ОПЕРАЦИОННАЯ СИСТЕМА РОСА ХРОМ 12

Руководство по эксплуатации

Версия 1.0

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

1.1. Аннотация документа

Настоящий документ содержит инструкции по эксплуатации программного изделия «Операционная система «РОСА ХРОМ 12».

Документ предназначен для администратора и пользователей ОС и содержит общие сведения об ОС, ее общей структуре, настройке и работе с основными приложениями.

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

```
пример написания команды
```

2. ОБЩИЕ СВЕДЕНИЯ ОБ ОПЕРАЦИОННОЙ СИСТЕМЕ

2.1. Установка и настройка

Установка и настройка ОС должна выполняться в соответствии с документом «РОСА ХРОМ 12. Руководство по установке».

2.2. Выключение системы

Для доступа к параметрам завершения работы системы нажмите на кнопку в нижнем правом углу экрана (Рис. 1), далее выберите одну из опций.

Ждущий режим – энергосберегающий режим работы компьютера без завершения работы.

Спящий режим – позволяет сохранить сохраняет текущее состояние рабочего стола на жестком диске, а затем завершает работу компьютера. Такая опция позволяет возобновить работу с того места, где она была прервана, все открытые приложения и файлы будут восстановлены с предыдущего сеанса.

Перезагрузка – опция производит полное завершение работы системы и затем включает её снова.

Выключить – полное завершение работы компьютера, закрытие всех приложений и файлов без сохранения.

Завершить сеанс – позволяет сменить пользователя системы и заблокировать текущий сеанс.

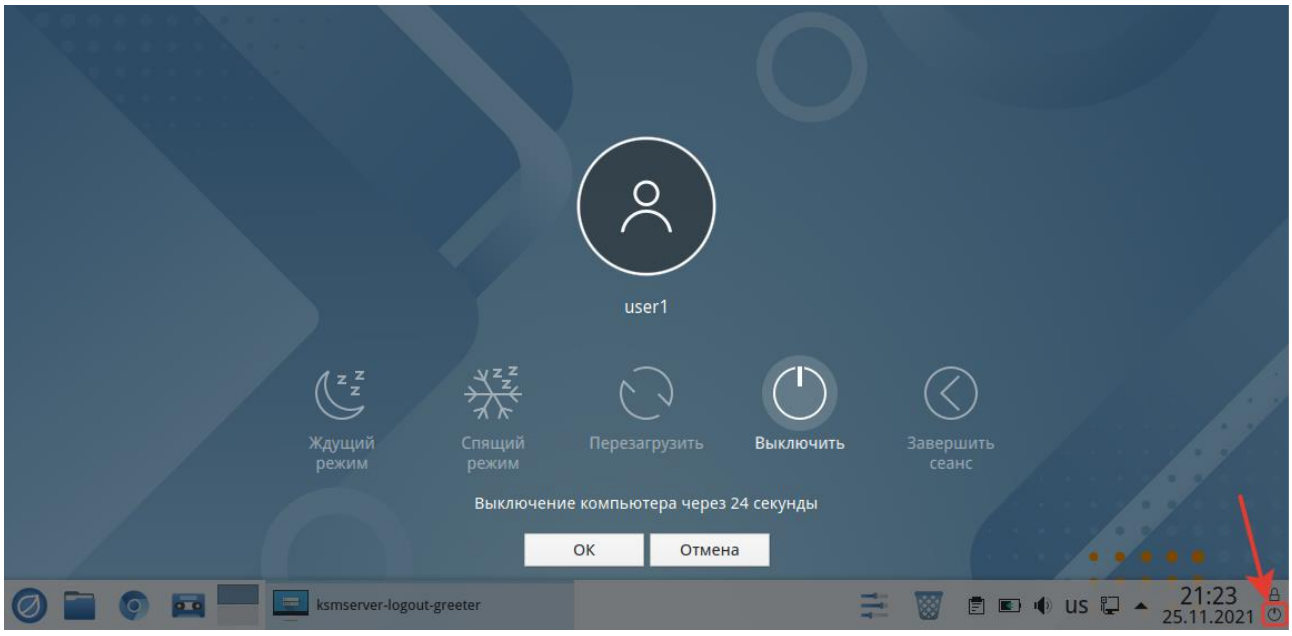

Рис. 1. Параметры завершения работы системы

Блокировка сеанса пользователя осуществляется нажатием на кнопку в нижнем правом углу экрана (Рис. 2). После нажатия на которую система предложит сменить пользователя или ввести пароль и вернуться к предыдущему сеансу.

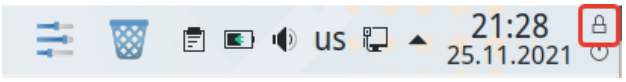

Рис. 2. Кнопка блокирования сеанса пользователя

2.3. Интерфейсы операционной системы

ОС РОСА ХРОМ 12 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 (Рис. **3**).

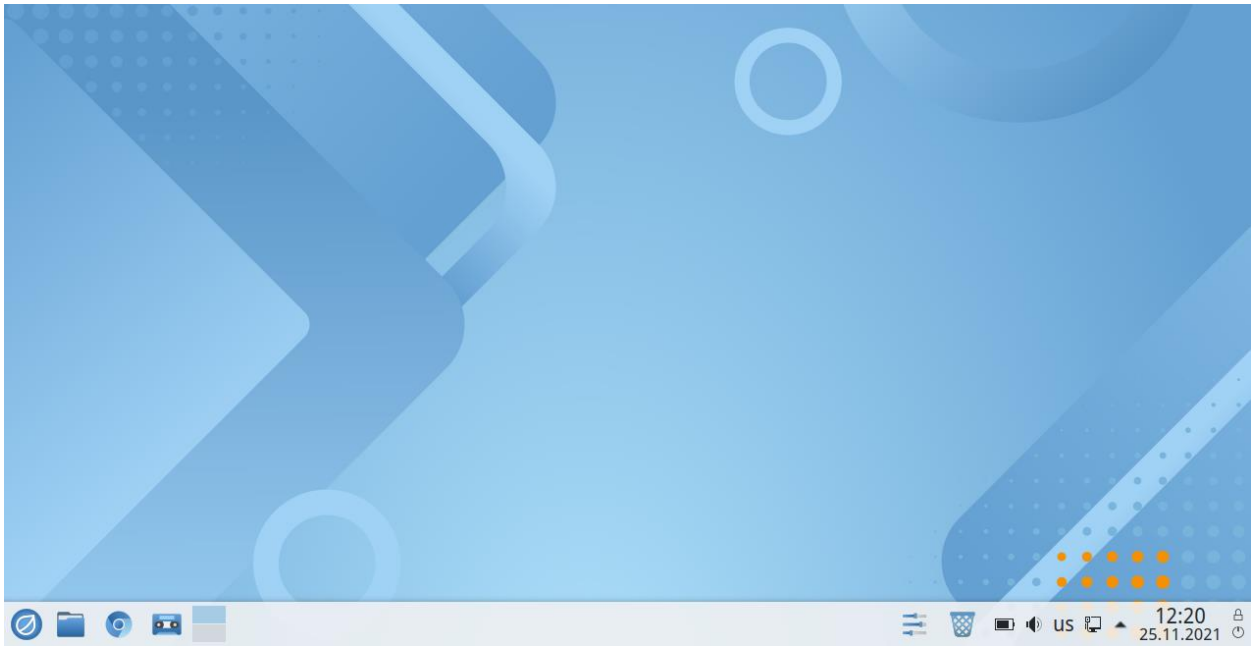

Рис. 3. Интерфейс рабочего стола

Доступ ко всему установленному в системе ПО осуществляется через главное меню запуска приложений. Для доступа в меню нажмите на кнопку в нижнем левом углу экрана, как показано на Рис. 4.

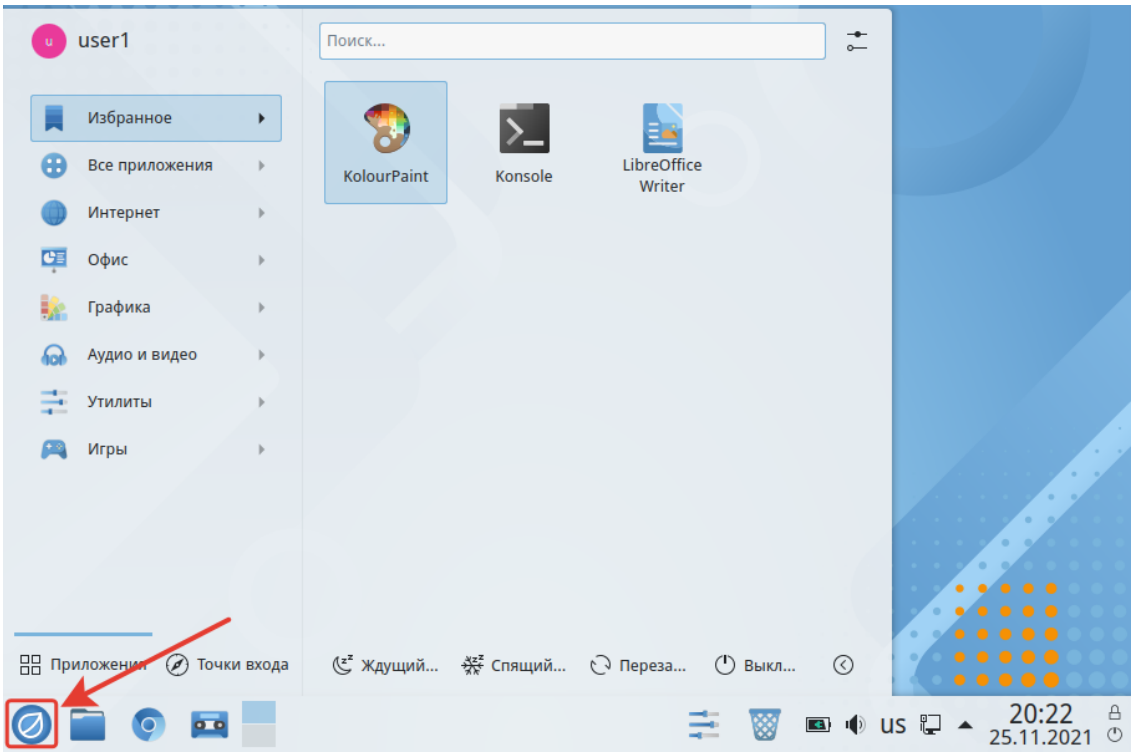

Рис. 4. Меню запуска приложений

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

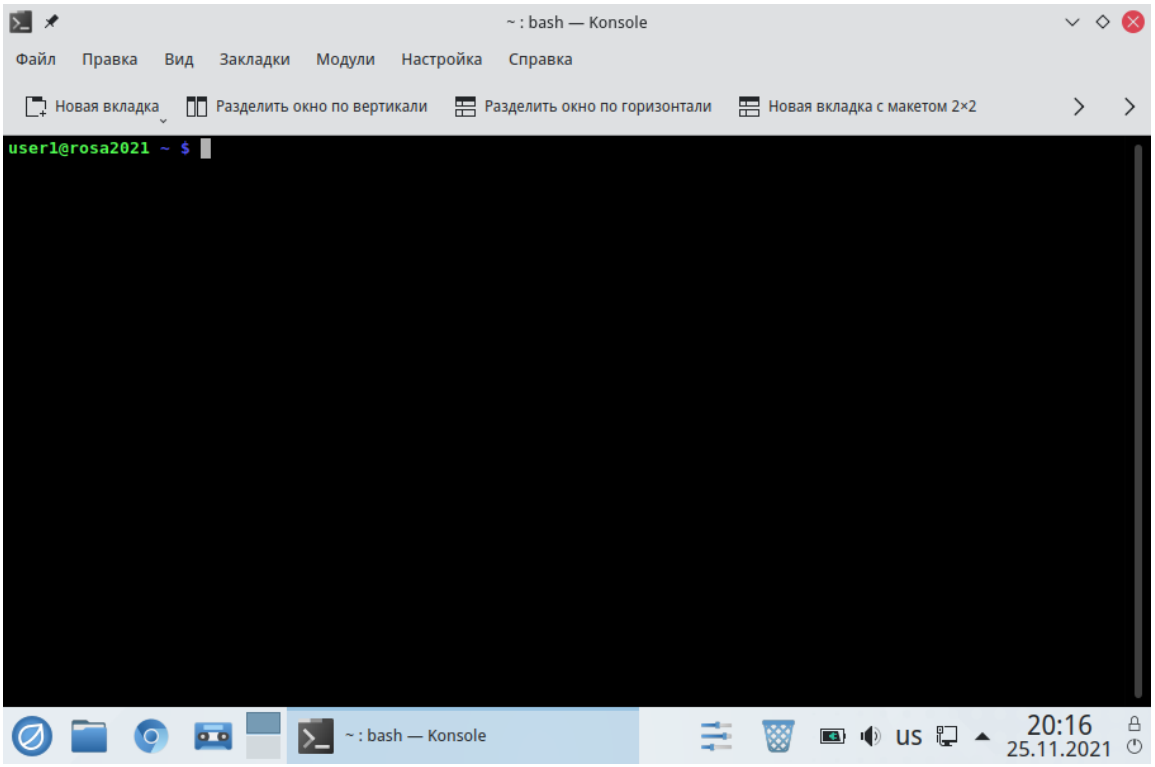

Рис. 5. Консоль

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

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

2.4. Персонализация

Базовые настройки персонализации системы осуществляются в меню [Параметры системы]. Для доступа к меню нажмите на значок в правой части панели задач (Рис. 6).

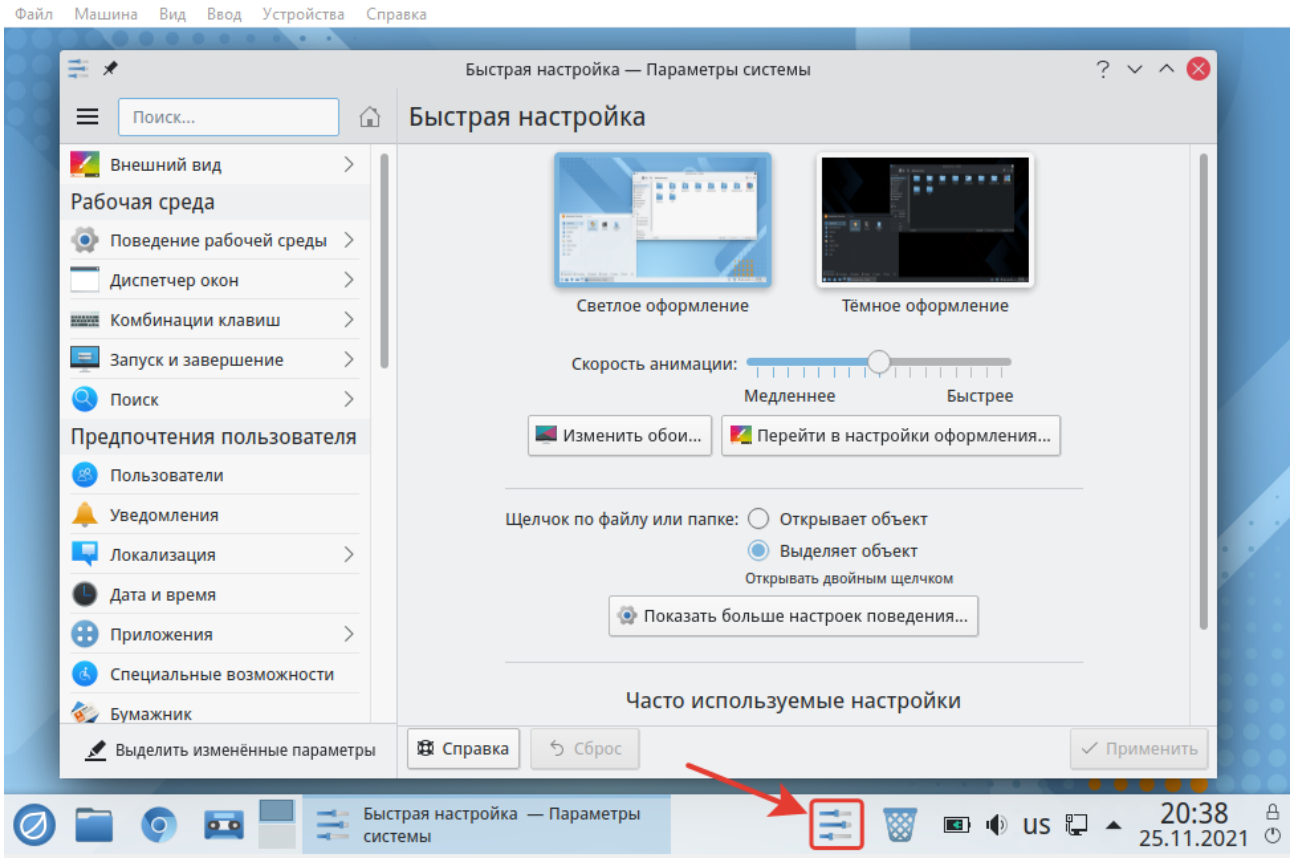

Рис. 6. Параметры настройки системы

В меню доступны настройки внешнего вида и среды рабочего стола, основные параметры внешнего вида и поведения ОС, пользовательские предпочтения, настройки сети и связи, оборудования, а также параметры системного администрирования.

Выберите необходимый раздел в меню слева и произведите настройки параметров справа, для сохранения изменений нажмите на кнопку [Применить] в правом нижнем углу экрана.

Многие из представленных параметров администрирования доступны только пользователям с правами администратора ОС.

2.4.1. Включение и отключение системных служб

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

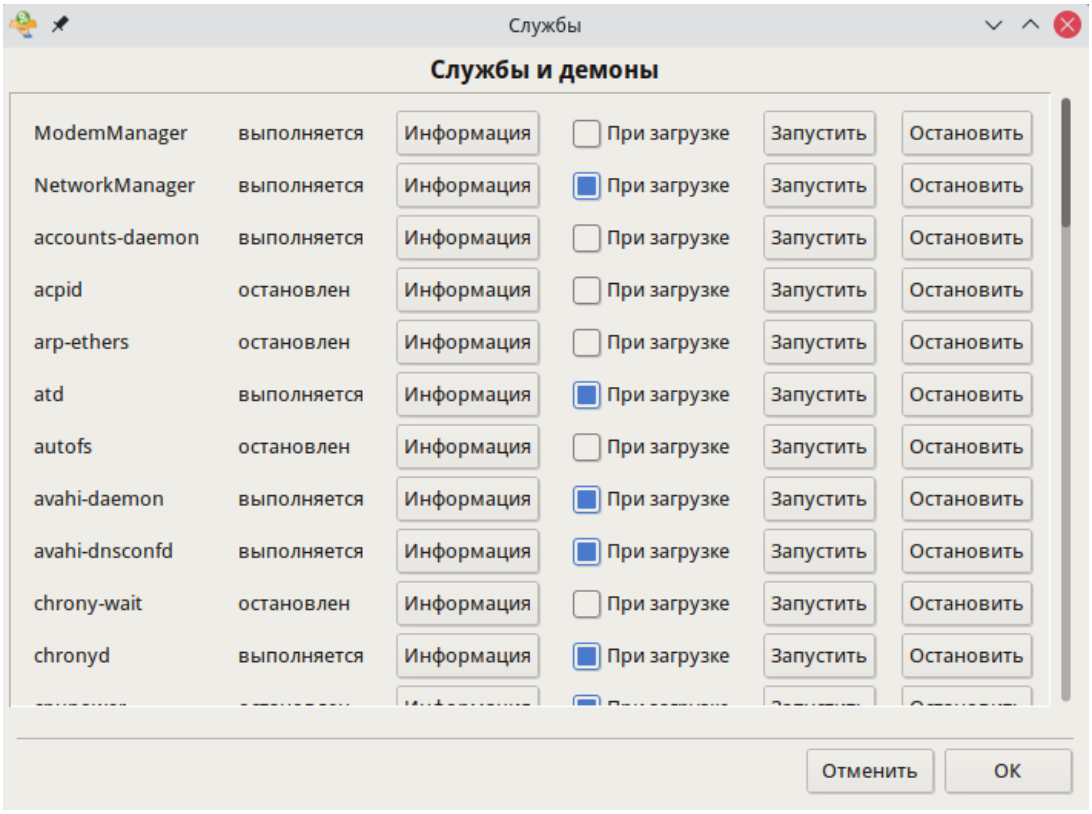

Рис. 7. Управление системными службами

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». Её 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. 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
```

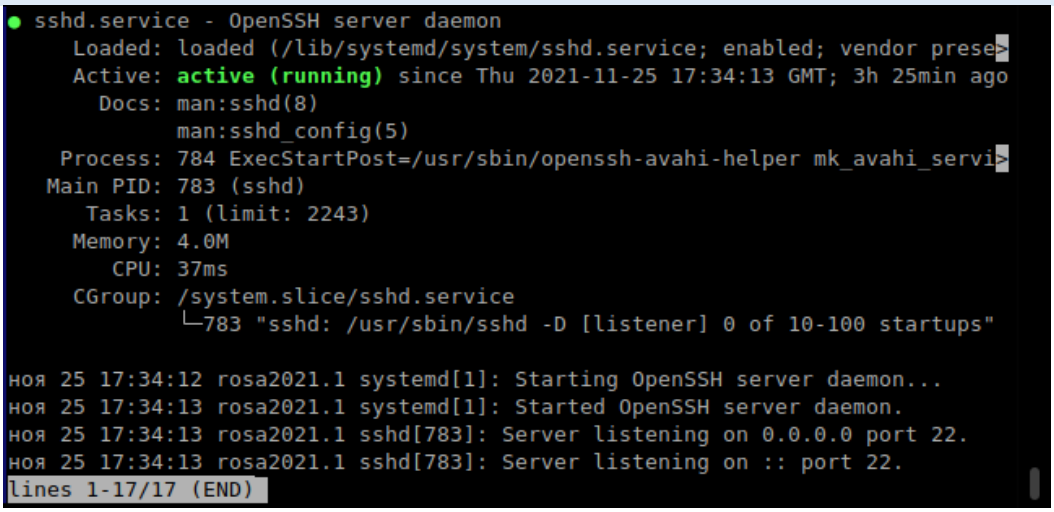

Рис. 8. Проверка статуса работы службы SSHD

2.4.2. 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 определённом размере и начертании.

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

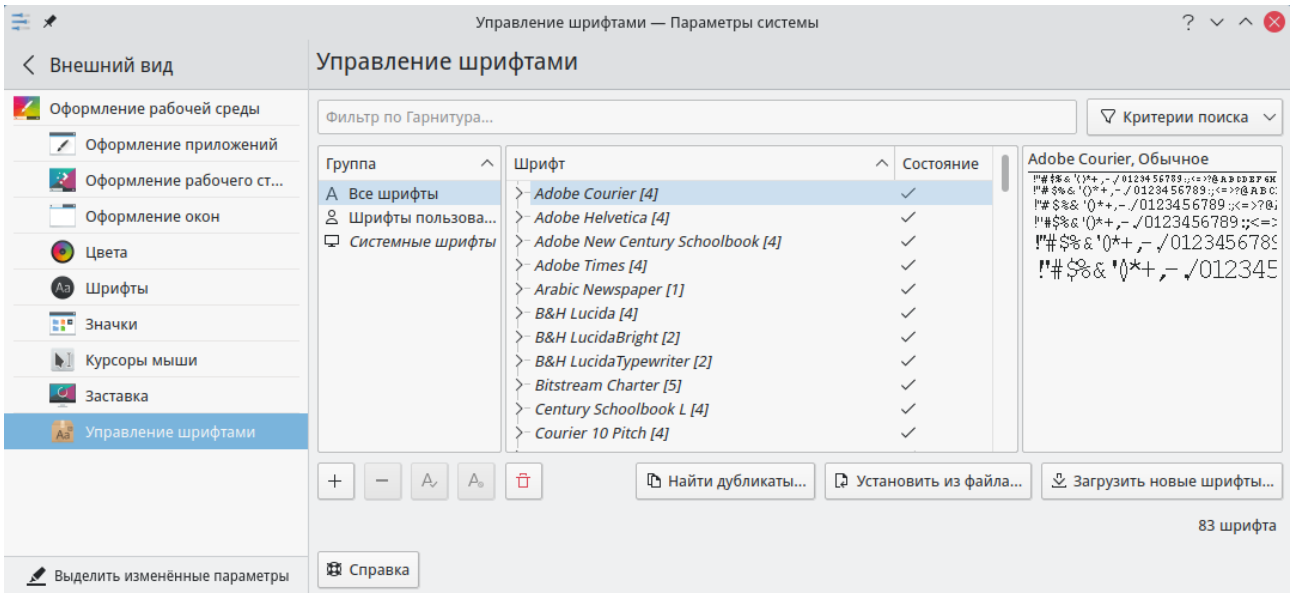

Рис. 9. Меню управления шрифтами

Кнопка [Загрузить новые шрифты] позволяет вручную добавить шрифты, не входящие в ОС РОСА ХРОМ 12. Поддерживаемые форматы шрифтов: TTF, PFA, PFB, PCF, PFM, GSF. При нажатии на кнопку [Установить из файла] 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].

В нём 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»).

2.4.3. Настройка даты и времени

Для настройки системных даты и времени используется программа [Дата и время]. Её можно найти в блоке [Предпочтения пользователя] меню [Параметры системы].

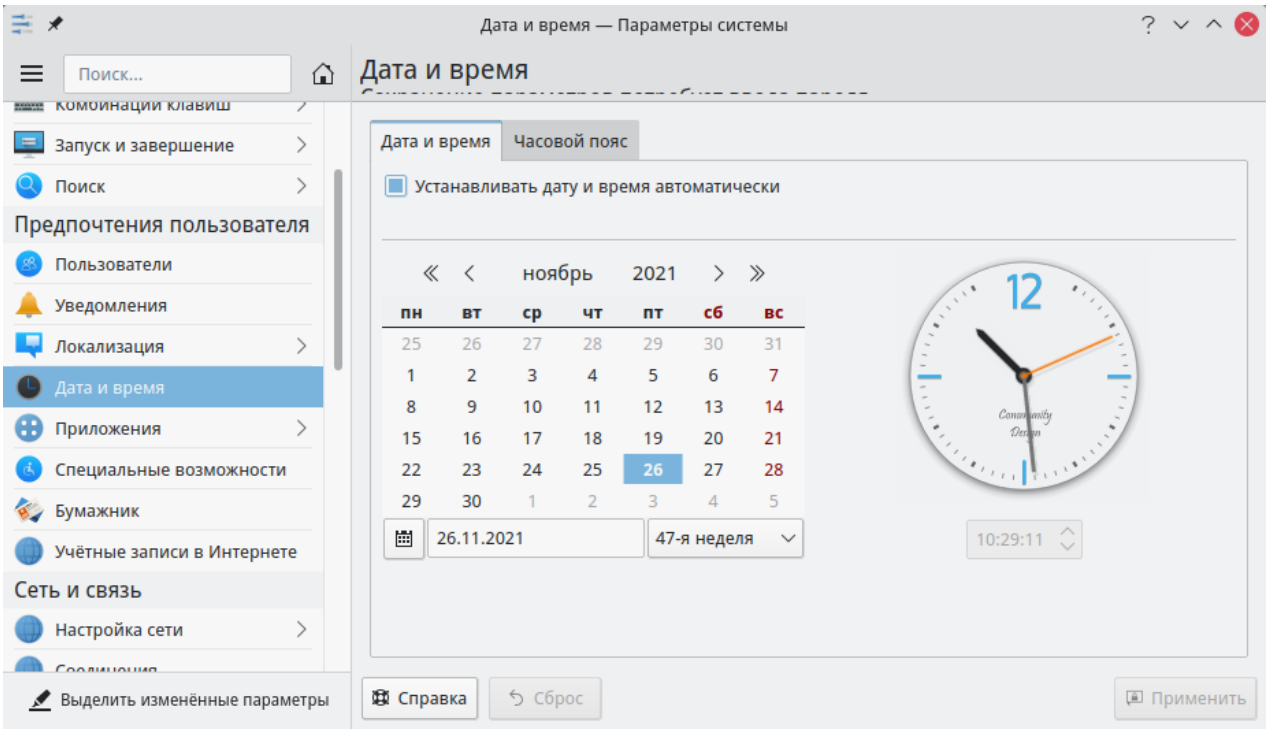

Рис. 10. Настройка даты и времени

Если у вас есть постоянное подключение к интернету, система может синхронизировать часы с серверами точного времени. Для этого установите флажок [Установить дату и время автоматически].

Установка даты и времени пояснений не требует, однако могут возникнуть вопросы насчёт 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 вашем компьютере 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. В Таблица 1 приведены часто используемые опции утилиты timedatectl. Подробное описание приведено в man timedatectl.

Синтаксис:

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

Таблица 1 – Опции утилиты timedatectl

Опция	Описание
status	Вывод текущей даты и времени, параметров времени

Опция	Описание
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

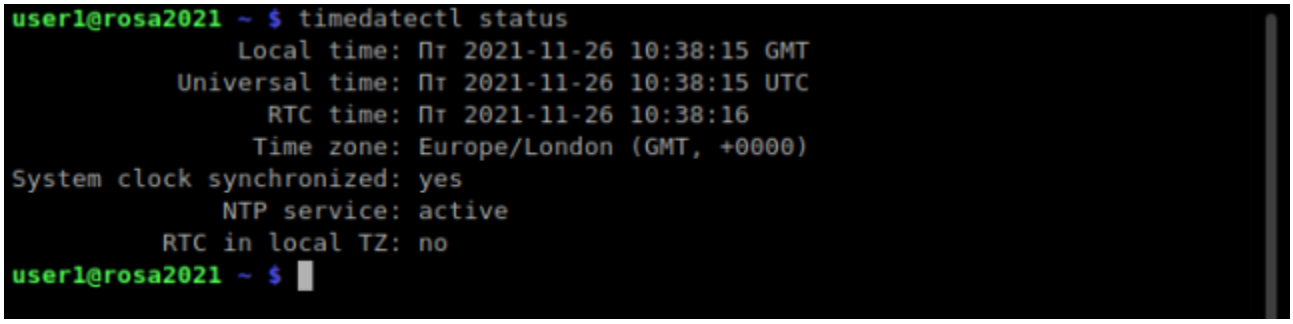

Рис. 11. Вывод команды на проверку статуса параметров времени (timedatectl status)

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.

2.4.4. Рабочий стол KDE

Вид рабочего стола KDE имеет привычный для пользователя интерфейс. На столе можно размещать файлы и каталоги. Нажав на файл левой кнопкой мыши дважды, вы откроете его в ассоциированном приложении.

Ключевыми объектами рабочего стола KDE являются:

- Панель (панель задач), расположена в нижней части рабочего стола, на которой можно размещать кнопки запуска приложений, размещен список открытых окон (программ), часы и системный лоток (трей);
- Рабочий стол — область, где находятся виджеты и ярлыки приложений;

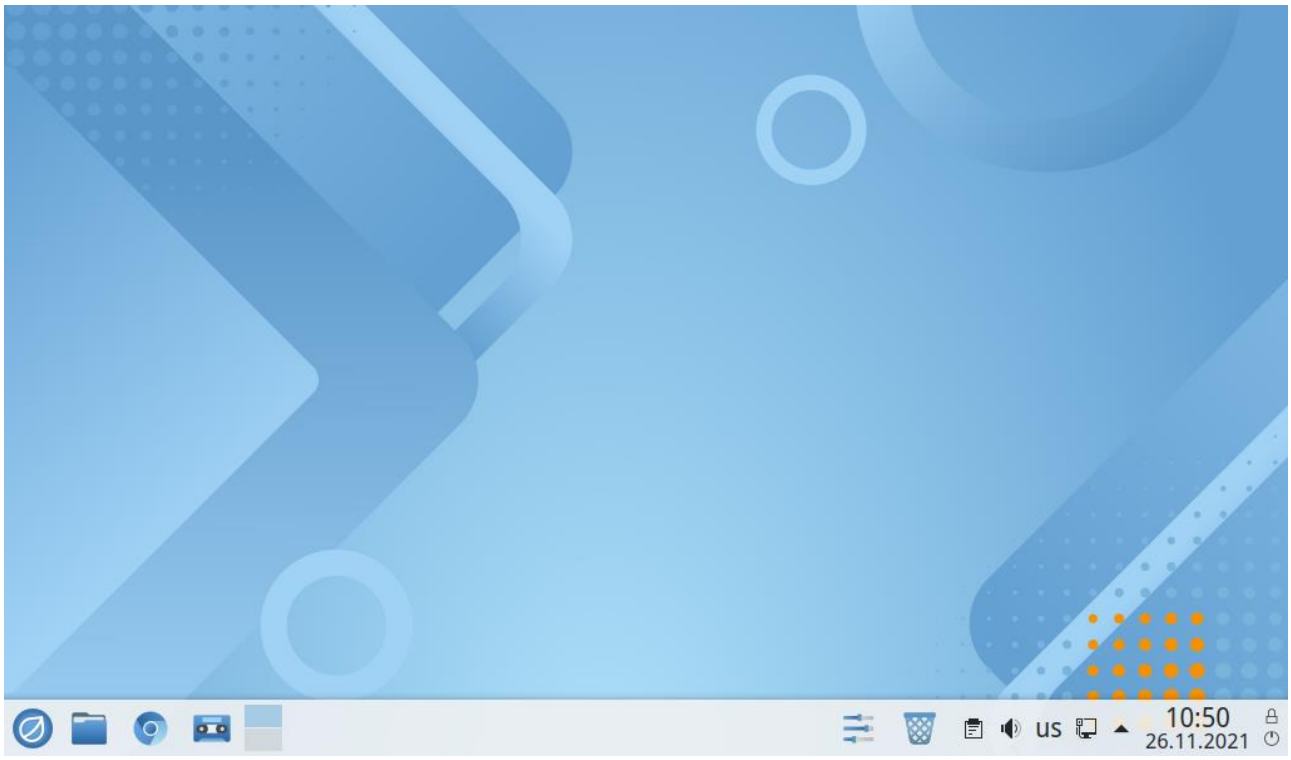

Рис. 12. Интерфейс рабочего стола

Для быстрого просмотра вложенной папки наведите на неё указатель мыши и нажмите на появившийся значок в виде стрелки. Будет открыто небольшое окно для просмотра содержимого вложенной папки (Рис. 13).

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

Рис. 13. Быстрый просмотр содержимого папки

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

Также в ОС РОСА ХРОМ 12 поддерживается функция Поворот экрана. Для реализации данной функции воспользуйтесь следующей командой в консоли:

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

2.4.5. Настройка рабочего стола

В разделе [Внешний вид] программы [Параметры системы] пользователь может настроить различные элементы рабочего стола (Рис. 14). В разделе доступна настройка оформления рабочей среды, приложений, рабочего стола и окон приложений, значков, а также действий, выполняемых с помощью кнопок мыши.

Выбирайте необходимую опцию в меню с левой части экрана и настраивайте желаемые параметры в правой части. Для загрузки дополнительных параметров нажмите на кнопку [Загрузить оформления], после чего откроется окно с выбором и загрузкой из Интернета дополнительных параметров.

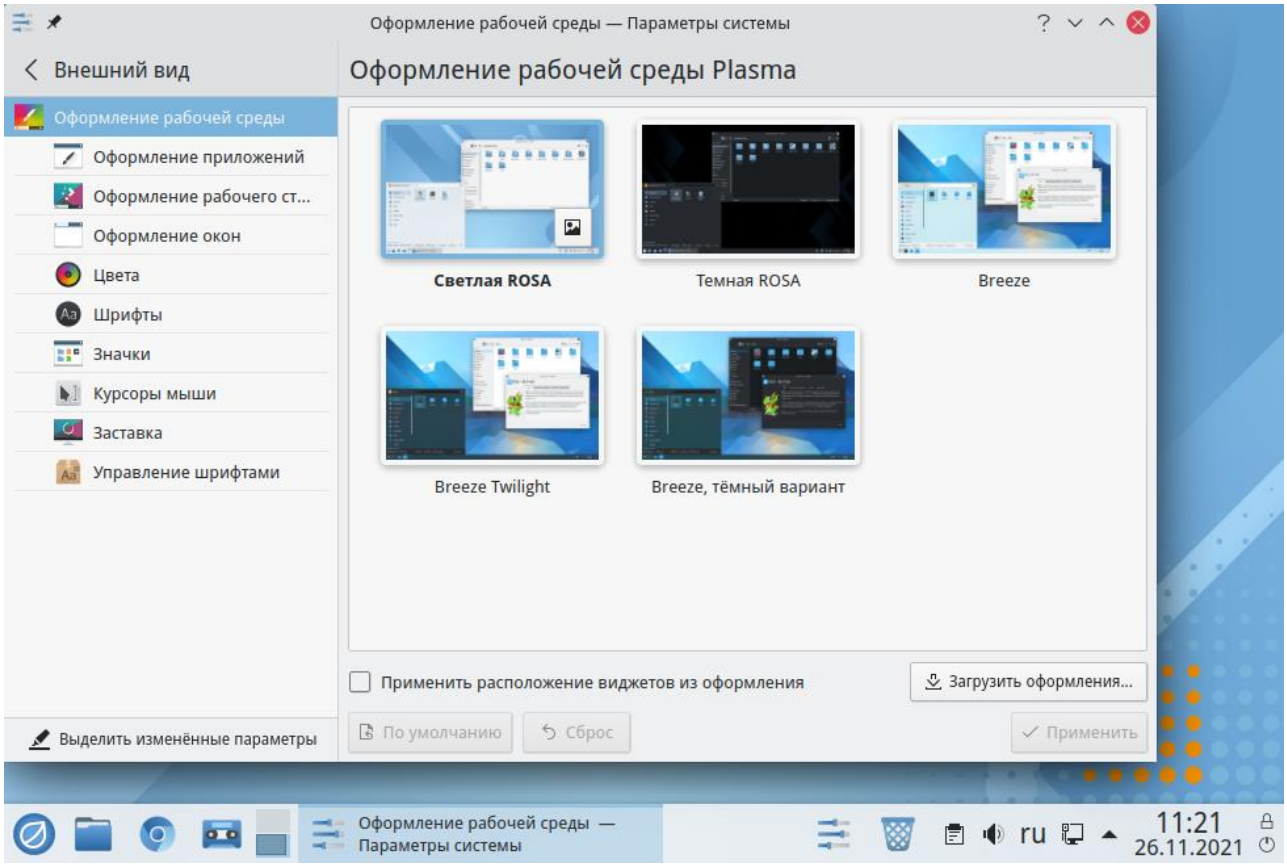

Рис. 14. Настройка параметров рабочего стола

3. РАБОТА С КОМАНДНОЙ СТРОКОЙ

3.1. Графический и текстовый режимы

В ОС РОСА ХРОМ 12 пользователю доступны два режима работы — графический и текстовый (консольный). В текстовом режиме работа осуществляется путём 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 (удалённый доступ по сети, проблемы с поддержкой видеокарты, сбои системы и т. п.). В таких случаях всегда остаётся 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.

3.2. Что такое терминал

Слово «терминал» даже в компьютерном мире имеет множество значений. Изначально так называли рабочее место, состоящее из монитора и клавиатуры, соединённых 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, зайдя в меню

приложений → [Утилиты] → [Konsole] (Рис. 15). Такой терминал будет виртуальным, созданным в рамках графического режима эмулятором терминала, но это не имеет значения — вам будут доступны все возможности консольного режима.

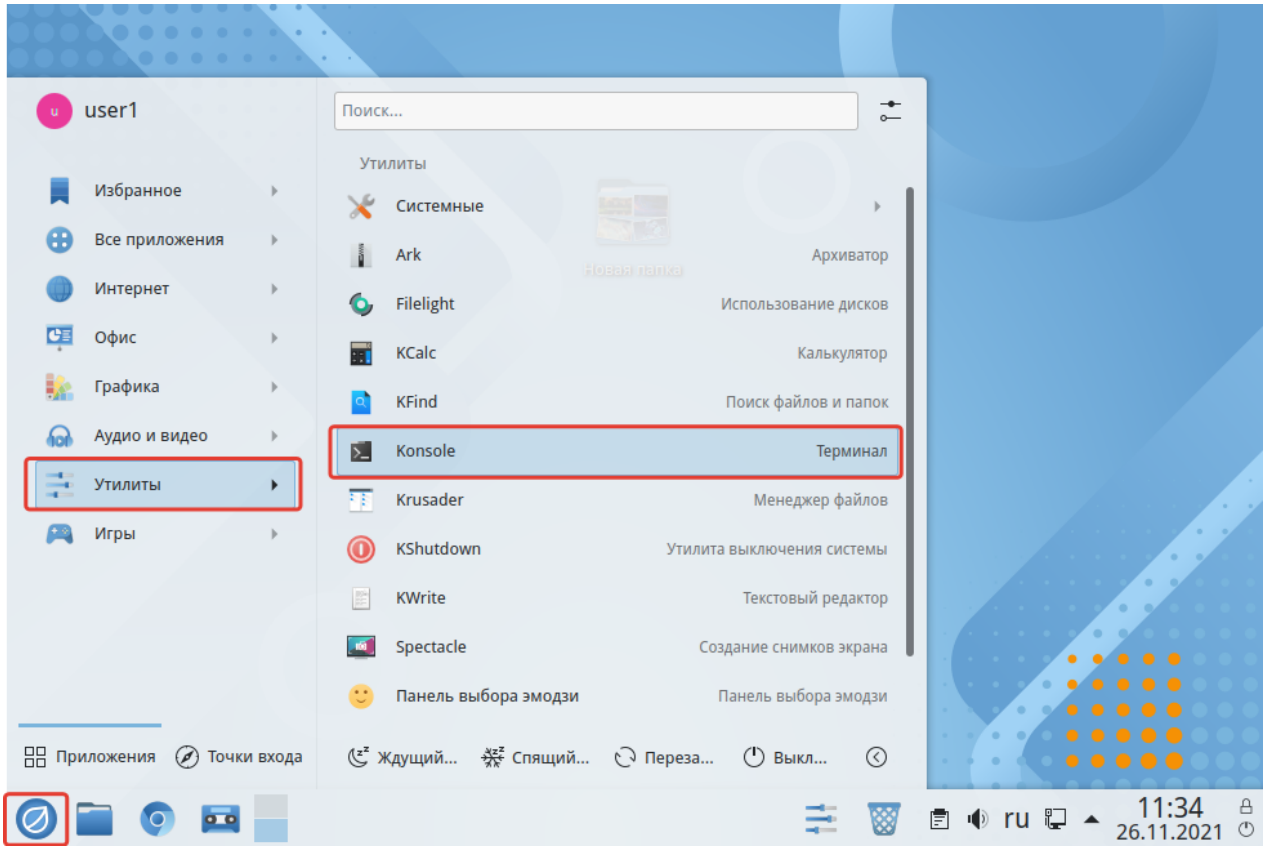

Рис. 15. Доступ к терминалу через панель приложений

Приглашение командной строки

Приглашение представляет собой фрагмент текста в начале строки. По умолчанию он включает имена пользователя и компьютера, 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.

Команда `clear` («очистить») сотрёт 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, щёлкнув 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 надёжнее, чем описывать действия, которые нужно произвести для достижения того же эффекта в графическом интерфейсе.

3.3. 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`.

- `-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.

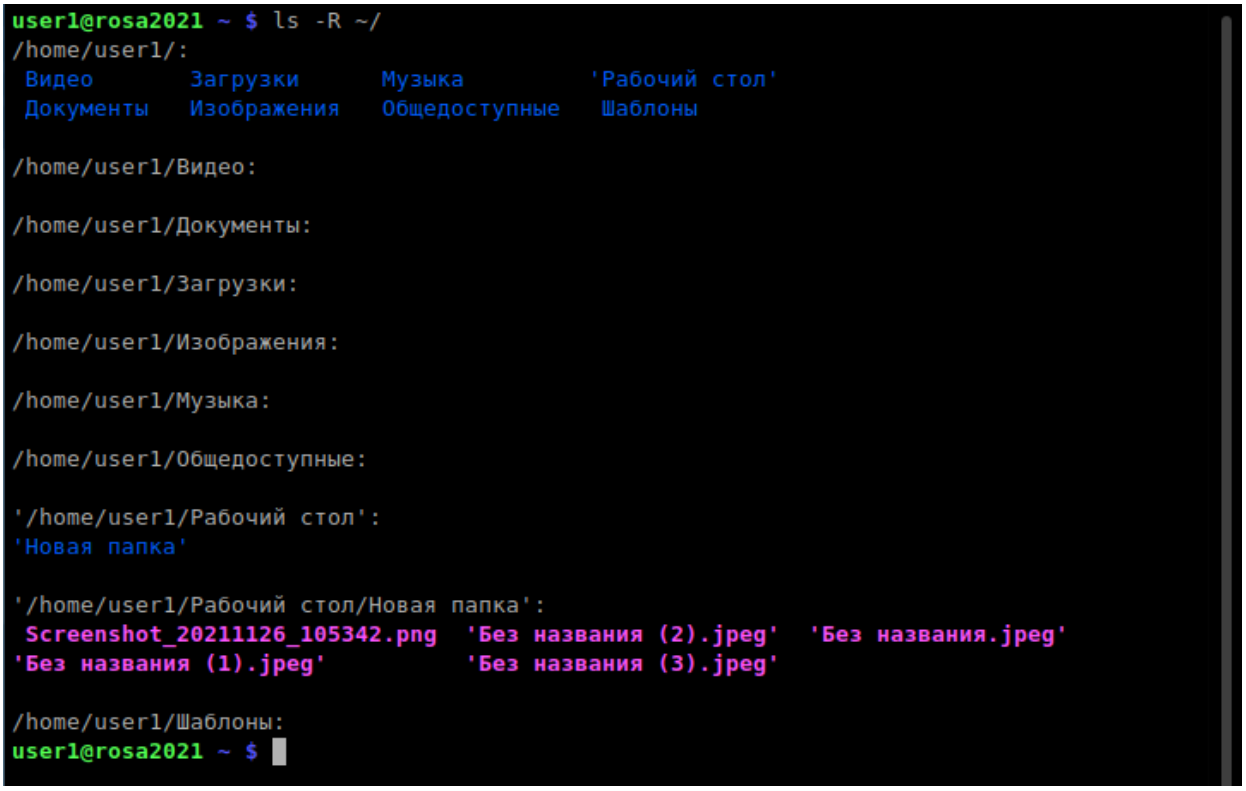

Рис. 16. Пример вывода команды ls -R ~/

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.

Следующими ключами 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 выдаётся.

```
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 создаёт 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 создаёт сразу всю цепочку родительских каталогов (если их ещё нет). Кроме того, ключ убирает сообщение об ошибке при попытке создать уже существующий каталог.

Примеры:

```
mkdir foo
```

Эта команда создаёт каталог `foo` в текущем каталоге.

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

Эта команда создаёт 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 файловой системы, 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 файловой системы.

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.

3.4. 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` выдаёт, согласно указанному критерию, список процессов, которые выполняются в системе в настоящий момент.

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

Рис. 17. Пример вывода команды ps

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 объёму 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».

4. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

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

Для доступа к параметрам аутентификации необходимо обладать правами администратора системы.

4.1. Создание, модификация, удаление учетных записей

4.1.1. Графический режим

Приложение «Управление пользователями» предоставляет возможность создания, модификации, удаления учетных записей пользователей и групп пользователей. Оно имеет интуитивно понятный интерфейс управления (Рис. **18**). Приложение можно запустить, выбрав пункт меню [Параметры системы] → [Управление пользователями].

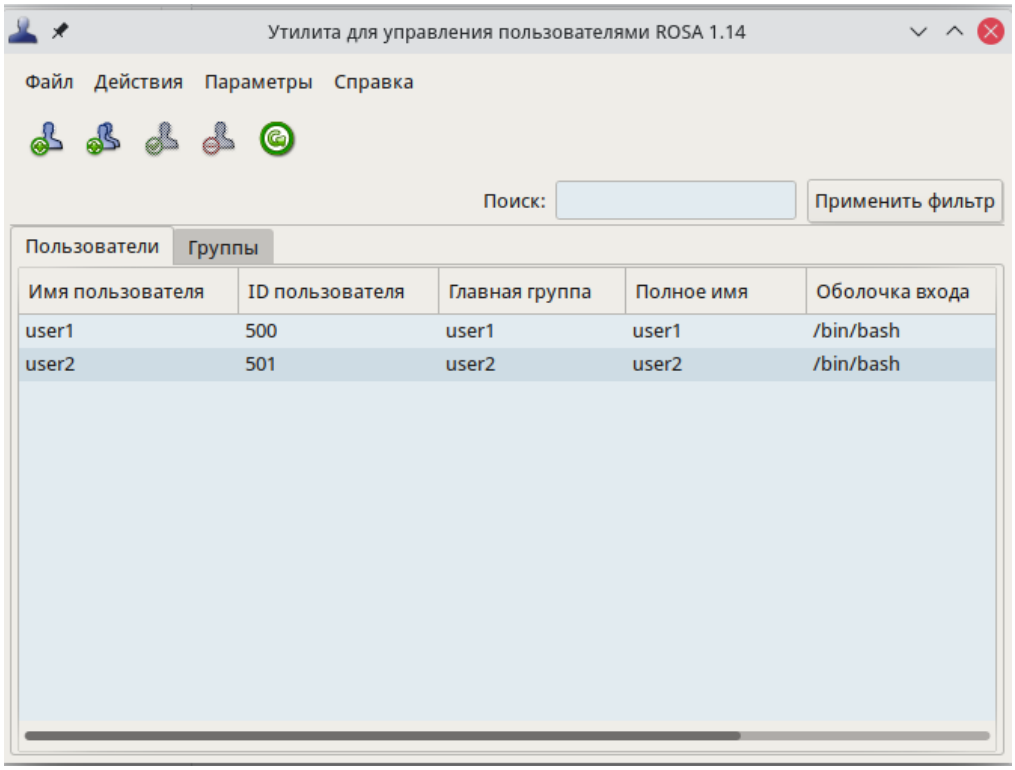

Рис. 18. Утилита Управление пользователями

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 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].

4.1.2. Терминальный режим

Имена учетных записей пользователей и их идентификаторы хранятся в файле /etc/passwd. Каждая запись в файле состоит из полей, описанных в Табл.2.

Таблица 2 – Поля файла /etc/passwd

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. В Таблица 3 3 приведены часто используемые опции утилиты useradd. Подробное описание приведено в man useradd.

Синтаксис:

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

Таблица 3 – Опции утилиты useradd

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. В Таблица 4 приведены часто используемые опции утилиты usermod. Подробное описание приведено в man usermod.

Синтаксис:

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

Таблица 4 – Опции утилиты usermod

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

Опция	Описание
-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 Таблица 5 5 приведены часто используемые опции утилиты userdel. Подробное описание приведено в man userdel.

Синтаксис:

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

Таблица 5 – Опции утилиты userdel

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
```

4.2. Создание, модификация, удаление групповых учетных записей

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 (Рис. 19).

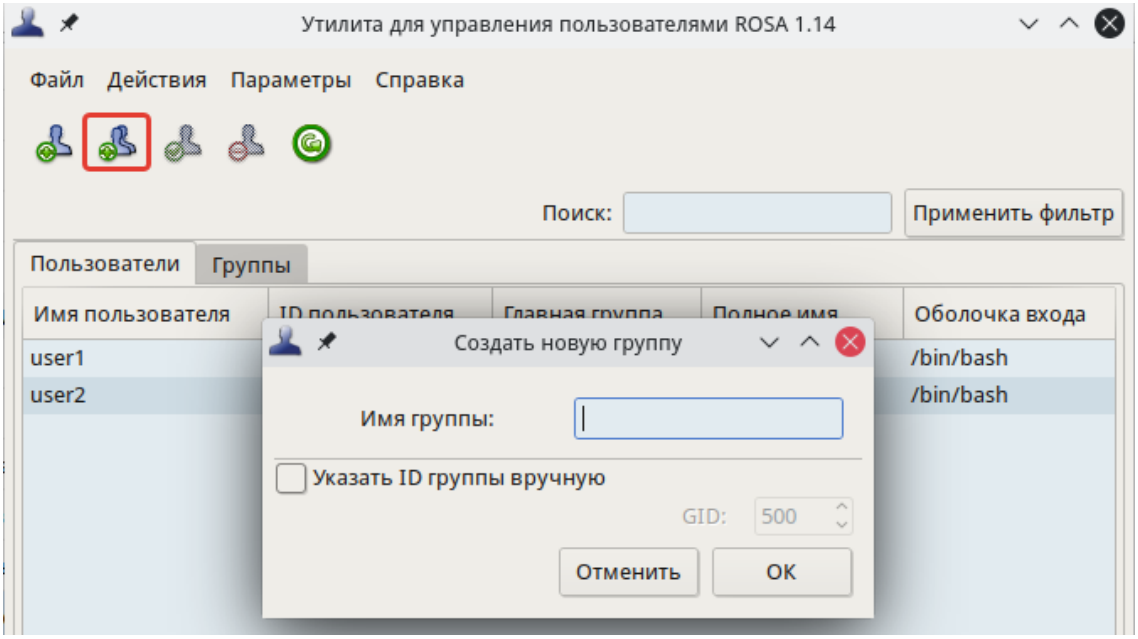

Рис. 19. Создание новой группы

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.

Имена групповых учетных записей (далее – имена групп) и их идентификаторы хранятся в файле /etc/group. Каждая запись в файле состоит из полей, описанных в

Таблица 6 6.

Таблица 6 – Поля файла /etc/group

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. В Таблица приведены часто используемые опции утилиты groupadd. Подробное описание приведено в man groupadd.

Синтаксис:

```
groupadd <опции> <имя группы>
```

Таблица 7 – Опции утилиты groupadd

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. В Таблица 8 приведены часто используемые опции утилиты groupmod. Подробное описание приведено в man groupmod.

Синтаксис:

```
groupmod <опции> <имя группы>
```

Таблица 8 – Опции утилиты groupmod

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>
```

5. НАСТРОЙКА ОБОРУДОВАНИЯ

Настройка аппаратных составляющих компьютера происходит в ОС РОСА ХРОМ 12 централизованно с помощью «Утилиты настройки оборудования», доступной в блоке «Системное администрирование» программы «Параметры системы». Для её запуска требуются права администратора системы.

Выделив устройство, вы увидите подробную информацию о нём 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 утилиты настройки**.** Запускает инструмент настройки, связанный с этим устройством. Например, для звуковой карты используется специальный конфигуратор, позволяющий выбрать драйвер и решить некоторые часто возникающие проблемы.

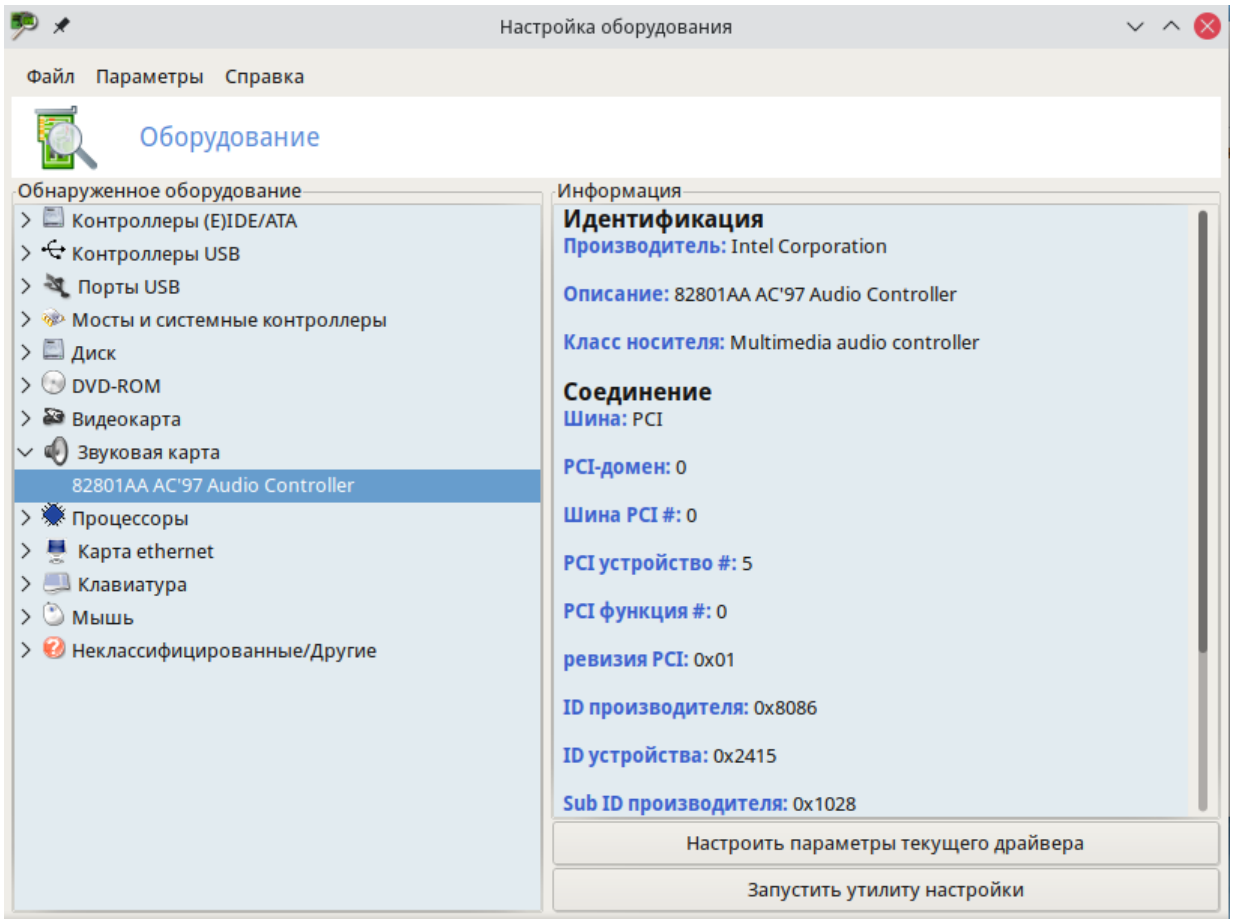

Рис. 20. Утилита настройка оборудования

Неклассифицированное оборудование. Возможно, вы увидите категорию, называющуюся «Неклассифицированные/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».

5.1. Настройка звуковой подсистемы

При возникновении проблем со звуком или при желании пользователя изменить изначальную конфигурацию звуковой подсистемы, созданную автоматически при установке ОС, запустите утилиту настройки оборудования, как это описывалось выше, выделите в списке оборудования слева звуковую карту и нажмите на кнопку «Запустить утилиту настройки» справа внизу. Будет открыто окно Настройка звука.

Смена драйвера

Вы можете переключиться с одного драйвера на другой, выбрав его из выпадающего списка «Драйвер» (Рис. **21**). 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 стрелку «Дополнительно» и затем «Выбрать другой драйвер».

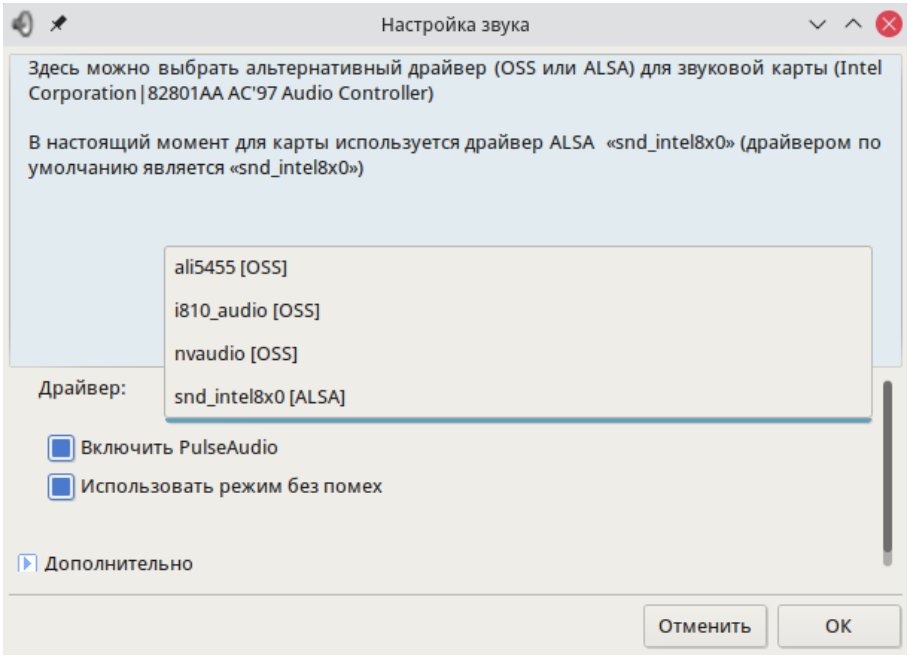

Рис. 21. Настройка звукового оборудования

5.2. Управление графической конфигурацией

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».

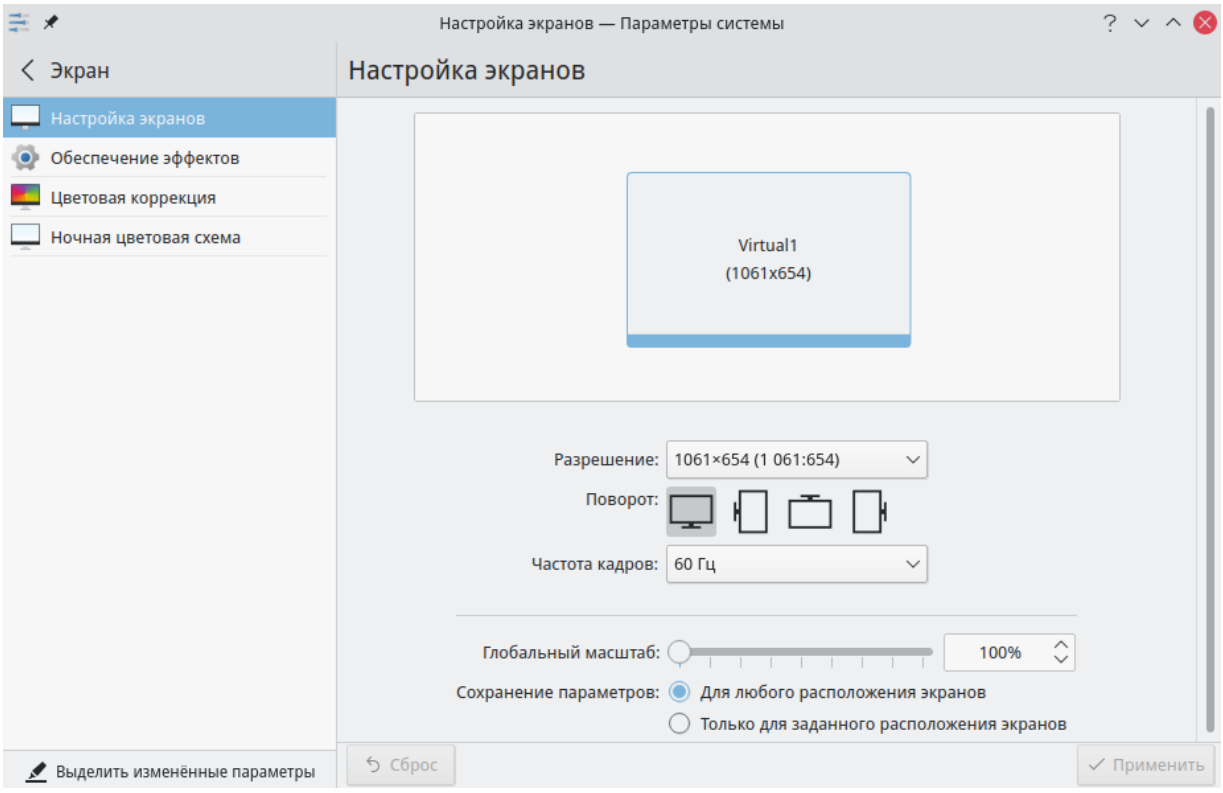

Рис. 22. Настройка параметров экрана

Настройка видеокарты

При возникновении проблем с графикой или при необходимости сменить драйвер графического устройства может пригодиться утилита «Настройка видеокарты», 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 эту кнопку, и вы сможете убедиться, что выбранная конфигурация работоспособна. Если изображение на экране вообще 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 будете предупреждены.
- Параметры — по умолчанию ОС РОСА ХРОМ 12 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.

5.3. Раскладка и тип клавиатуры

Утилита «Клавиатура» служит для определения параметров раскладки клавиатуры и аппаратного типа клавиатуры. Перейдите из меню [Параметры системы] → [Оборудование] → [Устройства ввода]. Далее выберите в левой части экрана клавиатуру.

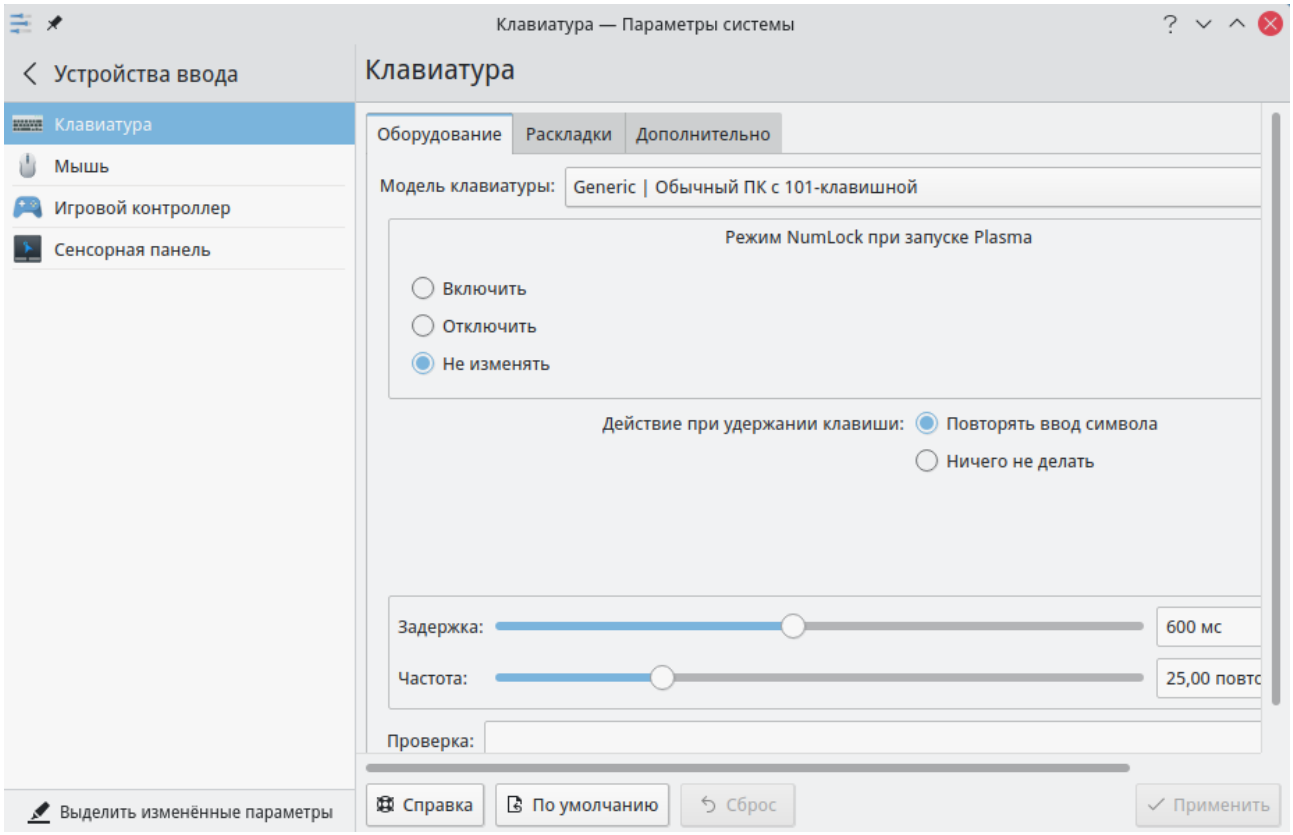

Рис. 23. Настройки клавиатуры

В открывшемся меню доступен выбор раскладку клавиатуры, её тип или модель. Изменения вступают в силу после нажатия [Применить]. 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.

5.4. Настройка принтеров

При первом включении принтера система постарается автоматически определить его модель и настроить его, о чём сообщается во всплывающем окне.

В комплекте поставки ОС РОСА ХРОМ 12 есть драйвера для большинства современных принтеров, поэтому, скорее всего, следом вы увидите сообщение об успешной установке.

Чтобы изменить параметры принтера или добавить новый, воспользуйтесь утилитой «Настройка принтера», расположенной в блоке «Оборудование» программы «Параметры системы».

Изменение параметров принтера

Двойной щелчок по значку принтера вызывает окно его настройки. Откройте нужный раздел, измените параметры и нажмите на кнопку [Применить].

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, приём 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).

Добавление локального принтера

1. Подключите принтер к компьютеру 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 вам 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 на ошибочный принтер.

5. Нажмите на кнопку [Применить принтер]. После этого он должен получить статусы «Готовность» и «Доступен».

Добавление удаленного принтера

1. Узнайте у администратора сети модель и название принтера, и используемый протокол. Убедитесь, что принтер включён.
2. Выберите пункт меню [Сервер] → [Новый] → [Принтер], затем укажите в списке «Устройства» сетевой протокол.
3. Дальнейшая настройка выполняется по аналогии с подключением локального принтера.

5.5. Подключение к сетям

ОС РОСА ХРОМ 12 автоматически подключается к доступным сетевым интерфейсам. Если автоматическое подключение не удалось, или если вы хотите настроить доступ в интернет или добавить новое соединение нажмите на кнопку [+] (Рис. 24) в меню [Параметры системы] → [Сеть и связь] → [Соединения].

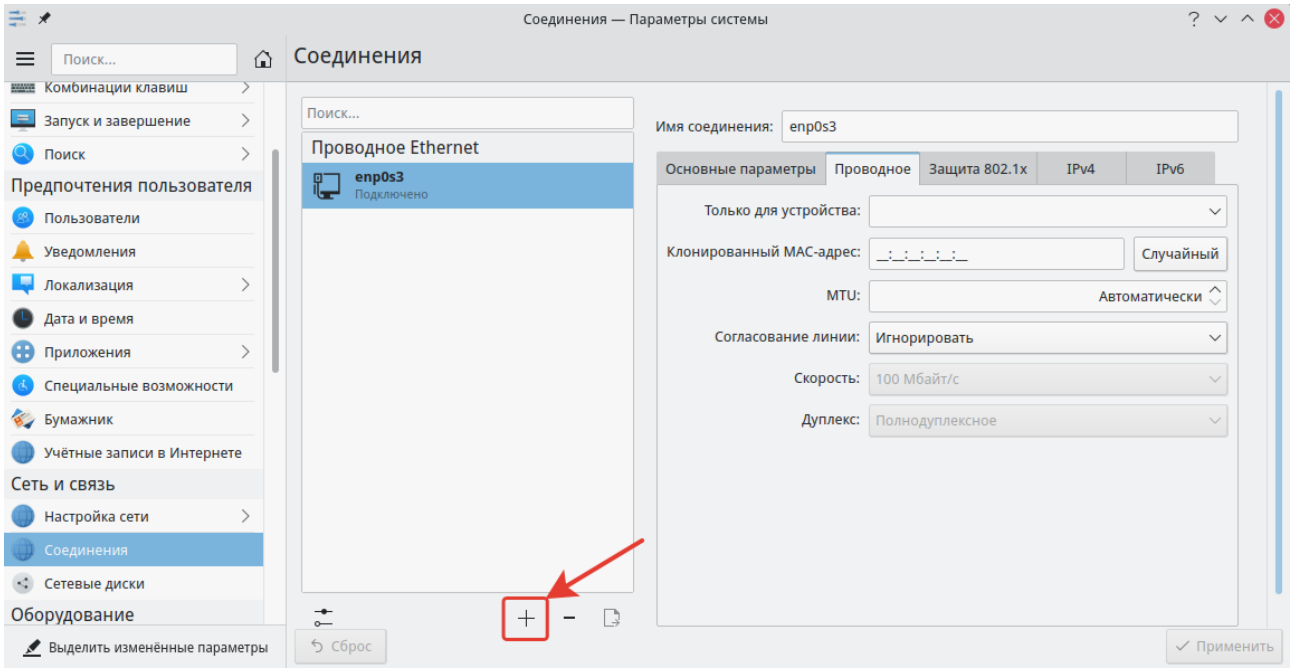

Рис. 24. Добавление новых соединений

Добавление проводного соединения

После подключения кабеля к сетевой карте компьютера выполняется автоматическое присвоение IP-адреса и других параметров локальной сети. Соединив компьютеры 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].

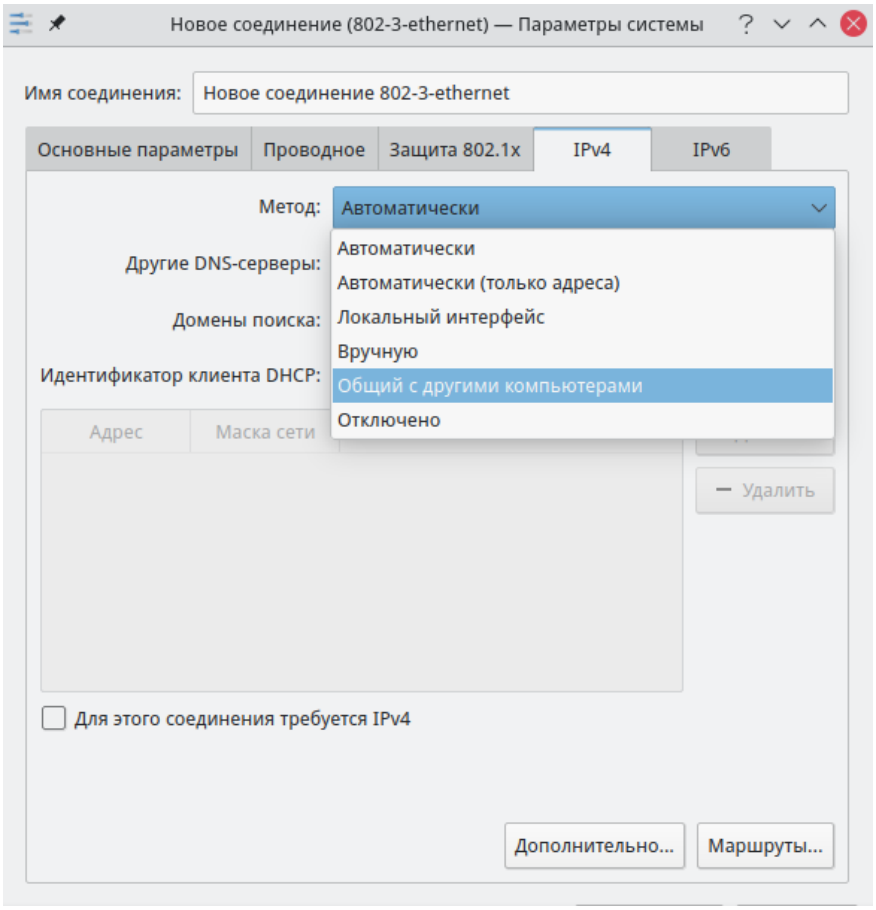

Рис. 25. Настройка параметров проводного соединения

Такую операцию необходимо проделать на всех компьютерах, которые вы хотите объединить в сеть. Как только хотя бы два компьютера будут настроены, локальная сеть должна заработать.

Добавление беспроводного соединения (Wi-Fi)

Подключение к общедоступной открытой сети без шифрования данных осуществляется автоматически.

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 её названию и занимает некоторое время. При подключении к защищённой сети

запрашивается пароль, и в этом случае соединение начинает устанавливаться только после ввода правильного пароля.

Настройка соединения

1. Выберите в окне настроек «Редактора соединений» вкладку «Беспроводные» и нажмите на кнопку [Сканировать] для поиска доступных сетей.
2. Обнаруженные сети можно просмотреть в виде таблицы или карты, на которой сети располагаются в зависимости от уровня радиосигнала: чем сильнее сигнал, тем ближе к компьютеру слева показана сеть.
3. Выбрав нужную сеть, нажмите [ОК]. Выбранная сеть появится на панели беспроводных соединений. Выделите её и нажмите на кнопку [Изменить].
4. 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».

Добавление мобильного соединения

После подключения USB-модема к порту компьютера его определение инициализация должны произойти автоматически. Если всё 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».
2. Ваш модем должен определиться автоматически и появиться в списке. Выберите его и нажмите на кнопку [Далее].
3. Укажите вашу 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 определён автоматически и изменить его будет нельзя. Если же вы приобрели универсальный модем, который может работать с разными SIM-картами, тарифный план следует вписать вручную.

5. После ввода необходимых данных мастер запросит подтверждение, и на этом настройка мобильного соединения будет завершена.

Для подключения дважды щёлкните по названию соединения. Если требование PIN-кода не отключено, его потребуется ввести. На панели подключения при необходимости можно отредактировать параметры соединения. Если всё верно, нажмите [OK], и соединение будет установлено.

Добавление VPN-соединения (PPTP)

VPN (Virtual Private Network, «виртуальная частная сеть») — это технология, позволяющая создать защищённой сетевое соединение поверх незащищённой 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)».
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».

6. МЕНЕДЖЕР ПАКЕТОВ

Управление программными пакетами осуществляется с помощью утилит командной строки rpm, dnf.

RPM является "низкоуровневым" пакетным менеджером, производящим установку, удаление и обновление пакетов в системе. DNF является "высокоуровневым" пакетным менеджером, в задачи которого входит разрешение зависимостей между пакетами, скачивание пакетов и их установка с использованием "низкоуровневого" RPM.

6.1. Управление с помощью командной строки

Рассмотрим основные операции с пакетами с помощью утилиты dnf, подробное описание опций утилиты приведено в man dnf.

Синтаксис команд:

```
sudo dnf <опции> <команда> <пакет>
```

Поле <Команда> определяет одно из действий, представленных в Таблица 9 .

Таблица 9 – 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

Команда	Описание
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 команд:

1. В результате выполнения этой команды произойдет установка пакета mc:

```
sudo 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:

```
sudo dnf update mc
```

3. В результате выполнения этой команды произойдет удаление пакета mc:

```
sudo dnf remove mc
```

6.2. Управление с помощью графического интерфейса

Менеджер пакетов имеет графическую оболочку в виде утилиты «Управление программами - dnfdragora».

Как правило, дополнительные приложения РОСА, необходимые пользователю, устанавливаются из официальных источников — репозиториев. По умолчанию, список репозиториев для ОС уже настроен. Чтобы его просмотреть, выполните в приложении «Управление программами - dnfdragora» переход по пунктам меню «Файл» → «Репозитории».

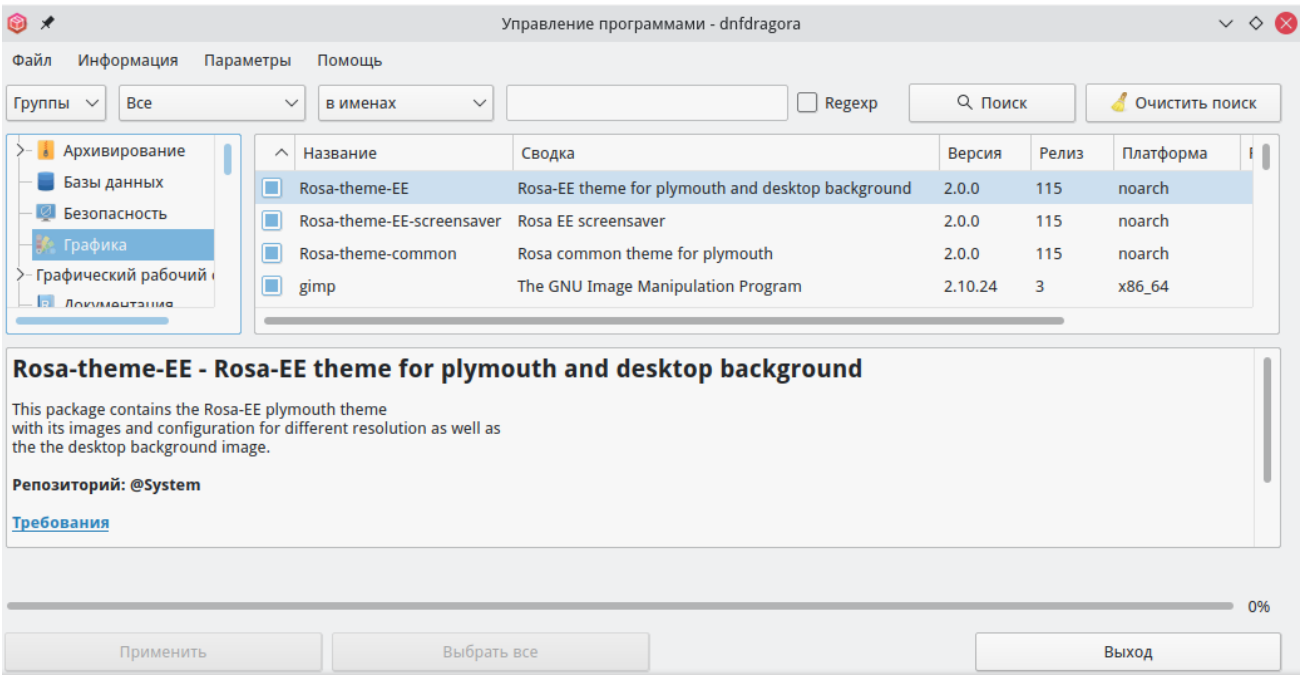

Рис. 26. Управление программами - dnfdragora

С помощью утилиты пакеты программ устанавливаются, удаляются или обновляются их версии. Все пакеты разбиты на категории, список которых находится в левой части главного окна программы.

Каждый раз при запуске программы менеджер пакетов проверяет списки онлайн-пакетов (источники), скачиваемые непосредственно с официальных серверов ROSA, и показывает при каждом запуске актуальные версии приложений и пакетов, доступные для вашей системы.

Система фильтров позволяет отображать пакеты только определённых типов: программа может отображать только установленные приложения (по умолчанию) или только доступные приложения. Можно выполнить поиск по имени пакета или по описанию, или по имени файла, включённого в пакет. По умолчанию программа запускается с фильтром «пакеты с графическим интерфейсом».

Приложение «Управление программами» организует фильтрацию установленных в ОС пакетов по различным категориям, таким как фильтр по типу и состоянию пакетов. Доступные режимы отображения: «Все», «Установленные», «Можно обновить», «Не установленные», «x86_64 + noarch»

В программе доступен режим поиска. Щёлкните левой кнопкой мыши по значку поиска (лупа), чтобы выбрать режим поиска: по имени пакета, по полному описанию пакета, по сводке пакета или по файлам, включённым в пакет.

Введите в поле поиска одно или несколько ключевых слов для поиска. Когда вы ищете пакет по имени, используйте дефис (-) вместо символа пробела.

Действия с пакетами

Выбрав в списке интересующий вас пакет, установите для него флажок действия. Если значка рядом с названием пакета нет, это значит, что пакет может быть установлен. Некоторые пакеты помечены значком «кирпич», это базовые пакеты, которые нельзя удалять, чтобы не нарушить работу системы; их флажки не могут быть сняты.

Чтобы начать непосредственно процесс установки или удаления пакетов, нажмите на кнопку [Применить]. Будет запрошено подтверждение, после чего появится новое окно, отображающее ход процесса.

Управление зависимостями

Может случиться, что вы выберете пакет, имеющий зависимости (требующий дополнительные библиотеки и т. п.). В этом случае утилита выдает информационное окно, в котором предлагает выбор: принять зависимости, отменить операцию или получить дополнительные сведения. Отметим, что из-за наличия зависимостей дисковое пространство, необходимое для установки выбранного пакета, может превышать размер самого пакета. Иногда зависимости могут быть удовлетворены несколькими пакетами. Список альтернатив при этом будет предоставлен. Дополнительные сведения можно получить, нажав на кнопку [Информация**...**], — не исключено, что это поможет сделать лучший выбор.

7. 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 системы (`/home/<имя_пользователя>`).

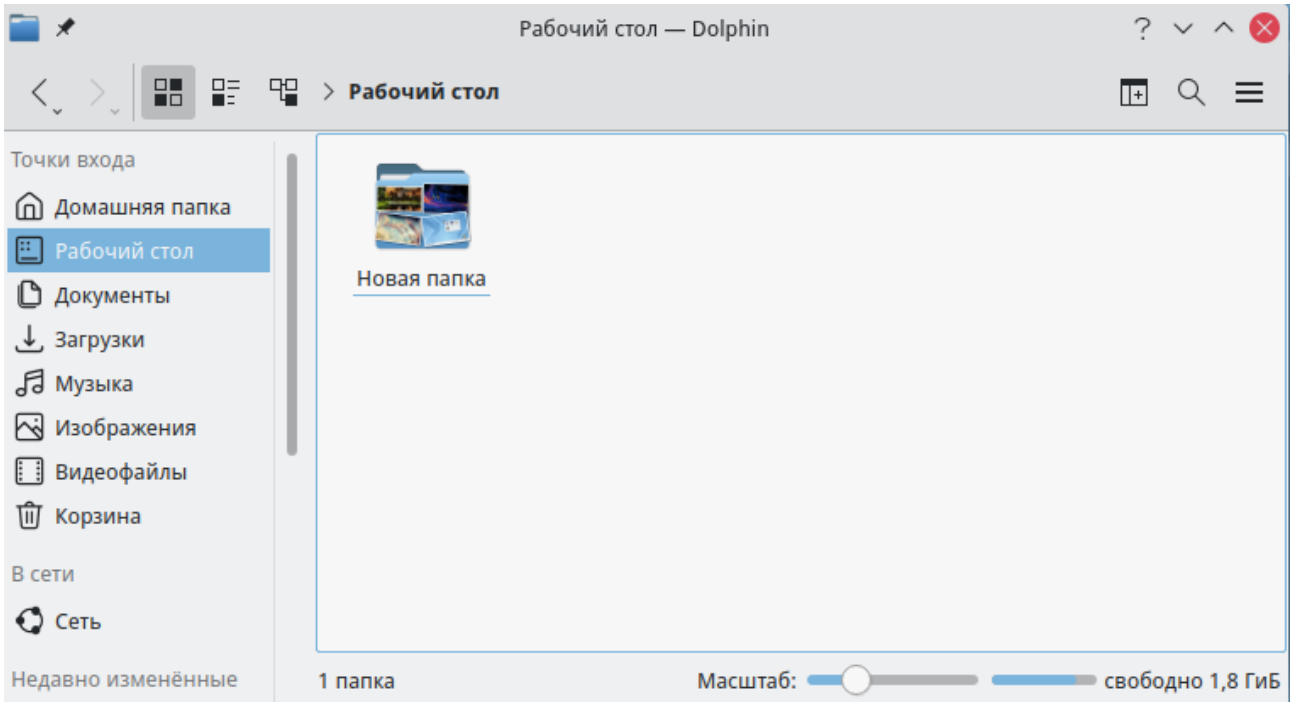

Рис. 27. Интерфейс менеджера пакетов

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.

Для создания нового каталога нажмите клавишу <F10> или щёлкните 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, щёлкните 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].

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

Корзина

В корзине хранятся удалённые файлы. Открыв корзину, можно найти и восстановить ошибочно удалённый файл.

Сменные устройства и носители

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

Сеть

Если компьютер 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 ваших 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), её 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 системы, для поиска файлов можно использовать и менеджер Dolphin. Панель поиска вызывается щелчком по значку с лупой. Поиск начинается при вводе искомого контекста, результаты выводятся в окне ниже. При

поиске файла по имени можно использовать маски, в которых звёздочка (*) заменяет любое количество любых символов, а вопросительный знак (?) — любой одиночный символ.

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 того, чтобы отправить файл или файлы в архив нажмите правой кнопкой мыши на необходимый файл(файлы) и в контекстном меню выберете параметр «Упаковать» и далее необходимый формат архива.

8. НАСТРОЙКА СЕРВЕРА SAMBA

В этом разделе описано создание домена — централизированного хранилища пользователей и их атрибутов.

Контроллер домена — программное обеспечение, обеспечивающее создание и функционирование сервера домена. В данном случае в качестве контроллера домена используется Samba.

AD — Active Directory — домен разработки Microsoft. Samba реализует Samba AD — совместимый с Microsoft Active Directory домен, в который можно вводить и Linux, и Windows-клиенты.

Клиент — конечный член домена или ПО, позволяющее обеспечить членство в домене.

В статье описывается создание лабораторной установки, состоящей из 1 сервера и 1 клиента, находящихся в одной подсети 192.168.122.0/24.

Все приведенные консольные команды выполняются от пользователя root, если не указано иное. Вход в root-консоль выполняется командой.

```
su -
```

или

```
sudo -i
```

8.1. Настройка контроллера домена

8.1.1. Настройка сети

Важно правильно настроить сеть на клиенте и сервере. В простых случаях, в том числе при поднятии тестовых стендов, необходимо, чтобы клиент и сервер находились в одной подсети. Например, чтобы у виртуальной машины с сервером был IP-адрес 192.168.10.2, а у виртуальной машины с клиентом — 192.168.10.3.

Рассмотрим настройку сети на сервере. Установите полноквалифицированное (FQDN) доменное имя, состоящее из: `имя_хоста.домен.зона`, например:

```
server1.samba.loc
```

Тогда именем хоста будет server1, доменом — samba, доменной зоной — loc, realm — samba.loc.

Избегайте использования зоны .local или выключите или перенастройте Avahi, чтобы использовать ее.

Установим имя хоста на контроллере домена:

```
hostnamectl set-hostname server1.samba.loc
```

Посмотрите IP-адрес командой:

```
/sbin/ip a
```

Пример вывода:

```
[root@server1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: host0@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
noqueue state UP group default qlen 1000
    link/ether 32:e2:0b:ba:17:c5 brd ff:ff:ff:ff:ff:ff link-
netnsid 0
    inet 169.254.212.10/16 brd 169.254.255.255 scope link host0
       valid_lft forever preferred_lft forever
    inet 192.168.122.12/24 brd 192.168.122.255 scope global dynamic
host0
       valid_lft 2577sec preferred_lft 2577sec
    inet6 fe80::30e2:bff:feba:17c5/64 scope link
       valid_lft forever preferred_lft forever
```

В данном примере IPv4-адрес — 192.168.122.12.

В файл /etc/hosts необходимо добавить строку вида:

```
192.168.122.12 server1.samba.loc server1
```

Как видите, необходимо, чтобы и FQDN, и краткое имя выводились в IP-адрес контроллера домена. Для этого откройте файл в консольном редакторе:

```
nano /etc/hosts
```

Добавьте указанную строку, сохраните сочетанием клавиш <Ctrl+O>, затем Enter, затем закройте консольный редактор сочетанием клавиш <Ctrl+X>.

Далее проверьте корректность записей в файле /etc/hosts командами

```
ping -c3 server1.samba.loc
ping -c3 server1
```

Обратите внимание, что сеть должна запускаться до входа пользователя в систему, если используется подключение к сети по WiFi, то настройте его соответствующим образом.

8.1.2. Запуск контроллера домена

Установите необходимые для работы пакеты:

```
dnf install samba-server /bin/ps /usr/bin/xargs /usr/bin/nslookup
```

Отключите лишние службы из состава набора программ Samba:

```
systemctl disable --now smb nmb winbind
```

Их обособленная работа не требуется и будет мешать контроллеру домена.

Убедитесь, что они действительно выключены, используя команду, которая в результате не должна ничего выдать:

```
ps ax | grep -E "samba|smbd|nmbd|winbindd" | grep -v grep
```

Сотрите старые файлы настроек, оставив их резервные копии:

```
mv -v /etc/samba/smb.conf /etc/samba/smb.conf.old
mv -v /etc/krb5.conf /etc/krb5.conf.old
```

Очистите старые базы данных, путь к которым можно узнать командой:

```
smbd -b | grep -E "LOCKDIR|STATEDIR|CACHEDIR|PRIVATE_DIR"
```

Используйте команду для очистки:

```
smbd -b | grep -E "LOCKDIR|STATEDIR|CACHEDIR|PRIVATE_DIR" | awk '{print $NF}' | xargs -I'{}' rm -fv '{}'/*.{tdb,ldb}
```

Если эта команда ничего не выдала, то у вас не было баз данных от прошлых запусков контроллера домена.

Запустите интерактивную настройку домена:

```
samba-tool domain provision --use-rfc2307 --interactive
```

Ниже приведем ее типовой вывод. В квадратных скобках ([ ]) указывается значение по умолчанию. Нажимайте Enter, чтобы с ним согласиться, или введите иное значение. Если сеть и имя хоста были настроены верны, то значения по умолчанию не должно потребоваться изменить.

```
 [root@server1 ~]# samba-tool domain provision --use-rfc2307 --interactive
 Realm [SAMBA.LOC]:
 Domain [SAMBA]:
 Server Role (dc, member, standalone) [dc]:
```

```
 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)
[SAMBA_INTERNAL]:
 DNS forwarder IP address (write 'none' to disable forwarding)
[192.168.122.1]:
 Administrator password:
 Retype password:
```

На последнем шаге вводится пароль доменного пользователя Administrator, при вводе пароль не отображается, пароль должен быть сложным.

DNS Forwarder — это адрес сервера, к которому перенаправляются DNS-запросу, на которые сам контроллер домена не может ответить, например, запрос DNS yandex.ru будет направлен в него.

Исполните команду:

```
mv -v /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

Теперь добавьте службу контроллера домена в автозапуск:

```
systemctl enable samba
```

Запустите контроллер домена:

```
systemctl restart samba
```

И посмотрите его лог, убедитесь, что он запустился без ошибок:

```
systemctl status samba
```

Статус службы должен быть "active" ("запущена"), но в конце лога может быть "ошибка":

```
dnsupdate_nameupdate_done: Failed DNS update with exit code 29
```

Сведения об ошибке не являются критическими, убедитесь в этом запустив команду:

```
samba_dnsupdate --verbose
```

В подробном логе будет сказано про ошибки "WERR_DNS_ERROR_RECORD_ALREADY_EXISTS", которые означают, что добавляемая запись DNS уже существует. Она была создана при создании домена. Запись "Failed update of 29 entries" означает, что такая ситуация возникла 29 раз, а это количество раз и стало кодом возврата samba_dnsupdate.

Проверьте работу DNS-сервера, на другом компьютере, например, будущем клиенте домена, выполнив команду:

```
nslookup server1.samba.loc 192.168.122.12
```

Для корректного выполнения необходимо подставить в пример ваши IP- адреса. Пример успешного ответа:

```
$ nslookup server1.samba.loc 192.168.122.12
Server:         192.168.122.12
Address:        192.168.122.12#53

Name:   server1.samba.loc
Address: 192.168.122.12
```

Для настройки клиентов будет полезно знать рабочую группу NT, ее можно узнать так:

```
[root@server1 ~]# cat /etc/samba/smb.conf | grep workgroup
    workgroup = SAMBA
```

Убедитесь, что этот сервер способен выдать DNS требуемого домена, выполнив на будущем клиенте домена (не на контроллере):

```
nslookup yandex.ru 192.168.122.1
```

Возможно, стоит указать 8.8.8.8 или иной сервер. После первоначальной настройки контроллера его можно заменить в файле `/etc/samba/smb.conf` перезапустив контроллер после изменения настроек командой

```
systemctl restart samba
```

8.1.3. Ввод ROSA-клиента в домен

Для настройки сети на Linux-клиенте необходимо:

- добавить адрес контроллера домена в DNS-серверы;
- добавить REALM (samba.loc, рассмотрено в примере выше) в список доменов поиска.

Для настройки через графический интерфейс перейдите в меню [Параметры системы] → [Сеть и связь] → [Соединения], откроются настройки сетевого соединения, далее откройте вкладку "IPv4". К DNS-серверам добавьте адрес контролера домена, в примере выше это 192.168.122.12. В параметр "Домены поиска" добавьте realm — samba.loc.

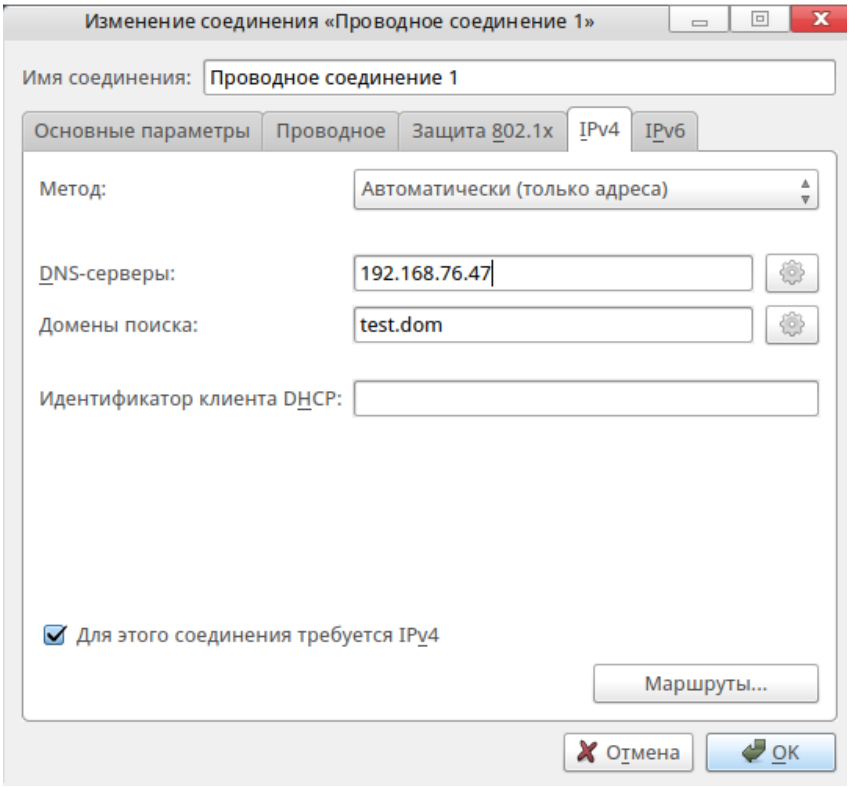

Рис. 28. Параметры настроек в меню «Соединения»

Также имеется интерактивный консольный интерфейс nmtui для редактирования настроек меню «Соединения» и утилита nmcli.

Утилиты меню «Соединения» редактируют файл /etc/resolv.conf. Альтернативой графическому интерфейсу является редактирование этого файла напрямую, написав в нем следующие строки:

```
nameserver 192.168.122.12
search samba.loc
```

с помощью команды:

```
ping server1
```

Проверьте сетевую доступность контроллера домена.

8.2. Подключение компьютера с ОС ROSA к домену

Установите необходимые пакеты командой:

```
dnf install drakxtools samba-server samba-client samba-winbind nss_ldap libnss-role pam_krb5 lib64sasl2-plug-gssapi urpmi perl-URPM
```

Запустите утилиту drakauth:

```
drakauth
```

После выполнения команды запустится графический интерфейс утилиты drakauth, в настройках которой выберите для параметра «Способ аутентификации» - «Домен Windows», нажмите кнопку «Далее».

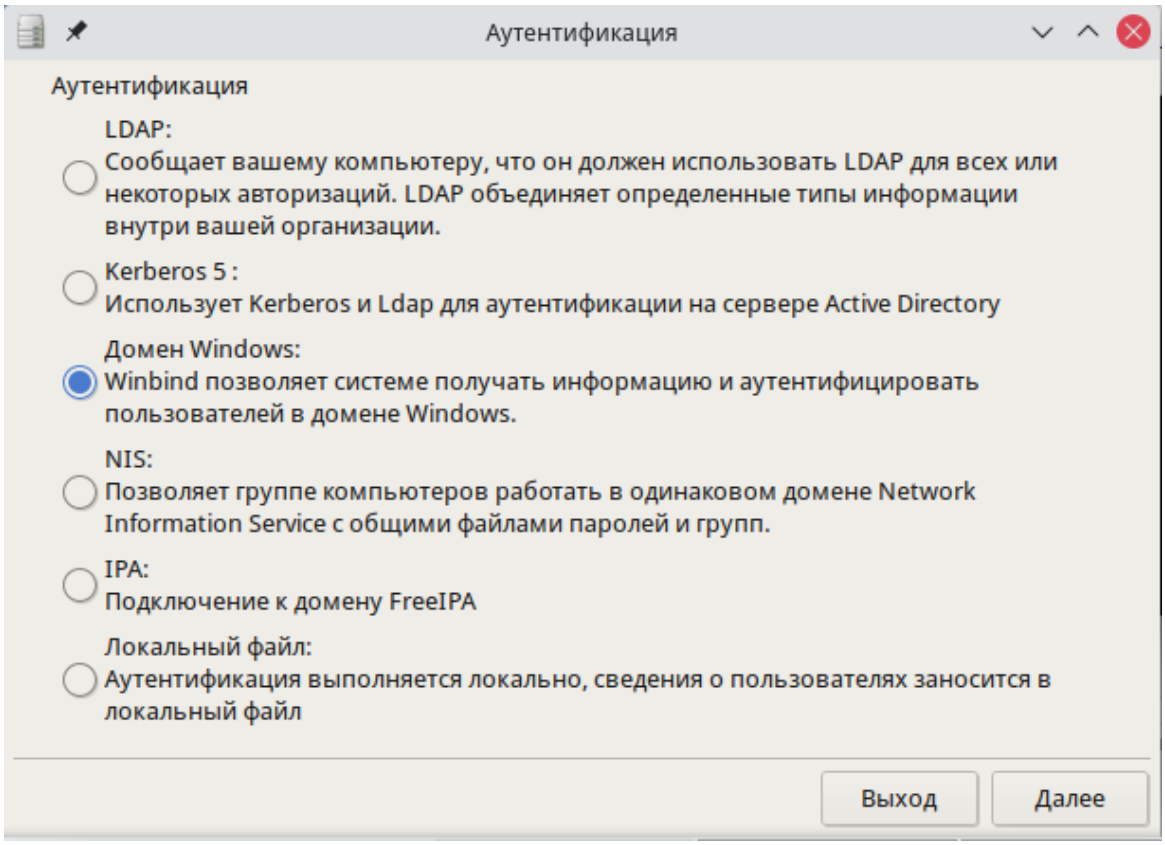

Рис. 29. Выбор способа аутентификации в утилите drakauth

Далее для параметра «Тип домена» - «Active Directory».

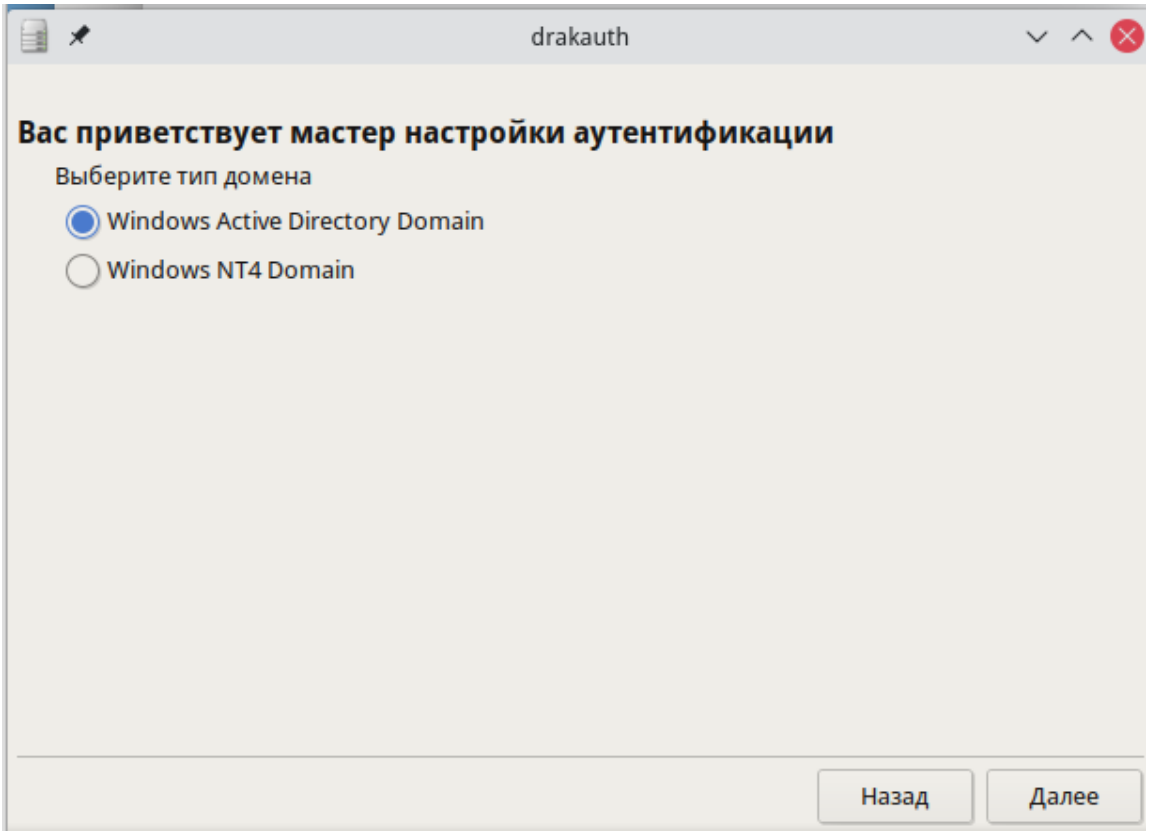

Рис. 30. Выбор домена в утилите drakauth

В предлагаемой лабораторной установке и большинстве типовых конфигураций все необходимые параметры должны оказаться автоматически заполнены правильно. Заполните следующие параметры и нажмите кнопку «Далее»:

— «Область Active Directory» - «samba.loc»

— «Домен DNS» - «samba.loc»

— «Рабочая группа» - «SAMBA»

— «Сервер DC» - «SERVER1.samba.loc»

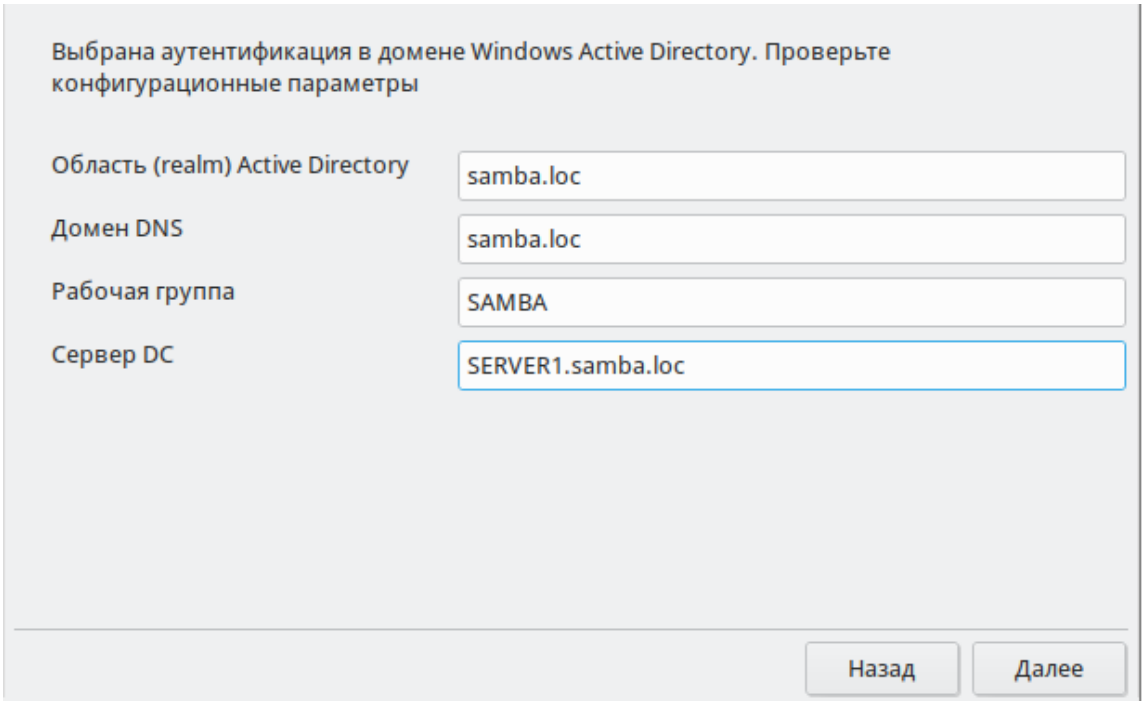

Рис. 31. Конфигурационные параметры аутентификации

Далее укажите желаемое имя NetBIOS (Рис. **32**.).

Поле "Описание компьютера" не обязательно для заполнения.

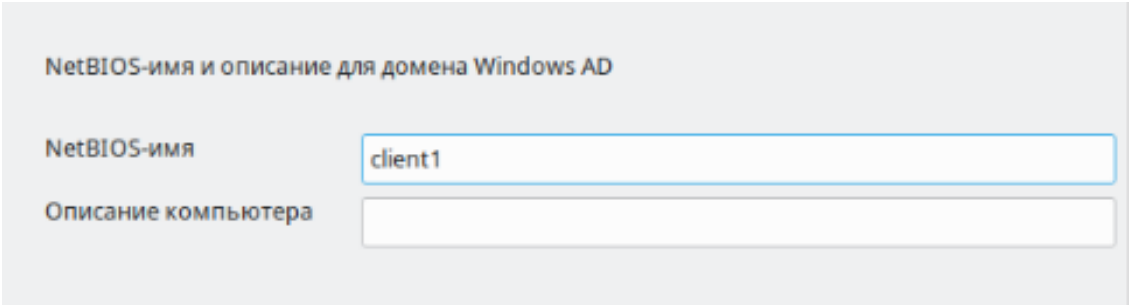

Рис. 32. Описание для домена Windows AD

Далее введите логина администратора домена и пароль администратора домена. Нажмите кнопку "Далее". В случае успешного ввода в домен будет предложено перезагрузить систему.

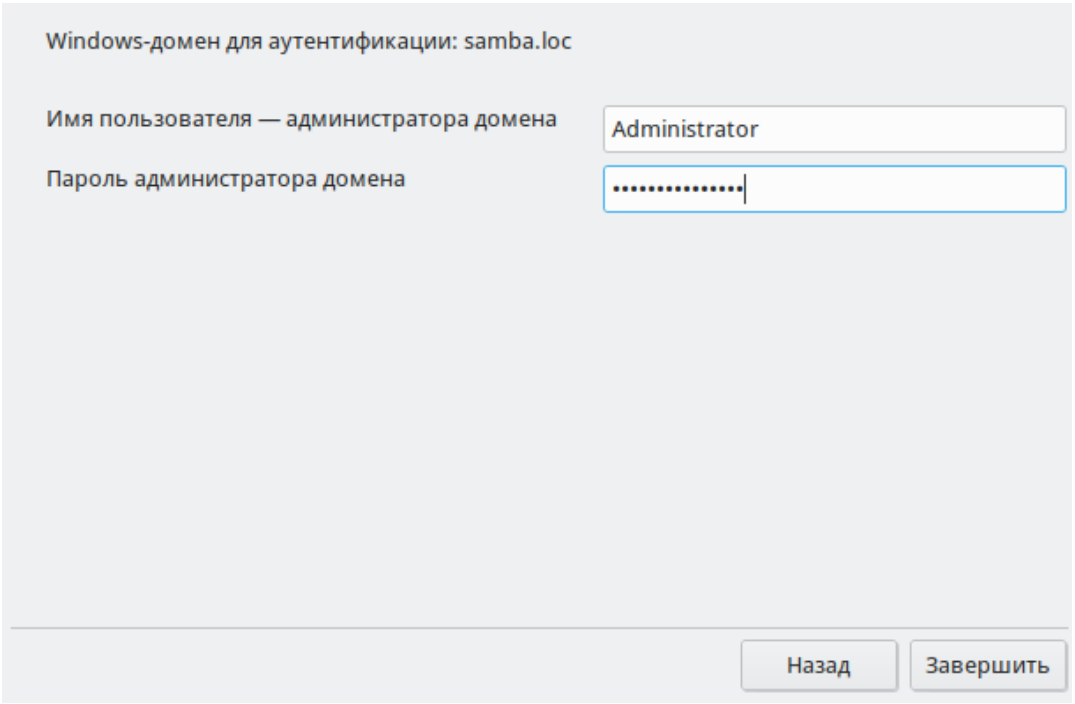

Рис. 33. Имя пользователя и пароль администратора Windows-домена

9. ИСПОЛЬЗОВАНИЕ NMCLI

nmcli - консольный инструмент графической утилиты NetworkManager. nmcli используется для создания, отображения, редактирования, удаления, активации и деактивации сетевых подключений.

Просмотр доступных интерфейсов осуществляется с помощью команд:

```
nmcli
nmcli connection show
nmcli device show
```

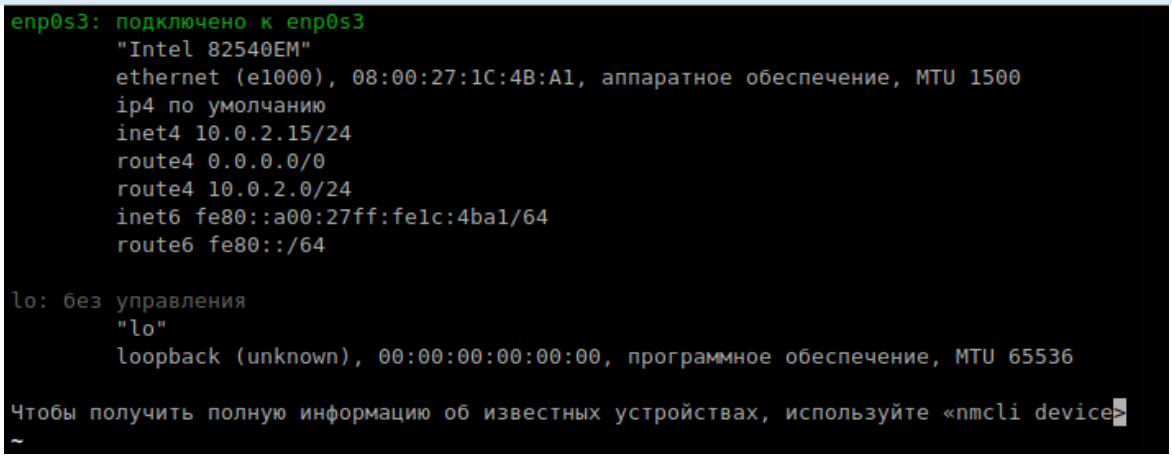

Рис. 34. Просмотр доступных подключений

9.1. Настройка статических соединений

Для статической настройки всех соединения статически в сетевом интерфейсе придерживайтесь следующих шагов.

В меню [Параметры системы] → [Сеть и связь] → [Соединения] обычно заполняются такие параметры как: выбор DNS-сервера, Домен поиска, Метод настройки сети (в данном случае - вручную), IP-адрес, Маска сети и Шлюз.

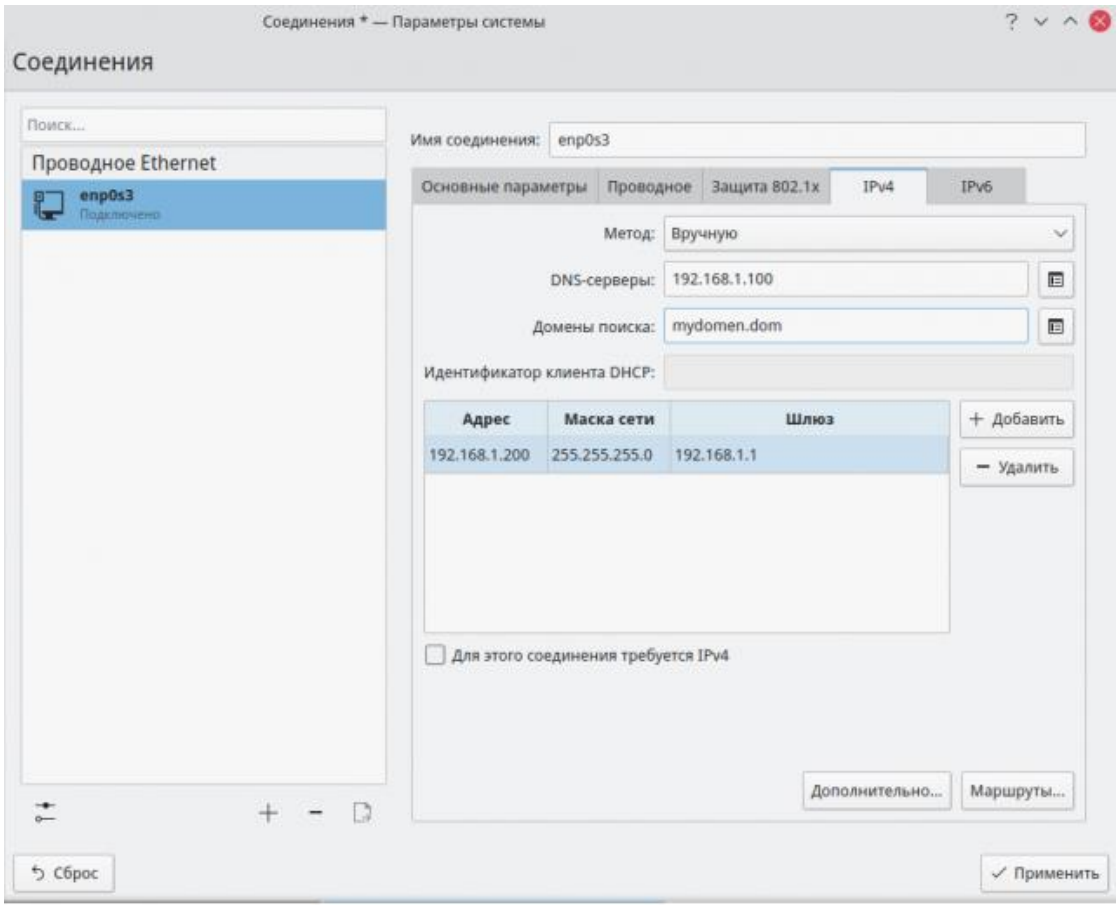

Рис. 35. Параметры статистического соединения

Для того, чтобы прописать такие же параметры в консоли, введите следующие команды:

```
nmcli connection modify enp0s3 connection.autoconnect yes ipv4.method manual ipv4.dns 192.168.1.100 ipv4.dns-search mydomen.dom ipv4.addresses 192.168.1.200/24 ipv4.gateway 192.168.1.1
```

где:

- connection modify – изменение соединения на интерфейсе enp0s3;
- connection.autoconnect yes - поднятие соединения при загрузке системы
- ipv4.method manual – команда делает соединение статическим
- ipv4.dns - IP адрес вашего DNS сервера
- ipv4.dns-search - домен поиска
- ipv4.addresses - прописываем IP адрес и маску /24 нашего интерфейса
- ipv4.gateway - прописываем IP адрес нашего шлюза

Далее необходимо перезапустить интерфейс:

```
nmcli connection down enp0s3
nmcli connection up enp0s3
```

```
user1@rosa2021 ~ $ nmcli connection down enp0s3
Подключение «enp0s3» успешно отключено (активный путь D-Bus: /org/freedesktop/NetworkManager/Ac
tiveConnection/1)
user1@rosa2021 ~ $ nmcli connection up enp0s3
```

Рис. 36. Перезапуск соединения командой connection down

Альтернативные команды для перезапуска:

```
nmcli device disconnect enp0s3
nmcli device connect enp0s3
```

```
user1@rosa2021 ~ $ nmcli device disconnect enp0s3
Устройство «enp0s3» отключено успешно.
user1@rosa2021 ~ $ nmcli device connect enp0s3
```

Рис. 37. Перезапуск соединения командой device disconnect

9.2. Настройка динамических соединений

Предположим, необходимо настроить все соединения динамически, в сетевом интерфейсе.

В меню [Параметры системы] → [Сеть и связь] → [Соединения] обычно заполняются такие параметры как: Метод настройки сети (в данном случае - автоматически), другие DNS-серверы, Домены поиска, Идентификатор клиента DHCP.

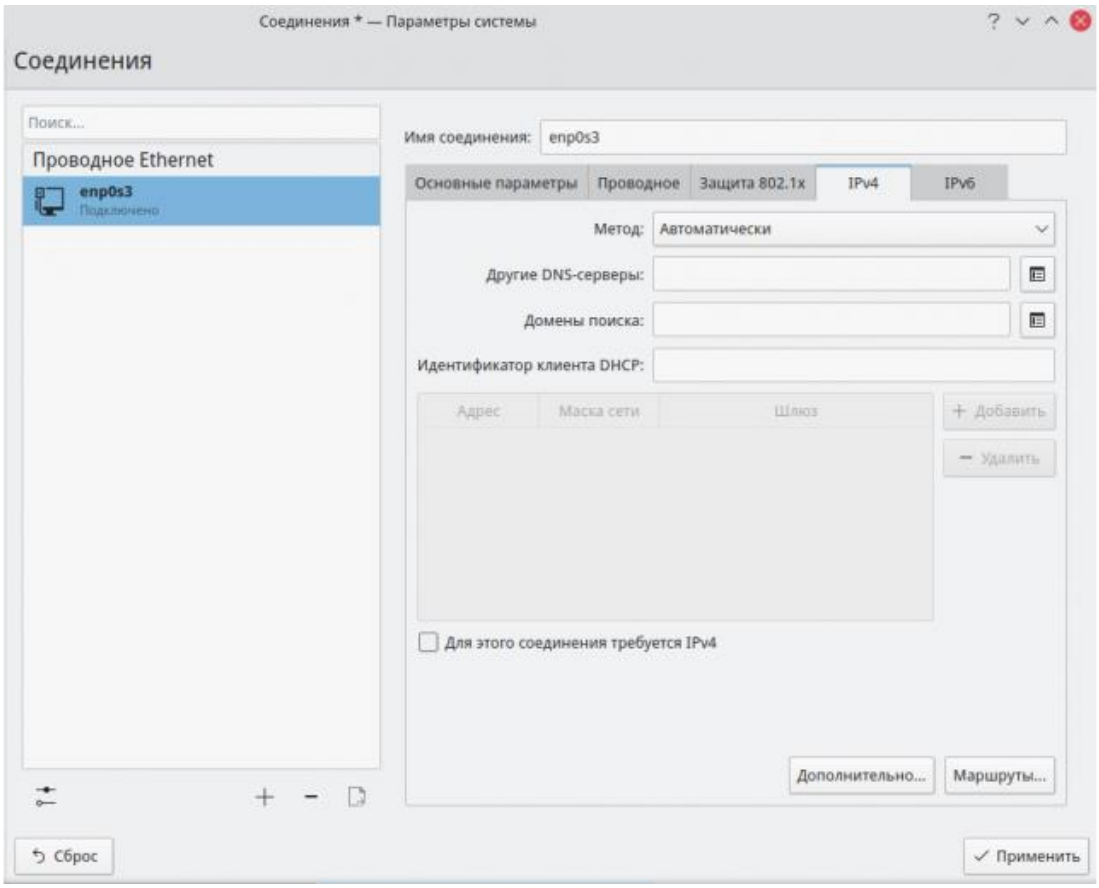

Рис. 38. Параметры динамического соединения

Для того, чтобы прописать все параметры в консоли, введите следующую команду:

```
nmcli connection modify enp0s3 ipv4.method auto ipv4.ignore-auto-dns no
```

где параметры:

- connection modify - изменение соединения на интерфейсе enp0s3;
- ipv4.ignore-auto-dns – прописываем параметр no, таким образом не игнорируются полученные по dhcp серверов DNS:
- ipv4.method auto - делаем наше соединение динамическим.

Далее необходимо перезапустить интерфейс:

```
nmcli connection down enp0s3
nmcli connection up enp0s3
```

Альтернативные команды для перезапуска:

```
nmcli device disconnect enp0s3
nmcli device connect enp0s3
```

9.3. Настройка динамических соединений (кроме DNS)

При необходимости настроить все соединения динамически в вашем сетевом интерфейсе, за исключением DNS, придерживайтесь следующей инструкции.

В NetworkManager обычно заполняются такие параметры как: Метод настройки сети (в данном случае – автоматически (только адреса)), другие DNS-серверы, Домены поиска, Идентификатор клиента DHCP.

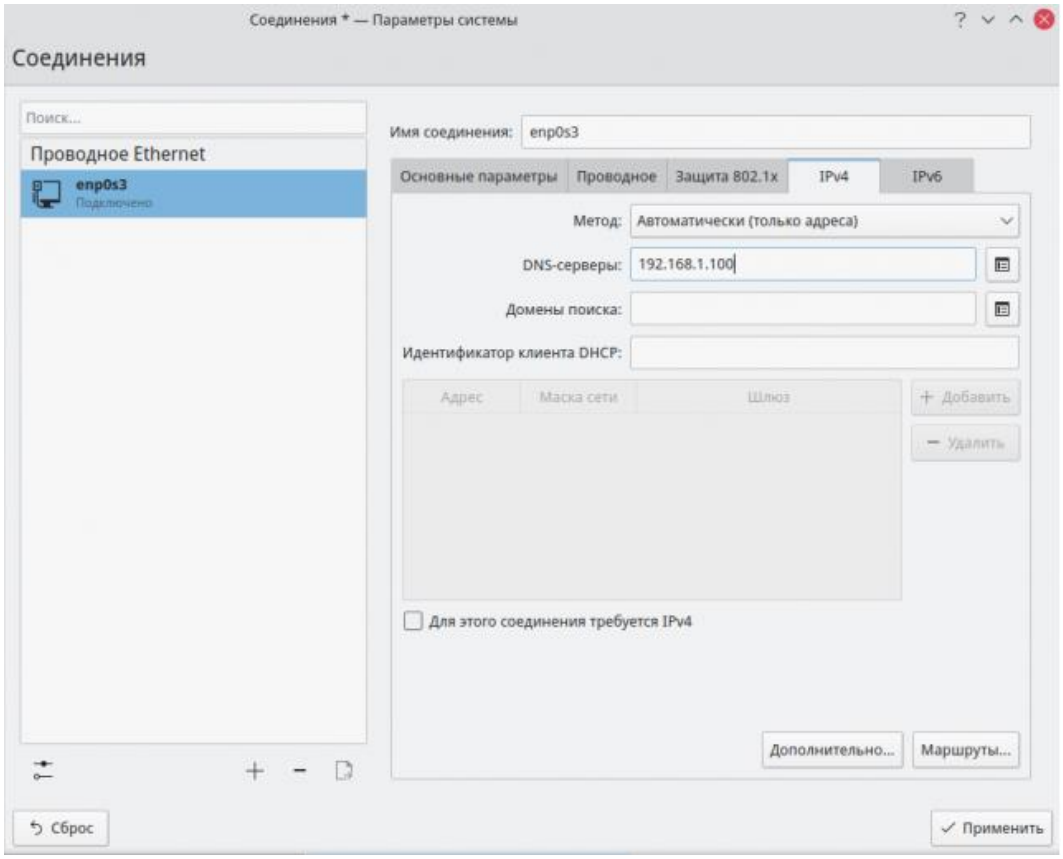

Рис. 39. Параметры динамических соединений (за исключением DNS)

Для того, чтобы прописать все параметры в консоли, введите следующие команды:

```
nmcli connection modify enp0s3 ipv4.ignore-auto-dns yes ipv4.dns 192.168.1.100
```

где:

- connection modify - изменение соединения на интерфейсе enp0s3;
- ipv4.ignore-auto-dns - прописываем параметр yes, таким образом игнорируются полученные по dhcp серверов DNS;
- ipv4.dns - прописываем IP адрес нашего DNS сервера.

Далее перезапустите интерфейс:

```
nmcli connection down enp0s3
nmcli connection up enp0s3
```

Либо воспользуйтесь альтернативным вариантом для перезапуска:

```
nmcli device disconnect enp0s3
nmcli device connect enp0s3
```

10. НАСТРОЙКА DHCP СЕРВЕРА

10.1. Установка DHCP сервера

Сначала нам надо обновить систему:

```
dnf --refresh distro-sync
```

Далее установите сам dhcp-server командой:

```
dnf install dhcp-server
```

10.2. Базовая настройка dhcpd

Настройки сервера хранятся в файле /etc/dhcpd.conf. Откройте конфигурационный файл и произведите настройки для подсети 10.198.1.0/24:

```
subnet 10.198.1.0 netmask 255.255.255.0 {
          option routers 10.198.1.1;
          option subnet-mask 255.255.255.0;
          option domain-search "rosaserver.lan";
          option domain-name-servers 10.198.1.2;
          range 10.198.1.10 10.198.1.100;
          default-lease-time 600;
          max-lease-time 7200;
          authoritative;
 }
```

Где:

- option routers - IP адрес шлюза;
- option subnet-mask - маска подсети;
- option domain-search - имя домена;
- option domain-name-servers - адреса DNS серверов в сети;
- range - пул выдаваемых IP адресов;
- default-lease-time - время аренды IP адреса;
- max-lease-time - максимальное время аренды IP адреса;
- authoritative - это "авторитетность" нашего сервера. Данный параметр определяет, если клиент запросит неправильный IP адрес, то в этом случае сервер ответит ему отказом и предложит получить новый адрес из выделенного диапазона.

В данном примере мы хотим выдать клиентам, адреса в диапазоне 10.198.1.10-10.198.1.100, с шлюзом 10.198.1.1 и dns сервером 10.198.1.2

10.3. Настройка статических IP адресов

Предположим, что два хоста, должны иметь определенные IP-адреса в сети. Тогда необходимо добавить описание к этим хостам в кониге:

```
host buh1-work {
        hardware ethernet 05:33:42:00:2a:5d;
        fixed-address 10.198.1.101;
}
host buh2-work {
        hardware ethernet 05:33:42:01:3b:4c;
        fixed-address 10.198.1.102;
}
```

10.4. Определение сетевого интерфейса

Откроем файл конфигурации etc/sysconfig/dhcpd и скорректируйте строчку:

```
DHCPDARGS=enp2s0
```

В данном примере, у DHCP сервер будет работать только на интерфейсе enp2s0.

Для проверки работы сервиса используйте команду:

```
systemctl status dhcpd.service
```

Вывод данной команды при успешном запуске сервиса должен иметь примерно такой вид, как показано на

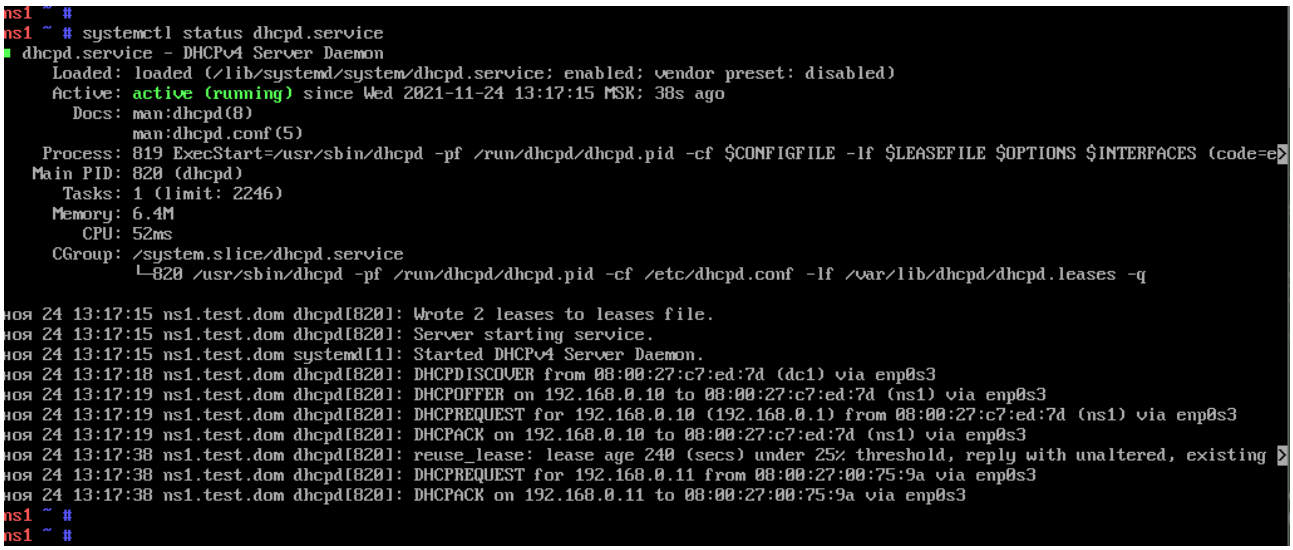

Рис. 40. Вывод команды systemctl status dhcpd.service

11. НАСТРОЙКА DNS СЕРВЕРА BIND

11.1. Установка bind

Перед установкой сервера необходимо обновить систему:

```
dnf --refresh distro-sync
```

Далее устанавливаем сам вервер Bind (пакет называется bind, а вот его сервис называться named). Обратите внимание, что все конфигурационные файлы/сервисы будут называться на named

Далее для настройки DNS сервера необходимо настроить параметр systemd-resolved в файле

/etc/systmd/resolved.conf.

Перед настройкой также необходимо запросить команду:

```
lsof -i :53
```

```
dc1 ~ #
dc1 ~ # lsof -i :53
COMMAND   PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r 610 systemd-resolve   17u  IPv4  22714      0t0  UDP localhost:domain
systemd-r 610 systemd-resolve   18u  IPv4  22715      0t0  TCP localhost:domain (LISTEN)
dc1 ~ #
```

Рис. 41. Вывод команды lsof -i :53

Правим следующие строки:

```
DNS=127.0.0.1
FallbackDNS=
DNSSEC=no
LLMNR=resolve
DNSStubListener=no
```

где:

- DNS=127.0.0.1 - это локальный ip адрес, на котором будет работать наш DNS сервер будущий;
- FallbackDNS= - оставляем пустым, чтобы systemd-resolved не переключался на fallback dns сервера;
- DNSSEC=no - отключаем DNSSEC;
- LLMNR=resolve - LLMNR переводим в режим resolve;
- DNSStubListener=no – параметр no, чтобы systemd-resolved не прослушивал порт 53.

Остальные опции в этом файле, следует оставить как есть и произвести перезапуск systemd-resolved:

```
systemctl restart systemd-resolved
```

После запуска снова запросите команду (вывод команды должен быть пустой):

```
lsof -i :53
```

Если вывод пустой, значит всё нормально, можно приступать к настройке и запуску bind.

11.2. Базовая настройка bind

Основной конфигурационный файл сервиса bind - named.conf

Откройте этот конфигурационный файл named.conf и для минимальной работы DNS сервера, исправьте следующие строки:

```
options {
        listen-on port 53 { any; };
        listen-on-v6 port 53 { any; };
        . . . . .
        allow-query     { any; };
```

где:

- listen-on port 53 { any; }; - пропишите параметр any для прослушивания на всех ip хоста;
- listen-on-v6 port 53 { any; }; - пропишите параметр any для прослушивания на всех ip хоста;
- allow-query { any; }; - разрешаем запросу отовсюду к нашему серверу.

После правки конфигурационного файла, можно запустит bind:

```
systemctl start named.service
```

Далее проверьте какие службы прослушивают 53 порт:

```
lsof -i :53
```

```
dc1 ~ #
dc1 ~ # lsof -i :53
COMMAND   PID  USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
named   38550 named   21u  IPv6  82860      0t0  TCP *:domain (LISTEN)
named   38550 named   22u  IPv4  82864      0t0  TCP localhost.localdomain:domain (LISTEN)
named   38550 named   23u  IPv4  82866      0t0  TCP dc1.testipa.dom:domain (LISTEN)
named   38550 named  512u  IPv6  82858      0t0  UDP *:domain
named   38550 named  513u  IPv4  82863      0t0  UDP localhost.localdomain:domain
named   38550 named  514u  IPv4  82865      0t0  UDP dc1.testipa.dom:domain
dc1 ~ #
```

Рис. 42. Вывод команды lsof -i :53

Если прописан параметр named, то все настроили правильно.

Далее необходимо проверить как работает DNS сервер с помощью команды:

```
dig @127.0.0.1 yandex.ru
```

Или

```
nslookup yandex.ru
```

Должны быть выведены IP адреса yandex.ru.

Также следует включить DNS сервис в автозагрузку.

```
systemctl enable named.service
```

11.3. Настройка Forward DNS сервера bind

Чтобы настроить bind для перенапрваления (forward) запросов к другим DNS серверам, выполните следующие шаги.

Откройте конфигурационный файл named.conf и для минимальной работы DNS сервера, исправьте следующие строки:

```
options {
        . . . . .
        recursion yes;
        . . . . .
        forward only;
        forwarders {
                77.88.8.8;
                77.88.8.1;
        };
```

где:

- forward - режим перенаправления
  1) forward only; - если ставить параметр only указывая, тем самым, что все запросы на наш DNS сервер будут перенаправляться на другие DNS сервера, прописанные в следующей опции forwarders {}
  2) forward first; - если ставить параметр first указывая, тем самым, что все запросы на наш DNS сервер будут перенаправляться на другие DNS сервера, прописанные в следующей опции forwarders {}, и если с помощью них не удастся разрешить запрос, то запрос будет пытать разрешаться нашим DNS сервером локально
- forwarders { 77.88.8.8; 77.88.8.1; }; - список DNS серверов, для перенаправления запросов

11.4. Настройка кеширующего DNS сервера bind

Чтобы настроить bind как кеширующий сервер DNS, выполните следующие шаги.

Откройте конфигурационный файл named.conf и для минимальной работы DNS сервера, исправьте следующие строки:

```
acl my_allowed {
        192.168.100.0/24;
        217.71.222.0/24;
        localhost;
};
options {
        listen-on port 53 { any; };
        listen-on-v6 port 53 { any; };
        directory       "/var/named";
        . . . . .
        allow-recursion { my_allowed; };
        allow-query     { my_allowed; };
        allow-transfer { none; };
        recursion yes;
        . . . . .
```

где:

- acl my_allowed - это ACL список доступа к нашему DNS серверу;
- my_allowed - название списка доступа. Выполнить данные действия необходимо для того, чтобы не разрешить злоумышленникам проводить расширенные DNS атаки на ваш кеширующий сервер.
- allow-recursion { my_allowed; }; - Определяет хосты, с которых разрешаются рекурсивные запросы
- allow-query { my_allowed; }; - Указывает, каким хостам разрешено делать запросы у сервера DNS
- allow-transfer { none; }; - Указывает, каким вторичным серверам разрешено делать запросы в нашей зоне.

После правки конфигурационного файла, запустите DNS сервер:

```
systemctl start named.service
```

В файле описана базовая настройка и конфигурация DNS сервера, настройки безопасности, настройки прослушивания других IP, настройка зон и т.д. Это все индивидуально.

12. ZABBIX

В данном разделе рассмотрим установку и особенности первоначальной настройки системы Zabbix для ОС м 12. Обратите внимание, что полная инструкция по настройке и всем возможным вариантам работы системы приведена в официальной документации разработчика по адресу https://www.zabbix.com/documentation/5.0/ru/manual.

Данная инструкция заменяет раздел "Установка" для ОС РОСА ХРОМ 12 из официальной документации.

Все описанные в инструкции действия выполняются от пользователя root, если не указано иное.

Настройках всех возможных конфигураций не рассматривается, рассмотрена следующая типовая конфигурация сервера с Zabbix:

- сервер Zabbix
- веб-интерфейс через веб-сервер Apache HTTPD
- база данных MySQL (MariaDB)

Также рассмотрена типовая настройка агента Zabbix.

Развертывание системы рекомендуется выполнять в отдельной виртуальной машине, которую можно сделать на основе серверного образа ROSA или в контейнере на основе rootfs. Доступные сборки rosa2021.1 можно найти здесь: https://abf.io/platforms/rosa2021.1/products

12.1. Сервер Zabbix

Для минимальной настройки сервера выполните следующие шаги.

Установите необходимые пакеты:

```
dnf install zabbix-server zabbix-server-mysql zabbix-web zabbix-web-mysql mariadb locales-ru
```

Это установит сервер Zabbix, веб-интерфейс Zabbix, компоненты для использованияч MySQL в качестве базы данных и саму базу данных — MariaDB (форк MySQL).

Установите имя хоста (это делать не обязательно, но рекомендуется), например:

```
hostnamectl set-hostname zabbix.infrastructure.dumalogiya.ru
```

Можно установить FQDN имя хоста, которое затем будет резолвится через ваш DNS-сервер. В приведенном примере на DNS-сервере, обслуживающем домен

dumalogiya.ru, будет добавлена A-запись zabbix.infrastructure.dumalogiya.ru, указывающая на необходимый IP-адрес. Это позволит иметь доступ к серверу из внешней сети. Будьте осторожны с открытием доступа из внешней сети, возможно, стоит настроить firewall и использовать VPN.

12.1.1. Настройка базы данных MySQL

Произведите тестовый запуск базы данных:

```
systemctl start mariadb
```

Убедитесь, что она запустилась без ошибок:

```
systemctl status mariadb
```

При ее первом запуске будут созданы файлы в /var/lib/mysql.

Добавьте базу данных в автозапуск:

```
systemctl enable mariadb
```

Запустите скрипт первоначальной настройки БД:

```
mysql_secure_installation
```

Ниже приведен вывод скрипта с комментариями к задаваемым им вопросам. Для ответа на вопросы нужно ввести Y для утвердительного или N для отрицательного ответа и нажать Enter.

```
[root@rosa-2019 ~]# /usr/bin/mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL
MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter
here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...
```

Для подтверждение необходимо просто нажать клавишу Enter.

```
Setting the root password or using the unix_socket ensures that
nobody
can log into the MariaDB root user without the proper authorisation.
```

```
 You already have your root account protected, so you can safely
answer 'n'.

 Switch to unix_socket authentication [Y/n] y
```

Далее запрашивается необходимо ли на время первоначальной настройки запретить авторизацию для подключений по сети? Введите параметр «y» – согласитесь с запросом.

```
 Enabled successfully!
 Reloading privilege tables..
  ... Success!



 You already have your root account protected, so you can safely
answer 'n'.

 Change the root password? [Y/n]
```

Выводиться запрос: хотим ли мы поставить root-пароль MySQL. Обратите внимание, что это пароль пользователя root внутри MySQL, но не в ОС. С Запросом также необходимо согласиться – ввести «y».

```
 New password:
 Re-enter new password:
```

Далее 2 раза вводим придуманный пароль. Создать случайный пароль можно, например, так:

```
 head -c 100 /dev/random | base64 | head -c 20
```

Запишите установленный пароль в безопасное место, например, в базу данных Keepass с помощью доступной в репозиториях ROSA графической программы KeepassXC (пакет keepassxc).

```
 Password updated successfully!
 Reloading privilege tables..
  ... Success!



 By default, a MariaDB installation has an anonymous user, allowing
anyone
```

```
 to log into MariaDB without having to have a user account created
for
 them.   This is intended only for testing, and to make the
installation
 go a bit smoother.  You should remove them before moving into a
 production environment.

 Remove anonymous users? [Y/n] y
```

Предлагается удалить существующего из коробки анонимного пользователя. Он не нужен. Необходимо согласиться с запросом.

```
  ... Success!

 Normally, root should only be allowed to connect from 'localhost'.
This
 ensures that someone cannot guess at the root password from the
network.

 Disallow root login remotely? [Y/n] y
```

Предлагается запретить входить в MySQL под root по сети. Также соглашаемся с запросом.

```
  ... Success!

 By default, MariaDB comes with a database named 'test' that anyone
can
 access.  This is also intended only for testing, and should be
removed
 before moving into a production environment.

 Remove test database and access to it? [Y/n] y
```

Далее предлагается удалить пустую базу данных с публичным доступом. Соглашаемся.

```
  - Dropping test database...
  ... Success!
  - Removing privileges on test database...
  ... Success!
```

```
 Reloading the privilege tables will ensure that all changes made
so far
 will take effect immediately.

 Reload privilege tables now? [Y/n] y
```

Предлагается перезагрузить таблицы привилегий, чтобы гарантировать вступление изменений в силу. Соглашаемся.

```
  ... Success!

 Cleaning up...

 All done!  If you've completed all of the above steps, your MariaDB
 installation should now be secure.

 Thanks for using MariaDB!
```

Работа скрипта первоначальной настройки MySQL закончена.

Теперь, согласно документации Zabbix (https://www.zabbix.com/documentation/5.0/ru/manual/appendix/install/db_scripts#mysql), произведем настройки базы данных для системы.

Войдем в консоль MySQL под пользователем root:

```
mysql -uroot -p
```

Далее система запросит пароль, введите ранее установленный пароль root для MySQL.

Создадим базу данных для Zabbix:

```
create database zabbix character set utf8 collate utf8_bin;
```

Теперь создадим пользователя базы данных и дадим ему доступ к ней:

```
grant all privileges on zabbix.* to zabbix@localhost identified by
'пароль';
```

Пароль можно создать уже приводившейся выше командой, которую можно выполнить в другой консоли:

```
head -c 100 /dev/random | base64 | head -c 20
```

Сохраните созданный пароль.

Выйдите из консоли MySQL:

```
quit;
```

Перейдите в папку, в которой хранится стандартное наполнение БД Zabbix, которым нужно наполнить базу данных до начала работы с ней:

```
cd /usr/share/zabbix-mysql
```

Импортируйте дамп базы данных:

```
mysql -uzabbix -p'пароль' zabbix < schema.sql
```

Вместо "пароль" укажите установленный ранее пароль пользователя MySQL "zabbix".

Аналогично выполните еще 2 SQL-запроса:

```
mysql -uzabbix -p'пароль' zabbix < images.sql
mysql -uzabbix -p'пароль' zabbix < data.sql
```

Обратите внимание, что пароль внутри использованных команды сохранился в логах консоли. Очистите историю bash:

```
history -cw
```

И историю MySQL:

```
rm -fv ~/.mysql_history
```

Если в процессе настройки базы данных что-то пошло не так, можно удалить всё и начать заново:

```
systemctl stop mariadb
rm -fvr /var/lib/mysql/*
systemctl start mariadb
```

И далее mysql_secure_installation по инструкции выше.

Создайте резервную копию файла конфигурации:

```
cp -v /etc/zabbix/zabbix_server.conf /etc/zabbix/zabbix_server.conf.orig
```

Откройте файл в nano или любом другом текстовом редакторе:

```
nano /etc/zabbix/zabbix_server.conf
```

В файле необходимо замените строку

```
# DBPassword=
```

на:

```
DBPassword=пароль
```

где вместо "пароль" укажите пароль пользователя MySQL "zabbix".

Рекомендуется также заменить стандартный порт на любой другой, чтобы меньше ботов пытались сканировать сервер. Для этого замените строку

```
# ListenPort=10051
```

на:

```
ListenPort=15889
```

где вместо 15889 — любое число от 1024 до 32767.

Посмотрите отличия между исходным файлом и тем, что получилось после редактирования:

```
diff -u --color /etc/zabbix/zabbix_server.conf.orig /etc/zabbix/zabbix_server.conf
```

Запустите сервер Zabbix в варианте для работы с MySQL:

```
systemctl start zabbix-server-mysql
```

Убедитесь, что он запустился успешно:

```
systemctl status zabbix-server-mysql
```

Добавьте его в автозапуск:

```
systemctl enable zabbix-server-mysql
```

12.1.2. Настройка веб-интерфейса

Разворачивание веб-интерфейса

Предыдущий шаг был закончен на запуске демона Zabbix. Теперь необходимо запустить веб-интерфейс, через который будет произведена первичная настройка сервера.

Работа веб-интерфейса обеспечивается с помощью PHP и веб-сервера Apache HTTPD, конфигурационный файл находится по адресу /etc/httpd/conf.d/zabbix.conf. Для работы в типовой конфигурации его править не нужно. То, что необходимо для работы, будет уже установлено по зависимостям пакетов из репозитория.

Проверьте правильность настройки часового пояса на сервере:

```
timedatectl
```

Если часовой пояс неверный, то найдите свой в списке по команде:

```
timedatectl list-timezones
```

Затем установите его:

```
timedatectl set-timezone Europe/Moscow
```

(вместо "Europe/Moscow введите нужный часовой пояс)

Настройте часовой пояс в интерпретаторе PHP, например:

```
echo "php_value date.timezone $(timedatectl show -p Timezone | awk -F '=' '{print $NF}')" > /etc/httpd/conf.d/timezone.conf
```

Проверьте, что получилось:

```
cat /etc/httpd/conf.d/timezone.conf
```

Пример правильного вывода:

```
php_value date.timezone Europe/Moscow
```

Произведите пробный запуск веб-сервера Apache HTTPD:

```
systemctl start httpd
```

Убедитесь, что он запустился успешно:

```
systemctl status httpd
```

Добавьте сервер в автозапуск:

```
systemctl enable httpd
```

Посмотрите адрес сервера с помощью команды

```
ip a
```

И откройте в браузере адрес http://server/zabbix/setup.php.

Например:

http://192.168.122.71/zabbix/setup.php

http://localhost/zabbix/setup.php

Обратите внимания, что до завершения настройки не рекомендуется делать сервер доступным из внешней сети.

Обратите внимание, что поставляемый в составе пакета из репозитория конфигурационный файл для Apache HTTPD /etc/httpd/conf.d/zabbix.conf настраивает Apache HTTPD так, чтобы открывать Zabbix при любом обращении к веб-серверу по адресу "/zabbix", независимо от домена. В конфигурации, по ходу разворачивания которой пишется настоящая инструкция, Zabbix работает в отдельном контейнере systemd-nspawn на базе rootfs rosa2019.1, доступ из внешней сети будет осуществляться через прокси средствами nginx, работающего на другом сервере, благодаря чему правки конфигов не понадобятся.

Ниже приведен скриншот с веб-страницей, которую вы должны увидеть:

Рис. 43. Настройка сервера Zabbix

Нажмите кнопку «Next step» для перехода к следующему шагу. Будет произведена проверка параметров и модулей PHP.

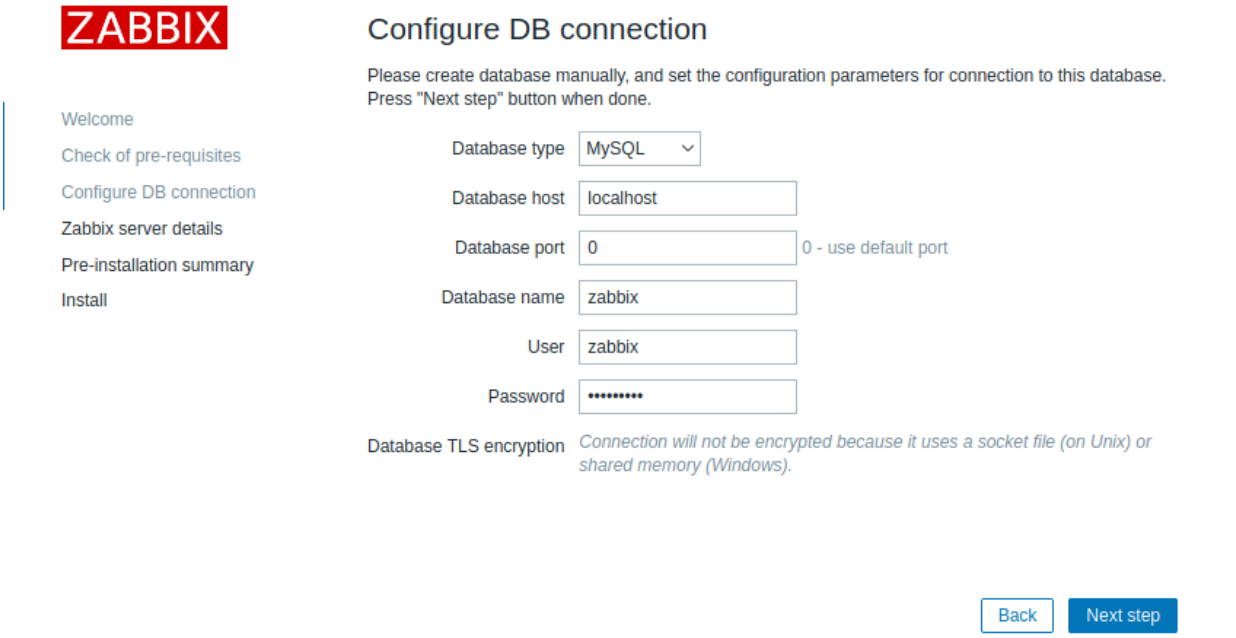

Рис. 44. Настройка подключения БД

В поле «Password» вставьте пароль от пользователя MySQL «zabbix», остальные поля оставьте без изменения и нажмите «Next step».

На шаге «Zabbix server details» рекомендуется изменить порт по умолчанию 10051 на иное значение, указанное ранее в конфиге сервера Zabbix (в этой инструкции было приведено значение 15889 в качестве примера).

По окончанию настройки будет выдано сообщение:

```
Congratulations! You have successfully installed Zabbix frontend.
Configuration file "/etc/zabbix/web/zabbix.conf.php" created.
```

Нажмите кнопку «Finish» для завершения установки. Вас переадресует на экран входа в систему:

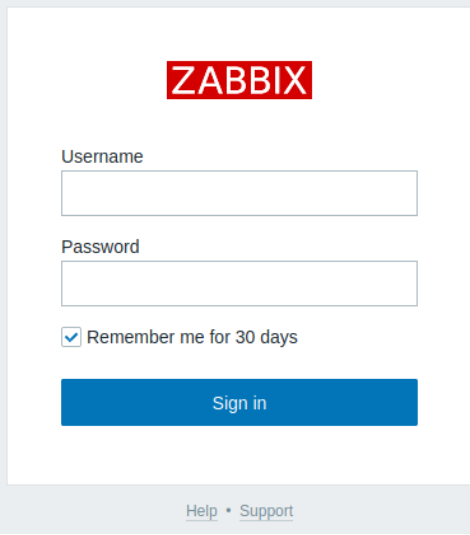

Рис. 45. Экран входа пользователя в систему Zabbix

Войдите с помощью стандартных логина и пароля: Логин: Admin Пароль: zabbix

Откроется веб-интерфейс, показанный на скриншоте ниже (Рис. 46).

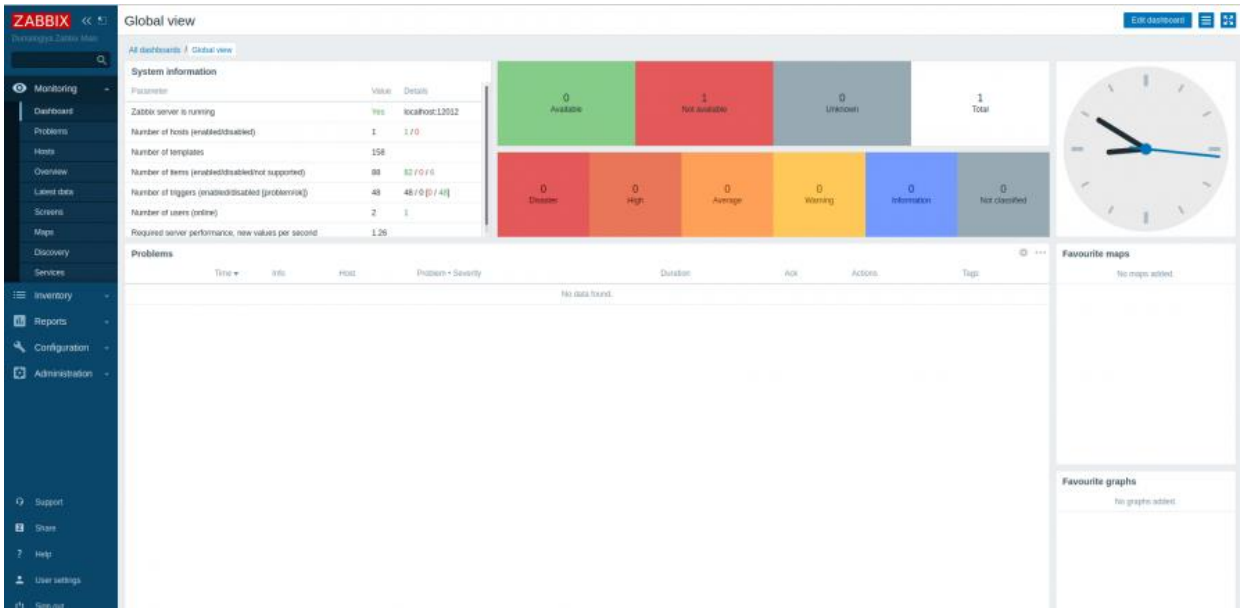

Рис. 46. Интерфейс агента Zabbix

Обратите внимание, что напротив параметра «Zabbix server is running» написано «YES». Если вы видите значение «NO», то значит веб-интерфейс не смог соединиться с демоном, возможно, вы перепутали порт. Тогда нужно синхронизировать порты в файлах /etc/zabbix/web/zabbix.conf.php и /etc/zabbix/zabbix_server.conf и перезапустить сервер:

```
systemctl restart zabbix-server-mysql
```

Узнать, что на каком порту работает, можно так:

```
ss -ntulp
```

Перейдите в раздел «User settings» в левом нижнем углу экрана (http://server/zabbix/zabbix.php?action=userprofile.edit) и при необходимости смените язык интерфейса на русский. После нажатия на кнопку "Update" интерфейс обновится на русский.

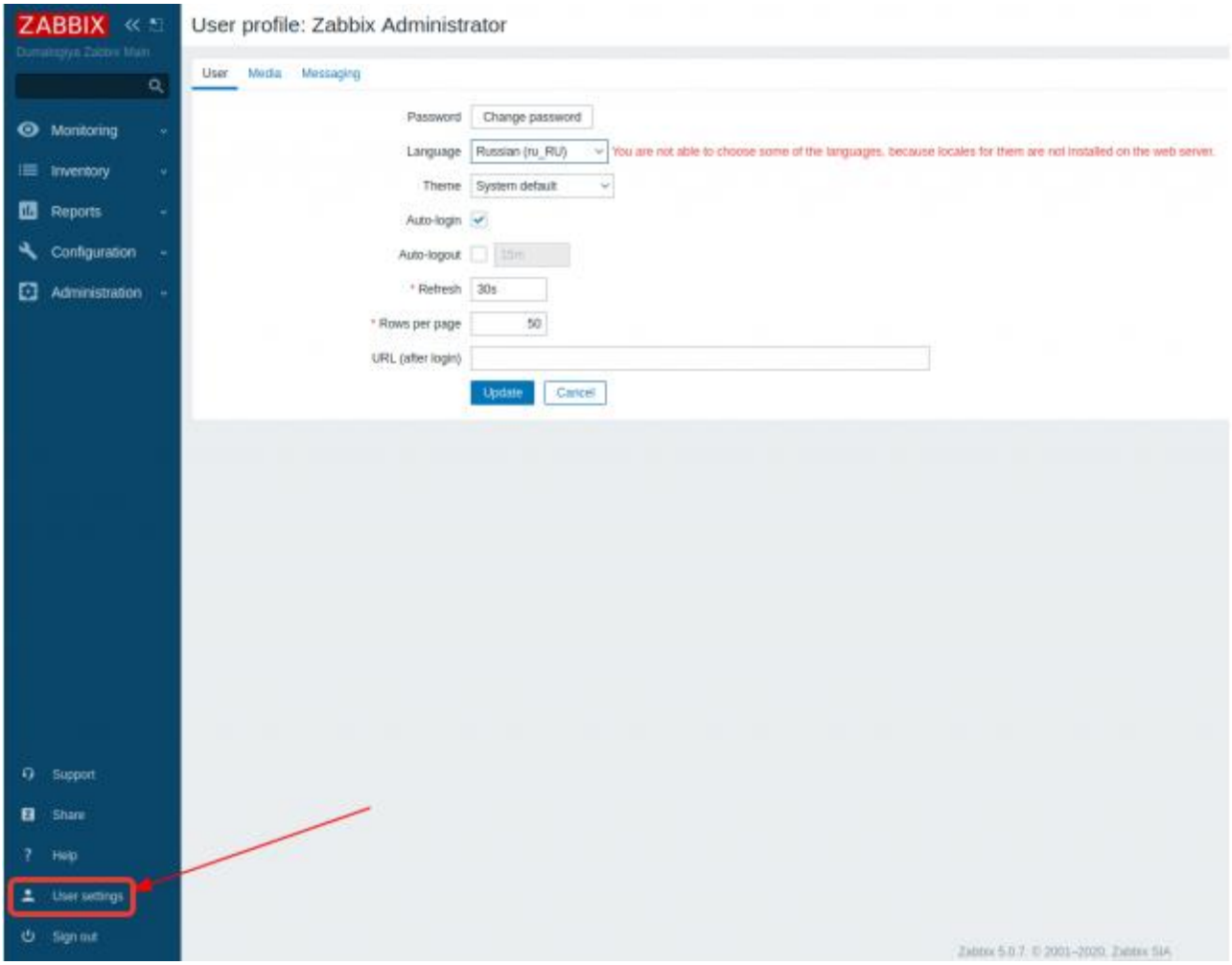

Рис. 47. Пользовательские настройки Zabbix

Обратите внимание, что должен быть установлен пакет locales-ru, аналогично для других языков.

Далее необходимо убрать возможность входить в панель администрирования под стандартным пользователем. Суть в том, чтобы создать нового пользователя и отключить стандартного.

Пошагово следуйте инструкции:

1. Перейдите в «Администрирование» → «Пользователи» (http://server/zabbix/zabbix.php?action=user.list)
2. Справа вверху нажмите «Создать пользователя»
3. В открывшемся разделе добавления пользователя перейдите во вкладку «Права доступа»

4. Установите «Тип пользователя» - «Zabbix Супер Администратор»
5. Во вкладке "Пользователь" добавьте группу «Zabbix administrators»
6. Заполните остальные поля
7. Нажмите «Добавить»
8. Слева внизу нажмите «Выход». Вас перенаправит на экран входа в систему. Войдите под только что созданным новым пользователем.
9. Перейдите в «Администрирование» → «Пользователи» (http://server/zabbix/zabbix.php?action=user.list)
10. Нажмите на пользователя «Admin»
11. В открывшемся разделе редактирования пользователя в поле «Группы» удалите группу «Zabbix administrators» и добавьте группу «Disabled»
12. Нажмите «Обновить» для сохранения изменений

Теперь под стандартными пользователем и паролем нельзя войти в систему.

При необходимости настройте firewall, VPN.

Теперь сервер Zabbix готов к работе. Следующий шаг — настройка мониторинга узлов. Если веб-интерфейс Zabbix будет доступен из глобальной сети, рекомендуется настроить шифрование трафика (HTTPS) по инструкции ниже.

12.1.3. Настройка HTTPS и сертификата Letsencrypt

В этом разделе описана настройка TLS-шифрования, то есть работы по протоколу HTTPS, с получением бесплатного сертификата от Letsencrypt. Для этого нужно:

- иметь настроенный DNS: доменное имя, на которое будет выдаваться сертификат, должно преобразовываться в IP-адрес на публичных DNS
- корень домена должен быть доступен из внешней сети (при этом путь /zabbix может быть недоступен, его доступность не требуется для получения сертификата)

Установите необходимые пакеты:

```
dnf install certbot python3-certbot-apache
```

Создайте файл /etc/httpd/conf.d/zabbix-vhost.conf со следующим текстом:

```
<VirtualHost *:80>
  ServerName zabbix.infrastructure.dumalogiya.ru
  ServerAlias www.zabbix.infrastructure.dumalogiya.ru
</VirtualHost>
```

Здесь и далее вместо zabbix.infrastructure.dumalogiya.ru ваш домен.

Перезагрузите конфигурацию Apache HTTPD:

```
systemctl reload httpd
```

Проверьте, что по адресу http://zabbix.infrastructure.dumalogiya.ru/zabbix открывается веб-интерфейс Zabbix.

Запустите процесс получения сертификата:

```
certbot --apache -d zabbix.infrastructure.dumalogiya.ru
```

В процессе будет задано несколько вопросов, отвечая на них, обратите внимание, что адрес электронной почты желательно ввести правильный, действительно существующий.

Если в процессе получения сертификата не возникло ошибок, проверьте, что по адресу https://zabbix.infrastructure.dumalogiya.ru/zabbix открывается веб-интерфейс Zabbix.

Настройте автоматическую переадресацию с http:// на https://, дописав соответствующие инструкции в файл /etc/httpd/conf.d/zabbix-vhost.conf, который приобретет следующий вид:

```
<VirtualHost *:80>
  ServerName zabbix.infrastructure.dumalogiya.ru
  ServerAlias www.zabbix.infrastructure.dumalogiya.ru
RewriteEngine on
RewriteCond %{SERVER_NAME}
=www.zabbix.infrastructure.dumalogiya.ru [OR]
RewriteCond %{SERVER_NAME} =zabbix.infrastructure.dumalogiya.ru
RewriteRule         ^         https://%{SERVER_NAME}%{REQUEST_URI}
[END,NE,R=permanent]
</VirtualHost>
```

Также будет автоматически создан файл /etc/httpd/conf.d/zabbix-vhost-le-ssl.conf следующего вида:

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
  ServerName zabbix.infrastructure.dumalogiya.ru
  ServerAlias www.zabbix.infrastructure.dumalogiya.ru
```

```
 SSLCertificateFile
/etc/letsencrypt/live/zabbix.infrastructure.dumalogiya.ru/fullchai
n.pem
 SSLCertificateKeyFile
/etc/letsencrypt/live/zabbix.infrastructure.dumalogiya.ru/privkey.
pem
 Include /etc/letsencrypt/options-ssl-apache.conf
 </VirtualHost>
 </IfModule>
```

Включите автоматическое продление сертификата:

```
 systemctl enable --now certbot-renew.timer
```

Узнать состояние работы службы продления можно так:

```
 systemctl status certbot-renew.timer certbot-renew.service
```

Веб-сервер Apache HTTPD в ОС РОСА ХРОМ 12 поддерживает работу по ГОСТ TLS (т.е. с шифрованием по ГОСТ). В файле /usr/share/doc/apache-mod_ssl/README.GOST (веб-версия: https://abf.io/import/apache/blob/rosa2021.1/README.GOST) описано, как его настроить. Обратите внимание, что Letsencrypt не поддерживает криптографию по ГОСТ, вам придется выпускать сертификаты иным образом, например, создавая их самостоятельно, как описано в этом файле.

12.2. Агент Zabbix

Агентом Zabbix называется программное обеспечение, устанавливаемое на узел мониторинга, за которым нужно следить. Агент Zabbix передает информацию на сервер Zabbix.

Существуют различные способы установки связи между агентом и сервером, автоматические и ручные способы добавления узла с агентом на сервер. Они рассмотрены в официальной документации: https://www.zabbix.com/documentation/5.0/ru/manual/concepts/agent

При организации связи между агентом и сервером Zabbix по сети важно учесть, что часть способов связи не имеют авторизации и/или шифрования, а потому не должны использоваться вне защищенного доверенного контура сети. Выше была рассмотрена настройка сервера Zabbix с доступом по глобальной сети. Приведем пример связности агента с сервером по глобальной сети с авторизацией и

шифрованием. Пример применения такой схемы: агент установлен на ноутбуке, который может находиться не только в офисе и сети компании. Агент будет сам связываться с сервером и передавать ему данные (возможно наоборот), что избавит от необходимости пробивать NAT.

12.2.1. Установка агента Zabbix в ОС ROSA

Сервер Zabbix в ОС ROSA может использоваться с агентами на других дистрибутивах и ОС, и наоборот. Для установки агента Zabbix на ROSA выполните:

```
dnf install zabbix-agent openssl
```

Для установки на другие ОС обратитесь к документации по ОС и ее репозиторию или найдите сборку агента на официальном сайте Zabbix: https://www.zabbix.com/ru/download_agents

12.2.2. Настройка межсетевого экрана для агента Zabbix

Мы организовываем связь агента и сервера по глобальной сети с авторизацией, однако в любом программном обеспечении, в частности в реализации авторизации, теоретически возможны ошибки, поэтому лучше поставить дополнительную защиту, запретив межсетевым экраном (фаерволом) связь агента с любыми другими серверами, кроме нашего. Ниже приведен пример настройки, если вы разбираетесь в вопросе, настройте межсетевой экран по своему усмотрению или опустите этот шаг.

На системе с установленным агентом Zabbix выполните:

```
EDITOR=nano systemctl edit zabbix-agent.service
```

Вставьте следующий текст:

```
[Service]
IPAccounting=yes
IPAddressDeny=any
IPAddressAllow=81.176.226.156
IPAddressAllow=127.0.0.0/8
```

Замените 81.176.226.156 на IP-адрес своего сервера Zabbix. Сохраните изменения в файле (Ctrl+O, Enter, Ctrl+X).

12.2.3. Настройка агента

Теперь создадим уникальный для данного агента ключ:

```
sh -c 'umask 0077 && openssl rand -hex 64 > /etc/zabbix/zabbix_agentd.d/psk'
chown zabbix:zabbix /etc/zabbix/zabbix_agentd.d/psk
```

Командой

```
stat /etc/zabbix/zabbix_agentd.d/psk
```

убедитесь, что файл имеет права 0600 и принадлежит пользователю zabbix, группе zabbix. Таким образом этот секретный ключ не может быть прочитан без root-прав извне Zabbix-агента.

Далее создадим файл с настройками Zabbix-агента, настройки из которого будут приоритетнее настроек в /etc/zabbix/zabbix_agentd.conf:

```
nano /etc/zabbix/zabbix_agentd.d/10-duma.conf
```

(вместо "10-duma.conf" можете придумать свое имя файла) со следующим содержимым (задайте свои значения параметров):

```
# уникальное человекопонятное имя узла мониторинга
Hostname=nickel-builder-1.rosalinux.ru
# сетевой порт агента Zabbix
ListenPort=15888
# авторизация по ключу и шифрование трафика
TLSConnect=psk
TLSAccept=psk
# уникальный произвольный текст-пароль (замените на свой!)
TLSPSKIdentity=Change to your text blablabla
TLSPSKFile=/etc/zabbix/zabbix_agentd.d/psk
# адрес и порт сервера Zabbix
#ServerActive=zabbix.infrastructure.dumalogiya.ru:15889
ServerActive=81.176.226.156:15889
# работаем только в активном режиме
# (не принимаем входящих соединений с сервера)
Server=
StartAgents=0
# запрещаем выполнение произвольных команд, поступивших с сервера,
# для защиты от компроментации системы с агентом в случае взлома
сервера
DenyKey=system.run[*]
```

Сделайте файл доступным для чтения агенту Zabbix, работающему от пользователя Zabbix:

```
chmod 0644 /etc/zabbix/zabbix_agentd.d/10-duma.conf
```

Обратите внимание, что выше предложено указать ServerActive IP-адресом, а не DNS-именем. Дело в том, что мы запретили подключения к любым серверам, кроме локальной петли и указанных. В зависимости от настроек в /etc/nsswitch.conf и /etc/resolv.conf, для резолва имен DNS может потребоваться доступ к DNS-серверу, который не внесен в список разрешенных. При использовании systemd-resolved (по умолчанию в rosa2021.1) такой проблемы нет, так как резолв DNS производится по D-BUS с DNS-сервером на локальной петле в качестве запасного варианта, а значит адрес сервера можно указать именем DNS.

ListenPort не имеет смысла при отключенных пассивных проверках, когда агент сам соединяется с сервером (StartAgents=0).

Пока не будем запускать агент, сначала добавим узел на сервере.

12.2.4. Добавление узла мониторинга

Добавим агент на сервер Zabbix. Обратите внимание, что мы рассматриваем лишь один из множества возможных вариантов настройки. Zabbix умеет и автоматически обнаруживать узлы сети (агенты).

В веб-интерфейсе Zabbix под пользователем-администратором или с иными необходимыми правами зайдите в «Настройка» → «Узлы сети»

Справа вверху нажмите: "Создать узел сети". Откроется страница как показана на Рис. 48.

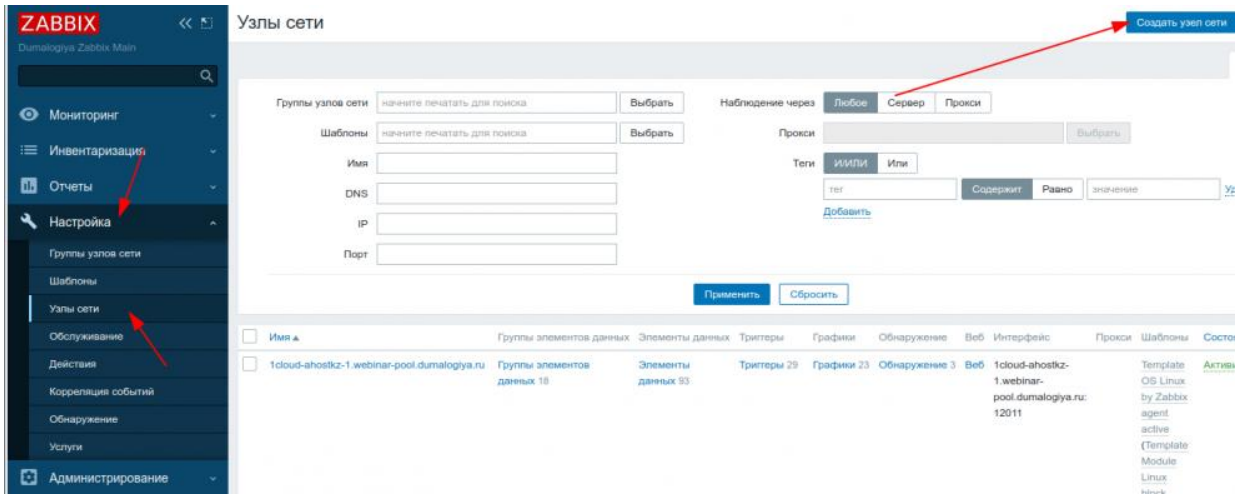

Рис. 48. Создание узлов сети

Заполните имя узла (как Hostname в настройках агента) и добавьте узел в хотя бы одну группу, например, «Linux servers».

Поменяйте порт на значение «ListenPort» в настройках агента (Рис. 49).

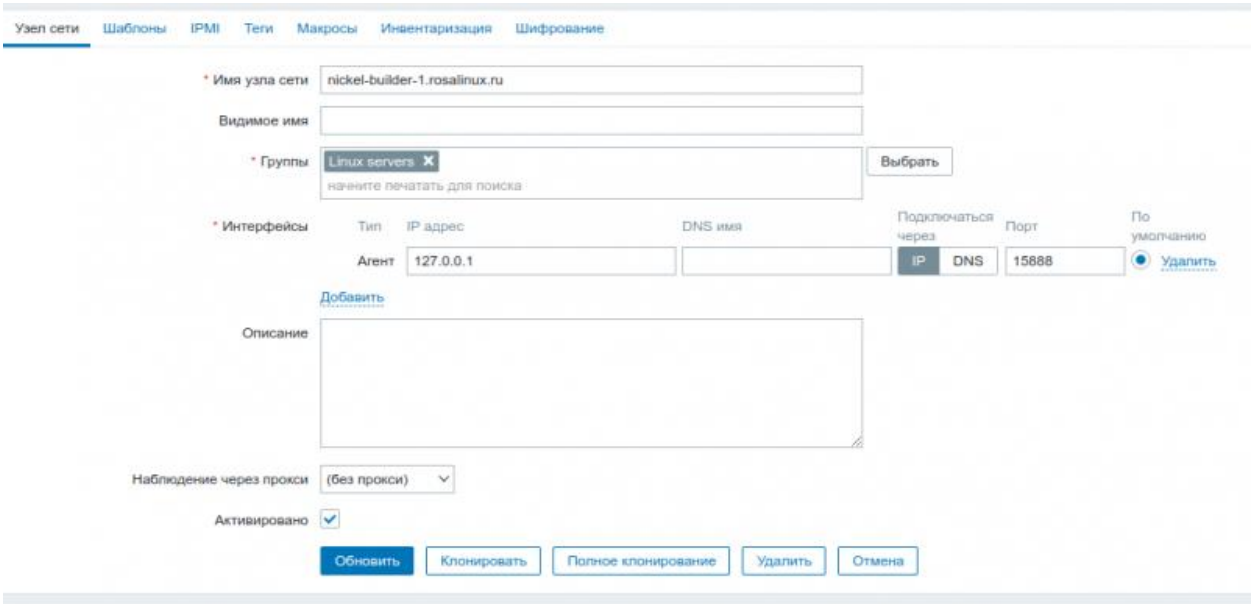

Рис. 49. Настройки узла сети

Перейдите во вкладку «Шаблоны». Отметьте галкой шаблон «Template OS Linux by Zabbix agent active» и нажмите «Выбрать» (Рис. 50).

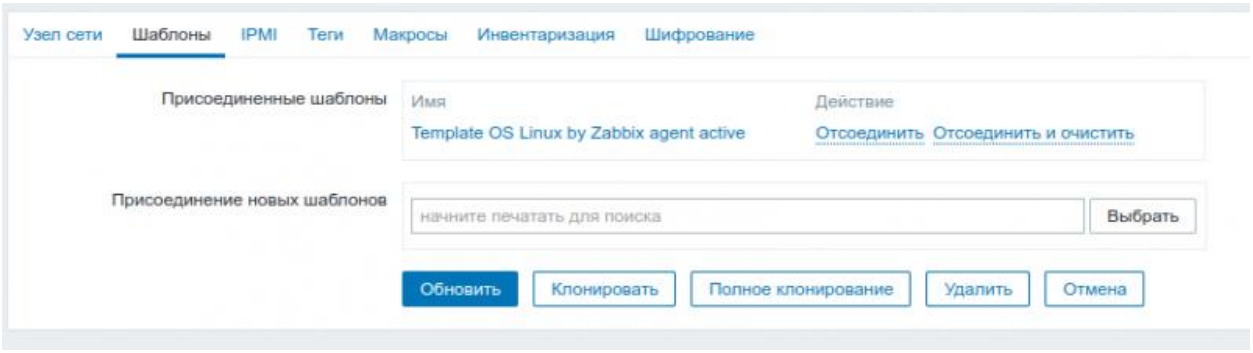

Рис. 50. Настройка шаблонов агента

Перейдите во вкладку «Шифрование». В разделе «Подключения к узлу сети» выберите "PSK" (но мы настроили агент так, чтобы только он сам мог подключаться к серверу, поэтому настройки, как сервер будет подключаться к агенту, в приведенном случае не играют роли).

В разделе «Соединения с узла сети» снимите галку «Без шифрования» и поставьте галку «PSK».

В поле «Идентификатор PSK» вставьте значение поля TLSPSKIdentity из настройки агента (своё, уникальное, не копируйте его из этой инструкции). В поле «PSK» вставьте вывод команды:

```
cat /etc/zabbix/zabbix_agentd.d/psk
```

(то есть ранее созданный уникальный ключ).

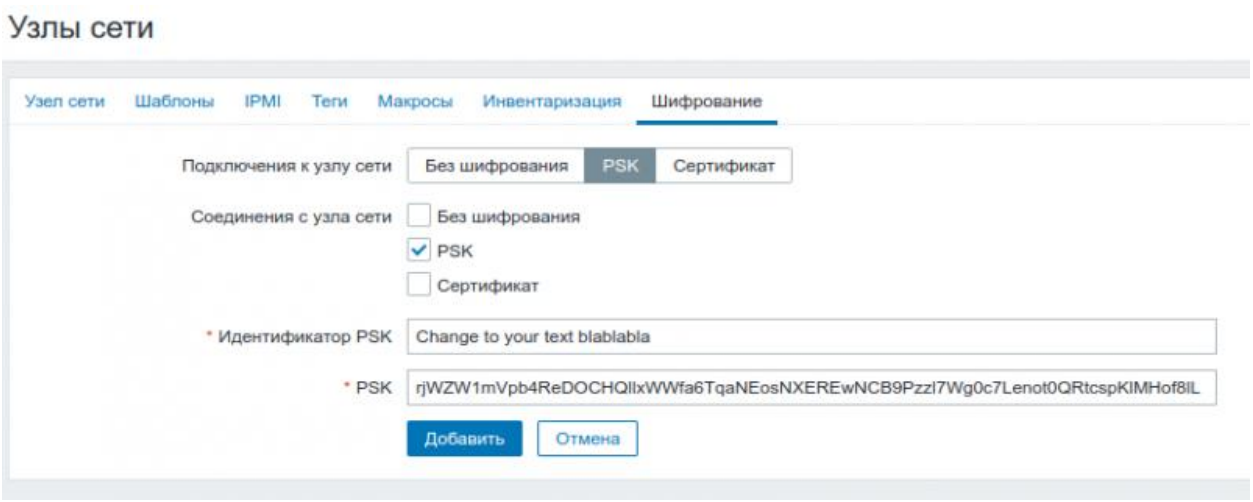

Рис. 51. Соединение с узлами сети

Нажмите "Добавить" для добавления узла мониторинга.

Теперь запустим и добавим в автозапуск агент Zabbix на нашем узле:

```
systemctl enable --now zabbix-agent
```

Убедимся, что он запустился без ошибок:

```
systemctl status zabbix-agent
```

Проверим, что в логе не сказано про ошибки соединения с сервером и др.:

```
tail /var/log/zabbix/zabbix_agentd.log
```

Через некоторое время в разделе «Мониторинг» → «Узлы сети» можно будет ознакомиться с данными с добавленного узла.

13. KUBERNATES

Kubernates – это открытое программное обеспечение для автоматизации развёртывания, масштабирования и управления контейнеризированными приложениями.

Установка kubernates master-node

1. Установка всех зависимостей kubernates:

```
# dnf install -y kubelet kubeadm kubectl docker docker-containerd
```

2. Запуск и добавление в автозагрузку сервисов:

```
# systemctl enable kubelet
# systemctl start kubelet
```

3. Добавляем узлы в hosts (master,worker):

```
# hostnamectl set-hostname master-node
# vi /etc/hosts
10.45.4.58 master-node
10.45.4.59 worker-node
```

4. Отключаем swap

```
#sed -i '/swap/d' /etc/fstab
#swapoff -a
```

5. Инициализация kubernates

```
#kubeadm init
```

6. Установщик даст токен подключения к master node, у вас будет свой токен подключения

```
kubeadm join 10.45.4.58:6443 --token ncb63c.pugf9xehkjakptqp --discovery-token-ca-cert-hash sha256:73cb40755a49b40f2a724984392f32fd7ff607a437da524619d4aba43a2c31b6
```

7. Создаем каталоги нужные для kubernates

```
# mkdir -p $HOME/.kube
# cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
# chown $(id -u):$(id -g) $HOME/.kube/config
# export kubever=$(kubectl version | base64 | tr -d '\n'
```

8. Добавляем сеть для работоспособности kubernates

```
# kubectl apply -f "https://cloud.weave.works/k8s/net?k8s-version=$kubever"
```

9. Перезагружаем kubernates

```
# systemctl restart kubelet
```

Установка kubernates worker-nodes (pods контейнеры)

1.Устанавливаем docker:

```
# dnf install docker docker-containerd
```

2. Запуск и добавление в автозагрузку сервисов docker

```
# systemctl start docker
# systemctl enable docker
```

3. Установка всех зависимостей kubernates

```
# yum install -y kubelet kubeadm kubectl
```

4. Добавляем в автозагрузку kubernates

```
# systemctl enable kubelet
```

5.Измененяем имя виртуального узла

```
# hostnamectl set-hostname worker-node
```

6.Добавляем узлы в hosts

```
# vi /etc/hosts
10.45.4.58 master-node
10.45.4.59 worker-node
```

7.Отключаем swap

```
#sed -i '/swap/d' /etc/fstab
#swapoff -a
```

8. Присоединяем worker-node к master, токен берем из предыдущего этапа установка master nodes, пункт 7:

```
# kubeadm join 10.45.4.58:6443 --token ncb63c.pugf9xehkjakptqp --discovery-token-ca-cert-hash sha256:73cb40755a49b40f2a724984392f32fd7ff607a437da524619d4aba43a2c31b6
```

9.Перезапуск сервиса

```
# systemctl restart kubelet.service
```

10.Проверка работоспособности Создание deployment

```
# vi deploy.yml
apiVersion : apps/v1            #версия api
kind: Deployment                #Принципал deployment
metadata:                       #Метаданные
```

```
   name: my-web-deployment
   labels:
     app : my-k8s-application
 spec:                              #Описание контейнера
   selector:
     matchLabels:
       project: kgb                 #Проект
   template:                        #Шаблон для контейнера
     metadata:
       labels:
         project: kgb
     spec:
       containers:                  #Контейнер
         - name : kgb-web           #Имя контейнера
           image: Debian           #Имидж на котором будет основываться
контейнер
           ports:                    #Порт который нужно пробросить в
хост машину
             - containerPort: 80
```

11.Применение deployment плана

```
 #kubectl apply –f deploy.yml
```

14. DOCKER

Docker — автоматизированное средство управления виртуальными контейнерами. Он решает множество задач, связанных с созданием контейнеров, размещением в них приложений, управлением процессами, а также тестированием ПО и его отдельных компонентов. Docker нужен для более эффективного использование системы и ресурсов, быстрого развертывания готовых программных продуктов, а также для их масштабирования и переноса в другие среды с гарантированным сохранением стабильной работы.

Docker-контейнеры работают в разных средах: локальном центре обработки информации, облаке, персональных компьютерах и других.

Установка и запуск сервиса docker:

```
# dnf install docker docker-containerd docker-compose -y
# systemctl start docker
# systemctl enable docker
```

Подробные инструкции о принципах работы, порядке и этапах создания проектов в Docker приведены на странице Эксплуатация Docker — Rosalab Wiki по адресу http://wiki.rosalab.ru/ru/index.php/%D0%AD%D0%BA%D1%81%D0%BF%D0%BB%D1%83%D0%B0%D1%82%D0%B0%D1%86%D0%B8%D1%8F_Docker .

15. РАБОТА С СЕРВЕРОМ FREEIPA

15.1. Настройка FreeIPA сервера

15.1.1. Подготовка к установке FreeIPA сервера

Для работы FreeIPA сервера необходимо настроить сеть на сервере и имя хоста.

Первым шагом является настройка сети.

- Для примера рассмотрим следующие названия для хоста FreeIPA сервера:
- имя хоста - dc1
- имя домена - testipa.dom

Далее пропишите статические адреса:

- IP адрес 192.168.1.6 — это адрес нашего freeipa сервера
- Маска сети 255.255.255.0 — это маска подсети в котором будет freeipa сервер и рабочие станции
- Шлюз — шлюз по умолчанию 192.168.1.1
- DNS сервер — 192.168.1.1
- DNS поиск домена — testipa.dom

15.1.2. Установка FreeIPA сервера

Установка сервера производится командой:

```
dnf install ipa-server
```

В ходе установки будет загружено порядка 400 пакетов.

Далее запускается непосредственно установка FreeIPA сервера, командой:

```
ipa-server-install
```

Далее следуйте приведенной ниже инструкцией по установке сервера.

```
dc1 / #
dc1 / # ipa-server-install

The log file for this installation can be found in /var/log/ipaserver-install.log
==============================================================================
This program will set up the FreeIPA Server.
Version 4.8.10

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]: _
```

Рис. 52. Запрос о настройке DNS севера

Установщик запрашивает, хотим ли мы настроить DNS север на нашем FreeIPA сервере? Необходимо ответить YES.

```
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 [dc1.testipa.dom]:

Warning: skipping DNS resolution of host dc1.testipa.dom
The domain name has been determined based on the host name.

Please confirm the domain name [testipa.dom]:

The kerberos protocol requires a Realm name to be defined.
This is typically the domain name converted to uppercase.

Please provide a realm name [TESTIPA.DOM]:
```

Рис. 53. Запрос о названии для хоста, домена и realm

Далее установщиком будут заданы вопросы о наименовании хоста, домена и realm. В данном случае для примера рассматриваем следующие: dc1.testipa.dom/testipa.dom/TESTIPA.DOM

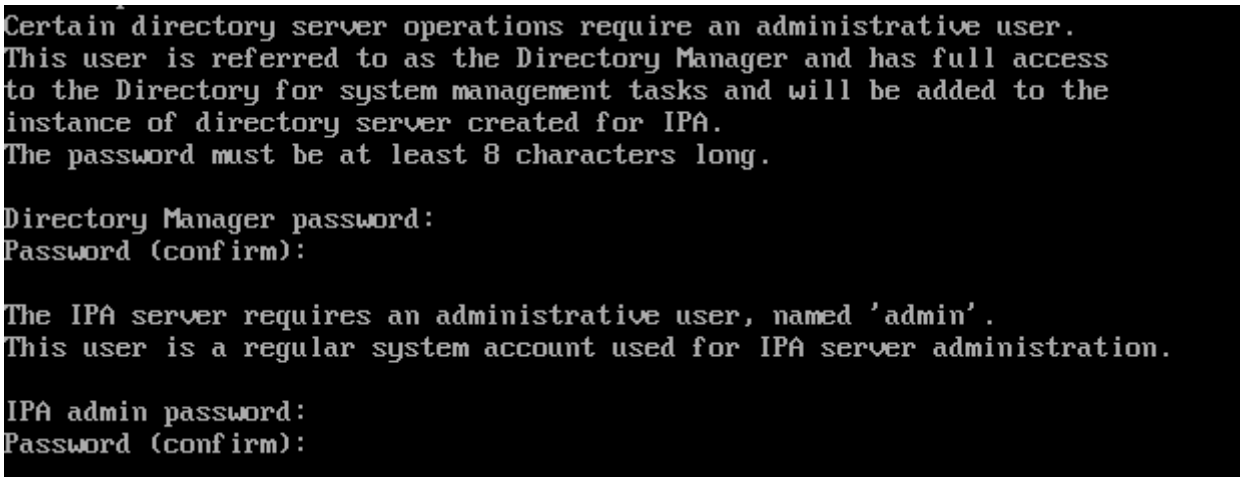

Рис. 54. Запрос пароля для Directory сервера и административного аккаунта FreeIPA

Следующими являются запросы о паролях для Directory сервера и административного аккаунта FreeIPA.

По умолчанию логин для администратора FreeIPA будет - admin.

Введите запрашиваемые пароли и запомните их.

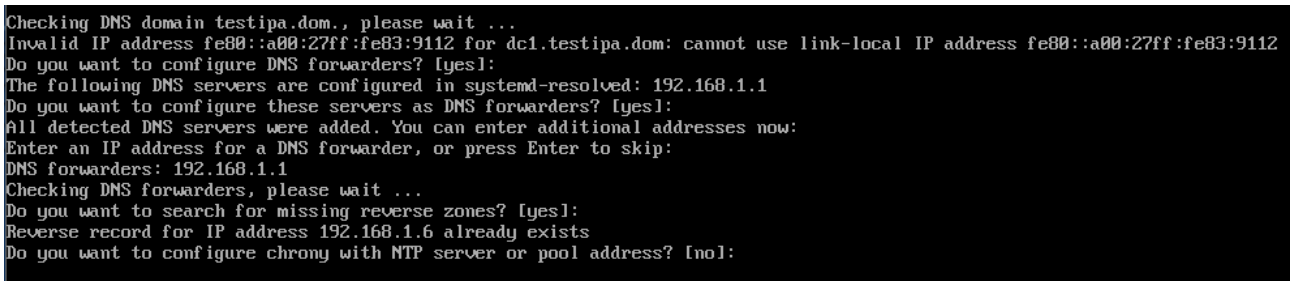

Рис. 55. Запросы про DNS сервер

Далее следуют вопросы про DNS сервер.

1. Do you want to configure DNS forwarders? Отвечаем YES, хотим сконфигурировать DNS сервера для форвардинга
2. Do you want to configure these servers as DNS forwarders? Отвечаем YES, хотим сконфигурировать найденный DNS сервера как сервер для форвардинга.
3. Enter an IP address for a DNS forwarder , or press Enter to skip: Нажимаем Enter, если не хотим вписывать дополнительные DNS сервера для форвардинга. Если хотим, тогда вписываем IP адреса DNS серверов для форвардинга.
4. Do you want to search for missing reverse zone? Отвечаем YES, хотим найти реверс зоны

5. Do you want to configure chrony with NTP server or pool address? Отвечаем NO, не хотим конфигурировать сервер chrony, так как нас устраивает его конфигурация по умолчанию.

Рис. 56. Запрос о конфигурации FreeIPA сервера

Следующим шагом установщик выведет конфигурационную информацию, и спросит, всё ли правильно мы сконфигурировали для дальнейшей установки FreeIPA сервера? Отвечаем YES, если все правильно сконфигурировали.

После этого шага начнется инсталляция FreeIPA сервера на ПК.

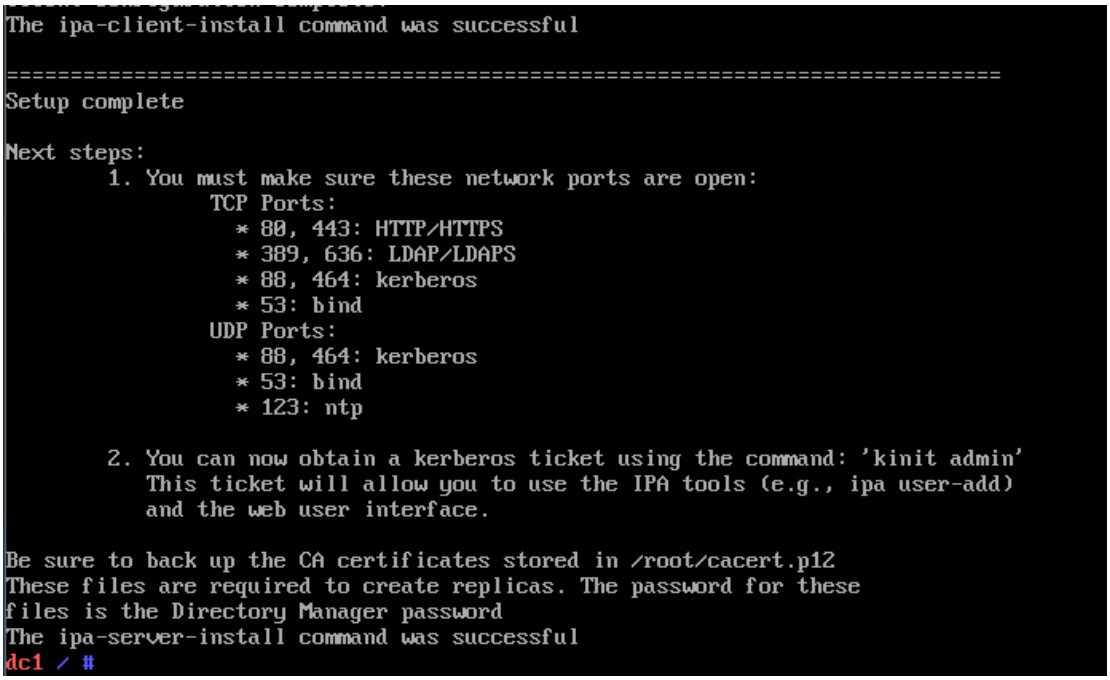

Рис. 57. Сообщение о завершении установки

Если установка прошла успешно, установщик FreeIPA сервера выведет конечную информацию об установленном сервере и его сервисах.

Далее необходимо проверить, все ли службы FreeIPA работают. Для этого используйте команду.

```
ipactl status
```

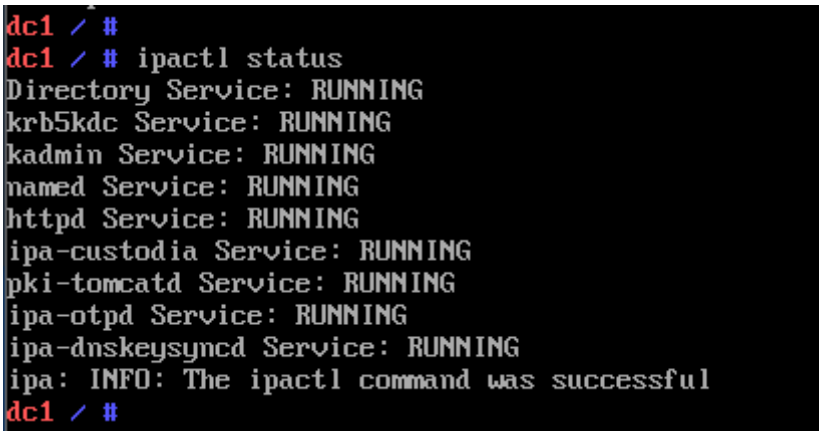

Рис. 58. Проверка работы сервера

Если в выводах команды везде написано RUNNING, значит все сервисы запущены и работают.

Следующим и последним шагом установки, необходимо инициализировать аккаунт администратора FreeIPA - admin:

```
kinit admin
```

Введите пароль, который был введен ранее, при установке FreeIPA:

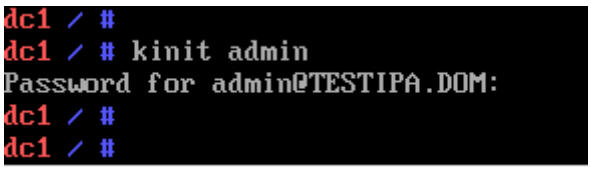

Рис. 59. Ввод пароля

Теперь можно открыть браузер и зайти по URL: https://dc1.testipa.dom/ipa/ui.

Откроется Web-интерфейс FreeIPA сервера, где можно зайти под учетной записью администратора, введя его логин (admin) и пароль.

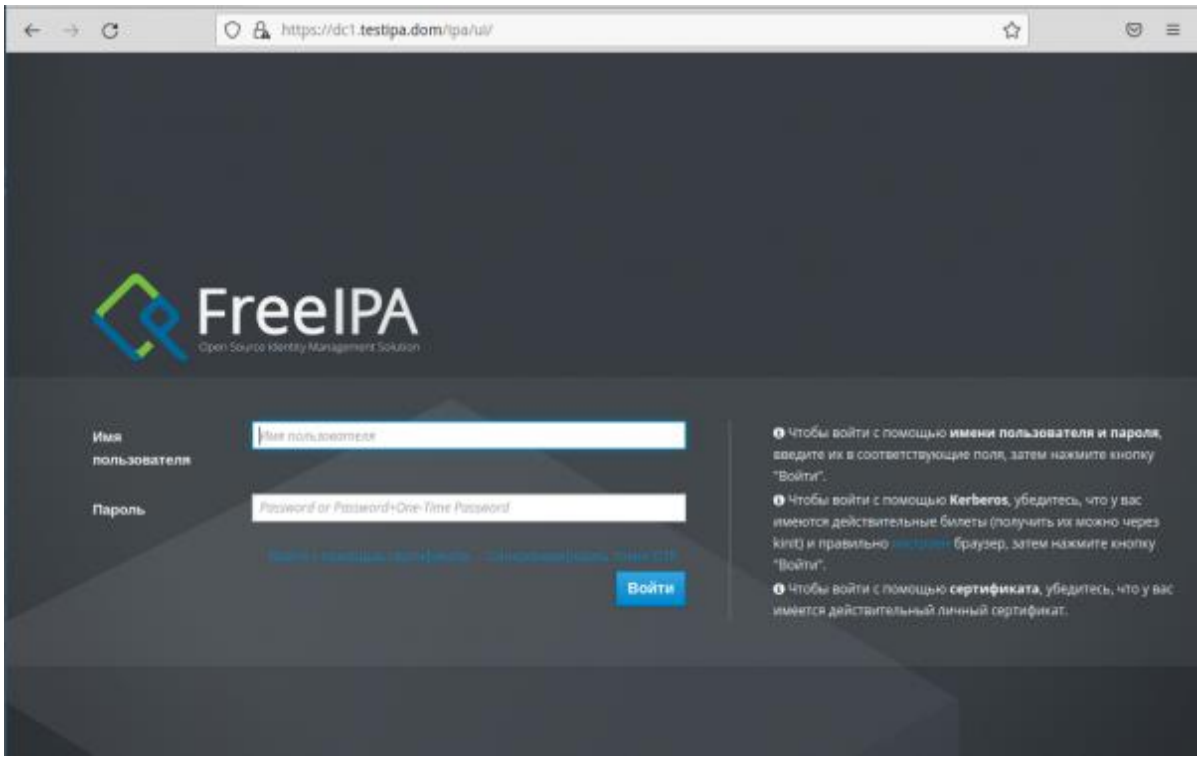

Рис. 60. Вход в Web-интерфейс FreeIPA сервера

После успешного входа откроется web-интерфейс FreeIPA сервера, работа с которым рассмотрена далее.

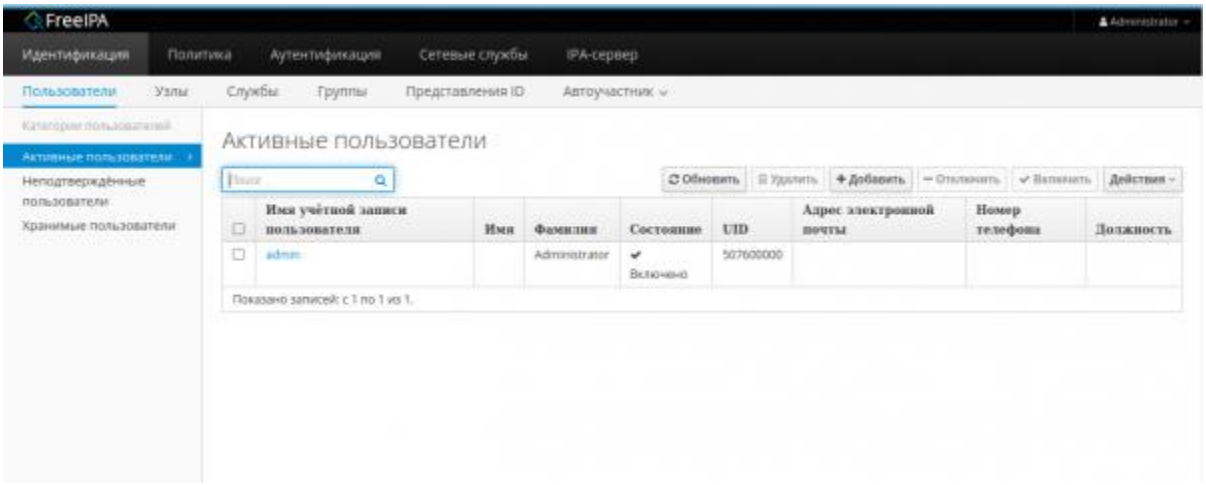

Рис. 61. Рабочий интерфейс FreeIPA

15.1.3. Создание пользователей FreeIPA сервера

Чтобы добавить пользователей в FreeIPA, перейдите в раздел [Идентификация] → [Активные пользователи] (этот раздел виден по умолчанию первым).

Заполните все необходимые параметры и далее нажмите кнопку "Добавить".

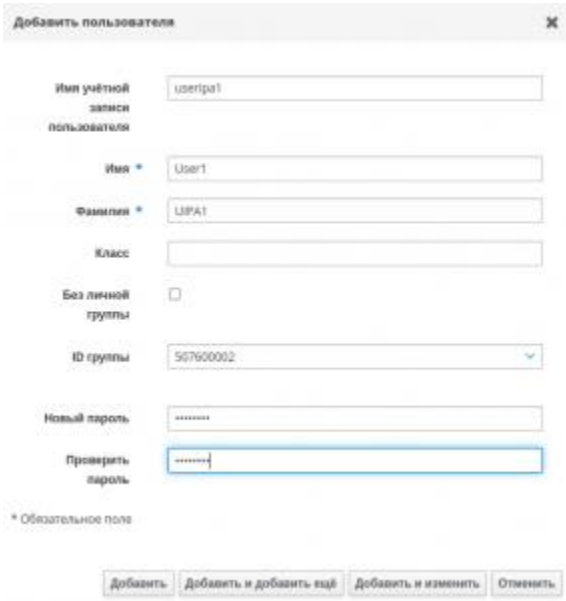

Рис. 62. Добавление нового пользователя FreeIPA сервера

Обратите внимание, что в поле «Имя учетной записи» логин будущего пользователя должен быть написан латинскими буквами.

Информация, вводимая в поля «Имя» и «Фамилия» будущего пользователя носят только справочную информацию и далее в работе ни на что не влияют.

В выпадающем списке поля «ID группы» необходимо выбрать группу «editors».

После внесения параметров нажмите кнопку «Добавить».

Для добавления каждого нового пользователя пройдите аналогичные шаги, после чего они все будут отражены в разделе «Активные пользователи».

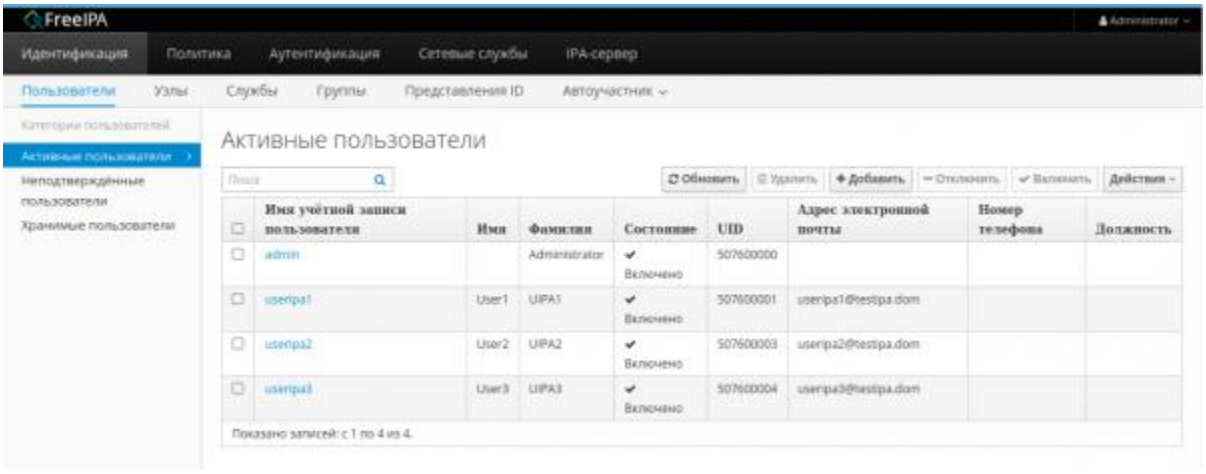

Рис. 63. Список пользователей FreeIPA сервера

Далее рассмотрим настройку FreeIPA клиента и вход в домен FreeIPA.

15.2. Настройка FreeIPA клиента

Для установки FreeIPA клиента, сначала надо установить пакет ipa-client:

```
dnf install ipa-client
```

15.2.1. Подготовка к настройке FreeIPA клиента

Наш настроенный FreeIPA сервер имеет хост и домен: dc1 / testipa.dom, соответственно клиент должен иметь такой же домен:

```
hostnamectl set-hostname st1.testipa.dom
```

В данном примере, у рабочей станции хост st1, и домен testipa.dom.

Следующим шагом является настройка сети. Перейдите в меню [Параметры системы] → [Соединения], далее выберите соединение и вкладку IPv4 (в правой части экрана).

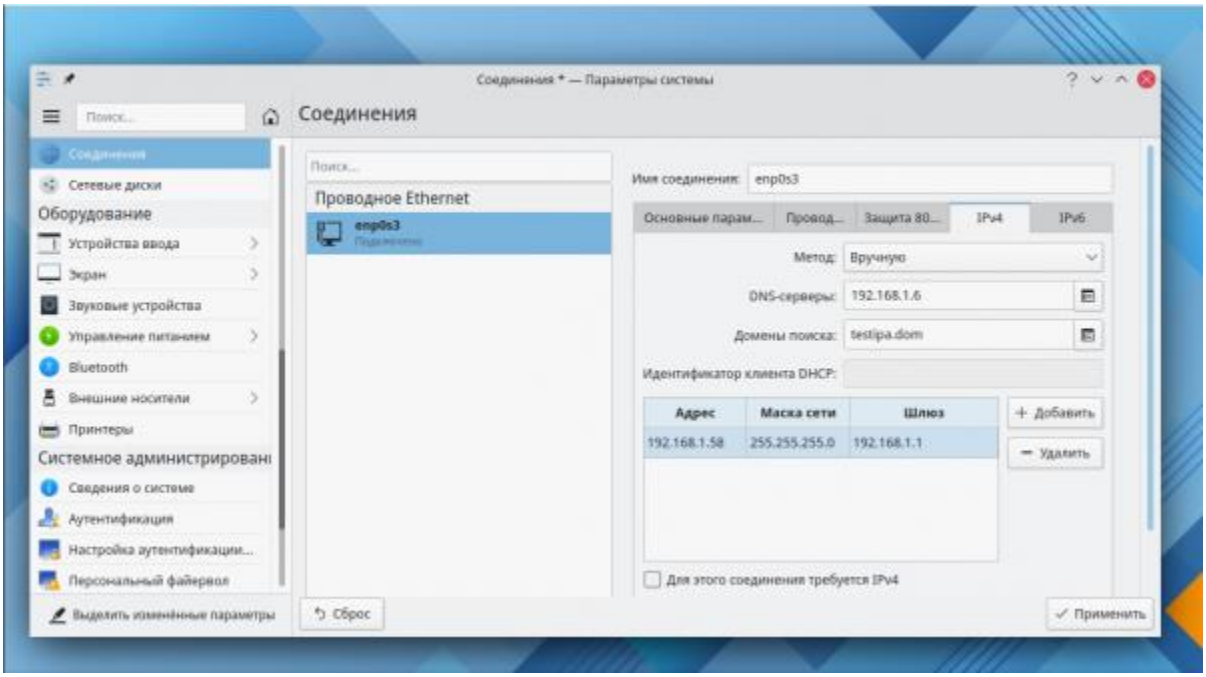

Рис. 64. [Параметры системы] → [Соединения], вкладка IPv4

Из выпадающего списка в параметре «Метод» выберите «Вручную».

В поле «DNS серверы» - IP адрес FreeIPA сервера.

В поле «Домены поиска» - testipa.dom.

Добавляем статические адреса:

- 192.168.1.58 – это IP адрес рабочей станции;
- 255.255.255.0 – маска подсети;
- 192.168.1.1 – шлюз.

По завершению - нажмите кнопку «Применить».

Далее необходимо переподключить сеть (отключаем ее и включаем снова).

Проверяем доступность нашего FreeIPA сервера по FQDN имени:

```
ping dc1.testipa.dom
```

15.2.2. Инсталляция и настройка FreeIPA клиента

Для того чтобы инсталлировать FreeIPA клиента, при уже установленном пакете ipa-client более ничего не требуется.

Следующим шагом необходимо ввести рабочую станцию в домен FreeIPA и инициализировать пользователя FreeIPA:

```
ipa-client-install –mkhomedir
```

Рассмотрим далее некоторые запросы инсталлятора.

```
st1 / #
st1 / # ipa-client-install --mkhomedir
This program will set up FreeIPA client.
Version 4.8.10

Discovery was successful!
Do you want to configure chrony with NTP server or pool address? [no]:
Client hostname: st1.testipa.dom
Realm: TESTIPA.DOM
DNS Domain: testipa.dom
IPA Server: dc1.testipa.dom
BaseDN: dc=testipa,dc=dom

Continue to configure the system with these values? [no]: yes
Synchronizing time
No SRV records of NTP servers found and no NTP server or pool address was provided.
Using default chrony configuration.
Attempting to sync time with chronyc.
Time synchronization was successful.
User authorized to enroll computers: admin
Password for admin@TESTIPA.DOM:
```

Рис. 65. Запрос о перенастройке сервера времени chrony

На запрос о перенастройке сервера времени chrony, ответить – NO.

Продолжить ли установку с выбранными параметрами, ответить YES.

Следующим шагом будет запрос пароля администратора FreeIPA - admin, для ввода рабочей станции в домен FreeIPA. Введите пароль администратора и нажмите клавишу <Enter>.

```
Successfully retrieved CA cert
    Subject:     CN=Certificate Authority,O=TESTIPA.DOM
    Issuer:      CN=Certificate Authority,O=TESTIPA.DOM
    Valid From:  2021-11-25 09:46:16
    Valid Until: 2041-11-25 09:46:16

Enrolled in IPA realm TESTIPA.DOM
Created /etc/ipa/default.conf
Configured sudoers in /etc/authselect/user-nsswitch.conf
Configured /etc/sssd/sssd.conf
Configured /etc/krb5.conf for IPA realm TESTIPA.DOM
Systemwide CA database updated.
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring testipa.dom as NIS domain.
Client configuration complete.
The ipa-client-install command was successful
st1 / #
```

Рис. 66. Сообщение об успешной установке

Если все прошло успешно, об этом будет сообщено в последней строке.

Рис. 67. Список работающих узлов

После этого, зайдем на FreeIPA сервер и проверим, принял ли он нашу рабочую станцию в домен.

Если все прошло успешно, в списке «Узлы» будет имя хоста рабочей станции.

Далее необходимо инициализировать пользователя FreeIPA:

```
kinit useripa1
```

Вводим пароль для пользователя FreeIPA сервера - useripa1

Далее, надо придумать новый пароль для пользователя, так как при добавлении нового пользователя пароль выдается временный. Введите новый пароль и подтвердите его.

15.2.3. Вход в домен FreeIPA

Для того чтобы войти пользователю в домен FreeIPA, необходимо на экране входа в систему (GDM) выбрать параметр «Нет в списке», после чего откроется поле ввода логина нового пользователя.

Рис. 68. Вход в домен FreeIPA

Вводим логин с доменом: useripa1@TESTIPA.DOM (имя домена необходимо вводить заглавными буквами)

Далее пароль, который придумали на предыдущем шаге.

После входа в рабочую станцию под доменным пользователем FreeIPA, запросите его ID.

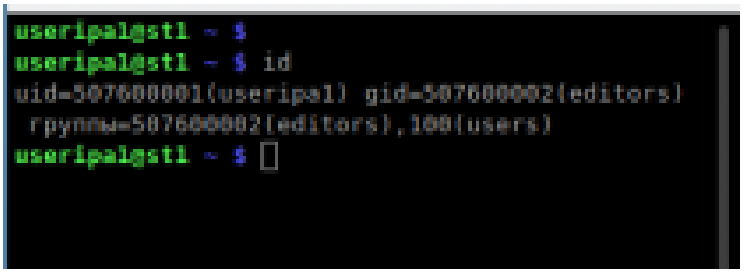

Рис. 69. Запрос ID пользователя

ID пользователя должно совпадать с его ID в FreeIPA сервере. (Не быть локальным, номером от 500 до 1000)

На этом вход в домен FreeIPA завершен.

16. НАСТРОЙКА СЕРВЕРА ВРЕМЕНИ CHRONY

Chrony — это гибкая реализация протокола сетевого времени - NTP. Он используется для синхронизации часов с различными NTP серверами.

Предпочтительнее использовать сервер времени Chrony вместо NTPD, поскольку Chrony может синхронизировать системные часы быстрее и с большей точностью, особенно для систем, которые не всегда находятся в сети.

В состав пакета Chrony входит две программы:

— chronyd - сервис, который запускается при старте системы и в режиме реального времени синхронизирует системные часы.

— chronyc - консольная программа для управления chrony.

Для того, чтобы проверить работу сервиса наберите:

```
systemctl status chronyd
```

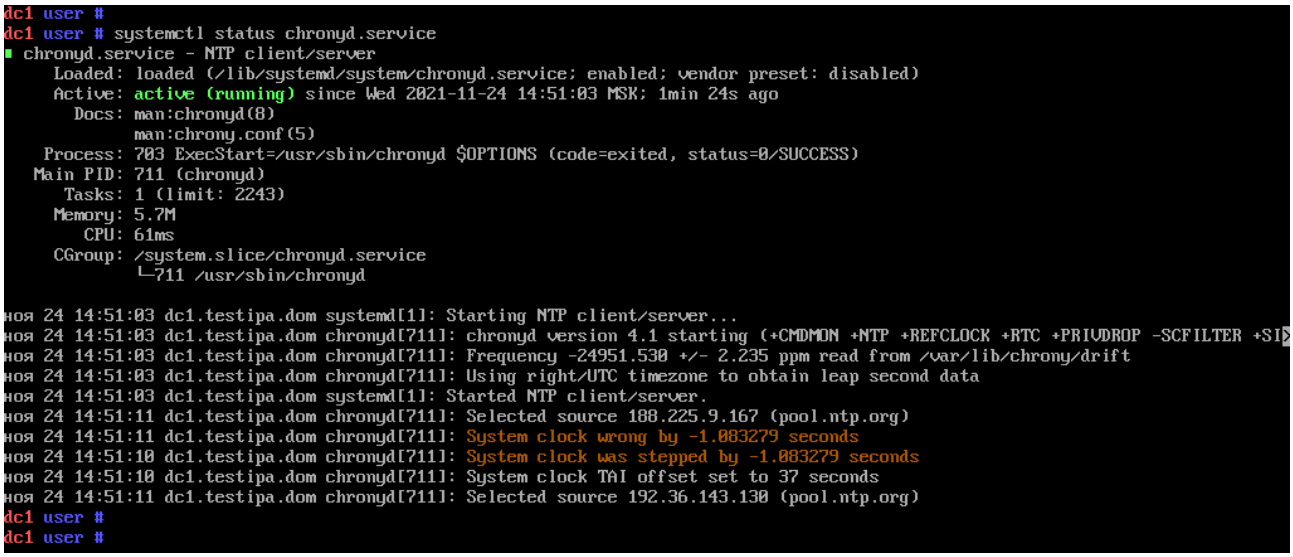

Рис. 70. Проверка работы сервера

Если вывод команды выглядит примерно также (с параметром active (running)) сервис настроен и работает, а также корректирует системное время.

Далее проверьте синхронизацию времени:

```
chronyc tracking
```

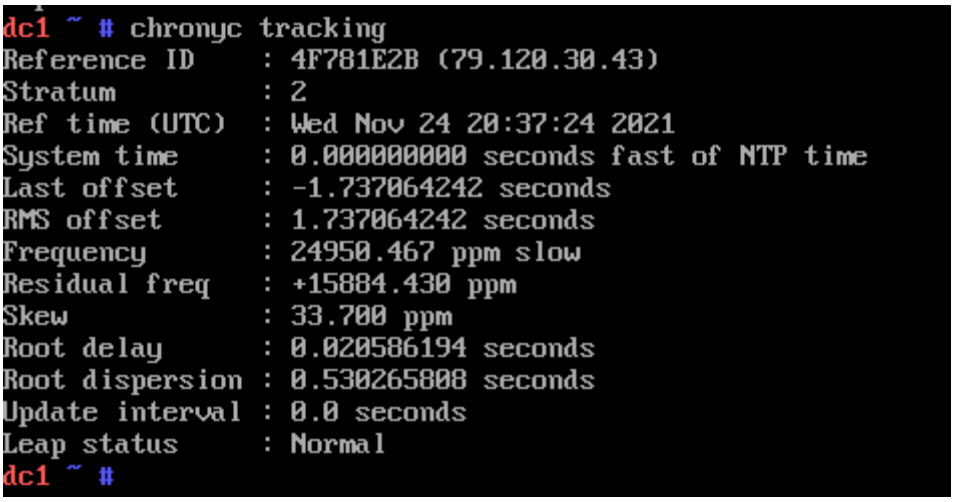

Рис. 71. Вывод команды chronyc tracking

Вывод команды должен выглядеть так, где:

— Reference ID — это сервер эталонного времени;

— Stratum — сколько раз производилась синхронизация;

— Ref time — это время по GMT в которое была произведена последняя синхронизация.

Посмотрим сервера эталонного времени:

```
chronyc sources
```

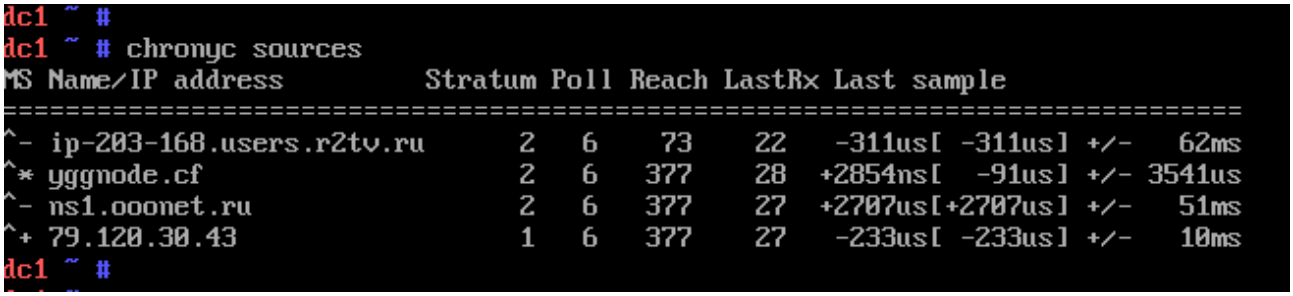

Рис. 72. Просмотр серверов эталонного времени

Настройка параметров сервера времени производится в конфигурационном файле /etc/chrony.conf

Из всех параметров в файле, в основном нужно править нужные NTP сервера, или пулы NTP серверов, за эту настройку отвечает параметр server.

Например, можем поменять на свои NTP сервера:

```
server ntp1.stratum1.ru iburst
server ntp2.stratum1.ru iburst
server ntp1.stratum2.ru iburst
server ntp2.stratum2.ru iburst
```

При ручном обновлении времени можно запустить команду:

```
chronyc makestep
```

Если вывод команды — 200 OK, тогда chrony произвел соединение с эталонным сервером и синхронизировал время.