к тому же содержащий зашифрованный раздел с ФС для резервного копирования. Как видно из примера, система присвоила этому диску номер 33.

Для разового разрешения подключения данного устройства, требуется выполнить (от имени суперпользователя root) следующую команду:

```
# usbguard allow-device 33
```

После чего система предложит смонтировать (подключить) диск. В том случае, если данные на нем зашифрованы с помощью LUKS, то ввести пароль расшифровки. Смонтированный в системе диск далее отображается штатным образом:

```
/dev/mapper/luks-d0c22f on /media/xxx/LUKSDEVICE type ext4 (rw,nosuid,nodev,relatime,stripe=8191,uhelper=udisks2)
```

14. ОБЕСПЕЧЕНИЕ НАДЕЖНОГО ФУНКЦИОНИРОВАНИЯ

14.1. Настройка даты и времени

Процесс настройки даты и времени в графическом и консольных режимах подробно описан выше в разделе 3.3.3.Настройка даты и времени.

14.2. Ограничение ресурсов для пользователя

14.2.1. Ограничение оперативной памяти

Для ограничения оперативной памяти, выделяемой пользователям, используется механизм ограничения pam_limits, описание приводится разделе 5.3.3.Ограничение числа параллельных сеансов пользователей и других ресурсов.

14.2.2. Ограничение дискового пространства для пользователей

Для ограничения дискового пространства пользователей используется комплекс программ quota. Для выделения дискового пространства (квот) пользователям необходимо включить поддержку квот в ФС. Для этого нужно отредактировать файл /etc/fstab: добавить опцию usrquota и/или grpquota при монтировании ФС, в которых требуется включить поддержку квот. Параметр usrquota обозначит поддержку квот для пользователей, а grpquota – для групп. Формат файла /etc/fstab:

```
<file system>    <dir>   <type>  <options> <dump>  <pass>
```

Описание полей файла /etc/fstab приведено в Таблица 59. Более подробное описание полей приведено в man fstab.

Таблица 59

Опция	**Описание**
<file system>	ФС (имя файла устройства, идентификатор устройства UUID или метка тома LABEL)
<dir>	Точка монтирования системы
<type>	Тип ФС (ext3, ext4, btrfs, xfs и др.)
<options>	Опции монтирования: - defaults (rw, suid, dev, exec, auto, nouser and async); - auto – монтирование ФС при загрузке происходит автоматически или после выполнения команды 'mount -a'; - noauto – монтирование ФС разрешено только вручную; - async - все операции ввода-вывода должны выполняться асинхронно; - exec – разрешено исполнение бинарных файлов; - noexec – запрещено исполнение бинарных файлов; - user – монтирование ФС разрешено любому пользователю

Опция	Описание
	(применяются опции noexec, nosuid, nodev, если они не переопределены); - nouser – монтирование ФС разрешено только суперпользователю (используется по умолчанию); - suid - операции с suid и sgid битами разрешены; - nosuid – операции с suid и sgid битами запрещены; - usrquota – поддержка квот для пользователей; - grpquota – поддержка квот для групп и др.
<dump>	Флаг резервного копирования (0 – выполнять, 1 – не выполнять)
<pass>	Порядок проверки ФС (0 – нет проверки, 1 – высокий приоритет, 2 – низкий приоритет

После редактирования файла /etc/fstab нужно перезагрузить систему или перемонтировать ФС, записи которых были изменены, выполнив команду:

```
# mount -o remount <file system>
```

В качестве аргумента <file system> указывается ФС, запись которой была изменена, или точка монтирования ФС.

После того, как все ФС, в которых включены поддержки квот, перемонтированы, система может работать с дисковыми квотами. Следующим действием должен быть запуск утилиты `quotacheck`. Утилита `quotacheck` предназначена для проверки ФС, в которых включена поддержка квот, и обновления таблицы текущего использования диска в ФС. Затем эта таблица используется для обновления системной копии данных об использовании диска.

В Таблица 60 часто используемые опции утилиты `quotacheck`. Подробное описание приведено в man `quotacheck`.

Синтаксис:

```
quotacheck <опции> <файловая система>
```

Таблица 60

Опция	Описание
-c, --create-files	Создание файлов квот
-a, --all	Проверка всех локально смонтированных ФС, в которых включена поддержка квот
-u, --user	Поддержка дисковых квот пользователей
-g, --group	Поддержка дисковых квот групп
-v, --verbose	Вывод подробной информации о процессе проверки квот

Чтобы создать в ФС файлы квот и проверить их, выполнить команды:

```
# quotacheck -cug <file system>
# quotacheck -avug
```

Утилита edquota предназначена для выделения дисковых квот. В Таблица 61 приведены часто используемые опции утилиты edquota. Подробное описание приведено в man edquota.

Синтаксис:

```
edquota <опции>
```

Таблица 61

Опция	Описание
-u, --user	Поддержка дисковых квот пользователей
-g, --group	Поддержка дисковых квот групп
-t, --edit-period	Редактирование периода отсрочки
-T, --edit-times	Редактирование периода отсрочки для пользователя/группы

Чтобы настроить квоты для пользователя user, выполнить команду:

```
# edquota -u user
```

Команда выводит квоту пользователя и предоставляет возможность отредактировать выделенные квоты в текстовом редакторе:

```
Disk quotas for user user (uid 1000):
Filesystem   blocks   soft   hard  inodes  soft  hard
 /dev/sdb    29824     0    2000      1     0     0
```

В первом столбце указывается название ФС, для которой включена поддержка квот. Во втором столбце указано, сколько блоков использует пользователь в данный момент, в следующих двух столбцах – мягкое и жесткое ограничение на число блоков для пользователя в данной ФС. В столбце inodes указано, сколько дескрипторов inodes использует пользователь, в следующих двух столбцах – мягкое и жесткое ограничение на число inode для пользователя в данной ФС.

Жесткий предел определяет абсолютный максимальный объем дискового пространства, которое может быть выделено пользователю. Если этот предел достигнут, получить дополнительное дисковое пространство невозможно. Мягкий предел определяет также максимальный объем дискового пространства. Однако, в отличие от жесткого предела, мягкий предел может быть превышен в течение некоторого времени. Это время называется периодом отсрочки. Период отсрочки можно задавать в секундах, минутах, часах, днях, неделях или месяцах. Если одно из этих значений равно 0, предел не устанавливается.

Утилита quota предназначена для просмотра квот. В Таблица 62 приведены часто используемые опции утилиты quota. Подробное описание приведено в man quota.

Синтаксис:

```
quota <опции>
```

Таблица 62 – Опции утилиты quota

Опция	Описание
-u, --user	Дисковые квоты пользователя
-g, --group	Дисковые квоты группы

Чтобы проверить, установились ли квоты для пользователя, выполнить команду:

```
quota -u user
```

Утилиты quotaon и quotaoff предназначены для включения и отключения поддержки квот. В таблицах Таблица 63 и Таблица 64 приведены часто используемые опции утилит quotaoff и quotaon соответственно. Подробные описания приведены в man quotaon и man quotaoff.

Таблица 63 – Опции утилиты quotaoff

Опция	Описание
-u, --user	Дисковые квоты пользователя
-g, --group	Дисковые квоты группы
-a, --all	Включение дисковых квот на всех ФС

Таблица 64 – Опции утилиты quotaon

Опция	Описание
-u, --user	Дисковые квоты пользователя
-g, --group	Дисковые квоты группы
-a, --all	Отключение дисковых квот на всех ФС

Описанный алгоритм применяется для выделения квот на ФС типа ext3 и ext4. Для выделения квот на ФС типа xfs нужно проделать действия, описанные выше, за исключением действий с утилитами quotacheck, quotaon и quotaoff.

14.3. Создание и восстановление резервных копий

Для работы с резервными копиями используются утилиты tar, rsync и система bacula.

14.3.1. Утилита tar

Утилита tar предназначена для создания резервных копий и архивирования ФС. Утилита позволяет сохранять файлы на архивном носителе и восстанавливать их с этого носителя. В Таблица 65 приведены часто используемые опции утилиты tar. Подробное

описание приведено в man tar.

Синтаксис:

```
tar <опции> <файл>
```

Таблица 65 – Опции утилиты tar

Опция	Описание
-c, --create	Создание архив
-x, --extract, --get	Извлечение файлов из архива на устройстве, заданном по умолчанию, или определенном опцией f
-f, --file=NAME	Создание (или чтение) архива с NAME, где NAME – имя файла или устройства
-Z, --compress, --uncompress	Сжатие или распаковка архива с помощью compress
-z, --gzip	Сжатие или распаковка архива с помощью gzip
-M, --multi-volume	Создание многотомный архив
-t, --list	Вывод списка сохраненных в архиве файлов
-v, --verbose	Вывод подробной информации о процессе
--acls	Сохранение (восстановление) списков контроля доступа ACL каталогов и файлов, вложенных в архив
--exclude=PATTERN	Исключение из обработки файла PATTERN

Примеры использования:

Для создания архива /backup/backup.tar всей системы за исключением директорий /proc, /mnt, /backup, /sys, /dev, /run, /temp с сохранением списков контроля доступа ACL файлов и каталогов можно использовать команду (предварительно создав папку командой `mkdir backup`):

```
# tar -cvf /backup/backup.tar / --exclude=proc --exclude=mnt --exclude=backup --exclude=sys --exclude=dev --exclude=run --exclude=tmp
```

Для извлечения файлов из архива с сохранением списков контроля доступа ACL файлов и каталогов можно использовать команду:

```
# tar -xv -f /backup/backup.tar --acls
```

14.3.2. Утилита rsync

rsync (remote synchronization) — утилита, которая эффективно выполняет синхронизацию файлов и каталогов в двух местах (необязательно локальных) с минимизированием трафика, используя кодирование данных при необходимости. Важным отличием rsync от многих других программ/ протоколов является то, что зеркалирование осуществляется одним потоком в каждом направлении (а не по одному

или несколько потоков на каждый файл). rsync может копировать или отображать содержимое каталога и копировать файлы, опционально используя сжатие и рекурсию. rsync передает только изменения файлов, что отражается на производительности программы.

Подробное описание работы утилиты, использование опций и команд можно найти в man rsync.

14.3.3. Bacula

Bacula – это система резервного копирования корпоративного уровня, предустановленная в дистрибутиве ОС РОСА «НИКЕЛЬ» и требует дальнейшей настройки администратором. Она имеет клиент-серверную архитектуру и состоит из следующих компонентов:

- Bacula Director (сервис bacula-dir) - основной сервис, который управляет всеми другими процессами по резервному копированию и восстановлению;
- Bacula Storage (сервис bacula-sd) - хранилище, предназначенное для сохранения резервных копий на диске;
- Bacula File Daemon (сервис bacula-fd) - клиентская часть сервиса, которая нужна для доступа к файлам на сервере, с которого будет выполнятся резервное копирование.

Все компоненты могут быть установлены как на одном сервере, так и на разных, но каждый из них должен иметь возможность обратится к другому по сети. Для управления утилитой используется утилита командной строки bconsole.

Работа системы связана с использованием базы данных, для этих целей в ОС РОСА «НИКЕЛЬ» имеется предустановленная СУБД PostgreSQL.

Настройка ФС

Необходимо создать несколько каталогов, которые будут использоваться в качестве точек резервного копирования и восстановления (для примера они будут называться backup и restore).

Запущенная с флагом –p команда mkdir создаст целевой каталог, а также все необходимые родительские каталоги:

```
sudo mkdir -p ./bacula/{backup,restore}
```

Далее необходимо изменить права на каталог, чтобы доступ к ним был только у утилиты bacula:

```
sudo chown -R bacula:bacula /bacula
sudo chmod 700 -R /bacula
```

Настройка Bacula

Bacula состоит из нескольких компонентов, которые требуют индивидуальной настройки. Все необходимые конфигурационные файлы находятся в каталоге /etc/bacula/.

Настройка bacula-dir.conf

Для начала отредактируйте файл bacula-dir.conf:

```
sudo nano /etc/bacula/bacula-dir.conf
```

Чтобы выполнить резервное копирование, запланированное в данном руководстве, нужно отредактировать несколько разделов файла.

Для начала найдите раздел `Standard Restore template`. В настройках `Job` нужно найти параметр `Where` и указать в нем созданную ранее точку восстановления.

```
Job {
Name = "RestoreFiles"
Type = Restore
Client=Blank-fd
FileSet="Full Set"
Storage = File
Pool = Default
Messages = Standard
Where = /bacula/restore
}
```

Затем найдите раздел `List of files to be backed up`. В настройки `FileSet` нужно внести опцию для поддержки утилиты gzip, которая будет сжимать файлы.

После этого в параметре `File =` укажите все файлы, которые нужно скопировать. Данный раздел может содержать несколько объявлений `File =`, каждый со своим путем.

В данном руководстве показано, как создать резервную копию всей системы root (/). Измените параметры следующим образом:

```
Include {
Options {
signature = MD5
compression = GZIP
}
#
# Put your list of files here, preceded by 'File =', one per line
# or include an external list with:
```

```
#
#                          File                =                file-name
#
#   Note:   /   backs   up   everything   on   the   root   partition.
#     if   you   have   other   partitions   such   as   /usr   or   /home
#        you    will    probably    want    to    add    them    too.
#
#  By  default  this  is  defined  to  point  to  the  Bacula  binary
#     directory   to   give   a   reasonable   FileSet   to   backup   to
#             disk      storage      during      initial      testing.
#
File                                                                = /
}
```

В завершение добавьте пути к файлам, которые должны быть исключены из резервной копии. Для этого необходимо отредактировать раздел `Exclude`, использующий все тот же синтаксис `File =`.

Стандартные настройки утилиты необходимо отредактировать, указав только путь к архиву; не стоит создавать копию резервной папки. Отредактируйте второй по счету параметр `File =`, указав путь к root-файлу bacula:

```
Exclude {
File = /var/lib/bacula
File = /bacula
File = /proc
File = /tmp
File = /.journal
File = /.fsck
}
```

Далее сохраните и закройте файл.

Настройка bacula-sd.conf

Конфигурация хранилища находится в файле /etc/bacula/bacula-sd.conf. Он определяет место хранения резервных копий. В конфигурационном файле есть несколько секций:

- Storage - секция, с основными настройками хранилища, здесь настраивается имя хранилища, а также IP адрес на котором оно будет доступно, для локальной сети пока достаточно 127.0.0.1.
- Director - настраивается авторизация для управляющего сервиса, где надо прописать имя сервиса, который может подключится и пароль, который он

должен использовать.

- Device - здесь настраивается способ хранения файлов на физическом диске и путь к папке, где они будут хранится.
- Messages - отправка сообщений, данный раздел можно оставить без редактирования, со стандартными настройками.

Каждая секция имеет такой синтаксис:

```
имя_секции {
параметр = значение
}
```

Далее переходим к редактированию файла bacula-sd.conf.

Откройте bacula-sd.conf с правами sudo:

```
sudo nano /etc/bacula/bacula-sd.conf
```

В разделе `Devices supported by this Storage daemon` найдите настройку `Device` и измените ее значение (Archive Device), указав путь к созданному ранее каталогу для копий:

```
Device {
Name = FileStorage
Media Type = File
Archive Device = /bacula/backup
LabelMedia = yes;           # lets Bacula label unlabeled media
Random Access = Yes;
AutomaticMount = yes;         # when device opened, read it
RemovableMedia = no;
AlwaysOpen = no;
}
```

Сохраните и закройте файл.

Проверка синтаксиса настроек

Прежде чем продолжить, убедитесь, что bacula распознает все настройки. Используйте внутренние команды тестирования bacula, чтобы убедиться, что синтаксис отредактированных файлов не содержит ошибок.

Для начала проверьте конфигурации bacula-dir:

```
sudo bacula-dir -tc /etc/bacula/bacula-dir.conf
```

Если команда не возвращает никакого результата, значит, конфигурационный файл не содержит ошибок.

Далее проверьте команду bacula-sd:

```
sudo bacula-sd -tc /etc/bacula/bacula-sd.conf
```

Опять же, отсутствие вывода команды означает, что конфигурационный файл действителен.

Далее необходимо перезапустить сервис bacula, чтобы активировать обновления.

```
sudo service bacula-sd restart
sudo service bacula-director restart
```

После выполнения перезагрузки все готово к созданию резервной копии.

Создание резервной копии системы

С сервисом bacula можно взаимодействовать при помощи консоли. Чтобы получить доступ к консоли bacula, запустите команду bconsole:

```
sudo bconsole
```

Эта команда откроет консоль bacula, командная строка которой начинается с (*). Сначала выполните команду `label`. Она запросит указать имя архива, который нужно создать.

```
label
Automatically selected Catalog: MyCatalog
Using Catalog "MyCatalog"
Automatically selected Storage: File
Enter new Volume name: MyArchiveName
```

Выберите pool как тип хранилища. Поскольку резервная копия будет храниться в виде файла, выберите №2:

```
2: File
```

Теперь Bacula имеет все инструкции о том, как нужно записать данные для резервной копии. Запустите тестовое резервное копирование, чтобы убедиться, что все работает должным образом:

```
run
A job name must be specified.
The defined Job resources are:
1: BackupClient1
2: BackupCatalog
3: RestoreFiles
Select Job resource (1-3):
```

Выберите 1, чтобы запустить предварительно настроенный процесс резервного копирования:

```
1: BackupClient1
```

Подтвердите запуск:

```
yes
```

Bacula сообщит, что вы получили несколько сообщений; это вывод, сгенерированный резервной копией. Проверьте сообщения на наличие ошибок, набрав:

```
messages
```

На экране появится несколько строк вывода. Повторяйте проверку до тех пор, пока на экране не появится резюме результатов выполнения резервного копирования:

```
Termination: Backup OK
```

Затем выполните контрольную проверку.

Восстановление копии

После создания резервной копии важно убедиться, что ее можно восстановить. В

консоли bacula введите:

```
restore all
```

Появится меню, содержащее широкий ряд опций. Чтобы восстановить последнюю резервную копию, выберите 5:

```
5: Select the most recent backup for a client
```

Это откроет дерево виртуальных файлов со структурой скопированных каталогов. Интерфейс позволяет легко добавлять и исключать файлы для восстановления при помощи простых команд.

Поскольку была выбрана опция restore all, каждый скопированный ранее файл будет восстановлен.

Чтобы выполнить тонкую настройку восстановления, просмотрите список файлов при помощи команды `ls` и `cd`, выберите файлы для восстановления при помощи команды mark и исключите ненужные файлы при помощи unmark. Чтобы получить полный список команд, запустите через консоль:

```
Help
```

Завершив, выйдите из режима выбора файлов с помощью команды:

```
done
```

Подтвердите восстановление копии:

```
yes
```

Проверьте сообщения об ошибках:

```
messages
```

Резюме восстановления должно иметь такой вид:

```
Termination: Restore OK
```

Завершив, ведите exit, чтобы закрыть консоль bacula.

```
exit
```

14.3.3.1. **Проверка ФС**

Чтобы убедиться, что резервное копирование прошло успешно, просмотрите содержимое резервного каталога. Для этого понадобятся привилегии sudo, поскольку права на структуру каталогов принадлежат пользователю bacula:

```
sudo ls /bacula/backup
```

На экране появится файл с именем, установленным ранее для архива.

Теперь проверьте точку восстановления. Чтобы просмотреть ее содержимое:

```
sudo ls /bacula/restore
```

Вы увидите зеркало файловой структуры root, за исключением файлов и каталогов, внесенных в раздел `Exclude` файла bacula-dir.conf.

14.4. Ручное восстановление системы

Эксплуатация ОС пользователем осуществляется в консольном и графическом режимах. Аварийным режим предназначен для восстановления системы после сбоев или ошибок, возникших в процессе эксплуатации.

Запуск в аварийном режиме осуществляется автоматически при невозможности системы загрузиться в консольном или графическом режимах. Если система не может самостоятельно загрузиться в аварийном режиме, необходимо выполнить следующие действия:

1) перезагрузить систему принудительно;

2) при выборе ядра загрузки указать нужный вариант и нажать на клавишу <e>;

3) ввести логин и пароль для входа в загрузчик;

4) выбрать строку, начинающуюся со слова «linux» и добавить в конец строчки слово «single»;

5) нажать комбинацию клавиш <Ctrl+X> для сохранения и загрузки в аварийный режим.

14.5. Отказоустойчивый кластер

Для создания кластера на уровне приложений с высокой отказоустойчивостью используется решение с использованием программ Corosync и Pacemaker.

Corosync — программный продукт, который позволяет создавать единый кластер из нескольких аппаратных или виртуальных серверов. Corosync отслеживает и передает состояние всех участников (нод) в кластере.

Это ПО позволяет:

- мониторить статус приложений;
- оповещать приложения о смене активной ноды в кластере;
- отправлять идентичные сообщения процессам на всех нодах;
- предоставлять доступ к общей базе данных с конфигурацией и статистикой;
- отправлять уведомления об изменениях, произведенных в базе.

Pacemaker — менеджер ресурсов кластера. Он позволяет использовать службы и объекты в рамках одного кластера из двух или более нод. Данное ПО предоставляет следующие возможности:

- позволяет находить и устранять сбои на уровне нод и служб;
- не зависит от подсистемы хранения;

- не зависит от типов ресурсов: все, что можно прописать в скрипты, можно кластеризовать;
- поддерживает STONITH (Shoot-The-Other-Node-In-The-Head), то есть поврежденная нода изолируется и запросы к ней не поступают, пока нода не отправит сообщение о том, что она снова в рабочем состоянии;
- поддерживает кворумные и ресурсозависимые кластеры любого размера;
- поддерживает практически любую избыточную конфигурацию;
- может автоматически реплицировать файл config на все узлы кластера;
- можно задать порядок запуска ресурсов, а также их совместимость на одном узле;
- поддерживает расширенные типы ресурсов: клоны (когда ресурс запущен на множестве узлов) и дополнительные состояния (master/slave и подобное) — актуально для СУБД (MySQL, MariaDB, PostgreSQL, Oracle);
- имеет единую кластерную оболочку CRM с поддержкой скриптов.

Общие сведения об отказоустойчивом кластере

В информационной сети кластер представлен тремя IP адресами:

- IP адрес управляющего интерфейса резервируемого сервера - используется для управления MASTER сервером в аварийном режиме работы кластера;
- IP адрес управляющего интерфейса резервирующего сервера - используется для управления SLAVE сервером в штатном режиме работы кластера;
- Виртуальный IP адрес кластера - используется всем клиентское оборудование (IP телефоны) для работы с системой вне зависимости от режима работы кластера. Данный адрес мигрирует в автоматическом режиме с одной системы на другую в зависимости от режима работы кластера.

Каждый сервер (MASTER и SLAVE) должен иметь свое уникальное имя в сети. Это имя определяется командой `hostname` в терминале ОС. На каждом сервере в файле /etc/hosts должна присутствовать одна и та же пара строк, каждая их которых содержит IP адрес сервера в кластере и его сетевое имя. Например, если сервер MASTER имеет в сети имя 'node-a' с управляющим интерфейсом '192.168.1.101', а SLAVE сервер имеет в сети имя 'node-b' с управляющим интерфейсом '192.168.1.102', то как на MASTER, так и на SLAVE сервере в файле /etc/hosts должны присутствовать следующие записи:

```
192.168.1.101 node-a
192.168.1.102 node-b
```

Для синхронизации работы кластера в сети, на узлах должен быть разрешен прием трафика, направляемый по multicast адресам. Ядро кластера будет рассылать пакеты в рамках multicast "сети" по порту 5405. Таким образом, необходимо заранее разрешить прием трафика по указанному порту, а также порту меньшем на единицу; а также разрешить обмен трафиком по протоколу IGMP:

```
service fail2ban stop
iptables -I INPUT -p igmp -j ACCEPT
iptables -I INPUT -m addrtype --dst-type MULTICAST -j ACCEPT
iptables -I INPUT -p udp -m multiport --dports 5404,5405 -j ACCEPT
service iptables save
service fail2ban start
```

Установка и настройка ядра кластеризации

Необходимо задать переменные окружения, которые будут использоваться при дальнейшей настройке. Обратите внимание, что переменные будут использоваться только при настройке, в работе самого сервиса кластеризации используются значения заданных переменных:

```
export ais_port=5405
export ais_mcast=226.94.1.1
```

Далее необходимо задать адрес сети, в которой будет работать `corosync`. Это должен быть адрес сетевого интерфейса, который соединяет два сервера напрямую. Последние 8 цифр адреса должны отличаться. Получить адрес можно используя следующую команду (строка универсальна как для master, так и для slave сервера):

```
ip addr | grep "inet " | tail -n 1 | awk '{print $4}' | sed s/255/0/
```

Если в результате выполнения команды был отображен адрес сети, которая установлена между серверами напрямую, то вышеуказанную команду можно использовать для установки переменной:

```
export ais_addr=`ip addr | grep "inet " | tail -n 1 | awk '{print $4}' | sed s/255/0/`
```

Отобразить полученные значения переменных можно выполнив следующую команду:

```
env | grep ais
```

Необходимо проверить полученный адрес сети ais_addr с реальный требуемым,

так как в некоторых случая команда получения адреса сети возвращает не верный результат (например, для сети /22). Проверить адрес сети можно любым сетевым калькулятором, например тут: http://ip-calculator.ru/ Если адрес сети будет указан не верно, узлы не найдут друг друга в составе кластера.

Далее необходимо создать файл конфигурации Corosync:

```
cat <<EOF >/etc/corosync/corosync.conf
compatibility: whitetank

totem {
version: 2
secauth: off
threads: 0
interface {
ringnumber: 0
bindnetaddr: $ais_addr
mcastaddr: $ais_mcast
mcastport: $ais_port
ttl: 1
}
}

logging {
fileline: off
to_stderr: no
to_logfile: yes
logfile: /var/log/cluster/corosync.log
to_syslog: yes
debug: off
timestamp: on
logger_subsys {
subsys: AMF
debug: off
}
}
EOF
```

Также необходимо разрешить сервису corosync работать с правами root. Для этого необходимо добавить в конфигурационный файл соответствующие строки, выполнив следующую команду:

```
cat <<END >>/etc/corosync/corosync.conf
aisexec {
user: root
group: root
}
END
```

Также необходимо указать, что `corosync` должен работать с Pacemaker-ом, но не должен его запускать самостоятельно. Если файл /etc/corosync/service.d/pacemaker существует, то нужно убедиться, что в нем значение параметра `ver: 1`.

Если файл /etc/corosync/service.d/pacemaker отсутствует, то в конфигурационный файл /etc/corosync/corosync.conf, добавлением соответствующие параметры:

```
cat <<END >>/etc/corosync/corosync.conf
service {
# Load the Pacemaker Cluster Resource Manager
name: pacemaker
ver: 1
use_mgmtd: no
use_logd: no
}
END
```

Параметр ver может принимать значения:

- 0 – сервис pacemaker запускает сервис corosync автоматически. Таким образом pacemaker добавлять в автозагрузку не нужно. Данный вариант использовать только для pacemaker-1.0 и младше.
- 1 – сервис pacemaker необходимо запускать вручную (индивидуальным скриптом в init.d). Таким образом нужно pacemaker добавлять в автозагрузку. Данный вариант нужно использовать с pacemaker-1.1 и выше.

Указанная выше конфигурация для pacemaker может присутствовать в файле /etc/corosync/service.d/pacemaker. Необходимо избежать дублирования данных параметров.

Полученный конфигурационный файл можно копировать на вторую ноду (или выполнить все те же самые команды на втором узле).

После того как конфигурация присутствует на двух узлах, можно запустить Corosync и Pacemaker на MASTER сервере, соблюдая следующий порядок:

```
service corosync start
service pacemaker start
chkconfig corosync on
chkconfig pacemaker on
```

Только после того, как сервисы будут запущены, необходимо выполнить те же самые команды на SLAVE сервере.

Проверить состояние работы кластера можно выполнив следующую команду (не имеет значения, на каком узле была выполнена команду):

```
crm status
```

В результате вывода оба узла должны быть помечены как `ONLINE`.

Настройка менеджера ресурсов

После того, как настроены узлы, можно переходить к этапу настройки менеджера ресурсов.

В первую очередь, необходимо выключить опцию `STONITH` в конфигурации менеджера ресурсов. Для этого на любом сервере нужно выполнить команду:

```
crm configure property stonith-enabled=false
crm configure property no-quorum-policy="ignore"
crm configure property start-failure-is-fatal=false
```

Результат выполнения команды внесет изменение в конфигурацию менеджера ресурсов как на MASTER, так и на SLAVE сервере автоматически.

Можно посмотреть текущую конфигурацию pacemaker, выполнив команду

```
crm configure show
```

В результате вывода должны быть строки со следующими значениями параметров:

```
property expected-quorum-votes="2"
property stonith-enabled="false"
property no-quorum-policy="ignore"
property start-failure-is-fatal=false
```

Если эти параметры не присутствуют в конфигурации, их нужно добавить по аналогии с параметром STONITH выше (по умолчанию данные параметры должны присутствовать в конфигурации, необходимо удостовериться в их наличии).

Типы ресурсов

- lsb – это init скрипты. При описании ресурса LSB указываются только общие для всех ресурсов параметр.

— ocf – это скрипты ядра кластера. При описании указываются индивидуальные параметры для каждого ресурса. Набор параметров у данных скриптов всегда разный.

Структура ресурсов

В кластере ресурсы могут быть объединены в группы, между ресурсами могут быть установлены зависимости, порядок запуска и другие параметры. На Рисунок 137 представлена схема (с отображением основных ресурсов) для упрощенного понимания структуры объединения ресурсов кластера серверов телефонии на базе DRBD.

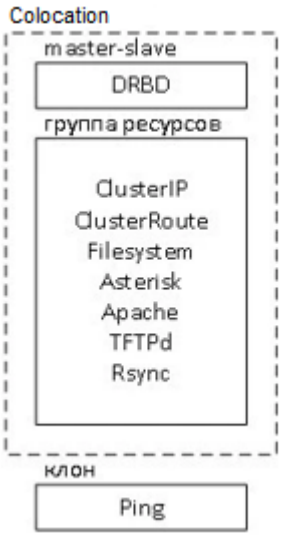


Рисунок 137. Схема структуры ресурсов

В виду того, что ресурсы и их объединения зависят друг от друга, необходимо соблюдать порядок их создания в конфигурации менеджера ресурсов. Для понимания последовательностей зависимостей представлена схема на Рисунок 138.

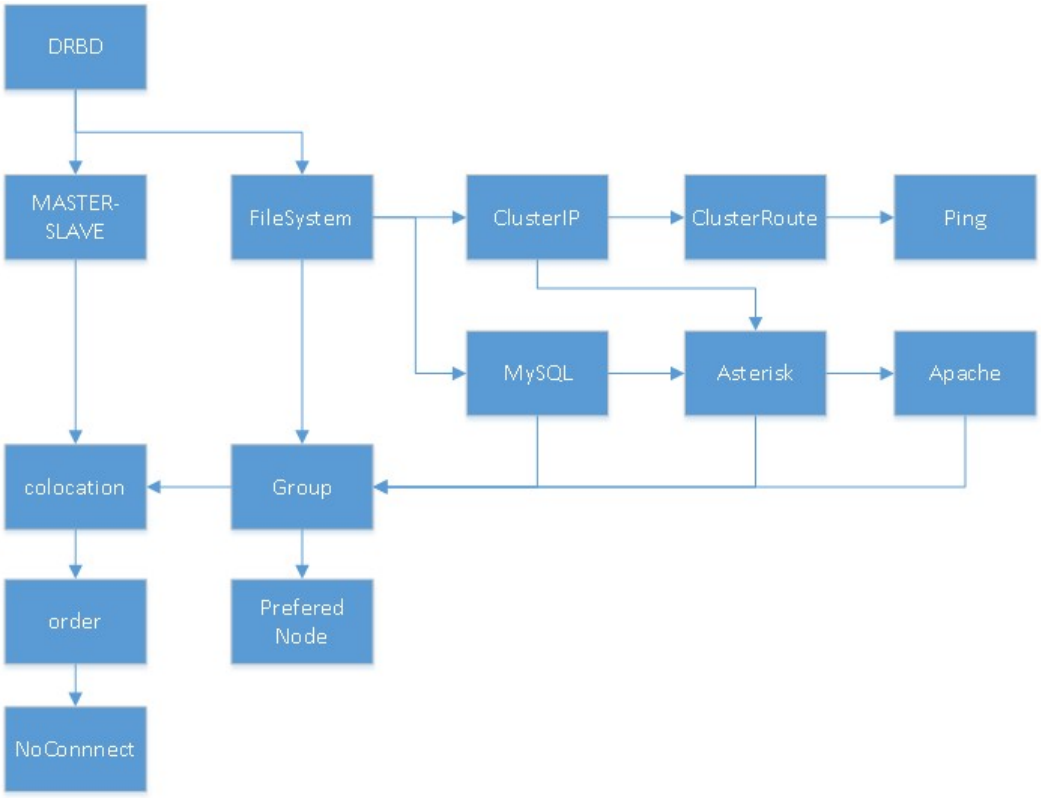


Рисунок 138. Схема последовательности определения ресурсов в кластере

Ресурс DRBD

Если выполнять команды `crm configure <опция команды>`, то они будут применяться на кластере моментально. Однако для ресурсов, использующих DRBD важна доступность самого DRBD, поэтому конфигурировать их лучше всего в теневом инстансе. Для этого необходимо перейти в терминальный режим управления кластером `crm` и выполнить команду для создания теневой конфигурации (позволит работать с конфигурацией до того, как будет применена в кластер):

```
crm(live)# cib new drbd
INFO: drbd shadow CIB created
crm(drbd)#
```

Изменение параметров `crm(live)` на `crm(drbd)` говорит о том, что работа ведется в теневом инстансе.

Далее необходимо описать ресурс `drbd_res` (имя ресурса) и конфигурацию `master_slave` (`drbd_master_slave` - имя конфигурации master_slave) для DRBD, после чего применить конфигурацию в live-инстанс:

```
configure primitive drbd_res ocf:linbit:drbd params drbd_resource=disk1 op monitor interval=29s role=Master op monitor interval=31s role=Slave
configure ms drbd_master_slave drbd_res meta master-max=1 master-
```

```
node-max=1 clone-max=2 clone-node-max=1 notify=true
 cib commit drbd
```

Здесь:

`drbd_res` – имя ресурса кластера, который будет использоваться в дальнейшем.

`drbd_resource` – указывает имя ресурса DRBD, который описан в соответствующем конфигурационном файле /etc/drbd.d/

Для конфигурации ресурса drbd используется ocf скрип, который обеспечивает переключение primary/secondary режимов сервиса DRBD узлов кластера в автоматическом режиме.

Конфигурация master-slave обеспечивает работу сервиса DRBD в состоянии primary только на одном узле в кластере.

Ресурс FileSystem

После того как ресурс DRBD определен, можно указать подключение раздела drbd к ФС, для этого будет также использоваться соответствующий ocf скрипт. Данный ocf скрипт можно использовать не только для раздела drbd, но и для любого другого раздела.

Подключение раздела к ФС тесно зависит от того, какой узел на текущий момент является DRBD primary. Поэтому необходимо создать привязку ресурса filesystem к активному DRBD узлу. Если этого не сделать, ресурс drbd может быть активен на одном узле, а примонтирование раздела к ФС произойдет на другом узле, что приведет к ошибке. Поэтому необходимо также в теневом инстансе создать описание ресурсов и конфигурации, а затем применить инстанс в текущую конфигурацию кластера, используя следующую команду:

```
 cib new fs
 configure primitive fs_res ocf:heartbeat:Filesystem params
device=/dev/drbd1 directory=/mnt/drbd fstype=ext4
```

Где:

- `fs_res` – название ресурса подключение раздела DRBD к ФС;
- `device` – указывает на блочный девайс раздела drbd;
- `directory` – указывает на директорию, куда нужно монтировать раздел;
- `fstype` – указывает на тип ФС, которой размечен раздел drbd.

Конфигурация расположения ресурса вместе с другим ресурсом тесно связана с конфигурацией описания порядка загрузки ресурсов. Таким образом кроме того, что ресурсы должны находиться вместе (colocation), необходимо также указать, в каком порядке их следует запускать (order).

```
 configure colocation fs_drbd_colo INFINITY: fs_res
```

```
drbd_master_slave:Master
 configure order fs_after_drbd mandatory: drbd_master_slave:promote
fs_res:start
 cib commit fs
```

Где:

- `fs_drbd_colo` – название конфигурации colocaion;
- `drbd_master_slave:Master` – состояние конфигурации master_slave равное Master, к которой привязывается расположение ресурса. ;
- `fs_after_drbd` – название конфигурации order;
- `drbd_master_slave:promote` – состояние конфигурции master_slave равное promote (i.e. the DRBD resource is promoted to master before the filesystem resource is started and any mount occurs);
- `fs_res:start` – состояние ресурса start.

В данной конфигурации правила `INFINITY` и `mandatory` указывают, что ресурсы должны располагаться на одном узле без исключения.

Ресурс Виртуального IP адреса

При переключении кластера из штатного режима функционирования в аварийный режим и обратно, между узлами должен мигрировать виртуальный IP адрес кластера, чтобы устройства в сети могли продолжать работать. Для этого необходимо описать соответствующий ресурс. Ресурс может быть описан двумя путями: через ocf (предпочтительней) в качестве alias и через lsb отдельным интерфейсом. Отдельный интерфейс менее желателен, так как сложнее контролировать доступность его подключения. Рассмотрим далее оба способа.

Описание в качестве alias

Для создания виртуального IP адреса в качестве alias на существующем интерфейсе (предпочтительный вариант), необходимо добавит ocf ресурс IPaddr2, выполнив следующую команду:

```
 crm configure primitive ClusterIP ocf:heartbeat:IPaddr2 params
ip="192.168.1.100" cidr_netmask="24" nic="eth0"
```

Где обязательными параметрами кластера ресурса являются:

- `ip` – указывается выделенный виртуальный IP адрес кластера;
- `cidr_netmask` – маска подсети выделенного виртуального IP адреса кластера;
- `nic` – имя сетевого интерфейса, на котором указан должен быть создан

alias.

Ресурс динамического маршрута

При переключении кластера можно также добавлять маршруты. В этом есть необходимость только в том случае, если статические маршруты, отличающиеся от маршрутов по умолчанию, назначены на виртуальный интерфейс кластера, сеть которого отличается от сети управляющего интерфейса. Например, управляющая сеть имеет адрес 192.168.1.0/24, а сеть виртуального интерфейса имеет адрес 192.168.2.0/24. В противном случае статические маршруты могут быть добавлены в конфигурацию сетевого интерфейса в ОС.

Для каждого маршрута нужно добавить отдельный ocf ресурс. Для это необходимо выполнить следующую команду:

```
crm configure primitive ClusterRoute ocf:heartbeat:Route params destination="default" gateway="192.168.1.1"
```

Где обязательными параметрами ресурса являются:

- `destination` – сеть или узел назначения, до которого прописывается маршрут. Может быть указан как 'default', так и конкретный IP адрес узла в сети, так и сеть в формате CIDR, т.е. с суффиксом /24, например;
- `gateway` – адрес шлюза, используемого для доступа к указанному назначению;
- `device` – сетевой интерфейс в системе (устройство), на котором должен быть прописан маршрут (не обязательный параметр);
- `source` – IP адрс сервера, с которого будут осуществляться подключения до указанного `destination` (не обязательный параметр, но указывается вместе с `gateway` или `device`);
- `table` – таблица, в которой должен присутствовать маршрут. Также может быть указан, но не является обязательным.

Ресурсы сервисов

Проще всего описываются ресурсы сервисов, для которых есть init скрипты. Достаточно для каждого сервиса прописать LSB ресурс. В частности, для кластера на DRBD описывают ресурсы MySQL, Asterisk, Apache. Однако, перед добавлением ресурсов в кластер необходимо остановить сервисы, иначе менеджер ресурсов в кластере выдаст ошибку при добавлении, из-за того, что сервис работает. Для этого сначала производится остановка сервисов:

```
service httpd stop
```

```
service asterisk stop
service mysqld stop
```

Затем добавляются сами ресурсы. Для этого нужно выполнить по одной команде создания ресурса для каждого init скрипта:

```
crm configure primitive Apache lsb:httpd op monitor interval=60s timeout=30s on-fail=restart
crm configure primitive Asterisk lsb:asterisk op monitor interval=5s timeout=30s on-fail=standby
crm configure primitive MySQL lsb:mysqld op monitor interval="60s" timeout="60s"
```

После добавления ресурсов сервисы сразу будут запущены.

Также могут быть добавлены ресурсы tftp и rsync:

```
crm configure primitive Rsyncd lsb:rsyncd op monitor interval="120s" timeout="60s"
crm configure primitive TFTPd lsb:in.tftpd op monitor interval="120s" timeout="60s"
```

Создание группы ресурсов

После того как в конфигурации кластера определены ресурсы под все необходимые сервисы, ресурсы можно объединить в группы. Группа ресурсов — это комбинированное описание совместного расположения и порядка загрузки (colocation + order). Совместное расположение, определяется тем, какие ресурсы входят в группу. Порядок загрузки определяется тем, в какой последовательности они вписаны в группу. Итак, следует соблюдать следующую последовательность загрузки ресурсов:

1. Виртуальный IP адрес кластера.
2. Динамические маршруты.
3. ФС.
4. MySQL
5. Asterisk
6. Apache
7. TFTPd
8. Rsyncd

Например, для кластера на DRBD достаточно прописать следующую конфигурацию группы:

```
crm configure group TelephonyGroup ClusterIP fs_res MySQL Asterisk Apache
```

В данном случае конфигурация группы будет называться TelephonyGroup (группа ресурсов для телефонии).

При выполнении данной команды конфигурации order и colocation, созданные ранее на этапе описания ресурса ФС, в состав которых входят `fs_res`, будут автоматически заменены на конфигурации с TelephonyGroup, о чем сообщит система.

Ресурс проверки подключения

Во избежание рассинхронизации информации на узлах кластера, активный узел должен проверять, подключен ли он к сети, не потерял ли он физическое подключение. В случае, если узел понимает, что подключение к сети потеряно, он должен перейти в аварийный режим и остановить все активные ресурсы.

Ping

Для этого активный узел в должен периодически проверять, отвечают ли ему на ICMP запросы контрольные сетевые узлы. Данную операцию выполняет ocf ресурс ping. Однако ресурс сам по себе не обеспечивает переключение режима кластера или изменение статуса ресурса, зато ресурс изменяет значение переменной ядра кластера, на основе которой ядро может принять решение о текущем состоянии. Таким образом для определения, имеется ли физическое подключение узла к локальной вычислительной сети, т.е. доступен ли контрольный узел в сети, необходимо определить следующий ресурс:

```
crm configure primitive ClusterPing ocf:pacemaker:ping params multiplier="111" host_list="192.168.1.1" name="ping_net" dampen="5s" op monitor interval="10s" timeout="60s"
```

Где:

- `multiplier` – множитель переменной для каждого хоста;
- `host_list` – список контрольных узлов в сети, разделенных пробелом;
- `name` – имя переменной, которой будут задаваться значения в результате расчета, используя множитель;
- `dampen` – задержка перед внесением изменений в окружение кластера, указанная в секундах. Используется для того, чтобы ресурсы не меняли свое положение между узлами, когда подключение теряется на очень маленькое время.

Данная конфигурация пингует хост. Каждый хост оценивается в 111 очков. Суммарное значение для каждой ноды хранится в переменной `ping_net`. Эти значения можно и нужно использовать при определении места расположения ресурса.

Клон ресурса

Для того, чтобы данный ресурс был запущен одновременно на двух нодах, необходимо создать его клон. Клон задается соответствующим ресурсом:

```
crm configure clone Cloned-Ping ClusterPing
```

Таким образом будет создан ресурс Cloned-Ping, который будет запускать ClusterPing на обоих узлах вне зависимости от их состояния в кластере. Далее необходимо указать менеджеру ресурсов, как работать со статусом подключения на основе данных от ресурса ClusterPing.

Расположение и приоритезация узлов

Чаще всего необходимо запретить узлу запускать на себе ресурсы, если узел определил, что он не имеет связи с контрольным узлом в сети. Таким образом, данная конфигурация применима, если доступность определяется только по одному контрольному узлу в сети. Для это необходимо определить ресурса, предписывающий размещение ресурсов на основании значения переменной `ping_net`:

```
crm configure location NoConnectionNode ClusterIP rule -inf: not_defined ping_net or ping_net lte 0
```

Данный ресурс NoConnectionNode, предписывающий расположение, запрещает размещать ресурс ClusterIP на узле, где пинг меньше либо равен 0 (lte — less then or equal) или не запущен ресурс пинга. Достигается это за счет того, что узел с отсутствующим подключением получает значение «минус бесконечность» очков.

Для того, чтобы ресурс вернулся на резервируемую ноду после возвращения подключения, необходимо определить ресурс, предписывающий расположение, устанавливающий 50 очков резервируемому узлу по умолчанию.

```
crm configure location PreferedNode ClusterIP 50: node-a
```

Данный ресурс PreferedNode, предписывает расположение ресурса ClusterIP на узле node, устанавливая узлу node на 50 очков больше.

Работа с Pacemaker

1. Отредактируйте файл /etc/hosts

Отредактируйте файл /etc/hosts на всех серверах, которые будут входить в предполагаемый кластер, с любого терминала в текстовом редакторе с помощью команды(где `nano` – название сервера):

```
nano /etc/hosts
```

Добавьте следующие строки в /etc/hosts:

```
10.45.4.58  webserver-01
10.45.4.59  webserver-02
```

2. Изменение индексной страницы Nginx по умолчанию

Необходимо внести изменения в индексной странице Nginx по умолчанию на сервере. Для этого выполните следующую команду на первом сервере:

```
echo '<h1>webserver-01</h1>' > /usr/share/nginx/html/index.html
```

Выполните следующую команду на втором сервере:

```
echo '<h1>webserver-02</h1>' > /usr/share/nginx/html/index.html
```

3. Установка и настройка Pacemaker выполняется следующими командами:

```
systemctl enable pacemaker
systemctl enable corosync
systemctl enable pcsd
```

4. Синхронизация конфигурации

Установка создаст пользователя системы «hacluster». Также необходимо запустить PCSD для синхронизации конфигурации:

```
systemctl start pcsd
```

5. Создание пароля

Далее создайте новый пароль для пользователя «hacluster», который был автоматически создан во время предыдущей установки, обратите внимание, что следует использовать один и тот же пароль для всех серверов, для чего зайдите на каждый сервер в кластере и поменяйте пароль:

```
passwd hacluster
```

6. Создание кластеров

Для создания кластера запустите эту команду ниже:

```
pcs cluster auth webserver-01 webserver-02
```

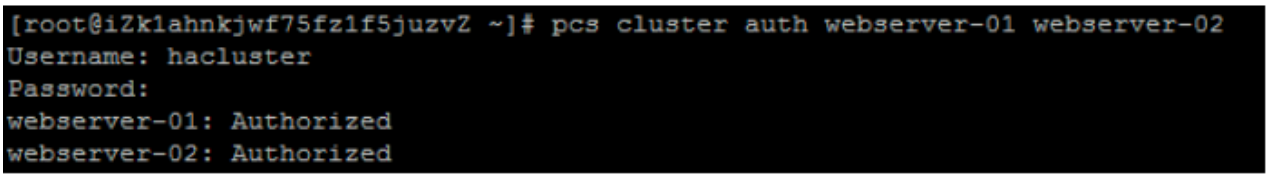


Рисунок 139. Создание кластера (1)

На данный момент все готово к созданию кластера.

```
pcs cluster setup --name rosacluster webserver-01 webserver-02
```

где `rosacluster` – это имя кластера, в то время как `webserver-01` и `webserver-02` являются серверы, которые будут частью `rosecluster`.

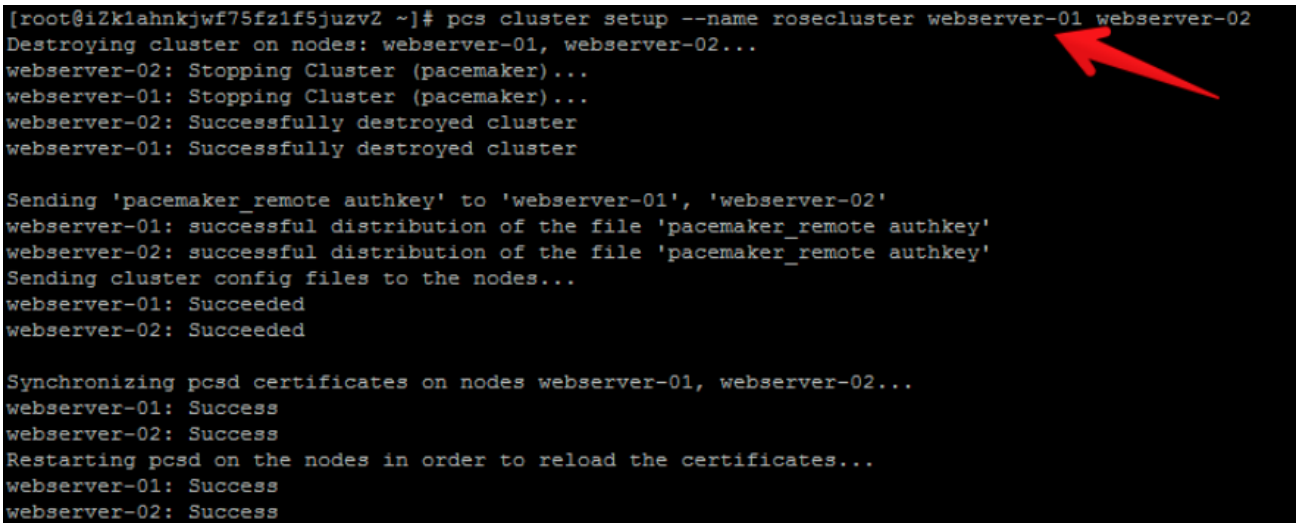


Рисунок 140. Создание кластера (2)

Можно проверить состояние кластера с помощью следующей команды (Рисунок 141):

```
pcs status
```

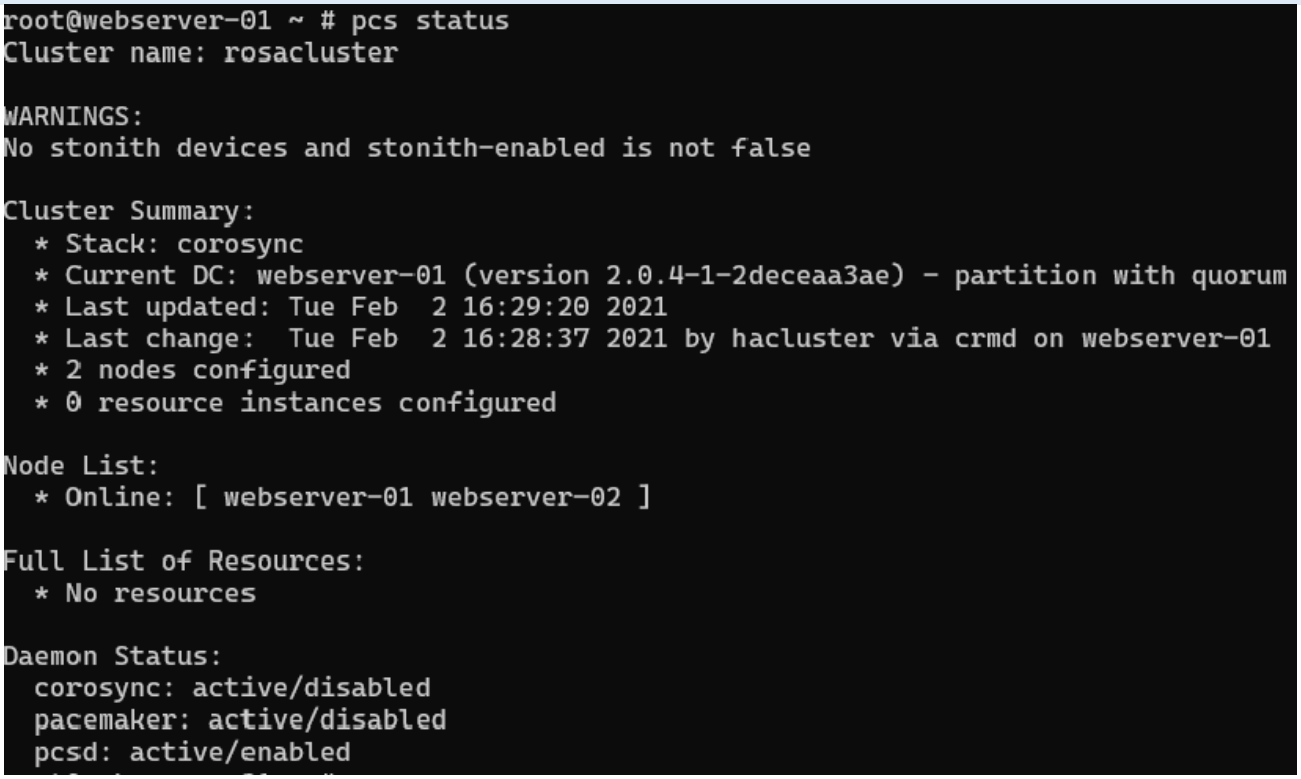


Рисунок 141. Проверка состояния кластера

7. Отключение STONITH

Для корректной работы Pacemaker необходимо выполнить отключение STONITH.

При выполнении команды `pcs status` вы увидите предупреждение в выходных данных о том, что никакие устройства STONITH не настроены, и STONITH не отключен:

```
no stonith devices and stonith-enabled is not false
```

Отключите STONITH с помощью следующей команды pcs:

```
pcs property set stonith-enabled=false
```

8. Игнорировать политику кворума

Здесь необходимо настроить Pacemaker игнорируя кворум:

```
pcs property set no-quorum-policy=ignore
```

Проверьте список свойств и убедитесь, что STONITH и политики quorum отключены (Рисунок 142. Проверка состояния STONITH):

```
pcs property list
```

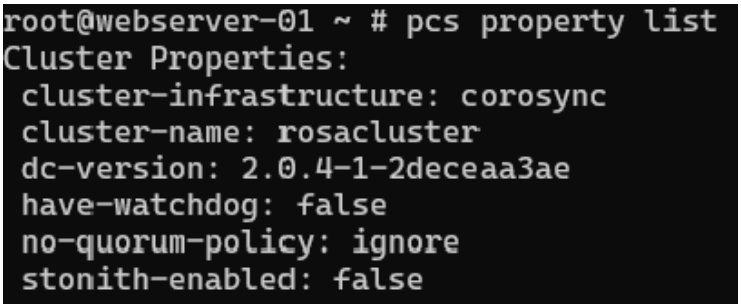


Рисунок 142. Проверка состояния STONITH

9. Добавление ресурсов

Добавить новый плавающий IP-адрес `v_ip` с помощью следующей команды:

```
pcs resource create v_ip ocf:heartbeat:IPaddr2 ip=10.45.4.60 cidr_netmask=24 op monitor interval=20s
```

где `ip=10.45.4.60` – плавающий IP-адрес для Pacemaker высокой доступности.

Далее, можно добавить второй ресурс в кластер. Ресурс агент службы `systemd:nginx` под названием `nginx`, таким образом можно добавить любой systemd юнит для отказоустойчивости в Pacemaker:

```
pcs resource create nginx systemd:nginx
```

Убедитесь, что нет ошибок, проверьте ресурсы:

```
pcs status resources
```

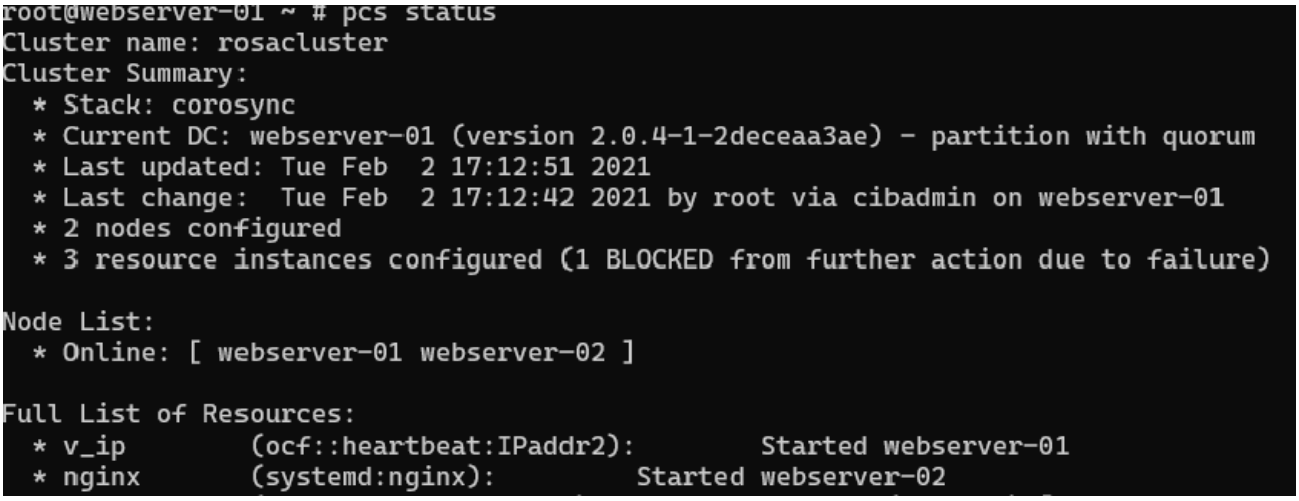


Рисунок 143. Добавление ресурсов в кластер

10. Настройка ограничения

На этом шаге оба ресурса, созданные ранее, добавляются к работе на одном хосте. Установите ограничение коллокации для ресурсов со счетом бесконечности:

```
pcs constraint colocation add nginx v_ip INFINITY
```

Также необходима установка Nginx ресурсов (`webserver`), чтобы всегда работать на том же хосте, где применяется активный адрес `v_ip`:

```
pcs constraint order v_ip then nginx
```

Чтобы проверить работающие ресурсы на том же хосте, используйте команду:

```
pcs status
```

11. Тест кластера.

Перейдите по адресу http:// 10.45.4.60 на вашем веб-браузере, вы увидите страницу Nginx по умолчанию на `webserver-01`.

Затем выполните следующую команду, чтобы остановить кластер `webserver-01`:

```
pcs cluster stop webserver-01
```

Теперь, если вы обновите страницу по адресу http://10.45.4.60, вы получите страницу Nginx по умолчанию от `webserver-02`.

Работа в командной строке Pacemaker (PCS)

Значение параметров PCS представлены в таблице Таблица 66.

Таблица 66 – Параметры команд PCS

Параметр	Значение параметра
`pcs property list`	Посмотреть параметры
`pcs status`	Посмотреть состояние кластера

`pcs cluster disable –all`	Отключить все ресурсы кластера
`pcs cluster stop --all`	Остановить все ноды
`pcs status resources`	Посмотреть состояние ресурсов
`pcs resource move CLUSTER_IP zs-node1`	Изменить активную ноду
`pcs cluster node remove node_name`	Удаление ноды
`pcs resource cleanup`	Очистка счетчиков сбоев

Работа в командном интерпретаторе CRM

Данная утилита имеет собственный SHELL, в котором довольно удобно работать. Из настроек данного интерпретатора можно отметить назначение редактора (например nano или mcedit):

```
crm options editor vim
crm opti edi mcedit
crm conf edit
```

Для просмотра конфигурации используйте следующую команду:

```
crm configure show
```

Для сохранения конфигурации используйте команду:

```
crm configure save _BACKUP_PATH_
```

Для того, чтобы выполнить восстановление конфигурации воспользуйтесь следующей командой:

```
crm configure load replace _BACKUP_PATH
```

Выгрузка сервисов

Все LSB ресурсы, которые прописаны в менеджере ресурсов pacemaker, должны быть исключены из автозагрузки (кроме сервиса DRBD, т.к. он описан OCF ресурсом, а сам сервис должен быть запущен одновременно на двух узлах для физической синхронизации данных).

Необходимо выполнить выгрузку сервисов на двух узлах, используя следующую команду:

```
chkconfig asterisk off
chkconfig httpd off
chkconfig mysqld off
chkconfig drbd on
chkconfig corosync on
chkconfig pacemaker on
```

Администрирование через WEB

Каждая из нод получает информацию от порта 2224, которая позволяет

подключиться и посмотреть, а также изменить конфигурацию

На Рисунок 144 рассмотрен пример просмотра конфигурации через https://100.201.203.54:2224.

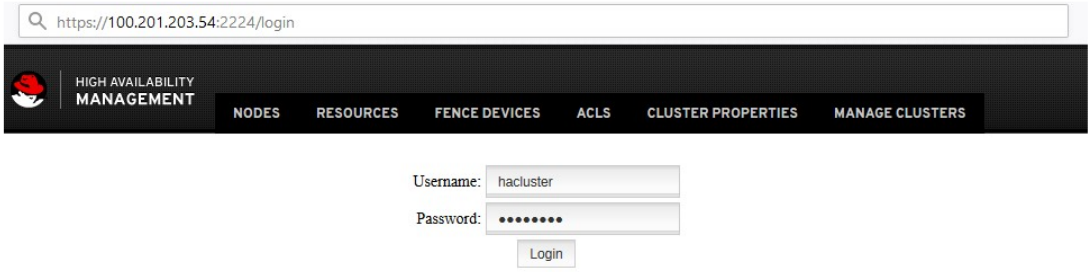


Рисунок 144. Просмотр конфигурации через WEB

Так же доступен и просмотр IP кластера (Рисунок 145 и Рисунок 146).

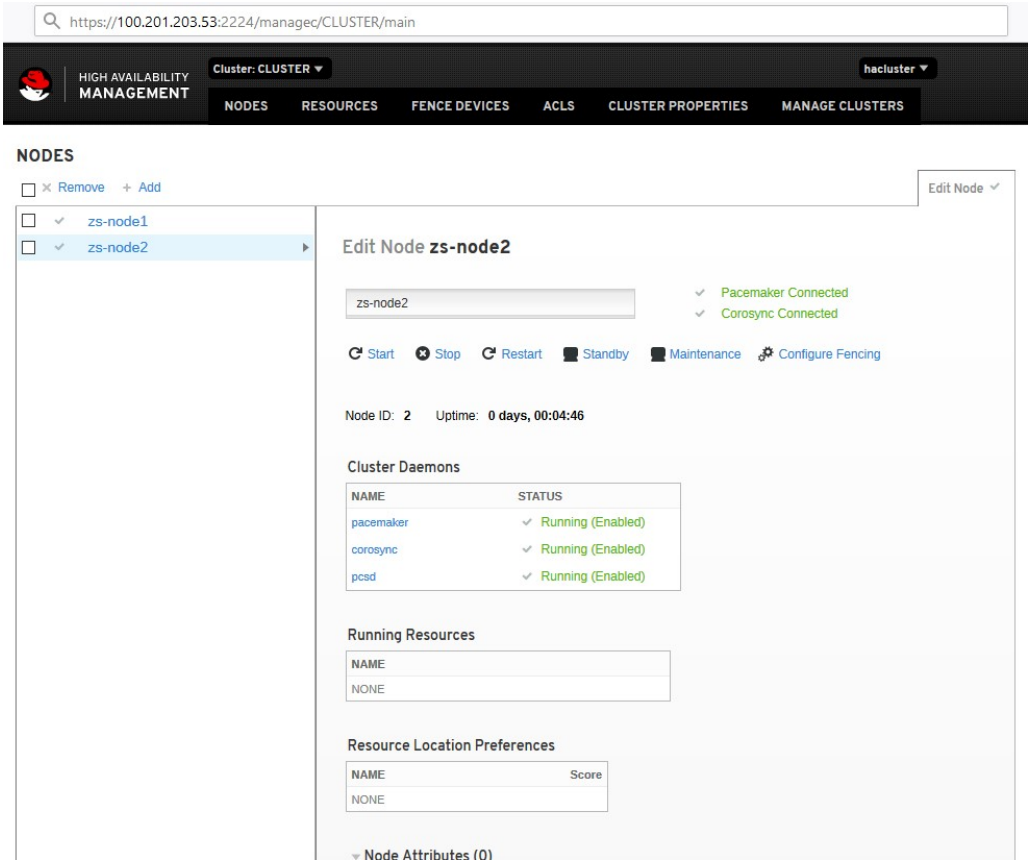


Рисунок 145. Просмотр конфигураций нода

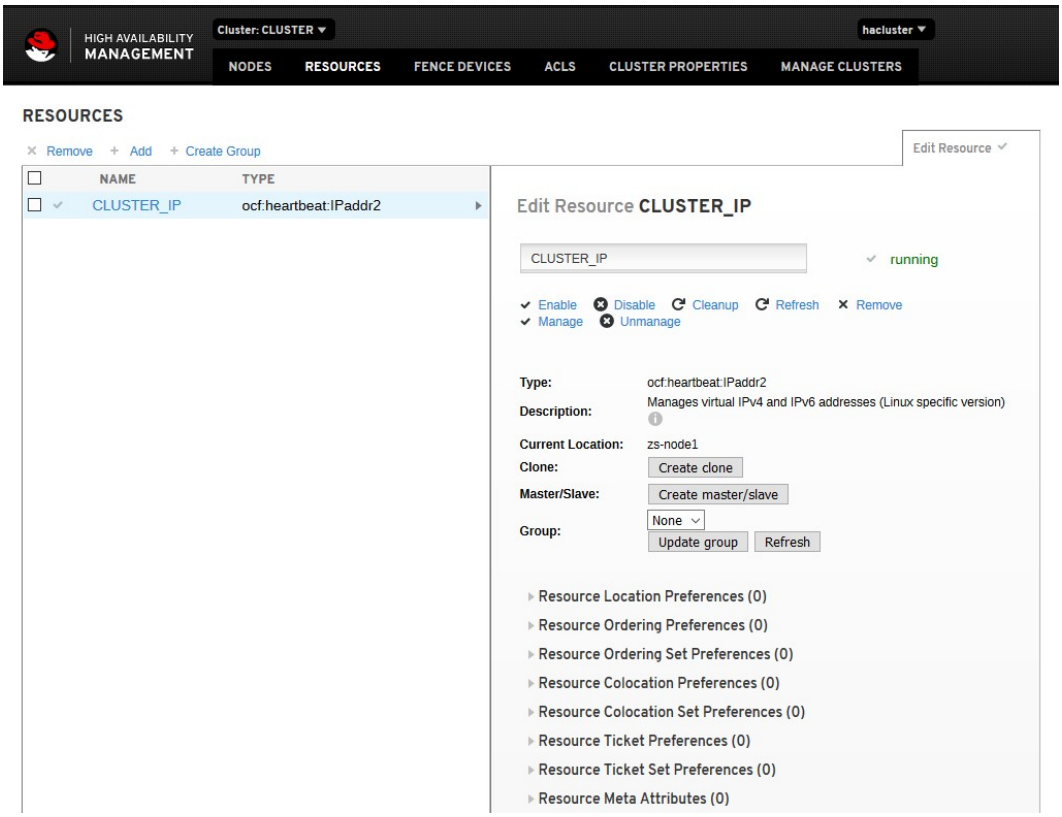


Рисунок 146. Просмотр конфигураций кластера

15. НАСТРОЙКА СЕТИ

15.1. Настройка сетевых интерфейсов

ОС РОСА «НИКЕЛЬ» автоматически подключается к доступным сетевым интерфейсам. Если автоматическое подключение не удалось, или если вы хотите настроить доступ в интернет, воспользуйтесь апплетом «Редактор соединений» (Network Manager) (Рисунок 147).

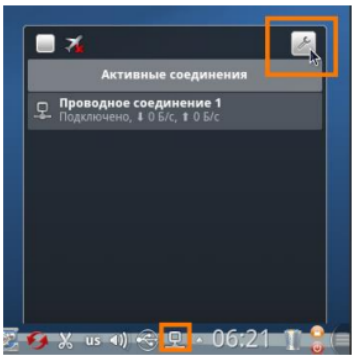


Рисунок 147

15.1.1. Добавление проводного соединения

После подключения кабеля к сетевой карте ПК выполняется автоматическое присвоение IP-адреса и других параметров локальной сети. Соединив ПК при помощи кабелей и сетевого оборудования (хабов, свитчей, роутеров), выберите в окне настроек «Редактора соединений» вкладку «Проводные» и нажмите на кнопку [Добавить]. В открывшемся окне перейдите на вкладку «IPv4» и выберите «Метод: Общий с другими компьютерами», после чего нажмите [OK] (Рисунок 148). .

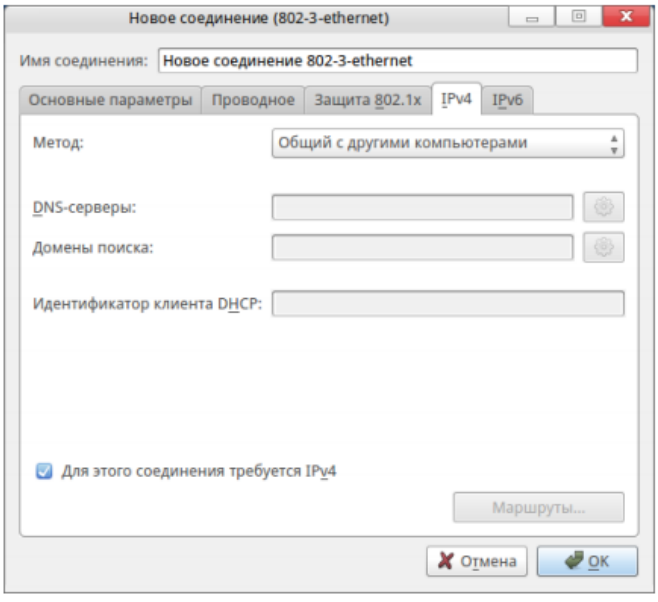


Рисунок 148

15.1.2. Добавление VPN-соединения

VPN (Virtual Private Network, «виртуальная частная сеть») — это технология, позволяющая создать защищенной сетевое соединение поверх незащищенной сети. С помощью VPN часто организуется подключение пользователей к интернету по выделенным линиям. Для создания нового подключения VPN необходимо знать сетевое имя или IP-адрес шлюза, логин и пароль. Эти данные предоставляет интернет-провайдер.

1. Откройте «Редактор соединений», нажмите на кнопку [Изменить соединения] и перейдите на вкладку «VPN». Нажмите [Добавить], чтобы открыть окно «Новое соединение (vpn)».

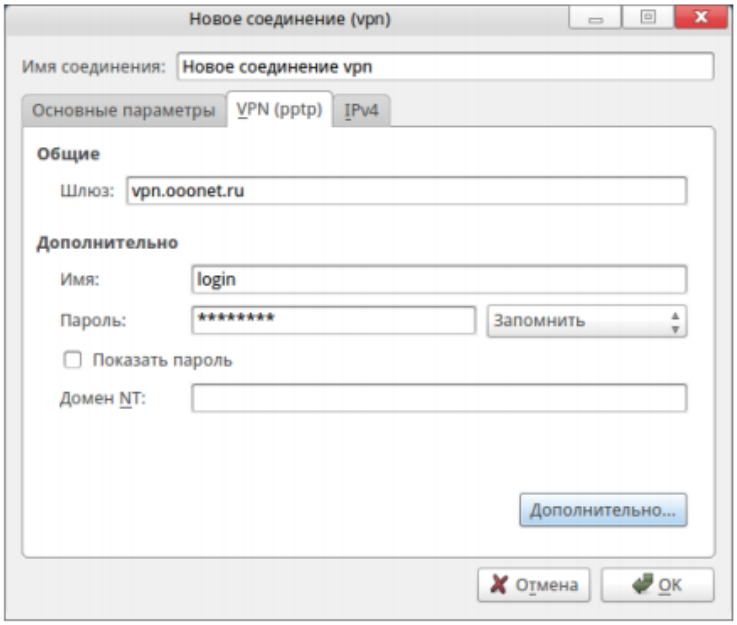


Рисунок 149

2. Перейдите на вкладку «VPN (pptp)» и введите данные, полученные от провайдера.

3. Нажмите на кнопку [Дополнительно...]. Выберите «Шифрование: Любое» и нажмите [OK]. После того, как вы завершите настройку соединения, подключение должно произойти автоматически. Если этого не происходит, запустите созданное соединение щелчком мыши в окне «Редактора соединений».

Консольные команды для управления сетями

Для оперативного получения информации о сетевых подключениях, доступности сетевых ресурсов и т. п. можно использовать следующие команды, выполняемые в консоли:

`ifconfig`

Команда позволяет показать параметры всех сетевых соединений.

`ping`

Команда позволяет проверить качество сетевого соединения с заданным узлом.

`route -n`

Команда выводит на экран таблицу маршрутизации.

15.2. Фильтрация сетевого потока

15.2.1. Использование службы iptables

iptables — утилита командной строки, является стандартным интерфейсом управления работой межсетевого экрана.

Кратко рассмотрим принцип работы утилиты: все сетевые пакеты, которые проходят через ПК, отправляются им или предназначены для него, ядро направляет через фильтр iptables, где пакеты поддаются проверкам и затем для каждой проверки, если она пройдена выполняется указанное в ней действие.

В фильтре iptables все сетевые пакеты делятся на три цепочки:

– Input - обрабатывает входящие пакеты и подключения.

– Forward - эта цепочка применяется для проходящих соединений. Сюда попадают пакеты, которые отправлены в вашу систему, но не предназначены ей, они просто пересылаются по сети к своей цели

– Output - эта цепочка используется для исходящих пакетов и соединений.

Для каждого типа пакетов можно установить набор правил, которые по очереди будут проверяться на соответствие с пакетом и если пакет соответствует, то применять к нему указанное в правиле действие. Правила образуют цепочку, поэтому input, output и forward называют цепочками правил. Действий для пакетов может быть несколько:

– ACCEPT - разрешить прохождение пакета дальше по цепочке правил;

– DROP - удалить пакет;

– REJECT - отклонить пакет, отправителю будет отправлено сообщение, что пакет был отклонен;

– LOG - сделать запись о пакете в лог файл;

– QUEUE - отправить пакет пользовательскому приложению.

Над цепочками правил в iptables есть еще один уровень управления – таблицы, которые имеют стандартный набор цепочек input, forward и output. Таблицы предназначены для выполнения разных действий над пакетами, например для модификации или фильтрации.

Типы таблиц:

– raw - предназначена для работы с сырыми пакетами, пока они еще не прошли обработку;

– mangle - предназначена для модификации пакетов;

– nat - обеспечивает работу nat, если вы хотите использовать ПК в качестве маршрутизатора;

– filter - основная таблица для фильтрации пакетов, которая используется по умолчанию.

Чтобы использовать службы iptables и ip6tables установите пакет iptables-services:

```
# dnf install iptables-services
```

Пакет iptables-services содержит службу iptables и службу ip6tables.

Чтобы запустить службы iptables и ip6tables, выполните:

```
# systemctl start iptables
# systemctl start ip6tables
```

Чтобы включить старт служб при каждом запуске системы, выполните:

```
# systemctl enable iptables
# systemctl enable ip6tables
```

Общий синтаксис утилиты имеет следующий общий вид:

```
$ iptables -t таблица действие цепочка дополнительные_параметры
```

Где параметры:

– таблица – указывается таблица, с которой нужно работать утилите;

– действие – необходимое действие (например, создать или удалить правило);

– цепочка – цепочка, с которой будет работать утилита;

– дополнительные параметры – описывают действие и правило, которое нужно выполнить.

Полное описание правил работы с утилитой можно найти по команде `man iptables`.

15.2.2. Служба nftables

Этот программный продукт обеспечивающая фильтрацию и классификацию как каждого сетевого пакета, так и потока.

Структуры для хранения правил nftables

Структуры для хранения правил nftables в целом схожи на структуры iptables:

– Таблицы - содержат ссылку на контейнеры цепочек правил.

– Цепочка - содержит наборы правил, выполняемых в порядке очереди

– Правило - семантическая конструкция, позволяющая выбрать действия,

которые нужно осуществить с описываемым правилом набором данных

Семьи nftables (families)

Вся инфраструктура nftables предназначена для работы с различными семействами адресов (families) разных протоколов (IPv4, IPv6, ARP, MAC). Ранее для обработки разных семейств адресов использовались разные утилиты - iptables, ip6tables, arptables, ebtables. Теперь с помощью введения понятия семейства обработка происходит в рамках одного программного продукта. На текущий момент существуют следующие семейства:

- Ip – таблицы этого семейства будут видеть трафик (пакеты) протокола IPv4;
- ip6 – таблицы этого семейства будут видеть трафик (пакеты) протокола IPv6;
- inet – в таблицах этого семейства будет обрабатываться трафик (пакеты) протоколов IPv4 и IPv6. Правила для ipv4 не будут влиять на пакеты IPv6. Правила, подходящие под оба протокола, будут влиять на пакеты обоих протоколов;
- arp – таблицы этого семейства видят трафик arp - протокола;
- bridge – в таблицах будут видеться пакеты, коммутируемые на уровне L2 OSI. Это семейство аналог ebtables;
- netdev — это семейство, аналогов которого нет в x_tables. Оно видит все пакеты, которые только были переданы драйвером в стек протоколов.

Примеры использования nftables

Теперь рассмотрим примеры nftables. Команда nft – это утилита администрирования фреймворком nftables при управлении потоками данных. Именно с помощью нее выполняется настройка nftables. Использует при работе интерфейс командной строки. Позволяет создавать новые правила nftables, удалять старые и просматривать уже созданные цепочки и таблицы правил.

Создание таблицы в nftables

При создании таблицы (table) должно быть определено семейство (family) адресов. Например, давайте создадим таблицу с именем, test_table, которая отрабатывает одновременно пакеты IPv4 и IPv6. Для этого выполните следующую команду:

```
sudo nft add table inet test_table
```

Создание цепочки в nftables

Цепочки (chain) являются контейнерами для правил. Существуют два типа цепочек:

- Базовые цепочки (base chain) - можно использовать в качестве точки входа для пакетов из стека протоколов.

– Регулярные цепочки (regular chain) - можно использовать с действием jump цель. Применяют для лучшей организации множества правил. При создании цепочки следует учитывать, что таблица, в которую добавляетсяцепочку, должна уже существовать.

```
sudo nft add chain inet [таблица] [цепочка] {set}
```

Например:

```
sudo nft add chain inet test_table test_chain {type filter hook input priority 0 \; policy accept \; }
```

Примечание: Чтобы командный интерпретатор не интерпретировал как конец команды необходимо экранировать точку с запятой следующим образом: \;

Эта цепочка фильтрует входящие пакеты. Приоритет (priority) задает порядок, в котором nftables обрабатывает цепочки с одинаковым значением hook. Параметр policy устанавливает действие по умолчанию для правил в этой цепочке. В данном случае было установили действие accept (принимать пакет).

Добавление правила

Добавить правило (rule) в настраиваемую конфигурацию можно с помощью следующей синтаксической конструкции:

```
sudo nft add rule [family] [table] [chain] [expression] [action]
```

Например:

```
sudo nft add rule inet table1 chain_input ip saddr 8.8.8.8 drop
```

Данное правило добавляется в таблицу с именем table1 в цепочку chain_input и отбрасывает пакеты с ip-адресом источника отправления 8.8.8.8.

Удаление правила

Для удаления правила nftables используется команда со следующим синтаксисом:

```
sudo nft delete rule [family] [table] [chain] handle [number]
```

Например:

```
sudo nft delete rule inet table1 chain_input handle 3
```

Удаление цепочки

Цепочка удаляется с помощью следующей команды:

```
sudo nft delete chain [family] [table] [chain]
```

Например:

```
sudo nft delete chain inet table1 chain_input
```

Удаление таблицы

Таблицу можно удалить с конструкции со следующим синтаксисом:

```
sudo nft delete table [family] [table]
```

Например:

```
sudo nft delete table inet table1
```

Полное руководство по использованию утилиты можно найти в `man nft`.

15.3. Создание домена ipa и подключение к нему станции

IPA (Identity, Policy and Audit) — централизованная система по управлению учетными записями пользователей. Она состоит из сервера, на котором ведется база учетных записей пользователей и подключенных к нему рабочих станций, с каждой из которых пользователь может авторизоваться под своей учетной записью. Для развертывания сервера IPA в ОС РОСА «НИКЕЛЬ» необходимо иметь не менее 4 Гб оперативной памяти на СВТ и войти в систему с правами администратора (группа wheel, SELinux-пользователь aib_u), что соответствует автоматически создаваемому первому пользователю системы.

Для установки репликации сервера IPA, надо перед установкой сервера IPA и реплики, перевести систему в umask 022. Для этого заходим в */etc/profile меняем umask 027 на umask 022, так же заходим в /etc/bashrc и меняем umask 027 на umask 022.* Перезагружаем систему. После этого инсталлируем IPA сервер и его реплику.

Имена для сервера и рабочих станций

Для корректной работы в домене и сервер, и рабочие станции должны иметь уникальные совместимые имена, включающие название домена. Для примера рассмотрим название домена - *domain.loc* тогда сервер назовем *server.domain.loc*.

Имя можно присвоить при установке системы, в инсталляторе, в пункте "Имя сети и узла" (и не забыть нажать на кнопку [Применить]).

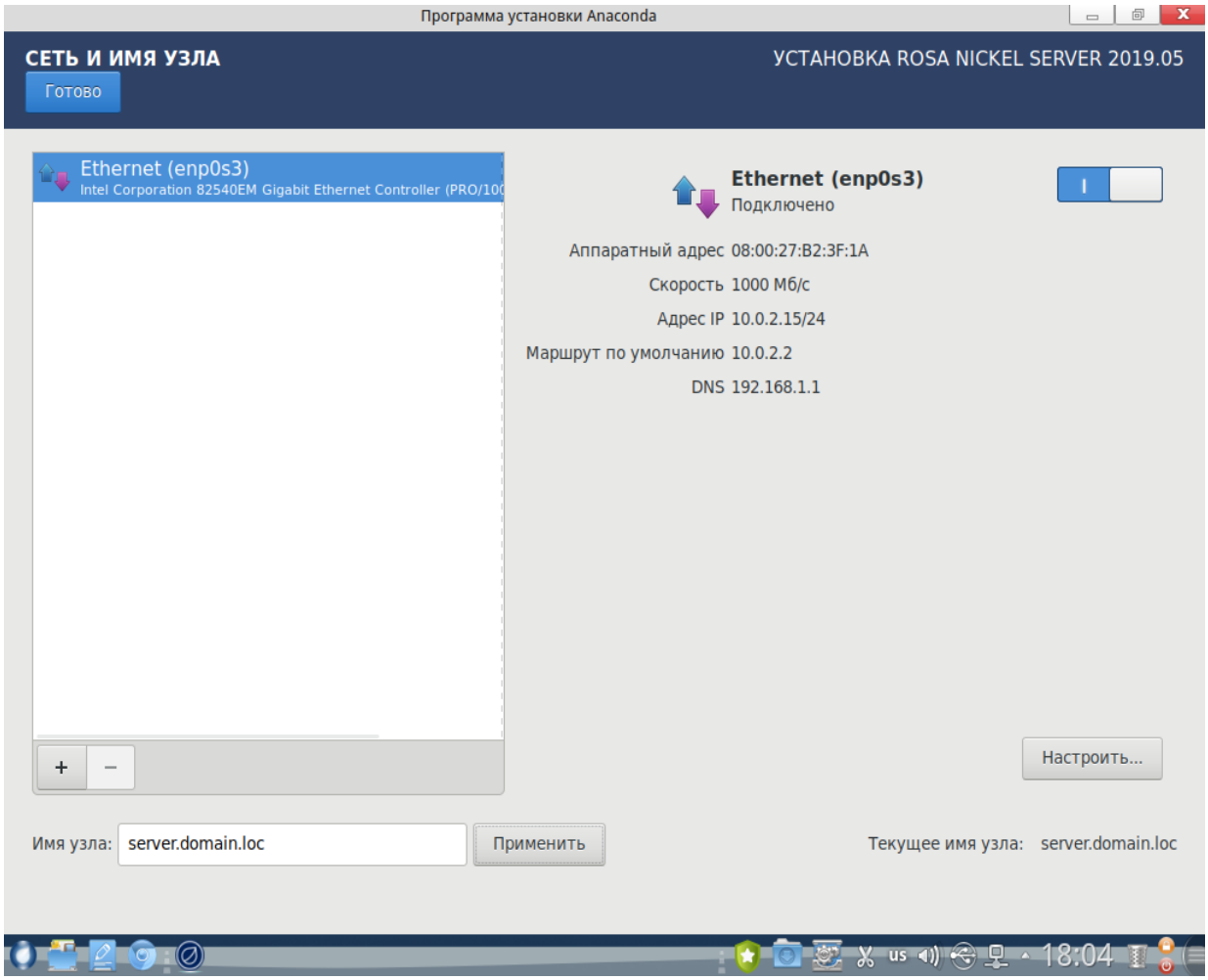


Рисунок 150

Также имя можно установить в консольном режиме в уже установленной системе с помощью команды:

```
sudo hostnamectl set-hostname station1.domain.loc
```

Таким образом присвоив вашей станции имя *station1* в домене *domain.loc* (Рисунок 151)

```
aib@localhost ~ $ sudo hostnamectl set-hostname station1.domain.loc
[sudo] пароль для aib:
aib@localhost ~ $ hostnamectl
   Static hostname: station1.domain.loc
         Icon name: computer-vm
           Chassis: vm
        Machine ID: 7a7fc1335efad57ceb57eb096107a25c
           Boot ID: 62b4b0bb932d4b71b810870d7c16a1d8
    Virtualization: oracle
  Operating System: ROSA Nickel Workstation
       CPE OS Name: cpe:/o:rosa:rosalinux:2019.05
            Kernel: Linux 5.4.137-nickel-2rosa2019.05-x86_64
      Architecture: x86-64
aib@localhost ~ $
```

Рисунок 151

Таким образом было присвоено серверу имя *server.domain.loc* а рабочей станции имя *station1.domain.loc.*

Имя всегда можно проверить вызовом команды `hostnamectl` без параметров.

15.4. Настройка адресов

15.4.1. Настройка сервера

Система-сервер IPA-домена должна иметь статические IP-адрес так как в типовой конфигурации она будет работать с DNS- сервером домена и этот адрес сервера будет прописан на станциях как адрес DNS. По умолчанию после установки в системе настроена динамическая адресация, которую нужно переключить в настройках сетевых соединений.

Для примера рассмотрим, что адрес нашего сервера будет 192.168.1.100, тогда настройка сетевого соединения будет выглядеть как продемонстрировано на рисунке 152.

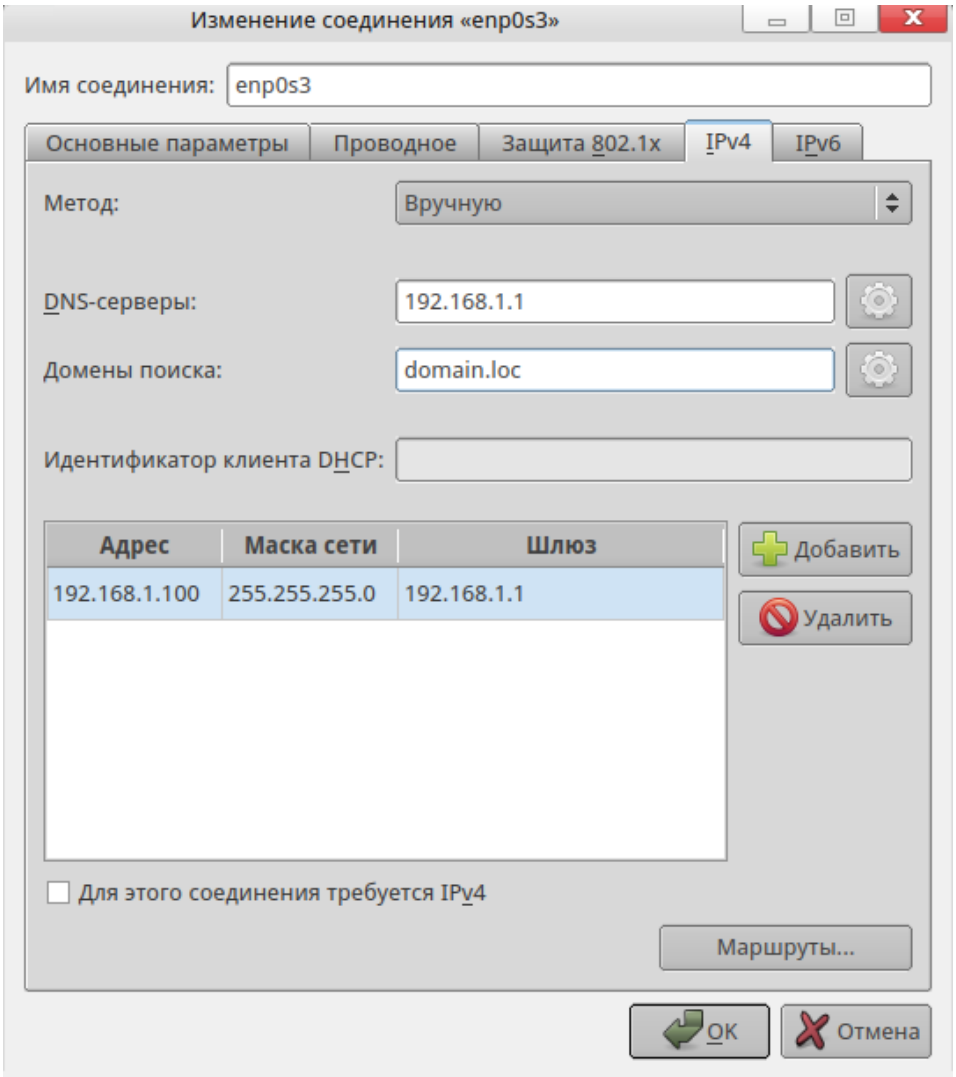


Рисунок 152

После настройки соединения необходимо разорвать его и вновь соединиться, иначе настройки текущего соединения не изменятся и дальнейшая настройка IPA-сервера будет неверной.

Итоговый результат можно посмотреть в системном лотке справа внизу крана (Рисунок 153).

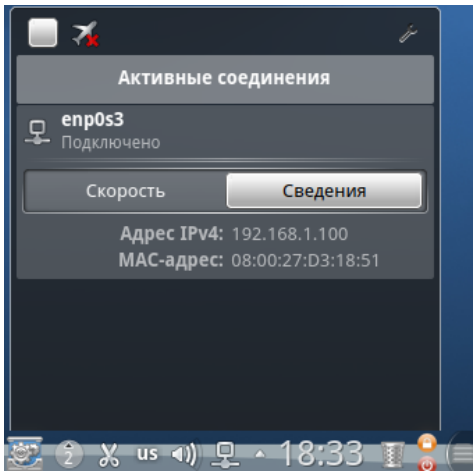


Рисунок 153

15.4.2. Настройка рабочей станции

Рабочая станция также может использовать и динамическую адресацию сети, от нее требуется указание DNS-сервером IP-адреса нашего IPA-сервера и домена поиска.

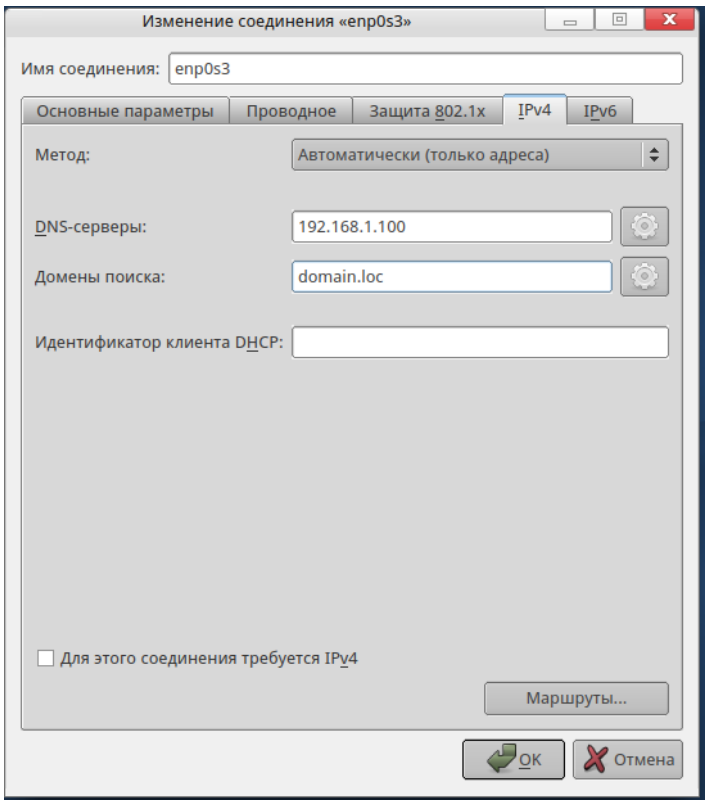


Рисунок 154

Так же как и для сервера, после изменения настроек сетевого соединения рабочей станции необходимо разорвать и вновь установить соединение, уже с новыми настройками.

15.4.3. Установка сервера IPA

После того, как настроено имена и сетевые соединения, можно приступать к настройке собственно сервера IPA. Для этого в консоли системного администратора необходимо ввести команду:

```
sudo ipa-server-install
```

И далее согласиться с предложениями утилиты, ответив `yes` на два первых вопроса, как указано на рисунке 155.

```
aib@server ~ $ sudo ipa-server-install
[sudo] пароль для aib:
Unexpected system mask: 0027, expected 0022
Do you want to continue anyway? [yes]: yes

The log file for this installation can be found in /var/log/ipaserver-install.log
==============================================================================
This program will set up the FreeIPA Server.
Version 4.8.9

This includes:
  * Configure a stand-alone CA (dogtag) for certificate management
  * Configure the NTP client (chronyd)
  * Create and configure an instance of Directory Server
  * Create and configure a Kerberos Key Distribution Center (KDC)
  * Configure Apache (httpd)
  * Configure the KDC to enable PKINIT

To accept the default shown in brackets, press the Enter key.

Do you want to configure integrated DNS (BIND)? [no]: yes
```

Рисунок 155

Далее установщик запросит имена сервера и домена. Если вы правильно указали настройки в предыдущих пунктах, то достаточно нажать клавишу [ENTER] трижды для подстановки значений по умолчанию.

```
Enter the fully qualified domain name of the computer
on which you're setting up server software. Using the form
<hostname>.<domainname>
Example: master.example.com.


Server host name [server.domain.loc]:

Warning: skipping DNS resolution of host server.domain.loc
The domain name has been determined based on the host name.

Please confirm the domain name [domain.loc]:

The kerberos protocol requires a Realm name to be defined.
This is typically the domain name converted to uppercase.

Please provide a realm name [DOMAIN.LOC]:
Certain directory server operations require an administrative user.
This user is referred to as the Directory Manager and has full access
to the Directory for system management tasks and will be added to the
instance of directory server created for IPA.
The password must be at least 8 characters long.

Directory Manager password:
Password (confirm):

The IPA server requires an administrative user, named 'admin'.
This user is a regular system account used for IPA server administration.

IPA admin password:
Password (confirm):
```

Рисунок 156

После этого необходимо ввести пароли менеджера директорий и администратора домена (admin). Внимание! В системе не должно быть пользователя с таким именем!

Далее система спросит настройки DNS-сервера, которые можно оставить по умолчанию (Рисунок 157).

```
Checking DNS domain domain.loc., please wait ...
Invalid IP address fe80::2dff:6ba5:3f2b:1975 for server.domain.loc: cannot use link-local IP address fe80::2dff
:6ba5:3f2b:1975
Do you want to configure DNS forwarders? [yes]:
Following DNS servers are configured in /etc/resolv.conf: 192.168.1.1
Do you want to configure these servers as DNS forwarders? [yes]:
All DNS servers from /etc/resolv.conf were added. You can enter additional addresses now:
Enter an IP address for a DNS forwarder, or press Enter to skip:
Checking DNS forwarders, please wait ...
DNS server 192.168.1.1 does not support DNSSEC: ответ на запрос ". SOA" не содержит подписи DNSSEC (нет данных
RRSIG)
Please fix forwarder configuration to enable DNSSEC support.

DNS server 192.168.1.1: ответ на запрос ". SOA" не содержит подписи DNSSEC (нет данных RRSIG)
Please fix forwarder configuration to enable DNSSEC support.
WARNING: DNSSEC validation will be disabled
Do you want to search for missing reverse zones? [yes]:
Checking DNS domain 1.168.192.in-addr.arpa., please wait ...
Do you want to create reverse zone for IP 192.168.1.100 [yes]:
Please specify the reverse zone name [1.168.192.in-addr.arpa.]:
Checking DNS domain 1.168.192.in-addr.arpa., please wait ...
Using reverse zone(s) 1.168.192.in-addr.arpa.
Do you want to configure chrony with NTP server or pool address? [no]:
```

Рисунок 157

Далее необходимо согласиться с запуском установки IPA-сервера с предложенными настройками, введя `yes` в знак согласия на вопрос установщика (Рисунок 158).

```
The IPA Master Server will be configured with:
Hostname:       server.domain.loc
IP address(es): 192.168.1.100
Domain name:    domain.loc
Realm name:     DOMAIN.LOC

The CA will be configured with:
Subject DN:   CN=Certificate Authority,O=DOMAIN.LOC
Subject base: O=DOMAIN.LOC
Chaining:     self-signed

BIND DNS server will be configured to serve IPA domain with:
Forwarders:       192.168.1.1
Forward policy:   only
Reverse zone(s):  1.168.192.in-addr.arpa.

Continue to configure the system with these values? [no]: yes
```

Рисунок 158

После нажатия на клавишу [ENTER] будет запущена установка сервера, она может продолжаться достаточно длительное время.

При успешной установке сервера экран консоли должен выглядеть как продемонстрированно на рисунке 159.

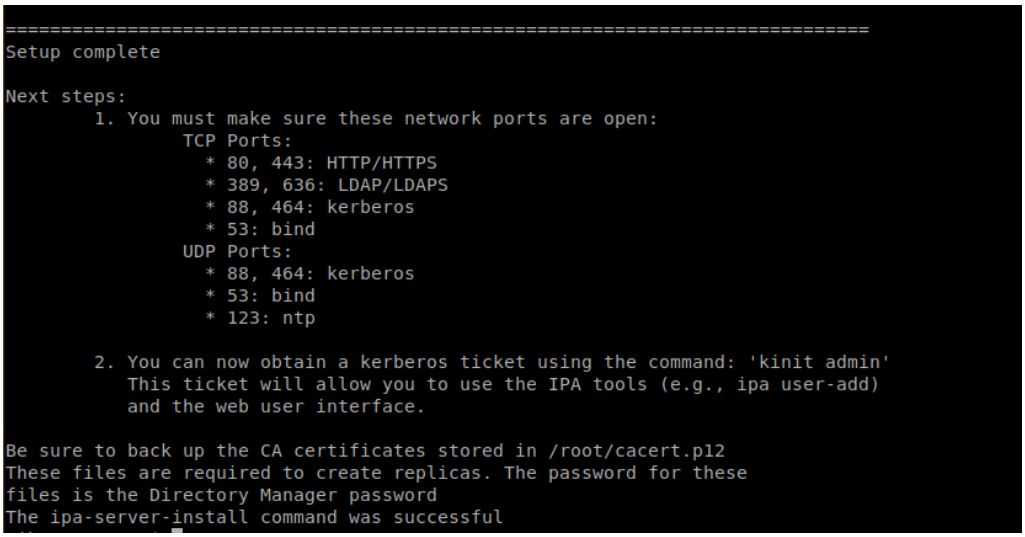


Рисунок 159

15.4.4. Проверка установки сервера

Для проверки того, что сервер установлен правильно, после его установки с рабочей станции, настроенной по инструкции выше, необходимо использовать команду:

```
ping server
```

Результат должен быть таким как показано на рисунке Рисунок 160. Такой результат показывает, что рабочая станция посылает корректные запросы по имени DNS-сервер и имеет правильные настройки.

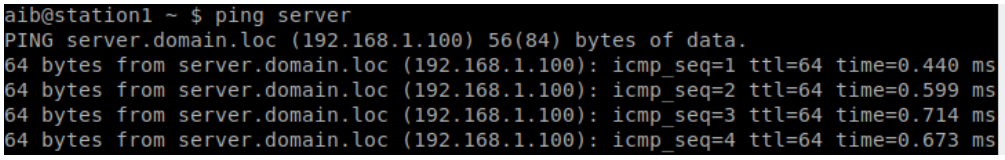


Рисунок 160

Перед дальнейшей настройкой станцию рекомендуется перезагрузить.

15.4.5. Добавление доменных пользователей

Для удобства добавления доменных пользователей рекомендуется использовать web-интерфейс.

Для доступа к нему откройте любой браузер в системе и введите адрес вашего IPA-сервера. В рассматриваем нами для примера случае это - *server.domain.loc.*

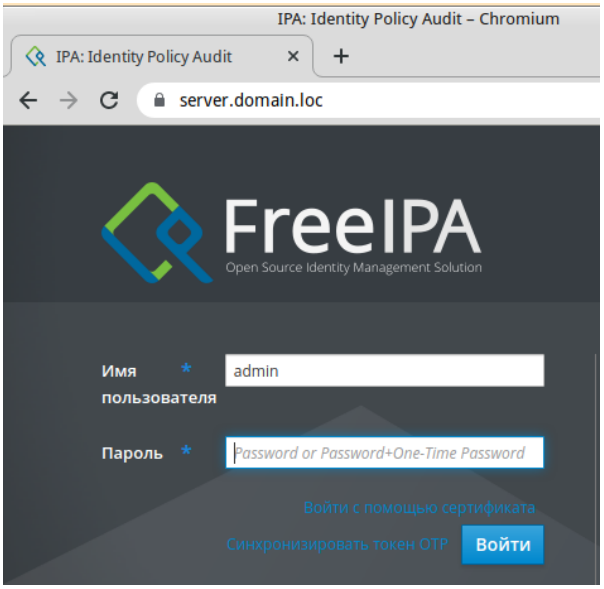


Рисунок 161

Далее на открывшейся странице введите имя пользователя (admin) и пароль, который вы задавали при установке сервера IPA. После нажатия на кнопку [Войти] откроется интерфейс добавления пользователей (Рисунок 162).

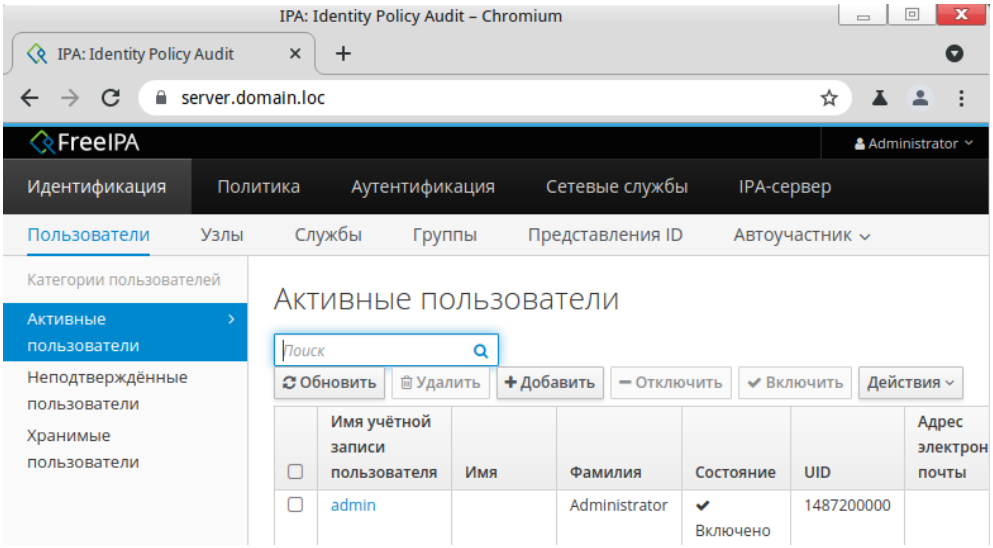


Рисунок 162

Добавьте нового пользователя, нажав на кнопку [Добавить], после чего откроется окно с запросом дополнительной информации о новом пользователе (Рисунок 163). Заполните все необходимые поля и сохраните введенную информацию.

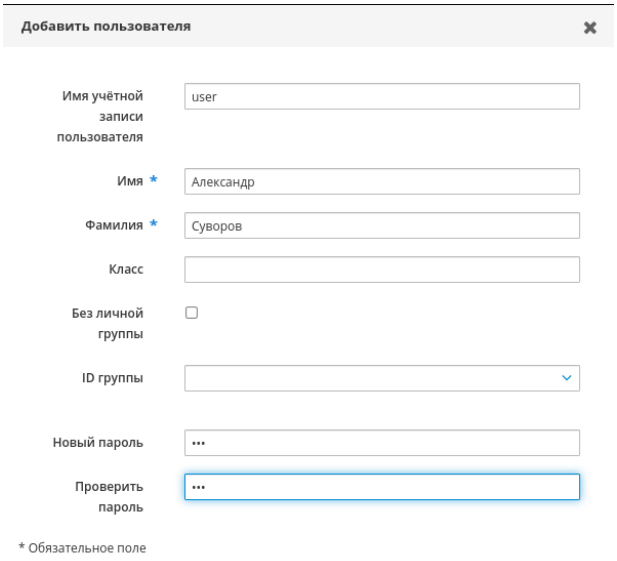


Рисунок 163

15.4.6. Добавление станции в домен и первый вход

Теперь, когда на сервере есть по крайней мере один доменный пользователь, попробуйте ввести имя станции *station1.domain.loc* (в которой уже предварительно настроено имя и проверено сетевое соединение) в домен и войти в него под созданным пользователем. Если имя станции было изменено уже после инсталляции, то рекомендуется сначала перезагрузить систему.

Для ввода станции в домен IPA введите в консоли команду

```
sudo ipa-client-install --mkhomedir
```

Также можно воспользоваться графическим способом входа: войдите в [Параметры системы] рабочей станции и выберете значок [Аутентификация] и далее выберете параметр **IPA** (Рисунок 164).

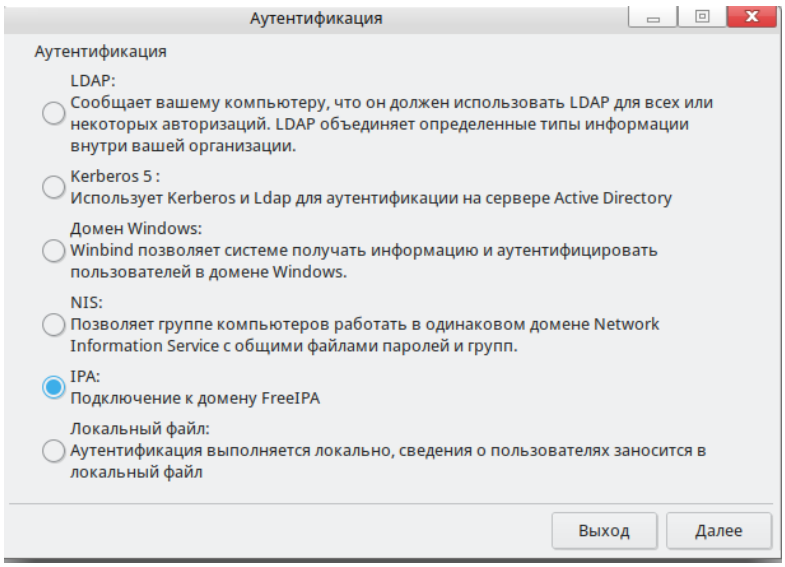


Рисунок 164

Потребуется ввести имя администратора IPA и его пароль (который задавался при инсталляции IPA-сервера) и нажать на кнопку [Подключиться] (Рисунок 165).

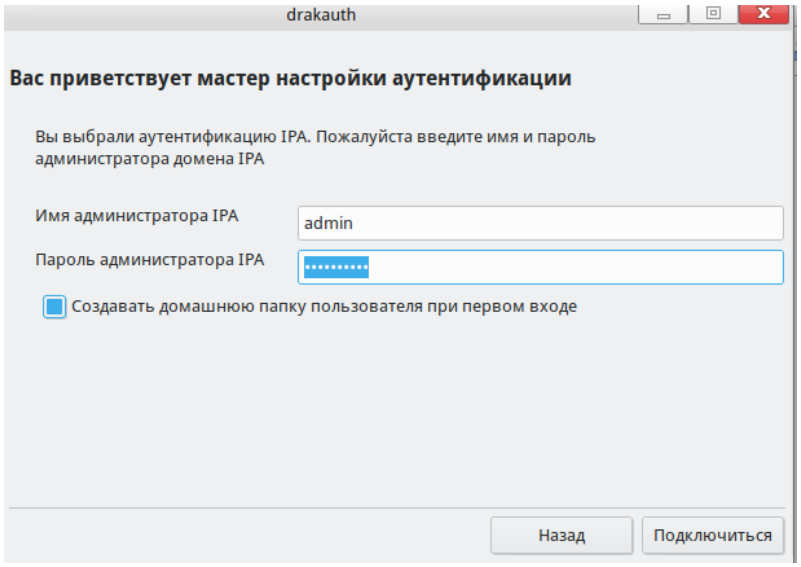


Рисунок 165

Подключение может занять некоторое время, после успешного установления соединения появиться соответствующее окно с сообщением.

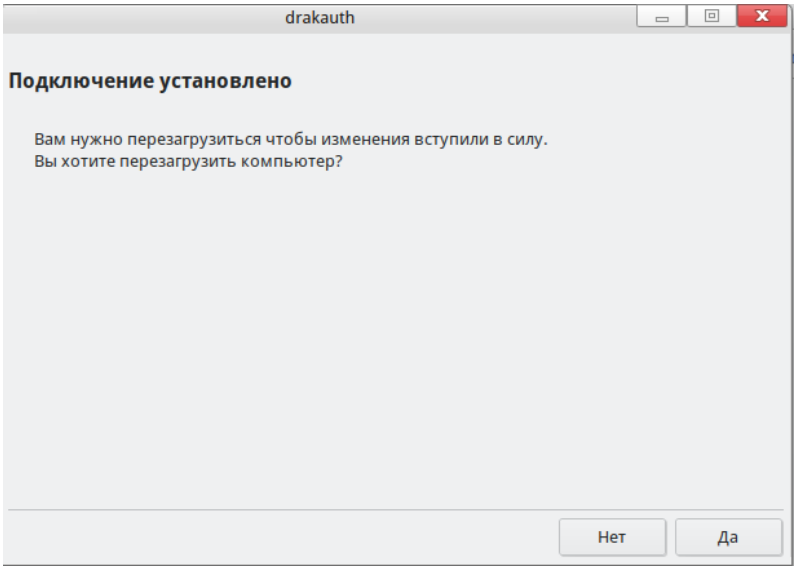


Рисунок 166

Далее рекомендуется перезагрузить рабочую станцию и выполнить следующий вход под доменным пользователем.

При первом входе будет предложено сменить пароль.

15.4.7. Настройка SELinux-пользователя для доменного пользователя IPA

По умолчанию новые доменные пользователи IPA будут являться SELinux-пользователями user_u и им будет сопоставлен нулевой уровень доступа, в этом можно убедиться, просмотрев информацию о контексте безопасности нажав на зеленый значок

в правом нижнем углу экрана (Рисунок 167).

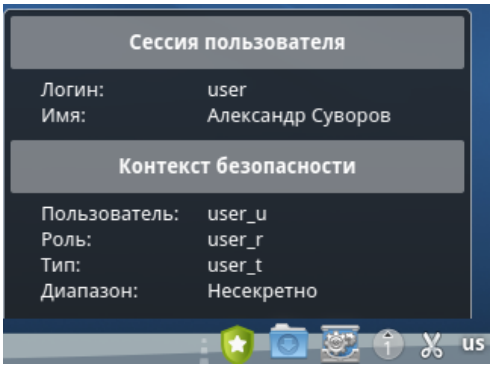


Рисунок 167

Если необходимо наделить пользователя большие права, проведите соответствующие настройки в web-интерфейсе IPA-сервера, а именно: перейдите во вкладку [Политика] → [Списки пользователей SELinux] (Рисунок 168).

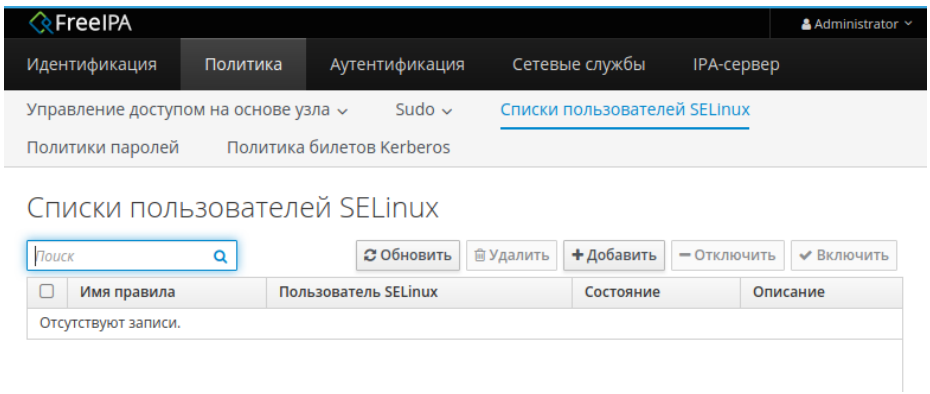


Рисунок 168

По умолчанию в данных списках отсутствуют записи. Введем новую группу, для примера назовем ее «Пользователи с доступом к секретным документа» и наделим ее контекстом **user_u:s0-s3** и сохраним ее (Рисунок 169).

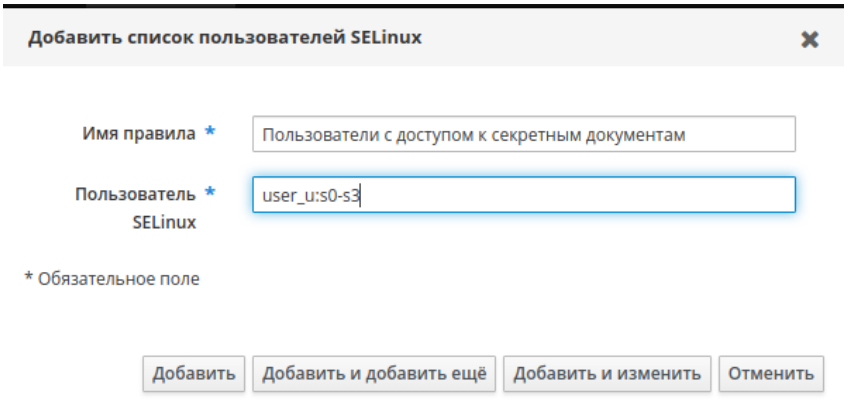


Рисунок 169

Далее добавьте в созданный список пользователя с возможностью входа с любой станции (узла) (Рисунок 170).

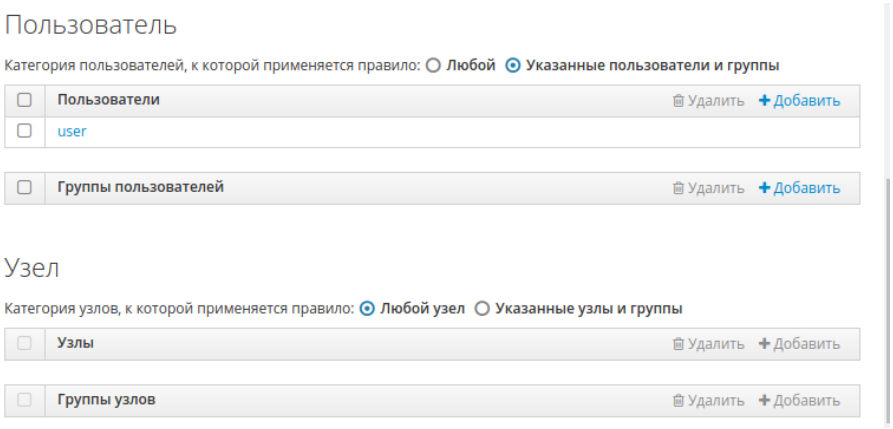


Рисунок 170

Для совершенно нового пользователя системы вышеописанных настроек было бы достаточно, но, если рассматриваемый пользователь уже работал в системе, для изменения его настроек секретности необходимо дополнительно изменить их в программе "Администрирование SELinux".

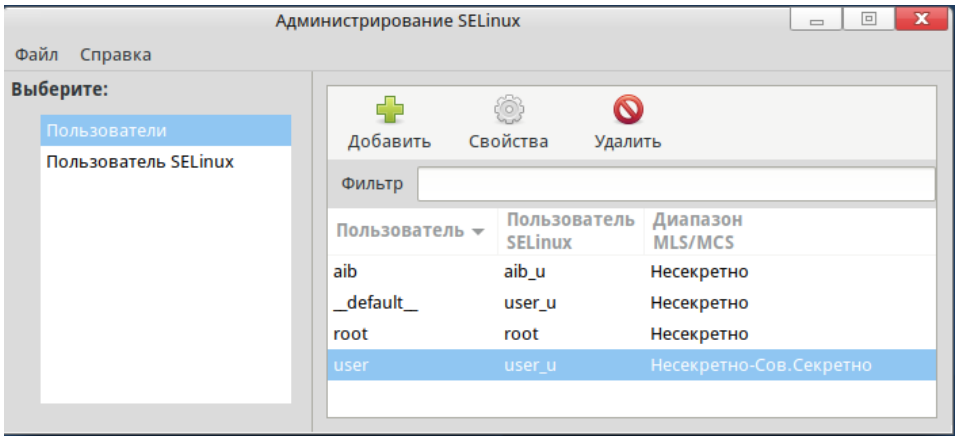


Рисунок 171

После внесения изменений рассматриваемый доменный пользователь получит доступ к созданию документов высшей степени секретности (s3, "Сов. Секретно), что будет отражено при входе пользователя в систему (Рисунок 172).

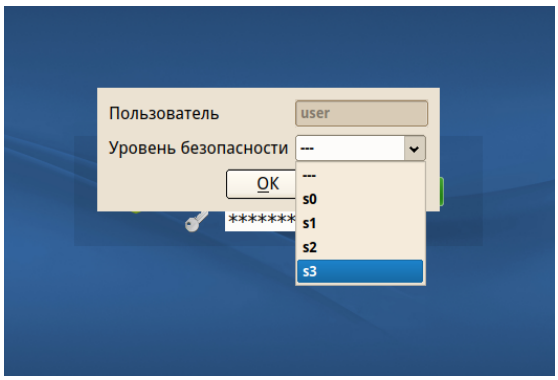


Рисунок 172

16. НАСТРОЙКА СЕТЕВЫХ СЛУЖБ

16.1. Настойка сервера NTP

Уровни NTP

NTP (Network Time Protocol — протокол сетевого времени) — сетевой протокол для синхронизации внутренних часов ПК с высокоточными серверами.

Серверы NTP классифицируются согласно дистанции их синхронизации с атомными часами, являющимися источником сигналов времени. Серверы рассматриваются как упорядоченные по уровням (или стратам, Stratum) от самого первого (1) наверху до пятнадцатого (15) в самом низу. Атомные часы считаются нулевым уровнем (0), поскольку являются непосредственным источником времени, но пакеты нулевого уровня никогда не посылаются в интернет. Все атомные часы нулевого уровня привязаны к серверу, который считается уровнем номер 1. Серверы первого уровня посылают в интернет-пакеты с пометкой Stratum 1 (первый уровень). Сервер, синхронизация которого происходит с использованием пакетов, помеченных как Stratum n, принадлежит к следующему, более низкому, уровню, и его пакеты помечаются как Stratum n+1. Серверы одного и того же уровня могут обмениваться пакетами друг с другом, но относятся к одному и тому же уровню, т. е. на один уровень ниже лучшего коррелятора, с которым они могут синхронизироваться. Уровень назначения 16 (Stratum 16) используется для обозначения того, что сервер в настоящий момент не выполняет синхронизацию с каким-либо надежным источником времени.

По умолчанию для систем, находящихся уровнем ниже, клиенты NTP работают как серверы.

Далее сделаем краткий обзор уровней NTP

Уровень 0, Stratum 0

- атомные часы и их сигналы, передаваемые по радио и GPS;
- система глобального позиционирования GPS (Global Positioning System);
- системы мобильной телефонной связи;
- низкочастотное радиовещание: станция WWVB (Колорадо, США), станции JJY-40 и JJY-60 (Япония), станция DCF77 (Германия) и станция MSF (Великобритания).

Вышеуказанные сигналы можно принимать с помощью специально предназначенных для этого устройств, обычно подключенных через интерфейс RS-232 к системе, используемой как сервер времени организации или сайтов.

Уровень 1, Stratum 1

ПК с подключенными к нему радио-часами, часами GPS или атомными часами.

Уровень 2, Stratum 2

Читает данные с уровня 1, служит сервером для нижнего уровня

Уровень 3, Stratum 3

Читает данные с уровня 2, служит сервером для нижнего уровня

Уровень n+1, Stratum n+1

Читает данные с уровня n, служит сервером для нижнего уровня

Уровень 15, Stratum 15

Читает данные с уровня 14; это самый низкий уровень.

Процесс снижается до уровня 15, являющегося нижайшим действительным уровнем. Метка Stratum 16 используется для обозначения статуса «без синхронизации».

UTC, часовые пояса и переход на летнее время

Поскольку NTP функционирует полностью на основе UTC (всемирное координированное время, Coordinated Universal Time), часовые пояса и переход на летнее время применяются в системах локально. Файл /etc/localtime является копией или символьной ссылкой на файл информации о часовом поясе из каталога /usr/share/zoneinfo. Системные часы могут отсчитывать местное время или UTC, что указывается в третьей строке файла /etc/adjtime, которая может иметь значение либо «LOCAL» либо «UTC» для обозначения того, как именно были настроены системные часы (т. е. часы реального времени, RTC). Как правило, рекомендуется настраивать часы реального времени на UTC, чтобы избежать различных проблем, связанных с переходом на летнее время.

Файл смещения

В файле смещения (drift file) обычно хранится значение смещения частоты между системными часами, работающими с номинальной частотой, и частотой, которая требуется для того, чтобы часы оставались синхронизированными с UTC. При наличии этого значения в файле смещения оно читается во время старта системы и используется для коррекции источника времени. Использование файла смещения сокращает время, требуемое для получения стабильного и точного времени. Расчет значения и соответствующая замена файла смещения производится один раз в час службой ntpd. Файл смещения заменяется, а не обновляется, поэтому важно, чтобы у службы ntpd имелись права на запись в соответствующий каталог.

Возможности аутентификации для NTP

В NTPv4 была добавлена поддержка для архитектуры системы безопасности Autokey (автоключ), основанной на открытом асимметричным шифровании, и в тоже

время по-прежнему поддерживающей шифрование с симметричным ключом. На странице руководства ntp_auth(5) описываются параметры и команды аутентификации для ntpd.

Злоумышленник может попытаться прервать выполнение службы с помощью отправки пакетов с неправильной информацией о времени. В системах, использующих открытый пул серверов NTP, риск снижается наличием нескольких серверов NTP в списке общедоступных серверов файла /etc/ntp.conf. Если только один источник времени будет скомпрометирован, ntpd проигнорирует этот источник. Администратор должен выполнить оценку рисков и обдумать влияние неточного времени на ресурсы подотчетной организации. При наличии внутренних источников времени нужно обдумать шаги, которые необходимо выполнить для защиты сети, по которой распространяются пакеты NTP. Если в итоге будет принято решение, что риски приемлемы, аутентификацию можно не использовать.

Для широковещательного и группового режимов по умолчанию требуется аутентификация. При использовании доверенной сети аутентификацию можно отключить при помощи директивы disable auth в файле ntp.conf. Настроить аутентификацию можно при помощи симметричных ключей SHA1 или MD5 или же с помощью открытого асимметричного шифрования по схеме автоключа. Их описания содержатся на страницах руководств ntp_auth(8) и ntp-keygen(8).

Настройка симметричной аутентификации с использованием ключа

Для настройки симметричной аутентификации с использованием ключа добавьте следующий параметр после команды server или peer:

```
key <число>
```

Здесь <число> может принимать значения от 1 до 65534 включительно. Этот параметр включает использование в пакетах кода проверки подлинности сообщения MAC и используется с командами peer, server, broadcast и manycastclient. В файле /etc/ntp.conf этот параметр используется следующим образом:

```
server 192.168.1.1
key 10
broadcast 192.168.1.255
key 20
manycastclient 239.255.254.254
key 30
```

Конфигурационный файл NTP

Демон ntpd читает параметры конфигурационного файла при запуске системы или во время перезапуска службы. Местоположение файла по умолчанию — /etc/ntp.conf.

Просмотреть файл можно с помощью команды cat:

```
$ cat /etc/ntp.conf
```

Команды конфигурации кратко описываются в настоящем документе. **Настройка NTP** и более подробно — на странице руководства ntp.conf.

Ниже объясняется содержимое конфигурационного файла по умолчанию.

Раздел файла смещения (driftfile)

Здесь указывается путь до файла смещения. Значение по умолчанию — `driftfile /var/lib/ntp/drift`.

При смене местоположения файла убедитесь, что служба ntpd имеет права на запись в этот каталог. Файл содержит только значения, используемые для настройки частоты системных часов после каждого старта системы или старта службы.

Следующая запись настраивает параметры контроля доступа по умолчанию:

```
restrict default nomodify notrap nopeer noquery
```

- `nomodify` - запрещает внесение изменений в параметры;
- `notrap` - запрещает ловушки протокола контроля сообщений ntpdc;
- `nopeer` - запрещает создание связей между узлами одноранговой сети;
- `noquery` - запрещает ответ на запросы ntpq и ntpdc, но разрешает запросы времени.

Запросы `ntpq` и `ntpdc` могут быть использованы злоумышленниками в атаках с лавинообразным умножением данных (amplification attacks), поэтому не следует удалять параметр `noquery` из параметров команды `restrict` по умолчанию в общедоступных системах.

Адреса в диапазоне 127.0.0.0/8 часто требуются разным процессам или приложениям. Как строка `restrict default` предотвращает доступ ко всему, не разрешенному явно, так и доступ к стандартному адресу петли (loopback) для IPv4 и IPv6 разрешается в следующих строках:

```
# the administrative functions.
restrict 127.0.0.1
restrict ::1
```

Явно требуемые приложениями адреса можно добавить ниже.

Хосты из локальной сети запрещаются записью `restrict default`, описанной выше. Чтобы изменить это поведение, например, разрешить только запросы времени и статистики из сети 192.0.2.0/24, требуется запись следующего формата:

```
restrict 192.0.2.0
mask 255.255.255.0
```

```
nomodify
notrap
nopeer
```

Чтобы разрешить полный доступ для конкретного хоста, например, 192.0.2.250/32, требуется запись следующего формата:

```
restrict 192.0.2.250
```

Если маска не указана явно, применяется маска 255.255.255.255.

Команды restrict объясняются на странице руководства ntp_acc.

Раздел общедоступных серверов (public servers)

По умолчанию файл ntp.conf содержит две записи для общедоступных серверов:

```
server ntp.rosalinux.ru iburst
server ntp2.rosalinux.ru iburst
```

Раздел многоадресных широковещательных серверов (broadcast multicast servers)

По умолчанию в файле ntp.conf содержится несколько закомментированных примеров. В основном эти примеры не требуют разъяснений. Объяснение конкретных команд см. в разделе 0 **Настройка NTP**. При необходимости добавляйте нужные команды непосредственно под примерами.

Обратите внимание, что, когда клиентская программа DHCP, dhclient, получает список серверов NTP от сервера DHCP, они добавляются в ntp.conf, после чего служба NTP перезапускается. Для отключения этого поведения добавьте в файл /etc/sysconfig/network запись PEERNTP=no.

Файл sysconfig службы ntpd

Файл читается начальным сценарием ntpd при запуске службы. Содержимое файла по умолчанию:

```
# Command line options for ntpd
OPTIONS="-g"
```

Параметр `-g` разрешает ntpd проигнорировать предел смещения в 1000 секунд и попробовать синхронизировать время даже в том случае, если смещение составляет более 1000 секунд, но только при загрузке системы. Без этого параметра, если смещение составляет больше 1000 секунд, ntpd завершит работу. ntpd также завершит работу даже и при наличии параметра -g, если после загрузки системы был произведен перезапуск службы NTP, и смещение составляет больше 1000 секунд.

Установка демона NTP (ntpd)

Сервер сетевого времени NTP реализован в виде демона (или службы) ntpd,

который содержится в пакете ntp.

Чтобы установить ntpd, выполните следующую команду с привилегиями суперпользователя root:

```
sudo dnf install ntp
```

Чтобы включить запуск ntpd при загрузке системы, выполните:

```
# systemctl enable ntpd
```

Чтобы проверить, выполняется ли служба ntpd и настроена ли она на автоматический запуск при старте системы, выполните следующую команду:

```
$ systemctl status ntpd
```

Чтобы получить краткую информационную сводку от службы ntpd, выполните:

```
$ ntpstat
unsynchronised
time server re-starting
polling server every 64 s
$ ntpstat
synchronised to NTP server (10.5.26.10) at stratum 2
time correct to within 52 ms
polling server every 1024 s
```

Настройка NTP

Чтобы изменить параметры по умолчанию службы NTP в файле /etc/ntp.conf, используйте текстовый редактор, запущенный с правами root. Файл устанавливается вместе со службой ntpd. На странице руководства ntp.conf описаны параметры, которые можно использовать в конфигурационном файле, помимо команд доступа и ограничения скорости ответа, которые объясняются на странице руководства ntp_acc.

Настройка контроля доступа к службе NTP

Для запрета или контроля доступа к запущенной в системе службе NTP используйте команду restrict в файле ntp.conf. См. закомментированный пример:

```
# Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
```

Команда restrict имеет следующий вид:

```
restrict <параметр>
```

Здесь <параметр> — это один или несколько следующих:

– ignore — игнорируются все пакеты, включая запросы ntpq и ntpdc;

– kod — для снижения количества нежелательных запросов необходимо послать пакет «Kiss-o'-death»;

– limited — не отвечать на запросы о предоставлении службы времени, если пакет нарушает значения ограничения скорости, установленные по умолчанию, или же указанные командой discard. На запросы ntpq и ntpdc этот параметр не влияет;

– lowpriotrap — ловушкам, установленным хостами, отвечающими указанному шаблону, присваивается низкий приоритет.

– nomodify — запрещает любые попытки изменения параметров;

– noquery — запрещает ответы на запросы ntpq и ntpdc, но не на запросы времени;

– nopeer — предотвращает создание связей между узлами одноранговой сети;

– noserve — сбрасывает все пакеты, кроме запросов ntpq и ntpdc;

– notrap — запрещает создание ловушек для управляющих сообщений ntpdc;

– notrust — сбрасывает все пакеты с аутентификацией без шифрования;

– ntpport — изменяет алгоритм сравнения таким образом, что ограничение применяется только если исходный порт является стандартным портом NTP UDP — 123;

– version — сбрасывает все пакеты, не совпадающие с текущей версией NTP.

Чтобы доступ с ограничением скорости трафика запрещал ответ на все запросы, соответствующая команда restrict должна иметь параметр limited. Если ntpd должен отвечать пакетом KoD, команда restrict должна иметь оба параметра — и limited, и kod.

Запросы ntpq и ntpdc могут использованы в атаках с лавинообразным умножением данных, поэтому не удаляйте параметр noquery из параметров по умолчанию для команды restrict в общедоступных системах.

Настройка доступа с ограничением интенсивности трафика для службы NTP

Чтобы включить ограничение по скорости трафика для доступа к службе NTP, работающей в системе, добавьте параметр limited для команды restrict. Если этот параметр по умолчанию по каким-либо причинам не используется, применяйте команду discard, как объясняется ниже.

Команда discard имеет следующий вид:

```
discard [average <значение>]
minimum <значение>]
monitor <значение>]
```

Здесь:

– average — указывает минимальный средний разрешенный интервал между пакетами, принимает аргумент в log2 секунд. Значение по умолчанию — 3 (23 равно 8 секундам);

– minimum — указывает минимальный разрешенный интервал между пакетами,

принимает аргумент в log2 секунд. Значение по умолчанию — 1 (21 равно 2 секундам);

– monitor — указывает возможность сброса для пакетов при превышении разрешенного ограничения. Значение по умолчанию — 3000 секунд. Этот параметр предназначается для серверов, получающих 1000 или более запросов в секунду.

Примеры команды discard:

```
discard average 4
discard average 4
minimum 2
```

Добавление адреса узла одноранговой сети

Чтобы добавить адрес узла одноранговой сети, то есть адрес сервера, на котором выполняется служба NTP и который расположен на том же уровне (stratum), в файле ntp.conf используется команда peer:

```
peer <адрес>
```

Здесь <адрес> — это одиночный адрес IP или имя, разрешаемое DNS. Адрес должен принадлежать системе, про которую известно, что она находится на одном уровне NTP (stratum) с вашей системой. У каждого узла одноранговой сети должен быть по крайней мере один источник времени, отличный от источников времени другого узла. Обычно узлами одноранговой сети являются системы в рамках одного и того же административного управления.

Добавление адреса сервера

Чтобы добавить адрес сервера, на котором выполняется служба NTYP и который находится на более высоком уровне (stratum) NTP, в файле ntp.conf используется команда server:

```
server <адрес>
```

Здесь <адрес> — это одиночный адрес IP или имя, разрешаемое DNS. Это адрес удаленного запрашиваемого сервера или сервера местных справочных часов, с которого нужно получать пакеты.

Добавление адреса широковещательного или многоадресного сервера

Чтобы добавить широковещательный или многоадресный адрес назначения, то есть адрес, на который нужно посылать широковещательные или многоадресные пакеты NTP, в файле ntp.conf используется команда broadcast.

Широковещательные и многоадресные режимы по умолчанию требуют аутентификации.

Команда broadcast имеет следующий вид:

```
broadcast <адрес>
```

Здесь <адрес> — это широковещательный или множественный IP-адрес, на который должны посылаться пакеты.

Эта команда превращает систему в широковещательный сервер NTP. Широковещательный адрес предполагает адрес IPv4 255.255.255.255. по умолчанию; маршрутизаторы не передают широковещательных сообщений. Широковещательный адрес должен быть адресом IPv4 класса D или адресом IPv6. Администрация адресного пространства интернет (IANA) присвоила службе NTP адреса многоадресной рассылки IPv4 224.0.1.1 и IPv6 FF05::101 (внутрисайтовый). Также можно использовать многовещательные адреса IPv4 административного назначения, как опоясано в документе RFC 2365 (https://www.rfceditor.org/info/rfc2365).

Добавление клиентского адреса manycast

Чтобы добавить клиентский адрес manycast, то есть настроить адрес многоадресного вещания так, чтобы он мог использоваться для обнаружения серверов NTP, в файле ntp.conf используется команда manycastclient:

```
manycastclient <адрес>
```

Здесь <адрес> — это IP-адрес многоадресного вещания, с которого нужно получать пакеты. На этот адрес клиент посылает запрос, среди ответов выбираются лучшие серверы, другие игнорируются. Затем соединение NTP использует одноадресные связи, как если бы обнаруженные серверы NTP были указаны в файле ntp.conf.

Эта команда превращает систему в клиент NTP. Система может быть одновременно как клиентом, так и сервером.

Добавление широковещательного клиентского адреса

Чтоб добавить широковещательный клиентский адрес, то есть настроить широковещательный адрес так, чтобы он отслеживался широковещательными пакетами NTP, в файле ntp.conf используется команда broadcastclient:

```
broadcastclient
```

Команда активирует получение широковещательных сообщений. По умолчанию требуется аутентификация.

Эта команда превращает систему в клиент NTP. Система может быть одновременно как клиентом, так и сервером.

Добавление серверного адреса manycast

Чтоб добавить серверный адрес manycast, то есть настроить адрес так, чтобы клиенты могли обнаруживать сервер с помощью многоадресных пакетов NTP, в файле ntp.conf используется команда manycastserver:

```
manycastserver <адрес>
```

Команда разрешает рассылку многоадресных сообщений, где <адрес> — это адрес, на который нужно посылать сообщения. Чтобы избежать перебоев в работе службы, для этой команды необходима аутентификация.

Эта команда превращает систему в сервер NTP. Система может быть одновременно как клиентом, так и сервером.

Добавление многоадресного адреса клиента

Чтобы добавить многоадресный клиентский адрес, то есть настроить многоадресный адрес так, чтобы он отслеживался многоадресным пакетами NTP, в файле ntp.conf используется команда multicastclient:

```
multicastclient <адрес>
```

Команда разрешает получение многоадресных сообщений, где <адрес> — это адрес подписки. Чтобы избежать перебоев в работе службы, для этой команды необходима аутентификация.

Эта команда превращает систему в клиент NTP. Система может быть одновременно как клиентом, так и сервером.

Параметр burst

Использование параметра burst для общедоступного сервера считается некорректным. Не используйте этот параметр на общедоступных серверах NTP. Используйте ее только для приложений в рамках своей организации.

Для повышения общего качества статистики смещения времени добавьте следующий параметр после команды server:

```
burst
```

В каждый интервал опроса при ответе сервера система будет посылать серию до восьми пакетов вместо обычного одного пакета.

Параметр iburst

Для улучшения времени, используемого для начальной синхронизации, добавьте следующий параметр после команды server:

```
Iburst
```

Если сервер недоступен, будет послана серия из 8 пакетов вместо обычного одного. Промежуток между пакетами обычно составляет 2 секунды; тем не менее, промежуток между первым и вторым пакетами можно изменить с помощью команды calldelay для получения дополнительного времени для завершения звонка модема или ISDN. Используется вместе с командой server для сокращения времени начальной синхронизации. Iburst является параметром по умолчанию в конфигурационном файле.

Приведем пример создания самого простого сервера NTP, с которого ваши

клиенты смогут получать данные для синхронизации времени. Эта инструкция будет полезна в случае, если у вас есть закрытая сеть без выхода в интернет.

Для настройки сервера точного времени ntpd выполните следующие действия:

1. Установить сервис ntp, если он еще не установлен, следующей командой:

```
dnf install ntp
```

2. Чтобы использовать ntpd в качестве службы сетевого времени по умолчанию, необходимо остановить и отключить демон chronyd. Выполните следующие команды:

```
# systemctl stop chronyd
# systemctl disable chronyd
```

3. Для настройки автоматического запуска демона при загрузке системы используйте специальную команду:

```
systemctl enable ntpd
```

4. Отредактируйте конфигурационный файл сервера /etc/ntp.conf. Он должен содержать как минимум следующие данные:

```
driftfile /var/lib/ntp/ntp.drift
statsdir /var/log/ntpstats/
#каталог для сбора статистики
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable
server 127.127.1.0
fudge 127.127.1.0 stratum 0
restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery
restrict 127.0.0.1
restrict <ваша сеть> mask <маска вашей сети>
nomodify notrap
```

5. Перезагрузите демон NTP:

```
systemctl restart ntpd
```

6. Добавьте ntp в автозагрузку:

```
systemctl enable ntpd
```

Расшифровка основных параметров

– driftfile — указывает файл для хранения информации о частоте смещения времени. В этом файле хранится значение, получаемое в результате предшествующих

корректировок времени. Если внешние NTP-серверы по той или иной причине становятся недоступными, значение будет взятого из него;

– statsdir — каталог для сбора статистики работы сервиса;

– server — укажите, если ваш сервер будет сам обновлять свое время с некоторого внешнего сервера. Если верхних серверов NTP нет, то указывается 127.127.1.0. В этом случае будет использоваться локальное время ОС;

– restrict — ограничивает работу сервиса в определенной подсети, например:

```
restrict 192.168.1.0
mask 255.255.255.0
nomodify notrap
```

Сервер NTP будет отвечать на запросы только из подсети 192.168.1.0/24. Крайне рекомендуется использовать данный параметр, чтобы ограничить нагрузку на сервер.

Дополнительные источники информации

Дополнительную информацию о NTP и ntpd можно найти в следующих руководствах:

– страница руководства ntpd — подробное описание ntpd, включая параметры командной строки;

– страница руководства ntp.conf — содержит информацию о том, как настраивать связи с серверами и узлами одноранговой сети;

– страница руководства ntpq — описывается утилита запросов NTP, используемая для выполнения запросов и отслеживания сервера NTP;

– страница руководства ntpdc — описывается утилита службы ntpd, используемая для запросов и смены статуса ntpd;

– страница руководства ntp_auth — описывается параметры ntpd, команды и управление ключами аутентификации для ntpd;

– страница руководства ntp_keygen — описывается создание открытых и частных ключей для ntpd;

– страница руководства ntp_acc — описывается контроль доступа с использованием команды restrict;

– страница руководства ntp_mon — описываются возможности мониторинга для сбора статистики;

– страница руководства ntp_clock — описываются команды для настройки опорной частоты;

– страница руководства ntp_misc — описываются дополнительные параметры;

– страница руководства ntp_decode — список слов состояния, сообщений о

событиях и кодах ошибок, используемых для отчетов и наблюдений за ntpd;

– страница руководства ntpstat — описывается утилита, используемая для получения статуса синхронизации демона NTP, выполняемого на локальной машине;

– страница руководства ntptime — описывается утилита для чтения и установки переменных времени в ядре;

– страница руководства tickadj — описывается утилита для чтения (и возможной установки) тактовой длины.

16.2. Настойка сервера DHCP

Данная инструкция не претендует на полное описание всех возможностей работы сервиса dhcp, а предлагает простой способ настройки сервера динамической конфигурации сети для быстрого старта.

1) Для создания сервера dhcp необходимо установить соответствующую службу:

```
dnf install dhcp
```

2) Для настройки автоматического запуска демона при загрузке системы используйте специальную команду:

```
systemctl enable dhcpd
```

3) Необходимо настроить один из интерфейсов сервера на статический адрес из той подсети, которую будет раздавать клиентам, иначе демон не будет работать корректно.

Для настройки сервиса нужно сначала скопировать файл с типовой конфигурацией сервиса /usr/share/doc/dhcp-<версия>/dhcpd.conf.sample в каталог /etc/dhcp/, переименовав его в файл dhcpd.conf: `cp /usr/share/doc/dhcp-4.2.5/dhcpd.conf.example /etc/dhcp/dhcpd.conf`

После этого следует отредактировать файл /etc/dhcpd.conf, указав в нем нужные параметры:

```
mcedit /etc/dhcp/dhcpd.conf
```

Приведите файл к следующему виду:

```
option domain-name "test.dom";
option domain-name-servers 192.168.10.1;
default-lease-time 600;
max-lease-time 7200;
authoritative;
```

```
log-facility local7;
subnet 192.168.10.0 netmask 255.255.255.0 {
range 192.168.10.10 192.168.10.200;
option routers 192.168.10.254;
option broadcast-address 192.168.10.255;
}
```

В данном примере предполагается, что станции, получающие сетевые настройки, работают в домене test.dom с сервером DNS 192.168.10.1 и шлюзом по умолчанию 192.168.10.254 и получают IP-адреса в промежутке от 192.168.10.10 до 192.168.10.200 с маской подсети 255.255.255.0.

Описание параметров

– option domain-name — определяет имя домена. Глобальный параметр. По умолчанию для всех подсетей;

– option domain-name-servers — определяет список адресов серверов DNS через запятую. Глобальный параметр. По умолчанию для всех подсетей;

– default-lease-time — время аренды по умолчанию;

– max-lease-time — определяет максимально допустимое время аренды. Независимо от длительности аренды, фигурирующей в запросе клиента, этот срок не может превышать значение, заданное данным параметром;

– authoritative — означает, что в вашей сети данный сервер является ответственным за выдачу сетевых адресов;

– log-facility — определяет направление потока логов;

– subnet — основной логический блок конфигурации. Он определяет настройки для конкретной сети. В том числе в нем можно менять глобальные параметры, такие как domain-name, domain-name-servers и др.;

– range — диапазон IP-адресов, доступный для аренды;

– option routers — адрес маршрутизатора по умолчанию;

– option broadcast-address — адрес для широковещательной рассылки.

После сохранения изменений в конфигурационном файле необходимо перезагрузить сервис dhcpd:

```
/etc/init.d/dhcpd restart
```

16.3. Веб-сервер Apache

Веб-сервер, поставляемый в составе ОС РОСА «НИКЕЛЬ»— это Apache HTTP Server.

Отдельный каталог /tmp

Для повышения уровня защищенности системы юнит systemd выполняет демон httpd с использованием частного каталога /tmp, отдельно от системного каталога /tmp.

Схема конфигурации по пакетам

Файлы конфигурации, с помощью которых загружаются модули, располагаются в каталоге /etc/httpd/conf.modules.d/. Пакеты, предоставляющие дополнительные загружаемые модули для httpd, например, php, разместят файлы в этом каталоге. Для включения таких файлов в каталог /etc/httpd/conf.modules.d/ в файле /etc/httpd/conf/httpd.conf существует директива Include, следующая перед главным разделом. Это означает, что любые файлы конфигураций, располагающиеся в каталоге /conf.modules.d, обрабатываются до начала обработки основной информации файла httpd.conf. Директива IncludeOptional для файлов из каталога /etc/httpd/conf.d/ помещается в конце файла httpd.conf. Это означает, что файлы из каталога /etc/httpd/conf.d/ теперь обрабатываются после обработки основной информации из httpd.conf.

Некоторые конфигурационные файлы предоставляются пакетом httpd:

– /etc/httpd/conf.d/autoindex.conf — параметры индексации каталога mod_autoindex;

– /etc/httpd/conf.d/userdir.conf — параметры доступа в пользовательские каталоги, например http://test.dom/~username/. Такой доступ по умолчанию отключен из соображений безопасности;

– /etc/httpd/conf.d/welcome.conf — как и в предыдущих релизах, этот файл отвечает за страничку приветствия, показываемую по адресу http://localhost/ в отсутствие другой информации.

Модель обработки

В ОС РОСА «НИКЕЛЬ» используется только один бинарный файл httpd, а три модели MPM доступны в виде загружаемых модулей: worker, prefork (по умолчанию) и event. Отредактируйте файл /etc/httpd/conf.modules.d/00-mpm.conf согласно требованиям конкретной системы, добавляя и убирая символ комментария # так, чтобы загружался только один модуль MPM.

Аутентификация, авторизация и контроль доступа

Для управления аутентификацией, авторизацией и контролем доступа используется синтаксис Require, значительно отличающийся от директив Order, Deny и Allow. Подробности см. в официальной документации разработчика: http://httpd.apache.org/docs/2.4/howto/auth.html .

suexec

В целях повышения уровня безопасности системы исполняемый файл suexec больше не устанавливается как if пользователем root. Вместо этого у него появился набор битов, устанавливающих права на данной ФС для более строгого набора прав доступа. В дополнение к этому изменению бинарный файл suexec больше не использует файл журнала /var/log/httpd/suexec.log. Теперь сообщения журнала посылаются в syslog; по умолчанию они появляются в файле журнала /var/log/secure.

16.3.1. Выполнение службы httpd

В данном подразделе описывается, как запустить, остановить, перезапустить и проверить текущий статус сервера Apache HTTP. Прежде чем использовать службу httpd, убедитесь, что в системе установлен httpd. Это можно сделать, выполнив следующую команду:

```
sudo dnf install httpd
```

Запуск службы

Чтобы запустить службу httpd, выполните следующую команду с правами администратора (sudo -i):

```
# systemctl start httpd.service
```

Для автоматического запуска службы при загрузке системы выполите:

```
# systemctl enable httpd.service
```

Примечание. Если сервер Apache HTTP работает как защищенный сервер, при использовании зашифрованного закрытого ключа SSL после загрузки ПК потребуется ввести пароль.

Остановка службы

Чтобы остановить выполняющуюся службу httpd, выполните следующую команду с правами администратора (sudo -i):

```
# systemctl stop httpd.service
```

Чтобы предотвратить автоматический запуск службы при загрузке системы, выполните:

```
# systemctl disable httpd.service
```

Перезапуск службы

Существуют три разных способа перезапустить выполняющуюся службу httpd.

1) Чтобы полностью перезапустить службу, выполните следующую команду:

```
# systemctl restart httpd.service
```

Это действие останавливает выполняющуюся службу httpd и немедленно запускает ее снова. Эта команда используется после установки или удаления динамически загружаемого модуля, например, PHP.

2) Чтобы просто перезагрузить конфигурацию, выполните:

```
# systemctl reload httpd.service
```

Это действие заставит работающую службу httpd перезагрузить файл конфигурации. Все запросы, обрабатываемые в это время, будут прерваны, что может вызвать показ сообщения об ошибке в браузере клиента или неполную загрузку страницы.

3) Для перезагрузки конфигурации, не отражающейся на активных запросах, выполните:

```
# apachectl graceful
```

Это действие заставит работающую службу httpd перезагрузить файл конфигурации. Все запросы, обрабатываемые в это время, будут использовать старую конфигурацию.

Проверка статуса службы

Чтобы проверить, работает ли служба httpd, выполните следующую команду с с правами администратора (sudo -i):

```
# systemctl is-active httpd.service
```

Редактирование файлов конфигурации

При запуске служба httpd по умолчанию читает конфигурационные файлы из следующих местоположений в системе:

– /etc/httpd/conf/httpd.conf — главный файл;

– /etc/httpd/conf.d/ — вспомогательный каталог для конфигурационных файлов, включаемых в главный файл.

Хотя параметры по умолчанию подходят для большинства ситуаций, желательно познакомиться с некоторыми из наиболее важных параметров конфигурации. Обратите внимание: чтобы изменения конфигурации вступили в силу, сервер сначала нужно перегрузить.

Чтобы проверить конфигурацию на наличие ошибок, выполните следующую команду с правами администратора (sudo -i):

```
# apachectl configtest
```

Чтобы облегчить процесс устранения ошибок, рекомендуется сделать резервную копию исходного файла перед его изменением.

Работа с модулями

Являясь модульным приложением, служба httpd поставляется вместе с некоторым числом модулей, которые при необходимости можно динамически загружать и выгружать в рабочем режиме. В ОС РОСА «НИКЕЛЬ» эти модули располагаются в

каталоге /usr/lib64/httpd/modules/.

Загрузка модулей

Чтобы загрузить модуль, используйте директиву LoadModule в одном из конфигурационных файлов в каталоге /etc/httpd/conf.modules.d. Обратите внимание, что модули, предоставляемые в отдельных пакетах, часто имеют свой собственный конфигурационный файл в каталоге /etc/httpd/conf.d/.

Пример: загрузка динамического разделяемого модуля mod_ssl

```
loadModule ssl_module modules/mod_ssl.so
```

Дождавшись выполнения команды, перезагрузите сервер для обновления конфигурации.

Написание модулей

Администраторам, желающим написать свой собственный динамический разделяемый модуль, нужно убедиться в том, что в системе установлен пакет httpd-devel. Для этого выполните следующую команду с правами администратора (sudo -i):

```
sudo dnf install httpd-devel
```

В этом пакете содержатся файлы include, файлы заголовков и утилита Apache eXtenSion (apxs), необходимая для компиляции модуля.

После написания модуля соберите его с помощью следующей команды:

```
# apxs -i -a -c module_name.c
```

Если результат сборки был удачен, модуль можно загружать точно так же, как и любой другой модуль, идущий в составе сервера Apache HTTP.

16.3.2. Настройка межсетевого экрана для разрешения трафика HTTP и HTTPS

ОС РОСА «НИКЕЛЬ» по умолчанию не разрешает трафик HTTP и HTTPS. Чтобы дать возможность системе работать как веб-сервер, убедитесь, что службы, поддерживаемые firewalld, разрешают пропуск трафика HTTP и HTTPS сквозь межсетевой экран.

Чтобы включить HTTP в консоли, выполните следующую команду с правами администратора (sudo -i):

```
# firewall-cmd --add-service http
```

Чтобы включить HTTPS в консоли, выполните:

```
# firewall-cmd --add-service https
```

Обратите внимание, что эти изменения будут действовать только до следующей перезагрузки системы. Чтобы сделать это изменение постоянным, повторно выполните команду с параметром `--permanent`.

Проверка сетевого доступа для входящего трафика HTTPS и HTTPS

Чтобы проверить, какие службы разрешены в межсетевом экране, выполните следующую команду с правами администратора (sudo -i):

```
# firewall-cmd --list-all
```

В выводе команды вы должны увидеть строки, разрешающие входящие соединения для протоколов http и https.

16.3.3. Параметры файла /etc/httpd/conf/httpd.conf

User http

По соображениям безопасности при запуске сервера Apache от имени суперпользователя (напрямую или через скрипт инициализации) происходит смена идентификатора пользователя (UID), от имени которого выполняется процесс сервера. По умолчанию используется пользователь http, который создается при установке и не имеет привилегированных полномочий в системе.

Listen 80

Это порт, через который Apache принимает входящие соединения. Если сервер имеет выход в интернет через маршрутизатор, необходимо будет настроить перенаправление этого порта.

Если Apache используется для разработки и тестирования, лучше разрешить только локальный доступ к нему. Для этого укажите `Listen 127.0.0.1:80`.

ServerAdmin you@test.dom

Адрес электронной почты администратора, который будет выводиться, например, на странице ошибки Apache.

DocumentRoot "/srv/http"

Это корневой каталог Apache, в котором можно разместить ваши веб-страницы.

Измените его, если нужно, но не забудьте также поменять путь в директиве `<Directory "/srv/http">` на новое расположение DocumentRoot, иначе вы, скорее всего, получите сообщение об ошибке «403 Error» (недостаточно полномочий) при попытке получить доступ к новому корневому каталогу Apache. Также не забудьте изменить строку Require all denied на Require all granted, иначе снова получите ошибку 403 Error. Помните, что каталог DocumentRoot и его родительские папки должны иметь разрешения на запуск для всех (можно установить командой `chmod o+x /путь/у/DocumentRoot`), в противном случае вы получите ошибку 403 Error.

AllowOverride None

Запрещает переопределение настроек. Если в секции `<Directory>` указана эта

директива, Apache будет полностью игнорировать настройки в файле .htaccess. Обратите внимание, что такая настройка для Apache 2.4 является настройкой по умолчанию, поэтому если вы планируете использовать .htaccess, необходимо дать соответствующие разрешения. Если вы собираетесь включить модуль mod_rewrite или использовать настройки в .htaccess, вы можете определить, какие из директив, объявленных в этих файлах, могут перезаписывать конфигурацию сервера. Для получения дополнительной информации обратитесь к документации Apache: http://httpd.apache.org/docs/current/mod/core.html#allowoverride.

Дополнительные настройки можно найти в /etc/httpd/conf/extra/httpd-default.conf.

Чтобы полностью отключить вывод версии Apache в генерируемых сервером страницах, добавьте директиву `ServerSignature Off`. Чтобы подавить вывод такой информации, как версии Apache и PHP, добавьте `ServerTokens Prod`.

16.3.4. Пользовательские каталоги

По умолчанию доступ к каталогам пользователей возможен по адресу

http://localhost/~"user"/, который показывает содержимое каталога ~/public_html (его имя и расположение задаются в файле /etc/httpd/conf/extra/httpd-userdir.conf).

Если вы не хотите, чтобы пользовательские каталоги были доступны через web, закомментируйте следующую строку в /etc/httpd/conf/httpd.conf: `Include conf/extra/httpd-userdir.conf`

Убедитесь, что права доступа к вашему домашнему каталогу и ~/public_html позволяют получать доступ к файлам в них всем пользователям:

```
$ chmod o+x ~
$ chmod o+x ~/public_html
$ chmod -R o+r ~/public_html
```

Однако с точки зрения безопасности вышеприведенное решение ненадежно. Правильнее поступить следующим образом:

1) Добавьте пользователя http в группу, которой принадлежит ваша домашняя папка. Например, если ваша домашняя папка и все ее подкаталоги принадлежат группе piter, можно проделать следующее:

```
# usermod -aG piter http
```

или

```
# gpasswd -a http piter
```

2) Назначьте права на чтение и исполнение для каталогов ~/, ~/public_html и, рекурсивно, на остальные подкаталоги для ~/public_html для членов группы (в нашем

примере для членов группы piter). Следуйте нижеприведенному образцу:

```
$ chmod g+xr-w /home/yourusername
$ chmod -R g+xr-w /home/yourusername/public_html
```

Примечание. В результате только пользователь http и все потенциальные пользователи группы piter будут иметь разделяемый доступ к вашему домашнему каталогу.

3) Перезапустите службу httpd, чтобы изменения вступили в силу.

16.3.5. TLS/SSL

Для использования TLS/SSL необходимо установить openssl.

Создайте закрытый ключ и запрос на получение сертификата (CSR). Также вы можете создать самоподписанный сертификат:

Примечание. Вы можете настроить длину ключа в битах (`rsa_keygen_bits:2048`). Также вы можете убрать опцию `-sha256` для использования SHA-1 вместо SHA-2 или изменить время его действия в днях (`-days 365`).

```
# cd /etc/httpd/conf
# openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048
-out server.key
# chmod 600 server.key
# openssl req -new -sha256 -key server.key -out server.csr
# openssl x509 -req -days 365 -in server.csr -signkey server.key
-out server.crt
```

Теперь раскомментируйте следующие строки в `/etc/httpd/conf/httpd.conf`:

```
LoadModule ssl_module modules/mod_ssl.so
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
Include conf/extra/httpd-ssl.conf
```

Перезапустите службу httpd.service, чтобы изменения вступили в силу.

16.3.6. Виртуальные хосты

Примечание. Необходимо добавить отдельную секцию `<VirtualHost dommainame:443>` для поддержки SSL на виртуальном хосте. Пример файла можно посмотреть ниже.

Если вы хотите, чтобы Apache обслуживал не один, а несколько хостов, раскомментируйте следующую строку в файле /etc/httpd/conf/httpd.conf:

```
Include conf/extra/httpd-vhosts.conf
```

Укажите виртуальные хосты в /etc/httpd/conf/extra/httpd-vhosts.conf. Файл уже содержит пример полностью рабочих настроек, что поможет быстро выполнить настройки под ваши нужды.

Для проверки виртуальных хостов на локальной машине добавьте их виртуальные имена в файл /etc/hosts:

```
127.0.0.1 domainname1.dom
127.0.0.1 domainname2.dom
```

Перезапустите httpd.service, чтобы изменения вступили в силу.

Управление большим количеством виртуальных хостов

Если Apache используется для обслуживания очень большого количества виртуальных хостов, может быть полезна возможность их легко включать и отключать. Для этого рекомендуется создавать собственный файл настроек на каждый хост и хранить все эти файлы в одном каталоге, например /etc/httpd/conf/vhosts.

1) Создайте каталог:

```
# mkdir /etc/httpd/conf/vhosts
```

2) Создайте в нем отдельные конфигурационные файлы:

```
# nano /etc/httpd/conf/vhosts/domainname1.dom
# nano /etc/httpd/conf/vhosts/domainname2.dom
...
```

3) Включите эти файлы в основной файл настроек /etc/httpd/conf/httpd.conf:

```
#Enabled Vhosts:
Include conf/vhosts/domainname1.dom
Include conf/vhosts/domainname2.dom
```

Теперь можно быстро включать/отключать требуемые виртуальные хосты, просто закомментировав или раскомментировав соответствующие директивы Include в основном файле настроек.

Очень простой файл виртуального хоста будет выглядеть следующим образом:

```
/etc/httpd/conf/vhosts/domainname1.dom
<VirtualHost *:80>
  ServerAdmin webmaster@domainname1.dom
  DocumentRoot "/home/user/http/domainname1.dom"
  ServerName domainname1.dom
  ServerAlias domainname1.dom
  ErrorLog "/var/log/httpd/domainname1.dom-error_log"
  CustomLog "/var/log/httpd/domainname1.dom-access_log" common
```

```
  <Directory "/home/user/http/domainname1.dom">
    Require all granted
  </Directory>
</VirtualHost>
<VirtualHost *:443>
  ServerAdmin webmaster@domainname1.dom
  DocumentRoot "/home/user/http/domainname1.dom"
  ServerName domainname1.dom:443
  ServerAlias domainname1.dom:443
  SSLEngine on
  SSLCertificateFile "/etc/httpd/conf/server.crt"
  SSLCertificateKeyFile "/etc/httpd/conf/server.key"
  ErrorLog "/var/log/httpd/domainname1.dom-error_log"
  CustomLog "/var/log/httpd/domainname1.dom-access_log" common
  <Directory "/home/user/http/domainname1.dom">
    Require all granted
  </Directory>
</VirtualHost>
```

16.3.7. Расширения

PHP

1) Установите пакеты php и php-apache.

2) Чтобы включить PHP, отредактируйте файл /etc/httpd/conf/httpd.conf. В конце списка LoadModule добавьте:

```
LoadModule php7_module modules/libphp7.so
AddHandler php7-script php
```

В конце списка Include добавьте:

```
Include conf/extra/php7_module.conf
```

3) Перезапустите службу httpd.service средствами systemd.

Чтобы убедиться в том, что PHP настроен корректно, создайте файл test.php в каталоге DocumentRoot (то есть в /srv/http/ или ~/public_html) и поместите в него следующий код:

```
<?php phpinfo(); ?>
```

По адресу http://localhost/test.php или http://localhost/"~пользователь"/test.php вы должны увидеть информационную страницу PHP.

Если PHP-код не исполняется, а на странице браузера вы видите содержимое

test.php, проверьте, добавили ли вы `Includes` в строку `Options` для вашего корневого каталога в /etc/httpd/conf/httpd.conf. Кроме того, убедитесь, что `TypesConfig conf/mime.types` раскомментирован в секции `<IfModule mime_module>`. Также можно попробовать добавить следующую строку в секцию `<IfModule mime_module>` файла `httpd.conf`:

```
AddHandler application/x-httpd-php .php
```

Использование php-fpm и mod_proxy_fcgi

В отличие от широко распространенной установки с ProxyPass, настройка прокси с SetHandler принимает во внимание другие директивы Apache, например, `DirectoryIndex`. Это гарантирует лучшую совместимость с программами, созданными для libphp7, mod_fastcgi и mod_fcgid. Если, тем не менее, необходимо использовать ProxyPass, попробуйте такую строку:

```
ProxyPassMatch ^/(.*\.php(/.*)?)$ unix:/run/php-fpm/php-fpm.sock|
fcgi://localhost/srv/http/$1
```

1) Установите пакет php-fpm.

2) Включите модули прокси:

```
/etc/httpd/conf/httpd.conf
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
```

Создайте файл /etc/httpd/conf/extra/php-fpm.conf следующего содержания:

```
/etc/httpd/conf/extra/php-fpm.conf
<FilesMatch \.php$>
SetHandler "proxy:unix:/run/php-fpm/php-fpm.sock|
fcgi://localhost/"
</FilesMatch>
```

3) Добавьте его в конец файла /etc/httpd/conf/httpd.conf:

```
Include conf/extra/php-fpm.conf
```

Примечание. До и после символа вертикальной линии не должно быть пробелов. Localhost можно заменить любой строкой. Подробности см. в документе по ссылке: https://httpd.apache.org/docs/2.4/mod/mod_proxy_fcgi.html

Можно настроить PHP-FPM в файле /etc/php/php-fpm.d/www.conf, но и параметры по умолчанию должны работать отлично.

Примечание. Если ранее были добавлены следующие строки в httpd.conf, удалите их, т. к. они более не нужны:

```
LoadModule php7_module modules/libphp7.so
Include conf/extra/php7_module.conf
```

2) Перезапустите службы httpd.service и php-fpm.service.

Решение проблем

Просмотр журнала и текущего состояния Apache

Чтобы узнать текущее состояние службы httpd, выполните следующую команду:

```
systemctl status httpd
```

Файлы журнала Apache расположены в каталоге /var/log/httpd.

Установленная документация по Apache:

- httpd — руководство по службе httpd с полным списком консольных параметров;
- genkey — руководство для утилиты genkey, поставляемой в пакете crypto-utils;
- apachectl — руководство по Apache HTTP Server Control Interface;
- http://localhost/manual/ — официальная документация для HTTP сервера Apache с полным описанием всех директив и доступных модулей. Обратите внимание, что для чтения этой документации необходимо установить пакет httpd-manual и запустить веб-сервер.

Перед чтением документации выполните следующие команды:

```
# dnf install httpd-manual
# apachectl graceful
```

16.4. Сетевой доступ к ФС NFS

Протокол сетевого доступа к ФС (NFS) позволяет монтировать ФС по сети и взаимодействовать с ними так, как если бы они были смонтированы локально. Это дает возможность системным администраторам консолидировать ресурсы вокруг централизованных серверов в сети.

На данный момент в ОС РОСА «НИКЕЛЬ» включены две мажорные версии NFS — NFSv3 и NFSv4.0. NFS версии 3 поддерживает защищенный асинхронный режим записи и более устойчива при возникновении ошибок, чем предыдущая NFSv2; также существует поддержка 64-битного размера файлов и смещения, что дает клиентам возможность доступа к файловым данным размером более 2 ГБ. NFS версии 4 работает с межсетевыми экранами и через интернет, не требует службы rpcbind, имеет поддержку ACL и использует операции с сохранением состояния.

В последней версии ОС РОСА «НИКЕЛЬ» добавлена поддержка для NFS версии 4.1 (NFSv4.1). Было произведено несколько улучшений производительности и безопасности, включая клиентскую поддержку для Parallel NFS (pNFS). NFSv4.1 больше

не требует отдельного соединения TCP для обратных вызовов, что дает возможность серверу NFS делегировать полномочия, даже если к клиенту невозможно подключиться (например, при вмешательстве со стороны NAT или межсетевого экрана), что предотвращает возможность ранее случавшихся ошибок, когда некоторые операции могли вернуть неточный результат вследствие потери ответа и повторной отправки операции.

По умолчанию клиенты NFS пытаются выполнить монтирование с использованием NFSv4.0, и, если операция оканчивается неудачей, выполняется откат к NFSv3.

Примечание. NFS версии 2 (NFSv2) не поддерживается.

Все версии NFS могут использовать протокол TCP, работающий по сети IP, а для версии NFSv4 он входит в требования. Для обеспечения сетевого соединения без сохранения состояния между клиентом и сервером NFSv3 может использовать протокол UDP, работающий по сети IP.

При использовании NFSv3 с протоколом UDP соединение UDP без сохранения состояния (в нормальных условиях) создает меньше служебной информации, связанной с работой протоколов. Как результат, в очень чистой, неперегруженной сети будет наблюдаться улучшение производительности. Тем не менее, поскольку протокол UDP работает без сохранения состояния, то в случае неожиданного отключения сервера клиенты UDP продолжают наполнять сеть запросами для сервера. Кроме того, при потере кадров в соединении UDP необходимо повторно передать весь запрос RPC целиком, тогда как в TCP нужно переслать только потерянный кадр. По этим причинам при подключении к серверу NFS предпочтительным является протокол TCP.

В протокол NFSv4 были встроены проколы блокировки и монтирования. Сервер также слушает на хорошо известном порту TCP 2049, поэтому для NFSv4 исчезла необходимость взаимодействия с демонами rpcbind, lockd и rpc.statd. Для настройки экспортов на сервере NFS все еще требуется работа демона rpc.mountd, но он не участвует ни в каких операциях передачи данных.

Примечание. В ОС РОСА «НИКЕЛЬ» протоколом по умолчанию для NFSv3 является TCP. Из соображений совместимости можно использовать UDP, но для широкого применения он не рекомендуется. NFSv4 требует TCP.

У всех демонов RPC/NFS существует консольный параметр `-p`, с помощью которого можно указать порт, что облегчает настройку межсетевого экрана. После того, как надстройки TCP получат доступ к клиенту, сервер NFS обращается к файлу /etc/exports, чтобы узнать, разрешен ли клиенту доступ к каким-либо экспортированным

ФС. После проверки все действия с файлами и каталогами становятся доступными для пользователя.

16.4.1. Требуемые службы

Для предоставления обмена файлами с помощью NFS в ОС РОСА «НИКЕЛЬ» используется сочетание поддержки на уровне ядра и процессов демонов. Все версии NFS зависят от удаленных вызовов процедур (Remote Procedure Calls, RPC) между клиентом и сервером. Службы RPC в ОС РОСА «НИКЕЛЬ» контролируются службой rpcbind. Чтобы смонтировать ФС NFS или сделать ее общей, необходима совместная работа следующих служб (в зависимости от реализованной версии NFS):

nfs

Команда

```
systemctl start nfs
```

запускает сервер NFS и соответствующие процессы RPC для обслуживания запросов к общим ФС NFS.

nfslock

Команда

```
systemctl start nfs-lock
```

активирует обязательную службу, которая запускает соответствующие процессы RPC, давая возможность клиентам NFS блокировать файлы на сервере.

rpcbind

Служба rpcbind принимает резервирование порта от локальных служб RPC. Затем эти порты анонсируются, чтобы соответствующие удаленные службы RPC поучили к ним доступ. rpcbind отвечает на запросы к службам RPC и настраивает соединения к запрошенным службам RPC. В NFSv4 это не используется.

Следующие процессы RPC облегчают работу служб NFS:

rpc.mountd

Этот процесс используется сервером NFS для обработки запросов MOUNT от клиентов NFSv3. Запрошенный общий ресурс NFS должен быть в текущий момент экспортирован сервером NFS, что и проверяет rpc.mountd, а также проверяется разрешение клиента на доступ к этому общему ресурсу. Если запрос на монтирование разрешается, сервер rpc.mountd посылает в ответ статус Success и отравляет описатель файла этого общего ресурса NFS назад клиенту NFS.

rpc.nfsd

Этот процесс разрешает определение явной версии NFS и протоков, которые

анонсирует сервер. Он работает с ядром Linux для удовлетворения потребностей клиентов NFS, таких как предоставление серверных потоков каждый раз при подключении клиента NFS. Этот процесс соответствует службе nfs.

lockd

Это поток ядра, выполняемый как на клиенте, так и на сервере. Он реализует протокол Network Lock Manager (NLM), позволяющий клиентам NFSv3 блокировать файлы на сервере. Он запускается автоматически при каждом запуске сервера NFS и при каждом монтировании ФС NFS.

rpc.statd

Этот процесс реализует прокол Network Status Monitor (NSM) RPC, который уведомляет клиентов NFS о перезапуске сервера NFS без корректного его выключения. rpc.statd автоматически запускается службой nfslock, и ему не требуются параметры пользователей. Он не используется с NFSv4.

rpc.rquotad

Этот процесс предоставляет информацию о квоте удаленных пользователей.

rpc.rquotad автоматически запускается службой nfs, и ему не требуются параметры пользователей.

rpc.idmapd rpc.idmapd предоставляет обратные вызовы клиента и сервера NFSv4, которые преобразуются между передаваемыми именами NFSv4 (записи в формате user@domain) и локальными UID и GID. Чтобы idmapd мог функционировать с NFSv4, необходимо настроить файл /etc/idmapd.conf. В минимальной конфигурации должен быть указан параметр «Domain», определяющий домен преобразования NFSv4. Если домен преобразования NFSv4 аналогичен доменному имени DNS, то этот параметр можно опустить. Чтобы преобразование ID функционировало корректно, клиент и сервер должны договориться о домене преобразования NFSv4.

Примечание. В ОС РОСА «НИКЕЛЬ» rpc.idmapd используется только сервером NFSv4. Клиент NFSv4 использует nfsidmap — id-преобразователь на базе связки ключей. nfsidmap — это отдельная программа, вызываемая по требованию ядром для выполнения преобразования ID; это не демон. При наличии проблем с nfsidmap клиент откатывается к использованию rpc.idmapd. Подробные сведения о nfsidmap можно найти на странице руководства nfsidmap.

16.4.2. Настройка клиента NFS

Команда `mount` монтирует общие ресурсы NFS на стороне клиента. Команда имеет следующий формат:

```
# mount -t nfs -o <параметры> <сервер>:</удаленный/экспорт>
</локальный/каталог>
```

Здесь:

– <параметры> — список параметров монтирования через запятую;

– <сервер> — имя хоста, IP-адрес или полное доменное имя сервера, экспортирующего ФС, которую нужно смонтировать;

– </удаленный/экспорт> — ФС или каталог, экспортируемый с сервера, то есть каталог, который нужно смонтировать;

– </локальный/каталог> — местоположение на клиенте, где смонтирован /remote/export.

Версия протокола NFS, используемого в ОС РОСА «НИКЕЛЬ», определяется параметрами монтирования nfsvers или vers. По умолчанию mount будет использовать NFSv4 в виде `mount -t nfs`. Если сервер не поддерживает NFSv4, клиент автоматически перейдет на версию, используемую сервером. Если параметр nfsvers/vers используется для передачи конкретной версии, не поддерживаемой сервером, монтирование окончится неудачей. Из соображений совместимости с устаревшими версиями также поддерживается тип ФС nfs4; это аналогично выполнению команды `mount -t nfs -o nfsvers=4 host:</удаленный/экспорт> </локальный/каталог>`.

Если общий ресурс NFS был смонтирован вручную, после перезагрузки системы он не будет снова смонтирован автоматически. ОС РОСА «НИКЕЛЬ» предлагает два способа монтирования удаленных ФС во время загрузки системы: файл /etc/fstab и служба autofs.

Монтирование ФС NFS с помощью /etc/fstab

Одним из способов монтирования общего ресурса NFS с другой машины является добавление записи в файл /etc/fstab. В записи должны указываться имя хоста сервера NFS, экспортируемый каталог сервера и каталог на локальной машине, куда должен монтироваться общий ресурс NFS. Для изменений файла /etc/fstab требуются права с администратора (sudo -i).

Пример синтаксиса

Общий синтаксис, используемый в строке файла /etc/fstab, выглядит следующим образом:

```
server:/usr/local/pub  /pub  nfs  defaults 0 0
```

Перед выполнением данной команды на клиентской машине должна быть создана точка монтирования /pub. После добавления указанной строки в файл /etc/fstab на

клиентской системе используйте команду mount /pub, и точка монтирования /pub будет смонтирована с сервера.

Действительная запись /etc/fstab для монтирования экспорта NFS должна содержать следующую информацию:

```
<сервер>:/remote/export /local/directory nfs <параметры> 0 0
```

Переменные `<сервер>`, `</удаленный/экспорт>`, `</локальный/каталог>` и `<параметры>` — это те же переменные, которые использовались при ручном монтировании общего ресурса NFS.

Примечание. Точка монтирования /local/directory должна быть создана на клиенте до чтения файла /etc/fstab. В противном случае монтирование окончится неудачей. Подробности о файле /etc/fstab см. на странице руководства fstab.

AUTOFS

Одним из минусов использования /etc/fstab является то, что вне зависимости от того, как часто пользователь получает доступ к смонтированной ФС NFS, ОС должна выделять ресурсы для удержания смонтированной ФС на месте. Это не является проблемой с одним или двумя смонтированными ресурсами, но когда система должна поддерживать смонтированными множество ресурсов одновременно, то это может отрицательно повлиять на общую производительность. Альтернативой использованию файла /etc/fstab является использование утилиты automount на базе ядра. Средство автоматического монтирования состоит из двух компонентов:

1) Модуля ядра, реализующего ФС.
2) Демона в пространстве пользователя, исполняющего другие функции.

Утилита automount может монтировать и размонтировать ФС NFS автоматически (монтирование по запросу), тем самым сберегая ресурсы ОС. С ее помощью также можно монтировать другие ФС, включая AFS, SMBFS, CIFS и локальные ФС.

Примечание. Перед попыткой автоматического монтирования общего ресурса NFS убедитесь в том, что в системе установлены nfs-utils.

Настройка autofs

Основной конфигурационный файл автомонтировщика — /etc/auto.master, также называемый «основной картой». В основной карте перечислены точки монтирования в системе, контролируемые autofs, а также соответствующие конфигурационные файлы или сетевые источники, известные как карты автомонтирования. Основная карта имеет следующий формат:

```
<точка_монтирования> <имя_карты> <параметры>
```

Здесь:

– <точка_монтирования> — точка монтирования autofs, например, /home. Это может быть имя отдельного каталога (для непрямого монтирования) или полный путь до точки монтирования (для прямого монтирования). Каждая запись прямого или непрямого монтирования может быть дополнена списком подкаталогов (каждое имя подкаталога начинается с /, элементы списка разделяются пробелами), что в итоге формирует запись, называемую записью множественного монтирования (multimount entry);

– <имя_карты> — имя источника карты, содержащего список точек монтирования и местоположение ФС, источника этих точек монтирования. Синтаксис записи карты описывается ниже;

– <параметры> — при их наличии они применяются ко всем записям указанной карты, если у записей отсутствуют собственные указанные параметры. Это поведение отличается от поведения autofs версии 4, где параметры имели накопительный характер. Это поведение было изменено в версии 5, для реализации совместимости со смешанным окружением.

Пример: файл /etc/auto.master

Ниже приведен пример записи из файла /etc/auto.master:

```
/home /etc/auto.misc
```

Общий формат карт аналогичен формату основной карты, но «параметры» размещаются между точкой монтирования и местоположением, в не в конце записи, как в основной карте:

```
<точка_монтирования> [<параметры>] <местоположение>
```

Под <местоположением> имеется в виду местоположение ФС, например, путь в локальной ФС (перед которым указывается экранирующий символ форматирования карт Sun «:» для имен карт, начинающихся с «/»), в ФС NFS или в другом действительном местоположении ФС.

Ниже приведен пример содержимого файла карты (например, /etc/auto.misc):

```
payroll -fstype=nfs
personnel:/dev/hda3
sales -fstype=ext3 :/dev/hda4
```

Первый столбец в файле карты указывает точку монтирования autofs (sales и payroll с сервера personnel). Второй столбец указывает параметры монтирования autofs, а третий столбец — источник монтирования. Следуя указанной конфигурации, точки монтирования autofs будут: /home/payroll и /home/sales. Параметр `-fstype=` часто опускается и, как правило, не нужен для корректного выполнения операции.

Автомонтировщик создаст два каталога, если они не существуют. Если до запуска

автомонтировщика эти каталоги существовали, во время завершения работы автомонтировщик не станет их удалять. Запустить или остановить демон автоматического монтирования можно с помощью одной из следующих команд:

- service autofs start (если демон был остановлен);
- service autofs restart.

Если процессу нужен доступ к каталогу, который был отмонтирован утилитой autofs, например, /home/payroll/2006/July.sxc, то с помощью вышеуказанной конфигурации демон автоматического монтирования автоматически смонтирует этот каталог. При указанном времени истечения срока ожидания каталог будет автоматически отмонтирован, если за указанный период к нему не был осуществлен доступ.

Статус демона автоматического монтирования можно просмотреть, введя следующую команду:

```
# service autofs status
```

Хранение карт автомонтирования с использованием LDAP

Для возможности получения карт автомонтировщика из LDAP в системе должны быть установлены клиентские библиотеки LDAP. В ОС РОСА «НИКЕЛЬ» пакет openldap должен устанавливаться автоматически как зависимость для автомонтировщика. Для настройки доступа к LDAP измените файл /etc/openldap/ldap.conf. Убедитесь, что BASE, URI и схема имеют параметры, соответствующие конкретному узлу.

Актуальная схема хранения карт автомонтирования в LDAP описана в документе rfc2307bis. Для использования этой схемы ее нужно настроить в параметрах autofs (/etc/sysconfig/autofs), удалив символы комментариев со строк определения схемы.

Часто используемые параметры монтирования NFS

Кроме монтирования ФС на удаленном хосте с помощью NFS, также можно указать другие параметры монтирования для облегчения работы со смонтированным общим ресурсом. Эти параметры можно использовать во время ручного монтирования с помощью команды mount, в конфигурации /etc/fstab, а также с autofs.

Ниже приводятся часто используемые параметры для монтирования ресурсов NFS: **intr**

Позволяет прерывать запросы NFS при отключении или недоступности сервера. **lookupcache=<режим>**

Указывает ядру, как нужно обрабатывать кэш каталогов для указанной точки монтирования. Действительные аргументы для <режима>: all, none или pos/positive.

nfsvers=<версия>

Указывает, какую версию протокола NFS нужно использовать, где <версия> — 3

или 4. Удобно для хостов с несколькими серверами NFS. Если версия не указана, NFS использует самую свежую версию, поддерживаемую ядром и командой mount. Параметр **vers** идентичен параметру **nfsvers** и включен в данную версию из соображений совместимости.

noacl

Отключает обработку ACL. Может понадобиться при работе со старыми версиями различных дистрибутивов Linux или Solaris.

nolock

Отключает блокировку файлов. Этот параметр иногда бывает нужен при подключении к старым серверам NFS.

noexec

Запрещает выполнение бинарных файлов на смонтированных ФС. Полезно, если в системе монтируются ФС, не принадлежащие семье Linux, содержащие несовместимые бинарные файлы.

nosuid

Отключает биты setuid или sgid, предотвращая получение повышенных привилегий удаленными пользователями с помощью запуска программы setuid.

port=<номер>

Указывает числовое значение порта сервера NFS. Если <номер> равен 0 (значение по молчанию), программа mount запрашивает службу rpcbind удаленного хоста, какой номер порта использовать. Если демон NFS удаленного хоста не зарегистрирован соответствующей службой rpcbind, используется стандартный номер порта TCP — 2049.

rsize= <число> и **wsize= <число>**

Эти параметры ускоряют соединение NFS для чтения (rsize) и записи (wsize), указывая увеличенный размер для передаваемого за один раз блока (<число> в байтах). Изменяйте эти значения осторожно: некоторые старые ядра Linux и сетевые карты не очень хорошо справляются с увеличенными размерами блоков. Для NFSv3 значения по умолчанию для обоих параметров составляют 8192. Для NFSv4 значения по умолчанию для обоих параметров составляют 32 768.

sec=<режим>

Значение по умолчанию — `sec=sys`, использующее локальные UNIX UID и GID, которые, в свою очередь, используют AUTH_SYS для аутентификации операций NFS.

– sec=krb5. Для аутентификации пользователей используется Kerberos V5 вместо локальных UNIX UID и GID;

– sec=krb5i. Для аутентификации пользователей используется Kerberos V5, и для

предотвращения преднамеренной порчи данных выполняется проверка целостности операций NFS с использованием защищенных контрольных сумм;

– sec=krb5p. Для аутентификации пользователей используется Kerberos V5, выполняется проверка целостности, а трафик NFS шифруется для предотвращения прослушивания. Это наиболее надежные параметры, но также и наиболее требовательные к производительности системы.

tcp

Требует использовать протокол TCP для операций монтирования NFS.

udp

Требует использовать протокол UDP для операций монтирования NFS.

Полный список параметров и более подробную информацию о каждом из них см. на страницах руководств mount и nfs.

16.4.3. Запуск и остановка сервера NFS

Для работы сервера NFS, использующего не только версию NFSv4, необходима запущенная служба rpcbind. Для проверки статуса службы rpcbind выполните следующую команду:

```
# systemctl status rpcbind
```

Если служба rpcbind выполняется, службу nfs можно запустить. Чтобы запустить сервер NFS, выполните:

```
# systemctl start nfs
```

Чтобы NFS автоматически запускалась при загрузке системы, выполните:

```
# systemctl enable nfs-server
```

Примечание. Если служба NFS настроена на запуск при загрузке системы, для версии NFSv3 необходимо также включить службу nfs-lock. В ОС РОСА «НИКЕЛЬ» nfslock при необходимости стартует автоматически, и попытка включить ее вручную окончится неудачей. Если же данная служба была отключена, для автоматического запуска nfslock при загрузке системы выполните:

```
systemctl enable nfs-lock
```

Чтобы остановить сервер, выполните:

```
# systemctl stop nfs
```

Параметр restart является наиболее быстрым способом остановки и затем перезапуска NFS. Это наиболее эффективный способ применить новые параметры после редактирования конфигурационного файла NFS. Чтобы перезапустить сервер, выполните:

```
# systemctl restart nfs
```

После редактирования файла /etc/sysconfig/nfs перезапустите службу nfs-config для применения новых параметров:

```
# systemctl restart nfs-config
```

Команда `try-restart` запускает nfs, только если она уже выполняется. Эта команда является эквивалентом `condrestart` (conditional restart) в сценариях инициализации ОС РОСА «НИКЕЛЬ» и удобна тем, что не запускает демон, если NFS уже выполняется.

Чтобы выполнить условный перезапуск сервера, выполните:

```
# systemctl try-restart nfs
```

Чтобы перезагрузить конфигурацию сервера NFS без перезапуска службы, выполните:

```
# systemctl reload nfs
```

16.4.4. Настройка сервера NFS

Существует два способа настройки экспортов на сервере NFS:

1) Ручное редактирование конфигурационного файла NFS /etc/exports.

2) Использование консольной команды exportfs.

Конфигурационный файл /etc/exports

В файле /etc/exports указывается, какие ФС экспортируются на удаленный хост. Применяются следующие правила синтаксиса:

- пустые строки игнорируются;
- комментарии начинаются с символа «#»;
- длинные строки переносятся с помощью косой черты «\»;
- для каждой экспортируемой ФС выделяется отдельная строка;
- любые списки авторизованных хостов, помещенные после экспортируемой ФС, должны отделяться символами пробела;
- параметры для каждого из хостов должны размещаться в скобках и идти непосредственно сразу за идентификатором хоста, без пробела между хостом и первой скобкой.

Каждая запись для экспортируемой ФС имеет следующую структуру:

```
export <хост>(<параметры>)
```

В вышеуказанной структуре используются следующие переменные:

- export — экспортируемый каталог;
- <хост> — хост или сеть, для которой этот ресурс делается общим;

– <параметры> — параметры хоста.

Можно указать несколько хостов, а также параметры для каждого из них. Для этого укажите их в одной строке через пробелы в соответствии со следующим примером:

```
export <хост_1>(<параметры_1>) <хост_2>(<параметры_2>) ...
```

В самом простом варианте в файле /etc/exports указываются только экспортируемый каталог и хосты, которым разрешен доступ к этому каталогу. См. пример ниже.

Пример: файл /etc/exports

```
</каталог/экспорта> bob.test.dom
```

Здесь `bob.test.dom` может монтировать `</каталог/экспорта>` с сервера NFS. Поскольку в этом примере никаких параметров не указано, NFS будет использовать параметры по умолчанию.

Параметры по умолчанию:

ro

Экспортируемая ФС доступна только для чтения. Удаленные хосты не могут изменять общие данные. Чтобы разрешить хостам вносить изменения в ФС (то есть читать и писать), укажите параметр rw.

sync

Сервер NFS не будет отвечать на запросы до того, как изменения, сделанные предыдущими запросами, не будут записаны на диск. Чтобы вместо этого включить асинхронную запись, укажите параметр **async**.

wdelay

Сервер NFS отложит запись на диск, если становится очевидным, что скоро поступит еще один запрос записи на диск. Такое поведение может улучшить производительность, т. к. уменьшает количество доступов к диску в результате разрозненных команд записи на диск, тем самым снижая потребление ресурсов записи. Чтобы отключить это поведение, укажите параметр **no_wdelay**. no_wdelay доступен, только если указан параметр по умолчанию sync.

root_squash

Не дает пользователям root, подключенным удаленно, получать привилегии root (в противовес локальным подключениям); вместо этого сервер NFS присвоит им идентификатор пользователя nfsnobody. Этот параметр «выжимает» (squash) привилегии из суперпользователя root, делая его первичным локальным пользователем и предотвращая возможные неавторизованные записи на удаленном сервере. Чтобы отключить это поведение, укажите параметр **no_root_squash**.

Чтобы «выжать» привилегии из каждого удаленного пользователя (включая root), используйте параметр **all_squash**. Чтобы указать идентификаторы пользователя и группы, которые сервер NFS должен присваивать удаленным пользователям с конкретного хоста, используйте соответственно, параметры anonuid и anongid, например:

```
export host(anonuid=uid,anongid=gid)
```

Здесь uid и gid — номер идентификатора пользователя и номер идентификатора группы, соответственно. Параметры `anonuid` и `anongid` дают возможность создать специальные учетные записи пользователя и группы, для общего использования их удаленными пользователями NFS.

По умолчанию в ОС РОСА «НИКЕЛЬ» служба NFS поддерживает списки контроля доступа (ACL). Для отключения этой возможности при экспорте ФС укажите параметр `no_acl`.

Каждое значение по умолчанию для каждой экспортируемой ФС должно переписываться явным образом. Если, например, не указывается параметр `rw`, экспортируемая ФС становится доступной только для чтения. Ниже приведен пример строки из файла /etc/exports, переписывающей два значения по молчанию:

```
</каталог/экспорта> 192.168.0.3(rw,async)
```

В этом примере 192.168.0.3 может монтировать `</каталог/экспорта>` на чтение/запись, и все записи на диск выполняются асинхронно. Подробности о параметрах экспорта см. на странице руководства exportfs.

Другие параметры доступны, если отсутствуют указанные значения по умолчанию. Это относится к возможности отключения проверки поддерева, разрешения доступа с незащищенных портов, а также разрешения незащищенных блокировок файлов (необходимые для некоторых ранних реализаций клиента NFS). Подробности об этих редко используемых параметрах см. на странице руководства exports.

Примечание. Формат файла /etc/exports является очень строгим, особенно относительно использования символа пробела. Не забывайте всегда отделять экспортируемые ФС от хостов, а хосты — друг от друга с помощью символа пробела. Но других символов пробела в этом файле быть не должно, за исключением пробелов в комментариях.

Две следующие строки, например, имеют различное значение:

```
/home bob.test.dom(rw)
/home bob.test.dom (rw)
```

Первая строка разрешает доступ на чтение/запись в каталог /home только пользователям с bob.test.dom. Вторая строка разрешает пользователям с bob.test.dom

монтировать каталог только для чтения (значение по умолчанию), а все остальные могут монтировать его для чтения-записи.

16.4.5. Команда exportfs

Каждая ФС, экспортируемая удаленным пользователям с помощью

NFS, а также уровень доступа к этим ФС, указываются в файле /etc/exports. При запуске службы nfs команда /usr/sbin/exportfs читает этот файл, передает управление фактическим процессом монтирования демону rpc.mountd (если используется версия NFSv3), а затем rpc.nfsd, после чего ФС становится доступной для удаленных пользователей.

При запуске вручную команда /usr/sbin/exportfs дает пользователю root возможность выборочно экспортировать или отменять экспорт без перезапуска службы NFS. Если указаны корректные параметры, команда /usr/sbin/exportfs записывает экспортируемые ФС в /var/lib/nfs/xtab. Поскольку при выдаче прав доступа к ФС rpc.mountd обращается к файлу xtab, изменения в списке экспортируемых ФС применяются сразу же.

Ниже перечислены часто используемые параметры команды /usr/sbin/exportfs:

– -r — экспортирует все каталоги, перечисленные в /etc/exports, с помощью нового списка экспорта, создаваемого в /etc/lib/nfs/xtab. Этот параметр эффективно актуализирует список экспорта относительно любых изменений, вносимых в /etc/exports;

– -a — экспортирует или отменяет экспорт всех каталогов в зависимости от других параметров, переданных команде /usr/sbin/exportfs. При отсутствии других параметров /usr/sbin/exportfs экспортирует все ФС, указанные в /etc/exports;

– -o <файловые_системы> — указывает каталоги для экспорта, отсутствующие в /etc/exports. Замените <файловые_системы> на дополнительные экспортируемые ФС. Формат указания ФС должен совпадать с форматом, используемым в /etc/exports. Этот параметр часто используется для тестирования экспортируемой ФС перед постоянным добавлением ее в список экспортируемых ФС.

– -i — файл /etc/exports игнорируется; для определения экспортируемых ФС используются только параметры командной строки;

– -u — отменяет экспорт всех общих каталогов. Команда /usr/sbin/exportfs -ua приостанавливает процесс доступа к общим файлам NFS, не прерывая работы всех демонов NFS. Чтобы возобновить процесс доступа к общим ресурсам NFS, используйте exportfs -r;

– -v — подробный отчет о действиях. При выполнении команды exportfs будут выводиться гораздо более подробные сведения об экспортируемых ФС.

При запуске `exportfs` без параметров она выдает список всех текущих экспортированных ФС.

Использование exportfs с NFSv4

В ОС РОСА «НИКЕЛЬ» не требуется специальных шагов для настройки NFSv4, т. к. любые упоминаемые ФС автоматически доступны клиентам NFSv3 и клиентам NFSv4 по одному и тому же пути. В предыдущих версиях NFS это было не так. Чтобы запретить клиентам использовать NFSv4, отключите ее, указав в файле /etc/sysconfig/nfs параметр `RPCNFSDARGS= -N 4`.

16.4.6. Работа NFS с межсетевым экраном

Для NFS необходим rpcbind, динамически присваивающий порты службам RPC, что может привести к проблемам при настройке правил межсетевого экрана. Чтобы разрешить клиентам доступ к общим ресурсам NFS за межсетевым экраном, отредактируйте файл /etc/sysconfig/nfs, указав, на каких портах выполняются службы RPC.

Не во всех системах файл /etc/sysconfig/nfs существует по молчанию. Если он отсутствует, создайте его, указав следующее содержимое:

```
RPCMOUNTDOPTS="-p port"
```

Эта запись добавляет `-p port` в командную строку `rpc.mount`.

Чтобы указать, какие порты будут использоваться службой nlockmgr, укажите номер порта для параметров `nlm_tcpport` и `nlm_udpport` в файле /etc/modprobe.d/lockd.conf.

Если NFS сбоит при запуске, проверьте /var/log/messages. Обычно запуск NFS заканчивается неудачей, если был указан уже используемый номер порта. После редактирования /etc/sysconfig/nfs необходимо перезапустить службу nfs-config для применения новых значений:

```
# systemctl restart nfs-config
```

Затем перезапустите сервер NFS:

```
# systemctl restart nfs-server
```

Чтобы проверить, что новые параметры вступили в силу, выполните `rpcinfo -p`.

Примечание. Чтобы разрешить обратным вызовам NFSv4 проход через межсетевой экран, настройте /proc/sys/fs/nfs/nfs_callback_tcpport и разрешите серверу подключаться к этому порту на клиенте.

Для NFSv4 и более поздней это действие не требуется. В окружении, где используется только NFSv4, также не нужны другие порты для mountd, statd и lockd.

16.4.7. Обнаружение экспортируемых каталогов NFS

Для обнаружения ФС, экспортируемых NFS, существуют два способа:

1) На любом сервере с поддержкой NFSv3 запустите команду `showmount`:

```
$ showmount –e myserver
Export list for mysever
/exports/foo
/exports/bar
```

2) На любом сервере с поддержкой NFSv4 смонтируйте и просмотрите /:

```
# mount myserver:/ /mnt/
#cd /mnt/
exports
# ls exports
foo
bar
```

На серверах с поддержкой NFSv3 и NFSv4 оба способа приведут к одинаковому результату.

16.4.8. Обеспечение безопасности NFS

NFS является прозрачным механизмом совместного использования целых ФС с большим числом известных хостов. Тем не менее, вместе с простотой использования приходит и некоторое число потенциальных проблем безопасности. Чтобы минимизировать риски безопасности при использовании NFS и обеспечить защиту данных на сервере, ознакомьтесь с данным подразделом перед тем, как приступать к экспорту ФС NFS или к монтированию их на клиенте.

Безопасность NFS с AUTH_SYS и контроль экспорта

Традиционно при использовании NFS существовало две возможности контроля доступа к экспортируемым файлам.

Во-первых, со стороны сервера существуют ограничения касательно того, каким хостам разрешено монтировать какие ФС. Хосты при этом идентифицируются по IP-адресу или по имени. Во-вторых, сервер принудительно применяет права доступа к ФС для пользователей на клиентах NFS (так же, как это делается и для локальных пользователей). Традиционно это делается с использованием AUTH_SYS (также называемой AUTH_UNIX), которая определяет UID и GID пользователя, основываясь на данных клиента. Необходимо понимать, что в такой ситуации намеренное злоумышленное изменение данных на клиенте может легко привести к нежелательным

ситуациям и предоставить пользователю доступ к данным, не предназначенным для него.

Для снижения риска администратор часто ограничивает доступ правами только на чтение или понижает права пользователя до непривилегированного ID пользователя и группы. К сожалению, такие решения не дают использовать NFS так, как исходно задумывалось при ее создании.

Кроме того, если злоумышленник получает контроль над сервером DNS, который используется системой, выполняющей экспорт NFS, систему, связанную с конкретным именем хоста или полным именем, можно направить на неавторизованную машину. На этом этапе неавторизованная машина становится системой, которой разрешено монтировать общий ресурс NFS, поскольку для дополнительной безопасности смонтированного ресурса NFS не требуется обмена информацией о пароле или имени пользователя.

С осторожностью используйте символы подстановки при экспорте каталогов, т. к. в область действия символа подстановки может попасть больше систем, чем планировалось.

Также можно ограничить доступ к службе rpcbind с помощью надстроек TCP. Создание правил iptables также может ограничить доступ к портам, используемым rpcbind, rpc.mountd и rpc.nfsd.

Подробности о том, как защитить NFS и TCP, см. в man iptables.

Защита NFS с помощью AUTH_GSS

NFSv4 радикально изменила защиту NFS требованием реализации RPCSEC_GSS и механизма GSS-API пятой версии Kerberos. Тем не менее, RPCSEC_GSS и механизм Kerberos доступны для всех версий NFS. В режиме FIPS можно использовать только алгоритмы, одобренные FIPS.

В отличие от AUTH_SYS, при использовании механизма Kerberos RPCSEC_GSS сервер не зависит от клиента в вопросе правильного представления того, какой именно пользователь получает доступ к файлу. Вместо этого для аутентификации пользователя на сервере используется шифрование, что не дает возможности клиенту-злоумышленнику представиться другим пользователем, не имея учетных данных Kerberos этого пользователя. Использование механизма Kerberos RPCSEC_GSS — это наиболее простой способ обеспечить защиту смонтированным ресурсам, т. к. после настройки Kerberos отпадает необходимость настраивать что-либо дополнительно.

Настройка Kerberos

Перед тем, как настраивать сервер NFSv4, совместимый с Kerberos, необходимо установить и настроить центр распределения ключей Kerberos (Key Distribution Centre,

KDC). Kerberos — это система сетевой аутентификации, дающая возможность аутентифицироваться клиентам и серверам с помощью симметричного шифрования и доверенной третьей стороны — центра KDC. Для настройки Kerberos рекомендуется использовать управление идентификационной информацией (Identity Management, IdM).

Настройка сервера и клиента NFS для использования RPCSEC_GSS 1) На стороне сервера NFS создайте принципал nfs/hostname.domain@REALM.

2) На стороне клиента и на стороне сервера создайте принципал host/hostname.domain@REALM.

3) Добавьте соответствующие ключи в таблицу ключей клиента и сервера.

4) На стороне сервера включите желаемые степени безопасности, используя sec= <параметр>. Чтобы включить все степени безопасности, а также монтирование ресурсов без шифрования, выполните:

```
/export *(sec=sys:krb5:krb5i:krb5p)
```

Действительные степени безопасности, которые используются с `sec=<параметр>`:

- sys: без защиты шифрованием (значение по умолчанию);
- krb5: только аутентификация;
- krb5i: защита целостности;
- krb5p: защита конфиденциальности.

5) На стороне клиента добавьте в параметры монтирования `sec=krb5`, `sec=krb5i` или `sec=krb5p`, в зависимости от конфигурации:

```
# mount -o sec=krb5 server:/export /mnt
```

Не смотря на то, что рекомендуется использовать управление службой идентификации и аутентификации, также поддерживаются серверы Kerberos в Active Directory (AD). Больше информации вы найдете в п. 16.4.9. Настройка аутентификации Kerberos с использованием SSSD и Active Directory.

Подробные сведения см. на страницах руководств exports и nfs.

Защита NFS в версии NFSv4

В NFSv4 поддержка ACL реализована на базе модели Microsoft Windows NT, а не модели POSIX, в связи с возможностями модели Windows NT и ее широким применением.

Другой важной возможностью безопасности NFSv4 является отказ от использования прокола MOUNT для монтирования ФС. Протокол MOUNT представлял возможные уязвимости для безопасности из-за итого, каким образом он обрабатывал дескрипторы файлов.

Права доступа к файлам

После того, как ФС NFS смонтирована удаленным хостом с правами на чтение-запись, единственной защитой для каждого общего файла являются его права доступа. Если одна и та же ФС NFS будет смонтирована двумя пользователями с одинаковыми записями идентификатора пользователя, то эти пользователи смогут изменять файлы друг друга. Кроме того, любой пользователь, авторизованный в системе с правами root, может использовать команду sudo для доступа к любым файлам в пределах общего ресурса NFS.

По умолчанию в ОС РОСА «НИКЕЛЬ» активированы списки контроля доступа (ACL). Рекомендуется оставить эту возможность включенной.

По умолчанию при экспорте ФС NFS использует понижение привилегий для root, что устанавливает идентификатор пользователя любого, получившего доступ к общему ресурсу NFS с правами root локальной машины, на уровень nobody. Понижение привилегий root контролируется параметром по умолчанию `root_squash`.

Рекомендуется никогда не отключать понижение привилегий root.

При экспорте общего ресурса NFS на чтение/запись лучше использовать параметр all_squash. Этот параметр принудительно выдает каждому пользователю, получающему доступ к экспортированной ФС, идентификатор пользователя nfsnobody.

NFS и RPCBIND

Примечание. Сведения в данном разделе касаются только реализации NFSv3, для которой требуется служба rpcbind для обратной совместимости.

Утилита rpcbind отображает службы RPC на порты, на которых эти службы слушают. Процессы RPC уведомляют rpcbind о своем запуске, регистрируя порты, на которых они слушают, и сообщая программные номера RPC, которые они собирается обслуживать. Далее клиентская система передает rpcbind на сервере конкретный программный номер RPC. Служба rpcbind перенаправляет клиента на соответствующий номер порта, чтобы состоялся обмен информацией требуемой службой.

Поскольку для создания соединений со входящими клиентскими запросами службам на основе RPC требуется rpcbind, rpcbind должен быть доступен в системе до запуска любой из этих служб.

Для контроля доступа служба rpcbind использует надстройки TCP, а правила контроля доступа для rpcbind влияют на все службы на основе RPC. Как вариант, можно указать правила контроля доступа для каждого из демонов NFS RPC. Точный синтаксис написания этих правил можно найти на страницах руководств rpc.mountd и rpc.statd.

Поиск и устранение проблем с NFS и rpcbind

Поскольку rpcbind предоставляет координацию между службами RPC и номерами

портов, используемых для обмена с ними информацией, то при решении проблем бывает полезным просмотреть статус текущих служб RPC с помощью rpcbind. Команда rpcinfo показывает информацию о каждой службе на базе RPC с номерами портов, программный номер RPC. Номер версии и тип протокола IP (TCP или UDP).

Чтобы убедиться в том, что для rpcbind включены сочувствующие службы NFS на базе RPC, выполните следующую команду:

```
# rpcinfo -p
```

16.4.9. Настройка аутентификации Kerberos с использованием SSSD и Active Directory

Принципалы Kerberos и Active Directory

Active Directory разделяет принципалы Kerberos на две категории: принципалы пользователей и принципалы службы. Принципалы пользователей используются в процессе обмена службы аутентификации (AS) для получения мандата на получение мандата (TGT, Ticket Granting Ticket), а принципалы службы получаются в процессе обмена TGS (службы, предоставляющей мандаты, Ticket Granting Service) с использованием TGT. Учетная запись Active Directory может иметь множество принципалов службы, но только один принципал пользователя. Как результат, даже если в таблице ключей есть ключ для принципала, получить TGT с использованием этого принципала (например, через kinit) можно, только если этот принципал присутствует в поле `userPrincipalName` учетной записи ПК в Active Directory. Помимо этого, можно всегда получить TGT, используя принципал, совпадающий с атрибутом `sAMAccountName` в Active Directory (при условии, что для этого принципала есть ключ в таблице ключей). Обычно `sAMAccountName` — это короткое имя хоста с добавленным в начале символом $.

Также обратите внимание, что если при присоединении к Active Directory с помощью команды `net ads join` был указан параметр createupn, это действие обновляет только поле `userPrincipalName` в Active Directory. Поле `servicePrincipalName` нужно будет обновить либо с помощью инструмента «Пользователи и компьютеры Active Directory» в графическом интерфейсе пользователя, либо с помощью команды setspn.exe в консоли.

Принципалы Kerberos и NFS

Клиент NFS выполняет поиск используемого ключа в таблице ключей в таком порядке:

```
<hostname>$@<REALM>
```

<HOSTNAME>$@<REALM>

root/<hostname>@<REALM>

nfs/<hostname>@<REALM>

host/<hostname>@<REALM>

root/<anyname>@<REALM>

nfs/<anyname>@<REALM>

host/<anyname>@<REALM>

Клиент NFS сделает попытку получить TGT с помощью первого же найденного совпадающего принципала. Если с помощью этого принципала получить TGT невозможно (например, этот принципал не совпадает с атрибутами учетной записи ПК sAMAccountName или userPrincipalName в Active Directory), то тогда попытка создания контекста безопасности с сервером NFS будет неудачной. Клиент NFS **не** станет продвигаться по списку к следующему принципалу.

Хотя клиент NFS может использовать различные принципалы, сервер NFS выполнит обратный запрос NFSv4 для клиента только если клиент использовал принципал службы (смотрите последний блок в gssp_accept_sec_context_upcall в net/sunrpc/auth_gss/gss_rpc_upcall.c кода ядра).

Сервер NFS будет использовать только принципала службы NFS nfs/<hostname>@<REALM>.

И наконец, когда сервер NFS выполняет обратный запрос клиента NFS, по сути, сервер становится клиентом, а клиент становится сервером. Это означает, что для использования обратных вызовов в NFS с настроенным Kerberos как на клиенте, так и сервере должны выполняться и rpc.gssd, и gssproxy.

Администратор должен решить, использовать ли делегирование NFSv4. Если в делегировании NFSv4 нет необходимости, не нужно будет беспокоиться о том, сможет ли сервер выполнить обратный запрос к клиенту, и процесс настройки немного упростится.

Для обеспечения максимальной функциональности протокола NFSv4 рекомендуется настраивать использование принципалов служб NFS как на клиентах, так и на серверах NFS.

Шаги настройки, универсальные для всех машин

1) Установите необходимые пакеты (обратите внимание, что будут также установлены и пакеты с зависимостями):

dnf install realmd krb5-workstation sssd adcli samba-common oddjob oddjob-mkhomedir

2) Настройте параметры Kerberos в файле etc/krb5.conf:

```
includedir /var/lib/sss/pubconf/krb5.include.d/
[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log
[libdefaults]
default_realm = test.dom
dns_lookup_realm = false
dns_lookup_kdc = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
[realms] test.dom = {
kdc = addc.test.dom admin_server = addc.test.dom
}
[domain_realm]
.test.dom = test.dom
test.dom = test.dom
```

3) Получите TGT Kerberos для пользователя, имеющего права на присоединение к ПК в домене:

```
# kinit Administrator
```

4) Перед присоединением к домену выполните `realm discover`:

```
# realm discover test.dom
test.dom type: kerberos
realm-name: test.dom
domain-name: test.dom
configured: no
server-software: active-directory
client-software: sssd
required-package: oddjob
required-package: oddjob-mkhomedir
required-package: sssd
required-package: adcli
required-package: samba-common
```

5) Присоединитесь к домену:

– Если делегирование NFSv4 не нужно:

```
# realm join test.dom
```

– Если делегирование NFSv4 нужно:

```
# realm join --user-principal=nfs/server.test.dom@test.dom
test.dom
```

Примечания.

1. В вышеуказанной команде используется условное имя хоста сервера; при выполнении на сервере вставьте соответствующее значение.

2. Параметр `-user-principal` обновляет поле `userPrincipalName` учетной записи ПК в Active Directory. В отличие от поля `servicePrincipalName`, являющегося списком, поле `userPrincipalName` может содержать только один принципал.

3. Команда `realm join` автоматически обновляет параметры SSSD, PAM и nsswitch, а также запускает службу SSSD.

Шаги настройки для серверов NFS

6) Выполните вход на контролер домена Active Directory и запустите команду `setspn` для добавления принципала службы nfs сервера:

```
PS C:\Users\Administrator> setspn -A nfs/server.test.dom server
Checking domain DC=example,DC=com
Registering ServicePrincipalNames for
CN=server,CN=Computers,DC=example,DC=com
nfs/server.test.dom
Updated object
PS C:\Users\Administrator> setspn -L server
Registered ServicePrincipalNames for
CN=server,CN=Computers,DC=example,DC=com:
nfs/server.test.dom HOST/server.test.dom
HOST/SERVER
PS C:\Users\Administrator>
```

7) Запустите демон(ы) GSS.

Примечание. В ОС РОСА «НИКЕЛЬ» обработка данных учетных записей Kerberos со стороны потоков ядра nfsd на сервере NFS, а также работа службы обратных вызовов NFSv4 на клиенте NFS теперь контролируется демоном gssproxy, а не rpc.svcgssd.

– Если делегирование NFSv4 не нужно:

Проверьте, что gssproxy выполняется. По молчанию, она уже должна

выполняться, и ее не нужно включать в systemd.

```
# systemctl status gssproxy
```

– Если делегирование NFSv4 нужно:

Проверьте, что gssproxy выполняется и запустите службу rpc-gssd. Это нужно только непосредственно после присоединения к домену. При последующих перезапусках обе службы ложны запускаться автоматически, и ни одну из них не нужно включать в systemd.

```
# systemctl status gssproxy
# systemctl start rpc-gssd
```

8) Создайте запись в /etc/exports:

```
/export *(rw,sec=krb5:krb5i:krb5p)
```

Шаги настройки для клиентов NFS

6) Если делегирование NFSv4 **не нужно**, переходите к шагу 10). В противном случае войдите на контролер домена Active Directory и выполните команду `setspn` для добавления принципала службы nfs для клиента:

```
PS C:\Users\Administrator> setspn -A nfs/client.test.dom client
Checking domain DC=example,DC=com
Registering ServicePrincipalNames for
CN=client,CN=Computers,DC=example,DC=com
nfs/client.test.dom
Updated object
PS C:\Users\Administrator> setspn -L client
Registered ServicePrincipalNames for
CN=client,CN=Computers,DC=example,DC=com:
nfs/client.test.dom
HOST/client.test.dom
HOST/CLIENT
PS C:\Users\Administrator>
```

7) Для создания таблицы ключей, содержащей только принципала nfs, используйте команду `ktutil` (это нужно, чтобы rpc-gssd обязательно первым нашла принципала службы nfs):

Несколько полезных советов по использованию ktutil

– у ktutil есть только несколько простых команд, которые можно просмотреть с помощью «?»;

– при использовании команды delent остальные элементы списка перемещаются

вверх по списку. По этой причине лучше начинать с последней записи, которую нужно удалить, и продвигаться дальше вверх;

– при записи файла таблицы ключей с использованием команды wkt, то если файл таблицы ключей уже существует, то записи в памяти будут добавлены в файл. Перед выполнением записи нужно сначала проверить, существует ли таблица ключей, если такое поведение нежелательно.

```
[root@client ~]# ktutil
ktutil: rkt /etc/krb5.keytab
ktutil: l
slot KVNO Principal
---- ----
---------------------------------------------------------------
----
1
2
host/client.test.dom@test.dom

2
host/client.test.dom@test.dom
3
2
host/client.test.dom@test.dom
4
2
host/client.test.dom@test.dom
5
2
host/client.test.dom@test.dom
6
2
host/client@test.dom
7
2
host/client@test.dom
8
```

```
2
host/client@test.dom
9
2
host/client@test.dom
10
2
host/client@test.dom
11
2
CLIENT$@test.dom
12
2
CLIENT$@test.dom
13
2
CLIENT$@test.dom
14
2
CLIENT$@test.dom
15
2
CLIENT$@test.dom
16
2
nfs/client.test.dom@test.dom
17
2
nfs/client.test.dom@test.dom
18
2
nfs/client.test.dom@test.dom
19
2
nfs/client.test.dom@test.dom
20
```

```
2
nfs/client.test.dom@test.dom
ktutil: delent 15
ktutil: delent 14
ktutil: delent 13
ktutil: delent 12
ktutil: delent 11
ktutil: delent 10
ktutil: delent 9
ktutil: delent 8
ktutil: delent 7
ktutil: delent 6
ktutil: delent 5
ktutil: delent 4
ktutil: delent 3
ktutil: delent 2
ktutil: delent 1
ktutil: l
slot KVNO Principal
---- ----
------------------------------------------------------------------
----


nfs/client.test.dom@test.dom
2
2
nfs/client.test.dom@test.dom

2
nfs/client.test.dom@test.dom

2
nfs/client.test.dom@test.dom

2
```

```
nfs/client.test.dom@test.dom
ktutil: wkt /etc/nfs.keytab
ktutil: q
[root@client ~]#
```

8) Если делегирование NFSv4 необходимо, отредактируйте файл etc/sysconfig/nfs, раскомментировав строку RPCGSSDARGS и добавив следующее:

```
RPCGSSDARGS="-k /etc/nfs.keytab"
```

9) Обновите конфигурацию NFS:

```
systemctl restart nfs-config
```

10)Запустите демоны GSS.

– Если делегирование NFSv4 не нужно:

Запустите службу rpc-gssd. Это нужно только непосредственно после присоединения к домену. Во время последующих перезапусков служба должна запускаться автоматически, и включать ее в systemd не нужно.

```
# systemctl start rpc-gssd
```

– Если делегирование NFSv4 нужно:

Проверьте, что gssproxy выполняется, и запустите службу rpc-gssd. Это необходимо только непосредственно после присоединения к домену. Во время последующих перезапусков обе службы должны запускаться автоматически, и включать их в systemd не нужно.

```
# systemctl status gssproxy
# systemctl start rpc-gssd
```

Примечание. В текущей версии ОС РОСА «НИКЕЛЬ» обработка данных учетных записей Kerberos со стороны потоков ядра nfsd на сервере NFS, а также работа службы обратных вызовов NFSv4 на клиенте NFS контролируются демоном gssproxy, а не rpc.svcgssd.

Теперь у системного администратора ОС РОСА «НИКЕЛЬ» есть возможность монтировать ФС NFS с помощью `sec=krb5`, `sec=krb5i` или `sec=krb5p`.

Доступная локально документация по NFS

Администрирование сервера NFS может быть нелегкой задачей. Для экспорта или монтирования общих ресурсов NFS существует много параметров, включая в том числе и упомянутые в данном руководстве. Подробности ищите на страницах следующих руководств:

– man mount — исчерпывающая информация о параметрах mount как для конфигурации сервера, так и для конфигурации клиента NFS;

– man fstab — сведения о формате файла /etc/fstab, который используется при монтировании ФС при загрузке системы;

– man nfs — подробности об операциях экспорта и импорта ФС NFS;

– man exports — общие параметры, используемые в файле /etc/exports для экспорта ФС NFS.

16.5. Samba

Samba — это стандартный набор свободных программ Linux для взаимодействия с ОС Windows, реализующий сетевой протокол Server Message Block (SMB). Протокол SMB предоставляет Microsoft Windows, Linux, Unix и другим ОС возможность доступа к общим файлам и принтерам с помощью серверов, поддерживающих этот протокол.

Примечание. Чтобы иметь возможность работать с Samba, убедитесь, что пакет samba установлен в системе. Для этого выполните следующую команду:

```
$ rpm -qa samba\*
```

Samba является важным компонентом бесшовной интеграции серверов и рабочих станций Linux в окружение Active Directory (AD). Она может выполнять роль как контроллера домена (в стиле NT4), так и обычного члена домена (в стиле Active Directory или NT4).

Что может Samba:

– обеспечивать доступ к деревьям каталога и принтерам;

– помогать в просмотре сети (с NetBIOS);

– выполнять аутентификацию для входа в домен Windows;

– предоставлять разрешение имен сервера доменных имен Windows (WINS);

– выступать первичным контроллером домена (PDC) в стиле Windows NT®;

– выступать резервным контроллером домена (BDC) для первичных контроллеров домена на базе Samba;

– выполняет роль сервера-члена домена Active Directory;

– присоединяться к Windows NT/2000/2003/2008 PDC/Windows Server 2012.

Чего не может Samba:

– выступать резервным контроллером домена (BDC) для первичного контроллера домена на базе Windows (PDC) (и наоборот);

– выполнять роль контроллера домена Active Directory.

Примечание. Перед установкой и настройкой SMB-сервера необходимо убедиться, что в файле /etc/hosts прописано верное FDQN-имя сервера. Для проверки

выполните следующую команду:

```
hostname -f
```

Убедитесь, что в ответ на нее система не выдает ошибку. В противном случае отредактируйте файл /etc/hosts, внеся в него следующую строку:

```
<IP-адрес> <каноническое_имя_сервера> <псевдоним(ы)>
```

16.5.1. Демоны и службы Samba

Samba базируется на работе трех демонов — smbd, nmbd и winbindd. Три службы — smb, nmb и winbind — контролируют процесс запуска и остановки демонов, а также выполняют другие служебные действия. Эти службы играют роль сценариев инициализации. Каждый демон подробно описывается ниже, а также указывается, какая именно служба его контролирует **smbd**

Серверный демон smbd предоставляет услуги по доступу к общим файлам и принтерам для клиентов Windows. Кроме того, он отвечает за аутентификацию пользователей, блокирование ресурсов и предоставление доступа к общим данным с использованием протокола SMB. Порты по умолчанию, на которых сервер слушает трафик SMB — порты TCP 139 и 445.

Демон smbd контролируется службой smb.

nmbd

Серверный демон nmbd понимает запросы службы имен NetBIOS и отвечает на них. Это могут быть, например, запросы SMB/CIFS в системах на базе Windows. Также демон принимает участие в протоколах просмотра, задействованных в сетевом окружении Windows. Порт по умолчанию, на котором сервер слушает трафик NMB, это UDP 137. Демон nmbd контролируется службой nmb.

winbindd

Служба winbind разрешает информацию пользователя и группы, полученную с сервера, на котором установлена ОС Windows NT, 2000, 2003, Windows Server 2008 или Windows Server 2012, и делает эту информацию понятной для платформ UNIX. Это достигается использованием вызовов Microsoft RPC, модулей PAM и NSS. В итоге, пользователи домена Windows NT и Active Directory представляются и действуют, как пользователи UNIX на машине UNIX. Несмотря на то, что служба winbind идет в программном составе Samba, она контролируется отдельно от службы smb.

Демон winbind контролируется службой winbind и не требует для своей работы запуска службы smb. winbind также используется с Samba в качестве члена Active Directory, и также может использоваться на контроллере домена Samba (для реализации

вложенных групп и доверия между доменами).

Примечание. Список утилит, включенных в состав Samba, можно посмотреть в подразделе Программы в составе Samba.

16.5.2. Подключение к общему ресурсу Samba с помощью smbclient

Утилита smbclient дает возможность подключаться к общему ресурсу SMB и выполнять действия, аналогичные действиям клиента FTP. Чтобы, например, подключиться к Demo_Share на хосте SMB-Server и выполнить аутентификацию с использованием имени пользователя administrator, выполните следующую команду:

```
# smbclient //SMB-Server/Demo_Share -Uadministrator
```

После удачного входа введите `help` для просмотра списка доступных команд:

```
smb:\> help
```

Чтобы, например, перейти в каталог Example, выполните:

```
smb:\> cd Example
```

Для отключения выполните:

```
smb:\> exit
```

16.5.3. Монтирование общего ресурса

Иногда бывает удобным смонтировать общий ресурс Samba в каталог, чтобы файлы в каталоге обрабатывались так, как будто они являются частью локальной ФС.

Чтобы смонтировать общий ресурс Samba в каталог, создайте каталог для монтирования (если он еще не существует) и выполните следующую команду:

```
mount -t cifs //servername/sharename /mnt/point/ -o username=username,password=password
```

Эта команда монтирует общий ресурс sharename с сервера servername в локальный каталог /mnt/point/.

Подробную информацию о монтировании общих ресурсов Samba см. на странице руководства mount.cifs.

Примечание. Утилита mount.cifs поставляется в отдельном пакете RPM (независимо от Samba). Перед использованием mount.cifs убедитесь, что в системе установлен пакет cifs-utils. выполните следующую команду:

```
# rpm install cifs-utils\*
```

Обратите внимание, что в пакет cifs-utils также включен бинарный файл cifs.upcall, вызываемый ядром для монтирования CIFS с настроенной поддержкой Kerberos. Подробности о cifs.upcall см. на странице руководства cifs.upcall(8).

Примечание. Некоторые серверы CIFS для аутентификации требуют

незашифрованные пароли в открытом виде. Поддержку простых текстовых паролей можно включить с помощью следующей команды:

```
# echo 0x37 > /proc/fs/cifs/SecurityFlags
```

Отмена шифрования паролей может стать причиной утечки паролей!

16.5.4. Настройка сервера Samba

Конфигурационный файл по умолчанию (/etc/samba/smb.conf) дает пользователям возможность рассматривать свои домашние каталоги как общий ресурс Samba. Также общими ресурсами Samba становятся настроенные в системе принтеры. На подключенный к системе принтер можно посылать задания печати с сетевых машин Windows.

Конфигурация в командной строке

В качестве конфигурационного файла Samba использует /etc/samba/smb.conf. Изменения, вносимые в этот файл, не применяются до перезапуска демона Samba:

```
# systemctl restart smb.service
```

Чтобы указать рабочую группу Windows и краткое описание сервера Samba, добавьте следующие записи в файл /etc/samba/smb.conf:

```
workgroup = WORKGROUPNAME
server string = <краткий_комментарий_о_сервере>
```

Чтобы создать общий каталог Samba в системе Linux, добавьте следующий раздел в файл /etc/samba/smb.conf (после того, как в него были внесены изменения, отражающие требования и параметры системы):

Пример: типовая конфигурация сервера Samba

```
[sharename]
comment = Insert a comment here
path = /home/share/
valid users = ivanov petrov
writable = yes
create mask = 0765
```

В примере выше пользователям ivanov и petrov разрешается читать и писать в каталоге /home/share/ на сервере Samba с клиента Samba.

Шифрование паролей

Шифрование паролей включено по умолчанию как более надежный вариант защиты. Чтобы создать пользователя с зашифрованным паролем, используйте утилиту smbpasswd:

```
smbpasswd -a username
```

16.5.5. Запуск и остановка Samba

Чтобы запустить сервер Samba, выполните следующую команду:

```
# systemctl start smb.service
```

Примечание. Чтобы настроить сервер как член домена, перед запуском службы smb нужно присоединиться к домену или к Active Directory с помощью команды net join. Кроме того, перед запуском smbd рекомендуется запустить winbind. Для остановки сервера выполните:

```
# systemctl stop smb.service
```

Параметр restart — быстрый способ остановить и затем сразу снова запустить Samba. Это самый надежный способ применить изменения, внесенные в конфигурацию Samba. Обратите внимание, что параметр restart запустит демон, даже если до этого он не был запущен.

Чтобы перезапустить сервер, выполните:

```
# systemctl restart smb.service
```

Параметр `condrestart` (conditional restart, условный перезапуск) перезапустит smb, только если он уже выполняется. Этот параметр удобен для сценариев, т. к. демон не будет запущен, если он не выполняется.

Примечание. Если в файл /etc/samba/smb.conf были внесены изменения, Samba автоматически перезагрузит его через несколько минут. Перезапуск или перезагрузка вручную имеет такой же результат.

Для условного перезапуска сервера выполните:

```
# systemctl try-restart smb.service
```

Ручная перезагрузка файла /etc/samba/smb.conf может пригодиться в случае сбоя автоматической перезагрузки со стороны службы smb.

```
# systemctl reload smb.service
```

По умолчанию служба smb не запускается автоматически при загрузке системы.

Чтобы настроить автоматический запуск службы, выполните:

```
# systemctl enable smb.service
```

16.5.6. Режимы безопасности Samba

Для Samba существуют два типа защиты — share-level и user-level — которые в совокупности известны как «уровни безопасности». Защита share-level устарела и была удалена из Samba, конфигурации с этим уровнем защиты необходимо обновить на использование user-level. Защита user-level может быть реализована одним из трех различных способов, которые называются режимами безопасности.

Защита user-level

Защита уровня user-level применяется по умолчанию и является рекомендуемым уровнем для Samba. Даже если директива `security = user` не указана в файле /etc/samba/smb.conf, она используется в Samba. Если сервер принимает имя пользователя и пароль клиента, то клиент может затем смонтировать несколько общих ресурсов без указания пароля для действий с каждым из них. Samba также принимает запросы имени пользователя и пароля на сеансовой основе. Клиент поддерживает несколько контекстов аутентификации, используя уникальный UID для каждого входа.

В файле /etc/samba/smb.conf директива security = user, настраивающая защиту уровня user-level, имеет следующий вид:

```
[GLOBAL]
...
security = user
...
```

Гостевые ресурсы Samba

Как упоминалось выше, режим защиты share-level является устаревшим. Чтобы настроить гостевой ресурс Samba без применения параметра security = share, выполните следующие шаги:

Настройка гостевых ресурсов Samba

1) Создайте файл отображения имени пользователя, в нашем примере это /etc/samba/smbusers, и добавьте в него следующую запись:

```
nobody = guest
```

2) Добавьте следующие директивы в главный раздел файла /etc/samba/smb.conf. Не используйте директив действительных пользователей:

```
[GLOBAL]
...
security = user map to guest = Bad User
username map = /etc/samba/smbusers
...
```

Директива username map указывает путь к файлу отображения пользователей, упоминаемому в предыдущем шаге.

3) Добавьте следующую директиву в раздел share файла /ect/samba/smb.conf. Не используйте директив действительных пользователей.

```
[SHARE]
...
```

```
guest ok = yes
...
```

Ниже описываются другие реализации защиты уровня user-level.

Режим domain security (уровень User-Level)

В режиме защиты domain сервер Samba имеет учетную запись ПК (учетная запись domain security trust) и принудительно направляет все запросы авторизации через контроллеры доменов. Сервер Samba превращается в сервер-член домена с помощью следующих директив в файле /etc/samba/smb.conf:

```
[GLOBAL]
...
security = domain
workgroup = ARKETING
...
```

Режим безопасности Active Directory (уровень user-level)

В окружении Active Directory есть возможность присоединения к домену в качестве естественного члена Active Directory. Даже если политика безопасности запрещает использование протоколов аутентификации, совместимых с NT, сервер Samba может присоединиться к Active Directory при помощи Kerberos. Samba в режиме члена Active Directory может принимать билеты Kerberos.

Следующие директивы в файле /etc/samba/smb.conf делают Samba членом сервера

Active Directory:

```
[GLOBAL]
...
security = ADS realm = XAMPLE.COM
password server = kerberos.example.com
...
```

Безопасность уровня share-level

На уровне безопасности share-level сервер принимает от клиента только пароль, без явно указанного имени пользователя. Для каждого ресурса сервер создает пароль, независимо от имени пользователя. Известны случаи, когда клиенты Microsoft Windows сталкивались с проблемами совместимости при работе с серверами с уровнем безопасности share-level. Этот режим устарел и был удален из Samba. Конфигурации, содержащие `security = share`, должны быть обновлены для использования уровня user-level.

16.5.7. Просмотр сетевых ресурсов Samba

Возможность просмотра сетевых ресурсов позволяет серверам Samba и Windows присутствовать в «Сетевом окружении» Windows. Внутри «Сетевого окружения» значки представляют серверы, и при их открытии показываются доступные общие ресурсы и принтеры сервера.

Возможности просмотра сети требуют реализации NetBIOS по TCP/IP. Для возможности управления списком просмотра ресурсов, в сетях на базе NetBIOS используются широковещательные сообщения (UDP). В отсутствие таких наиболее очевидных способов для разрешения имен хостов TCP/IP, как NetBIOS и WINS, необходимо использовать другие способы, например статичные файлы (/etc/hosts) или DNS.

Главный обозреватель сети домена собирает и сравнивает списки просмотра локальных главных обозревателей всех подсетей, так чтобы просмотр сети можно было осуществлять между всеми рабочими группами и подсетями. Кроме того, главный обозреватель домена предпочтительно должен быть локальным главным обозревателем в своей подсети.

Просмотр доменов

По умолчанию Windows-первичный контроллер домена также является главным обозревателем сети этого домена. Сервер Samba не должен настраиваться как главный сервер домена в таких ситуациях.

Для подсетей, в которых отсутствует первичный контроллер домена под управлением Windows, сервер Samba может быть реализован как локальный главный обозреватель. Параметры файла /etc/samba/smb.conf для главного локального обозревателя сети (или совсем без просмотра сети) в окружении контроллера домена совпадают с параметрами для рабочей группы (см. подраздел 16.5.4. Настройка сервера Samba.).

16.5.8. WINS (Windows Internet Name Server)

В качестве сервера WINS может выступать либо сервер Samba, либо сервер Windows NT. Если сервер WINS используется с включенном NetBIOS, одноадресные передачи UDP можно маршрутизировать, что позволяет использовать разрешение имен между различными сетями. В отсутствии сервера WINS передача UDP ограничена локальной подсетью и, соответственно, не может быть маршрутизирована в другие подсети, рабочие группы или домены. Если необходимо использовать репликацию WINS, не используйте Samba в качестве первичного сервера WINS, поскольку на настоящее

время Samba не поддерживает репликацию WINS.

В смешанном окружении Samba и сервера NT/2000/2003/2008 рекомендуется использовать возможности Microsoft WINS. В чистом окружении Samba рекомендуется для WINS использовать только один сервер Samba.

Ниже приведен пример файла /etc/samba/smb.conf, в котором сервер Samba настроен в качестве сервера WINS:

Пример: пример конфигурации сервера WINS

```
[global]
wins support = yes
```

Примечание. Все серверы, включая Samba, для разрешения имен должны подключаться к серверу WINS. Без WINS можно осуществлять просмотр только локальной подсети. И даже если каким-то образом будет доступен список всех машин домена, хосты невозможно будет разрешить без WINS.

16.5.9. Программы в составе Samba

net

```
net <протокол> <функция> <дополнительные_параметры>
<параметры_цели>
```

Утилита net похожа на утилиту net, используемую в Windows и MS-DOS. Первый аргумент служит для указания протокола, используемого при выполнении команды. Значения протокола для указания типа серверного подключения могут быть следующими: `ads`, `rap` или `rpc`. Active Directory использует `ads`, Win9x/NT3 — `rap`, а Windows NT4/2000/2003/2008/2012 — `rpc`. Если протокол не указывается, net автоматически попытается его определить.

В примере ниже показывается список общих ресурсов, доступных для хоста с именем wakko:

```
$ net -l share -S wakko
Password:
Enumerating shared resources (exports) on remote server:
Share name  Type   Description
----------  ----   ----------
data     Disk   Wakko data share
tmp     Disk   Wakko tmp share
IPC$     IPC   IPC Service (Samba Server)
ADMIN$    IPC   IPC Service (Samba Server)
```

В примере ниже показывается список пользователей Samba для хоста с именем

wakko:

```
$ net -l user -S wakko
root password:
User name       Comment
-----------------------------------
andriusb       Documentation
joe          Marketing
lisa         Sales
```

nmblookup

```
nmblookup <параметры> <имя_netbios>
```

Программа nmblookup разрешает имена NetBIOS в IP-адреса. Программа посылает свои запросы в локальную подсеть до тех пор, пока целевая машина не ответит.

В примере ниже показан IP-адрес трека имени NetBIOS:

```
$ nmblookup trek
querying trek on 10.1.59.255
10.1.56.45 trek<00>
```

pdbedit

```
pdbedit <параметры>
```

Программа pdbedit управляет учетными записями, расположенными в базе данных SAM. Поддерживаются все серверные программы, включая smbpasswd, LDAP и библиотека баз данных tdb.

Ниже показан пример добавления, удаления и получения списка пользователей:

```
$ pdbedit -a kristin
new password:
retype new password: Unix
username:    kristin
NT username:
Account Flags:    [U     ]
User SID:       S-1-5-21-1210235352-3804200048-1474496110-
2012
Primary Group SID:  S-1-5-21-1210235352-3804200048-1474496110-
2077
Full Name: Home Directory:    \\wakko\kristin
HomeDir Drive:
```

```
Logon Script:
Profile Path:     \\wakko\kristin\profile
Domain:        WAKKO
Account desc:
Workstations: Munged
dial:
Logon time:      0
Logoff time:     Mon, 18 Jan 2038 22:14:07 GMT
Kickoff time:     Mon, 18 Jan 2038 22:14:07 GMT
Password last set:  Thu, 29 Jan 2004 08:29:28
GMT Password can change: Thu, 29 Jan 2004 08:29:28 GMT
Password must change: Mon, 18 Jan 2038 22:14:07 GMT
$ pdbedit -v -L kristin
Unix username:    kristin NT username:
Account Flags:    [U     ]
User SID:       S-1-5-21-1210235352-3804200048-1474496110-
2012
Primary Group SID:  S-1-5-21-1210235352-3804200048-1474496110-
2077
Full Name:
Home Directory:    \\wakko\kristin HomeDir Drive:
Logon Script:
Profile Path:     \\wakko\kristin\profile
Domain:        WAKKO Account desc:
Workstations: Munged
dial:
Logon time:      0
Logoff time:     Mon, 18 Jan 2038 22:14:07 GMT
Kickoff time:     Mon, 18 Jan 2038 22:14:07 GMT
Password last set:  Thu, 29 Jan 2004 08:29:28 GMT
Password can change: Thu, 29 Jan 2004 08:29:28 GMT
Password must change: Mon, 18 Jan 2038 22:14:07 GMT
$ pdbedit -L
andriusb:505:
joe:503:
lisa:504:
```

```
kristin:506:
~]$ pdbedit -x joe
~]$ pdbedit -L andriusb:505: lisa:504: kristin:506:
```

rpcclient

```
rpcclient <сервер> <параметры>
```

Программа rpcclient вызывает административные команды, используя Microsoft RPC (вызов удаленных процедур Microsoft), предоставляя доступ к графическому интерфейсу администратора Windows для управления системами. Чаще всего этот интерфейс используется продвинутыми пользователями, понимающими всю сложность вызова удаленных процедур Microsoft.

smbcacls

```
smbcacls <//сервер/общий_ресурс> <имя_файла> <параметры>
```

Программа smbcacls изменяет списки доступа Windows к файлам и каталогам, являющимися общими ресурсами на сервере Samba или Windows.

smbclient

```
smbclient <//сервер/общий_ресурс> <пароль> <параметры>
```

Программа smbclient — это гибкий клиент UNIX с возможностями, аналогичными возможностям утилиты ftp.

smbcontrol

```
smbcontrol -i <параметры>
smbcontrol <параметры> <место_назначения> <тип_сообщения> <аргументы>
```

Программа smbcontrol посылает контрольные сообщения выполняющимся демонам smbd, nmbd или winbindd. Выполнение `smbcontrol -i` запускает команды интерактивно до тех пор, пока не будет введена пустая строка или символ `q`.

smbpasswd

```
smbpasswd <параметры> <имя_пользователя> <пароль>
```

Программа smbpasswd управляет зашифрованными паролями. Эта программа может выполняться суперпользователем для изменения пароля любого обычного пользователя, а также обычным пользователем для изменения своего собственного пароля Samba.

smbspool

```
smbspool <задача> <пользователь> <название> <копий> <параметры>
<имя_файла>
```

Программа smbspool представляет собой интерфейс печати Samba, совместимый

с CUPS. Разработанный в первую очередь для работы с принтерами CUPS, smbspool может работать также и принтерами, не управляемыми CUPS.

smbstatus

```
smbstatus <параметры>
```

Программа smbstatus показывает статус текущих подключений к серверу Samba.

smbtar

```
smbtar <параметры>
```

Программа smbtar создает (а также распаковывает обратно) резервные копии общих файлов и каталогов Windows в ленточных архивах. Программа похожа на утилиту tar, но эти две программы не совместимы между собой.

testparm

```
testparm <параметры> <имя_файла> <имя_хоста адрес_IP>
```

Программа testparm проверяет синтаксис файла /etc/samba/smb.conf. Если файл smb.conf расположен в каталоге по умолчанию (/etc/samba/smb.conf), местоположение файла указывать не нужно. При указании имени хоста и IP-адреса проверяется правильность конфигурации в файлах hosts.allow и host.deny. После проверки программа testparm также выводит сводку текущего файла smb.conf и выполняемой роли сервера (одиночный, домен и т. д.). Это удобно при отладке, поскольку комментарии отсекаются, и информация предоставляется в сжатом виде, в котором ее могут прочитать опытные администраторы. Например:

```
$ testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[tmp]"
Processing section "[html]" Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions
<enter>
# Global parameters
[global]
workgroup = MYGROUP
server string = Samba Server
security = SHARE
log file = /var/log/samba/%m.log
```

```
max log size = 50
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
dns proxy = no
[homes]
comment = Home Directories
read only = no browseable = no
[printers]
comment = All Printers
path = /var/spool/samba
printable = yes
browseable = no
[tmp]
comment = Wakko tmp path = /tmp guest only = yes
[html]
 comment = Wakko www
path = /var/www/html force
user = andriusb force
group = users
read only = no guest
only = yes
```

wbinfo

```
wbinfo <параметры>
```

Программа wbinfo показывает информацию, поступающую от демона winbindd. Для работы программы wbinfo необходим запущенный демон winbindd.

Доступная локально документация по Samba

/usr/share/doc/samba-<номер-версии>/ — все дополнительные файлы, входящие в состав пакета программ Samba. Сюда включены все вспомогательные сценарии, примеры конфигурационных файлов, а также документация.

Подробные сведения о конкретных возможностях Samba ищите на страницах следующих руководств:

- smb.conf(5);
- samba(7);
- smbd(8);
- nmbd(8);
- winbindd(8).

17. УПРАВЛЕНИЕ ПЕЧАТЬЮ

17.1. Служба CUPS и консольная утилита lpadmin

CUPS (Common UNIX Printing System) — сервер печати, используемый в ОС на основе Linux. СВТ с запущенным сервером CUPS представляет собой сетевой узел, который принимает задания на печать от клиентов, обрабатывает их и отправляет на соответствующий принтер.

17.1.1. Установка и управление службой CUPS

```
# dnf -y install cups
```

Запуск службы:

```
# systemctl start cups.service
```

Автоматический запуск службы при загрузке системы:

```
# systemctl enable cups.service
```

Перезапуск службы:

```
# systemctl restart cups.service
```

Просмотр статуса службы:

```
$ systemctl status cups.service
```

Немедленная остановка службы:

```
# systemctl stop cups.service
```

Базовый источник документации в локальной установке службы CUPS расположен по адресу http://localhost:631/help.

17.1.2. Консольная утилита lpadmin

Утилита lpadmin служит для настройки параметров службы печати lp в системах Linux.

lpadmin настраивает очереди принтеров и классов, предоставленных службой печати CUPS. Также lpadmin можно использовать для указания принтера или класса по умолчанию на сервере.

Параметры команды lpadmin:

– `-E`, указанный перед параметрами `-d`, `-p` или `-x`, служит для принудительного использования шифрования при соединении с сервером;

– `-d` – указывает цель (принтер или класс) по умолчанию. Дальнейшие задачи печати, переданные с использованием команд lp или lpr, будут использовать эту цель до

тех пор, пока пользователь не укажет другой принтер с помощью команды lpoptions;

– -p – настраивает именованный принтер или класс. Дополнительные параметры описываются ниже;

– -x – удаляет цель (принтер или класс) по умолчанию. Любые задачи, стоящие в очереди для этой цели, будут удалены, а текущее задание печати будет аварийно отменено.

Синтаксис команды lpadmin

```
lpadmin [ -E ] [-U <имя_пользователя>] [ -h <сервер>[:<порт>] ]
-d <цель>
lpadmin [ -E ] [-U <имя_пользователя>] [ -h <сервер>[:<порт>] ]
-p <цель>
    [ -R <имя_по_умолчанию> ] <параметр(ы)>
lpadmin [ -E ] [-U <имя_пользователя>] [ -h <сервер>[:<порт>] ]
-x <цель>
```

Параметры lpadmin

Для настройки очереди принтера используются следующие параметры:

– -c <класс> добавляет именованный принтер к классу. Если класс не существует, он создается автоматически;

– -i <интерфейс> настраивает сценарий интерфейса для принтера в стиле System V. Этот параметр нельзя уточнить с помощью параметра -P (файл PPD), и он предназначен для поддержки драйверов старых принтеров;

– -m <модель> настраивает стандартный сценарий с интерфейсом System V, файл PPD из каталога моделей или с использованием одного из интерфейсов драйвера. Для получения списка поддерживаемых моделей применяйте команду lpinfo с ключом -m;

– -o cupsIPPSupplies=true, -o cupsIPPSupplies=false указывает, нужно ли сообщать значения уровня ресурсов IPP (Internet Printing Protocol, «протокол печати через интернет»);

– -o job-k-limit=value устанавливает лимит квоты на каждого пользователя (в КБ). Значение — целое число килобайтов, один килобайт = 1024 байт;

– -o job-page-limit=value устанавливает лимит страниц для квот на каждого пользователя. Значение — целое число страниц, которое можно напечатать; при двусторонней печати одна сторона = одна страница;

– -o job-quota-period=value устанавливает учетный период для квот на каждого пользователя. Значение — целое число секунд; один день равен 86 400 с;

– -o job-sheets-default=<титул>[, <титул>] настраивает титульную страницу (или страницы) по умолчанию для задач печати;

– -o имя=значение указывает параметр PPD для принтера. Список параметров PPD можно получить с помощью команды lpoptions -l;

– -o <имя_по_умолчанию>=<значение> указывает серверный параметр по умолчанию для цели. Любой параметр печати можно сделать параметром по умолчанию; чтобы, например, установить значение cpi по умолчанию равным 17, используйте -o cpi-default=17;

– -o port-monitor=<имя> указывает, какую программу бинарной связи нужно использовать во время печати — нет, bcp или tbcp. По умолчанию — нет. Указанный монитор порта должен присутствовать в файле PPD;

– -o printer-error-policy=<имя> указывает политику ошибок, используемую, если фоновая программа принтера не может послать задачу на принтер. Имя должно быть одним из следующих: abort-job, retry-job, retry-current-job или stop-printer. Политика ошибок по умолчанию: stop-printer для принтеров, retry-current-job — для классов;

– -o printer-is-shared=[true|false] делает цель общей/опубликованной (shared/published) или недоступной для общего пользования/неопубликованной (unshared/unpublished). Общие/опубликованные цели публично объявляются сервером в LAN на основе параметра Browse в cupsd.conf, а недоступные для общего пользования/неопубликованные цели не объявляются. Значение по умолчанию — true;

– -o printer-op-policy=<имя> указывает политику работы IPP (протокол печати через интернет), связанную с целью. Имя должно быть указано в файле cupsd.conf в разделе Policy. Политика работы по умолчанию — default;

– -R <имя_по_умолчанию> удаляет параметр named для принтера

– -r <класс> удаляет именованный принтер из класса. Если в итоге класс становится пустым, он тоже удаляется.

– -u [allow: пользователь, пользователь, @группа; deny: пользователь, пользователь, @группа; allow: all, deny: none] настраивает контроль доступа пользователей для цели. Имена, начинающиеся с символа @, интерпретируются как группы UNIX. Последние два параметра отключают контроль за доступом на пользовательском уровне;

– -v "device-uri" устанавливает атрибут device-uri для очереди принтера. Для получения списка поддерживаемых адресов URI и схем для устройства используйте

команду `lpinfo -v`;

– `-D "info"` предоставляет текстовое описание цели;

– `-E` активирует цель и принимает задачи; аналог выполнения программ cupsaccept и cupsenable для цели;

– `-L "<местонахождение>"` предоставляет текстовое местонахождение цели;

– `-P <файл_ppd>` указывает на файл PPD, который нужно использовать для принтера. При наличии этого параметра он имеет больший приоритет, чем параметр `-i` (сценарий интерфейса).

Примеры использования lpadmin

Примечание. Параметры, используемые в командной строке, нельзя группировать.

Получение списка устройств

```
# lpinfo -v
$ /usr/lib/cups/backend/snmp <адрес_ip> # для нахождения URI ис-
пользуйте SNMP
```

Получение списка моделей

```
$ lpinfo -m
```

Добавление новой очереди

```
# lpadmin -p имя_очереди -E -v uri -m модель
```

Имя очереди определяет пользователь.

Пример:

```
# lpadmin -p HP_DESKJET_940C -E -v "usb://HP/DESKJET%20940C?
serial=CN16E6C364BH" -m drv:///HP/hp-deskjet_940c.ppd.gz
# lpadmin -p AirPrint -E -v "ipp://10.0.1.25/ipp/print" -m
everywhere # очередь без драйвера (Apple AirPrint или IPP
Everywhere)
# lpadmin -p SHARED_PRINTER -m raw # простая очередь; без PPD
или фильтра
```

Указание принтера по умолчанию (цели)

```
$ lpoptions -d имя_ очереди
```

Смена параметров

Просмотр списка параметров:

```
$ lpoptions -p имя_ очереди -l
```

Назначение параметров:

```
$ lpoptions -p имя_ очереди -o option=value
```

Пример:

```
$ lpoptions -p HP_DESKJET_940C -o PageSize=A4
```

Проверка статуса

```
$ lpstat -s
$ lpstat -p <имя_очереди>
```

Отключение принтера

```
# cupsdisable <имя_очереди>
```

Включение принтера

```
# cupsenable <имя_очереди>
```

Настройка принтера на принятие задач

```
# cupsaccept <имя_очереди>
```

Удаление принтера

1) Настройте принтер на сброс всех входящих запросов:

```
# cupsreject <имя_очереди>
```

2) Отключите принтер:

```
# cupsdisable <имя_очереди>
```

3) Удалите принтер:

```
# lpadmin -x <имя_очереди>
```

Печать файла

```
$ lpr файл
$ lpr -# 17 файл # напечатать файл 17 раз
$ echo "Hello, world!" | lpr -p # напечатать вывод команды. Параметр -p добавляет заголовок
```

Проверка очереди

```
$ lpq
$ lpq -a # во всех очередях
```

Очистка очереди

Команда для удаления последнего элемента в очереди:

```
# lprm
```

Команда удаляет все элементы в очереди:

```
# lprm -
```

Добавление принтера

Чтобы добавить принтер с именем Laserjet, расположенный в сети по адресу 10.1.1.1., с использованием файла драйвера CUPS laserjet.ppd, выполните:

```
lpadmin -p LaserJet -E -v socket://10.1.1.1 -m laserjet.ppd
```

Дополнительную информацию об использовании утилит командной строки CUPS можно найти в локальной документации по адресу http://localhost:631/help/options.html. Примеры установки параметров печати в командной строке с помощью lpadmin.

Данный параграф содержит ответы на следующие вопросы:

– Как настроить принтер, драйверы которого есть в составе пакетов ОС РОСА «НИКЕЛЬ», с использованием командной строки?

– Как с помощью консоли добавить очередь печати, которая бы указывала на последовательное устройство?

– Как добавить принтер(ы) в сервер печати CUPS без использования графических утилит?

– У нас в организации настроены сотни принтеров, но на данный момент мы имеем неупорядоченную смесь из сокетов/LPD, имен/адресов IP и различных драйверов. Как нам стандартизировать и упорядочить все имеющиеся принтеры и их параметры с использованием консольных команд?

Решение:

Если для устанавливаемого принтера уже имеется файл PPD (PostScript Printer Definition), переходите к шагу 4.

1) Установите самые свежие пакеты foomatic и hplip:

```
dnf -y install foomatic hplip
```

2) Получите список поддерживаемых принтеров с помощью команды lpinfo:

```
lpinfo -m
```

Пример: требуется получить список файлов PPD, доступных для принтера Ricoh Aficio MP 2000.

```
# lpinfo -m | grep -i 'aficio.*2000'
foomatic-db-ppds/Ricoh/PS/Ricoh-Aficio_CL2000_PS.ppd.gz Ricoh
Aficio
CL2000 PS
foomatic-db-ppds/Ricoh/PS/Ricoh-Aficio_MP_2000_PS.ppd.gz Ricoh
Aficio MP
2000 PS
foomatic-db-ppds/Ricoh/PXL/Ricoh-Aficio_MP_2000_PXL.ppd.gz Ricoh
Aficio
MP 2000 PXL
```

3) Для получения списка доступных устройств печати воспользуйтесь командой lpinfo. Например:

```
# lpinfo -v
network socket
network https
network ipps
network ipp
network http
network lpd
direct hp
serial serial:/dev/ttyS0?baud=115200
network beh
direct hpfax
network smb
```

4) Соберите все в одну очередь печати с помощью команды lpadmin:

```
lpadmin -p <имя_очереди_печати> -m <модель_из_lpinfo> -v <deviceuri> -E
```

или

```
lpadmin -p <имя_очереди_печати>-P </путь/до/файла/ppd/> -v <uri_устройства> -E
```

Здесь:

– `-p <имя_очереди_печати>` — имя очереди печати, которую нужно настроить;

– `-m <модель_из_lpinfo>` — информация о модели принтера, возвращенная командой `lpinfo -m`;

– `-P </путь/до/файла/ppd/>` — имеющийся файл PPD;

– `-v <uri_устройства>` — действительный адрес URI устройства, созданный на основе информации, возращенной командой `lpinfo -v`;

– `-E` — команда включения принтера.

Пример: требуется установить ранее упомянутый принтер Ricoh Aficio MP 2000 (предположим, что его адрес IP равен 10.1.2.3, а очередь печати называется «rpm2000»):

```
lpadmin -m -P rmp2000 -m foomatic-db-ppds/Ricoh/PS/RicohAficio_MP_2000_PS.ppd.gz -v socket://10.1.2.3/ -E
```

Примеры

Сеть — JetDirect/AppSocket

```
# lpadmin -p 5th-floor-mfp -v socket://10.1.2.3:9100 -m foomaticdb-ppds/Ricoh/PS/Ricoh-Aficio_CL2000_PS.ppd.gz -E
```

Сеть — LPD

```
# lpinfo -m | grep Canon | grep imageRunner | grep 'C6800'
foomatic:Canon-imageRunner_C6800-hpijs-pcl5c.ppd Canon imageRunner
C6800
Foomatic/hpijs-pcl5c
foomatic:Canon-imageRunner_C6800-Postscript.ppd Canon
imageRunner
C6800
Foomatic/Postscript
# lpadmin -p canon-west -v lpd://10.1.2.3/PASSTHRU -m
foomatic:Canon-
imageRunner_C6800-hpijs-pcl5c.ppd -E
```

Подробности о том, как выполнять печать с помощью принтеров LPD, см. далее в настоящем документе.

USB

```
# lpinfo -m | grep Epson | grep Photo
drv:///sample.drv/stphoto2.ppd Epson New Stylus Photo Series
foomatic:Epson-Stylus_Photo_750-stcolor.ppd Epson Stylus Photo
750
Foomatic/stcolor
drv:///sample.drv/stphoto.ppd Epson Stylus Photo Series
# lpadmin -p local-epson-photo -E -v usb:/dev/usb/lp0 -m
drv:///sample.drv/stphoto2.ppd
```

Последовательный порт

```
# lpinfo -v | grep serial serial serial:/dev/ttyS0?baud=115200
# lpinfo -m | grep Epson | grep Dot
foomatic:Epson-Dot_Matrix-eps9high.ppd Epson Dot Matrix
Foomatic/eps9high
foomatic:Epson-Dot_Matrix-eps9mid.ppd Epson Dot Matrix
Foomatic/eps9mid
foomatic:Epson-Dot_Matrix-epson.ppd Epson Dot Matrix
Foomatic/epson
foomatic:Epson-Dot_Matrix-epsonc.ppd Epson Dot Matrix
Foomatic/epsonc
# lpadmin -p local-dot-matrix -E -v
serial:/dev/ttyS0?baud=115200
```

```
-m
foomatic:Epson-Dot_Matrix-epson.ppd
```

Параллельный порт

```
# lpinfo -m | grep Epson | grep Photo
drv:///sample.drv/stphoto2.ppd Epson New Stylus Photo Series
foomatic:Epson-Stylus_Photo_750-stcolor.ppd Epson Stylus Photo
750
Foomatic/stcolor drv:///sample.drv/stphoto.ppd Epson Stylus
Photo Series
# lpadmin -p local-epson-photo -E -v usb:/dev/usb/lp0 -m
foomatic:Epson-Stylus_Photo_750-stcolor.ppd
```

Samba/принтеры Windows

```
# lpinfo -m | grep HP | grep LaserJet | grep 8150 foomatic:HP-
LaserJet_8150-lj4dith.ppd HP LaserJet 8150
Foomatic/lj4dith foomatic:HP-LaserJet_8150-lj5gray.ppd HP
LaserJet 8150
Foomatic/lj5gray foomatic:HP-LaserJet_8150-ljet4.ppd HP LaserJet
8150
Foomatic/ljet4 foomatic:HP-LaserJet_8150-Postscript.ppd HP
LaserJet 8150
Foomatic/Postscript foomatic:HP-LaserJet_8150-pxlmono.ppd HP
LaserJet 8150
Foomatic/pxlmono
# lpadmin -p winprinter -E -v
smb://username:password@10.1.2.3/HP
-m
foomatic:HP-LaserJet_8150-Postscript.ppd
```

Установка файлов PPD, отсутствующих в репозиториях ОС РОСА «НИКЕЛЬ»

Данный подраздел содержит ответы на следующие вопросы:

– Как установить сторонние файлы PPD (PostScript Printer Definition, «описание принтера PostScript»), если при добавлении нового принтера через веб-интерфейс или графическую утилиту его модель отсутствует?

– Как установить новый принтер, если для него отсутствует файл PPD в списке доступных драйверов?

Что такое PPD

Описание принтера PostScript (PPD) — это файлы конфигурации, которые сообщают системе печати CUPS сведения о том, как преобразовывать документы в формат, воспринимаемый принтером. Файлы PPD также передают системе печати CUPS доступные для печати параметры (приемный лоток, размер бумаги, параметры сшивания и т. д.). Файлы PPD в Linux иногда называются драйверами принтера.

Источники файлов PPD

Файлы печати PPD, не включенные в комплект поставки ОС РОСА «НИКЕЛЬ», можно скачать из разных источников, в том числе:

База данных принтеров проекта Open Printing

1) Зайдите в базу данных проекта Open Printing по адресу http://www.openprinting.org/printers, выберите производителя имеющегося принтера и нажмите на кнопку [Показать все].

2) Выберите принтер из списка поддерживаемых моделей. Если точная модель имеющегося принтера не указана, можно выбрать наиболее близкую по характеристикам модель. Если, например, в наличии имеется модель C5502, выбор C5000 может дать рабочую информацию.

3) Выбор модели открывает страницу, на которой указан уровень поддержки в Linux, доступной для этого принтера. При наличии ссылки на файл PPD скачайте его и сохраните во временном каталоге.

Официальный сайт производителя

Многие производители размещают файлы PPD в разделе загрузок на своем официальном сайте. Файлы PPD часто включаются в архивы вместе с другим ПО для печати. Если для файла PPD не требуется другого программного обеспечения (что обычно бывает, если искомый принтер поддерживает печать PostScript), можно скачать весь архив и извлечь из него только файл PPD.

17.2. Установка файла PPD

1) Скопируйте файл PPD, полученный одним из описанных выше способов, в каталог /usr/share/cups/model.

2) Перезапустите службу CUPS:

```
systemctl restart cups.service
```

После перезапуска службы модель нового принтера должна появиться в списке, доступном в веб-интерфейсе CUPS по адресу http://127.0.0.1:631.

Добавить принтер с новым файлом PPD также можно с помощью следующей команды:

```
# lpadmin -p <имя_очереди> -E -v <протокол>://<IP-адрес_принтера>
-P /usr/share/cups/model/<имя_файла_ppd>.ppd
```

Здесь:

- <имя_очереди> — имя очереди печати, с которой будет связан принтер;
- <протокол> — тип протокола, используемого для связи с принтером (обычно это сокет для принтеров, подключенных по сети, lpd — для принтеров, подключенных через LPD или smb — для принтеров, подключенных к системам Windows);
- <IP-адрес_принтера> — адрес IP или имя хоста принтера, подключенного по сети;
- <имя_файла_ppd> — имя файла PPD, который был сохранен в каталог /usr/share/cups/model.

Пример: как настроить главный сервер печати с использованием CUPS в ОС РОСА «НИКЕЛЬ»?

Необходимо настроить главный сервер печати CUPS для создания общих принтеров для клиентов в нашей сети. Пользователь непосредственного сервера печати может выполнять печать на любом настроенном принтере, но при попытках печати с клиентов выводится ошибка «lp: Connection refused».

Решение

Создание главного сервера печати CUPS

1) Остановите выполнение службы CUPS и создайте резервную копию текущих параметров CUPS:

```
# service cups stop
# cp -a /etc/cups /etc/cups.saved
```

2) Внесите изменения в файл /etc/cups/cupsd.conf, разрешающие другим серверам подключаться к принтерам на главном сервере. Сначала поменяйте Listen localhost:631 на Listen *:631 или на Listen 0.0.0.0:631. Это действие настроит CUPS на прослушивание всех сетевых интерфейсов. Если нужно ограничить прослушивание CUPS каким-то конкретным интерфейсом, введите адрес этого интерфейса вместо символа * или адреса 0.0.0.0. Например: `Listen 192.168.102.32:631`

3) В конец записи <Location /> добавьте Allow @LOCAL. Запись должна выглядеть следующим образом:

```
<Location />
# Allow shared printing
Order allow,deny
```

```
Allow @LOCAL
</Location>
```

Этот параметр даст возможность клиентам в сети «local» (подсеть, в которой расположен главный сервер печати) получить доступ к службе CUPS на главном сервере печати. Если доступ к главному серверу печати необходимо разрешить всем клиентам, вместо Allow @Local используйте Allow all.

4) Если CUPS должна посылать широковещательные пакеты с информацией об общих спринтерах, убедитесь, что в файле /etc/cups/cupsd.conf присутствуют следующие записи (эти записи имеются в версии файла по умолчанию):

```
Browsing On
BrowseLocalProtocols cups dnssd
```

Если сервер CUPS не должен рассылать широковещательные пакеты, а вместо этого клиенты CUPS должны опрашивать серверы CUPS на наличие общих принтеров, внесите в файл /etc/cups/cupsd.conf следующую запись: `Browsing Off`

5) Убедитесь, что каждая из очередей печати является общей. Действие по умолчанию — очередь делается общей при ее создании, поэтому проблем возникнуть не должно. Статус общей доступности очереди печати можно проверить, выполнив команду lpoptions и просмотрев вывод на наличие параметра printer-is-shared:

```
# lpoptions -p textonly
copies=1 device-uri=socket://10.3.4.5/ finishings=3 job-holduntil=no-hold job-priority=50 job-sheets=none,none
marker-change-time=0 number-up=1 printer-commands=none printerinfo=textonly printer-is-accepting-jobs=true
printer-is-shared=true printer-location printer-make-andmodel='Generic text-only printer' printer-state=3 printer-state-change-time=1478741330 printer-state-reasons=none printer-type=4100
printer-uri-supported=ipp://localhost:631/printers/textonly
```

В этом выводе обратите внимание на запись printer-is-shared=true в третьей строчке.

6) Убедитесь, что служба avahi-daemon установлена и выполняется. Это можно сделать с помощью следующих команд:

```
# dnf -y install avahi
# systemctl enable avahi-daemon
# systemctl start avahi-daemon
```

7) Запустите службу CUPS:

```
# systemctl restart cups.service
```

8) Проверьте вывод команды lpstat -t и убедитесь, что на главном сервере печати эти принтеры определены и активированы:

```
# lpstat -t scheduler is running no system default destination
device for pcl: socket://10.1.2.3/ device for postscript:
socket://10.2.3.4/ device for textonly: socket://10.3.4.5/
pcl accepting requests since Wed 09 Nov 2016 05:28:19 PM PST
postscript accepting requests since Wed 09 Nov 2016 05:28:37 PM
PST
textonly accepting requests since Wed 09 Nov 2016 05:28:50 PM
PST printer pcl is idle. enabled since Wed 09 Nov 2016 05:28:19 PM
PST
printer postscript is idle. enabled since Wed 09 Nov 2016
05:28:37 PM
PST
printer textonly is idle. enabled since Wed 09 Nov 2016 05:28:50
PM PST
```

9) Если на главном сервере печати работает межсетевой экран, администратор должен разрешить внешний доступ к порту 631/ipp, а также к порту 5353/mdns в новой версии ОС РОСА «НИКЕЛЬ» для протоколов UDP и TCP.

Настройка клиентов CUPS

Следующие шаги включают внесение изменений в конфигурационный файл CUPS `/etc/cups/cups-browsed.conf`.

Вносимые изменения зависят от условий конкретного окружения. Если клиенты должны активно опрашивать сервер CUPS на наличие информации от общих принтеров, или же если клиенты и главный сервер печати находятся в разных подсетях, в соответствующий конфигурационный файл CUPS необходимо добавить следующую запись, заменив текущий адрес IP (или имя хоста) главного сервера печати на адрес 10.12.13.14:

```
BrowsePoll 10.12.13.14
```

При наличии в окружении нескольких главных серверов печати (как, например, в случае настройки CUPS с высокой доступностью) для каждого из них используется отдельная запись BrowsePoll. Поскольку параметр BrowsePoll активно опрашивает главный сервер на наличие информации (с использованием запроса IPP CUPS-Get-Printers), этот способ действует для всех подсетей. Тем не менее, поскольку для опроса

сервера требуется подключение TCP, в итоге потребляемый объем сетевых ресурсов будет чуть выше, чем при использовании способа, описываемого далее.

Если клиенты должны пассивно ожидать широковещательной информации от главного сервера печати, в конфигурационный файл CUPS нужно добавить следующую запись:

```
BrowseRemoteProtocols dnssd cups
```

Эти параметры дадут возможность клиентам CUPS собирать информацию об общих принтерах с главного сервера печати в локальной подсети. Для обнаружения общих принтеров здесь используется mDNS/DNS-SD, поэтому сетевые ресурсы будут использоваться чуть менее интенсивно, чем в способе с активным опросом, описанным выше. Тем не менее, этот способ не сработает, если главный сервер печати (или серверы) находится в разных подсетях с клиентами (если только между подсетями не настроен мост mDNS/DNS-SD).

1) Запустите CUPS:

```
# systemctl start cups.service
```

2) Установите, активируйте и запустите службу avahi-daemon:

```
# dnf -y install avahi
# systemctl enable avahi-daemon
# systemctl start avahi-daemon
```

3) Активируйте и запустите службу cups-browsed:

```
# systemctl enable cups-browsed
# systemctl start cups-browsed
```

4) Убедитесь, что удаленные принтеры теперь доступны на локальном клиенте:

```
$ lpstat -t scheduler is running no system default destination
device for pcl: ipps://master-server.local:631/printers/pcl
device for postscript: ipps://master-printserver.local:631/printers
/postscript
device for textonly: ipps://master-printserver.local:631/printers
/textonly
pcl accepting requests since Wed 09 Nov 2016 05:18:09 PM PST
postscript accepting requests since Wed 09 Nov 2016 05:18:09 PM
PST
textonly accepting requests since Wed 09 Nov 2016 05:18:09 PM
```

```
PST printer pcl is idle. enabled since Wed 09 Nov 2016 05:18:09 PM PST
      printer postscript is idle. enabled since Wed 09 Nov 2016
      05:18:09 PM
      PST
      printer textonly is idle. enabled since Wed 09 Nov 2016 05:18:09
PM PST
```

5) Попробуйте выполнить тестовую печать:

```
$ lp -d textonly /etc/fstab request id is textonly-1 (1 file(s))
```

При правильно настроенных параметрах тестовая печать должна выполниться успешно.

17.3. Маркирование документов

17.3.1. Порядок печати документов с маркировкой

1) Для печати документов с маркировкой в текстовом или ином редакторе документов нажать клавиши <Ctrl> и <P>. Откроется системный диалог печати (Рисунок 173).

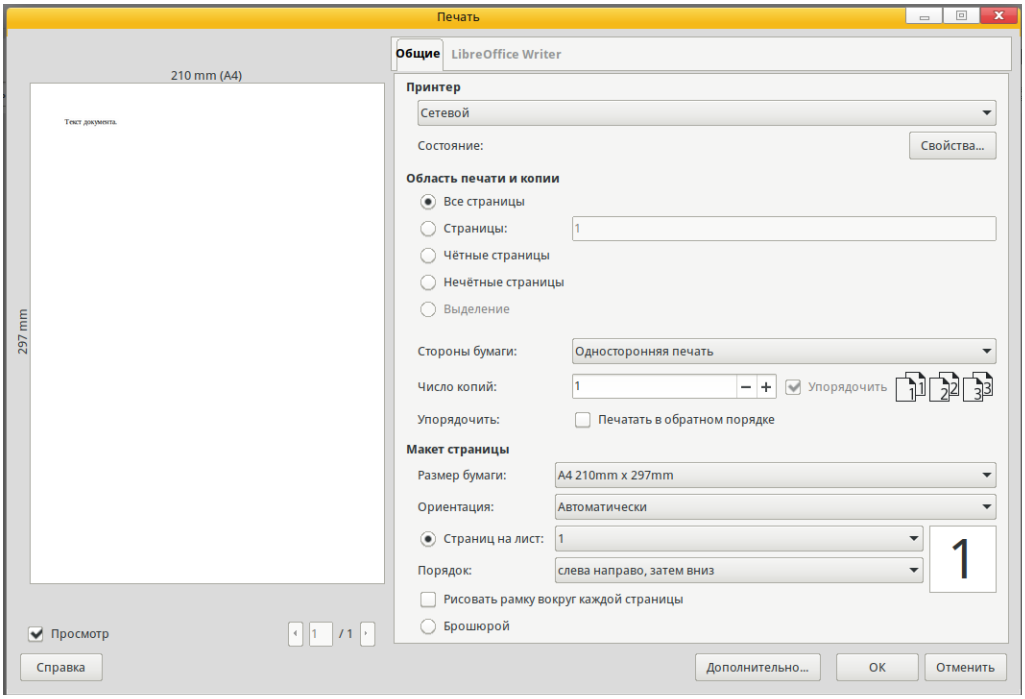


Рисунок 173

В поле принтер выбрать принтер, поддерживающий функцию маркировки документов. При необходимости дополнительно выберете другие параметры. После настройки всех параметров нажмите [OK].

2) Далее откроется новое окно маркировки печати (Рисунок 174).

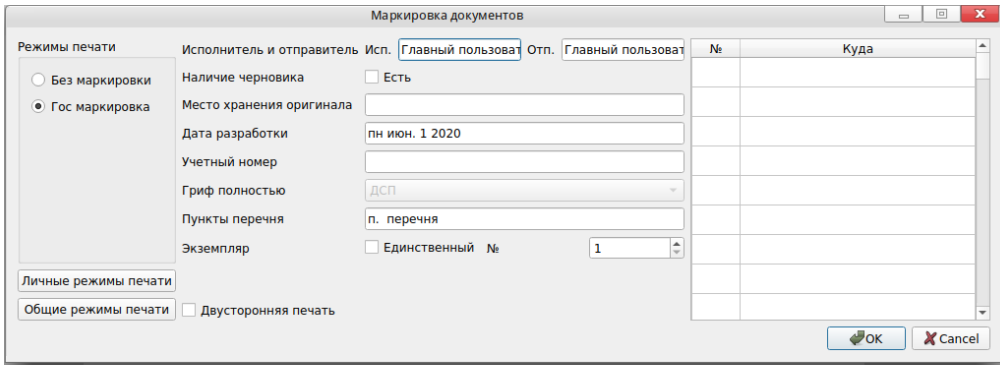


Рисунок 174

В данном окне слева приведен список доступный режимов печати.

Режим [Без маркировки] по умолчанию будет не доступен при печати на уровне *Секретно* и *СовершенноСекретно* или при других режимах, установленных по усмотрению администратора системы.

Далее необходимо заполнить поля маркировки, состав которых зависит от выбранного режима печати. Последние несколько введенных вариантов каждого поля сохраняются и доступны для выбора при частичном вводе нескольких символов строки.

При выборе предустановленного режима печати [Гос маркировка] следует заполнить следующие поля в соответствии с правилами маркировки:

– **Исполнитель и отправитель** – По умолчанию это имя пользователя, зарегистрированного в системе, при отличии от реального имени следует исправить их, при следующей печати данные поля будут сохранены;

– **Наличие черновика** – при наличии черновика следует установить параметр [Есть], при печати на обороте последней страницы будет напечатано [Б/ч] перед местом хранения оригинала при отсутствии галочки;

– **Место хранения оригинал**а – следует указать место хранения оригинала для печати на обороте последней страницы;

– **Дата разработки** – следует указать дату разработки документа, которая будет на обороте последней страницы;

– **Учетный номер** – необходимо указать номер документа без символа «№» (он будет добавлен автоматически);

– **Гриф полностью** – текущий уровень доступа и уровень доступа документа, значение данного поля поменять в окне печати невозможно, при несоответствии данного уровня реальному уровню данного документа следует прервать печать нажав кнопку [Отмена] и перед печатью войти в систему под требуемым уровнем доступа;

– **Пункты перечня** – при наличии грифа на документе следует указать в соответствии с какими пунктами перечня документ получил данный гриф;

– **Экземпляр** – описывает количество существующих экземпляров и номер данного экземпляра, если экземпляр единственный, следует установить соответствую галочку, далее написать номер данного экземпляра (автоматически заполняется номером 1);

– **Список экземпляров** – поле справа окна содержащее номер экземпляра и то, куда направляется данных экземпляр документа;

В случае поддержки принтера двухсторонней печати установить параметр [Двусторонняя печать]. В противном случае система предложит перевернуть последнюю страницу вручную.

3) По завершению заполнения всех параметров нажмите кнопку [Ок] для печати.

Закрытие окна или нажатие кнопки [Отмена] приведет к отмене печати документа.

17.3.2. Настройка личных режимов маркировки

При работе на некоторых уровнях доступа пользователям разрешается не использовать маркировку или создавать собственные шаблоны (режимы) маркировки. Для перехода к редактированию режима маркировки необходимо войти в меню печати документов. Для этого в текстовом или ином редакторе документов нажмите клавиши <Ctrl> и <P> и перейдите в раздел [Личные режимы печати]. При этом будет скопирован текущий выбранный режим как новый или открыт для редактирования личный.

17.3.3. Настройка общих режимов маркировки

Редактирование общих режимов маркировки выполняется администратором системы.

Для этого необходимо перейти в редактор режимов маркировки документов, который можно запустить из системного меню [Приложения] или воспользоваться функцией поиска в меню.

В открывшемся окне необходимо ввести пароль администратора (Рисунок 175) и нажать кнопку [ОК].

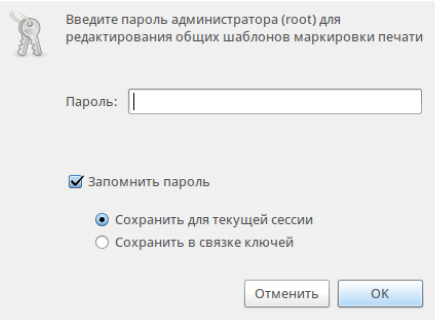


Рисунок 175

Далее откроется окно редактирования режимов печати.

17.3.4. Редактирование режимов печати

Редактирования режимов печати происходит в окне «Настройка маркировки» (Рисунок 176). В левой верхней части окна выбирается режим (шаблон) маркировки. При изменении имени и последующем сохранении шаблон будет сохранен с новым именем.

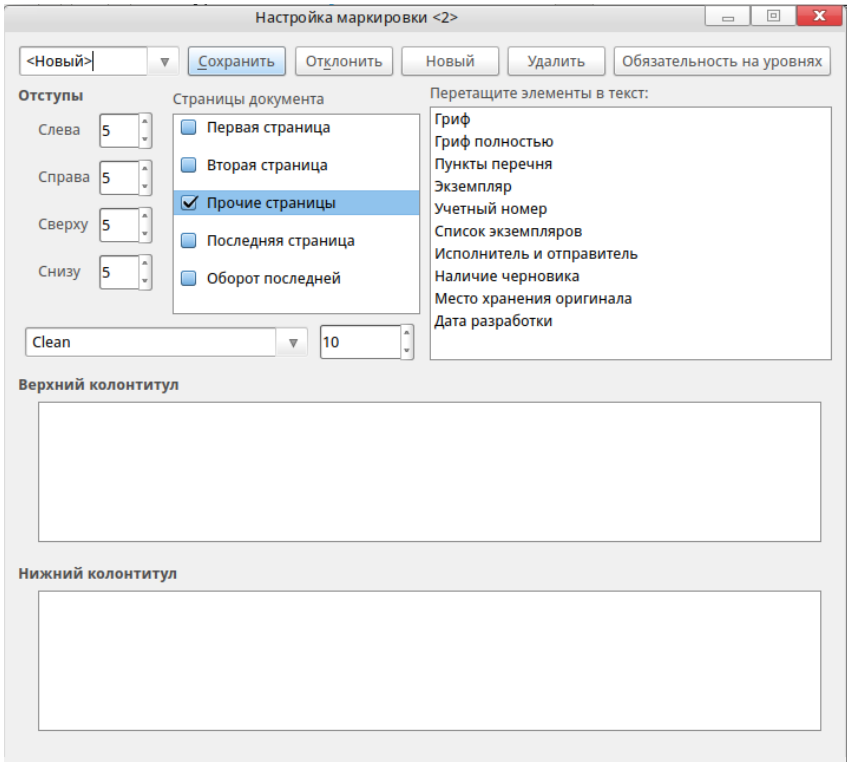


Рисунок 176

Обратите внимание на кнопку [Обязательность на уровнях] (в правой верхней части окна), при нажатии на которую вы можете выбрать уровни доступа, зарегистрированные в системе, на которых необходима данная маркировка (Рисунок 177).

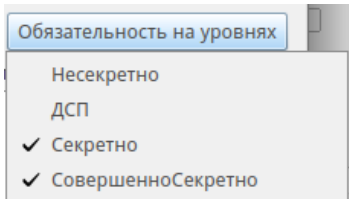


Рисунок 177

При входе в систему на отмеченных уровнях разрешается печать без маркировки и работа с личными режимами маркировки. Данный пункт работает независимо от выбранного режима маркировки. Имена и количество уровней доступа получаются из настроек SELinux:

– кнопка [Сохранить] сохраняет текущий режим маркировки с текущим именем;

– кнопка [Отклонить] отменяет правки в текущем режиме маркировки. Кнопка [Новый] создает новый режим маркировки и добавляет его в список (при этом не обходимо дать имя нового шаблона);

– кнопка [Удаления] удаляет текущий режим маркировки;

– в области [Отступы] задаются размеры отступов для всех страниц для наносимой маркировки. Обратите внимание, отступы должны быть такими, что с одной стороны не менее допустимых для вашего принтера (обычно не менее 5, иногда не менее 15), с другой стороны не должны быть слишком большими, чтобы весь текст маркировки уместился вне текстовой информации документа (обычно соответствует отступам страницы или отступам с колонтитулами).

Ниже расположена область задания шрифта, в которой предоставляется выбор среди всех зарегистрированных в системе шрифтов. Обратите внимание, что в списке будут представлены только шрифты с поддержкой кириллицы и моноширины. Также задается и размер шрифта;

– в области [Страницы документа] перечислены и отмечены те страницы, на которых будет наноситься маркировка. При этом текущая выделенная строка редактируется в данный момент ниже. Для очистки одной из страниц необходимо снять отметку в соответствующей строке.

При добавлении маркировки на текущую страницу отметка будет установлена автоматически.

При переключении страниц не требуется сохранять параметры каждой, однако после изменения всех страниц, необходимо сохранить шаблон маркировки:

– в правой части окна в области [Перетащите элементы в текст] находится палитра элементов маркировки. Для их использования следует «перетащить» их в область верхнего или нижнего колонтитула. Содержимое внутри скобок < > не следует исправлять, это специальные теги заменяемые при печати. Кроме специальных тегов в текстах колонтитулов допускается использование свободно введенного текста, который будет добавлен как есть;

– колонтитулы всех страниц кроме оборота последней страницы выравниваются по правому краю, оборот последней – по левому краю.

Номера страниц располагаются вверху страницы справа, начиная со второй страницы.

18. НАСТРОЙКА ОБОРУДОВАНИЯ

Настройка аппаратных составляющих ПК происходит в ОС РОСА «НИКЕЛЬ» централизованно с помощью «Утилиты настройки оборудования» (*Harddrake*), доступной в блоке «Оборудование» программы «Параметры системы».

Для ее запуска требуются права администратора системы.

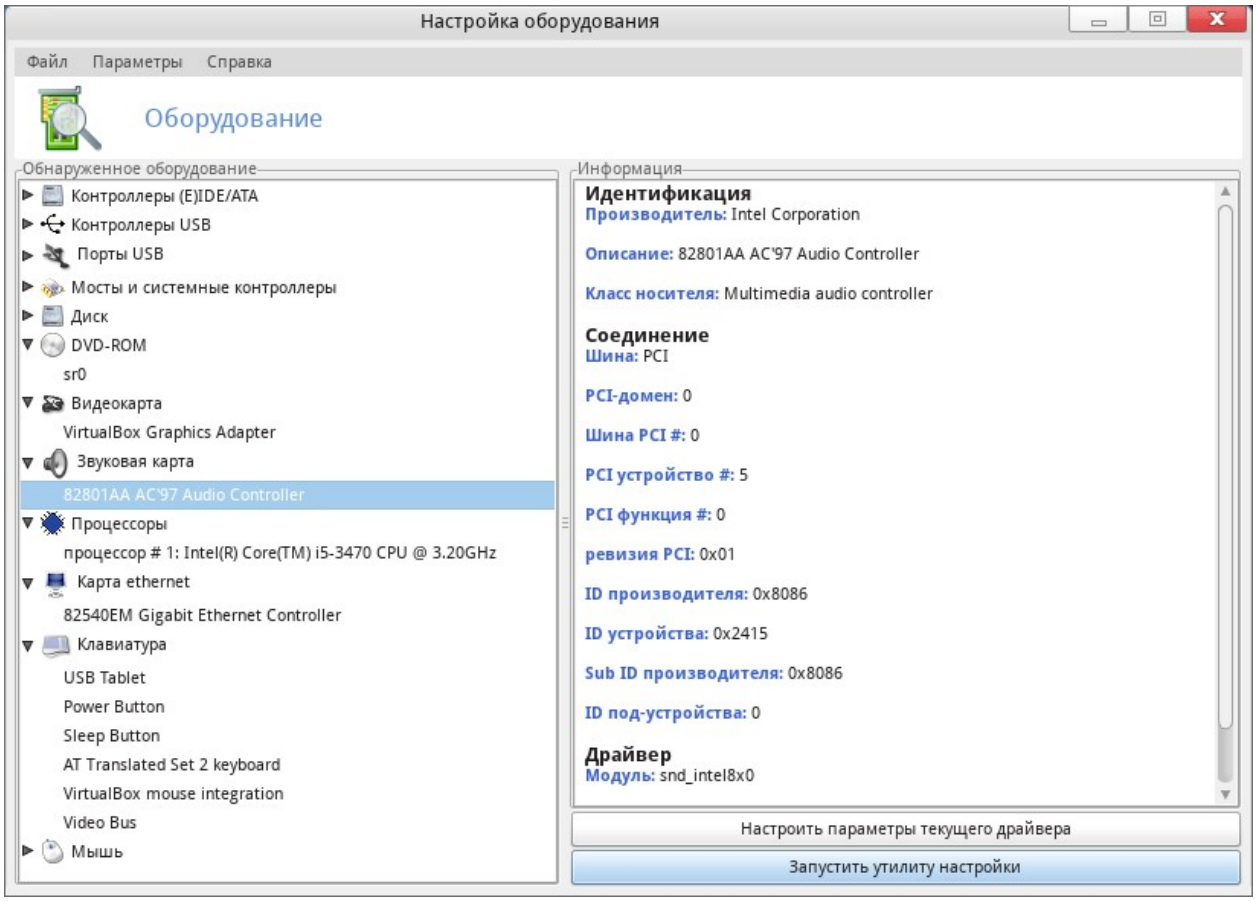


Рисунок 178

Выделив устройство, вы увидите подробную информацию о нем в правой части окна. Описание полей доступно в контекстной справке («Справка → Поля с описанием»). В зависимости от того, какое устройство выбрано, могут появиться и другие кнопки:

– **Настроить параметры текущего драйвера**. Кнопка выводит окно со списком параметров драйвера устройства;

– **Запуск инструмента настройки**. Запускает инструмент настройки, связанный с этим устройством. Например, для звуковой карты используется специальный конфигуратор, позволяющий выбрать драйвер и решить некоторые часто возникающие проблемы;

– **Неизвестное оборудование.** Возможно, вы увидите категорию, называющуюся «Неизвестный/Другие» и содержащую как неизвестное оборудование, так

и настроенные устройства, которые, тем не менее, не вписываются в существующие категории (например, температурный датчик, генератор случайных чисел и т. п.);

– **Автоматическое определение специальных устройств.** Инструменты для автоматического определения устройств, которые не могут быть найдены стандартным образом, находятся в меню Параметры. Чтобы изменения вступили в силу, необходимо перезапустить «Утилиту настройки оборудования».

18.1. Настройка звуковой подсистемы

Если возникли проблемы со звуком или если нужно изменить конфигурацию звуковой подсистемы, созданную автоматически при установке ОС, запустите утилиту настройки оборудования, как это описывалось выше, выделите в списке оборудования звуковую карту и нажмите на кнопку [Запустить утилиту настройки] справа внизу. Откроется окно «Настройка звука» (Рисунок 179).

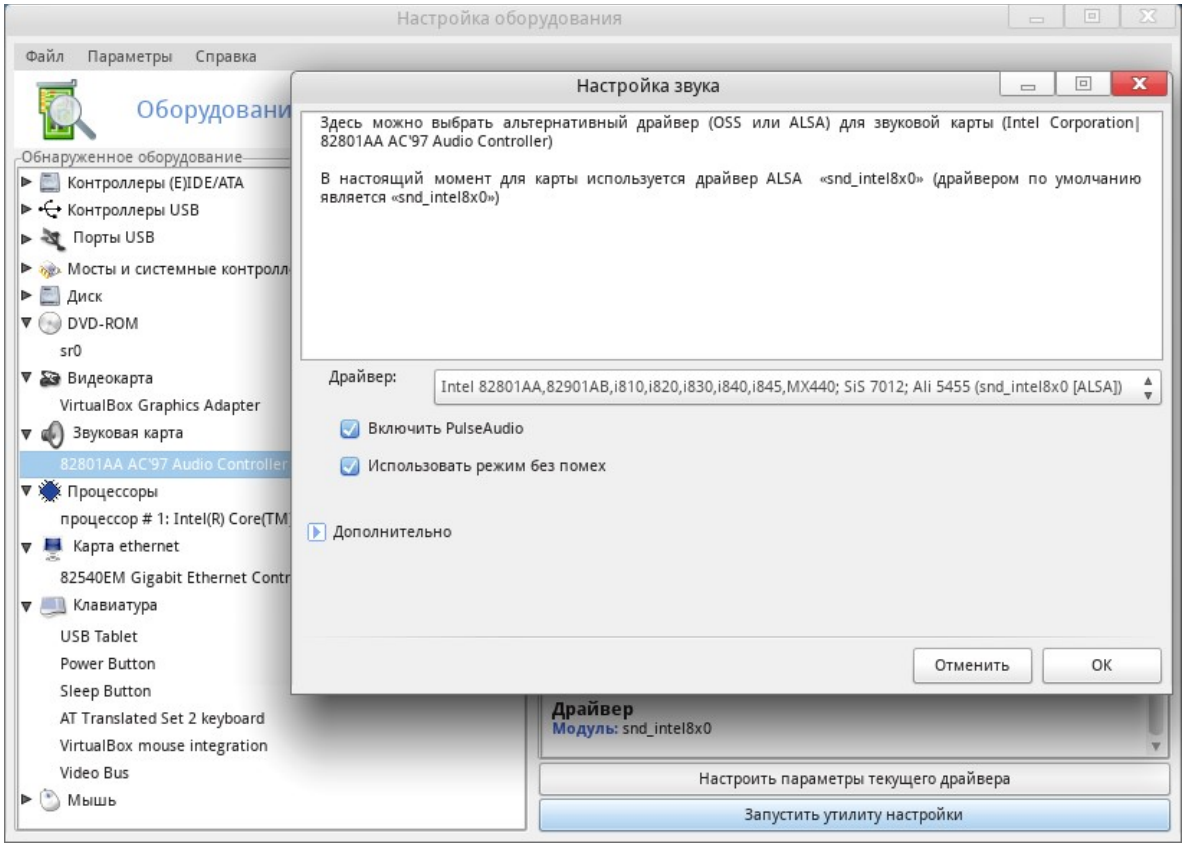


Рисунок 179

18.1.1. Смена драйвера

Можете переключиться с одного драйвера на другой, выбрав его из выпадающего списка «**Драйвер**». Там будут отображены все совместимые с вашей звуковой картой драйверы; вы можете выбрать между OSS или ALSA API. Рекомендуем использовать более развитые драйверы ALSA; только для очень старых карт, возможно, придется

использовать OSS. Если точно известен нужный драйвер, можно выбрать его из полного списка, нажав на стрелку возле слова «**Дополнительно**» и затем — «**Выбрать другой драйвер**».

18.1.2. Другие параметры

Включить PulseAudio

Активация звукового сервера. PulseAudio принимает звуковой вход из многих источников и смешивает их в один выходной поток. Он совместим с большинством источников звука. PulseAudio является звуковым сервером по умолчанию.

Включить 5.1 звук через PulseAudio65

Отметьте эту опцию, если у вас есть многоканальная аудиосистема и вы хотите воспользоваться всеми ее функциями.

Включить переключение пользователей для звуковых приложений

Когда пользователь входит в систему, он монополизирует звуковое оборудование: если другой пользователь войдет в систему, звук в программах у него окажется отключен. Если на ПК несколько пользователей, выберите этот параметр для обеспечения обмена звуком между зарегистрированными пользователями.

Рекомендуем оставить этот параметр активным. Выключить его имеет смысл лишь в случае, когда первый вошедший пользователь должен получать эксклюзивный доступ к звуковому оборудованию.

18.2. Управление графической конфигурацией

18.2.1. Настройка монитора

Настроить разрешение, сменить тип блокировки экрана, а также выполнить калибровку монитора можно с помощью утилиты «Экран», расположенной в блоке «Оборудование» программы «Параметры системы».

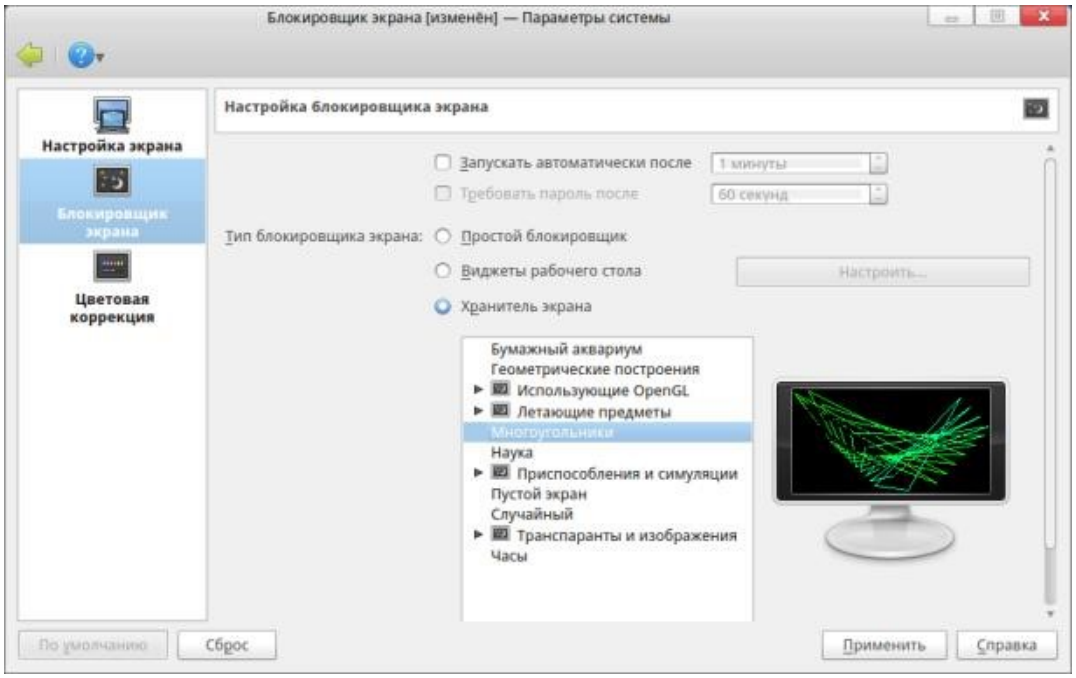


Рисунок 180

18.2.2. Настройка видеокарты

При возникновении проблем с графикой или при необходимости сменить драйвер графического устройства может пригодиться утилита «Настройка видеокарты» (*XFdrake*), расположенная в блоке «Оборудование» программы «Параметры системы». Также получить к ней доступ можно из программы «Настройка оборудования». Для этого выделите в блоке слева нужную графическую карту и нажмите на кнопку [Запустить утилиту настройки] в правой нижней части окна программы:

- **Видеокарта** — модель видеокарты, на которую на данный момент настроена система. Для изменения нажмите эту кнопку. В зависимости от вашей карты могут быть доступны различные сервера: с 3D-ускорением или без него. Может возникнуть необходимость попробовать несколько вариантов, пока вы не добьетесь наилучшего результата. В случае, если вашей карты в списке нет, но известен драйвер, который ее поддерживает, выберите этот драйвер в нижней части меню Xorg;
- **Монитор** — выбор типа монитора с помощью утилиты, рассмотренной выше;
- **Разрешение —** ширина и высота изображения;
- **Проверить** — обязательно нажмите на эту кнопку, и вы сможете убедиться, что выбранная конфигурация работоспособна. Если изображение на экране пропало, просто подождите немного, и система вернется в рабочий режим. Если изображение есть, но искажено или видны помехи, можно не ждать: нажмите [Нет], и вы будете возвращены в главное меню *XFdrake*. Если протестировать видеорежим невозможно, вы получите предупреждение.

Если тестирование не было проведено, а выставленные параметры оказались неподходящими, дисплей работать не будет. Придется войти в систему в терминальном режиме и воспользоваться текстовой версией *XFdrake*.

– Параметры — по умолчанию RED X3 запускается в графическом режиме. Отметьте вариант «Нет», если вы предпочитаете использовать текстовый вход в систему;

– Выход — если в процессе работы с XFdrake конфигурация графической подсистемы была изменена, XFdrake спросит, хотите ли вы сохранить изменения. Это последний шанс отказаться от изменений. Изменения вступят в силу после того, как вы подтвердите их и перезапустите графическую среду.

18.3. Раскладка и тип клавиатуры

Утилита «Клавиатура» служит для определения параметров раскладки клавиатуры и аппаратного типа клавиатуры. Запустить утилиту можно из утилиты настройки оборудования, которая расположена в блоке «Оборудование» программы «Параметры системы». Выделив слева на панели найденного оборудования клавиатуру, нажмите на кнопку [Запустить утилиту настройки] в правой нижней части окна программы. Откроется окно «Клавиатура».

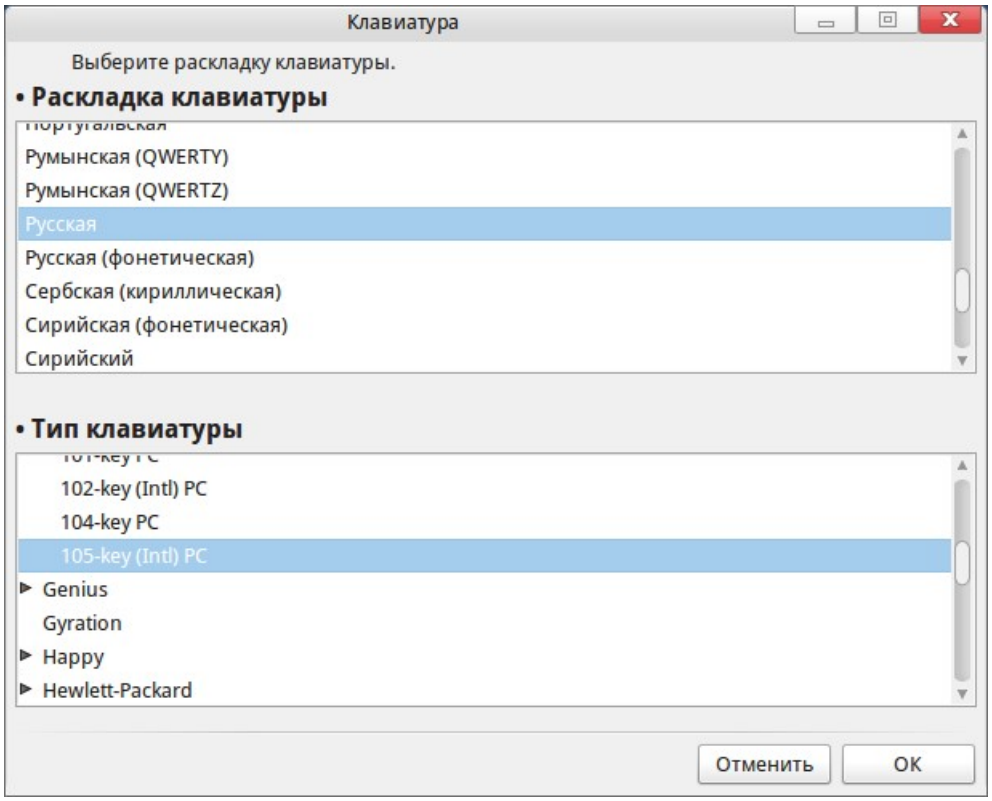


Рисунок 181

Выберите раскладку клавиатуры, ее тип или модель. Изменения вступают в силу после нажатия [ОК]. Если выбрана раскладка для языка, использующего кириллицу или

иную систему письменности, основанную не на латинском алфавите, в следующем диалоговом окне будет предложено выбрать комбинацию клавиш для переключения между латинской и нелатинской раскладками.

Гораздо большее число параметров клавиатуры можно найти в модуле KDE «Клавиатура», вызвать который можно двумя способами:

1. Щелкнуть правой кнопкой по виджету смены языка на панели RocketBar и в контекстном меню выбрать пункт «Настроить...»;

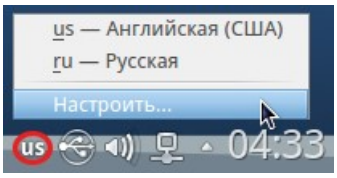


Рисунок 182

2. Запустить утилиту «Устройства ввода» из блока «Оборудование» программы «Параметры системы» (Рисунок 183).

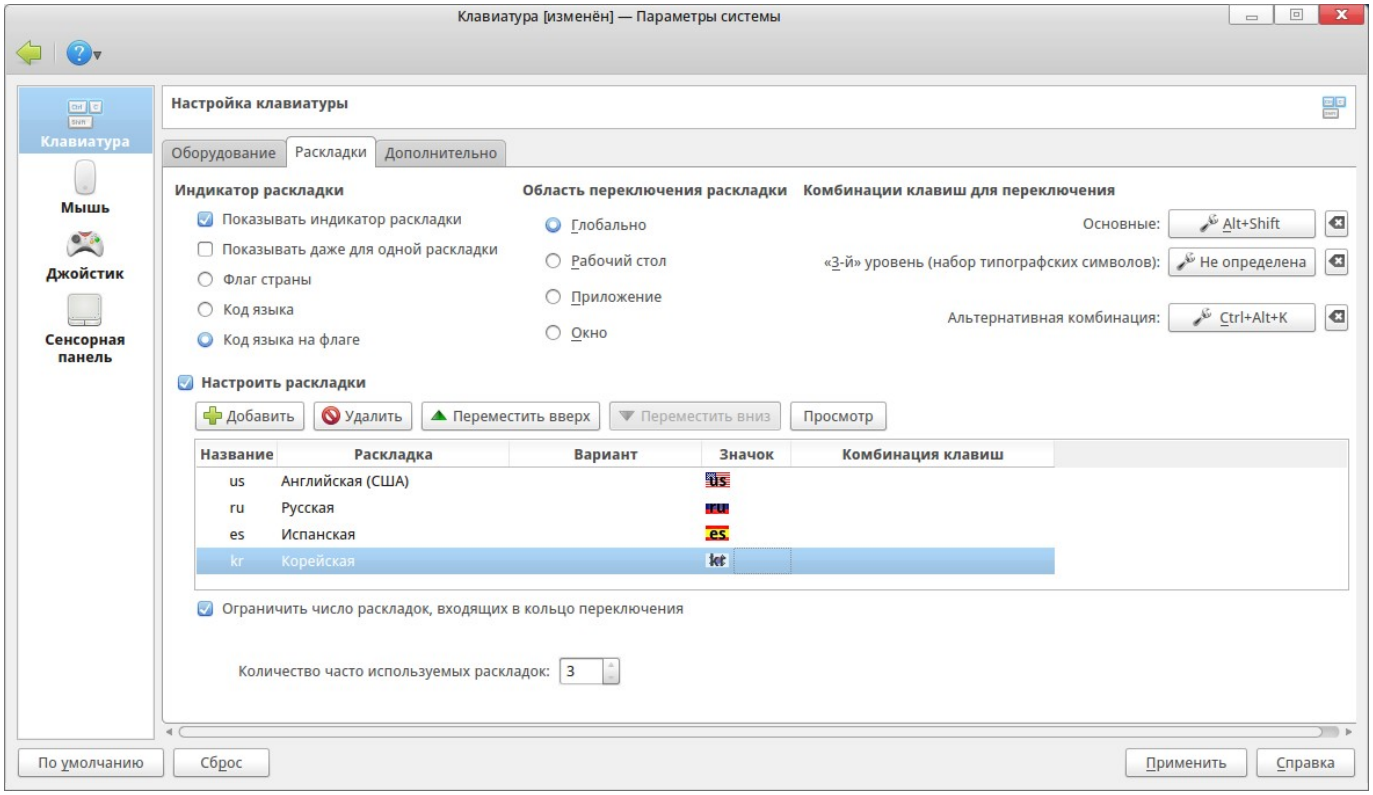


Рисунок 183

На трех вкладках модуля «Клавиатура» можно настроить параметры оборудования, параметры раскладки и дополнительные параметры.

В ОС РОСА «НИКЕЛЬ» также поддерживается экранная клавиатура, для того чтобы открыть ее, необходимо в меню приложений найти ярлык **Kvkbd.** По щелчку мыши на рабочем столе появиться экранная клавиатура.

Рисунок 184

18.4. Настройка принтеров

При первом включении принтера система постарается автоматически определить его модель и настроить его, о чем сообщается во всплывающем окне (Рисунок 185):

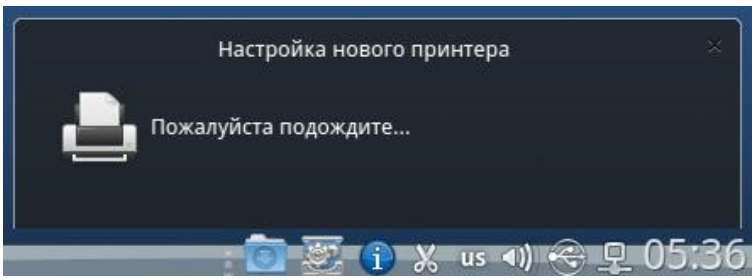


Рисунок 185

В комплекте поставки ОС РОСА «НИКЕЛЬ» есть драйвера для большинства современных принтеров, поэтому, скорее всего, следом вы увидите сообщение об успешной установке (Рисунок 186).

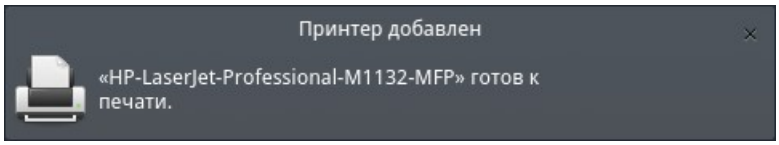


Рисунок 186

Чтобы изменить параметры принтера или добавить новый, воспользуйтесь утилитой «Настройка принтера», расположенной в блоке «Оборудование» программы «Параметры системы».

18.4.1. Изменение параметров принтера

Двойной щелчок по значку принтера вызывает окно его настройки. Откройте нужный раздел, измените параметры и нажмите на кнопку [**Применить**].

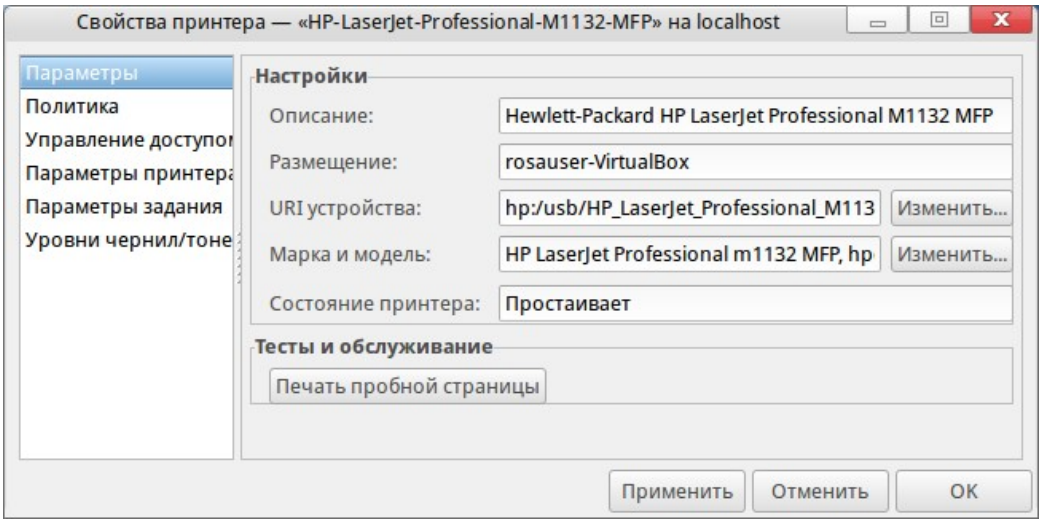


Рисунок 187

Краткое описание вкладок окна настройки:

– Параметры — здесь можно изменить драйвер и описание принтера, напечатать тестовую страницу и выполнить операции обслуживания, если они предусмотрены драйвером;

– Политика — здесь можно настроить статус подключения, прием заданий, общий доступ и действия в случае ошибки печати;

– Управление доступом — по умолчанию все пользователи имеют возможность печати на системном принтере. Если требуется ввести ограничения, можно либо разрешить, либо запретить его использование всем, кроме тех пользователей, которых вы укажете персонально. Для добавления пользователя в список нажмите на кнопку [Добавить] и выберите имя пользователя, зарегистрированного в системе;

– Параметры принтера — здесь можно настроить формат бумаги, качество печати и другие параметры, предусмотренные принтером и его драйвером;

– Параметры задания — здесь можно задать число копий, масштабирование, ориентацию страницы и т. п.;

– Уровни чернил/тонера — информационная вкладка, позволяющая определить, когда пора менять картридж(и).

18.4.2. Добавление локального принтера

1. Подключите принтер к ПК и включите питание принтера;
2. Выберите пункт меню «Сервер+Новый → Принтер». Если принтер обнаружен автоматически, от появится первым в списке «Устройства», в противном случае нужно будет выбрать порт и драйвер вручную;
3. Выберите драйвер принтера. Если принтер был обнаружен автоматически, рекомендованный драйвер уже будет предложен, и останется только нажать на кнопку

[Вперед]. Можно также задать свой собственный PPD-файл или найти нужный драйвер в интернете;

4. Заполните поля описания принтера. Для единственного домашнего принтера это, наверное, ни к чему, но в большом офисе с несколькими сетевыми принтерами это поможет не отправить случайно свой документ куда-нибудь на другой этаж;

5. Нажмите на кнопку [Применить принтер]. После этого он должен получить статусы «**Готовность**» и «**Доступен**».

18.4.3. Добавление удаленного принтера

1. Узнайте у администратора сети модель и название принтера, а также используемый протокол. Убедитесь, что принтер включен;

2. Выберите пункт меню [Сервер+Новый] → [Принтер], затем укажите в списке «Устройства» сетевой протокол;

3. Дальнейшая настройка выполняется по аналогии с подключением локального принтера.

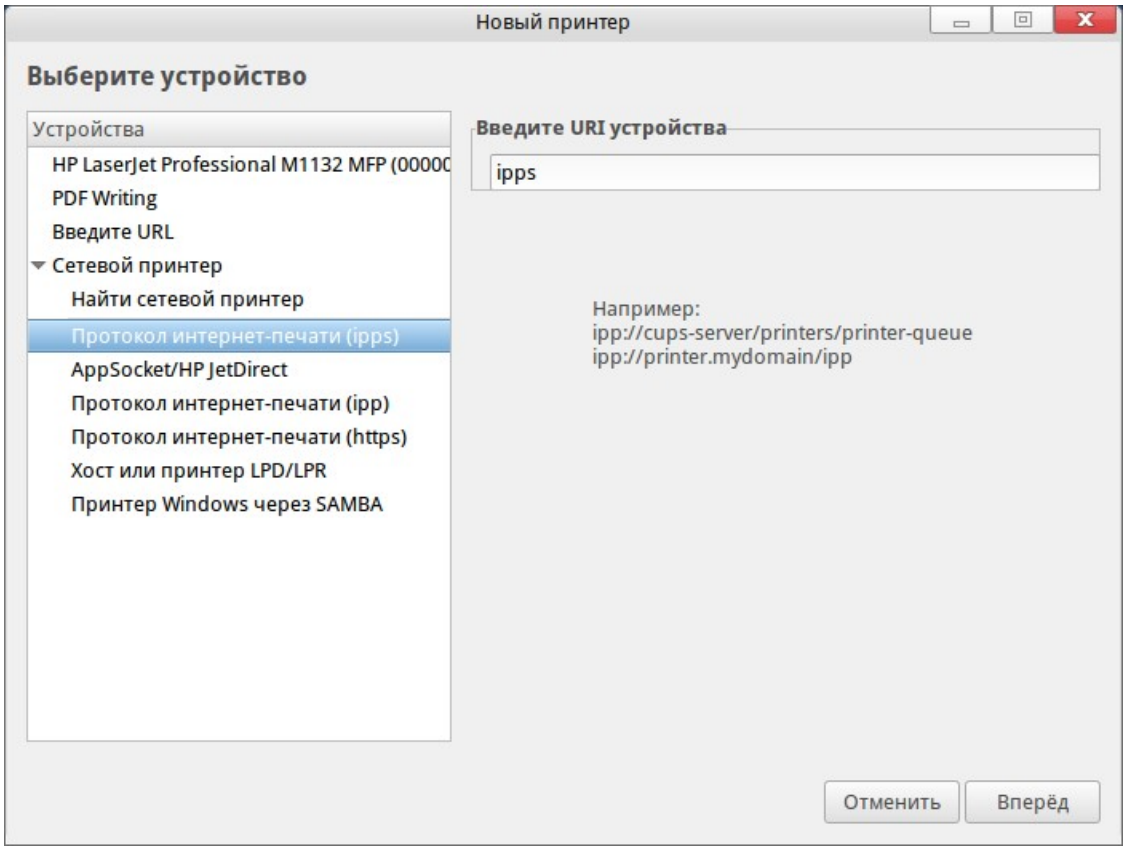


Рисунок 188

18.5. Подключение к сетям

ОС РОСА «НИКЕЛЬ» автоматически подключается к доступным сетевым

интерфейсам. Если автоматическое подключение не удалось, или если вы хотите настроить доступ в интернет, воспользуйтесь апплетом «Редактор соединений» (Network Manager) (Рисунок 189).

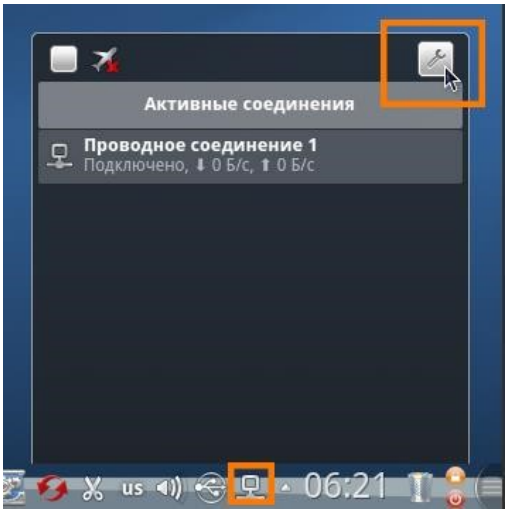


Рисунок 189

18.5.1. Добавление проводного соединения

После подключения кабеля к сетевой карте ПК выполняется автоматическое присвоение IP-адреса и других параметров локальной сети. Соединив ПК при помощи кабелей и сетевого оборудования (хабов, свитчей, роутеров), выберите в окне настроек «Редактора соединений» вкладку «Проводные» и нажмите на кнопку [Добавить]. В открывшемся окне перейдите на вкладку «IPv4» и выберите «Метод: Общий с другими компьютерами», после чего нажмите [OK].

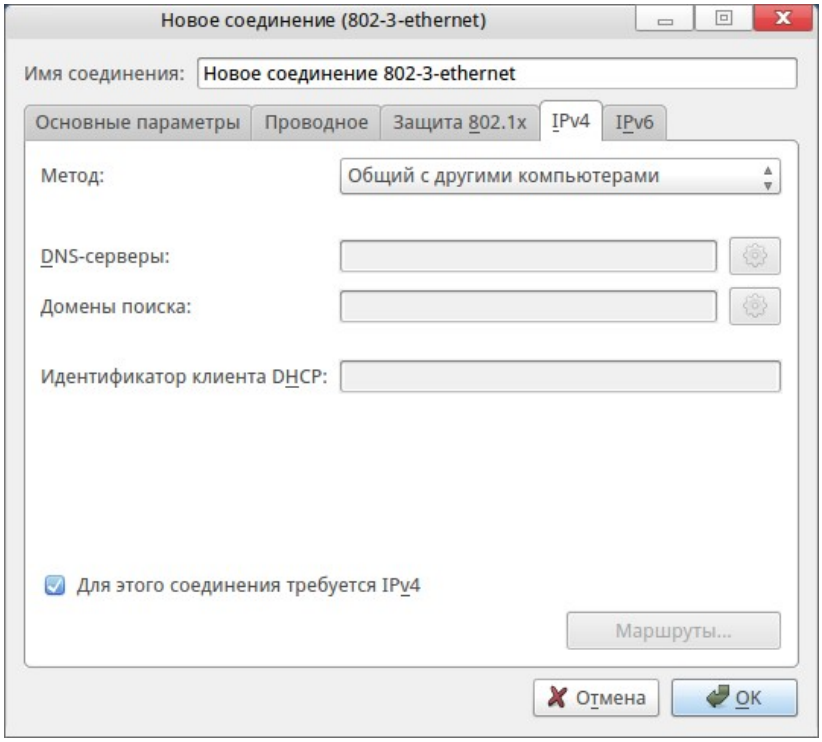


Рисунок 190

Такую операцию необходимо проделать на всех ПК, которые вы хотите объединить в сеть. Как только хотя бы два ПК будут настроены, локальная сеть должна заработать.

Если для подключения к интернету используется уже настроенный ADSL-модем, выход в интернет через проводное подключение станет доступным автоматически. Для настройки модема вы должны знать параметры сетевого подключения, в противном случае придется вызывать специалиста вашего интернет-провайдера.

18.5.2. Добавление беспроводного соединения (Wi-Fi)

Подключение к общедоступной открытой сети без шифрования данных осуществляется автоматически.

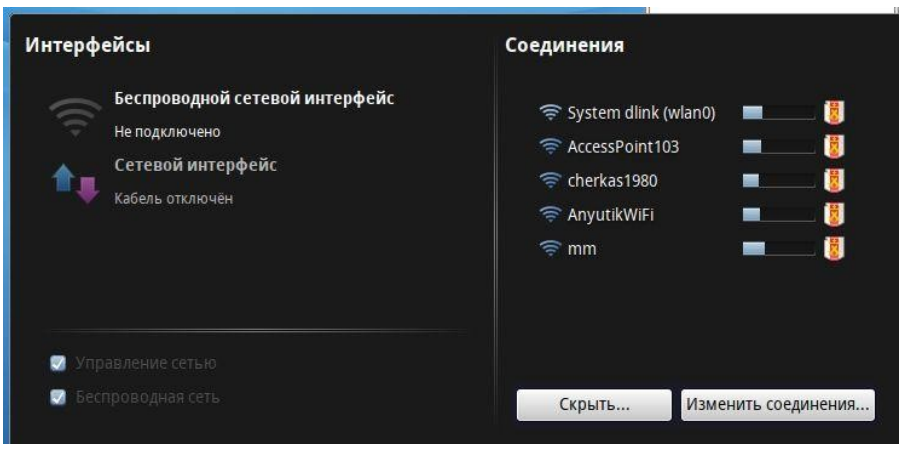


Рисунок 191

Такая сеть может предоставляться, например, посетителям каких-либо общественных мест. На панели «Редактора соединений» по умолчанию будет показан список обнаруженных открытых сетей. Чтобы увидеть список всех доступных сетей, нажмите на кнопку [Дополнительно]. Подключение к выбранной сети происходит после щелчка по ее названию и занимает некоторое время. При подключении к защищенной сети запрашивается пароль, и в этом случае соединение начинает устанавливаться только после ввода правильного пароля.

18.5.3. Настройка соединения

1. Выберите в окне настроек «Редактора соединений» вкладку «Беспроводные» и нажмите на кнопку [Сканировать] для поиска доступных сетей.

Обнаруженные сети можно просмотреть в виде таблицы или карты, на которой сети располагаются в зависимости от уровня радиосигнала: чем сильнее сигнал, тем ближе к ПК слева показана сеть;

2. Выбрав нужную сеть, нажмите [ОК]. Выбранная сеть появится на панели беспроводных соединений. Выделите ее и нажмите на кнопку [Изменить];

3. Нажмите «Copy current AP's MAC to BSSID» для заполнения поля BSSID, а остальные параметры оставьте по умолчанию. На вкладке «Защита беспроводной сети» выберите тип шифрования и введите пароль подключения в соответствии с полученными от провайдера данными и характеристиками вашего Wi-Fi-роутера.

Закончив настройку, вы увидите системное уведомление, и беспроводное соединение появится в окне «Редактора соединений».

18.5.4. Добавление мобильного соединения

После подключения USB-модема к порту ПК его определение инициализация должны произойти автоматически. Если все прошло успешно, система запросит у вас PIN-код SIM-карты и пароль подключения.

Если автоматическое подключение не удалось, выполните следующие действия:

1. Откройте «Редактор соединений», нажмите на кнопку [Изменить соединения] и перейдите на вкладку «Мобильное». Нажмите [Добавить], чтобы открыть окно «Новое мобильное соединение» (Рисунок 192);

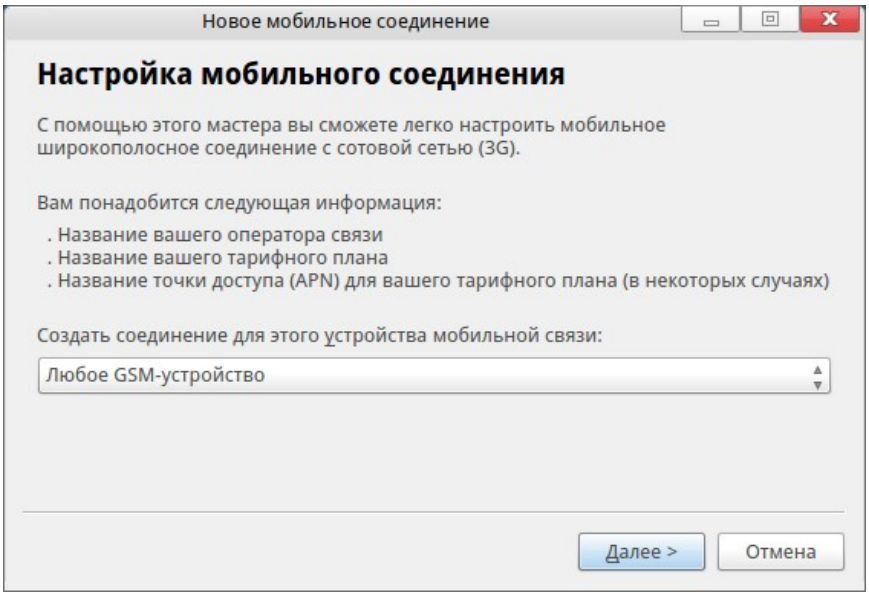


Рисунок 192

2. Модем должен определиться автоматически и появиться в списке. Выберите его и нажмите на кнопку [Далее];

3. Укажите страну и выберите оператора услуг связи, через которого будет осуществляться соединение;

4. Если необходимо, выберите тарифный план соединения. Обычно это не требуется, поскольку чаще всего USB-модем приобретается у оператора сотовой связи вместе с SIM-картой и конкретным тарифом. В этом случае тарифный план будет определен автоматически и изменить его будет нельзя. Если же вы приобрели универсальный модем, который может работать с разными SIM-картами, тарифный план следует вписать вручную (Рисунок 193).

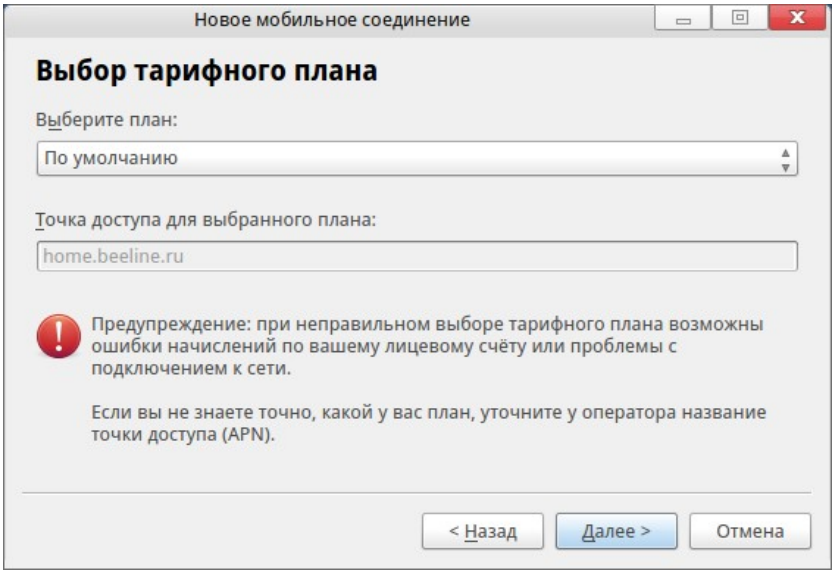


Рисунок 193

После ввода необходимых данных мастер запросит подтверждение, и на этом настройка мобильного соединения будет завершена.

Для подключения дважды щелкните по названию соединения. Если требование PIN-кода не отключено, его потребуется ввести. На панели подключения при необходимости можно отредактировать параметры соединения. Если все верно, нажмите [**OK**], и соединение будет установлено.

18.5.5. Добавление VPN-соединения (PPTP)

VPN (Virtual Private Network, «виртуальная частная сеть») — это технология, позволяющая создать защищенной сетевое соединение поверх незащищенной сети. С помощью VPN часто организуется подключение пользователей к интернету по выделенным линиям.

Для создания нового подключения VPN необходимо знать сетевое имя или IP-адрес шлюза, логин и пароль. Эти данные предоставляет интернет-провайдер.

1. Откройте «Редактор соединений», нажмите на кнопку [Изменить соединения] и перейдите на вкладку «VPN». Нажмите [Добавить], чтобы открыть окно «Новое соединение (vpn)» (Рисунок 194);

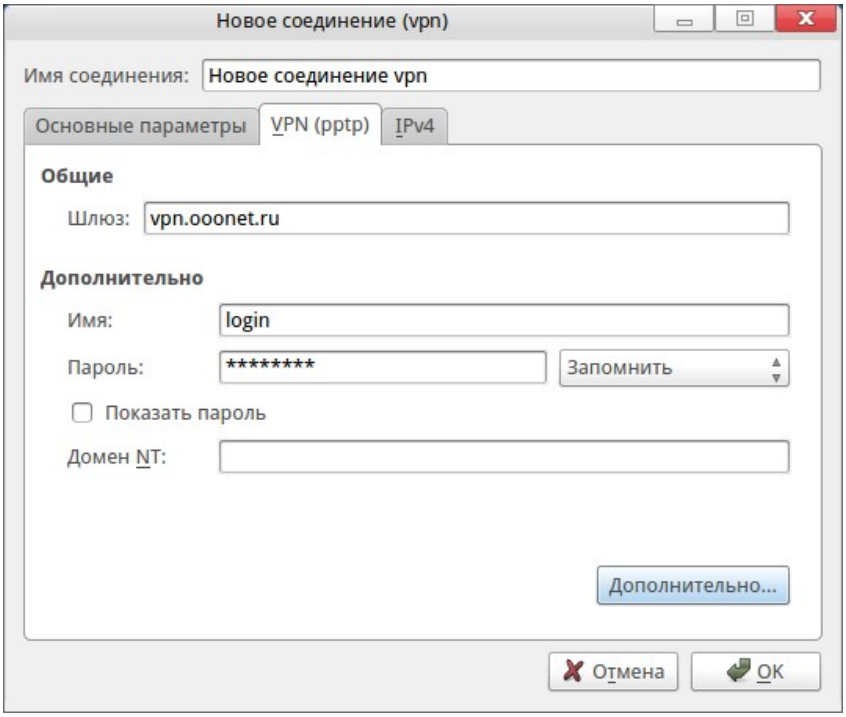


Рисунок 194

2. Перейдите на вкладку «VPN (pptp)» и введите данные, полученные от провайдера;

3. Нажмите на кнопку [Дополнительно...]. Выберите «Шифрование: Любое» и нажмите [OK].

После того, как вы завершите настройку соединения, подключение должно произойти автоматически. Если этого не происходит, запустите созданное соединение

щелчком мыши в окне «Редактора соединений».

18.5.6. Добавление DSL-соединения

Подключите сетевой кабель ADSL-модема к сетевой карте ПК. При настроенном модеме подключение к интернету произойдет автоматически. Если автоматическое подключение не удалось, выполните следующие действия:

1. Откройте «Редактор соединений», нажмите на кнопку [Изменить соединения] и перейдите на вкладку «DSL». Нажмите [Добавить], чтобы открыть окно «Новое соединение (pppoe)» (Рисунок 195);

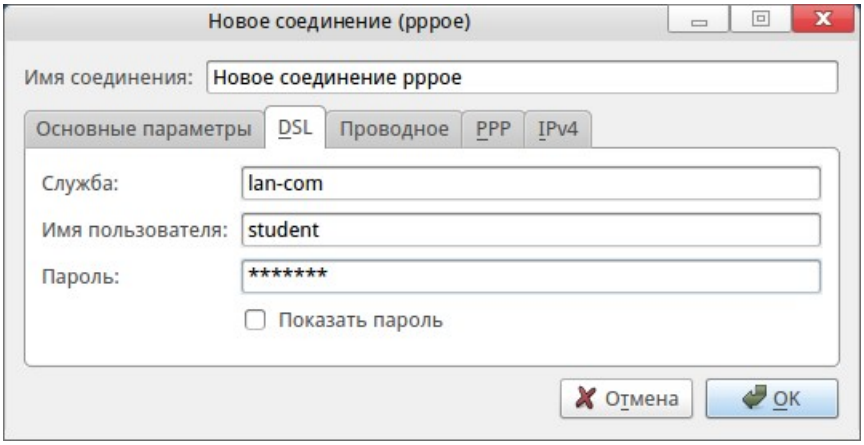


Рисунок 195

2. Заполните поля на вкладках «DSL», «Проводное» и «IPv4». Необходимые данные должен предоставить ваш интернет-провайдер. На вкладке «IPv4» выберите «Метод: Автоматически (PPPoE)». Клиент DHCP автоматически получит у провайдера нужные данные и передаст их «Редактору соединений»;

3. Если соединение не устанавливается, нужно связаться с технической поддержкой провайдера и получить данные для подключения вручную. В этом случае на вкладке «IPv4» выберите «Метод: Отключено».

18.5.7. Консольные команды для управления сетями

Для оперативного получения информации о сетевых подключениях, доступности сетевых ресурсов и т. п. можно использовать следующие команды, выполняемые в консоли:

- `ifconfig` — показать параметры всех сетевых соединений;
- `ping` <адрес_узла> — проверить качество сетевого соединения с заданным узлом;
- `route -n` — вывести на экран таблицу маршрутизации.

19. ИСПОЛЬЗОВАНИЕ УТИЛИТЫ ROSA CRYPTO TOOL

Утилита ROSA Crypto Tool установлена в дистрибутиве по умолчанию. Она используется в качестве графической оболочки для утилит командной строки, входящих в состав КриптоПро. Утилита предназначена для работы с электронной подписью и шифрованием.

Для работы с ROSA Crypto Tool необходимо сначала подключить устройство, а затем запустить саму программу.

Утилита ROSA Crypto Tool работает с электронно-цифровыми подписями, хранящимися в контейнере формата .sig СКЗИ КриптоПро.

В программе предусмотрена реализация подписи и проверки подписи файлов в соответствии с ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001.

19.1. Описание элементов интерфейса

Пользовательский интерфейс программы приведен на рисунке 196.

Рисунок 196

Далее будут описаны основные компоненты рабочего окна программы. Полное руководство пользователя можно найти, перейдя во вкладку Параметры →Справка.

19.1.1. Панель инструментов

На панели инструментов располагаются пять кнопок. Первые четыре кнопки предназначены для переключения режимов работы с СКЗИ, а именно:

1) Подписать файл;
2) Проверить подпись;

3) Шифровать;

4) Расшифровать.

На следующем рисунке представлена панель инструментов.

Рисунок 197

Последняя кнопка называется [Параметры] и содержит в себе дополнительное подменю, не относящееся напрямую к работе с СКЗИ.

19.1.2. Рабочая область

Рабочая область программы располагается под панелью инструментов.

Если все компоненты, необходимые для полного функционирования программы, успешно установлены и функционируют, в рабочей области будет отображаться только приветствующий текст:

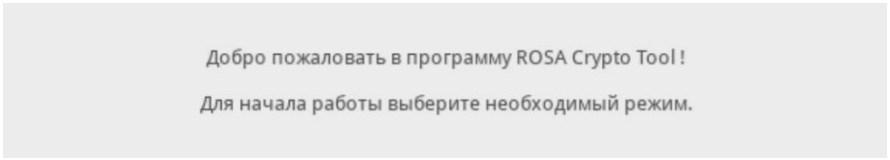


Рисунок 198

В противном случае под приветствующем текстом будет выведено соответствующее сообщение:

Рисунок 199

При подключении или извлечении токена из ПК под текстом приветствия будет выведено соответствующее сообщение.

После выбора кого-либо из режимов на панели инструментов в рабочей области появится набор графических элементов для работы с СКЗИ.

На рисунке Рисунок 200 представлено поле, информирующее о статусе токенов.

Рисунок 200

Это поле доступно во всех режимах.

19.2. Подпись файла

Чтобы подписать файл, необходимо:

1) На панели инструментов выбрать режим «Подписать файл» (Рисунок 201);

2) Указать файл с помощью кнопки [Выбрать];

3) Если в ПК установлено несколько токенов, в поле «Сертификат» из выпадающего списка выбрать необходимый;

4) Нажать на кнопку [Подписать файл].

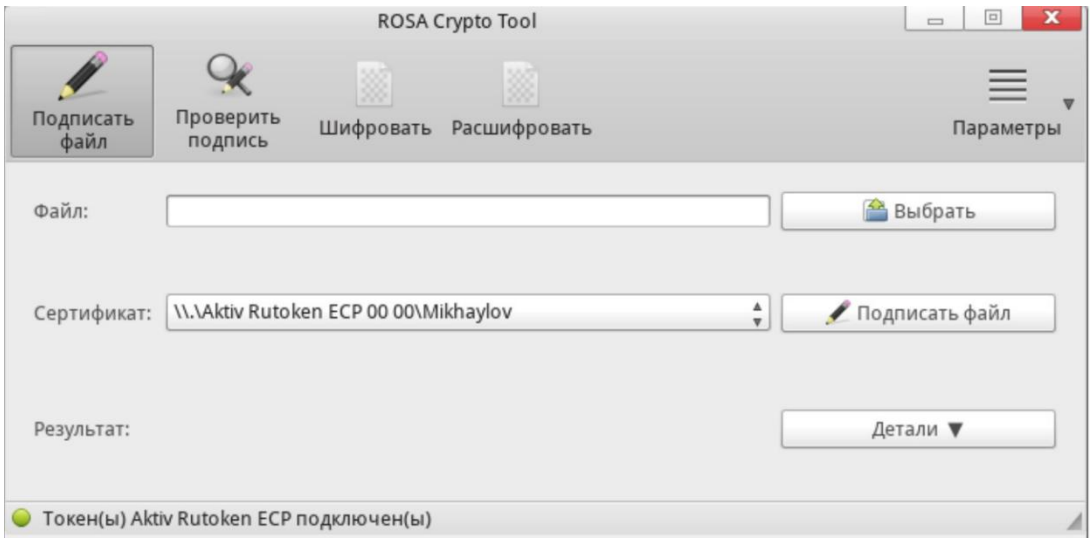


Рисунок 201

После успешного выполнения операции в поле «Результат» будет выведено соответствующее оповещение, и в папке выбранного файла появится подписанный файл с расширением .sig.

Кнопка [Детали] раскрывает поле «Результат» для отображения более полной информации, доступной для выделения и копирования.

19.3. Проверка подписи

Чтобы проверить подпись файла, необходимо:

1) На панели инструментов выбрать режим «Проверить подпись»;

2) Указать файл с помощью кнопки [Выбрать];

3) Если дополнительно необходимо установить сертификат из файла подписи и/или отделить исходный файл от файла подписи, выставить галочки слева от имени соответствующей дополнительной опции;

4) Нажать на кнопку [Проверить подпись] (Рисунок 202).

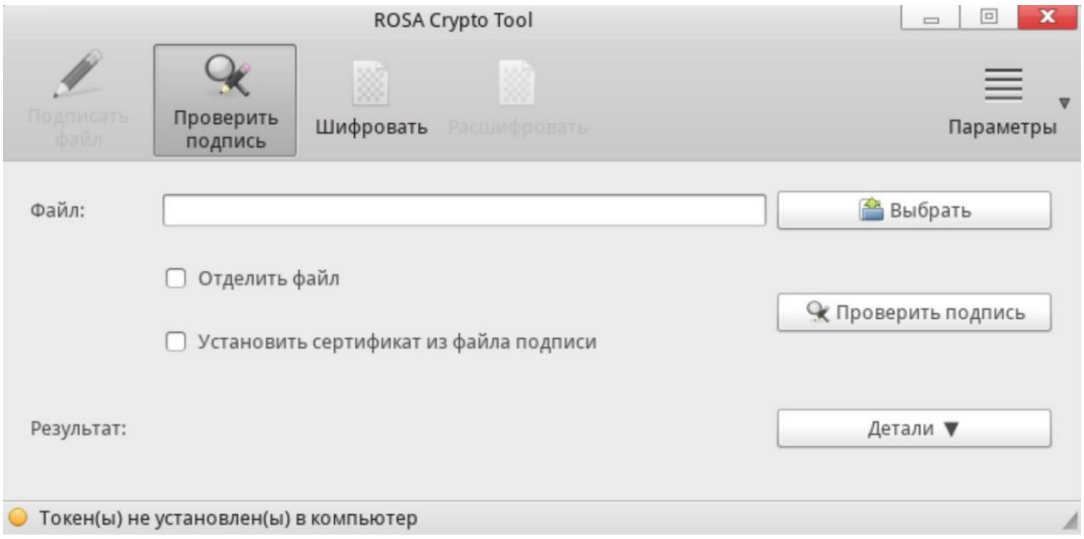


Рисунок 202

После выполнения операции в поле «Результат» будет выведено соответствующее оповещение.

Кнопка [Детали] раскрывает поле «Результат» для отображения более полной информации, доступной для выделения и копирования.

19.4. Шифрование файла

Чтобы выполнить шифрование файла, необходимо:

1) На панели инструментов выбрать режим «Шифровать» (Рисунок 203);
2) Указать файл с помощью кнопки [Выбрать];
3) В поле «Сертификат» выбрать сертификат, с помощью которого необходимо зашифровать файл;
4) Нажать на кнопку [Шифровать].

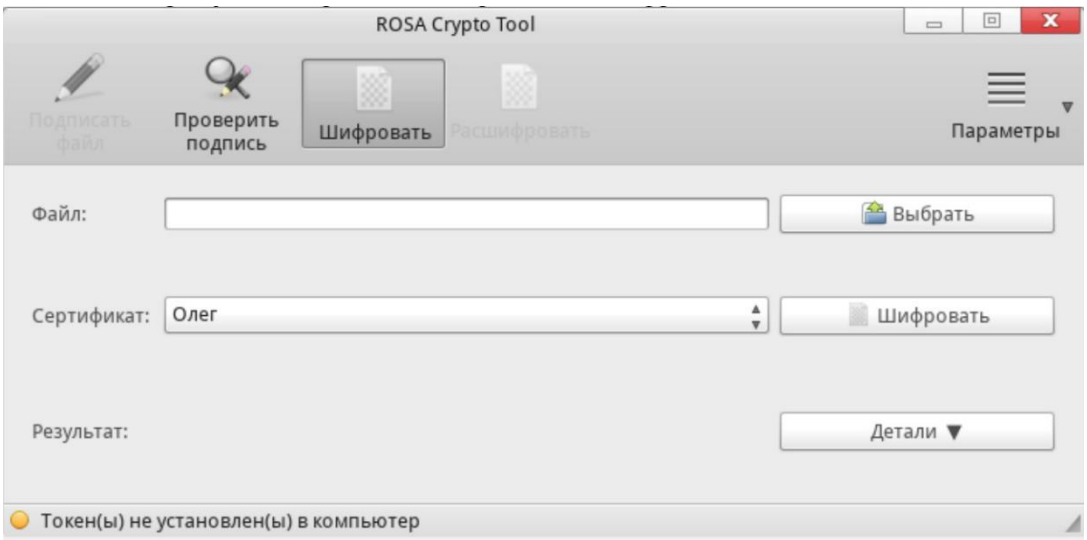


Рисунок 203

После успешного выполнения операции в поле «Результат» будет выведено

соответствующее оповещение, и в каталоге выбранного файла появится файл подписи с расширением .enc.

Кнопка [Детали] раскрывает поле «Результат» для отображения более полной информации, доступной для выделения и копирования.

19.5. Расшифрование файла

Чтобы выполнить расшифровывание файла, необходимо:

1) На панели инструментов выбрать режим «Расшифровать» (Рисунок 204);

2) Указать файл с помощью кнопки [Выбрать];

3) Если в ПК установлено несколько токенов, в поле «Сертификат» из выпадающего списка выбрать необходимый;

4) Нажать на кнопку [Расшифровать].

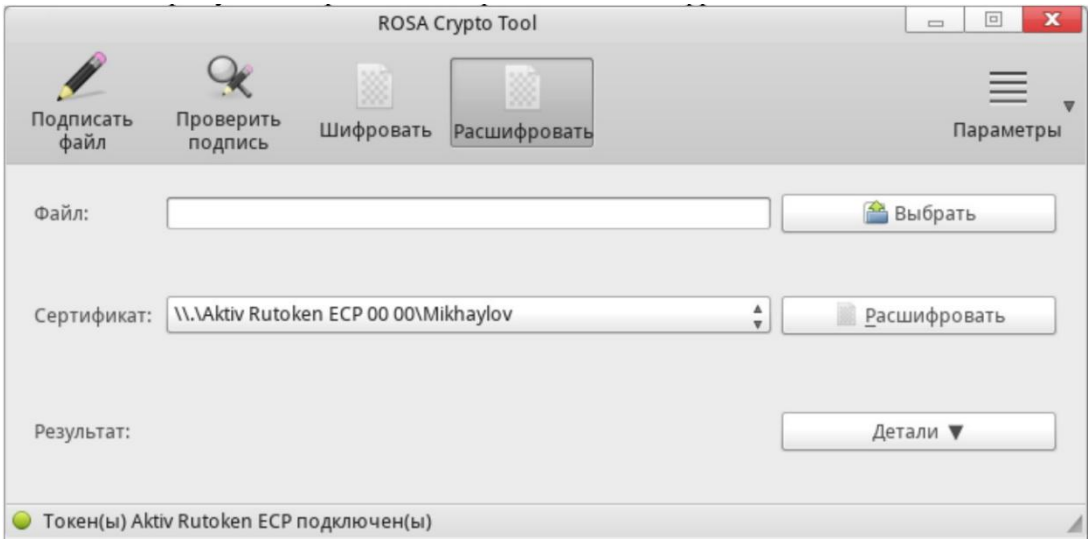


Рисунок 204

После выполнения операции в поле «Результат» будет выведено соответствующее оповещение.

Кнопка [Детали] раскрывает поле «Результат» для отображения более полной информации, доступной для выделения и копирования.

19.6. Параметры

Кнопка [Параметры] содержит в себе дополнительное подменю, включающее в себя такие опции, как:

– «Проверка компонентов программы» — проверяет наличие необходимых компонентов для успешной работы программы и соответствующее оповещение пользователя;

– «О программе ROSA Crypto Tool» — выводит краткую информацию о программе;

– «Справка» — открывает руководство пользователя;

– «Выход» — осуществляет выход из программы.

20. ЗАЩИТА SSH-СОЕДИНЕНИЙ

Secure Shell (SSH) — это мощный сетевой протокол, используемый для организации удаленного подключения к системе по защищенному каналу. Передача данных по SSH шифруется и защищена от перехвата.

Примечание. В этом разделе рассказывается о наиболее стандартных способах защиты SSH, и предлагаемые здесь способы ни в коем случае не должны считаться исчерпывающими или окончательными. Описание всех значений параметров, доступных для изменения поведения демона sshd, можно просмотреть на странице руководства sshd_config, а объяснения базовых принципов работы SSH — на странице руководства man ssh.

20.1. Криптографический вход в систему

SSH поддерживает использование криптографических ключей для входа в систему. Этот способ гораздо более надежен, чем использование пароля. Сочетание этого способа с другими способами аутентификации может считаться многофакторной аутентификацией.

Использование криптографических ключей для аутентификации возможно, если параметр `PubkeyAuthentication` файла /etc/ssh/sshd_config имеет значение `yes` (так установлено по умолчанию).

Чтобы отключить возможность использования паролей для входа в систему, установите `no` для параметра `PasswordAuthentication`.

Ключи SSH можно создать с помощью команды `ssh-keygen`. При вызове без дополнительных аргументов эта команда создает набор ключей RSA длиной 2048 бит. По умолчанию ключи хранятся в каталоге ~/.ssh/. Для изменения надежности ключа используйте аргумент `-b`. Обычно ключа длиной 2048 бит вполне достаточно.

Теперь в каталоге ~/.ssh/ можно увидеть два ключа. Если при вызове команды `ssh-keygen` были приняты значения по умолчанию, эти два ключа будут называться `id_rsa` и `id_rsa.pub` и содержать закрытый и открытый ключи, соответственно. Закрытый ключ необходимо защитить от внешнего воздействия, сделав его нечитаемым для всех, кроме владельца файла. Открытый ключ должен быть перенесен в ту систему, в которую предполагается вход. Для переноса ключа на сервер используйте следующую команду:

```
$ ssh-copy-id -i user@server
```

Эта команда также автоматически добавит открытый ключ в файл `~/.ssh/authorized_keys` на сервере. Демон sshd будет проверять этот файл при попытке входа на сервер.

Как и пароли, ключи SSH необходимо регулярно менять. При это не забывайте удалять любые неиспользуемые ключи из файла authorized_keys.

20.2. Методы многофакторной аутентификации

Использование нескольких способов аутентификации, или многофакторная аутентификация, повышает уровень защиты от неавторизованного доступа и поэтому должно рассматриваться при укреплении системы для защиты от взлома. Для получения доступа к системе, в которой используется многофакторная аутентификация, пользователи должны успешно пройти все этапы аутентификации.

Используемые способы аутентификации указываются в файле /etc/ssh/sshd_config. Обратите внимание, что с помощью его параметров можно указать более одного списка требуемых методов аутентификации, и в таком случае пользователь должен будет успешно пройти каждый метод как минимум из одного списка. Элементы списка разделяются пробелами, а отдельные названия способов аутентификации — запятыми. Например:

```
AuthenticationMethods publickey, gssapi-with-mic publickey, keyboard-interactive
```

Демон sshd, настроенный с помощью вышеуказанной директивы `AuthenticationMethods`, предоставит доступ только в том случае, если пользователь успешно пройдет аутентификацию по открытому ключу либо в совокупности с gssapi с микрофоном, либо в совокупности с интерактивной аутентификацией с помощью клавиатуры. Обратите внимание, что каждый из запрашиваемых методов аутентификации должен быть явным образом активирован с помощью соответствующей директивы конфигурации (например, `PubkeyAuthentication`) в файле /etc/ssh/sshd_config.

20.3. Другие средства защиты SSH

20.3.1. Версия протокола

Хотя реализация протокола SSH, поставляемая в ОС РОСА «НИКЕЛЬ», поддерживает как первую, так и вторую версию протокола для клиентов SSH, только вторая версия должна быть использована везде, где это возможно. Версия SSH-2

содержит многочисленные улучшения по сравнению со старой версией 1, и большинство продвинутых конфигураций возможны только при использовании SSH-2.

20.3.2. Типы ключей

Хотя по умолчанию команда ssh-keygen создает пару ключей SSH-2 RSA, с помощью переданного параметра -t ей можно указать создать также и ключи DSA или ECDSA. Алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm) предоставляет лучшую производительность при той же эквивалентной длине симметричного ключа. Также он создает более короткие ключи.

20.3.3. Порт не по умолчанию

По умолчанию демон sshd слушает TCP порт 22. Смена порта сокращает возможное число уязвимостей системы для атак с использованием автоматического сканирования сети, повышая таким образом защиту по принципу «безопасность через неясность» (security through obscurity). Указать порт можно с помощью директивы `Port` в конфигурационном файле /etc/ssh/sshd_config. Также обратите внимание, что для использования порта не по умолчанию нужно изменять политику SELinux по умолчанию. Это можно сделать, изменив тип SELinux ssh_port_t при помощи следующей команды:

```
# semanage -a -t ssh_port_t -p tcp <номер_порта>
```

Замените `<номер_порта>` на новый номер, указанный с помощью директивы `Port`.

20.3.4. Запрет входа в систему под учетной записью root

Если частный случай использования не предусматривает возможности входа в систему под учетной записью root, укажите значение `no` для директивы `PermitRootLogin` в файле /etc/ssh/sshd_config. Отключив возможность прямого входа в систему под учетной записью root, системный администратор может проверить, какие именно команды выполняются с полученными привилегиями root, и какие именно пользователи их выполняют, получив доступ в систему и затем получив права root.

20.3.5. Использование PAM для ограничения доступа к службам с привилегиями root

Модуль PAM /lib/security/pam_listfile.so предоставляет очень гибкое средство ограничения доступа для различных учетных записей. Администратор может использовать этот модуль для указания списка пользователей, которым запрещен вход в систему. Для ограничения доступа root к системной службе отредактируйте файл нужной

службы в каталоге /etc/pam.d/ так, чтобы для аутентификации требовался модуль pam_listfile.so.

В примере ниже можно увидеть, как этот модуль используется для сервера vsftpd FTP в конфигурационном файле PAM /etc/pam.d/vsftpd (символ \ в конце первой строки необязателен, если директива умещается в одну строку):

```
auth required pam_listfile.so item=user sense=deny file=/etc/vsftpd.ftpusers onerr=succeed
```

Эти параметры указывают PAM обратиться к файлу /etc/vsftpd.ftpusers и отказать в доступе к службе любому из указанных пользователей. Администратор может изменить название этого файла, а также может либо хранить отдельный список для каждой службы, либо использовать один главный список для отказа в доступе ко многим службам.

При необходимости отказать в доступе к нескольким службам аналогичную строку можно добавить в конфигурационные файлы PAM /etc/pam.d/pop и /etc/pam.d/imap (для почтовых клиентов) или /etc/pam.d/ssh (для клиентов SSH).

21. СУБД POSTGRESQL

21.1. Общая информация

В качестве СУБД в составе ОС РОСА «НИКЕЛЬ» используется СУБД PostgreSQL. Данный раздел является кратким описанием встроенных функций, основного синтаксиса языка запросов SQL, создания отказоустойчивых решений. Дальнейшее описание представляет собой краткий обзор официальной документации PostgreSQL.

С полной версией руководств СУБД PostgreSQL вы можете ознакомиться в разделе Документации на официальном сайте разработчика https://postgrespro.ru/docs/.

СУБД PostgreSQL предназначена для создания и управления реляционными БД и предоставляет многопользовательский доступ к расположенным в них данным. Данные в реляционной БД хранятся в отношениях (таблицах), состоящих из строк и столбцов. При этом единицей хранения и доступа к данным является строка, состоящая из полей, идентифицируемых именами столбцов. Кроме таблиц, существуют другие объекты БД (виды, процедуры и т. п.), которые предоставляют доступ к данным, хранящимся в таблицах. Для работы СУБД на диске выделяется область для хранения БД, называемая «кластером БД». Кластер БД является набором БД, управляемых одним экземпляром сервера СУБД. Настройка работы отдельного экземпляра сервера СУБД также определяется в рамках кластера соответствующими конфигурационными файлами.

Рабочий сеанс Postgres включает следующие взаимодействующие процессы (программы):

– главный серверный процесс, управляющий файлами баз данных, принимающий подключения клиентских приложений и выполняющий различные запросы клиентов к базам данных. Эта программа сервера БД называется postgres;

– клиентское приложение пользователя, желающее выполнять операции в базе данных. Клиентские приложения могут быть очень разнообразными: это может быть текстовая утилита, графическое приложение, веб-сервер, использующий базу данных для отображения веб-страниц, или специализированный инструмент для обслуживания БД.

21.2. Основные параметры управления сервисом

Используйте команду `systemctl` в консоли для управления службой PostgreSQL:

Для того, чтобы начать обслуживание сервиса используйте команду:

```
systemctl start postgresql
```

Для остановки обслуживания:

```
systemctl stop postgresql
```

Для отключения службы используйте следующую команду, после которой PostgreSQL больше не будет запускаться автоматически:

```
systemctl disable postgresql
```

Для активации автоматического запуска PostgreSQL воспользуйтесь командой:

```
systemctl enable postgresql
```

22. СРЕДСТВО АВТОМАТИЗАЦИИ ANSIBLE

Ansible – это программное обеспечение, которое занимается автоматизацией рутинных и повторяющихся задач, таких как управление и настройка удаленных серверов.

Для организации настройки администратору системы необходимо лишь описать, как достичь необходимых параметров с помощью так называемых сценариев – playbooks. Такая технология позволяет очень быстро осуществлять переконфигурирование системы: достаточно всего лишь добавить несколько новых строк в сценарий.

Для работы на клиенте приложению Ansible достаточно лишь ssh-соединения с сервером или несколькими серверами.

Полная справка по программе дана в man ansible.

22.1. Синтаксис Ansible

Все операции, выполняемые Ansible записываются в playbook в простом формате и построены на yaml-разметке.

Рассмотрим пример записи сценария:

```
- name: "First step"
 hosts: localhost
 tasks:
 - taskA
 - taskB
```

Где параметр:

– name: «First step» – имя группы задач;

– hosts: localhost – хосты, на которых будут выполнены задачи;

– параметры, перечисленные после команды tasks – перечень задач, которые необходимо выполнить.

В одном playbook может быть несколько блоков с задачами, для чего необходимо добавить дополнительные параметры `name`, после завершения описания предыдущей группы задач.

Далее рассмотрим непосредственно команды программы - `tasks`. Команды являются модулями Ansible. Таким образом задавая параметры task, вызывается модуль Ansible с его параметрами.

Записать task можно в двух видах: кратком, и полном. Вот пример команды установки curl при помощи dnf модуля в кратком виде:

```
- dnf: name=curl state=latest
```

Тогда play с этим task будет выглядеть как отражено ниже, где модуль `dnf` устанавливает пакет `curl`:

```
- name: "First step"
 hosts: localhost
 tasks:
- dnf: name=curl state=latest
```

где параметры

- name: - имя задачи;
- hosts: - хост, на котором будет применяться playbook;
- tasks: - блок задачи.

Существует возможность более полно описать команду task, присвоить ей имя (name). Совсем как в блоках задач (play). Тогда получившийся текст выглядит как подзадача основного блока задач.

```
- name: "First step"
 hosts: localhost
 tasks:
  - name: "Add curl packege"
 dnf: name=curl state=latest
```

В этому случае сразу видно, что есть блок задач «First step», в нем существует 1 задача - установка пакета curl.

22.2. Запуск программы

Текстовый файл, содержащий сценарии, необходимо сохранить в файл “first.yml” и запустить его, придерживаясь нижеописанной инструкции.

1. Предварительно установим сам пакет Ansible командой

```
dnf install –y ansible
```

2. Для запуска playbook, необходимо разархивировать архив и зайти в папку из архива:

```
ansible-playbook ./dnf_user_install.yml
```

Запуск playbook с помощью команды ansible-playbook при помощи написанного playbook dnf_user_install.yml.

3. После реализации данной команды получиться следующий вывод:

```
      [WARNING]: provided hosts list is empty, only localhost is
available. Note that the implicit localhost does not match 'all'
      PLAY                              [First                              step]
*********************************************************************
*********************************************************************
******************
      TASK                          [Gathering                          Facts]
*********************************************************************
*********************************************************************
*************
      ok: [localhost]
      TASK                 [Add                 curl                 packege]
*********************************************************************
*********************************************************************
************
      ok: [localhost]
      TASK                  [Add                  user                  rosa]
*********************************************************************
*********************************************************************
***************
      ok: [localhost]
      PLAY                                                              RECAP
*********************************************************************
*********************************************************************
************************
      localhost                  : ok=3   changed=0   unreachable=0   failed=0
skipped=0   rescued=0   ignored=0
```

Где блок задач `PLAY`, называемый `First step`, а также команды (`TASK`) по установке программы curl и добавление пользователя rosa. Все задачи завершились успешно `(ok=3, failed=0) (changed=2)`, а именно: выполнено три действия (ok=3), завершилось с ошибкой 0 действий (filed=0) и на хосте произошло 2 изменения.

`Gathering Facts (Дополнительная задача)` – получение информации о хосте (такой как имя хоста и пр.), вызвалась автоматически. Она необходима для использования данных о хосте в своих сценариях, это своеобразный мониторинг о системе, который собирает такую информацию имя машины, ip-адресацию и другие

параметры. Можно запретить эту задачу, указав `gather_facts : false`

```
- name: "First step"
 hosts: localhost
 gather_facts: false
 ....
```

22.3. Файл инвентаризации

Так называемый файл инвентаризации (файл hosts*)* – это файл, в котором хранится перечень машин, с которыми будет работать Ansible.

Располагаться он может в вашей директории и иметь примерно такой вид:

```
[mail]
192.168.1.1
192.168.1.2

[web]
192.168.1.3
```

Где параметры

- `[mail]` и `[web]` – имена групп хостов;
- `192.168.1.1, 192.168.1.2, 192.168.1.3` - ip адрес второго хоста.

Тут, как видно, указываются группы, в них имена хостов, можно с указанием переменных для хоста. Структура inventory-файла очень гибкая, в нем допустимо комбинировать группы, включать одну в другую, задавать переменные для групп, глобальные значения:

```
[all:vars]
ansible_user=root
hosts: web
```

Где параметры

- [all:vars] – переменные для всех хостов;
- ansible_user=root – пользователь, от которого будет работать ansible на удаленных машинах;
- hosts: web – группа хостов, на которых будут выполняться playbook.

А затем вызвать playbook, указав параметром файл инвентаризации (предварительно этот файл нужно заполнить, так как инфраструктура у всех разная):

```
ansible-playbook ./dnf_user_install.yml –i ./hosts
```

С помощью данной команды запускается `ansible-playbook`, запустите

playbook /dnf_user_install.yml который применится на хостах из файла ./hosts где описана инвентаризация сетевой инфраструктуру ip адреса до хостов.

Примеры использования:

Рассмотрим пример доверенной установки, удаления и централизованной настройки средств защиты данных.

1. Для установки используем playbook install.yml его содержимое выглядит так:

```
- name: "install rosa-removable-drive-manager
 hosts: localhost
 tasks:
  - name: "install rosa-removable-drive-manager
        dnf: name=rosa-removable-drive-manager state=latest
```

Где параметры

- name – имя выполняемого таска;
- hosts – имя хоста, на котором будет выполняться таск;
- tasks - блок выполнения задания.

Запускаем playbook:

```
ansible-playbook install.yml
```

2. Для удаления используем playbook remove.yml его содержимое выглядит так:

```
- name: "remove rosa-removable-drive-manager"
 hosts: localhost
 tasks:
  - name: "Remove rosa-removable-drive-manager
    dnf: name=rosa-removable-drive-manager state=absent
```

Запускаем playbook:

```
ansible-playbook remove.yml
```

3. Для централизованной настройки используем playbook provision.yml его содержимое выглядит следующим образом:

```
- name: "insert template rosa-removable-drive-manager"
 hosts: localhost
 tasks:
  - name: "putt template rosa-removable-drive-manager"
    template: src=00-rosa-removable-drive-manager.rules.j2
dest=/etc/polkit-1/rules.d/src=00-rosa-removable-drive-manager.rules
```

В данном блоке берется конфигурационный файл из папки `templates(00-rosa-removable-drive-manager.rules.j2` и распространяется по пути `/etc/polkit-`

`1/rules.d/` тем самым осуществляется централизованная настройка приложений.

4. Запускаем playbook:

```
ansible-playbook provision.yml
```

22.4. Роли Ansible

Роли обеспечивают основу для полностью независимых или взаимозависимых наборов переменных, задач, файлов, шаблонов и модулей.

В Ansible роли являются основным механизмом разбиения playbook на несколько файлов. Это упрощает написание сложных сценариев и облегчает их повторное использование. Роли позволяют логически разбить playbook на компоненты многократного использования.

Каждая роль в основном ограничена определенной функциональностью или желаемым результатом со всеми необходимыми шагами для обеспечения этого результата либо внутри самой роли, либо в других ролях, перечисленных как зависимости.

22.4.1. Создание новой роли

Структура каталогов для ролей необходима для создания новой роли.

Роли имеют структурированное дерево файлов в системе. Структура по умолчанию может быть изменена, но далее рассмотрим пример создания каталога ролей со значениями по умолчанию.

Каждая роль представляет собой дерево каталогов само по себе. Имя роли — это имя каталога в каталоге / role.

22.4.2. Создание каталога ролей

Приведенная выше команда описывает структуру каталога роли.

```
$ tree role/
rosa_install_tcpdump/
├── task
│   └── main.yml
├── files
├── templates
└── vars
    └── main.yml
```

Где параметры:

– task – папка, где хранятся таски и playbook;

- main.yml – файл с playbook где описываются действия;
- files – папка, где хранятся файлы или скрипты;
- templates – папка, где хранятся файлы шаблонов программ;
- vars – папка, где хранятся переменные;
- main.yml – файл, где хранятся переменные для инфраструктуры.

23. МЕРЫ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ

ОС разрешается устанавливать и использовать только на совместимом оборудовании. Использовать ОС на не совместимом оборудовании воспрещается.

ОС можно использовать только в том случае, если обеспечивается доверенная загрузка, а именно:

– попытки несанкционированной загрузки блокированы (пароль на загрузчик либо в АПМДЗ должен быть установлен в соответствии с политикой, действующей в АС/ИС);

– осуществляется контроль доступа субъектов доступа к процессу загрузки (имя администратора загрузки обязательно должно быть установлено);

– контроль целостности компонентов загружаемой операционной среды (в АПМДЗ должны быть активизированы функции контроля целостности для загружаемой ОС или ее компонентов).

Персонал, отвечающий за установку, конфигурирование и эксплуатацию ОС должен в точности руководствоваться эксплуатационной документацией при работе с ней. Необходимо, чтобы каждый пользователь ОС, участвующий в процессе обработки информации или настройке ОС, проходил соответствующее обучение (инструктаж), прежде чем приступить к работе. В составе документации у подразделения, отвечающего за эксплуатацию ОС, должен быть соответствующий документ, регламентирующий процессы обучения (инструктажа) персонала для работы с ОС.

Воспрещается несанкционированное вскрытие или иные воздействия, направленные на нарушение целостности СВТ, на которых осуществляется работа с ОС.

Воспрещается эксплуатация ОС в том случае, если СВТ, которые работают под ее управлением, не отвечают требованиям минимальной конфигурации. Резервные копии ОС и данных, которые включены в состав резервных копий, должны быть надежно защищены. В составе документации у подразделения, отвечающего за эксплуатацию ОС, должен быть соответствующий документ, регламентирующий процессы резервного копирования.

Требуется ограничивать использование программ (или их компонентов), непосредственно не задействованных в технологическом процессе обработки информации или в его обеспечении.

При взаимодействии ОС с пользователям (администраторам), должен быть обеспечен контроль источников ввода информации. Использование несанкционированных источников ввода информации не допускается.

При взаимодействии ОС с другими доверенными продуктами ИТ, должен обеспечиваться доверенный канал передачи данных между ОС и средствами вычислительной техники, на которых происходит обработка информации, а также с которых происходит их администрирование.

Меры, направленные на несанкционированное отключение СВТ, на которых функционирует ОС должны быть реализованы. Как минимум, должны быть отключены параметры ядра ОС, позволяющие использовать Magic Sys RQ (отключены по умолчанию).

При работе с ОС пользователям воспрещается раскрывать свою аутентификационную информацию (пароль) кому бы то ни было. Пользователи должны в строгой тайне хранить свой пароль. В том случае, если у пользователя появилось подозрение, что пароль может быть скомпрометирован, пользователь обязан доложить об этом персоналу, отвечающему за обслуживание системы, либо непосредственному руководителю (если иное не предписано в соответствующих документах, регламентирующих парольную защиту). В составе документации у подразделения, отвечающего за эксплуатацию ОС, должен быть соответствующий документ, регламентирующий процессы жизненного цикла аутентификационной информации (назначение, хранение, удаление и т.п.).

Персонал, отвечающему за эксплуатацию ОС рекомендуется следовать указаниям, определенным производителем оборудования, на котором функционирует ОС. Например, если производитель оборудования рекомендует активизировать биты процессора (NX/XD) для защиты от переполения буфера, или если рекомендуется отключать функции SMT для противостояния атакам типа Meltdown/Spectre -- такие меры должны как минимум оцениваться персоналом, отвечающим за эксплуатацию ОС, и по возможности предприниматься, если они не противоречат целям обработки информации.

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в Таблица 67.

Таблица 67

Термин/Сокращение	Расшифровка
Администратор	Пользователь ОС, уполномоченный выполнять некоторые действия по администрированию ОС (имеющий административные полномочия) в соответствии с установленной ролью и требуемыми привилегиями в ОС на выполнение этих действий
АПМДЗ	Аппаратно-программный модуль доверенной загрузки
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
БД	База данных
БДУ	База данных уязвимостей
ИБ	Информационная безопасность
ИС	Информационная система
ИФБО	Интерфейс к функции безопасности
КЦ	Контроль целостности
Непривилегированный субъект доступа	Процесс, порождаемый пользователем
Неуполномоченный субъект доступа	Процесс, порождаемый лицами, не являющимися пользователями ОС, при попытке несанкционированного доступа
Объект доступа	Единица информационного ресурса (файл, каталог, том, устройство и (или) иные), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции
ОЗУ	Оперативное запоминающее устройство (энергозависимая память)
ОС	Операционная система. ПС (комплекс программ), реализующее (реализующий) функции защиты от

Термин/Сокращение	Расшифровка
	несанкционированного доступа к информации, обрабатываемой на СВТ, находящихся под управлением данного ПС (комплекса программ)
ПЗ	Профиль защиты
ПК	Персональный компьютер
ПО	Программное обеспечение
ПС	Программное средство
Пользователь	Пользователь ОС, не имеющий административных полномочий
Пользователь ОС	Лицо (администратор, пользователь), которому разрешено выполнять некоторые действия (операции) по администрированию ОС или обработке информации в ОС
Привилегированный субъект доступа	Процесс, порождаемый администратором или от имени служебной учетной записи ОС
Роль	Предопределенная совокупность правил, устанавливающих допустимое взаимодействие с ОС
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
СУБД	Система управления базами данных
Субъект доступа	Процесс, порождаемый пользователем ОС (пользователем или администратором)
ТК	Технический комитет
УБИ	Угроза безопасности информации
Уполномоченный непривилегированный субъект доступа	Процесс, порождаемый пользователем в соответствии с правами доступа к объекту доступа
Уполномоченный привилегированный субъект доступа	Процесс, порождаемый администратором или от имени служебной учетной записи в соответствии с ролью
ФБО	Функция безопасности
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ФС	Файловая система
ФТБ	Функциональное требование безопасности
AMD	Advanced Micro Devices — компания (США), производитель

Термин/Сокращение	Расшифровка
	микроэлектроники
ACL	Access Control List — список контроля доступа
ASLR	Address Space Layout Randomization — механизм предоставления случайной адресации при выделении страниц виртуальной памяти
BIOS	Basic Input-Output System — базовая система ввода-вывода
CIS	Center for Internet Security — некоммерческая международная организация, разрабатывающая стандарты и инструменты в области ИБ
CUPS	Common UNIX Print System — служба печати для UNIX/Linux
DAC	Discretional Access Control — механизм дискреционного разграничения доступа
DNS	Domain Name System — система (служба) доменных имен
DHCP	Dynamic Host Configuration Protocol — протокол динамической настройки
FIPS	Federal Information Processing Standard — Федеральный стандарт обработки информации (американский и международный стандарт в области защиты информации и криптографии)
GRUB	GRand Unified Bootloader — современный загрузчик ОС Linux
HIDS	Host-Based Intrusion Detection System — система обнаружения вторжений
IP	Internet Protocol — основной протокол передачи данных в сетях Internet
ISO	International Standard Organisation – Международная организация по стандартам
LDAP	Lightweight Directory Access Protocol — сервис (служба), предоставляющий возможность использования службы каталогов
Linux	Акроним от Linux Is Not UniX — Linux это не UNIX. Несовершенная реализация системы UNIX, выполненная финским студентом Л. Торвальдсом в полемическом задоре (при споре со своим преподавателем Э. Танненбаумом).

Термин/Сокращение	Расшифровка
LLMNR	Link-local Multicast Name Resolution — протокол разрешения имен, предложенный компанией Microsoft
MAC	Mandatory Access Control — механизм полномочного разграничения доступа
mDNS	Multicast-DNS — протокол разрешения имен, предложенный компанией Apple
NFS	Network File System — сервис (служба), предоставляющий возможность использования сетевых ресурсов
NIS	Network Information Service — клиент-серверный протокол, созданный Sun Microsystems, который позволяет обеспечивать доступ к системной конфигурации по всей сети
NIST	National Institute of Standard and Technology — Национальный институт стандартов и технологии (регулирующая организация, США)
NTP	Network Time Protocol — протокол службы единого времени
NX	No eXecute bit — бит отключения выполнения кода процессоров AMD x86
PCI DSS	Payment Card Industry Data Security Standart — современный международный стандарт безопасности для ИС финансового сектора
PID	Process IDentificator — идентификатор процесса
RBAC	Role-Based Access Control — механизм ролевого разграничения доступа
RPC	Remote Procedure Call — удаленный вызов процедур
SGID	Superuser Group IDentificator — бит смены идентификатора группы суперпользователя
SUID	SuperUser IDentificator – бит смены идентификатора суперпользователя
SMT	Symmetric Multi-Thread — симметричная многопоточность (технология распределения ресурсов для обработки данных в современных процессорах)
TCP	Transmission Control Protocol — протокол передачи данных с контролем передачи

Термин/Сокращение	Расшифровка
UDP	User Datagramm Protocol — протокол передачи данных без контроля передачи
UEFI	Unified Extensible Firmware Interface — единый расширяемый интерфейс базовой системы ввода-вывода
UID	User IDentificator — идентификатор пользователя
UNIX	Бывшая UNICS — UNIplexed Information and Computing System — несложная информационно-вычислительная система
XD	EXecute Disable bit — бит отключения выполнения кода процессоров Intel x86

ПРИЛОЖЕНИЕ 1. «ДОСТУПНОСТЬ ИНТЕРФЕЙСОВ ДЛЯ РОЛЕЙ»

Графические интерфейсы к функциям безопасности.

Таблица 68

Интерфейс (команда)	Пользователь		Администратор		
	user_r	auditadm_r	sysadm_r	secadm_r	auditadm_r
“Администрирование Selinux” **system-config-selinux**	-	-	-	+	-
“Аудит” **rosa-central-panel-logviewer**	-	+	-	-	+
“Аутентификация” **drakauth**	-	-	+	+	+
“Диагностика Selinux” **sealert**	-	-	-	-	+
Диспетчер файлов Dolphin **dolphin**	+	+	+	+	+
Менеджер входа KDM **kdm**	-	-	+	+	+
Настройка блокировщика экрана **kcmshell4 screensaver**	-	-	+	+	+
Настройка времени **kcmshell4 clock**	-	-	+	+	+
Настройка входа в систему **kcmshell4 kdm**	-	-	+	+	+
“Настройка маркировки печати” **adminprintgui**	-	-	-	+	-
“Настройка загрузчика grub2” (*) **kcmshell4 kcm_grub2**	-	-	-	-	-
“Настройка оборудования” **harddrake2**	-	-	+	+	+
РОСА шредер **rosa-shred**	+	+	+	+	+
“Системный монитор” **ksysguard**	+**	+**	+	+	+
“Управление пользователями” **userdrake**	-	-	+	+	-
“Учет и контроль съемных носителей” **rosa-removable-drive-manager**	-	-	+	+	-

(*) - доступ к изменению настроек загрузчика имеет только технический пользователь, сопоставленный с selinux-пользователем root, по-умолчанию вход под ним выключен.

(**) Возможно удаление только своих процессов, для удаления системных процессов нужна аутентификация в учетную запись администратора

Таблица 69— текстовые интерфейсы (конфигурационные файлы) к функциям безопасности, доступ на чтение, на запись (++)
По-умолчанию параметры в текстовых интерфейсах приведены к безопасному виду, если специально не оговорено обратное.

Интерфейс (файл настройки)	Пользователь		Администратор		
	user_r	auditadm_r	sysadm_r	secadm_r	auditadm_r
/etc/fstab	**+-**	**+-**	**++**	**++**	**++**
/etc/passwd	**+-**	**+-**	**++**	**++**	**+-**
/etc/shadow /etc/shadow-	**--**	**--**	**++**	**++**	**+-**
/etc/gshadow /etc/gshadow-	**--**	**--**	**++**	**++**	**+-**
/etc/group /etc/group-	**+-**	**+-**	**++**	**++**	**+-**
/etc/security/*	**+-**	**+-**	**++**	**++**	**++**
/etc/login.defs	**+-**	**+-**	**++**	**++**	**++**
/etc/audit/*	**--**	**--**	**+-**	**++**	**++**
/etc/audisp/*	**--**	**--**	**+-**	**++**	**++**
/etc/rosa-audisp-sender.conf	**+-**	**+-**	**++**	**++**	**++**
/etc/rosa-central-panel-serverd.conf	**+-**	**+-**	**++**	**++**	**++**
/etc/rosa-central-panel-logviewer.conf	**--**	**--**	**++**	**++**	**++**
/etc/rosa-central-panel-ui.conf	**+-**	**+-**	**++**	**++**	**++**
/etc/rosa-printmarkerd/main.conf	**+-**	**+-**	**++**	**++**	**++**
/etc/syslog.conf	**+-**	**--**	**++**	**++**	**--**
/etc/rsyslog.conf	**+-**	**--**	**++**	**++**	**--**
/etc/rsyslog.d/*	**+-**	**--**	**++**	**++**	**--**
/etc/cron.*/*	**+-**	**+-**	**++**	**++**	**+-**
/etc/crontab	**--**	**--**	**++**	**++**	**--**
/etc/cron.deny	**+-**	**+-**	**++**	**++**	**++**
/etc/chrony.conf	**+-**	**+-**	**++**	**++**	**++**
/etc/hosts	**+-**	**+-**	**++**	**++**	**+-**
/etc/hosts.*	**+-**	**+-**	**++**	**++**	**+-**
/etc/resolv.conf	**+-**	**+-**	**++**	**++**	**+-**
/etc/hostname	**+-**	**+-**	**++**	**++**	**+-**
/etc/networks	**+-**	**+-**	**++**	**++**	**++**
/etc/ssh/sshd_config	**--**	**--**	**++**	**++**	**++**
/etc/ssh/sshd_config.d/*	**--**	**--**	**++**	**++**	**++**
/etc/ntp.conf	**+-**	**+-**	**++**	**++**	**+-**
/etc/authselect/nsswitch.conf	**+-**	**+-**	**++**	**++**	**++**

Интерфейс (файл настройки)	Пользователь		Администратор		
	user_r	auditadm_r	sysadm_r	secadm_r	auditadm_r
/etc/sysctl.conf	**+-**	**+-**	**++**	**++**	**++**
/etc/sysctl.d/*	**+-**	**+-**	**++**	**++**	**++**
/etc/sudo.conf	**+-**	**+-**	**++**	**++**	**++**
/etc/sudoers	**--**	**--**	**++**	**++**	**++**
/etc/sudoers.*	**--**	**--**	**++**	**++**	**++**
/etc/systemd/*.conf	**+-**	**+-**	**++**	**++**	**++**
/etc/pam.d/*	**+-**	**+-**	**++**	**++**	**++**
/etc/pam_script	**+-**	**+-**	**++**	**++**	**++**
/etc/pam-script.d/*	**+-**	**+-**	**++**	**++**	**++**
/etc/selinux/config	**+-**	**+-**	**+-**	**+-**	**+-**
/etc/selinux/semanage.conf	**+-**	**+-**	**+-**	**++**	**+-**
/etc/selinux/mls/*	**+-**	**+-**	**+-**	**++**	**+-**
/etc/motd /etc/motd/*	**+-**	**+-**	**++**	**++**	**++**
/etc/motd-ssh /etc/motd.sconfigs	**+-**	**+-**	**++**	**++**	**++**
/etc/grub.d/*	**--**	**--**	**+-**	**+-**	**+-**
/etc/default/grub	**+-**	**+-**	**+-**	**+-**	**+-**
/etc/modprobe.d/*.conf	**+-**	**--**	**++**	**++**	**--**
/etc/modprobe.preload	**+-**	**+-**	**++**	**++**	**++**
/etc/tmux.conf	**+-**	**+-**	**++**	**++**	**++**
/etc/profile	**+-**	**+-**	**++**	**++**	**++**
/etc/profile.d/*	**+-**	**+-**	**++**	**++**	**+-**
/etc/bashrc	**+-**	**+-**	**++**	**++**	**++**
/etc/yum.repos.d/*	**+-**	**+-**	**++**	**++**	**+-**
/etc/cups/cupsd.conf	**+-**	**--**	**++**	**++**	**--**
/etc/cups/cups-files.conf	**+-**	**+-**	**++**	**++**	**--**
/etc/sysconfig/iptables	**--**	**--**	**++**	**++**	**+-**
/etc/sysconfig/iptables-config	**--**	**--**	**++**	**++**	**+-**
~/.kde4/share/config/kscreensaverrc	**--**	**--**	**++**	**++**	**--**
~/.kde4/share/config/powermanagementprofilesrc	**--**	**--**	**++**	**++**	**--**
~/.kde4/share/config/powerdevilrc	**--**	**--**	**++**	**++**	**--**

Таблица 70— командные интерфейсы к функциям безопасности.

«+» означает возможность запустить программу путем указания полного пути к файлу и выполнить с ее помощью полезные функции, соответствующие ее задокументированному назначению. «-» означает невозможность запустить или возможность запустить без возможности выполнить таковые полезные функции.

Для user_r командные интерфейсы ограничены отсутствием доступа к консольному интерфейсу. Для пользователя интерфейсы ограничены работой с его файлами и процессами. Документация по командам доступна следующим образом: man <команда>.

Оранжевым цветом веделены строки с командами, имеющими «+» не во всех случаях.

Интерфейс (команда запуска)	Путь к исполняемому файлу, запускаемому командой	Пользователь		Администратор		
		user_r	auditadm_r	sysadm_r	secadm_r	auditadm_r
adduser	**/usr/sbin/adduser**	**-**	**-**	**+**	**+**	**-**
aide	**/usr/sbin/aide**	**-**	**-**	**+**	**+**	**+**
auditctl	**/sbin/auditctl**	**-**	**-**	**+**	**+**	**+**
aureport	**/sbin/aureport**	**-**	**-**	**-**	**+**	**+**
ausearch	**/sbin/ausearch**	**-**	**-**	**-**	**+**	**+**
capsh	**/usr/sbin/capsh**	**-**	**-**	**+**	**+**	**+**
cd	встроенная в командную оболочку команда	**-**	**+**	**+**	**+**	**+**
chattr	**/usr/bin/chattr**	**-**	**+**	**+**	**+**	**+**
chgrp	**/bin/chgrp**	**-**	**+**	**+**	**+**	**+**
chmod	**/bin/chmod**	**-**	**+**	**+**	**+**	**+**
chown	**/bin/chown**	**-**	**+**	**+**	**+**	**+**
chpasswd	**/usr/sbin/chpasswd**	**-**	**-**	**+**	**+**	**-**
cp	**/bin/cp**	**-**	**+**	**+**	**+**	**+**
dd	**/bin/dd**	**-**	**+**	**+**	**+**	**+**
dmesg	**/bin/dmesg**	**-**	**-**	**+**	**+**	**+**
dnf	**/usr/bin/dnf**	**-**	**-**	**+**	**+**	**-**
evmctl	**/usr/bin/evmctl**	**-**	**+**	**+**	**+**	**+**
fsck	**/sbin/fsck**	**-**	**+**	**+**	**+**	**+**
getcap	**/usr/sbin/getcap**	**-**	**-**	**+**	**+**	**+**
getfacl	**/usr/bin/getfacl**	**-**	**+**	**+**	**+**	**+**
groupadd	**/usr/sbin/groupadd**	**-**	**-**	**+**	**+**	**-**
groupdel	**/usr/sbin/groupdel**	**-**	**-**	**+**	**+**	**-**
groupmod	**/usr/sbin/groupmod**	**-**	**-**	**+**	**+**	**-**
htop	**/usr/bin/htop**	**-**	**-**	**+**	**+**	**-**

Интерфейс (команда запуска)	Путь к исполняемому файлу, запускаемому командой	Пользователь		Администратор		
		user_r	auditadm_r	sysadm_r	secadm_r	auditadm_r
id	**/bin/id**	**-**	**+**	**+**	**+**	**+**
ifconfig	**/sbin/ifconfig**	**-**	**+**	**+**	**+**	**+**
ip	**/sbin/ip**	**-**	**+**	**+**	**+**	**+**
iptables	**/usr/sbin/iptables**	**-**	**-**	**+**	**+**	**-**
journalctl	**/bin/journalctl**	**-**	**+**	**+**	**+**	**+**
kill	**/bin/kill**	**-**	**+**	**+**	**+**	**+**
ln	**/bin/ln**	**-**	**+**	**+**	**+**	**+**
lp	**/usr/bin/lp**	**-**	**+**	**+**	**+**	**+**
ls	**/bin/ls**	**-**	**+**	**+**	**+**	**+**
lsmod	**/sbin/lsmod**	**-**	**+**	**+**	**+**	**+**
mknod	**/bin/mknod**	**-**	**+**	**+**	**+**	**+**
modprobe	**/sbin/modprobe**	**-**	**-**	**+**	**-**	**-**
mount	**/bin/mount**	**-**	**+**	**+**	**+**	**+**
mv	**/bin/mv**	**-**	**+**	**+**	**+**	**+**
newrole	**/usr/bin/newrole**	**-**	**-**	**+**	**+**	**-**
passwd	**/usr/bin/passwd**	**-**	**-**	**+**	**+**	**-**
ps	**/bin/ps**	**-**	**-**	**+**	**+**	**-**
rm	**/bin/rm**	**-**	**+**	**+**	**+**	**+**
rmdir	**/bin/rmdir**	**-**	**+**	**+**	**+**	**+**
rmmod	**/sbin/rmmod**	**-**	**-**	**+**	**-**	**-**
rosa-central-panel-ui	**/usr/sbin/rosa-central-panel-ui**	**-**	**-**	**-**	**+**	**+**
route	**/sbin/route**	**-**	**-**	**+**	**+**	**-**
rpm	**/bin/rpm**	**-**	**-**	**+**	**+**	**-**
semanage	**/usr/sbin/semanage**	**-**	**-**	**-**	**+**	**-**
sestatus	**/usr/sbin/sestatus**	**-**	**+**	**+**	**+**	**+**
setcap	**/usr/sbin/setcap**	**-**	**-**	**+**	**+**	**+**
setfacl	**/usr/bin/setfacl**	**-**	**+**	**+**	**+**	**+**
su	**/bin/su**	**-**	**+**	**+**	**+**	**+**
sudo	**/usr/bin/sudo**	**-**	**+**	**+**	**+**	**+**
systemctl	**/bin/systemctl**	**-**	**-**	**+**	**+**	**-**
tar	**/bin/tar**	**-**	**+**	**+**	**+**	**+**
top	**/usr/bin/top**	**-**	**-**	**+**	**+**	**-**
touch	**/bin/touch**	**-**	**+**	**+**	**+**	**+**

Интерфейс (команда запуска)	Путь к исполняемому файлу, запускаемому командой	Пользователь		Администратор		
		user_r	auditadm_r	sysadm_r	secadm_r	auditadm_r
umask	встроенная в командную оболочку команда	**-**	**+**	**+**	**+**	**+**
umount	**/bin/umount**	**-**	**-**	**+**	**+**	**-**
unlink	**/bin/unlink**	**-**	**+**	**+**	**+**	**+**
useradd	**/usr/sbin/useradd**	**-**	**-**	**+**	**+**	**-**
userdel	**/usr/sbin/userdel**	**-**	**-**	**+**	**+**	**-**
usermod	**/usr/sbin/usermod**	**-**	**-**	**+**	**+**	**-**
vlock	**/usr/bin/vlock**	**-**	**+**	**+**	**+**	**+**
wipe	**/usr/bin/wipe**	**-**	**+**	**+**	**+**	**+**

Лист регистрации изменений									
Изм.	*Номера листов (страниц)*				*Всего листов (страниц) в докум.*	*№ документа*	*Входящий № сопрово-дительного докум. и дата*	*Подп.*	*Дата*
	изменен-ных	*заменен-ных*	*новых*	*аннулиро ванных*					