ДОКУМЕНТАЦИЯ ALT LINUX TEAM

Альт Сервер 10.2 для Эльбрус

Документация

Руководство пользователя

Редакция февраль, 2024

Аннотация

Добро пожаловать в документацию дистрибутива Альт Сервер для Эльбрус. Данное руководство предназначено как для начинающих, так и для опытных пользователей. Руководство описывает подготовку системы для установки, процесс установки дистрибутива, а также процедуру настройки и использования системы.

Данное руководство соответствует текущему состоянию сведений, но какие-либо окончательные правки могли не попасть в него. В случае обнаружения ошибок и неточностей в руководство вносятся изменения.

Часть I. Что такое Альт Сервер для Эльбрус?

В этой части рассматривается что такое Linux и Альт Сервер для Эльбрус.

Содержание

Глава 1. Что такое Альт Сервер для Эльбрус

Операционная система Альт Сервер для Эльбрус — многофункциональный дистрибутив для серверов с возможностью использования в качестве рабочей станции разработчика комплексных систем, прежде всего, предназначен для использования в корпоративных сетях.

Альт Сервер для Эльбрус представляет собой совокупность интегрированных программных продуктов, созданных на основе ОС Linux и обеспечивает обработку, хранение и передачу информации в круглосуточном режиме эксплуатации. Дистрибутив предоставляет интегрированную операционную систему на единой оптимизированной пакетной базе с поддержкой различных аппаратных платформ, с возможностью установки графического окружения.

Всё программное обеспечение работает в основном режиме процессора (в двоичных кодах «Эльбрус»). Это обеспечивает более высокую производительность по сравнению с режимом бинарной трансляции, который позволяет запускать программы, собранные под процессоры x86.

Альт Сервер для Эльбрус это комплекс серверных приложений, оснащённый удобным пользовательским интерфейсом для настройки. Управление сервером может осуществляться с любого компьютера через веб-браузер.

Альт Сервер для Эльбрус представляет собой решение уровня предприятия, позволяющее осуществить миграцию на импортозамещающее программное и аппаратное обеспечение.

Основные преимущества ОС Альт Сервер для Эльбрус:

- установка серверных решений и решений конечных пользователей с одного диска;
- графическая рабочая среда MATE;
- возможность как развернуть, так и использовать только определённые службы без Alterator;
- возможность обеспечить единую аутентификацию, общие ресурсы и совместную работу через сервер каталогов.

Глава 2. Что такое Linux

2.1. Свободные программы

Операционная система (далее — ОС) Linux — ядро, основные компоненты системы и большинство её пользовательских приложений — свободные программы. Свободные программы можно:

- запускать на любом количестве компьютеров;
- распространять бесплатно или за деньги без каких-либо ограничений;
- получать исходные тексты этих программ и вносить в них любые изменения.

Свобода программ обеспечила их широкое использование и интерес к ним со стороны тысяч разработчиков. Основные программы для Linux выходят под лицензией GNU General Public License (далее — GPL). Лицензия GNU не только гарантирует свободу, но и защищает её. Она допускает дальнейшее распространение программ только под той же лицензией, поэтому исходный код ядра Linux, компиляторов, библиотеки glibc, пользовательских графических оболочек не может быть использован для создания приложений с закрытым кодом. В этом принципиальное отличие Linux от свободных ОС семейства BSD (FreeBSD, NetBSD, OpenBSD), фрагменты которых вошли в Microsoft Windows и даже стали основой OS X. Linux включает в себя многие разработки BSD, но его компиляторы и системные библиотеки разработаны в рамках проекта GNU (http://www.gnu.org/home.ru.html).

2.2. Разработка Linux

В отличие от распространённых несвободных ОС, Linux не имеет географического центра разработки. Нет фирмы, которая владела бы этой ОС, нет и единого координационного центра. Программы для Linux — результат работы тысяч проектов. Большинство из них объединяет программистов из разных стран, связанных друг с другом только перепиской. Лишь некоторые проекты централизованы и сосредоточены в фирмах. Создать свой проект или присоединиться к уже существующему может любой программист, и, в случае успеха, результаты этой работы станут известны миллионам пользователей. Пользователи принимают участие в тестировании свободных программ, общаются с разработчиками напрямую. Это позволяет за короткий срок добавлять в программное обеспечение новые возможности, оперативно находить ошибки и исправлять их.

Именно гибкая и динамичная система разработки, невозможная для проектов с закрытым кодом, определяет исключительную экономическую эффективность Linux. Низкая стоимость свободных разработок, отлаженные механизмы тестирования и распространения, привлечение независимых специалистов, обладающих индивидуальным, самостоятельным видением проблем, защита исходного текста программ лицензией GPL — всё это стало причиной успеха свободных программ.

Такая высокая эффективность разработки не могла не заинтересовать крупные фирмы. Они стали создавать свои свободные проекты, основывающиеся на тех же принципах. Так появились Mozilla, LibreOffice, свободный клон Interbase, SAP DB. IBM способствовала переносу Linux на свои мейнфреймы.

Открытый код программ значительно снизил себестоимость разработки закрытых систем для Linux и позволил снизить цену решения для пользователя. Вот почему Linux стала платформой, часто рекомендуемой для таких продуктов, как Oracle, DB2, Informix, Sybase, SAP ERP, Lotus Domino.

2.3. Защищённость

ОС Linux унаследовала от UNIX надёжность и отличную систему защиты. Система разграничения доступа к файлам позволяет не бояться вирусов. Но всё же, программ без ошибок не бывает, и Linux не исключение. Благодаря открытости исходного кода программ, аудит системы может осуществить любой специалист без подписок о неразглашении и без необходимости работы в стенах нанявшей его компании. Сообщества разработчиков и пользователей свободных программ создали множество механизмов оповещения об ошибках и их исправления. Сообщить об ошибке и принять участие в её исправлении независимому программисту или пользователю так же просто, как специалисту фирмы-разработчика или автору проекта. Благодаря этому ошибки защиты эффективно выявляются и быстро исправляются.

2.4. Дистрибутивы Linux

Большинство пользователей для установки Linux используют дистрибутивы. Дистрибутив — это не просто набор программ, а готовое решение для выполнения различных задач пользователя, обладающее идентичностью установки, управления, обновления, а также едиными системами настройки и поддержки.

2.5. Новичку

Linux — самостоятельная операционная система. Все операционные системы разные: Linux — не Windows, не OS X и не FreeBSD. В Linux свои правила, их необходимо изучить и к ним необходимо привыкнуть. Терпение и настойчивость в изучении Linux обернётся значительным повышением эффективности и безопасности вашей работы. То, что сегодня кажется странным и непривычным, завтра понравится и станет нормой.

Не стесняйтесь задавать вопросы, ведь самый простой способ найти ответ — совет опытного специалиста. Взаимопомощь и общение — традиция в мире Linux. Всегда можно обратиться за помощью к сообществу пользователей и разработчиков Linux. Большинство вопросов повторяются, поэтому для начала стоит поискать ответ на свой вопрос в документации, затем в сети Интернет. Если вы не нашли ответа в перечисленных источниках, не стесняйтесь, пишите на форум или в списки рассылки так, как писали бы своим друзьям, и вам обязательно помогут.

Глава 3. Что такое системы Альт

3.1. ALT Linux Team

Команда ALT Linux (http://www.altlinux.org/ALT_Linux_Team) — это интернациональное сообщество, насчитывающее более 200 разработчиков свободного программного обеспечения.

3.2. Сизиф

Sisyphus (https://packages.altlinux.org) — наш ежедневно обновляемый банк программ (часто называемый репозиторий). Поддерживаемая ALT Linux Team целостность Sisyphus, оригинальная технология сборки программ, утилита **`apt-get`** и её графическая оболочка **synaptic** позволяют пользователям легко обновлять свои системы и быть в курсе актуальных новостей мира свободных программ.

Ежедневно изменяющийся репозиторий содержит самое новое программное обеспечение со всеми его преимуществами и недостатками (иногда ещё неизвестными). Поэтому, перед обновлением вашей системы из Sisyphus, мы советуем взвесить преимущества новых возможностей, реализованных в последних версиях программ, и вероятность возникновения неожиданностей в работе с ними (http://www.altlinux.org/Sisyphus_changes).

Разработка Sisyphus полностью доступна. У нас нет секретных изменений кода и закрытого тестирования с подписками о неразглашении. То, что мы сделали сегодня, завтра вы найдёте в сети. По сравнению с другими аналогичными банками программ (Debian unstable, Mandriva Cooker, PLD, Fedora), в Sisyphus есть немало самобытного. Особое внимание уделяется защите системы, локализации на русский язык, полноте и корректности зависимостей.

Название Sisyphus (Сизиф) заимствовано из греческой мифологии. С кропотливым Сизифом, непрерывно закатывающим в гору камни, команду ALT Linux Team объединяет постоянная работа над усовершенствованием технологий, заложенных в репозиторий.

Sisyphus, в первую очередь, — открытая лаборатория решений. Если вам это интересно, если вы хотите дополнить Sisyphus новыми решениями, если вы считаете, что можете собрать какую-то программу лучше — присоединяйтесь к проекту ALT Linux Team (http://www.altlinux.org/Join).

3.3. Что такое десятая платформа

Как уже говорилось ранее, Sisyphus является часто обновляемым репозиторием, скорее предназначенным для разработчиков. Решением для тех пользователей, которым стабильность и предсказуемость работы системы важнее расширенной функциональности (а это в первую очередь начинающие и корпоративные пользователи), являются дистрибутивы Альт. Такие дистрибутивы базируются на стабильном срезе репозитория Sisyphus. Эти срезы называются платформами.

Десятая платформа (p10) была создана в июле 2021 года и её поддержка продлится до июля 2025.

3.3.1. Основные новшества в десятой платформе

- Синхронная сборка p10 производится для пяти основных архитектур:
  - 64-битных x86_64, aarch64 и ppc64le;
  - 32-битных i586 и armh (armv7hf);
- Ядра реального времени — для архитектуры x86_64 собраны два realtime-ядра: Xenomai и Real Time Linux (PREEMPT_RT);
- Расширение набора групповых политик — групповые политики поддерживают параметры gsettings для управления рабочими средами MATE и Xfce;
- Центр администрирования Active Directory (admc) — графическое приложение для управления пользователями, группами и групповыми политиками домена Active Directory;
- Платформа Deploy — предназначена для развёртывания системных служб на локальном компьютере с помощью Ansible. Поддерживаемые роли: Apache, MariaDB, MediaWiki, Nextcloud, PostgreSQL и Moodle;
- Модуль настройки многотерминального режима alterator-multiseat.

Часть II. Установка дистрибутива

В этой части рассматривается процесс установки дистрибутива.

Содержание

Глава 4. Подготовка установочного диска

Наиболее частый способ установки операционной системы на компьютер представляет собой установку с установочного DVD-диска. Также можно производить установку, записав установочный образ на USB Flash.

4.1. Запись образа ISO дистрибутива на DVD

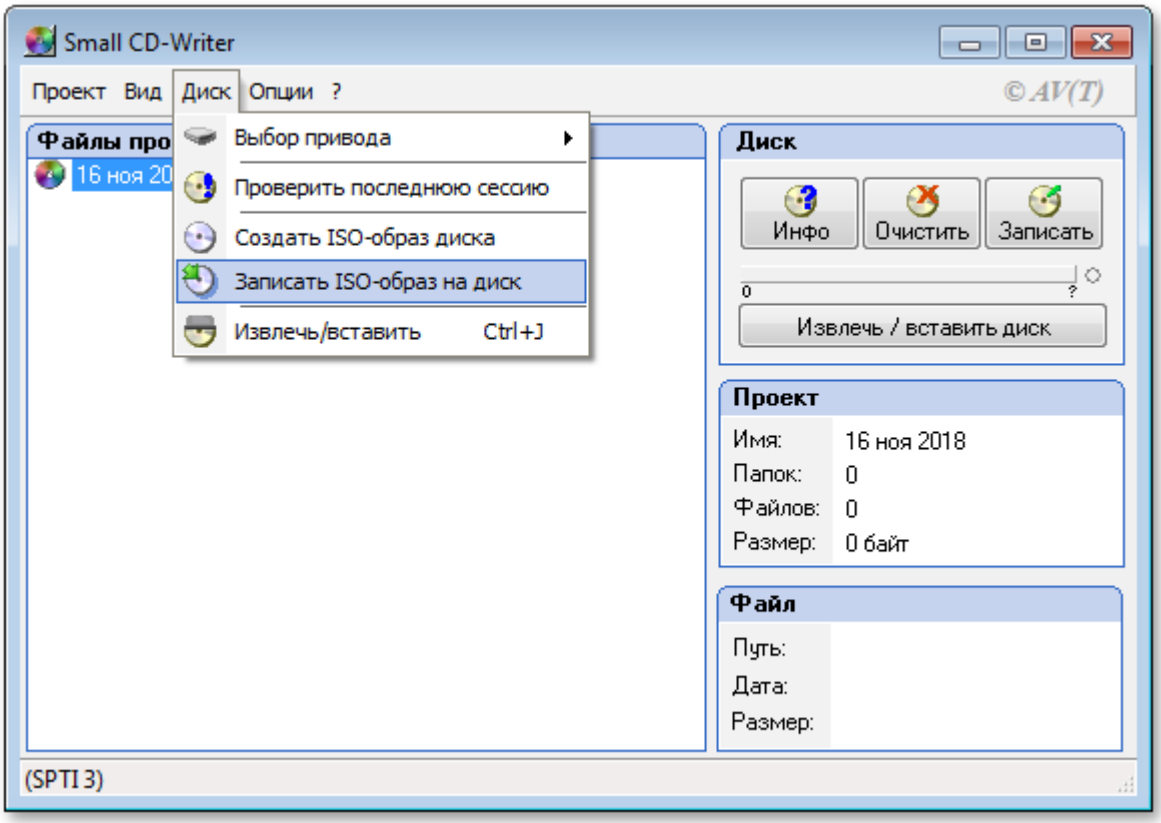
4.1.1. В операционной системе MS Windows

Файл ISO-образа диска — это файл специального формата, подготовленный для записи на диск. Для записи ISO-образа под операционной системой MS Windows используйте специальные программы: SCDWriter, Nero BurningROM и другие. Рекомендуем для записи использовать новые диски от известных производителей, таких как: Verbatim, TDK. Записанный на плохой диск образ может вызвать неразрешимые проблемы при установке.

4.1.1.1. Запись образа диска с помощью Small CD-Writer

Весь процесс записи установочного диска при помощи **Small CD-Writer** состоит из следующих шагов:

- скачать образ дистрибутива;
- скачать архив программы Small CD-Writer http://gluek.info/wiki/_media/software/scdwriter14.zip;
- распаковать файлы программы из архива в любой каталог;
- вставить чистый диск в привод;
- войти в распакованный каталог и запустить программу **`SCDWriter.exe`**;
- открыть пункт меню **Диск** → **Записать ISO-образ на диск** и, в появившемся окне, указать путь к образу диска;
- нажать кнопку **`Записать`**.



4.1.1.2. Запись образа диска с помощью Nero BurningROM

Процесс записи установочного диска при помощи **Nero BurningROM** состоит из следующих шагов:

- скачать образ дистрибутива;
- скачать программу **Nero BurningROM** с сайта производителя http://www.nero.com и установить её;
- запустить программу и выбрать в списке устройств необходимый для записи CD/DVD дисковод;
- нажать кнопку **Открыть** в главном окне. В появившемся окне выбрать необходимый ISO-образ для записи и нажать кнопку **Открыть**;
- в окне **Записать проект** на вкладке **Запись** установить отметку в поле **Запись** и настроить необходимые параметры прожига;
- записать ISO-образа на диск, щёлкнув по кнопке **Прожиг**.

4.1.2. В операционной системе Linux

Для записи ISO-образов можно использовать множество утилит и программ с графическим или текстовым интерфейсом. Наиболее удобно использовать программы **K3b** или **Brasero**, которые поставляются в комплекте большинства дистрибутивов операционной системы Linux.

4.1.2.1. Запись образа диска с помощью K3b

Весь процесс записи установочного диска при помощи **K3b** состоит из следующих шагов:

- если программа **k3b** отсутствует, необходимо установить её в систему, используя стандартные для вашего дистрибутива инструменты установки программ;
- запустить программу **k3b**. При правильных настройках программа сообщит об отсутствии проблем с системой и предложит перейти к записи на диск;
- в меню главного окна **Сервис (Service)** выбрать пункт **Записать образ DVD (Burn DVD image)**;
- в появившемся окне **`Записать образ DVD (Burn DVD image)`** нажать на кнопку **`Выбор файла для записи`**. Откроется диалог, в котором необходимо выбрать ISO-образ для записи и после выбора нажать кнопку **`OK`**;
- программа **k3b** покажет информацию о ISO-файле и начнёт вычислять контрольную сумму. Эта операция может занять несколько минут. Полученную контрольную сумму можно сравнить с MD5SUM суммой на странице дистрибутива;
- если контрольные суммы не совпадают, значит, для записи был выбран не тот файл или скачанный ISO-образ был испорчен во время передачи данных по сети;
- если контрольные суммы совпадают, вставить диск для записи в дисковод. Дождаться активации кнопки **`Начать (Start)`**;
- нажать на кнопку **`Начать (Start)`**.

4.2. Запись установочного образа на USB Flash

Предупреждение

Для загрузки ВК Эльбрус требуется наличие на установочном носителе одного раздела в стиле MBR с файловой системой ext2/ext3; скрипт **`write.sh`** разбивку не меняет во избежание более тяжёлых последствий ошибок.

Для создания загрузочного flash-носителя понадобится файл ISO-образа установочного диска с дистрибутивом. ISO-образы установочных дисков для семейства архитектур e2k **не** являются гибридными (ПНС не декларирует возможность загрузки с ISO-образа на разделе, mcst#5322).

4.2.1. В операционной системе Linux

Скопируйте полное содержимое ISO-образа, включая скрытый каталог **`.disk`**, на раздел USB-носителя с файловой системой ext2 или ext3, и по желанию замените в файле конфигурации загрузчика **`boot.conf`** умолчание **`default=install`** на **`default=install_flash`**, чтобы не выбирать его вручную при загрузке.

Для упрощения этой процедуры на Linux-системах можно воспользоваться скриптом **`write.sh`**, который входит в состав ISO-образов или может быть найден рядом с ними:

- извлечение скрипта (требуется однократно):

```
# mount -o loop,ro <файл-образа.iso> /mnt
# cp -a /mnt/write.sh /usr/local/bin
# umount /mnt
```

- запись образа:

```
# sleep 1; write.sh <файл-образа.iso> /dev/sdX1
```

где sdX — устройство, соответствующее целевому flash-диску (см. вывод команды **lsblk**); при необходимости на указанном разделе, который должен уже существовать, будет создана файловая система ext2.

Примечание

Для выполнения скрипта на применяемой системе должна быть доступна команда **rsync**.

Глава 5. Начало установки: загрузка системы

5.1. Способы первоначальной загрузки

Простейший способ запустить программу установки — загрузить компьютер с помощью загрузочного носителя, находящегося на установочном DVD с дистрибутивом (при условии, что система поддерживает загрузку с устройства для чтения DVD).

Примечание

Для загрузки с USB Flash выбирайте цель **install_flash** (в любом случае достаточно нажать **Enter** в меню **boot#**).

5.2. Загрузка системы

После включения вычислительного комплекса «Эльбрус» происходит инициализация программы начальной загрузки, в процессе которой есть возможность вмешательства после вывода строки:

```
Autoboot in 03 sec. PRESS SPACE TO DISABLE IT.
```

Необходимо нажать пробел, после чего должны появиться следующие строки:

```
Key pressed. Autoboot canceled.
CPU#00: Starting menu.

                BOOT SETUP
 Press command letter, or press 'h' to get help
:
```

Можно запросить подсказку нажатием клавиши **h**, но необходимыми являются следующие пункты:

- **d** — show Disks and partitions (показать диски и разделы);
- **c** — Change boot parameters (изменить параметры загрузки);
- **u** — show cUrrent parameters (показать текущие параметры);
- **m** — save params to NVRAM (сохранить параметры в NVRAM);
- **b** — start Boot.conf menu (запустить меню Boot.conf).

При нажатии на клавишу **d** получим список дисков:

```
:d
CPU#00: Drive [2]: SATA - PCI BUS[1]:DEV[3]:FUNC[0], MCST SATA COMBINED Port
[0] - KINGSTON SMS200S3120G
CPU#00:         Partition [0]: Linux EXT2;
                   U:246194e7-0512-4db3-a821-cbcbe3c92c38 L:""
CPU#00:         Partition [1]: Linux swap
CPU#00:         Partition [3]: Extended
CPU#00:         Partition [4]: Unknown file system type
CPU#00: Drive [10]: ATAPI device
```

В данном случае идентификатор 10 присвоен внешнему USB DVD-приводу, с которого и будет произведена установка операционной системы; следует выбрать его, указав идентификатор ответом на первый вопрос команды **c** и нажав клавишу **Esc** на остальные:

```
:c

                CHANGE BOOT PARAMETERS

        Current Settings:
drive_number:      '2'
drive label:       '*'
partition_number:  '0'
file system id:    '07bde958-ec62-492e-933c-17334bb02da2'
command_string:    ''
filename:          ''
initrdfilename:    ''
autoboot in:       '10'

To advance to next setting press ENTER. To skip setting press ESC
Enter drive number    : 10
Enter partition number: < Skipped >
Enter command string  : < Skipped >
Enter filename        : < Skipped >
Enter initrd file name: < Skipped >
Enter autoboot value  : < Skipped >
```

```
        Current Settings:
drive_number:      '10'
drive label:       ''
partition_number:  '0'
file system id:    ''
command_string:    ''
filename:          ''
initrdfilename:    ''
autoboot in:       '10'
CPU#00: Search drive and partition by label or uuid succeed
```

Затем необходимо перейти к загрузке последовательным нажатием клавиш **b Tab Enter**:

```
:b
boot# install
CPU#00: Label 'install' found, loading parameters
CPU#00: Search drive and partition by label or uuid succeed

Trying to load and start image with following parameters:
drive_number:      '10'
drive label:       ''
partition_number:  '0'
file system id:    ''
command_string:    'hardreset fastboot live automatic=method:cdrom'
filename:          '/alt0/vmlinux.0'
initrdfilename:    '/alt0/full.cz'
```

Примечание

Мышь на этом этапе установки не поддерживается. Для выбора опций установки и различных вариантов необходимо использовать клавиатуру.

После загрузки инсталлятора установка продолжается штатным образом.

После установки системы, если установка производилась на диск, отличный от того, с которого ВК загружается по умолчанию — следует повторно зайти в конфигурацию программы начальной загрузки, определить загрузочный диск (**d**) и указать его в качестве загрузочного диска по умолчанию (**c**). После изменений параметров загрузки, следует воспользоваться командой **m** для записи изменений в NVRAM и их применения в дальнейшем.

Глава 6. Последовательность установки

До того как будет произведена установка базовой системы на жёсткий диск, программа установки работает с образом системы, загруженным в оперативную память компьютера.

Если инициализация оборудования завершилась успешно, будет запущен графический интерфейс программы-установщика. Процесс установки разделён на шаги. Каждый шаг посвящён настройке или установке определённого свойства системы. Шаги нужно проходить последовательно. Переход к следующему шагу происходит по нажатию кнопки **Далее**. При помощи кнопки **Назад**, при необходимости, можно вернуться к уже пройденному шагу и изменить настройки. Однако возможность перехода к предыдущему шагу ограничена теми шагами, в которых нет зависимости от данных, введённых ранее.

Если по каким-то причинам возникла необходимость прекратить установку, необходимо нажать кнопку <Reset> на корпусе системного блока компьютера.

Примечание

Совершенно безопасно выполнить отмену установки только до шага Подготовка диска, поскольку до этого момента не производится никаких изменений на жёстком диске.

Технические сведения о ходе установки можно посмотреть, нажав **Ctrl**+**Alt**+**F1**, вернуться к программе установки — **Ctrl**+**Alt**+**F7**. По нажатию **Ctrl**+**Alt**+**F2** откроется отладочная виртуальная консоль.

Каждый шаг сопровождается краткой справкой, которую можно вызвать, щёлкнув кнопку **Справка** или нажав клавишу **F1**.

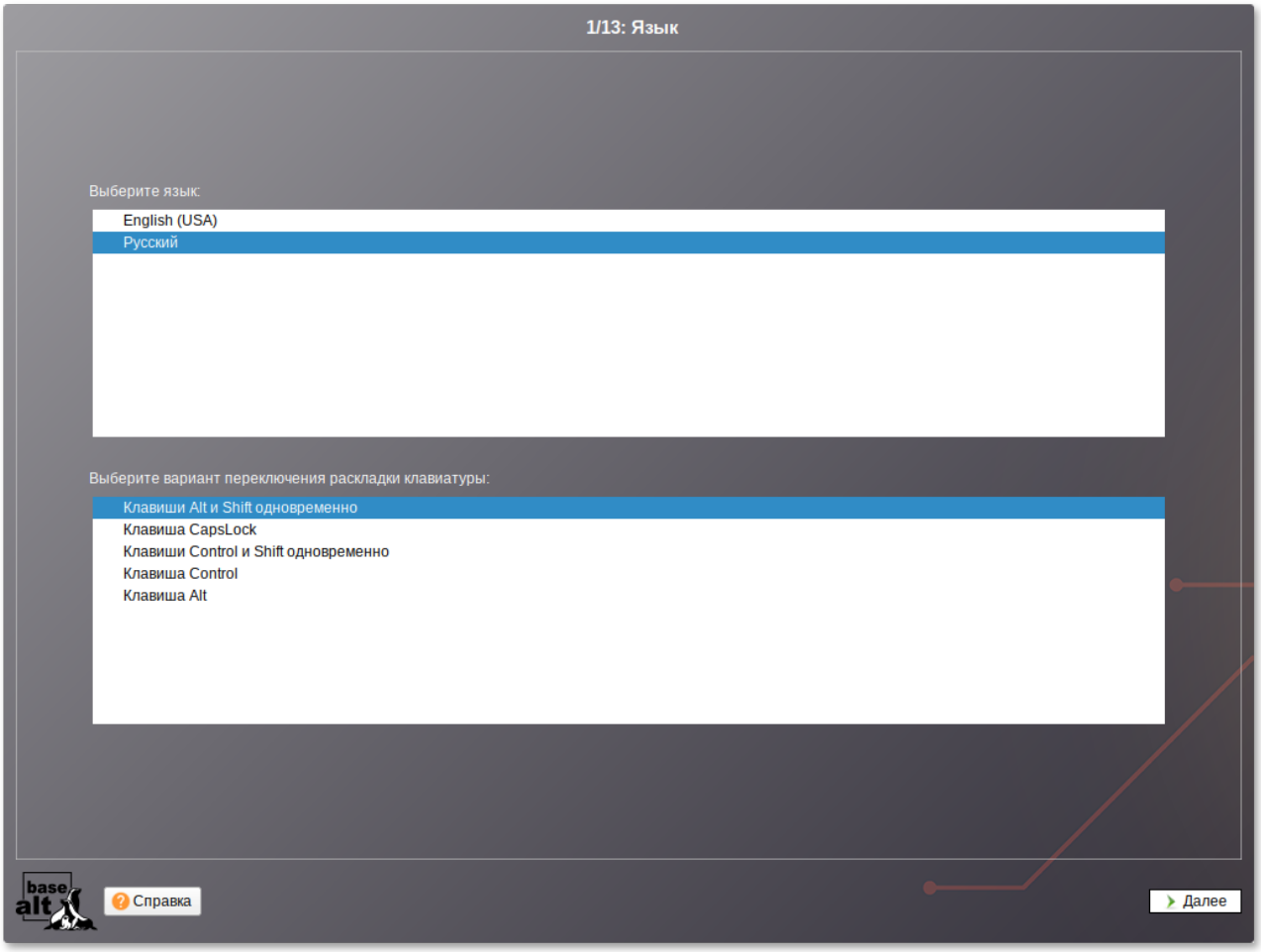
Нажатие на кнопку

позволяет показать/скрыть панель со списком шагов установки.

Во время установки системы выполняются следующие шаги:

- Язык;
- Дата и время;
- Подготовка диска;
- Перемонтирование;
- Установка системы;
- Сохранение настроек;
- Настройка сети;
- Администратор системы;
- Системный пользователь;
- Завершение установки.

Глава 7. Язык



Установка Альт Сервер для Эльбрус начинается с выбора основного языка — языка интерфейса программы установки и устанавливаемой системы. В списке, помимо доступных языков региона (выбранного на этапе начальной загрузки), указан и английский язык.

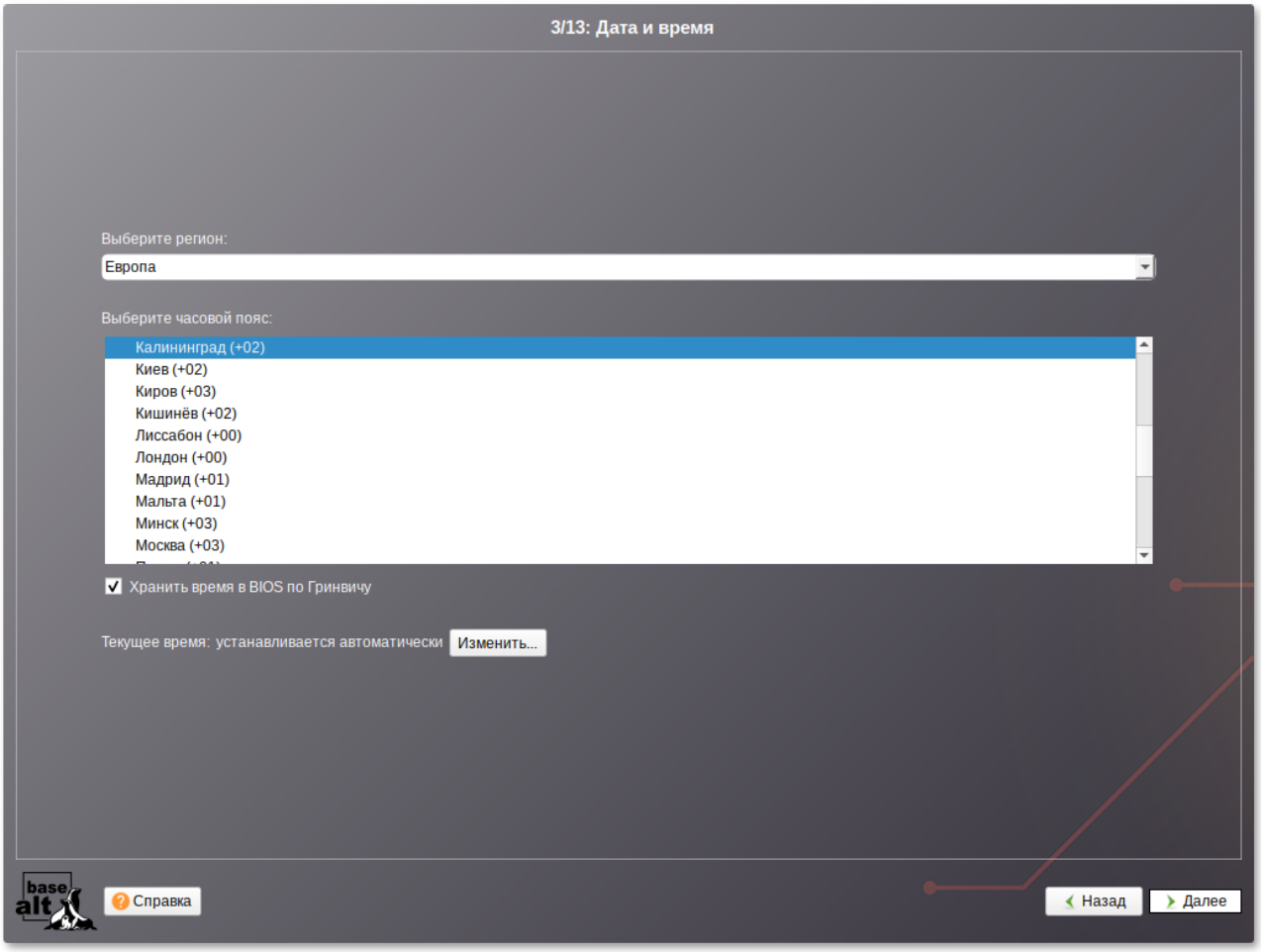
На этом же этапе выбирается вариант переключения раскладки клавиатуры. Раскладка клавиатуры — это привязка букв, цифр и специальных символов к клавишам на клавиатуре. Помимо ввода символов на основном языке, в любой системе Linux необходимо иметь возможность вводить латинские символы (имена команд, файлов и т.п.). Для этого обычно используется стандартная английская раскладка клавиатуры. Переключение между раскладками осуществляется при помощи специально зарезервированных для этого клавиш. Для русского языка доступны следующие варианты переключения раскладки:

- клавиши **`Alt`** и **`Shift`** одновременно;
- клавиша **`CapsLock`**;
- клавиши **`Control`** и **`Shift`** одновременно;
- клавиша **`Control`**;
- клавиша **`Alt`**.

Если выбранный основной язык имеет всего одну раскладку (например, при выборе английского языка в качестве основного), эта единственная раскладка будет принята автоматически.

Глава 8. Дата и время

На данном этапе выполняется выбор региона и города, по которым будет определен часовой пояс и установлены системные часы.



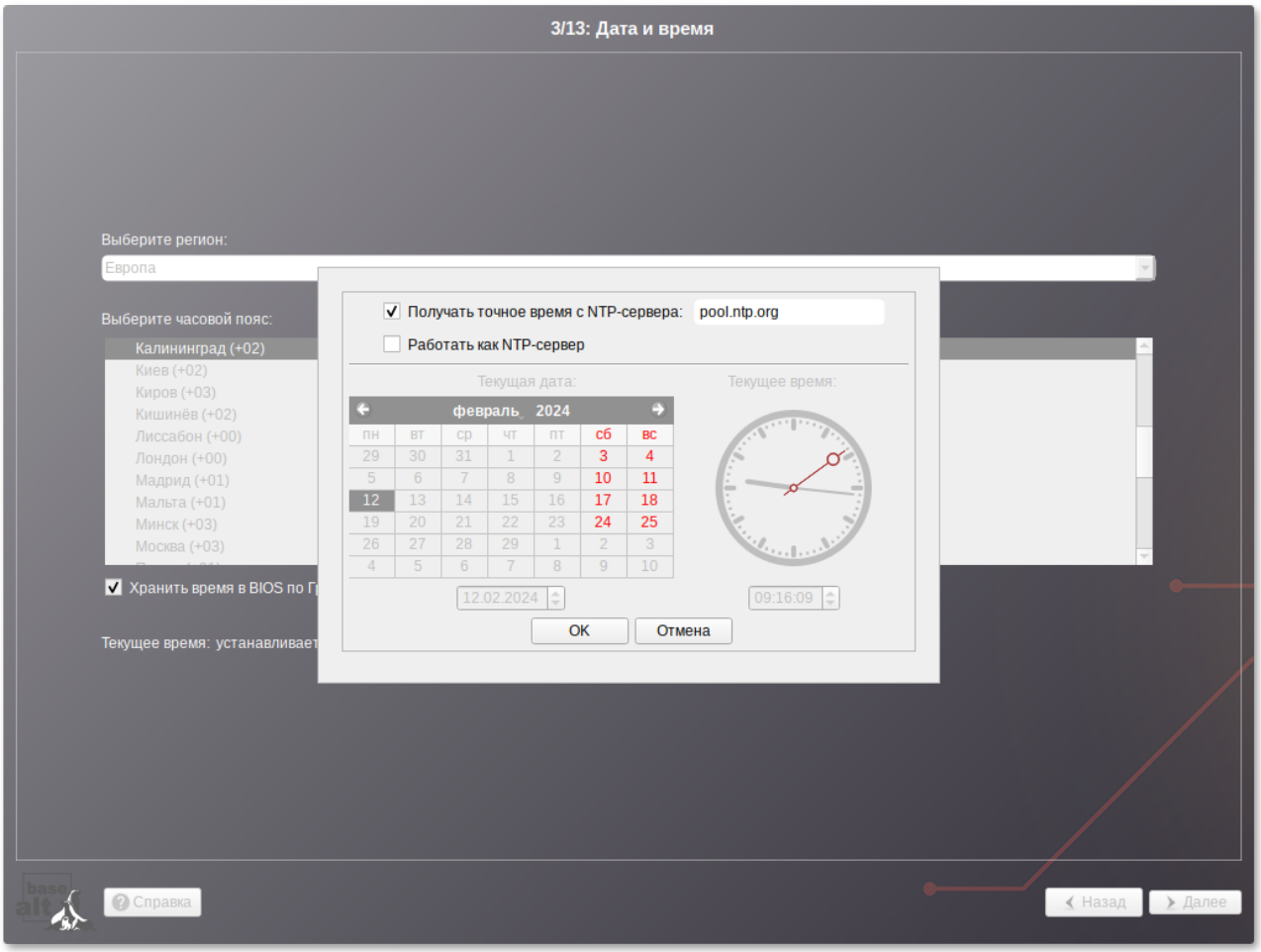
Для корректной установки даты и времени достаточно правильно указать часовой пояс и выставить желаемые значения для даты и времени.

На этом шаге следует выбрать часовой пояс, по которому нужно установить часы. Для этого в соответствующих списках выберите регион, а затем город. Поиск по списку можно ускорить, набирая на клавиатуре первые буквы искомого слова.

Пункт **Хранить время в BIOS по Гринвичу** выставляет настройки даты и времени в соответствии с часовыми поясами, установленными по Гринвичу, и добавляет к местному времени часовую поправку для выбранного региона.

После выбора часового пояса будут предложены системные дата и время по умолчанию.

Для ручной установки текущих даты и времени нужно нажать кнопку **Изменить…**. Откроется окно ручной настройки системных параметров даты и времени.



Для сохранения настроек и продолжения установки системы в окне ручной установки даты и времени необходимо нажать кнопку **OK** и затем в окне **Дата и время** нажать кнопку **Далее**.

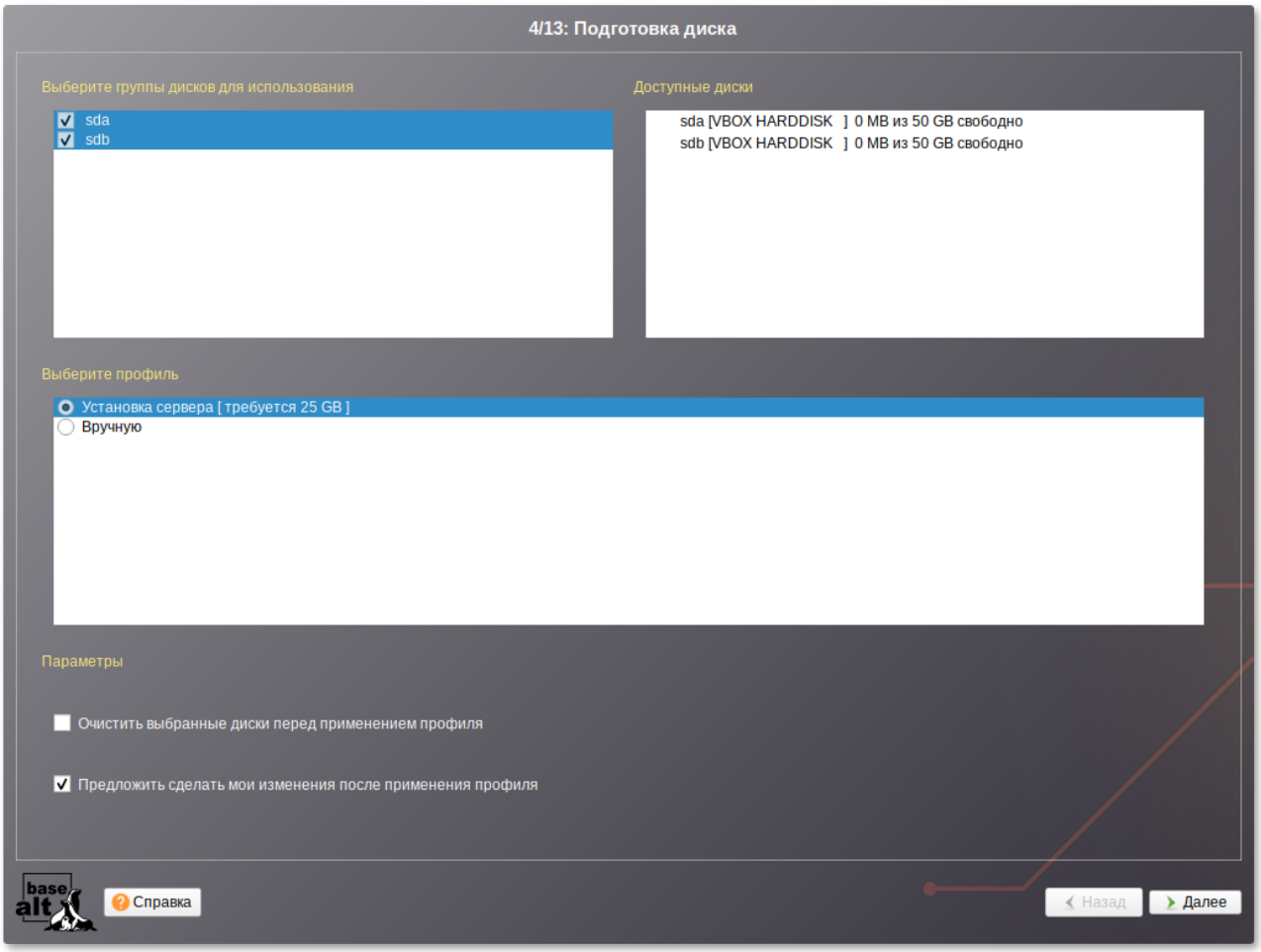
Глава 9. Подготовка диска

На этом этапе подготавливается площадка для установки Альт Сервер для Эльбрус, в первую очередь — выделяется свободное место на диске.

Переход к этому шагу может занять некоторое время. Время ожидания зависит от производительности компьютера, объёма жёсткого диска, количества разделов на нём и других параметров.

9.1. Выбор профиля разбиения диска

После завершения первичной конфигурации загрузочного носителя откроется окно **Подготовка диска**. В списке разделов перечислены уже существующие на жёстких дисках разделы (в том числе здесь могут оказаться съёмные flash-диски, подключённые к компьютеру в момент установки).



В списке **Выберите профиль** перечислены доступные профили разбиения диска. Профиль — это шаблон распределения места на диске для установки ОС. Можно выбрать один из профилей:

- **Установка сервера**;
- **Вручную**.

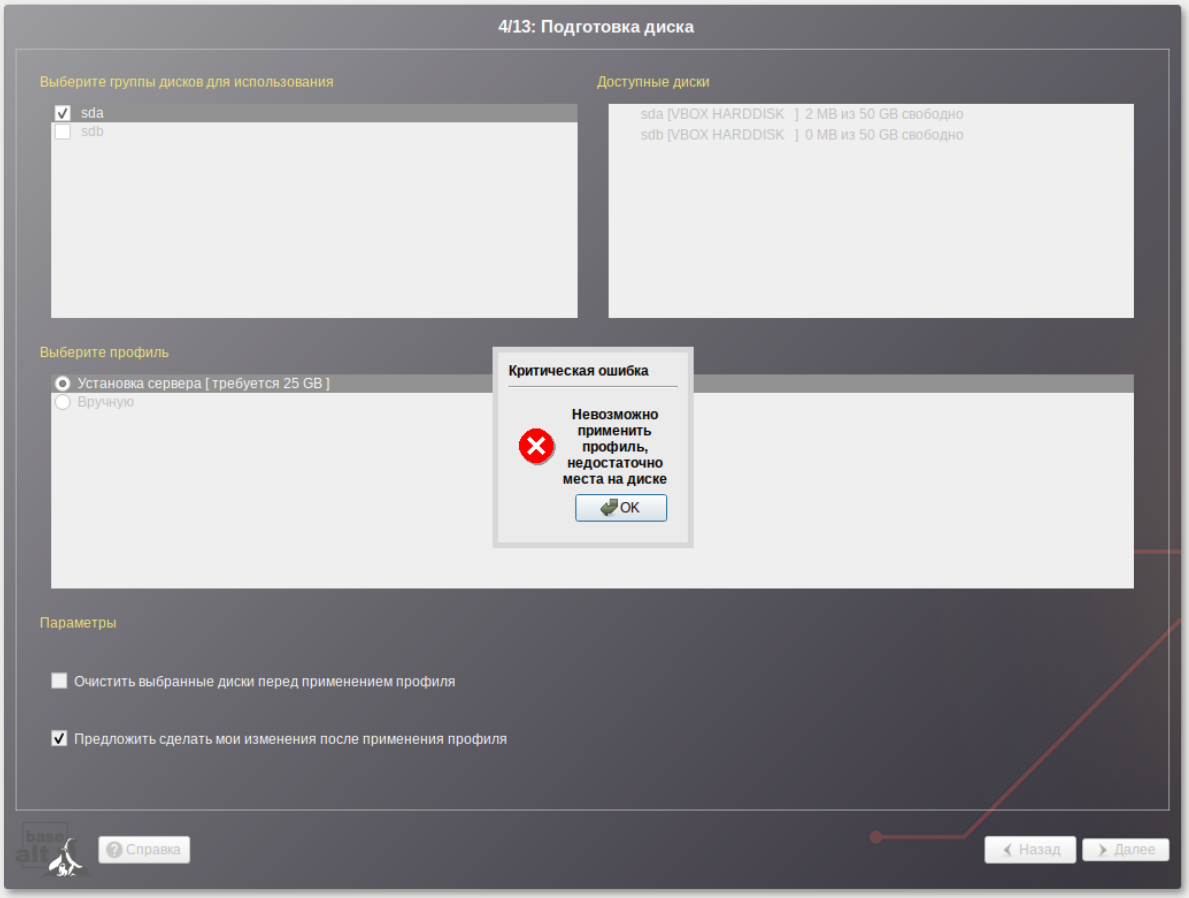
Первый профиль предполагает автоматическое разбиение диска.

9.2. Автоматический профиль разбиения диска

Профиль **Установка сервера** предполагает автоматическое разбиение диска. При выборе этого профиля будет создан раздел под корень. Если размер диска больше 100 ГБ, будет также создан раздел **/var**.

Примечание

Если при применении профиля автоматического разбиения диска доступного места на диске окажется недостаточно, то на монитор будет выведено сообщение об ошибке: **Невозможно применить профиль, недостаточно места на диске**.



Для решения этой проблемы можно полностью очистить место на диске, отметив пункт **Очистить выбранные диски перед применением профиля** и применить профиль повторно.

Если сообщение о недостатке места на диске появляется и при отмеченном пункте **Очистить выбранные диски перед применением профиля**, то это связано с недостаточным для использования автоматических методов разметки объёмом выбранных дисков. В этом случае вы можете воспользоваться методом ручной разметки: профиль **Вручную**.

Предупреждение

При отмеченном пункте **Очистить выбранные диски перед применением профиля** будут удалены все данные с выбранных дисков (включая внешние USB-носители) без возможности восстановления. Рекомендуется использовать эту возможность при полной уверенности в том, что диски не содержат никаких ценных данных.

Примечание

Разбивка не затрагивает CF-диск, на котором может храниться система бинарной трансляции.

9.3. Ручной профиль разбиения диска

При необходимости освободить часть дискового пространства следует воспользоваться профилем разбиения **Вручную**. В этом случае можно удалить некоторые из существующих разделов или содержащиеся в них файловые системы. После этого можно создать необходимые разделы самостоятельно или вернуться к шагу выбора профиля и применить автоматический профиль. Выбор этой возможности требует знаний об устройстве диска и технологиях его разметки.

Важно

В случае ручной разбивки необходимо создать и подключить на первом разделе диска (не MD RAID) раздел для ядра **/boot** с файловой системой ext2 (т.е. без extents и журнала).

По нажатию кнопки **Далее** будет произведена запись новой таблицы разделов на диск и форматирование разделов. Только что созданные на диске программой установки разделы пока не содержат данных и поэтому форматируются без предупреждения. Уже существовавшие, но изменённые разделы, которые будут отформатированы, помечаются специальным значком в колонке **Файловая система** слева от названия. При уверенности в том, что подготовка диска завершена, подтвердите переход к следующему шагу нажатием кнопки **Далее**.

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

9.4. Дополнительные возможности разбиения диска

Ручной профиль разбиения диска позволяет установить ОС на программный RAID-массив, разместить разделы в томах LVM и использовать шифрование на разделах. Данные возможности требуют от пользователя понимания принципов функционирования указанных технологий.

9.4.1. Создание программного RAID-массива

Избыточный массив независимых дисков RAID (redundant array of independent disks) — технология виртуализации данных, которая объединяет несколько жёстких дисков в логический элемент для избыточности и повышения производительности.

Примечание

Для создания программного RAID-массива потребуется минимум два жёстких диска.

Программа установки поддерживает создание программных RAID-массивов следующих типов:

- RAID 1;
- RAID 0;
- RAID 4/5/6;
- RAID 10.

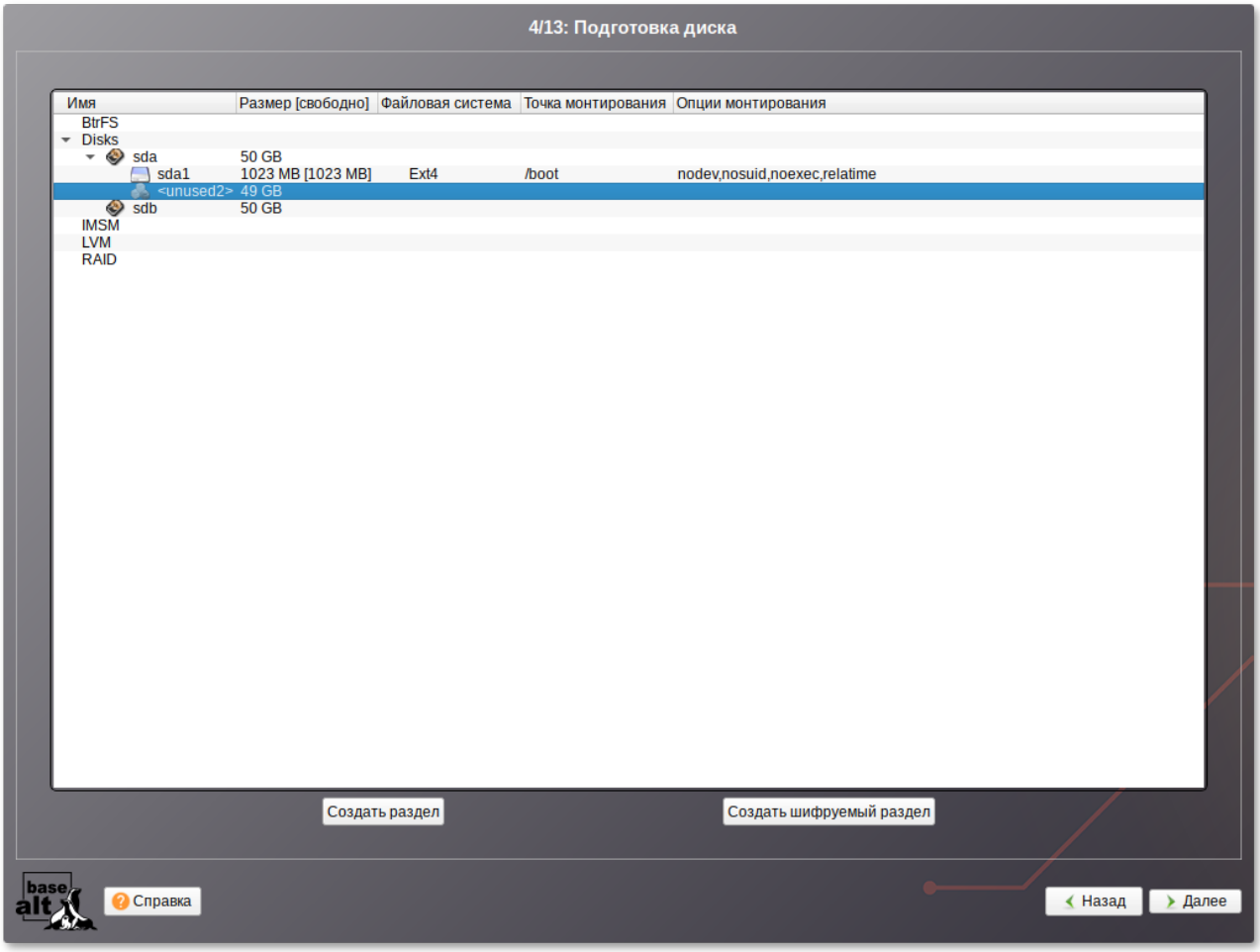
Процесс подготовки к установке на RAID условно можно разбить на следующие шаги:

- создание разделов на жёстких дисках;
- создание RAID-массивов на разделах жёсткого диска;
- создание файловых систем на RAID-массиве.

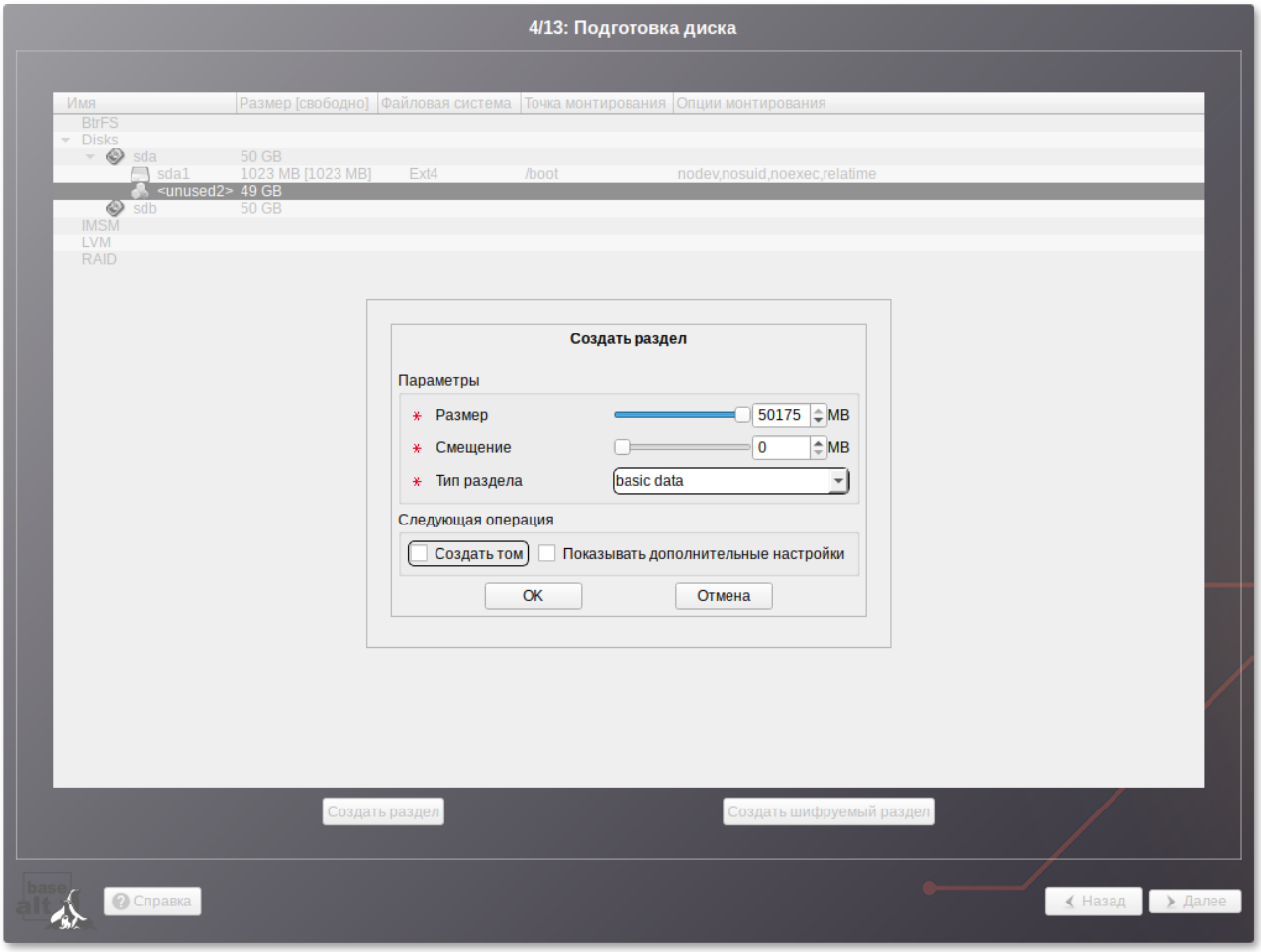
Важно

Для создания программного RAID-массива может потребоваться предварительно удалить существующую таблицу разделов с жёсткого диска.

Для настройки параметров нового раздела из состава RAID-массива необходимо выбрать неразмеченный диск в окне профиля разбивки пространства **Вручную** и нажать кнопку **Создать раздел**.



Для создания программного массива на GPT-разделах следует сначала создать разделы типа **basic data** и не создавать на них том (снять отметку с пункта **Создать том**):

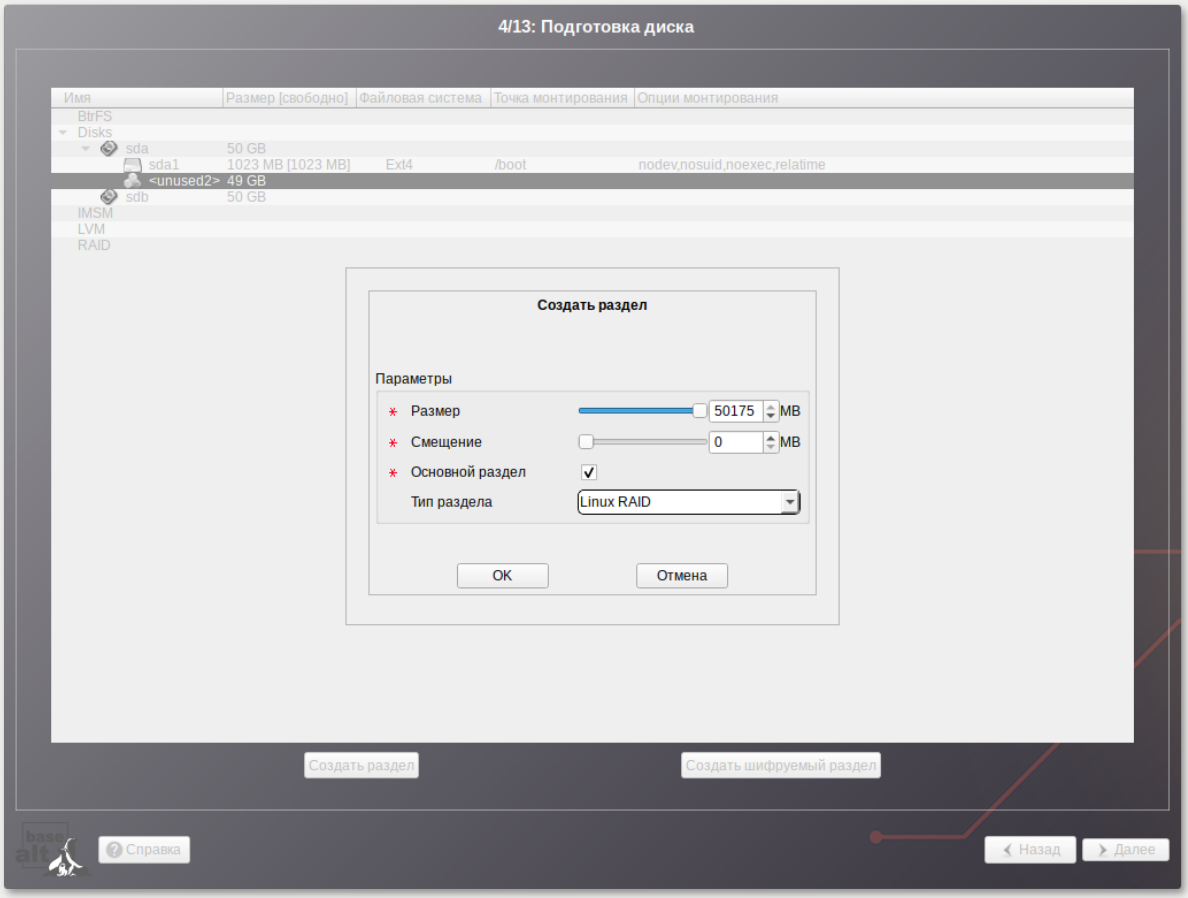


В этом окне необходимо настроить следующие параметры:

- **Размер** — в поле необходимо указать размер будущего раздела в Мбайт;
- **Смещение** — в поле необходимо указать смещение начала данных на диске в Мбайт;
- **Тип раздела** — в выпадающем поле нужно выбрать значение **basic data** для последующего включения раздела в RAID-массив.

Примечание

Для создания программного массива на MBR-разделах при создании разделов на жёстких дисках следует указать **Тип раздела** равным **Linux RAID**:

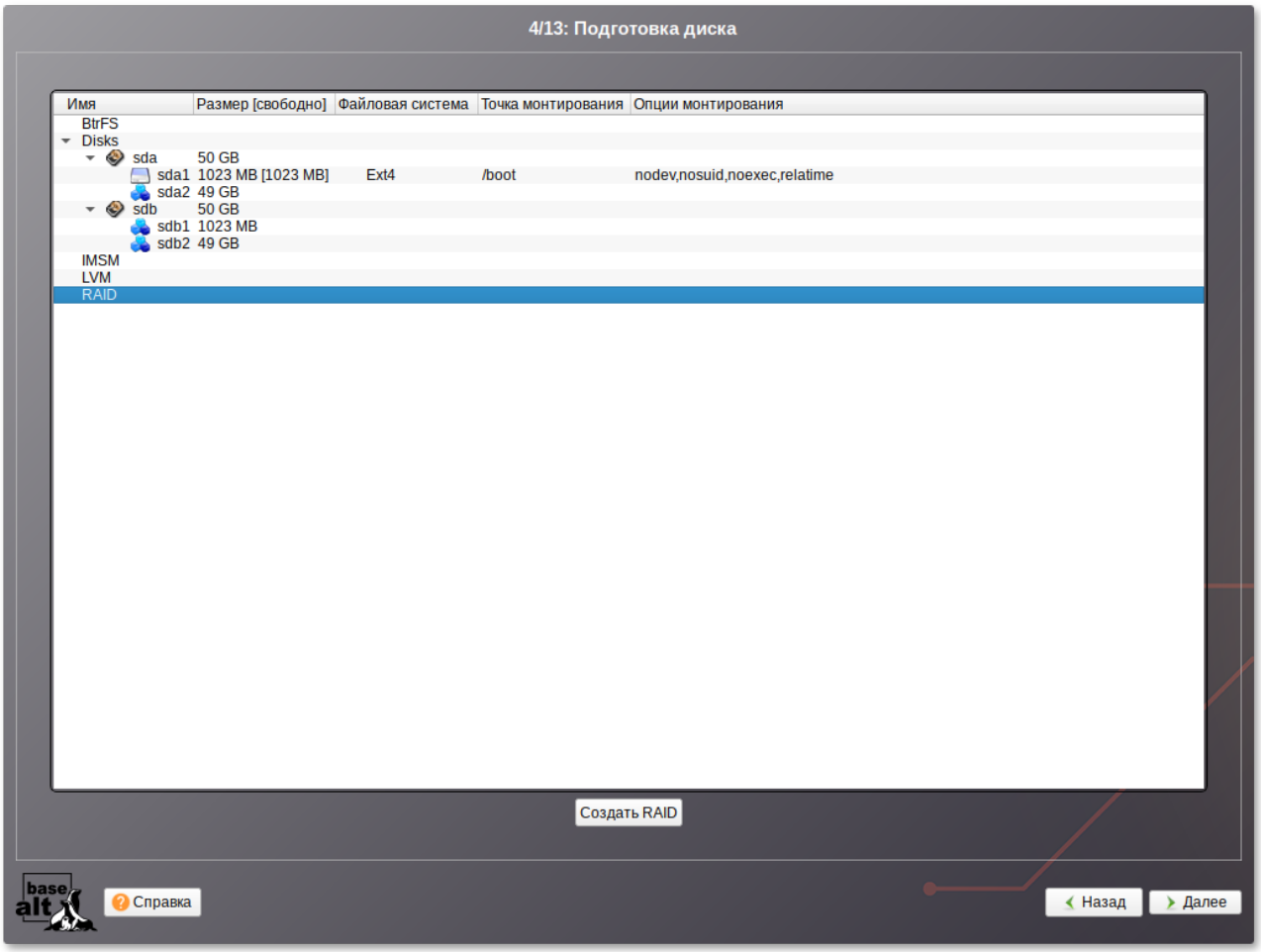


На втором диске создать два раздела с типом **basic data** без создания на них томов. При этом разделы на разных дисках должны совпадать по размеру.

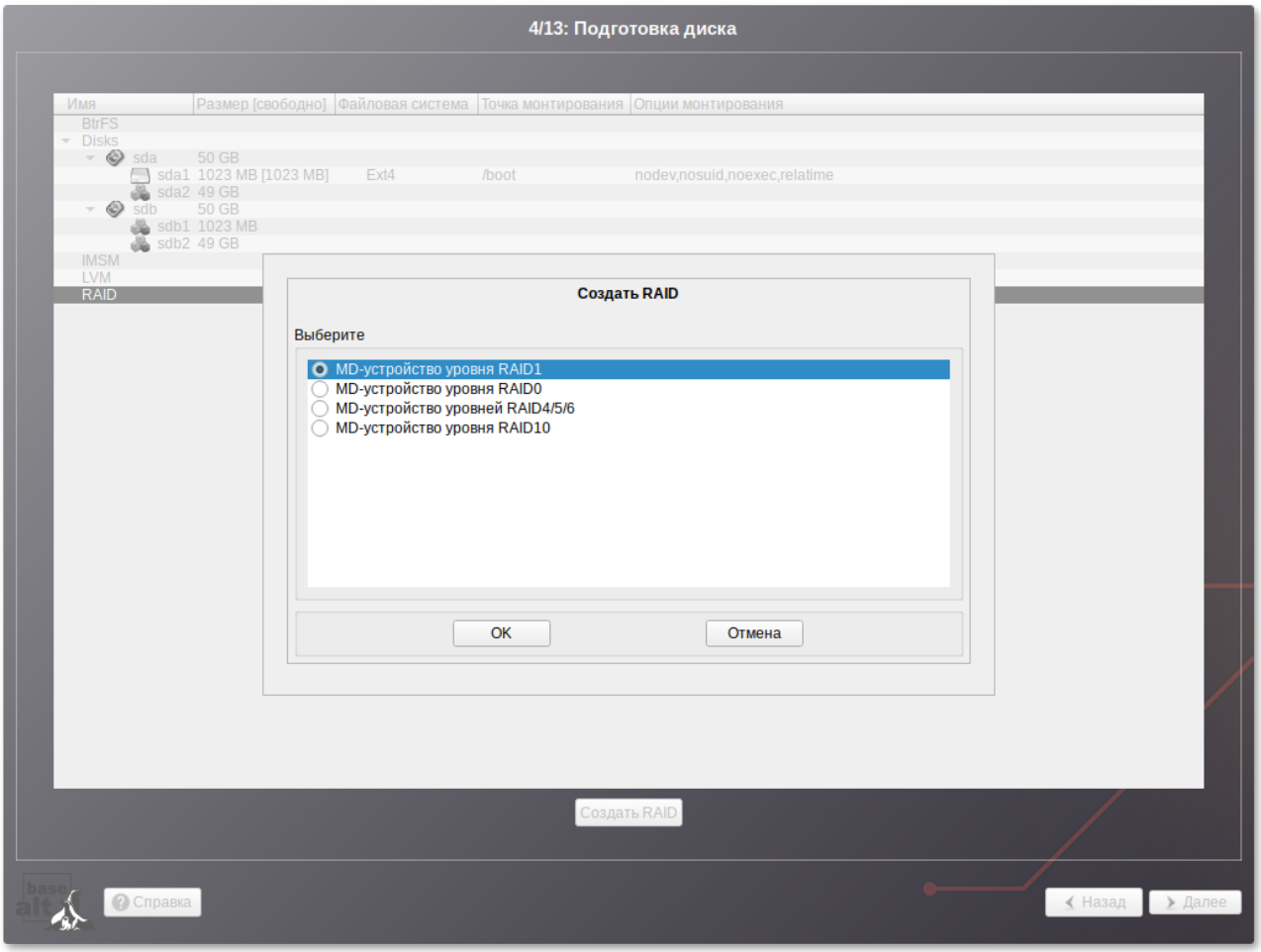
Примечание

При создании разделов следует учесть, что объём результирующего массива может зависеть от размера, включённых в него разделов жёсткого диска. Например, при создании RAID 1 результирующий размер массива будет равен размеру минимального участника.

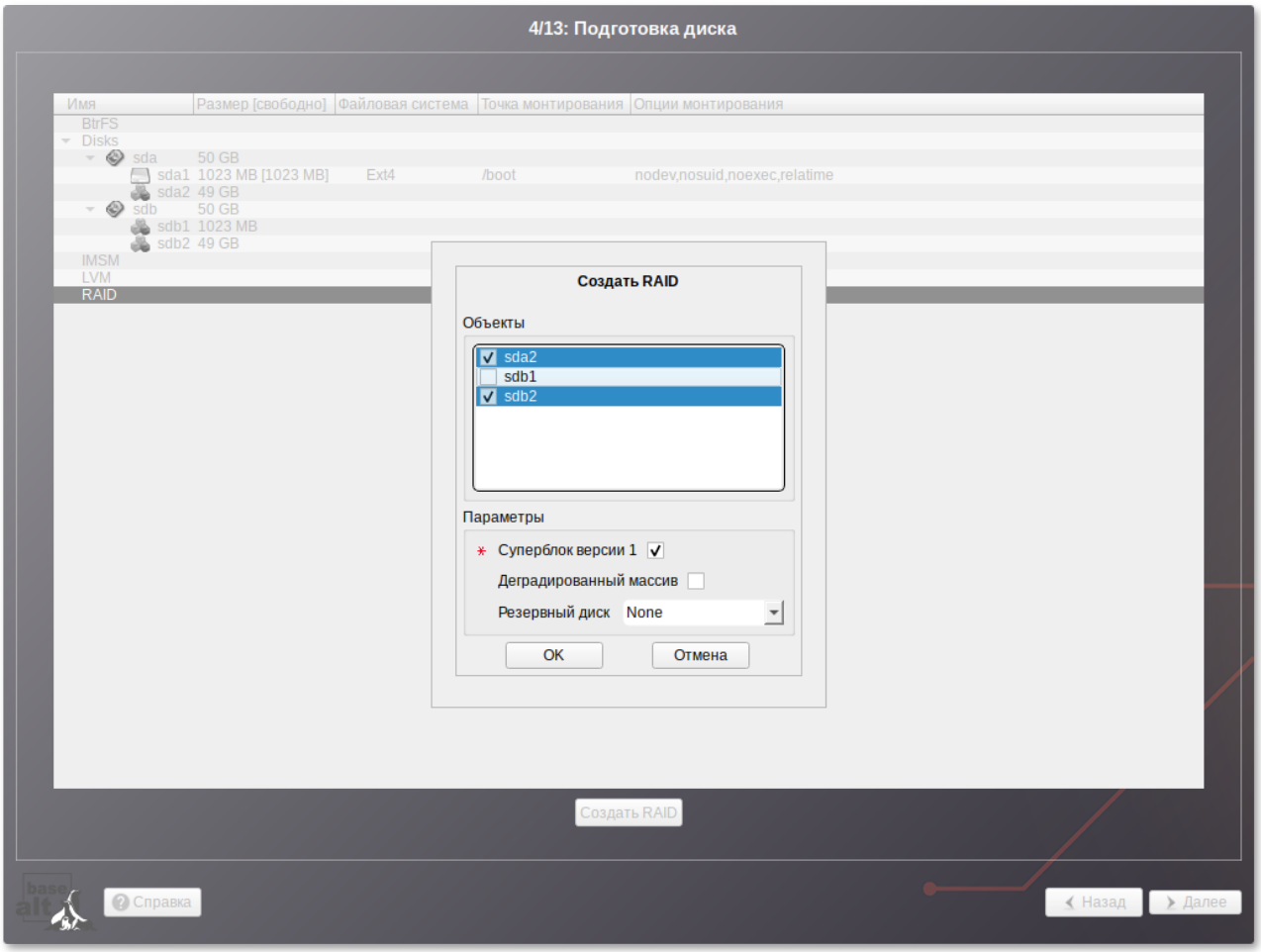
После создания разделов на дисках можно переходить к организации самих RAID-массивов. Для этого в списке следует выбрать пункт **RAID**, после чего нажать кнопку **Создать RAID**:



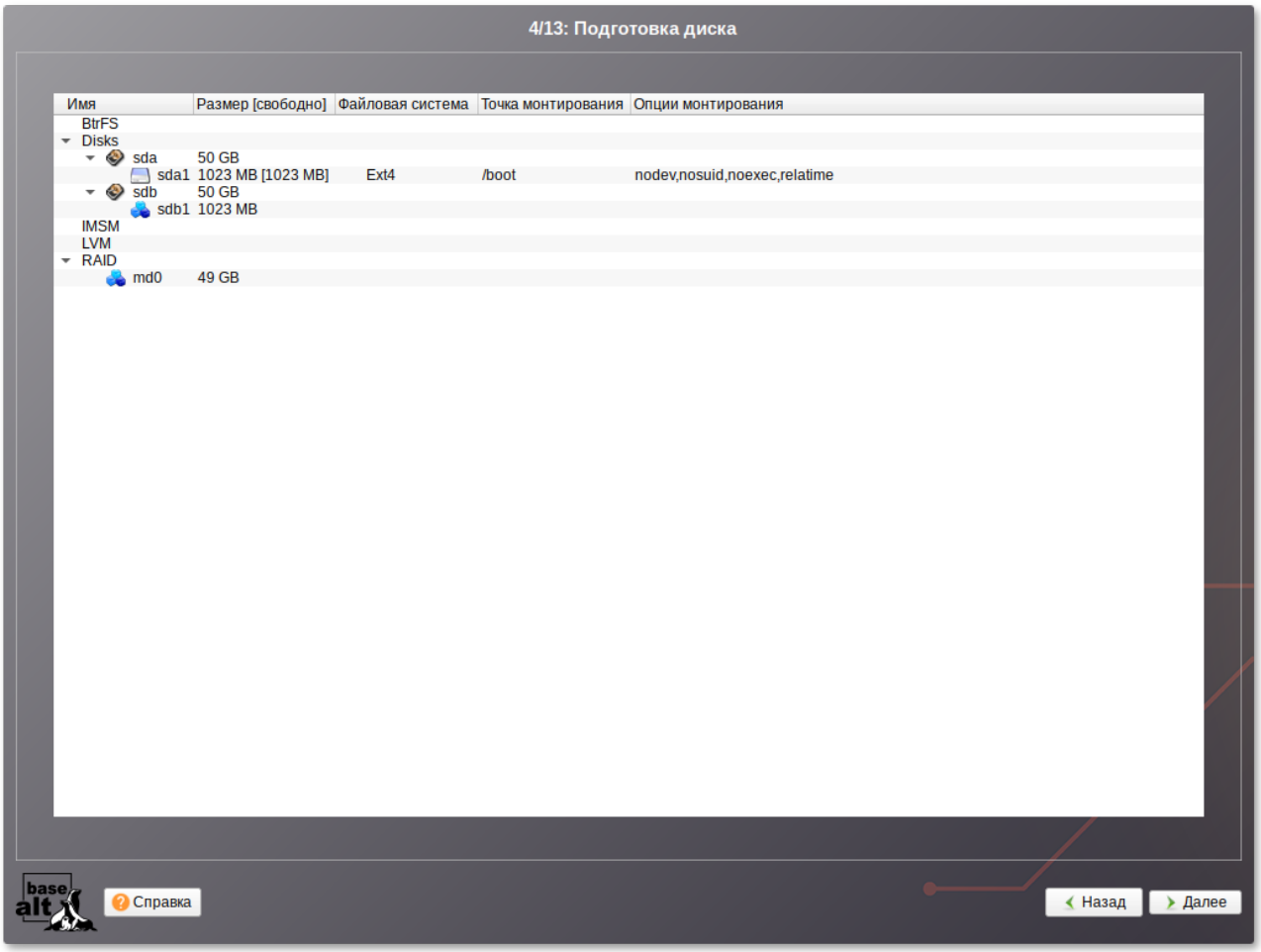
Далее мастер предложит выбрать тип массива:



И указать участников RAID-массива (по умолчанию выбираются все разделы, поэтому необходимо снять отметку с раздела **sdb1**):



Результат создания RAID-массива:



После того, как RAID-массив создан, его можно использовать как обычный раздел на жёстких дисках, то есть на нём можно создавать файловые системы или же, например, включать в LVM-тома.

9.4.2. Создание LVM-томов

Менеджер логических дисков LVM (Logical Volume Manager) — средство гибкого управления дисковым пространством, позволяющее создавать поверх физических разделов (либо неразбитых дисков) логические тома, которые в самой системе будут видны как обычные блочные устройства с данными (обычные разделы).

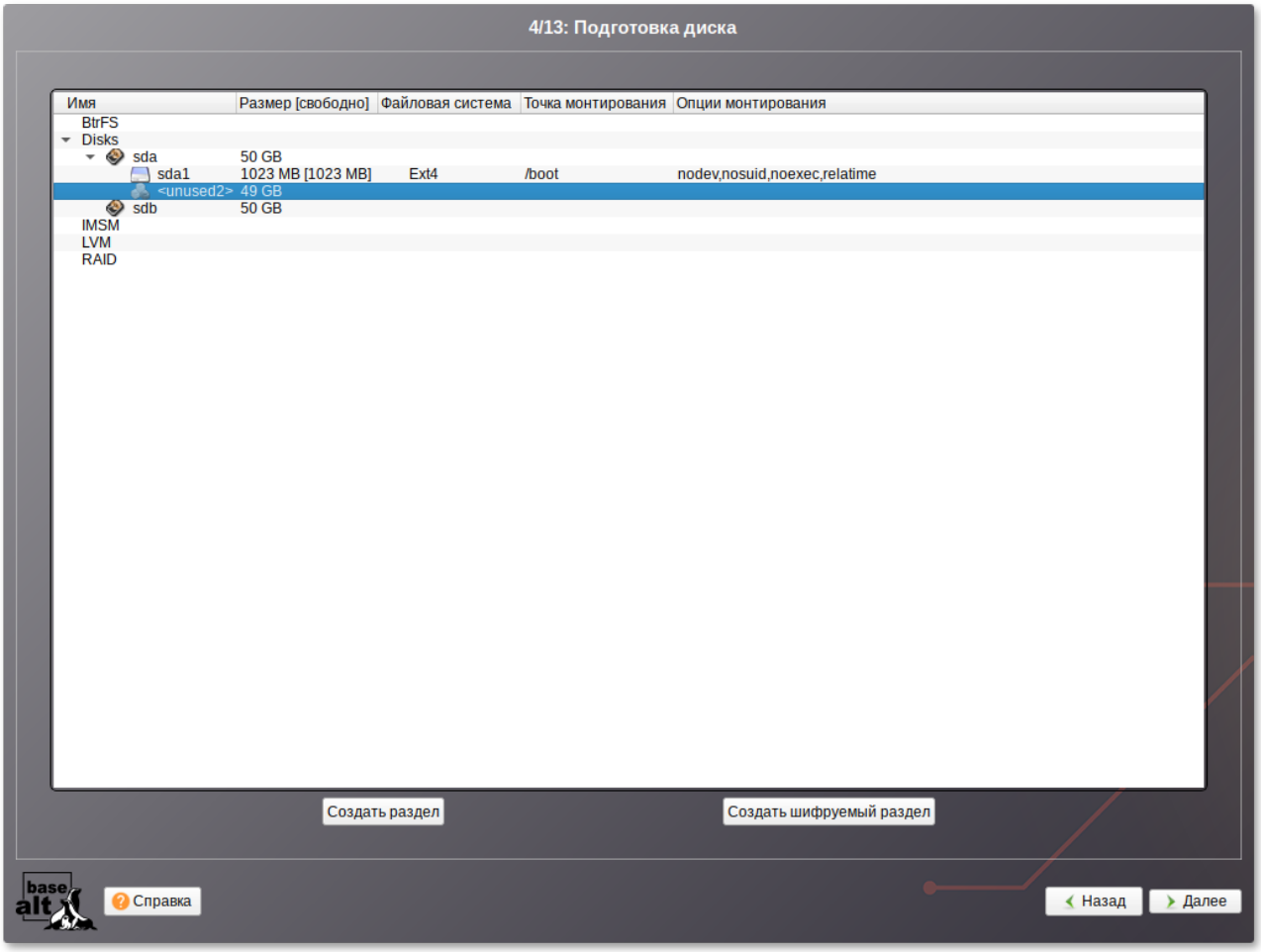
Процесс подготовки к установке на LVM условно можно разбить на следующие шаги:

- создание разделов на жёстких дисках;
- создание группы томов LVM;
- создание томов LVM;
- создание файловых систем на томах LVM.

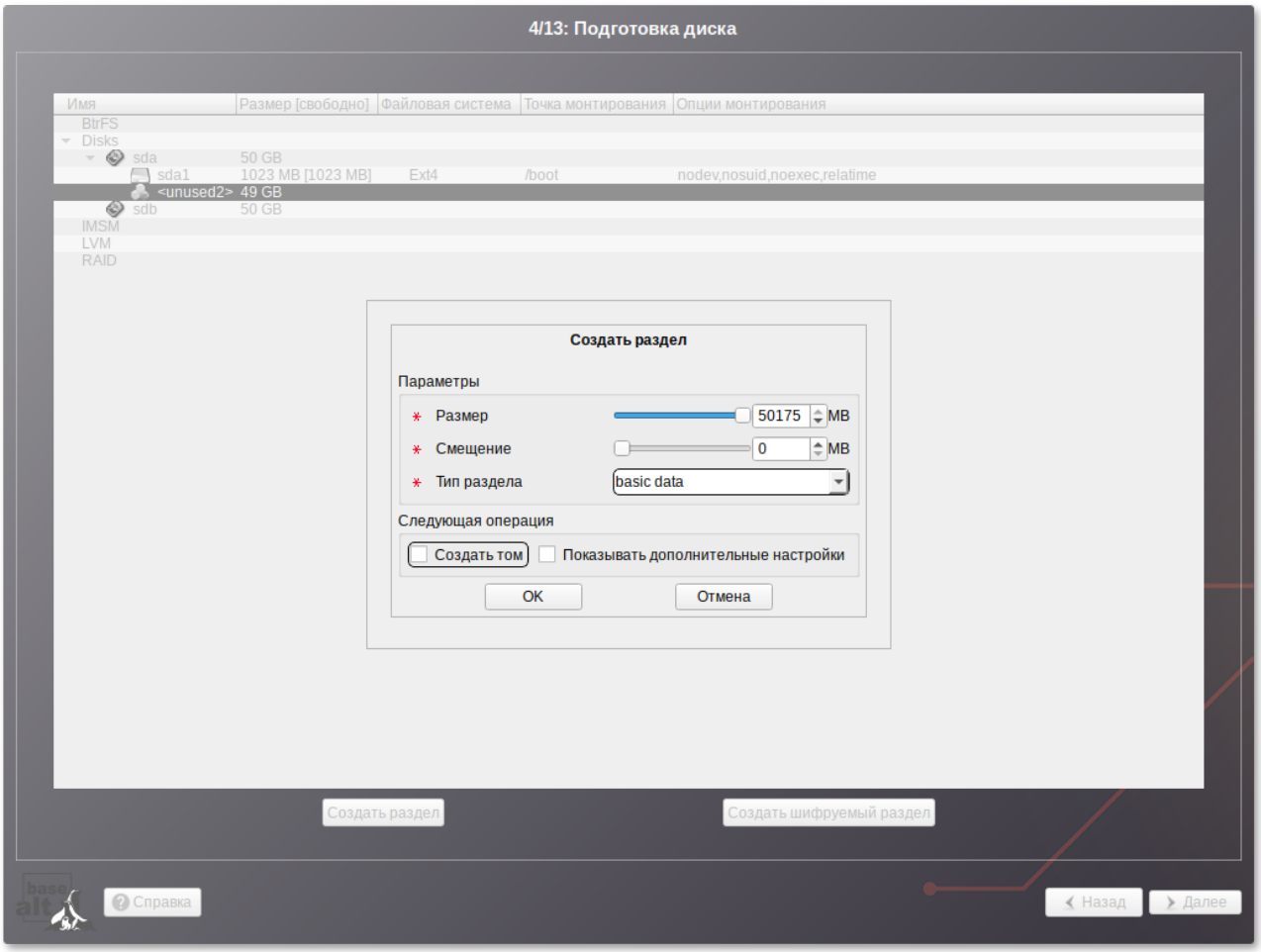
Важно

Для создания группы томов LVM может потребоваться предварительно удалить существующую таблицу разделов с жёсткого диска.

Для настройки параметров нового раздела необходимо выбрать неразмеченный диск в окне профиля разбивки пространства **Вручную** и нажать кнопку **Создать раздел**:

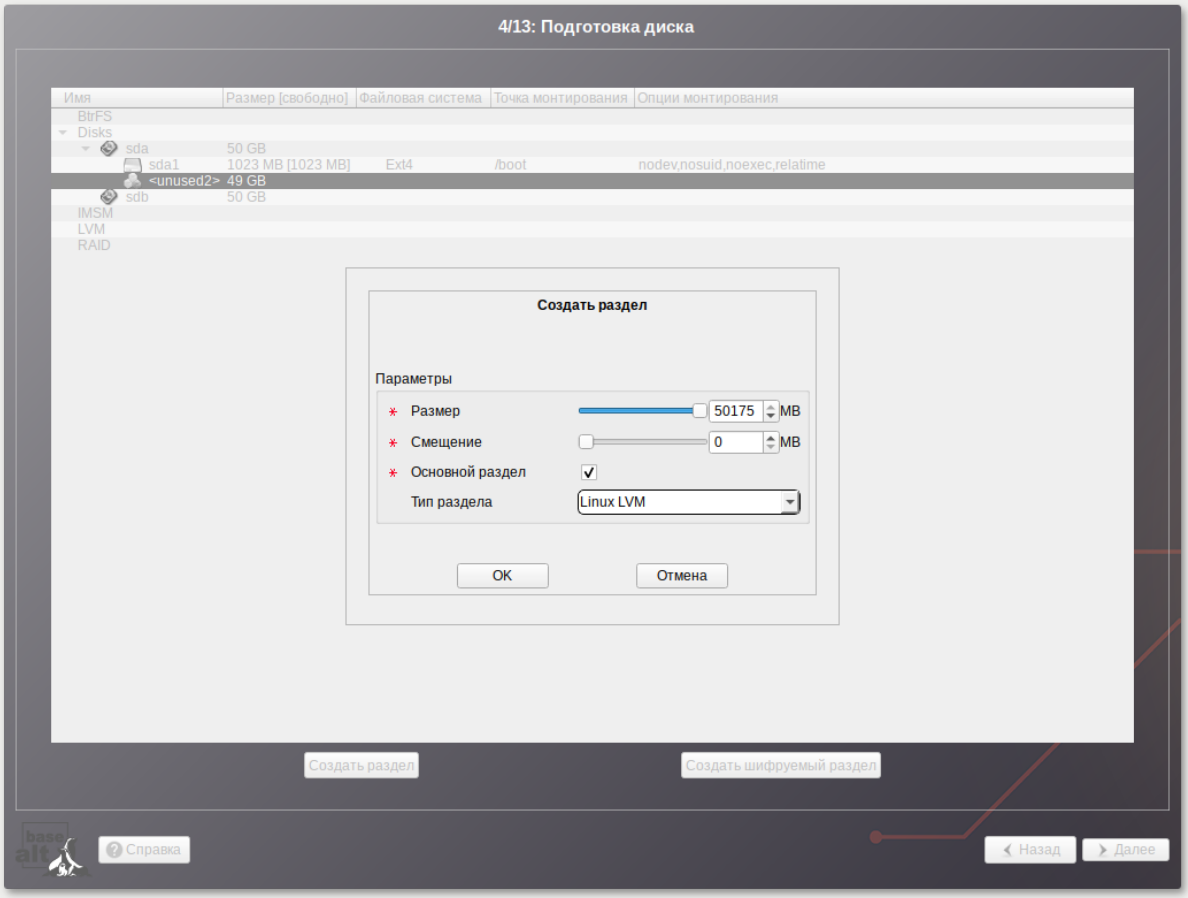


При создании разделов на жёстких дисках для последующего включения их в LVM-тома следует указать **Тип раздела** для них равным **basic data** и не создавать на них том (снять отметку с пункта **Создать том**):

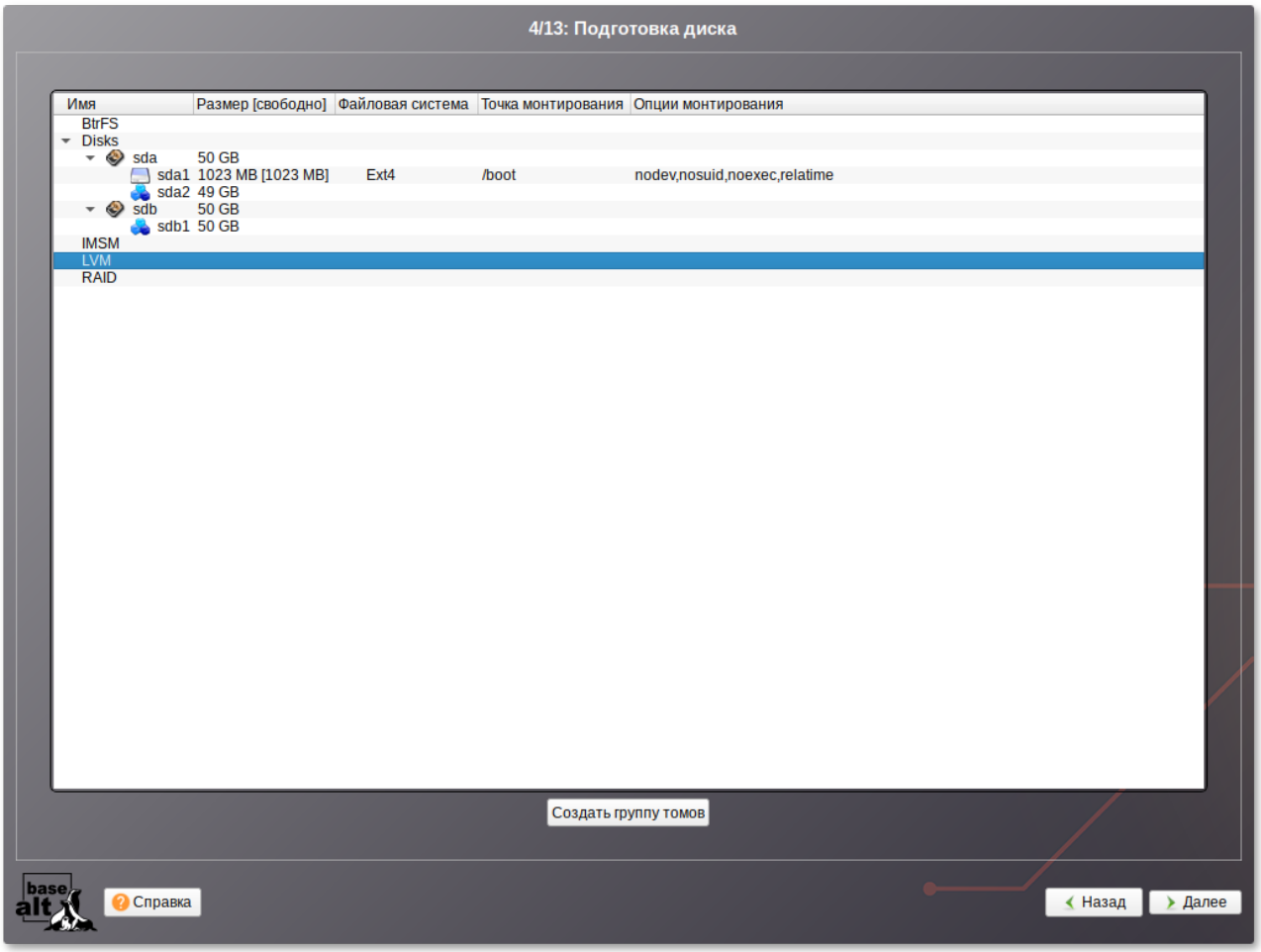

4/13: Подготовка диска
Имя
Размер [свободно]
Файловая система
Точка монтирования
Опции монтирования
BtrFS
Disks
sda
50 GB
sda1
1023 MB [1023 MB]
Ext4
/boot
nodev,nosuid,noexec,relatime
<unused2>
49 GB
sdb
50 GB
IMSM
LVM
RAID
Создать раздел
Параметры
Размер
50175
MB
Смещение
0
MB
Тип раздела
basic data
Следующая операция
Создать том
Показывать дополнительные настройки
OK
Отмена
Создать раздел
Создать шифруемый раздел
Справка
Назад
Далее

Примечание

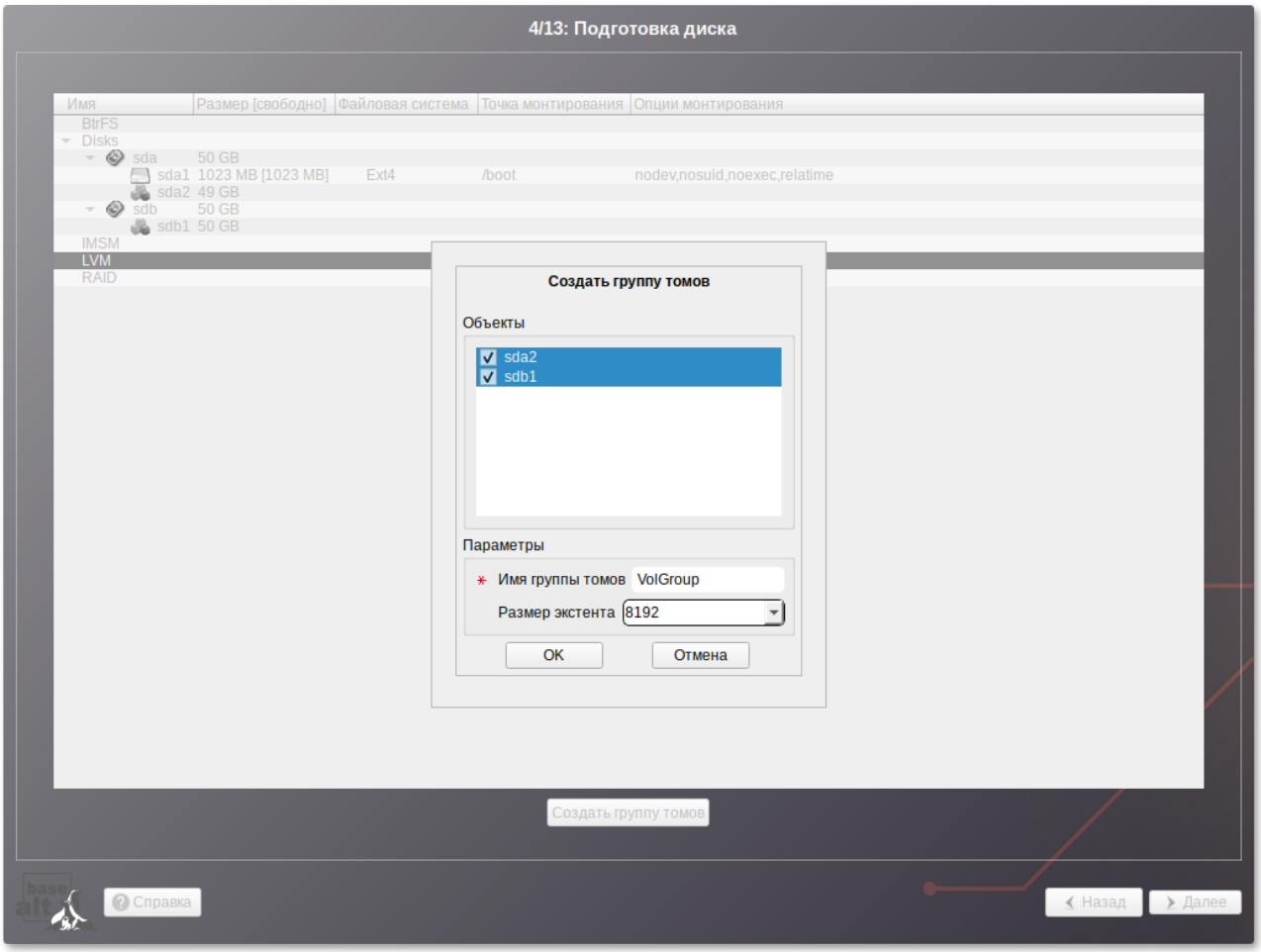
Для создания LVM-тома на MBR-разделах при создании разделов на жёстких дисках следует указать **Тип раздела** равным **Linux LVM**:



После создания разделов на дисках можно переходить к созданию группы томов LVM. Для этого в списке следует выбрать пункт **LVM**, после чего нажать кнопку **Создать группу томов**:



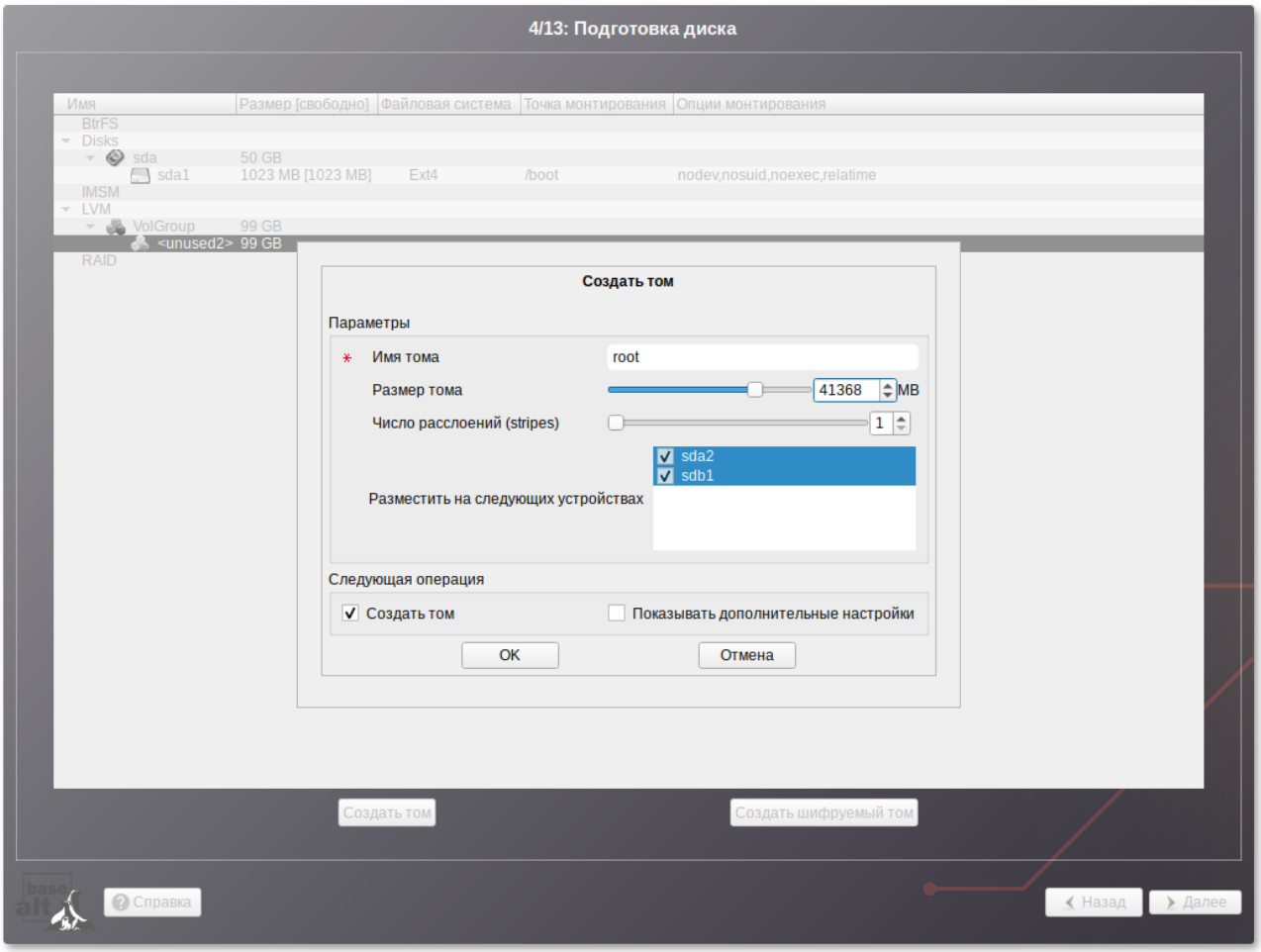
В открывшемся окне необходимо выбрать разделы, которые будут входить в группу томов, указать название группы томов и выбрать размер экстента:



Примечание

Размер экстента представляет собой наименьший объем пространства, который может быть выделен тому. Размер экстента по умолчанию 65536 (65536*512 байт = 32 Мб, где 512 байт — размер сектора).

После того, как группа томов LVM создана, её можно использовать как обычный жёсткий диск, то есть внутри группы томов можно создавать тома (аналог раздела на физическом жёстком диске) и файловые системы внутри томов.



9.4.3. Создание подтомов BtrFS

Подтом (subvolume) не является блочным устройством, но в каждом томе btrfs создаётся один подтом верхнего уровня (subvolid=5), в этом подтоме могут создаваться другие подтома и снапшоты. Подтома (подразделы, subvolumes) создаются ниже вершины дерева BtrFS по мере необходимости, например, для `/` и `/home` создаются подтома с именами @ и @home. Это означает, что для монтирования подтомов необходимы определенные параметры вместо корня системы BtrFS по умолчанию:

- подтом @ монтируется в `/` с помощью опции subvol=@;
- подтом @home, если он используется, монтируется в `/home` с помощью параметра монтирования subvol=@home.

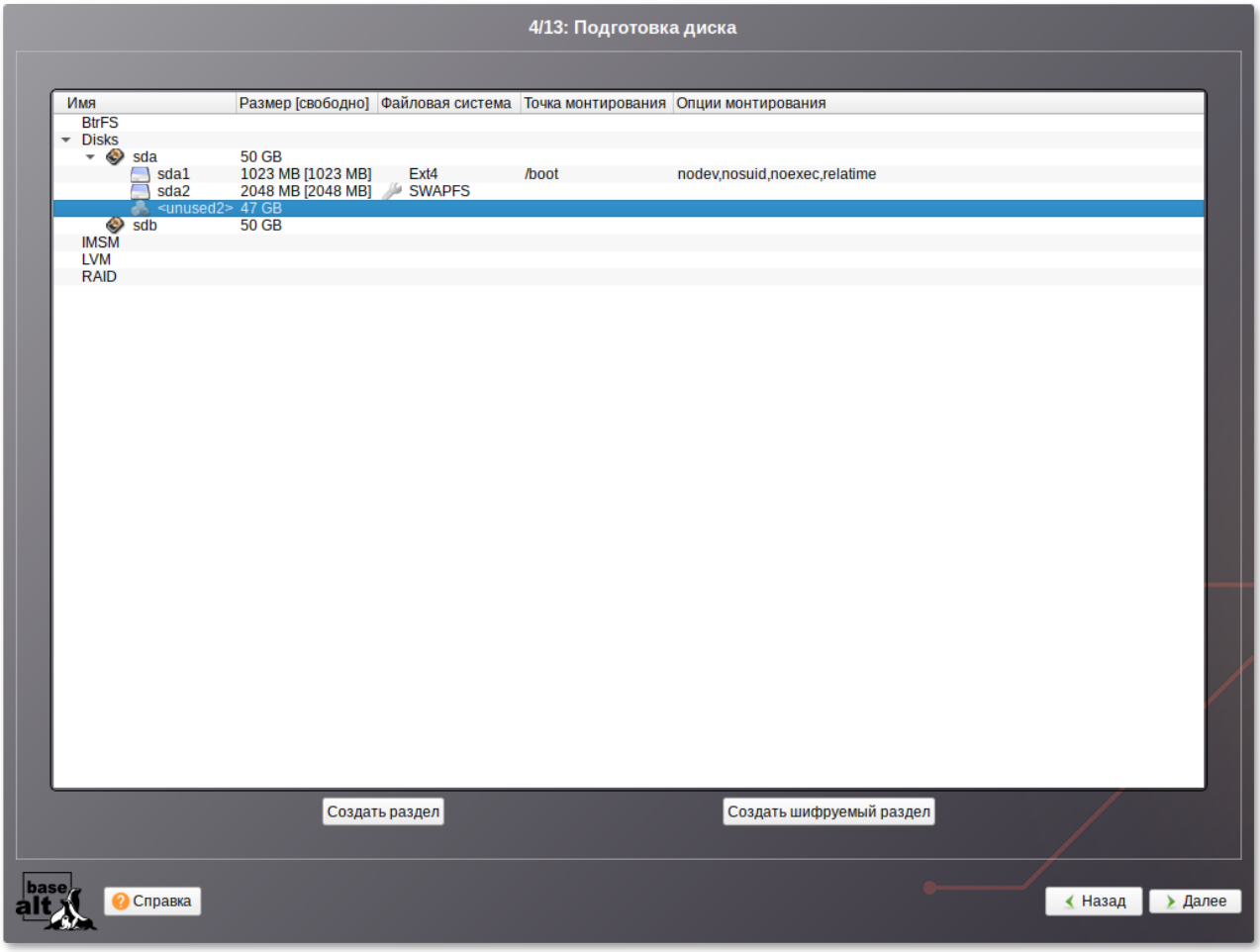
Программа установки Альт Сервер для Эльбрус позволяет создать подтома (subvolume), указав разные точки монтирования.

Процесс подготовки к установке на подтома условно можно разбить на следующие шаги:

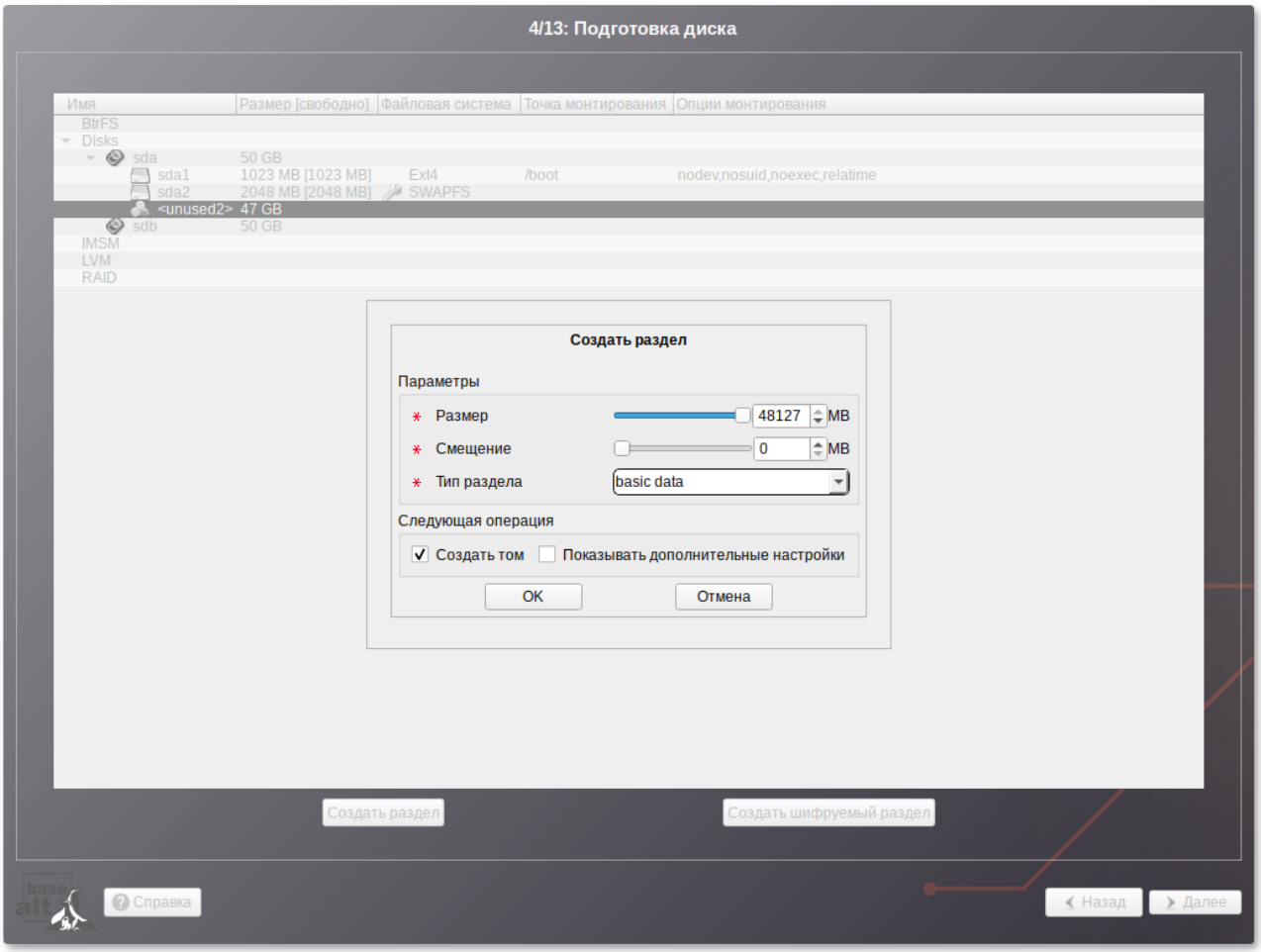
- создание разделов на жёстких дисках;
- создание подтомов на разделах жёсткого диска.

В данном разделе рассмотрен вариант подготовки раздела BtrFS с разбивкой на подразделы @ и @home.

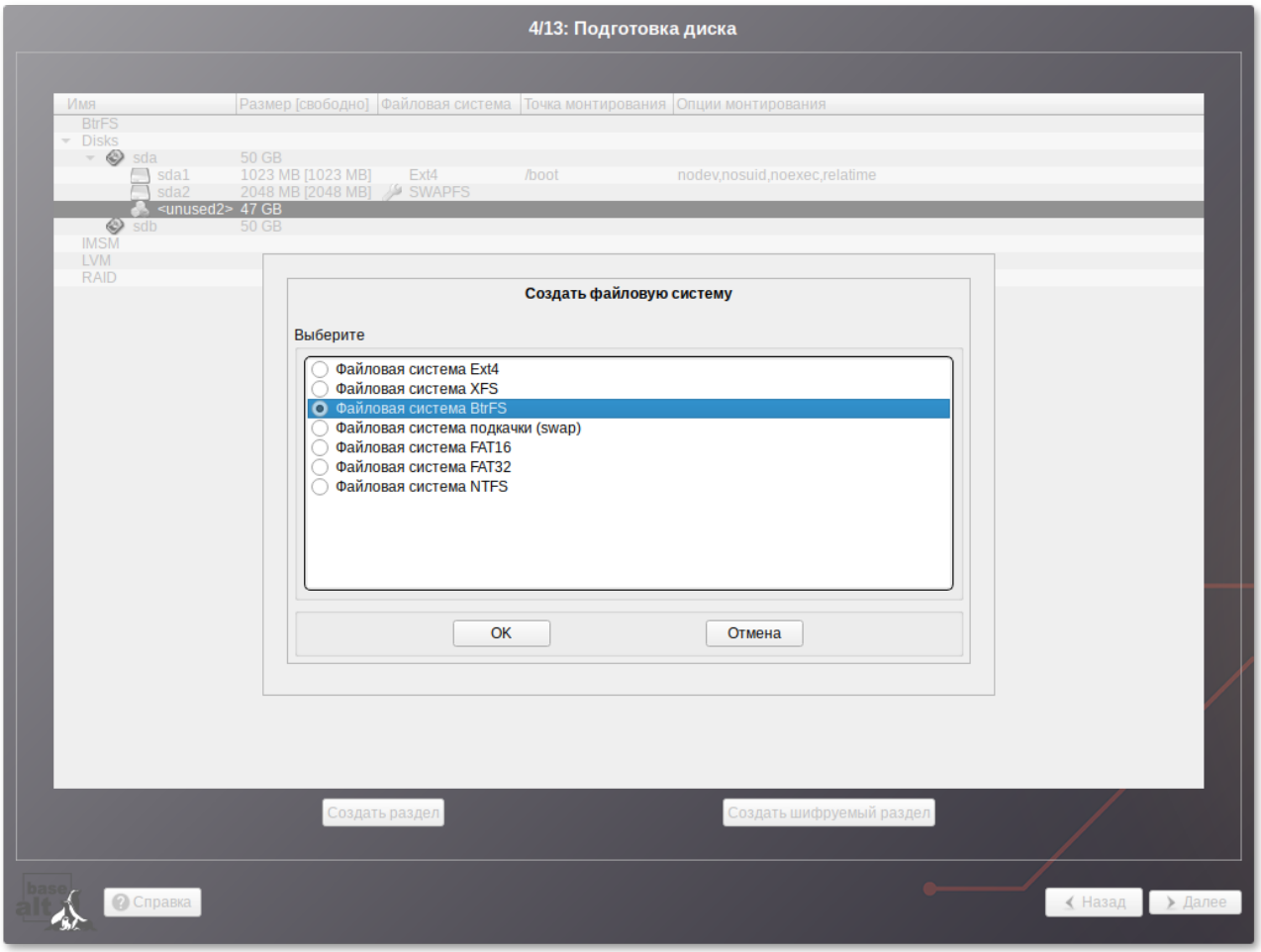
Для настройки параметров нового раздела необходимо выбрать неразмеченный диск в окне профиля разбивки пространства **Вручную** и нажать кнопку **Создать раздел**:



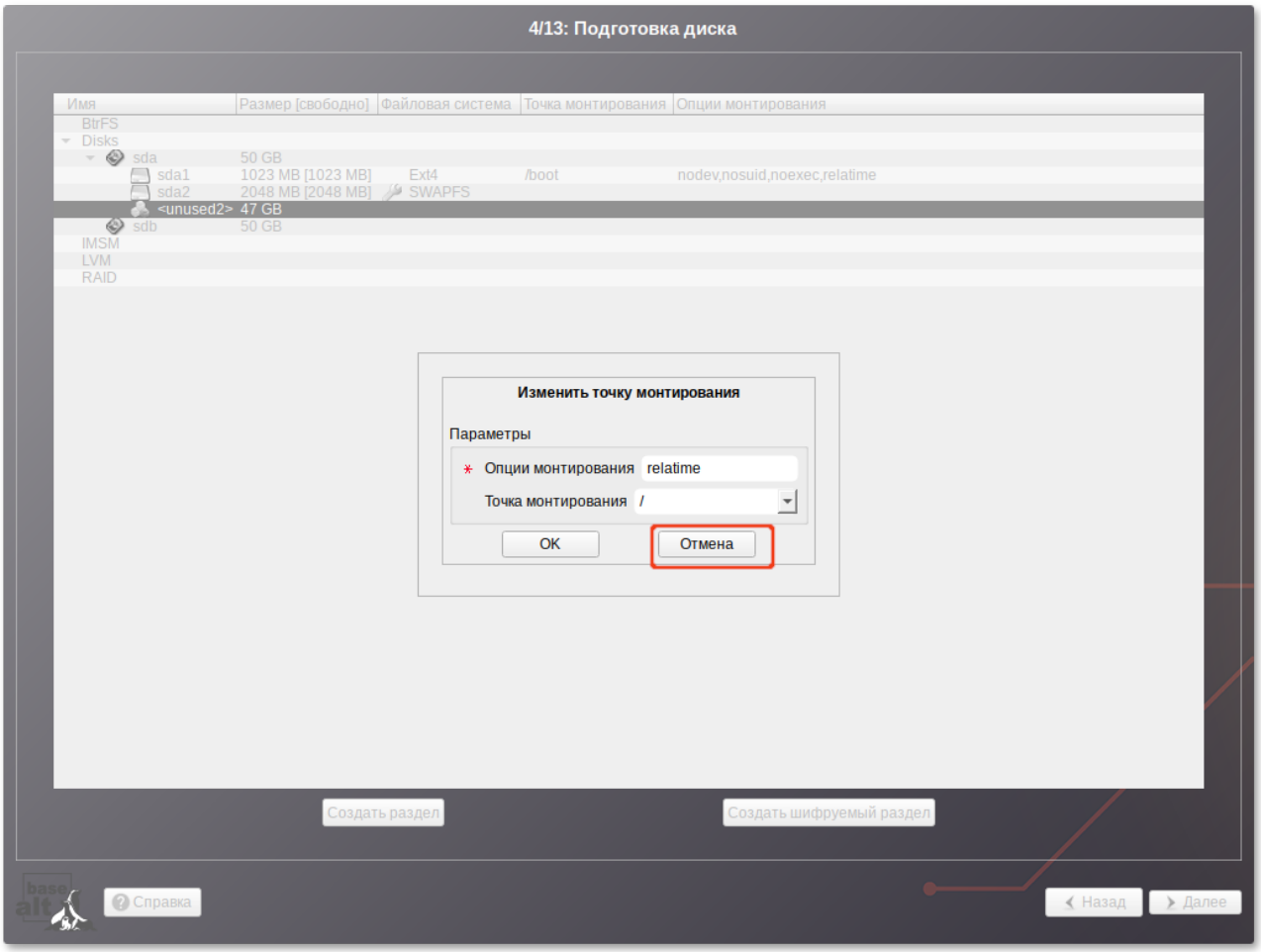
При создании раздела на жёстком диске следует указать **Тип раздела** равным **basic data** (**Linux** для MBR):



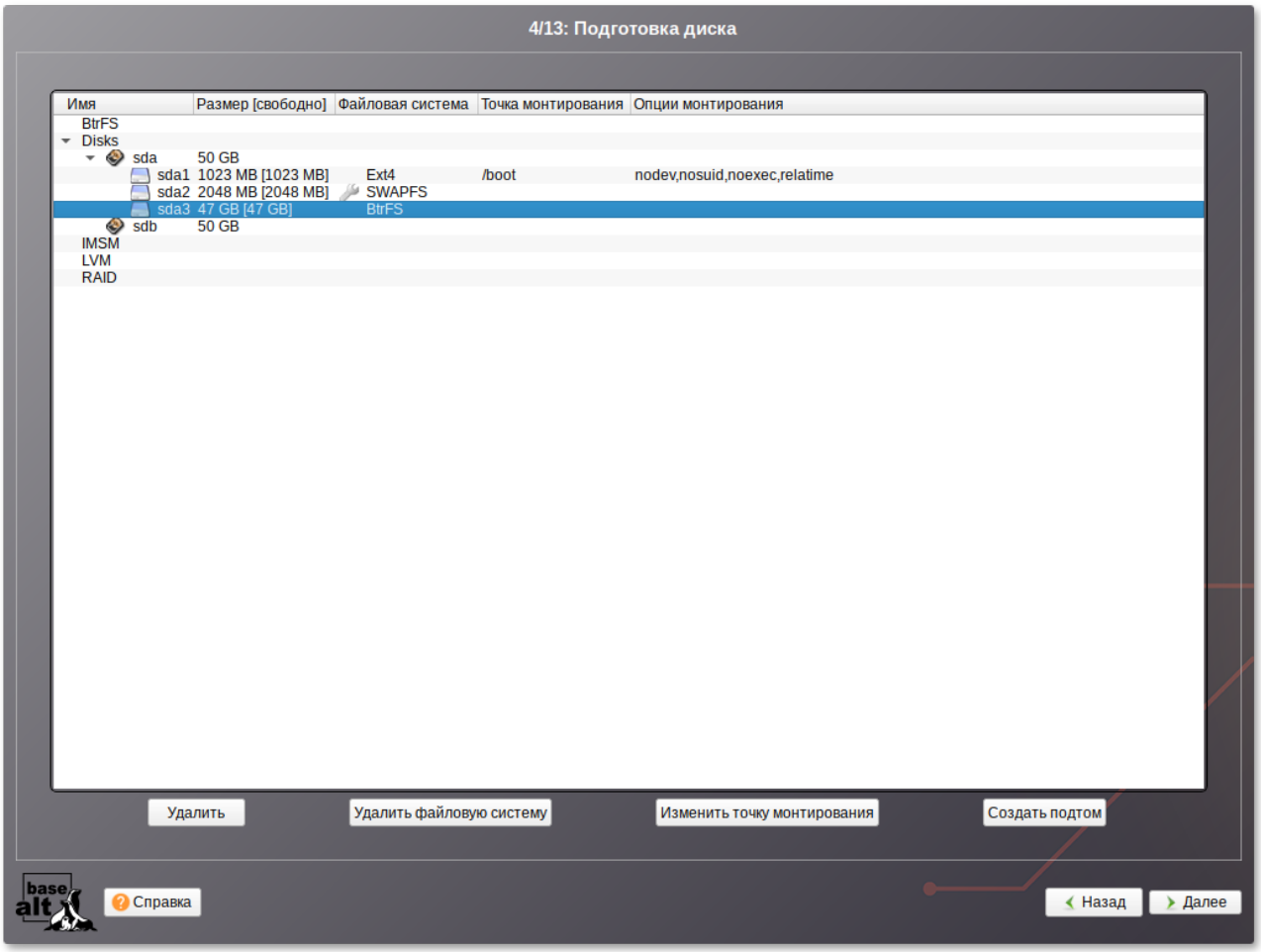
На следующем шаге выбрать файловую систему BtrFS:



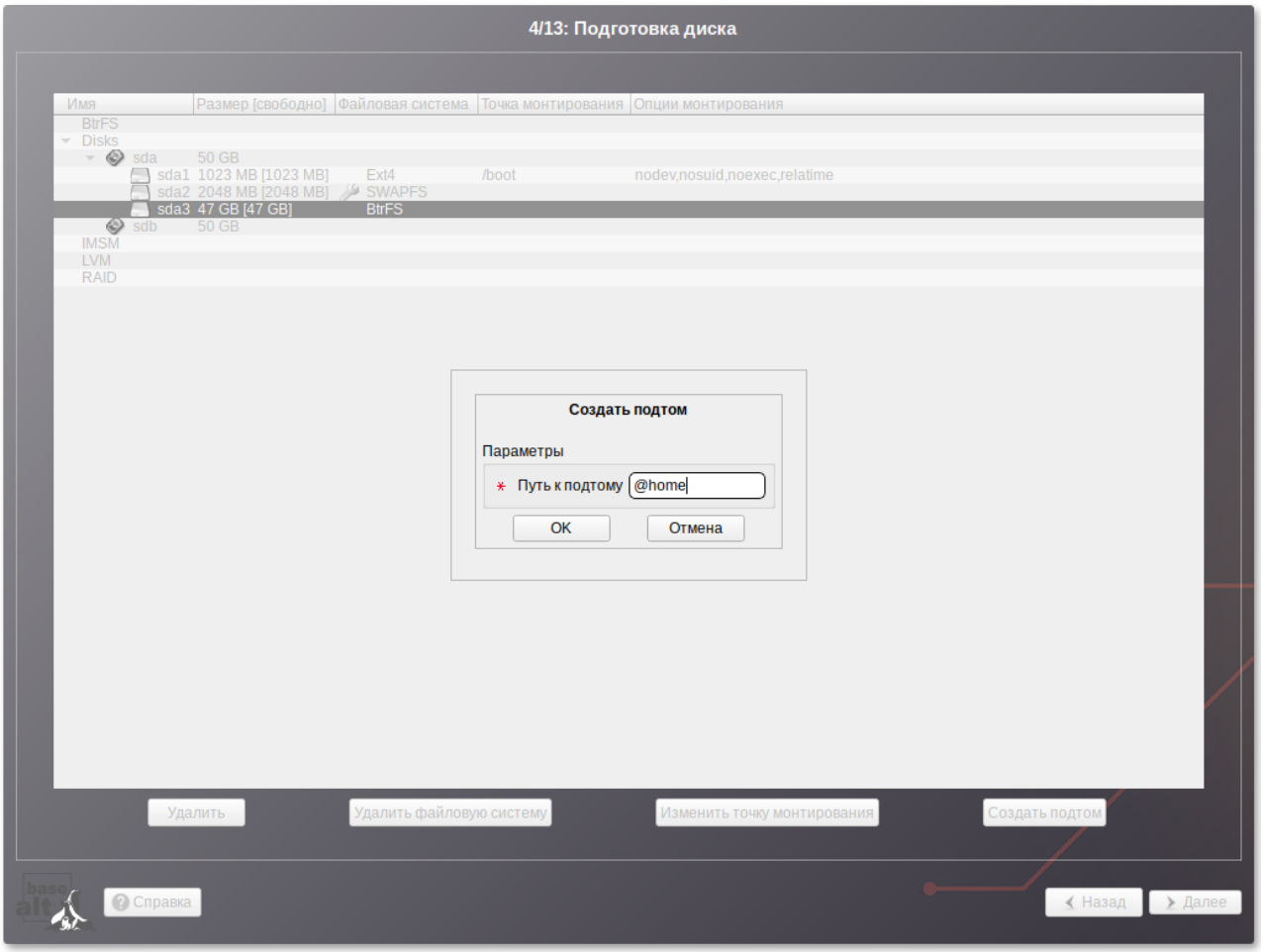
В окне **`Изменить точку монтирования`** нажать кнопку **`Отмена`** (не указывать точку монтирования для раздела):



После создания раздела можно переходить к созданию подтомов. Для этого в списке следует выбрать раздел с файловой системой BtrFS, после чего нажать кнопку **`Создать подтом`**:

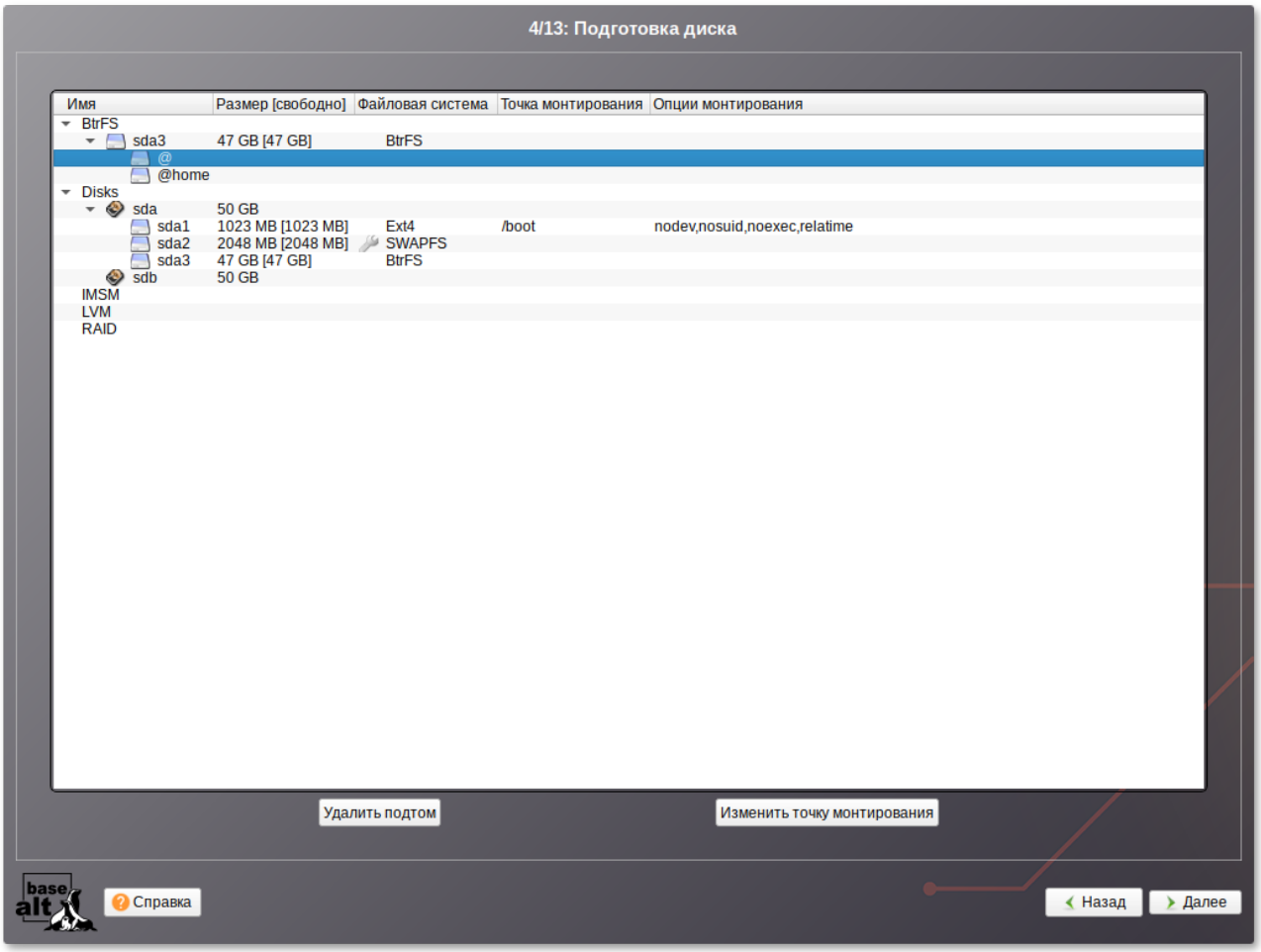


В открывшемся окне следует указать имя подтома или путь до него. Создание подтома @home:

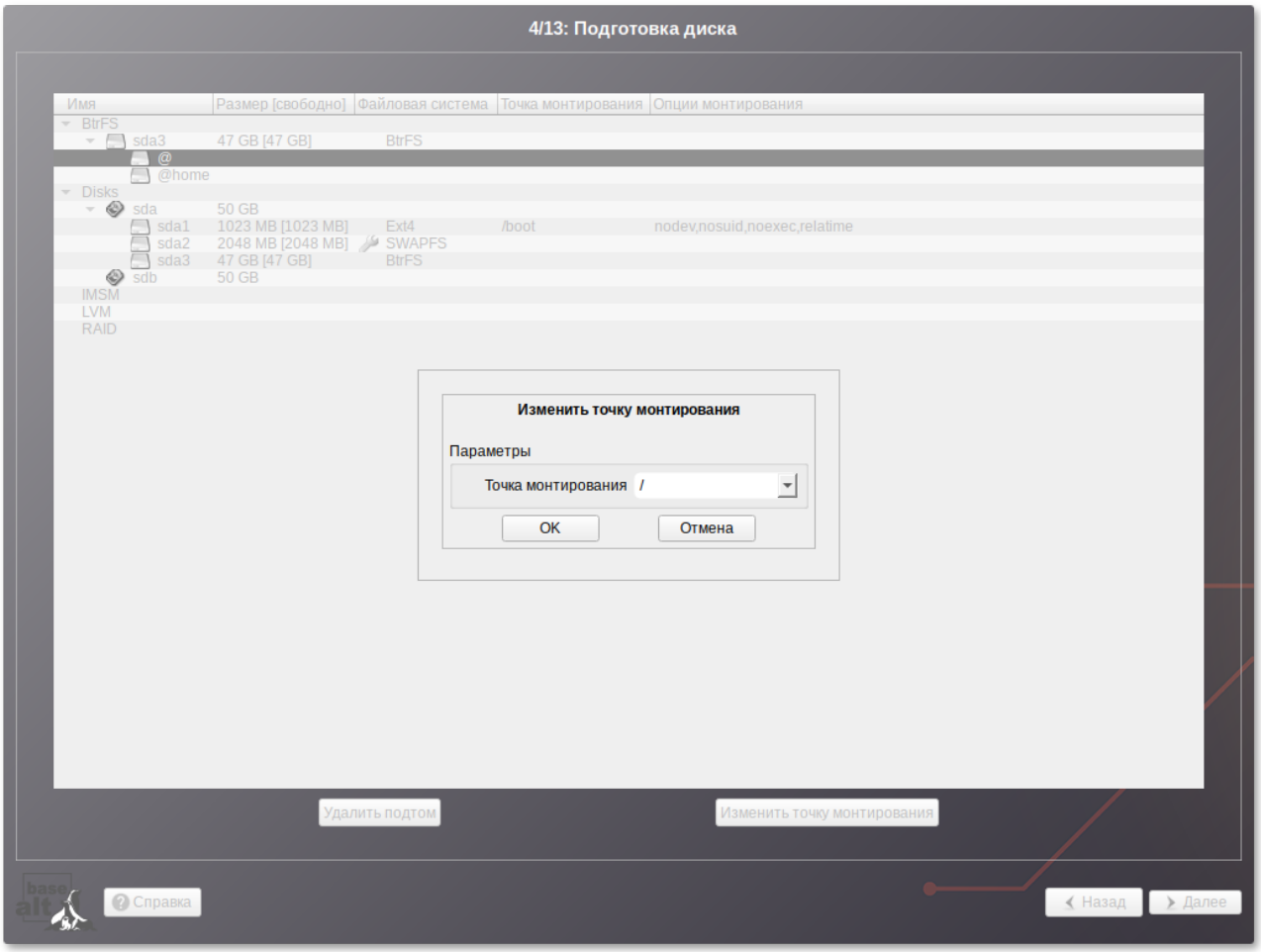


Данное действие следует повторить для создания подтома @.

После создания подтомов необходимо указать точки монтирования для каждого тома. Для этого выбрать подтом и нажать кнопку **`Изменить точку монтирования`**:



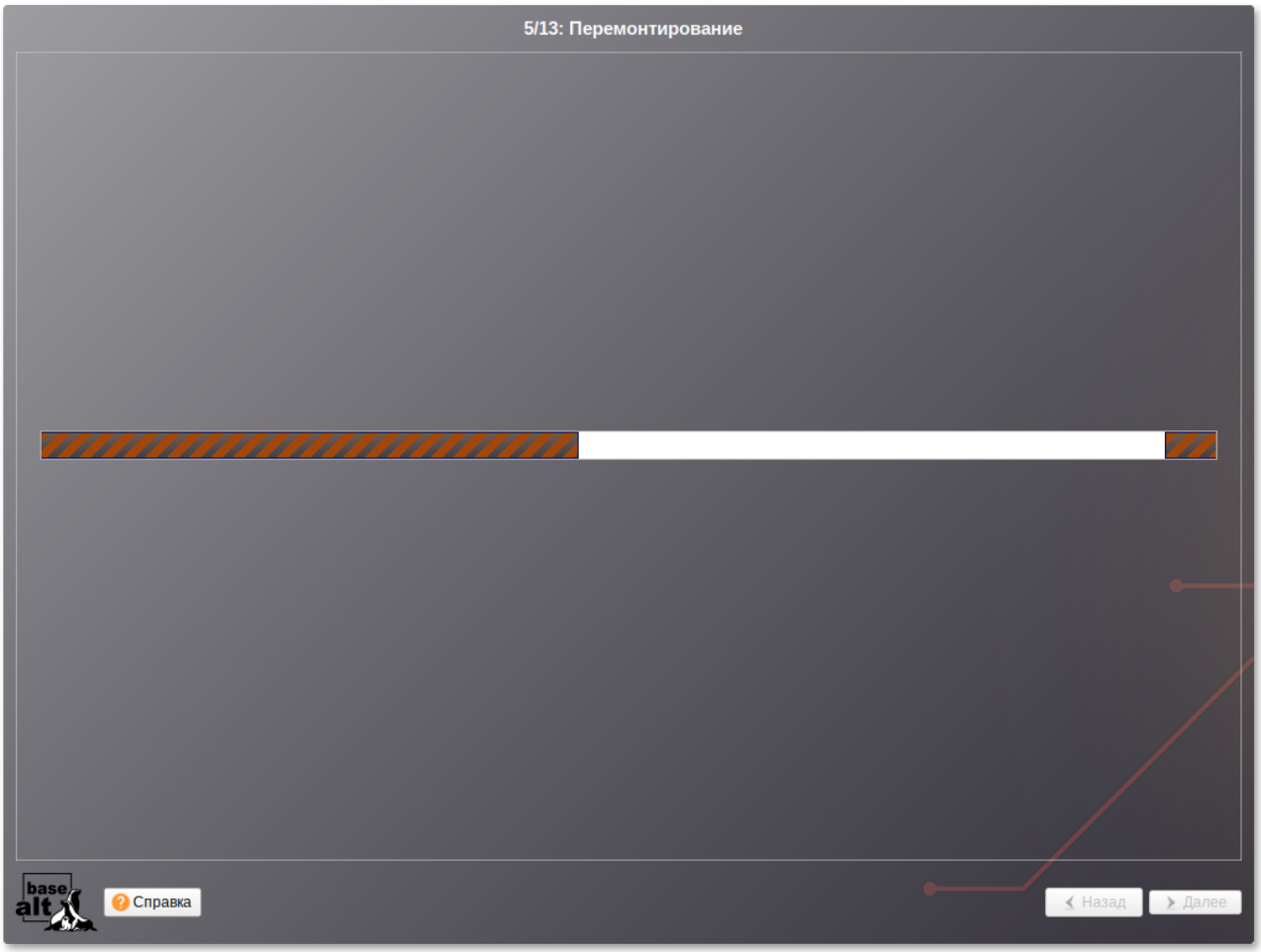
В открывшемся окне указать точку монтирования:



Далее можно установить систему как обычно.

Глава 10. Перемонтирование

По завершении этапа подготовки диска начинается шаг перемонтирования. Он проходит автоматически и не требует вмешательства пользователя. На экране отображается индикатор выполнения.

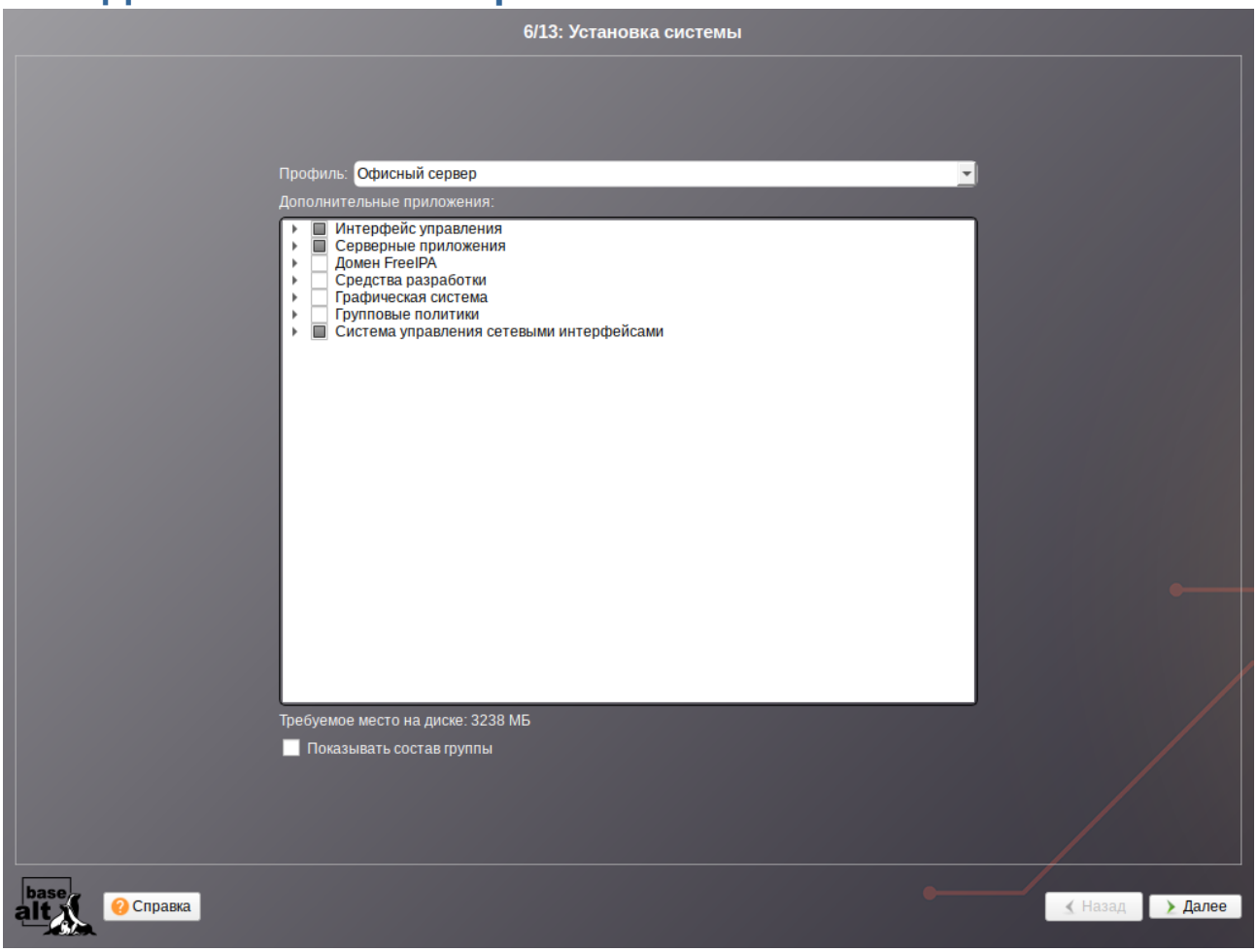


Глава 11. Установка системы

На данном этапе происходит распаковка ядра и установка набора программ, необходимых для работы Альт Сервер для Эльбрус.

Программа установки предлагает выбрать дополнительные пакеты программ, которые будут включены в состав Альт Сервер для Эльбрус и установлены вместе с ней на диск.

11.1. Дополнительные приложения



В дистрибутиве Альт Сервер для Эльбрус доступно значительное количество программ, часть из них составляет саму операционную систему, а остальные — это прикладные программы и утилиты.

В Альт Сервер для Эльбрус все операции установки и удаления производятся над пакетами — отдельными компонентами системы. Пакет и программа соотносятся неоднозначно: иногда одна программа состоит из нескольких пакетов, иногда один пакет включает несколько программ.

В процессе установки системы обычно не требуется детализированный выбор компонентов на уровне пакетов — это требует слишком много времени и знаний от проводящего установку, тем более, что комплектация дистрибутива подбирается таким образом, чтобы из имеющихся программ можно было составить полноценную рабочую среду для соответствующей аудитории пользователей. Поэтому в процессе установки системы пользователю предлагается выбрать из небольшого списка групп пакетов именно те, которые необходимы для решения наиболее распространённых задач. Под списком групп на экране отображается информация об объёме дискового пространства, которое будет занято после установки пакетов, входящих в выбранные группы.

При установке сервера доступны следующие профили:

- **Офисный сервер** — для установки будут предложены группы пакетов с серверными приложениями и система управления сетевыми интерфейсами systemd-networkd;
- **Сервер Samba DC (контроллер AD)** — для установки будут предложена группа пакетов для конфигурации сервера в качестве контроллера AD;

- **Домашний сервер** — в состав устанавливаемых пакетов будут включены инструменты диагностики, графическая среда MATE и система управления сетевыми интерфейсами NetworkManager;
- **Минимальная установка** — дополнительное ПО в состав устанавливаемых пакетов включаться не будет.

После выбора профиля можно изменить состав устанавливаемых пакетов.

Примечание

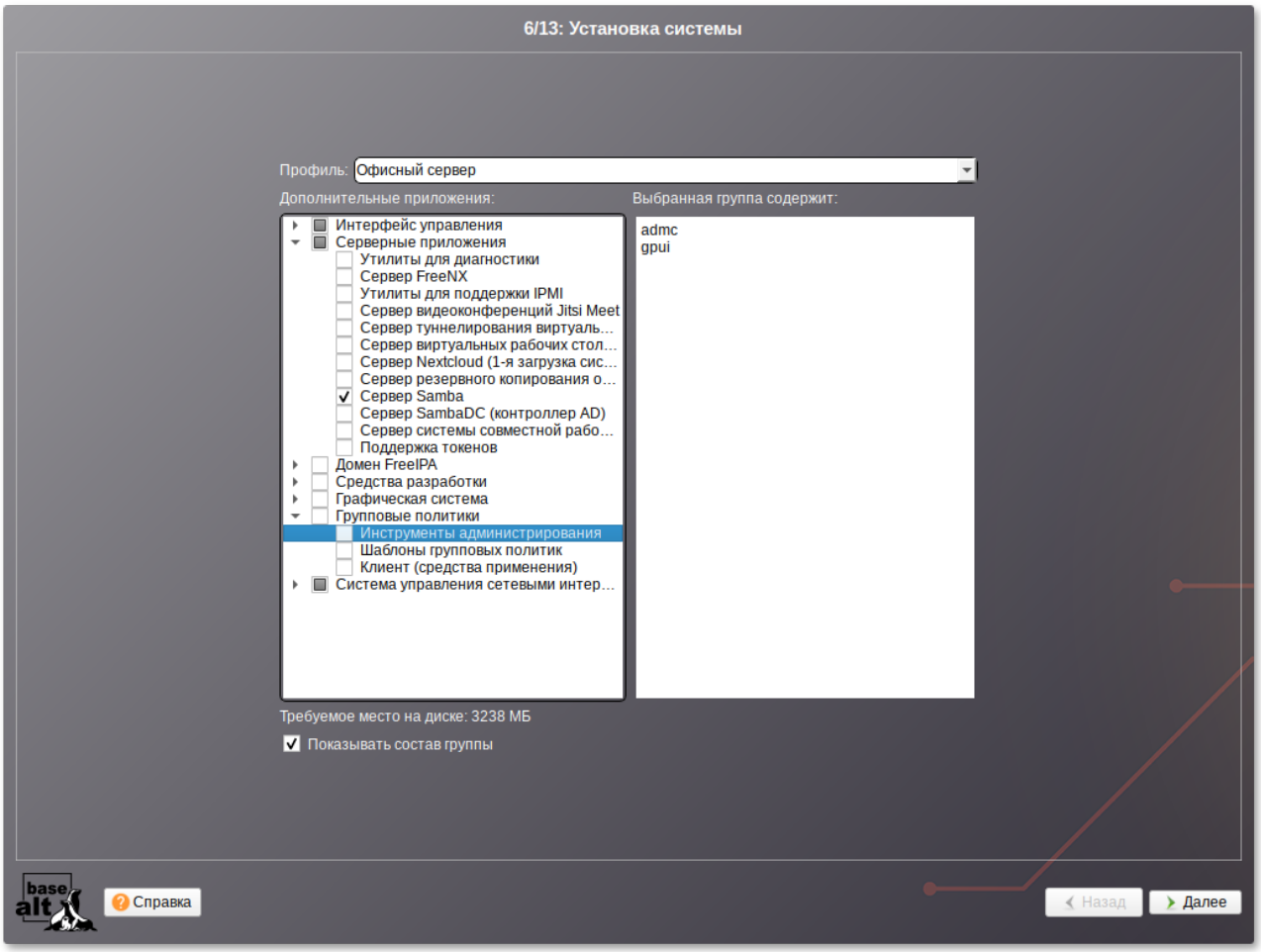
При установке серверного приложения **Сервер Nextcloud** после загрузки будет доступна служба Nextcloud 27. Для доступа к административным функциям этого приложения через веб-интерфейс необходимо сменить пароль администратора в «Центре управления системой» (пароль должен быть достаточно сложным и содержать не менее 10 символов).

Веб-приложение Nextcloud, установленное при установке системы, будет доступно по адресу https://localhost/nextcloud/. Администратор: ncadmin, пароль: пароль пользователя root.

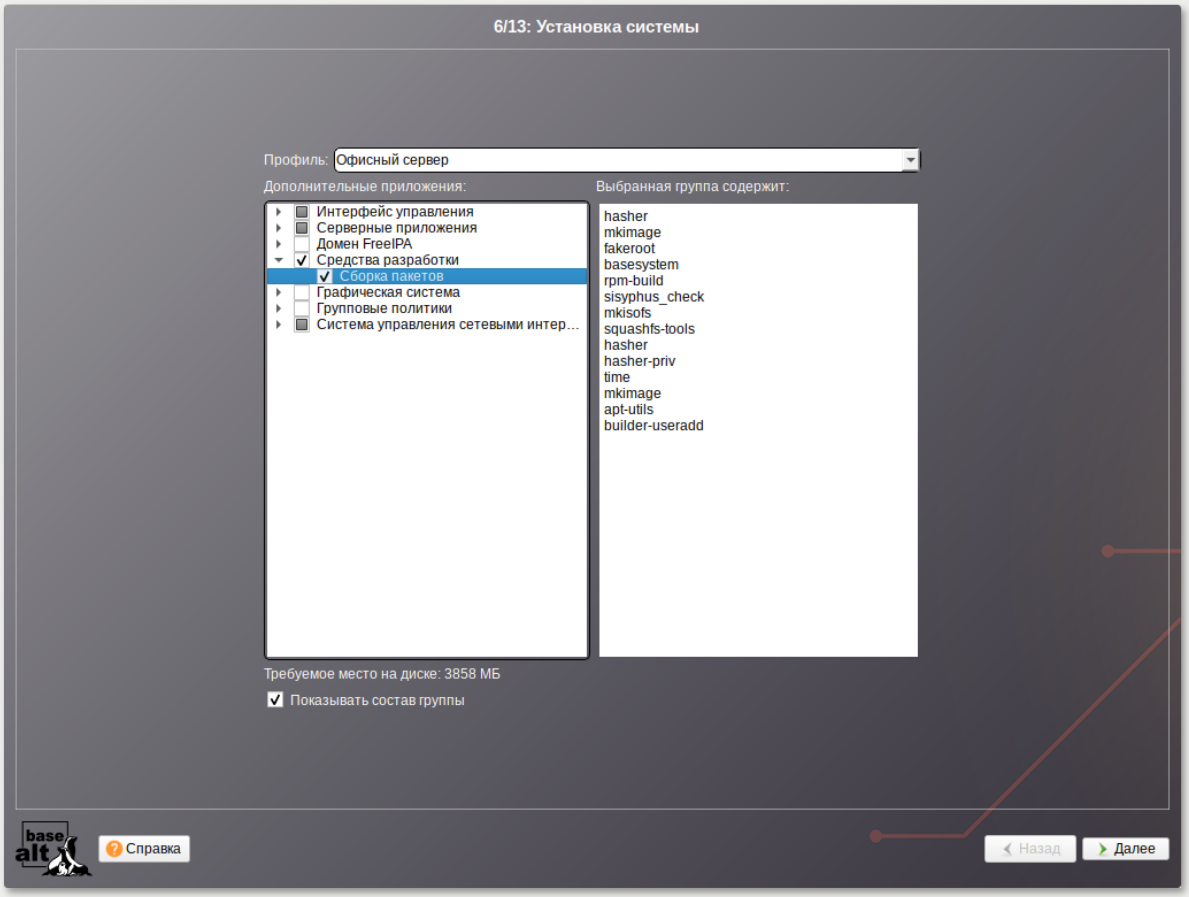
При первом запуске установленной системы запускаются скрипты настройки данного приложения, поэтому первый запуск системы может занять достаточно продолжительное время.

Под списком групп на экране отображается информация об объёме дискового пространства, которое будет занято после установки пакетов, входящих в выбранные группы.

Опция **Показать состав группы** выводит список программных пакетов, входящих в состав той или иной группы пакетов.


6/13: Установка системы
Профиль: Офисный сервер
Дополнительные приложения:
Выбранная группа содержит:
Интерфейс управления
Серверные приложения
Утилиты для диагностики
Сервер FreeNX
Утилиты для поддержки IPMI
Сервер видеоконференций Jitsi Meet
Сервер туннелирования виртуаль…
Сервер виртуальных рабочих стол…
Сервер Nextcloud (1-я загрузка сис…
Сервер резервного копирования о…
Сервер Samba
Сервер SambaDC (контроллер AD)
Сервер системы совместной рабо…
Поддержка токенов
Домен FreeIPA
Средства разработки
Графическая система
Групповые политики
Инструменты администрирования
Шаблоны групповых политик
Клиент (средства применения)
Система управления сетевыми интер…
admc
gpui
Требуемое место на диске: 3238 МБ
Показывать состав группы
Справка
Назад
Далее

Примечание



Если выбрана группа пакетов **`Сборка пакетов`**, после установки системы необходимо настроить пользователя для сборки. Для этого следует выполнить команду (если пользователь не существует, он будет создан):

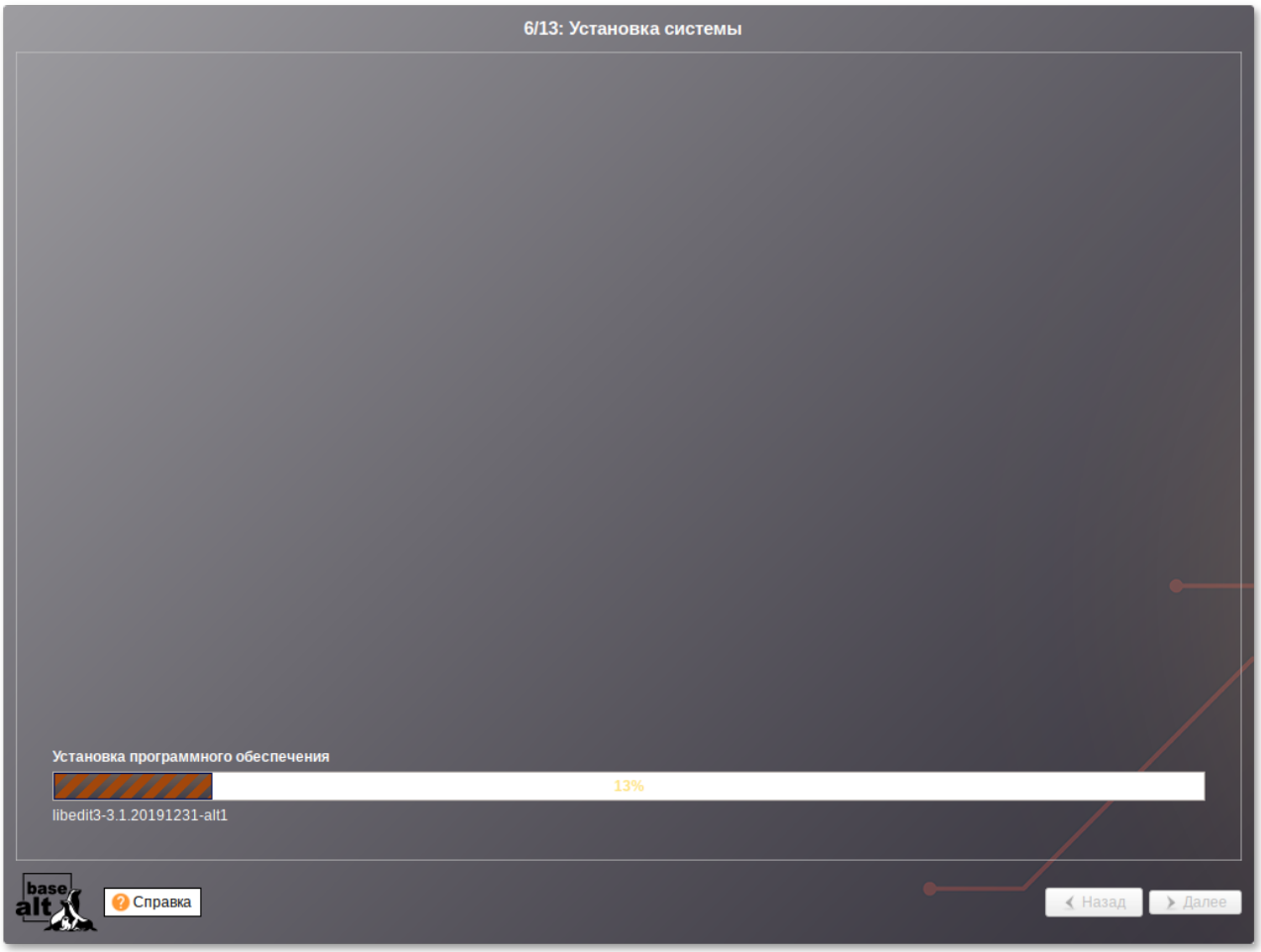
```
# builder-useradd <имя_пользователя>
```

и перелогиниться.

Выбрав необходимые группы, следует нажать кнопку **Далее**, после чего начнётся установка пакетов.

11.2. Установка пакетов

На этом этапе происходит установка набора программ, необходимых для работы системы.



Установка происходит автоматически в два этапа:

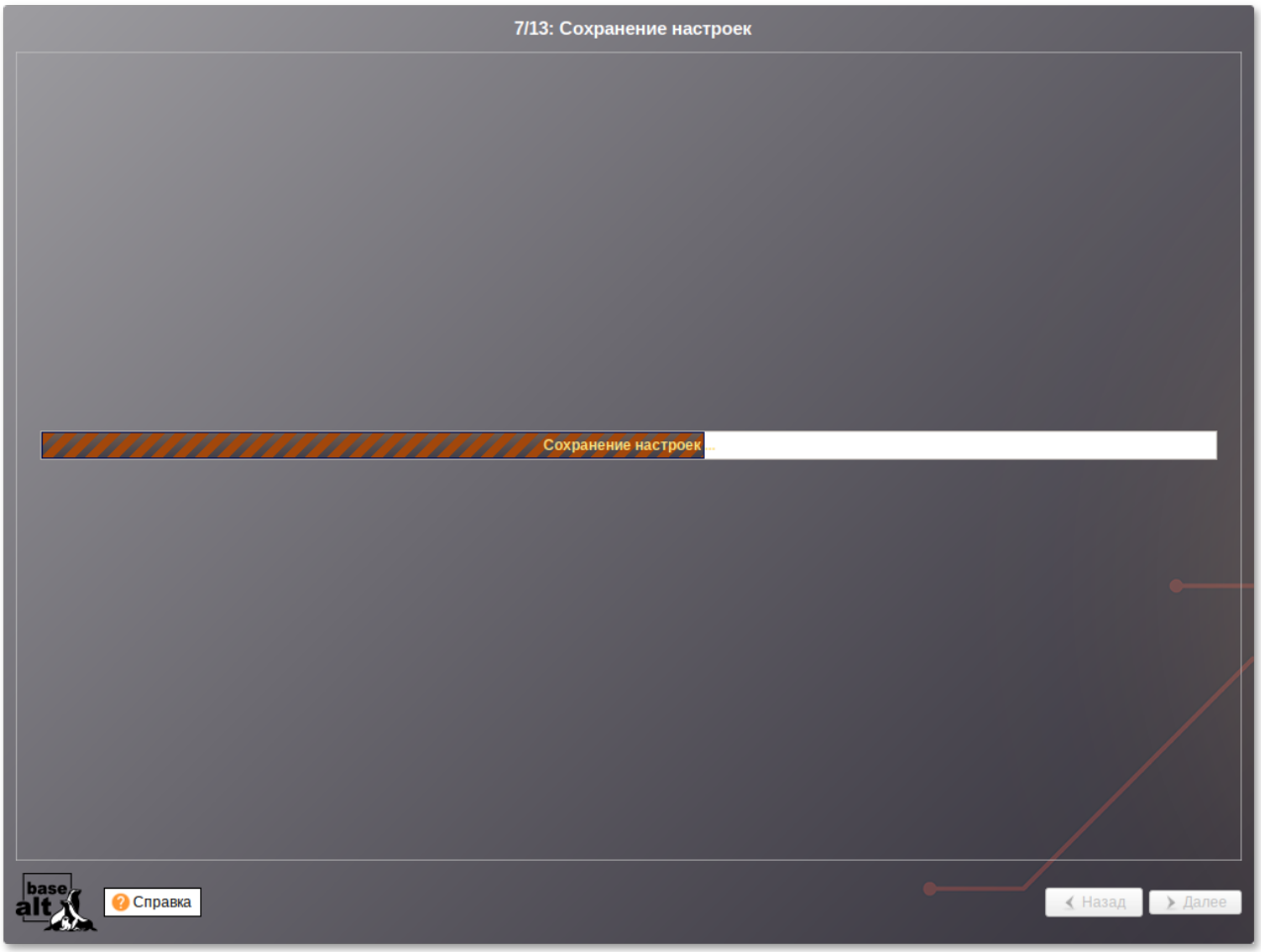
- получение пакетов;
- установка пакетов.

Получение пакетов осуществляется из источника, выбранного на этапе начальной загрузки. При сетевой установке (по протоколу FTP или HTTP) время выполнения этого шага будет зависеть от скорости соединения и может быть значительно большим в сравнении с установкой с лазерного диска.

Глава 12. Сохранение настроек

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

По завершении установки базовой системы начинается шаг сохранения настроек. Он проходит автоматически и не требует вмешательства пользователя. На экране отображается индикатор выполнения.

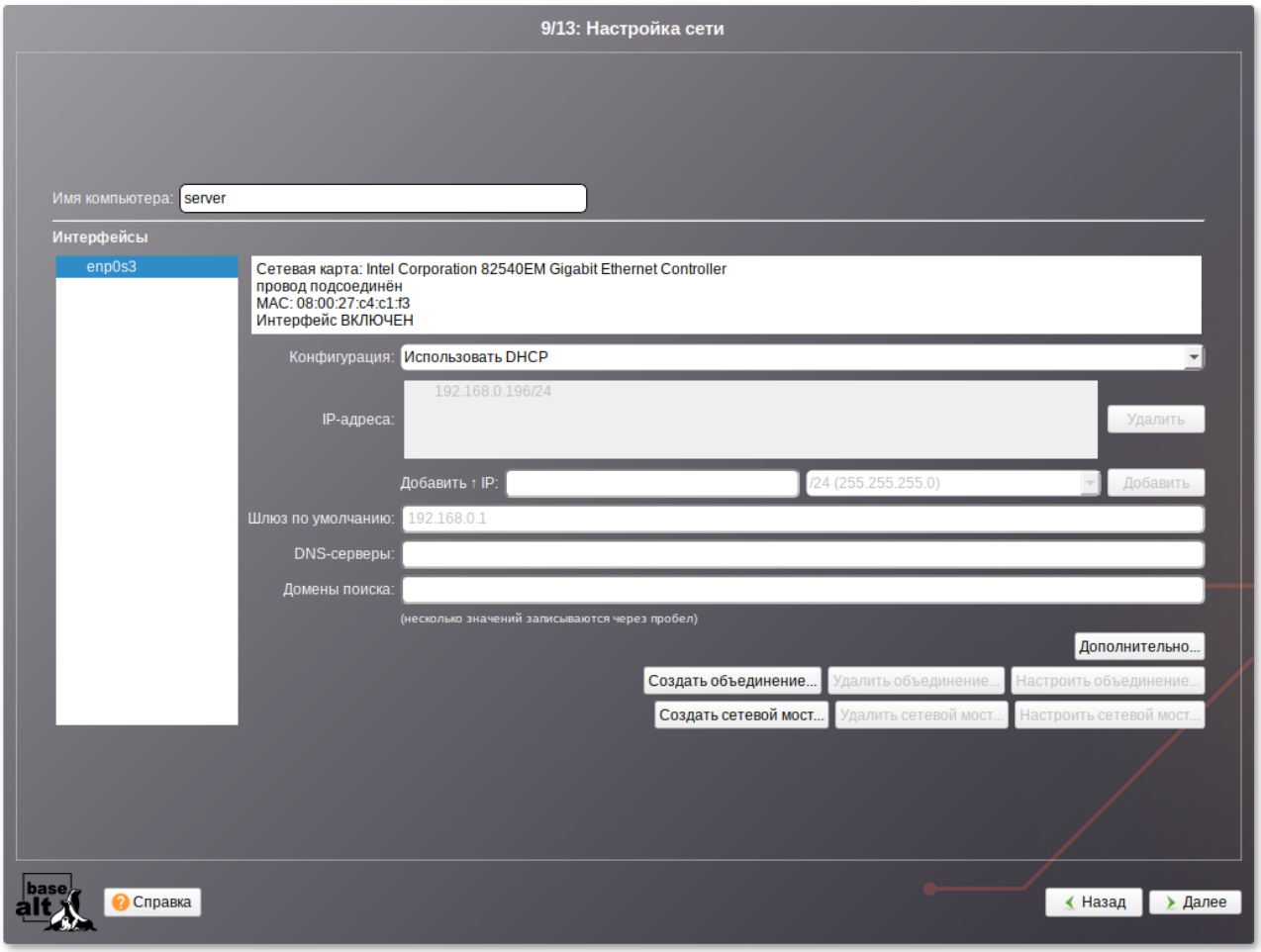


На этом шаге производится перенос настроек, выполненных на первых шагах установки, в только что установленную базовую систему. Производится также запись информации о соответствии разделов жесткого диска смонтированным на них файловым системам (заполняется конфигурационный файл **`/etc/fstab`**).

После сохранения настроек осуществляется автоматический переход к следующему шагу.

Глава 13. Настройка сети

На этом этапе необходимо задать параметры работы сетевой карты и настройки сети: IP-адреса сетевых интерфейсов, DNS-сервер, шлюз и т.п. Конкретные значения будут зависеть от используемого вами сетевого окружения. Ручного введения настроек можно избежать при наличии в сети настроенного DHCP-сервера. В этом случае все необходимые сетевые настройки будут получены автоматически.



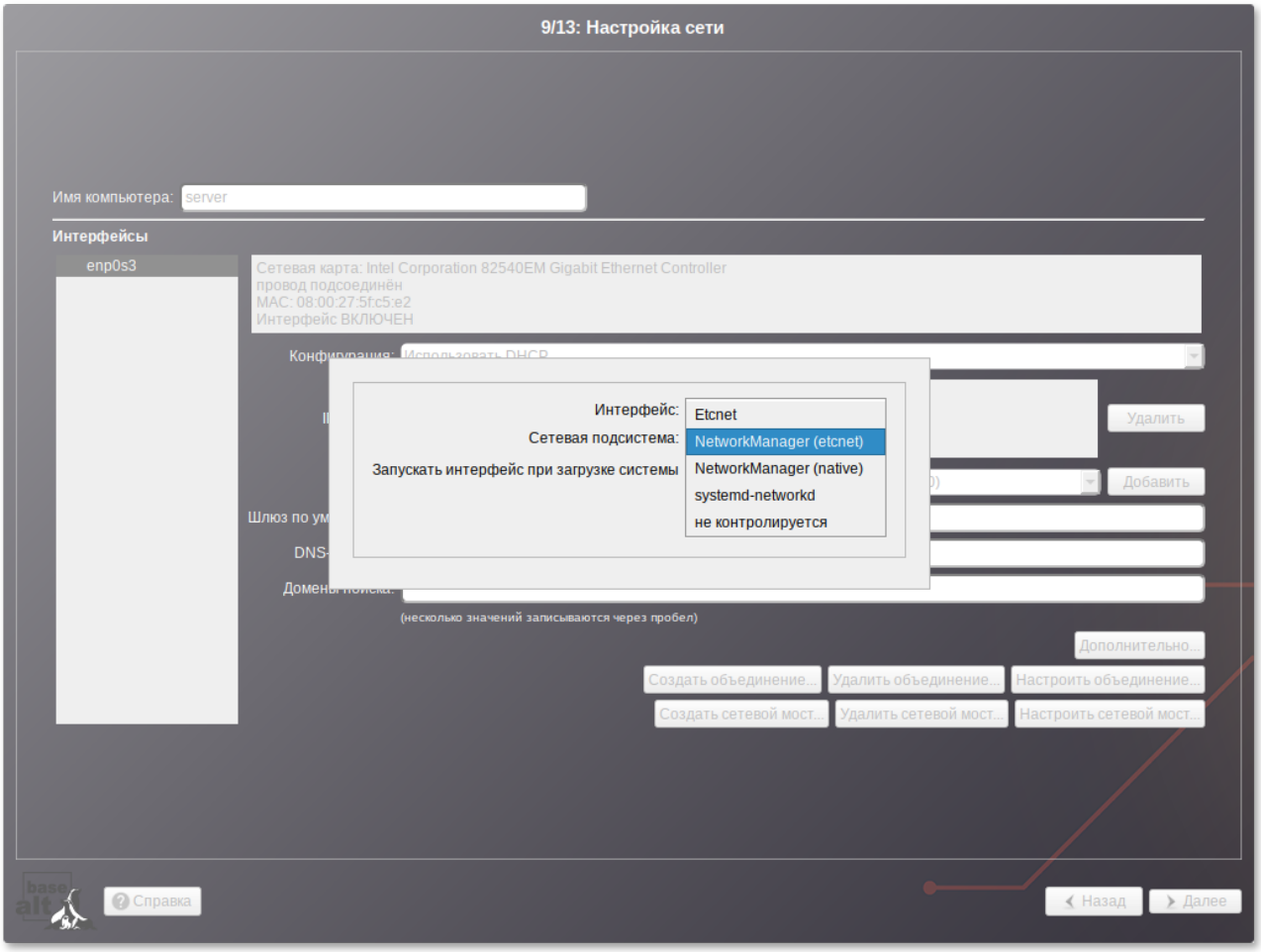
В окне **Настройка сети** доступны следующие поля:

- **Имя компьютера** — сетевое имя компьютера (это общий сетевой параметр, не привязанный к какому либо конкретному интерфейсу);
- **Интерфейсы** — список доступных сетевых интерфейсов;
- **Конфигурация** — способ назначения IP-адресов (**Использовать DHCP**, **Использовать Zeroconf**, **Вручную**);
- **IP-адреса** — пул назначенных IP-адресов из поля **Добавить ↑ IP**, выбранные адреса можно удалить нажатием кнопки **Удалить**;
- **Добавить ↑ IP** — позволяет ввести IP-адрес вручную и выбрать в выпадающем поле предпочтительную маску сети. Для переноса адреса в пул поля **IP-адреса** необходимо нажать кнопку **Добавить**;
- **Шлюз по умолчанию** — адрес шлюза, который будет использоваться сетью по умолчанию;
- **DNS-серверы** — список предпочтительных DNS-серверов, которые будут получать информацию о доменах, выполнять маршрутизацию почты и управлять обслуживающими узлами для протоколов в домене;
- **Домены поиска** — список предпочтительных доменов, по которым будет выполняться поиск.

Примечание

При переключении конфигурации с **Использовать DHCP** на **Вручную** в поле **IP-адреса** может отображаться IP-адрес, полученный по DHCP. Этот адрес никак не используется в дальнейшей настройке. Необходимо удалить отображаемый IP-адрес и задать адрес вручную, иначе сетевому интерфейсу будет назначен IP-адрес локальной заглушки (например, 127.0.0.2).

В окне, открываемом при нажатии кнопки **Дополнительно**, можно выбрать сетевую подсистему (NetworkManager, Etcnet, systemd-networkd) для интерфейса, а также указать должен ли запускаться данный интерфейс при загрузке системы.



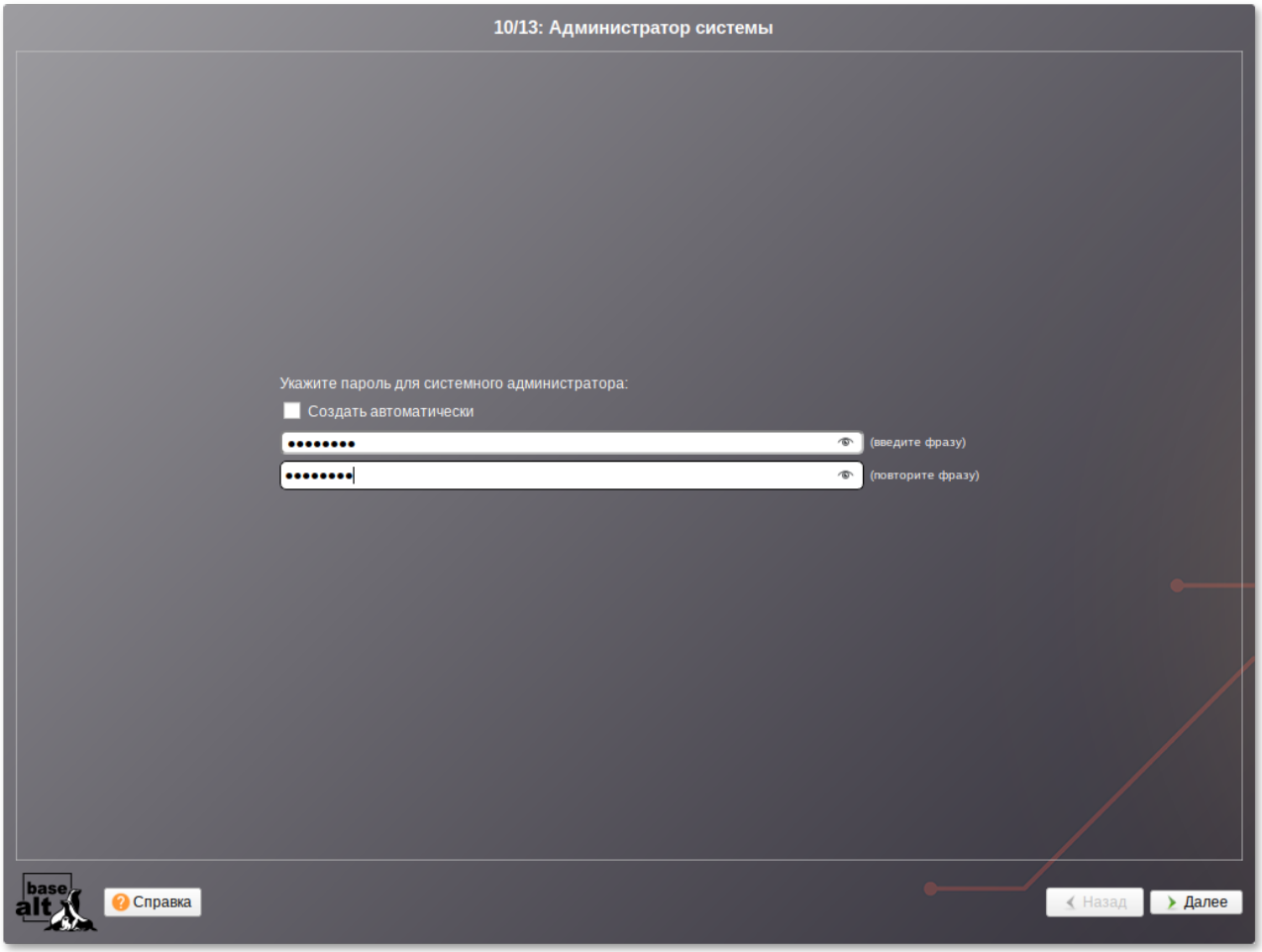
Примечание

Список доступных сетевых подистем зависит от пакетов, выбранных на этапе Установка системы (группа пакетов **Система управления сетевыми интерфейсами**). Более подробную информацию о сетевых подсистемах вы можете прочитать в главе Конфигурирование сетевых интерфейсов.

Для сохранения настроек сети и продолжения работы программы установки необходимо нажать кнопку **Далее**.

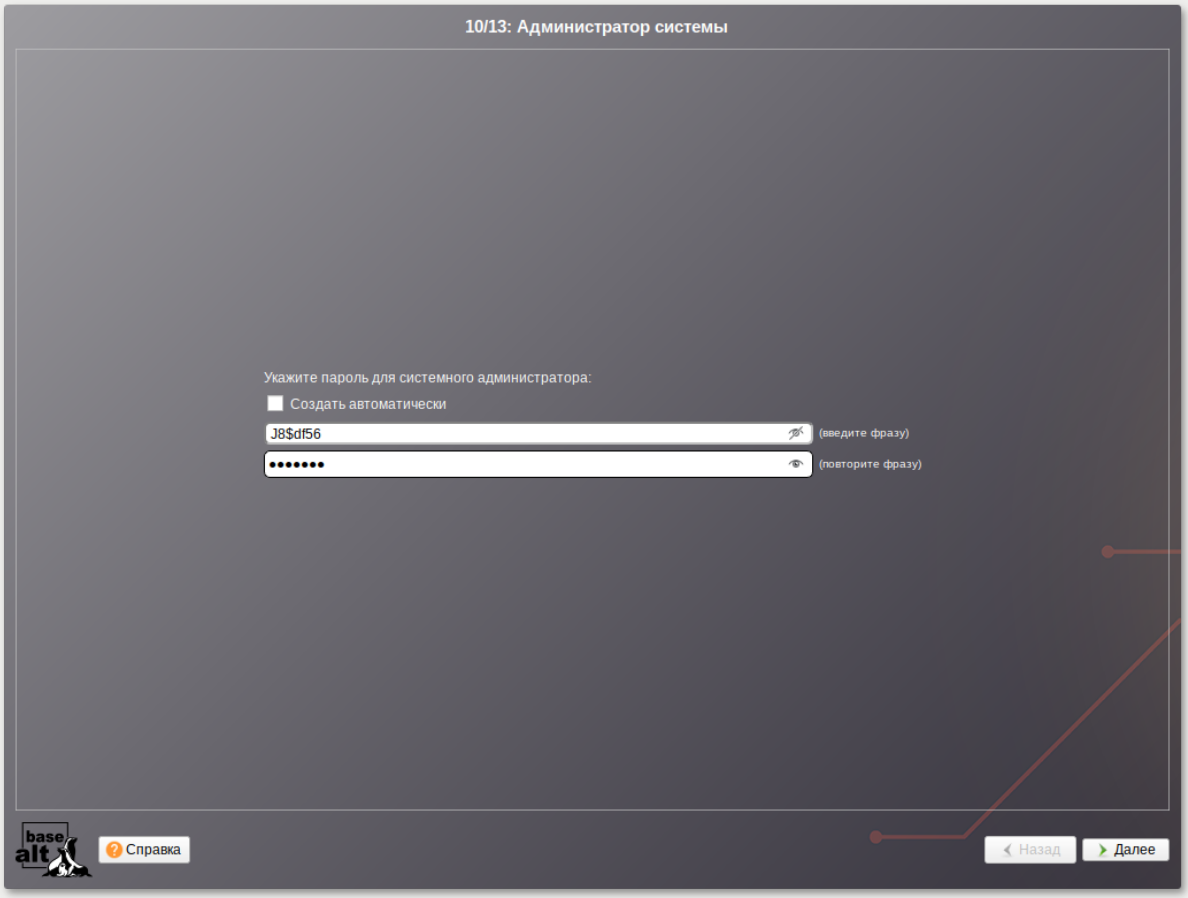
Глава 14. Администратор системы

На данном этапе загрузчик создает учетную запись администратора. В открывшемся окне необходимо ввести пароль учетной записи администратора (root). Чтобы исключить опечатки при вводе пароля, пароль учетной записи вводится дважды.



Примечание

Чтобы избежать последствий неверной раскладки клавиатуры можно просмотреть пароль, который будет сохранен. Для этого нажмите на значок глаза в поле ввода:



Для автоматической генерации пароля необходимо отметить пункт **`Создать автоматически`**. Система предложит пароль, сгенерированный автоматическим образом в соответствии с требованиями по стойкости паролей.

В любой системе Linux всегда присутствует один специальный пользователь — *администратор системы*, он же *суперпользователь*. Для него зарезервировано стандартное системное имя — root.

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

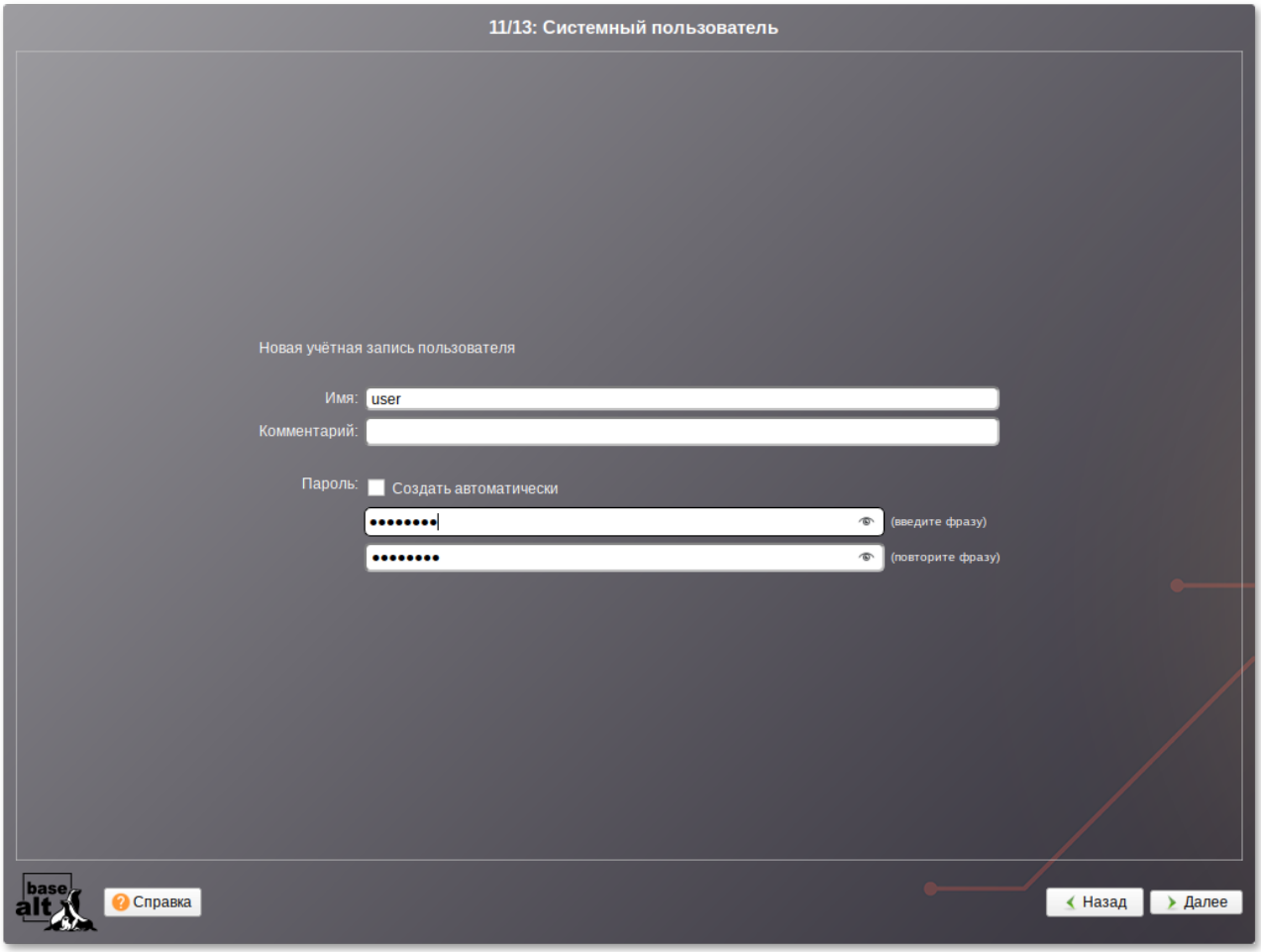
Важно

Стоит запомнить пароль root — его нужно будет вводить для получения права изменять настройки системы с помощью стандартных средств настройки Альт Сервер для Эльбрус. Более подробную информацию о режиме суперпользователя вы можете прочитать в главе Режим суперпользователя.

Подтверждение введенного (или сгенерированного) пароля учетной записи администратора (root) и продолжение работы программы установки выполняется нажатием кнопки **Далее**.

Глава 15. Системный пользователь

На данном этапе программа установки создает учетную запись системного пользователя (пользователя) Альт Сервер для Эльбрус.



Помимо администратора (root) в систему необходимо добавить, по меньшей мере, одного обычного *системного пользователя*. Работа от имени администратора системы считается опасной, поэтому повседневную работу в Linux следует выполнять от имени ограниченного в полномочиях системного пользователя.

При добавлении системного пользователя предлагается ввести имя учётной записи пользователя. Имя учётной записи всегда представляет собой одно слово, состоящее только из строчных латинских букв (заглавные запрещены), цифр и символа подчёркивания «_» (причём цифра и символ «_» не могут стоять в начале слова).

Для того чтобы исключить опечатки, пароль пользователя вводится дважды. Пароль пользователя можно создать автоматически, по аналогии с автоматическим созданием пароля суперпользователя.

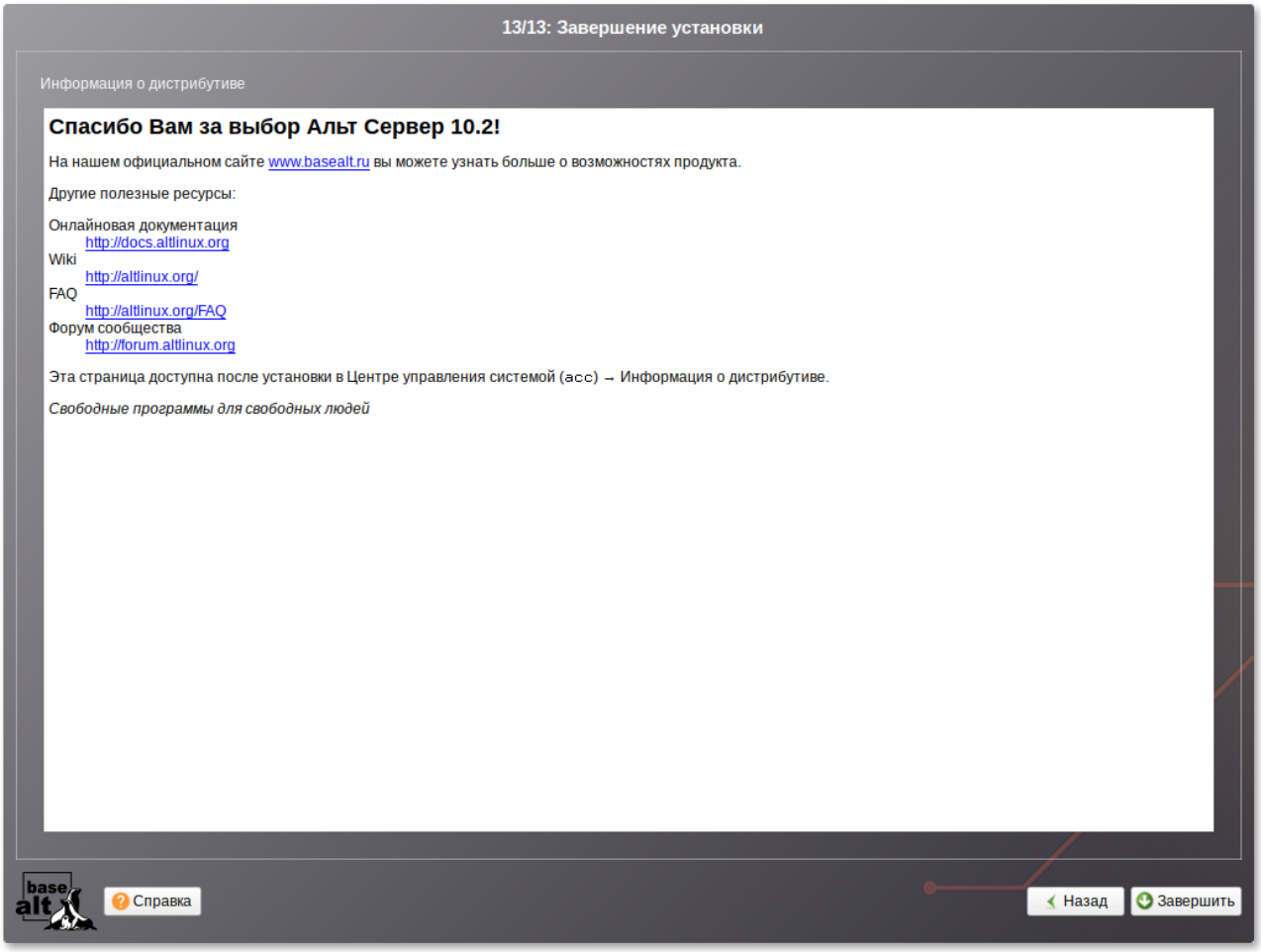
Для автоматической генерации пароля необходимо отметить пункт **Создать автоматически**. Система предложит пароль, сгенерированный автоматическим образом в соответствии с требованиями по стойкости паролей.

В процессе установки предлагается создать только одну учётную запись системного пользователя — от его имени можно выполнять задачи, не требующие привилегий суперпользователя. Учётные записи для всех прочих пользователей системы можно будет создать в любой момент после установки операционной системы.

Подтверждение введенного (или сгенерированного) пароля учетной записи системного пользователя и продолжение работы программы установки выполняется нажатием кнопки **Далее**.

Глава 16. Завершение установки

На экране последнего шага установки отображается информация о завершении установки Альт Сервер для Эльбрус.



После нажатия кнопки **Завершить** автоматически начнется перезагрузка системы.

Примечание

Если установка производилась на диск, отличный от того, с которого ВК загружается по умолчанию — следует повторно зайти в конфигурацию программы начальной загрузки, определить загрузочный диск (**d**) и указать его в качестве загрузочного диска по умолчанию (**c**). После изменений параметров загрузки, следует воспользоваться командой **m** для записи изменений в NVRAM и их применения в дальнейшем.

Не забудьте извлечь установочный DVD (если это не происходит автоматически). Далее можно загружать установленную систему в обычном режиме.

Глава 17. Обновление системы до актуального состояния

После установки системы, её лучше сразу обновить до актуального состояния. Можно не обновлять систему и сразу приступать к работе только в том случае, если вы не планируете подключаться к сети или Интернету, не собираетесь устанавливать дополнительных программ.

Для обновления системы необходимо выполнить команды (с правами администратора):

```
# apt-get update
# apt-get dist-upgrade
# update-kernel
# apt-get clean
# reboot
```

Примечание

Получить права администратора можно, выполнив в терминале команду:

```
$ su -
```

или зарегистрировавшись в системе (например, на второй консоли **Ctrl**+**Alt**+**F2**) под именем **root**. Про режим суперпользователя можно почитать в главе Режим суперпользователя.

Примечание

Подробнее про обновление пакетов можно прочитать в главах Обновление системы, Обновление всех установленных пакетов и Обновление ядра.

Часть III. Начало использования Альт Сервер для Эльбрус

В этой части рассматривается загрузка установленной операционной системы и вход в среду рабочего стола.

Содержание

Глава 18. Использование кабеля RS232 (COM) для подключения к консоли

Программа начального старта (ПНС) вычислительного комплекса «Эльбрус» является командно-строчной, что позволяет легко управлять ей через последовательный порт (порт RS232). Этот вариант подключения имеет ряд преимуществ — вывод диагностики начинается практически мгновенно после включения машины, ввод буферизуется (пробельный символ для перехода в меню можно отправить заранее, не дожидаясь подсказки), на принимающей стороне могут быть доступны средства копирования/вставки.

В случае терминала, подключенного к последовательному порту, ввод и вывод производится через оба имеющихся последовательных порта в полудуплексном режиме.

Для организации подключения используется кабель USB-COM «гнездо» («мама»), либо COM-COM («мама»/«мама»).

Примечание

При использовании кабеля COM-COM возможна ситуация, когда «общаться» начнут два экземпляра ПНС или, например, agetty — что может привести к неожиданным результатам; поэтому и предпочтителен асимметричный вариант USB-COM (ведомый компьютер — COM порт, ведущий — USB).

В качестве эмулятора последовательного терминала можно применять графические программы (**cutecom**), текстовые (**minicom**) или командно-строчные (**cu**, **miniterm.py**).

Параметры последовательного порта (115200 8N1):

- скорость — 115200 бит/сек;
- кадр — 8 бит;
- четность — нет;
- стоп-бит — 1;
- регулировка потока — нет.

Подключение к консоли на примере входящего в дистрибутив пакета *python-module-serial* и кабеля USB-COM:

```
miniterm.py /dev/ttyUSB0 115200
```

либо по кабелю COM-COM с применением команды **cu** из пакета *uucp*:

```
cu -l /dev/ttyS0 -s 115200
```

Далее можно вводить данные, которые вы хотите отправить в порт. Приходящие в порт данные от внешних устройств также будут выводиться.

Примечание

ПНС ожидает конец строки в форме **CR+LF**, загруженная система — **LF**. Может понадобиться соответственно настроить терминальную программу, либо передать дополнительные аргументы (в случае miniterm.py это может быть ***--lf*** или ***--eol LF***).

Глава 19. Загрузка системы

После включения вычислительного комплекса «Эльбрус» происходит инициализация программы начального старта.

Загрузка операционной системы начинается автоматически после небольшого времени ожидания (обычно несколько секунд).

```
Autoboot in xx  sec, PRESS SPACE TO DISABLE IT
```

Загрузка операционной системы может занять некоторое время, в зависимости от производительности компьютера. Основные этапы загрузки операционной системы — загрузка ядра, подключение (монтирование) файловых систем, запуск системных служб — периодически могут дополняться проверкой файловых систем на наличие ошибок. В этом случае время ожидания может занять больше времени, чем обычно.

Основной задачей программы начальной загрузки является загрузка ОС. Загрузку можно произвести по одной из четырех схем:

- Дождаться конца таймера обратного отсчета. В этом случае будет произведена загрузка заранее выбранной программы, с параметрами, хранящимися в энергонезависимой памяти либо в файле **boot.conf** (при его наличии) (метка, указанная как default;). Приоритетом обладает загрузка по параметрам, указанным в файле **boot.conf**. В этом случае из энергонезависимой памяти берется только значение номера устройства загрузки.

- Прервать таймер обратного отсчета и нажать клавишу **s**. В этом случае загрузка произойдет по параметрам, взятым из энергонезависимой памяти. Содержимое файла **boot.conf** приниматься в расчет не будет.

- Прервать таймер обратного отсчета и, нажав клавишу **c**, изменить параметры, взятые из энергонезависимой памяти. Потом, нажав клавишу **s**, загрузить программу.

- Прервать таймер обратного отсчета и, войдя в диалог загрузки с использованием конфигурационного файла **boot.conf** (**b** основного режима или **#boot** расширенного), загрузить одну из меток файла **boot.conf**.

Примечание

Подробнее о работе с программой начального старта можно узнать в штатной документации ВК «Эльбрус», например, п. 3.2 документа «Программа начального старта. Руководство оператора. ТВГИ.00315-03 34 01 изм. 30».

Глава 20. Вход в систему

20.1. Вход и работа в консольном режиме

Стандартная установка Альт Сервер для Эльбрус включает базовую систему, работающую в консольном режиме.

При загрузке в консольном режиме работа загрузчика Альт Сервер для Эльбрус завершается запросом на ввод логина и пароля учетной записи. В случае необходимости на другую консоль можно перейти, нажав **Ctrl**+**Alt**+**F2**.

Примечание

Сразу после загрузки в консоли будут показаны имя и IP-адрес компьютера.

Для дальнейшего входа в систему необходимо ввести логин и пароль учетной записи пользователя.

```
Welcome to ALT Server 10.2 (Mendelevium)!

Hostname: server
IP: 192.168.0.199
Hint: Num Lock on

server login: user
Password:
[user@server ~]$ _
```

В случае успешного прохождения процедуры аутентификации и идентификации будет выполнен вход в систему. ОС Альт Сервер для Эльбрус перейдет к штатному режиму работы и предоставит дальнейший доступ к консоли.

20.2. Виртуальная консоль

В процессе работы ОС Альт Сервер для Эльбрус активно несколько виртуальных консолей. Каждая виртуальная консоль доступна по одновременному нажатию клавиш **Ctrl**, **Alt** и функциональной клавиши с номером этой консоли от **F1** до **F6**.

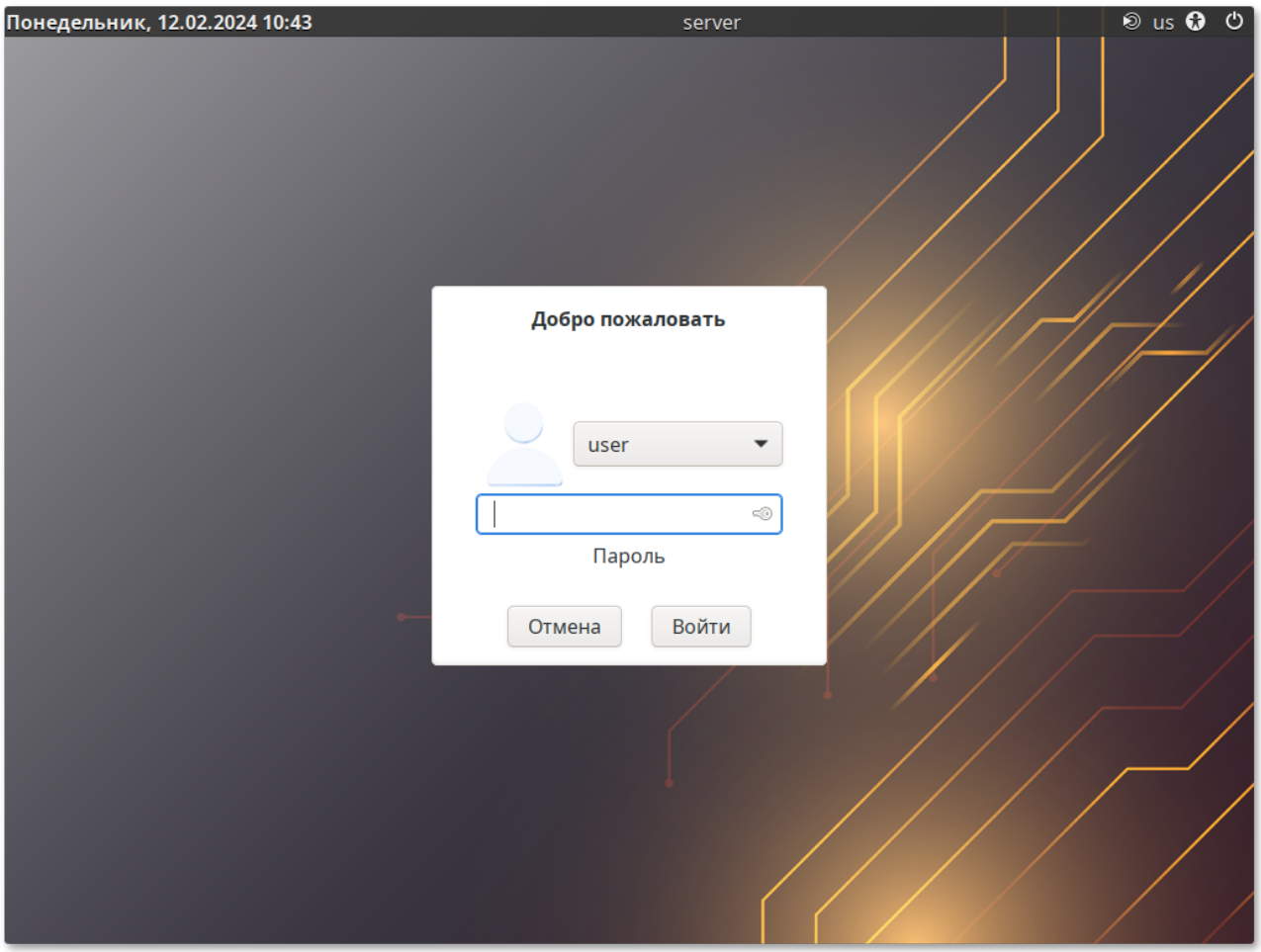
При установке системы в профиле по умолчанию на первой виртуальной консоли пользователь может зарегистрироваться и работать в графическом режиме. При нажатии **Ctrl**+**Alt**+**F1** осуществляется переход на первую виртуальную консоль в графический режим.

Двенадцатая виртуальная консоль (**Ctrl**+**Alt**+**F12**) выполняет функцию системной консоли — на неё выводятся сообщения о происходящих в системе событиях.

20.3. Вход и работа в системе в графическом режиме

В состав ОС Альт Сервер для Эльбрус также может входить графическая оболочка MATE. Графическая оболочка состоит из набора различных программ и технологий, используемых для управления ОС и предоставляющих пользователю удобный графический интерфейс для работы в виде графических оболочек и оконных менеджеров.

При загрузке в графическом режиме работа загрузчика ОС заканчивается переходом к окну входа в систему.



Для регистрации в системе необходимо выбрать имя пользователя из выпадающего списка. Далее необходимо ввести пароль, затем нажать **Enter** или щелкнуть на кнопке **Войти**. После непродолжительного времени ожидания запустится графическая оболочка операционной системы.

Добавлять новых пользователей или удалять существующих можно после загрузки системы с помощью стандартных средств управления пользователями.

Если систему устанавливали не вы, то имя *системного пользователя* и его *пароль* вам должен сообщить системный администратор, отвечающий за настройку данного компьютера.

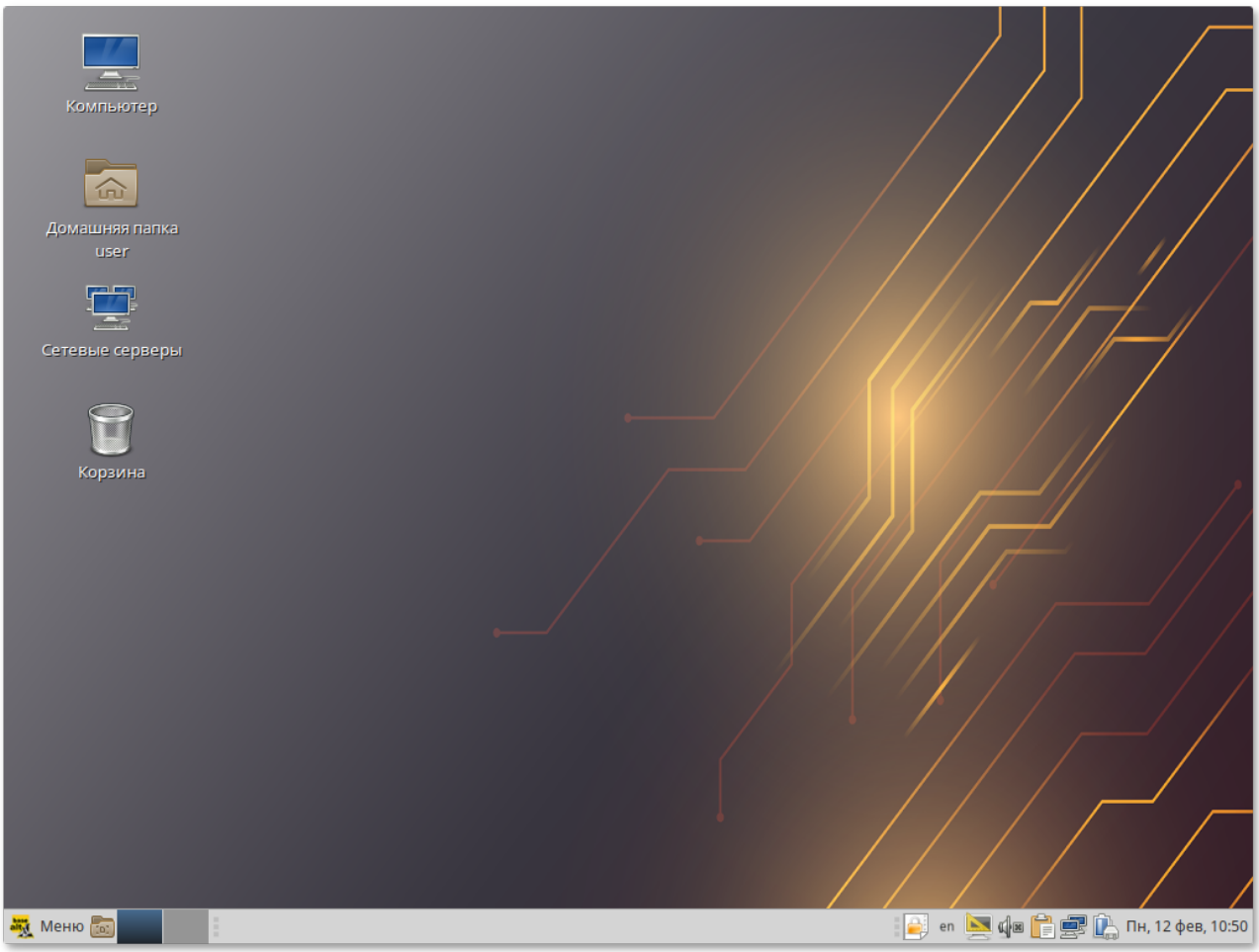
Важно

Поскольку работа в системе с использованием учётной записи *администратора системы* небезопасна, вход в систему в графическом режиме для суперпользователя root запрещён. Попытка зарегистрироваться в системе будет прервана сообщением об ошибке.

Часть IV. Рабочий стол MATE

Содержание

Глава 21. Рабочий стол MATE



На рабочем столе MATE есть две особые области. Сверху вниз:

- область рабочего стола (рабочая площадь в центре, занимающая большую часть экрана);
- панель MATE (серая полоса внизу экрана).

21.1. MATE: Область рабочего стола

Область рабочего стола включает в себя значки:

- **Компьютер** — предоставляет доступ к устройствам хранения данных;
- **Домашняя папка пользователя** — предоставляет доступ к домашнему каталогу пользователя **`/home/<имя пользователя>`**. В этой папке по умолчанию хранятся пользовательские файлы (например, аудиозаписи, видеозаписи, документы). Домашняя папка есть у каждого пользователя системы, и по умолчанию содержащиеся в ней файлы недоступны для других пользователей (даже для чтения);
- **Сетевые серверы** — позволяет просматривать сетевые подключения компьютера;
- **Корзина** — доступ к «удаленным файлам». Обычно удаляемый файл не удаляется из системы. Вместо этого он помещается в «Корзину». С помощью этого значка можно просмотреть или восстановить «удаленные файлы». Чтобы удалить файл из системы, нужно очистить «Корзину». Чтобы очистить «Корзину», необходимо щелкнуть правой кнопкой мыши по значку **Корзина** и выбрать в контекстном меню пункт **Очистить корзину**.

Примечание

Можно сразу удалить файл из системы, минуя корзину. Для этого необходимо одновременно с удалением файла зажать клавишу **`Shift`**.

На область рабочего стола можно перетащить файлы и создать ярлыки программ с помощью меню правой кнопки мыши.

Щелчок правой кнопкой мыши на свободной области рабочего стола открывает контекстное меню рабочего стола, где можно, например, настроить фон рабочего стола (пункт **Параметры внешнего вида**).

21.2. Панель MATE

Панель MATE расположена в нижней части экрана. Панель MATE универсальна: она может содержать значки загрузчика, панели задач, переключатель окон или любое другое сочетание; и её можно удобно настроить. Для того чтобы увидеть возможные варианты настройки, необходимо щелчком правой кнопки мыши вызвать контекстное меню и переместить, удалить или изменить содержание вашей панели по форме и существу.

На левой части панели расположены:

- основное меню — **Меню MATE**, обеспечивающее доступ ко всем графическим приложениями и изменениям настроек;

- **Свернуть все окна** — кнопка позволяет свернуть (развернуть) все открытые окна на текущем рабочем месте;

- **Переключатель рабочих мест** — это группа квадратов в правом нижнем углу экрана. Они позволяют вам переключать рабочие места. Каждое рабочее место предоставляет отдельный рабочий стол, на котором можно расположить приложения. По умолчанию активно два рабочих места. Можно изменить это число, нажав правой кнопкой мыши на **переключателе рабочих мест** и выбрав в контекстном меню пункт **Параметры**.

> **Примечание**
>
> Для переключения между рабочими столами необходимо использовать комбинацию клавиш **`Ctrl`**+**`Alt`**+**`стрелка влево`** или **`Ctrl`**+**`Alt`**+**`стрелка вправо`**

Любые открытые приложения отображаются как кнопки в средней части окна. Тут отображаются все окна с области рабочего стола вне зависимости от того, видно окно или нет. Кнопка приложения, которое выбрано в данный момент, будет с серым фоном. Чтобы переключиться на другое приложение, можно кликнуть по нему левой кнопкой мыши.

> **Примечание**
>
> Используйте комбинацию клавиш **`Alt`**+**`Tab`** для переключения между открытыми окнами.
>
> Удерживая нажатой клавишу **`Alt`**, нажимайте **`Tab`** для последовательного переключения между окнами. Отпустите обе клавиши, чтобы подтвердить свой выбор.

На правой части панели находятся:

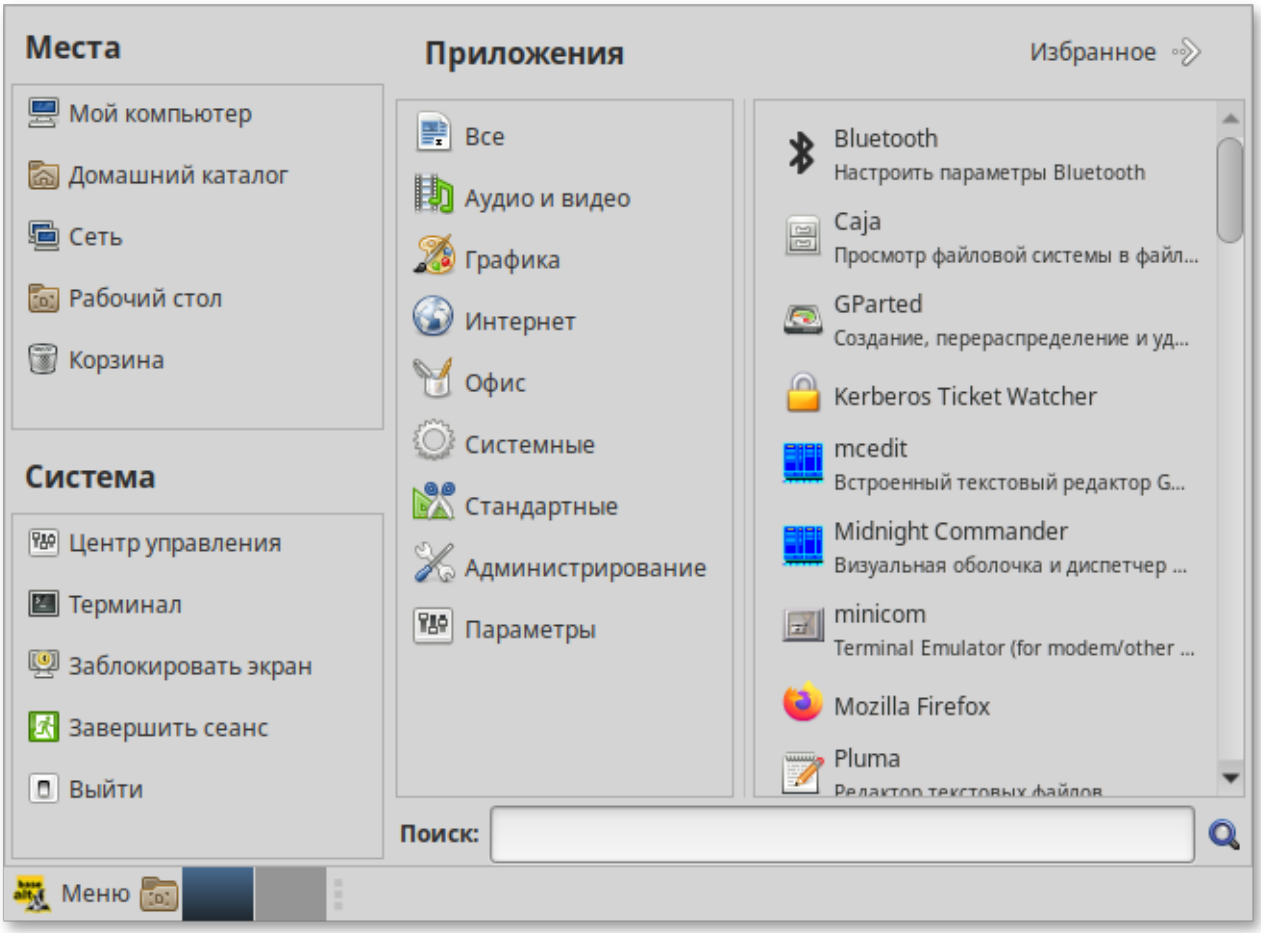
- область уведомлений;
- регулятор громкости и апплет настройки звука;
- приложение «Сетевые соединения»;
- часы и календарь;
- параметры клавиатуры;
- параметры управления питанием.

> **Примечание**
>
> Если вы остановите указатель мыши на меню или на значке, то появится короткое описание.

21.3. Запуск приложений

В левой части панели MATE находится **Меню MATE**. Через **Меню MATE** осуществляется запуск всех приложений, установленных на компьютер.

Левая часть меню включает раздел **Места** и раздел **Система**. Правая часть может иметь вид избранных приложений или всех доступных программ:



Щелчок по любому пункту в подменю **Места** открывает файловый менеджер Caja:

- **Мой компьютер** — позволяет увидеть все файлы в компьютере и файлы на подключённых внешних носителях;
- **Домашний каталог** — в этой папке по умолчанию хранятся личные файлы пользователя;
- **Сеть** — позволяет просматривать сетевые подключения компьютера. Осуществляет получение доступа к файлам и другим ресурсам, доступным в этих сетях;
- **Рабочий стол** — папка внутри «Домашней папки», содержащая файлы и папки, отображаемые на рабочем столе;
- **Корзина** — позволяет получить доступ к «удаленным файлам».

В разделе **Система** находятся кнопки, предоставляющие быстрый доступ к важным функциям системы:

- **Центр управления** — запускает приложение, позволяющее настроить все аспекты рабочего окружения MATE;

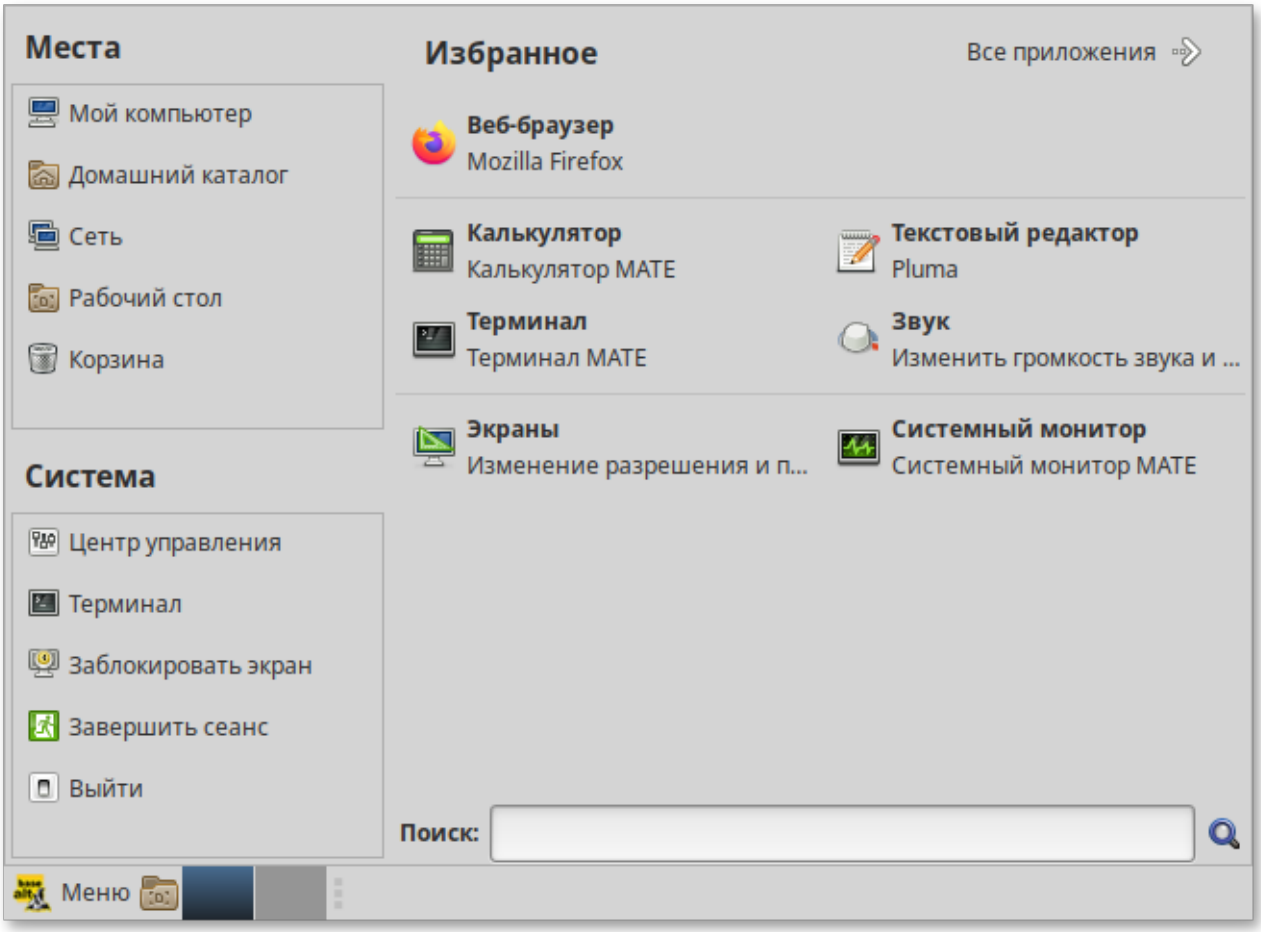
- **Терминал** — запускает приложение **Терминал**, которое позволяет вводить команды непосредственно с клавиатуры;
- **Заблокировать экран** — блокирует сеанс доступа пользователя;
- **Завершить сеанс** — запускает диалог, который позволяет завершить сеанс или переключить пользователя;
- **Выйти** — выводит диалоговое окно, которое позволяет перезагрузить или выключить компьютер.

Установленные приложения доступны в следующих разделах **Меню MATE**:

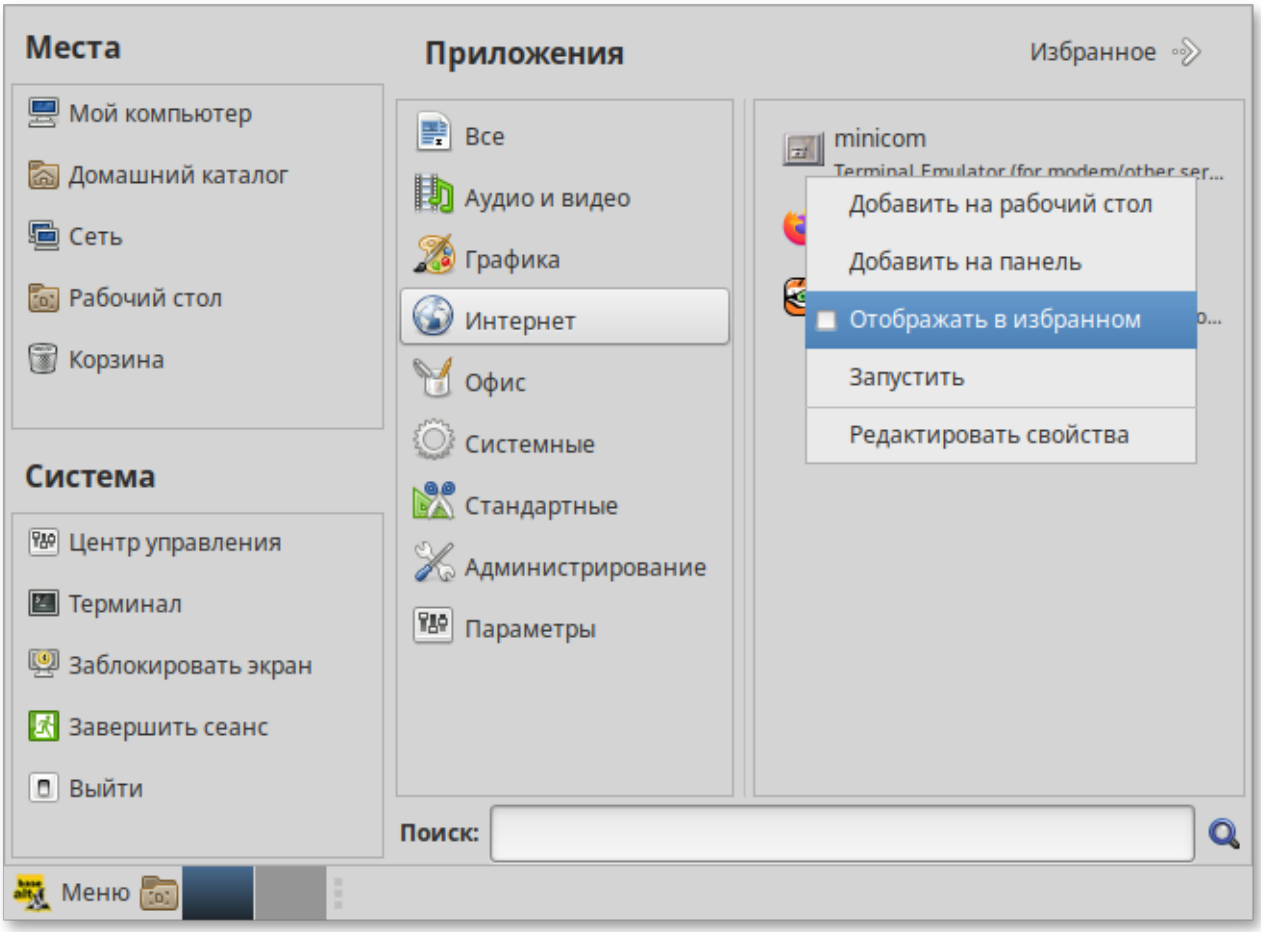
- **Все** — показывает полный список установленных приложений;
- **Аудио и видео**;
- **Графика**;
- **Интернет**;
- **Офис**;
- **Системные**;
- **Стандартные**;
- **Администрирование** — содержит инструменты, позволяющие администрировать систему;
- **Параметры** — содержит инструменты, позволяющие конфигурировать систему.

Этот список обновляется при установке или удалении программ.

Раздел **Избранное** позволяет получить быстрый доступ к выбранным приложениям.

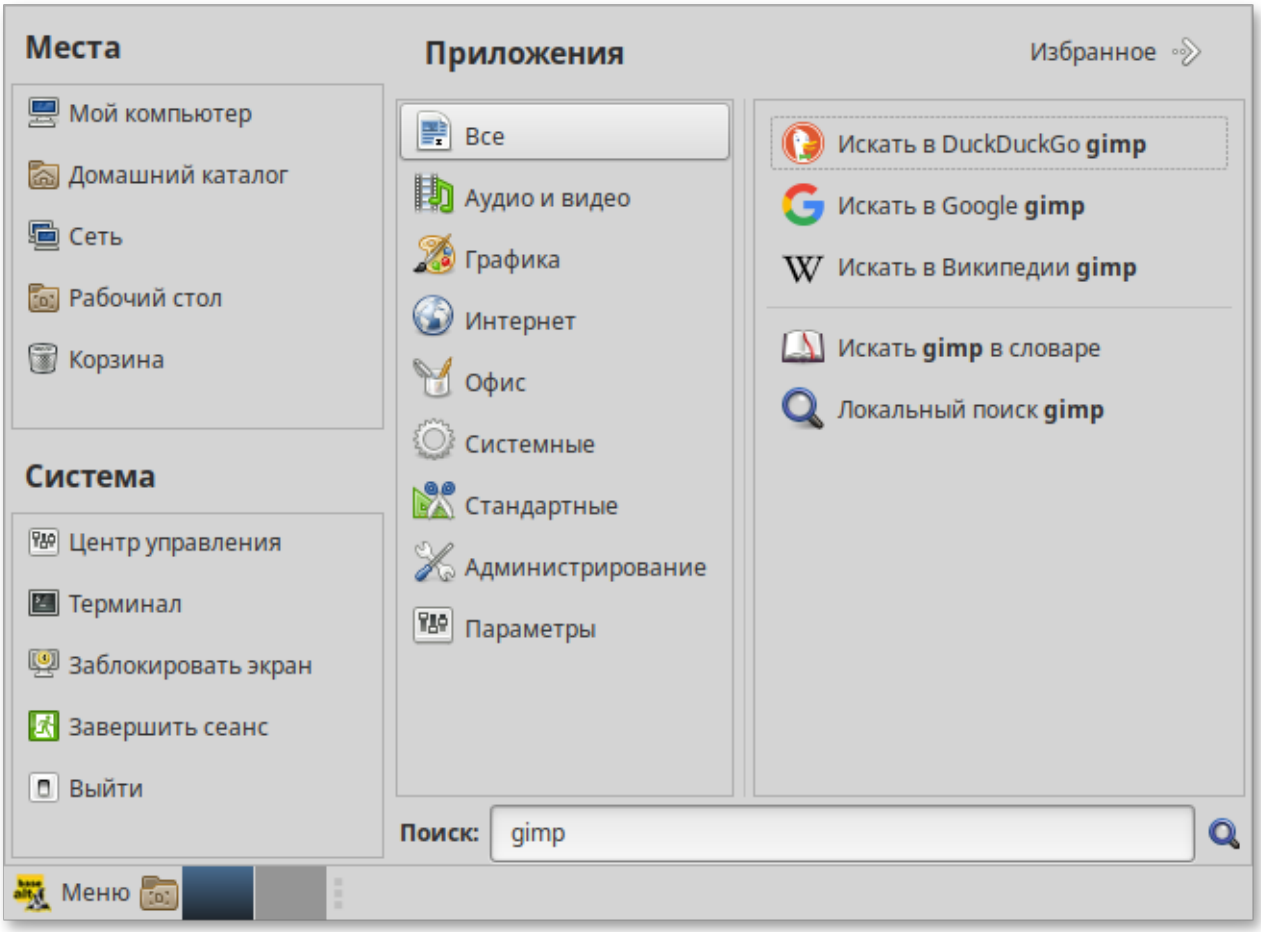


Для добавления приложения в раздел **Избранное** нужно в контекстном меню нужного приложения выбрать пункт **Отображать в избранном**. Можно также перетащить иконку приложения на кнопку **Избранное**, находящуюся в верхнем правом углу меню.



Нажатие правой клавиши мыши позволяет, как добавить, так и удалить элементы раздела **Избранное** (в том числе отступы и разделители).

Поле **Поиск** позволяет быстро запустить нужное приложение. Для этого достаточно приступить к вводу названия или описания искомого приложения, по мере ввода символов, в меню остаются видны только те приложения, которые соответствуют запросу. Если объект поиска отсутствует в меню, функция **Поиск** «предложит» другие возможные действия, например, поиск в файлах ОС или поисковой системе:



Предупреждение

Если ваш компьютер запрашивает пароль администратора (root), то это значит, что будут производиться важные системные настройки. Будьте предельно внимательны к выводимым сообщениям.

Часть V. Настройка системы

Содержание

Глава 22. Центр управления системой

22.1. Описание

Для управления настройками установленной системы вы можете воспользоваться **Центром управления системой**. **Центр управления системой** (ЦУС) представляет собой удобный интерфейс для выполнения наиболее востребованных административных задач: добавление и удаление пользователей, настройка сетевых подключений, просмотр информации о состоянии системы и т.п.

ЦУС включает также веб-ориентированный интерфейс, позволяющий управлять сервером с любого компьютера сети.

Центр управления системой состоит из нескольких независимых диалогов-модулей. Каждый модуль отвечает за настройку определённой функции или свойства системы.

22.2. Применение центра управления системой

Вы можете использовать ЦУС для разных целей, например:

- Настройки **`Даты и времени`** (datetime);
- Управления выключением и перезагрузкой компьютера (ahttpd-power, доступно только в веб-интерфейсе);
- Управления **`Системными службами`** (services);
- Просмотра **`Системных журналов`** (logs);
- Настройки **`OpenVPN-подключений`** (openvpn-server и net-openvpn);
- Конфигурирования **`Сетевых интерфейсов`** (net-eth);
- Изменения пароля **`Администратора системы (root)`** (root);
- Создания, удаления и редактирования учётных записей **`Пользователей`** (users);
- Настройки ограничения **`Использования диска (квоты)`** (quota).

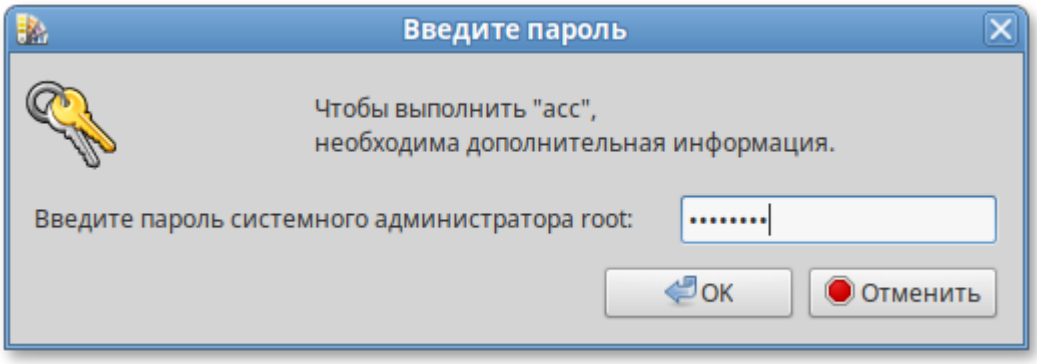
Вы всегда можете воспользоваться кнопкой **`Справка`**. Модули ЦУС имеют справочную информацию.

22.3. Запуск центра управления системой в графической среде

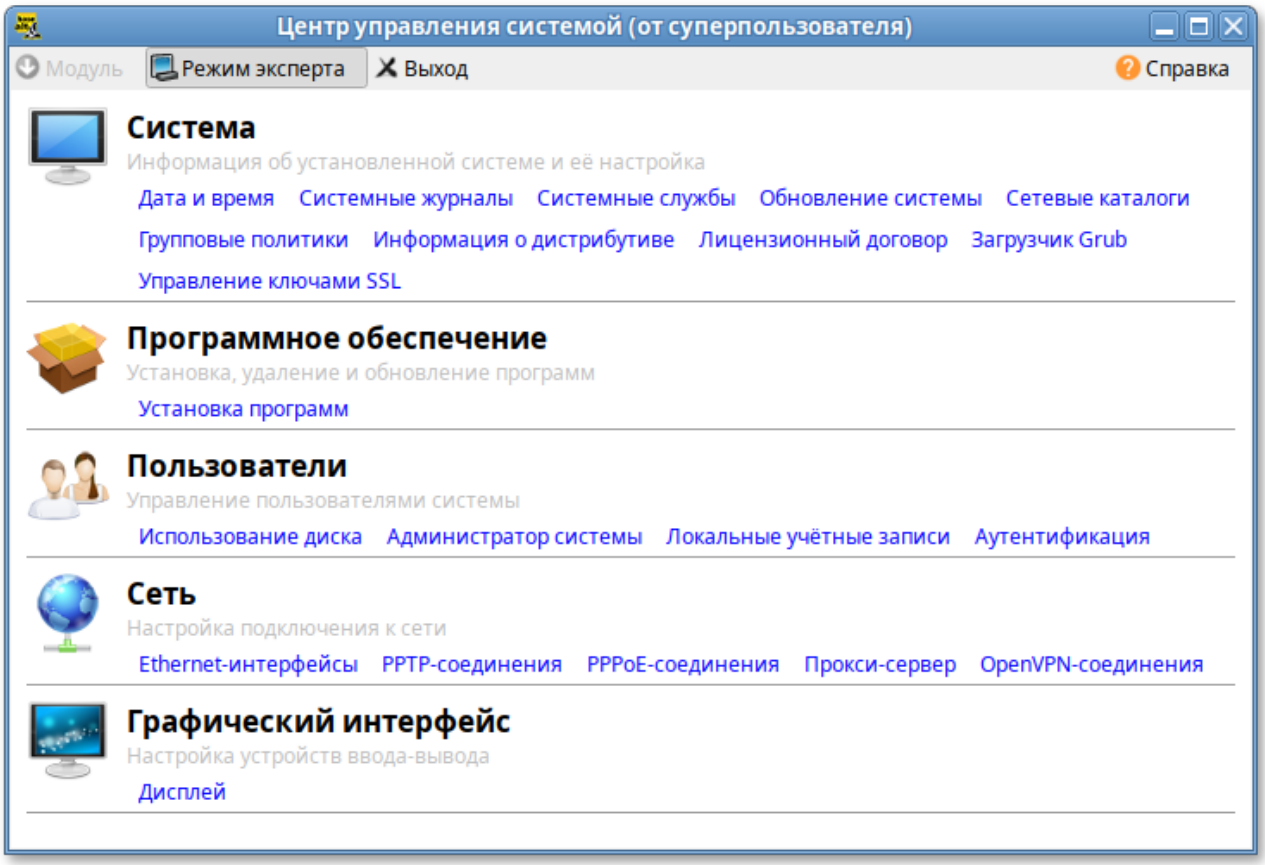
Центр управления системой можно запустить следующими способами:

- в графической среде MATE: **Приложения** → **Администрирование** → **Центр управления системой**;
- из командной строки: командой **`acc`**.

При запуске необходимо ввести пароль администратора системы (root).



После успешного входа можно приступать к настройке системы.



Кнопка **Режим эксперта** позволяет выбрать один из режимов:

- основной режим (кнопка отжата);
- режим эксперта (кнопка нажата).

Выбор режима влияет на количество отображаемых модулей. В режиме эксперта отображаются все модули, а в основном режиме только наиболее используемые.

22.4. Использование веб-ориентированного центра управления системой

ЦУС имеет веб-ориентированный интерфейс, позволяющий управлять данным компьютером с любого другого компьютера сети.

Работа с ЦУС может происходить из любого веб-браузера. Для начала работы необходимо перейти по адресу **`https://ip-адрес:8080/`**.

Например, для сервера задан IP-адрес **`192.168.0.122`**. В таком случае:

- интерфейс управления будет доступен по адресу: **`https://192.168.0.122:8080/`**;
- документация по дистрибутиву будет доступна по адресу **`https://192.168.0.122/`**.

Примечание

IP-адрес сервера можно узнать, введя на сервере команду:

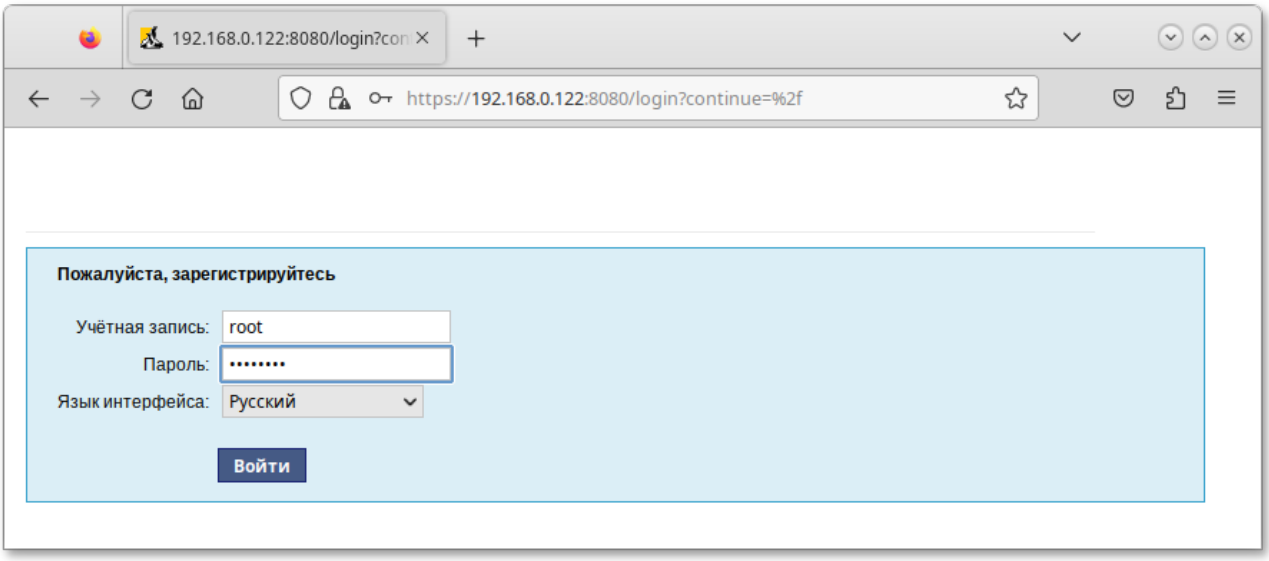
```
$ ip addr
```

IP-адрес будет указан после слова ***`inet`***:

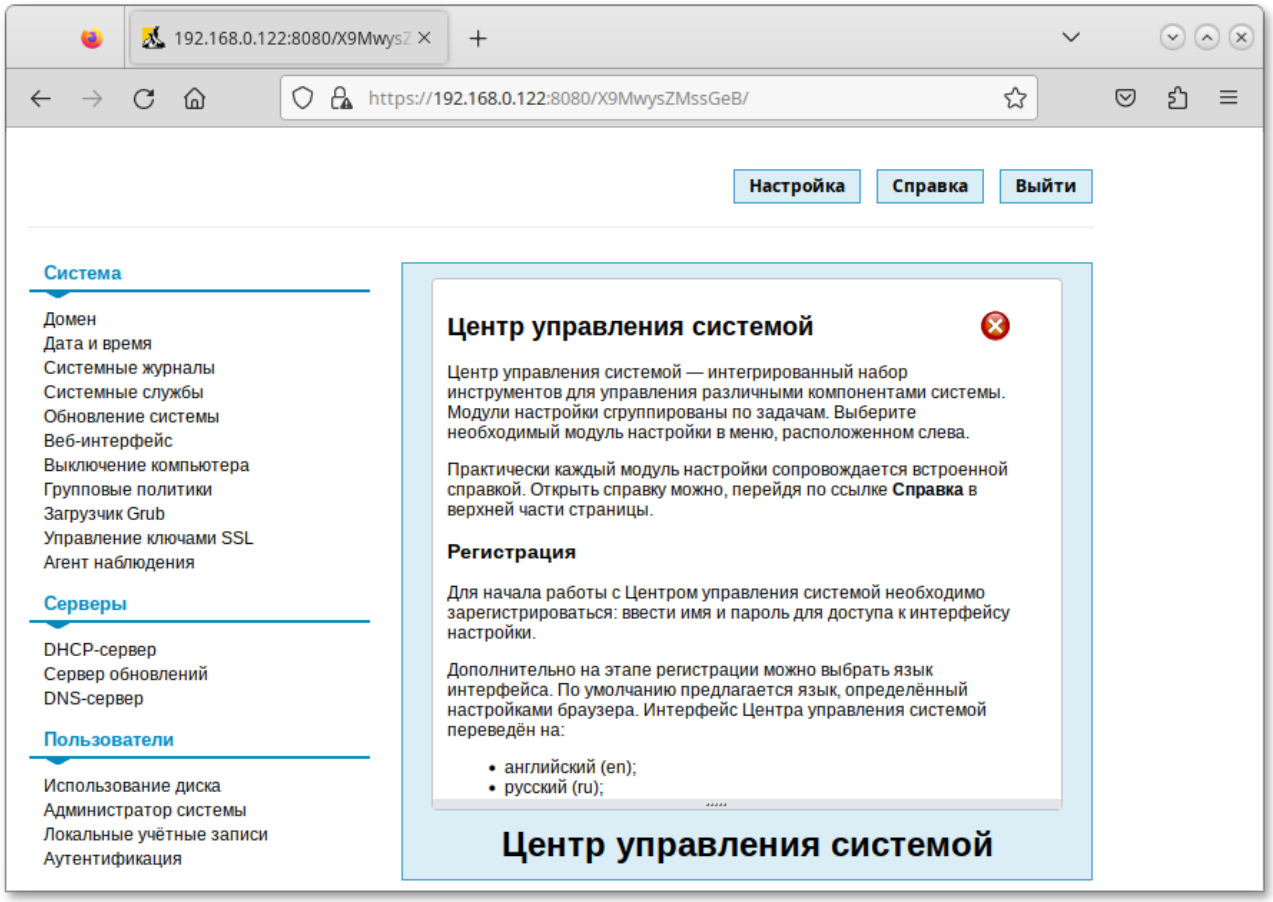
```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
qlen 1000
    link/ether 60:eb:69:6c:ef:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.122/24 brd 192.168.0.255 scope global enp0s3
```

Например, тут мы видим, что на интерфейсе enp0s3 задан IP-адрес **`192.168.0.122`**.

При запуске центра управления системой необходимо ввести в соответствующие поля имя пользователя (**root**) и пароль пользователя:



После этого будут доступны все возможности ЦУС на той машине, к которой было произведено подключение через веб-интерфейс.



Примечание

Если в сети нет компьютера, который вы могли бы использовать для доступа к веб-ориентированному **Центру управления системой**, то вы можете воспользоваться браузером непосредственно на сервере. Для работы предустановленного браузера firefox следует запустить графическую оболочку. Для этого выполните команду **`startx`**, предварительно войдя в консоль сервера, используя имя и пароль созданного при установке непривилегированного пользователя.

Веб-интерфейс ЦУС можно настроить (кнопка **`Режим эксперта`**), выбрав один из режимов:

- основной режим;
- режим эксперта.

Выбор режима влияет на количество отображаемых модулей. В режиме эксперта отображаются все модули, а в основном режиме только наиболее используемые.

Веб-интерфейс ЦУС можно настроить (кнопка **`Настройка`**), выбрав один из режимов:

- основной режим;
- режим эксперта.

Выбор режима влияет на количество отображаемых модулей. В режиме эксперта отображаются все модули, а в основном режиме только наиболее используемые.

Центр управления системой содержит справочную информацию по включённым в него модулям. Об использовании самого интерфейса системы управления можно прочитать, нажав на кнопку **Справка** на начальной странице центра управления системой.

Предупреждение

После работы с центром управления системой, в целях безопасности, не оставляйте открытым браузер. Обязательно выйдите, нажав на кнопку **Выйти**.

Примечание

Подробнее об использовании **Центра управления системой** можно узнать в главе Средства удаленного администрирования.

Глава 23. Настройка сети

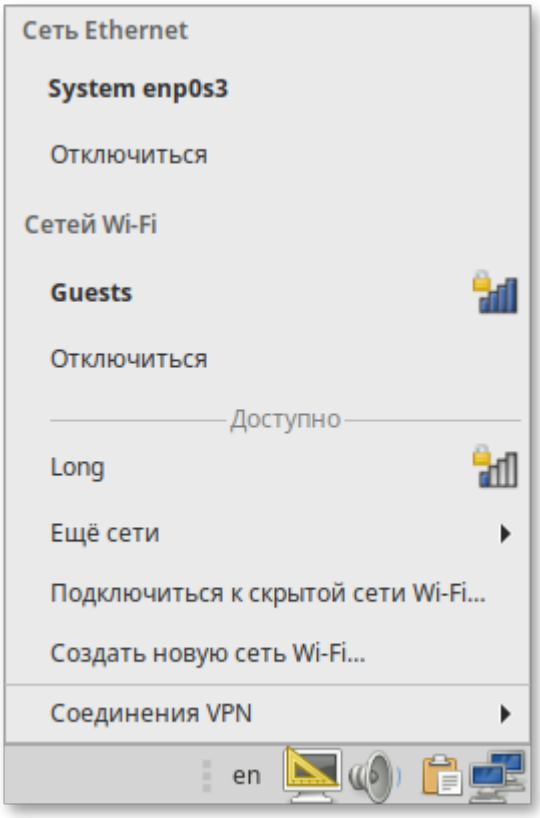
23.1. NetworkManager

Для управления настройками сети в Альт Сервер для Эльбрус может использоваться программа **NetworkManager**.

NetworkManager позволяет подключаться к различным типам сетей: проводные, беспроводные, мобильные, VPN и DSL, а также сохранять эти подключения для быстрого доступа к сети. Например, если вы подключались к сети в каком-либо интернет-кафе, то можно сохранить настройки этого подключения и в следующее посещение этого кафе подключиться автоматически.

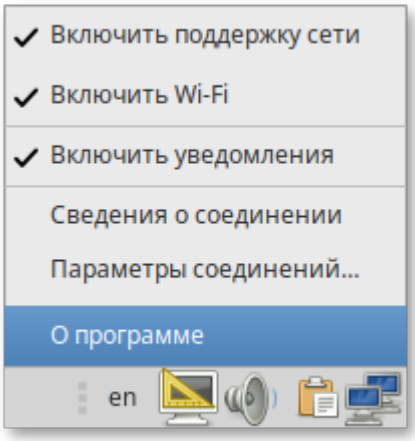
NetworkManager доступен как апплет, находящийся в системном лотке.

При нажатии левой кнопки мыши на значок **Управление сетью**, откроется меню, в котором показана информация о текущих соединениях. Здесь также можно выбрать одну из доступных Wi-Fi сетей и подключиться к ней, или отключить активное Wi-Fi соединение.



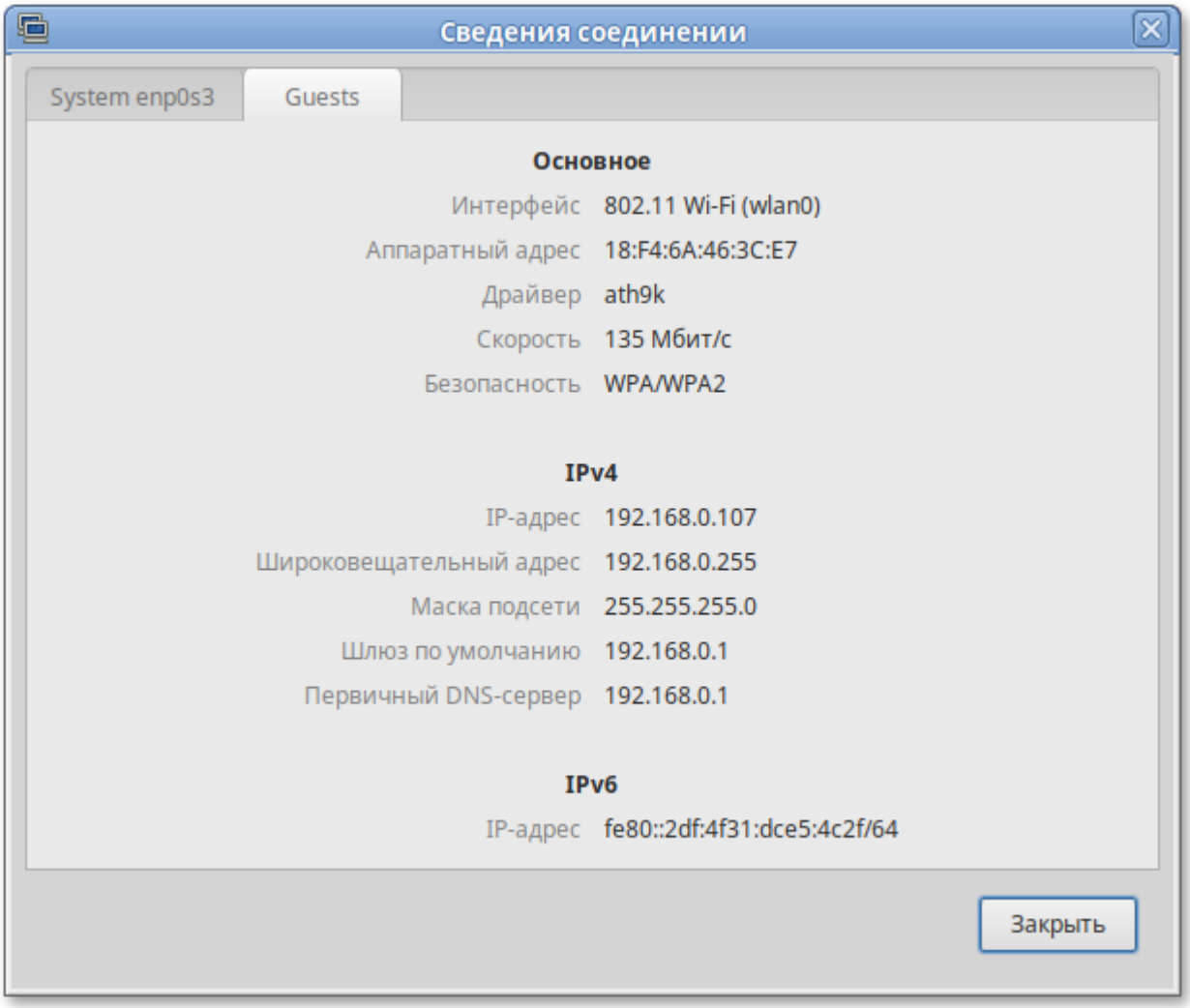
Примечание

При подключении к беспроводной сети в первый раз может понадобиться указать некоторые сведения о защите сети (например, указать аутентификационные данные).

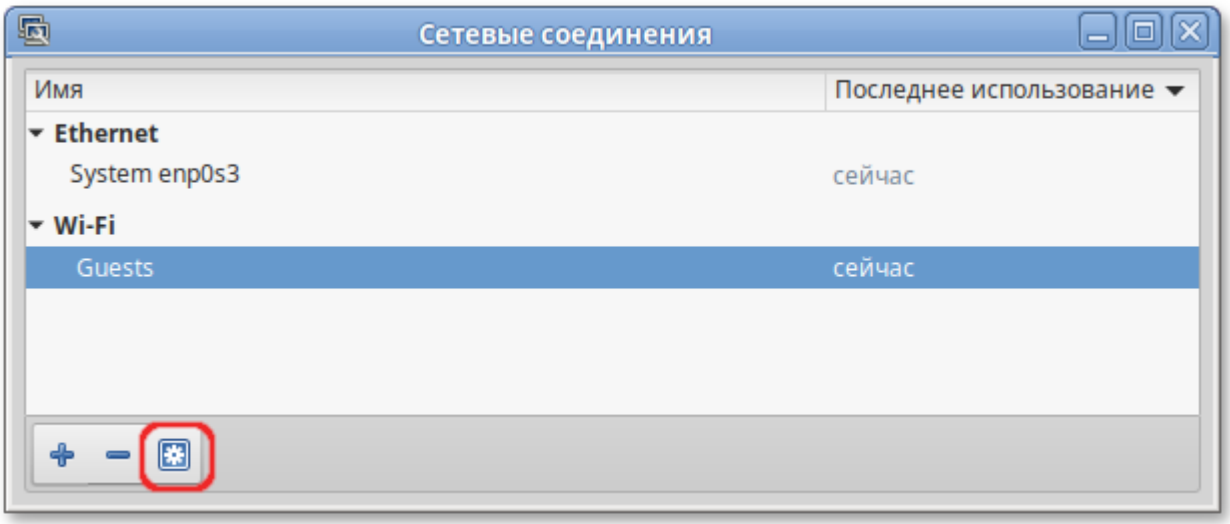


При нажатии правой кнопкой мыши на значок **NetworkManager**, появляется меню, из которого можно получить доступ к изменению некоторых настроек. Здесь можно посмотреть версию программы, получить сведения о соединении, изменить соединения (например, удалить Wi-Fi сеть, чтобы не подключаться к ней автоматически).

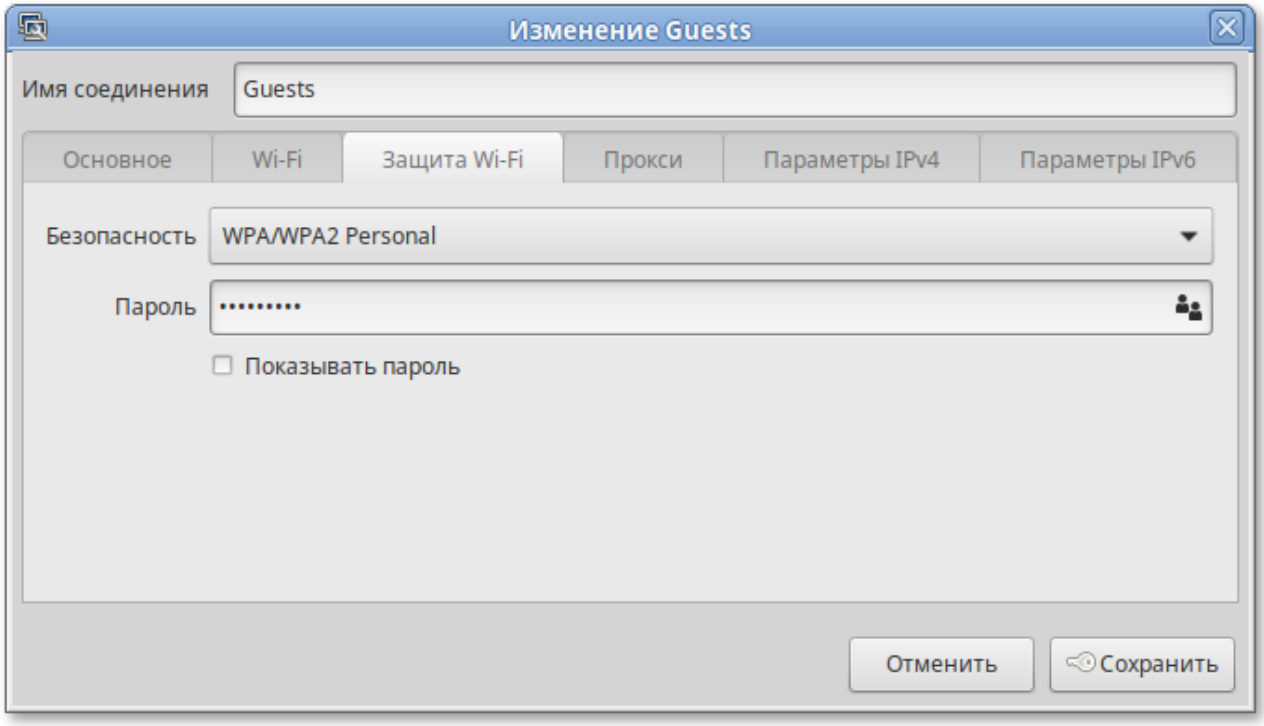
Для того чтобы просмотреть информацию о сетевом соединении, следует в меню **NetworkManager**, вызываемом нажатием правой кнопкой мыши, выбрать пункт **Сведения о соединении**. Сведения об активных соединениях будут отображены в диалоговом окне, каждое в отдельной вкладке:



Для настройки соединений, следует в меню **NetworkManager**, вызываемом нажатием правой кнопкой мыши, выбрать пункт **Параметры соединений…**. В открывшемся окне будет показан сгруппированный по типам список соединений. Необходимо выбрать нужную сеть и нажать кнопку **Изменить**:



В открывшемся окне можно изменить настройки сетевого интерфейса:

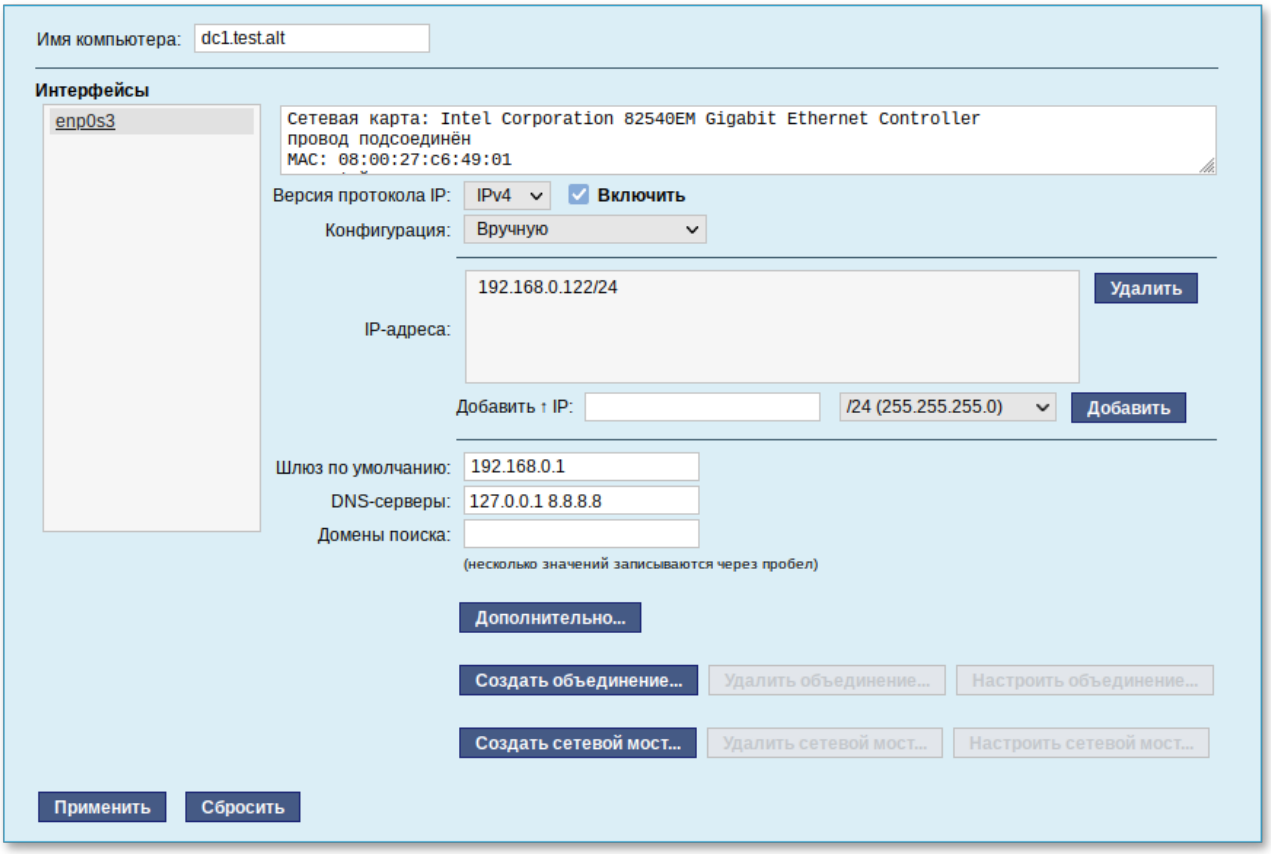


Примечание

NetworkManager под именем **System enp0s3** показывает системное Ethernet-соединение, создаваемое Etcnet. Изменить его в диалоге **Сетевые соединения** невозможно. Это соединение можно изменить в ЦУС, там же можно выбрать, какой именно интерфейс какой подсистемой обслуживается (подробнее о выборе сетевой подсистемы рассказано в разделе Конфигурирование сетевых интерфейсов).

23.2. Настройка в ЦУС

Настройку сети можно выполнить в **Центре управления системой** в разделе **Сеть** → **Ethernet интерфейсы**. Здесь можно задать как глобальные параметры сети (адрес сервера DNS, имя компьютера), так и настройки конкретного сетевого интерфейса:



Подробнее о настройке сетевых интерфейсов в ЦУС рассказано в разделе Конфигурирование сетевых интерфейсов.

Часть VI. Установка дополнительного программного обеспечения

После установки Альт Сервер для Эльбрус при первом запуске вам доступен тот или иной набор программного обеспечения. Количество предустановленных программ зависит от набора программ конкретного дистрибутива или от выбора, сделанного вами при установке системы. Если вы не обнаружили в своей системе интересующие вас программы, то вы имеете возможность доустановить их из разных источников.

Дополнительное программное обеспечение может находиться на установочном диске и/или в специальных банках программ (репозиториях), расположенных в сети Интернет и/или в локальной сети. Программы, размещённые в указанных источниках, имеют вид подготовленных для установки пакетов.

Примечание

В установочный комплект Альт Сервер для Эльбрус включено наиболее употребительное программное обеспечение. В то же время вы можете использовать репозиторий продукта (p10_e2k) для установки дополнительных программных пакетов.

Содержание

Глава 24. Установка дополнительного ПО

24.1. Введение

Для установки дополнительного ПО вы можете использовать **Центр управления системой** либо программу управления пакетами **Synaptic**.

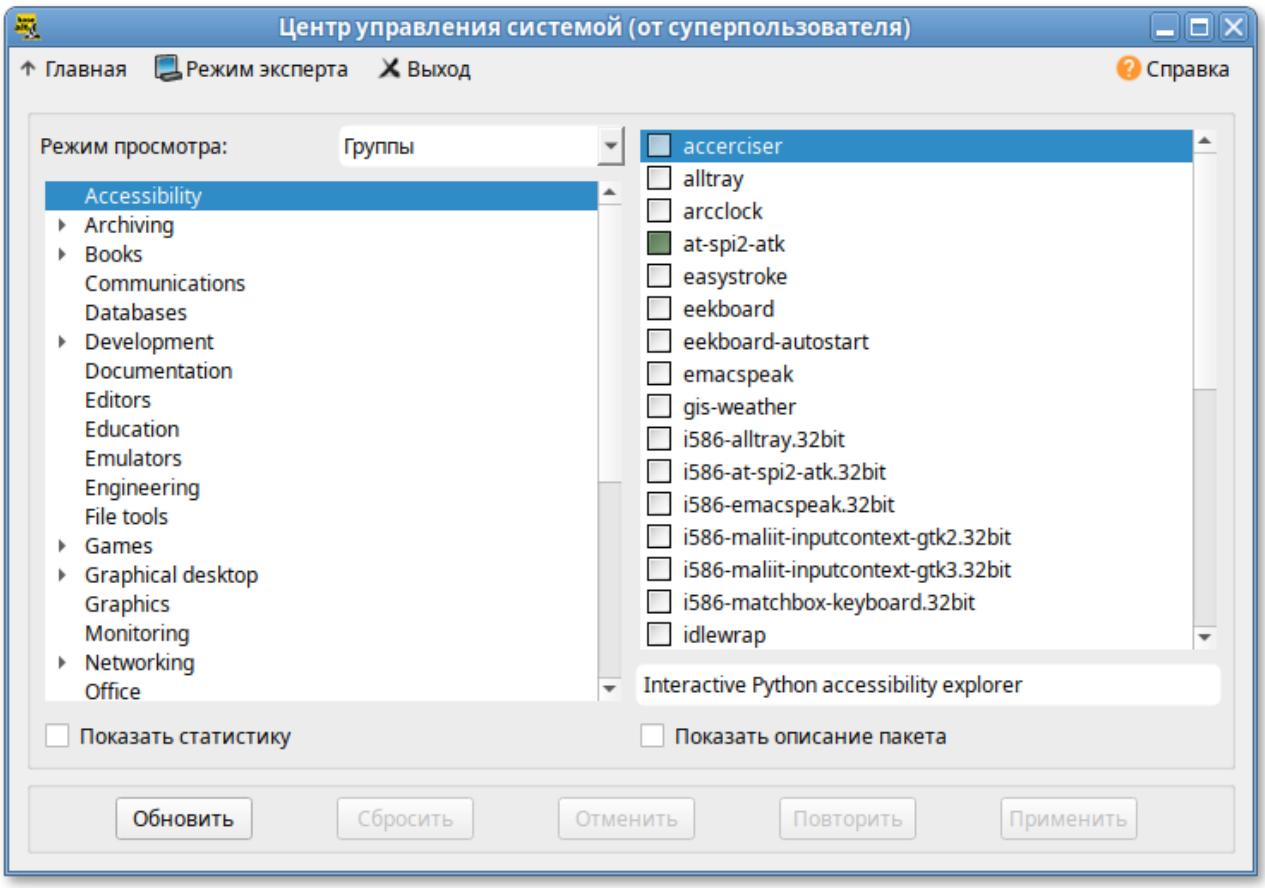
Предупреждение

Не используйте одновременно два менеджера пакетов, так как это может привести к их некорректной работе.

24.2. Установка дополнительного ПО в ЦУС

Центр управления системой содержит модуль установки дополнительных пакетов: **Программное обеспечение** → **Установка программ**. Для облегчения поиска доступные для установки программы разделены на группы, выводимые в левой части окна программы. Справа расположен список самих программ с указанием их текущего состояния:

- зелёная метка — пакет уже установлен;
- белая — пакет не установлен.



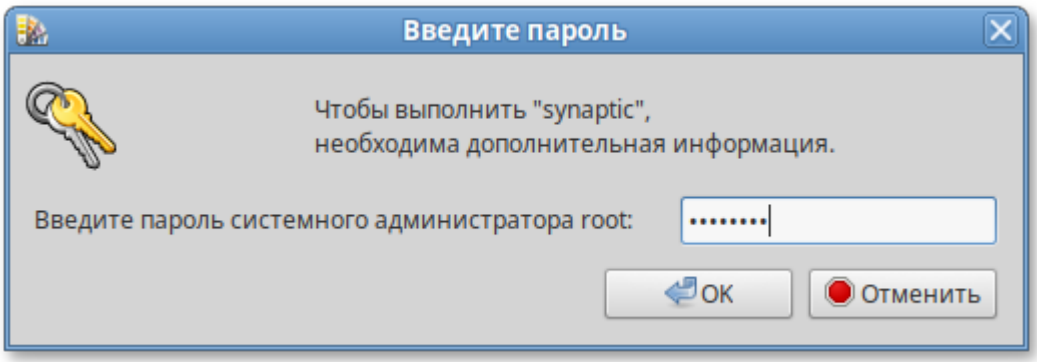
Объяснение всех обозначений можно увидеть, отметив пункт **Показать статистику**.

Для начала установки двойным щелчком мыши отметьте неустановленный пакет в правой половине окна и нажмите **Применить**. При необходимости менеджер пакетов попросит вставить установочный диск.

24.3. Программа управления пакетами Synaptic

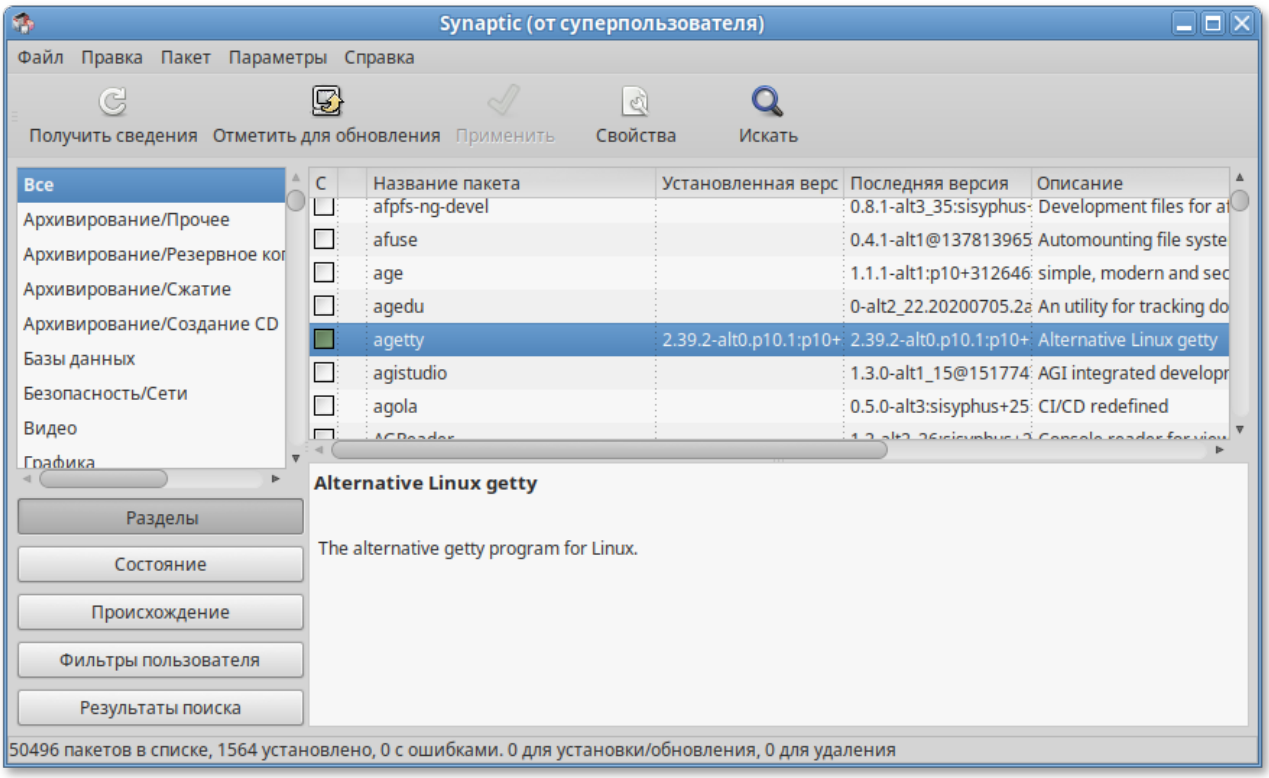
Запустить программу управления пакетами **Synaptic** можно, выбрав пункт **Меню MATE** → **Приложения** → **Параметры** → **Программа управления пакетами Synaptic**.

При запуске необходимо ввести пароль администратора системы (root).



Для облегчения поиска доступные для установки программы разделены на группы, выводимые в левой части окна программы. Справа расположен список самих программ с указанием их текущего состояния:

- зелёная метка — пакет уже установлен;
- белая метка — пакет не установлен.



При выборе пакета из списка в нижней части отображаются сведения о нем и его описание.

Перед тем как устанавливать или обновлять пакет, необходимо нажать на кнопку **Получить сведения** (**Ctrl**+**R**), для того чтобы скачать список самых последних версий ПО.

Для начала установки двойным щелчком мыши отметьте неустановленный пакет в правой половине окна и нажмите **Применить**.

Глава 25. Управление репозиториями

25.1. Программа управления пакетами Synaptic

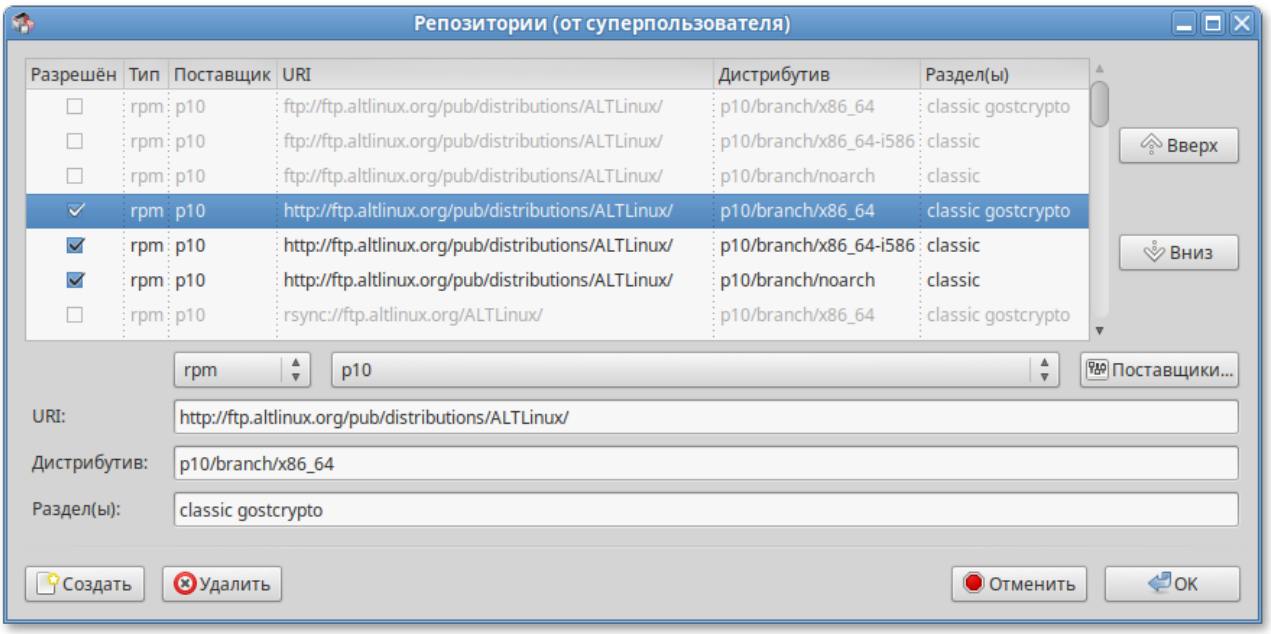
Эта информация может пригодиться вам для установки дополнительного программного обеспечения из внешних репозиториев.

Примечание

Репозитории для архитектуры **Эльбрус** могут быть недоступны в сети Интернет публично.

25.1. Программа управления пакетами Synaptic

Программа **Synaptic** может использоваться для выбора репозитория, совместимого с вашим дистрибутивом. Для указания конкретного репозитория в меню **Параметры** → **Репозитории** отметьте один из предлагаемых вариантов и нажмите кнопку **OK**. Если вы сомневаетесь, то выбирайте строки, содержащие ftp://ftp.altlinux.org/. К предложенному списку вы можете самостоятельно добавить любые репозитории, нажав на кнопку **Создать** и введя необходимые данные.



Предупреждение

Внимательно отнеситесь к настройкам источников! Ни в коем случае не стоит выбирать всё подряд!

Важно

После выбора и добавления репозиториев необходимо получить сведения о находящихся в них пакетах. В противном случае, список доступных для установки программ будет не актуален.

Для обновления информации о репозиториях можно выбрать пункт меню: **Правка** → **Получить сведения о пакетах** или нажать кнопку **Получить сведения** на панели инструментов.

Непосредственная установка пакетов из добавленных репозиториев ничем не отличается от описанной выше в главе Установка дополнительного ПО .

Примечание

Есть и другие способы работы с репозиториями и пакетами. Некоторые из них описаны в главе Установка пакетов для опытных пользователей .

Глава 26. Обновление системы

26.1. Обновление всех установленных пакетов

Synaptic поддерживает два варианта обновления системы:

Интеллектуальное обновление (рекомендуется)

Интеллектуальное обновление попытается разрешить конфликты пакетов перед обновлением системы. Действие интеллектуального обновления аналогично действию команды **`apt-get dist-upgrade`**.

Стандартное обновление

Стандартное обновление обновит только те пакеты, которые не требуют установки дополнительных зависимостей.

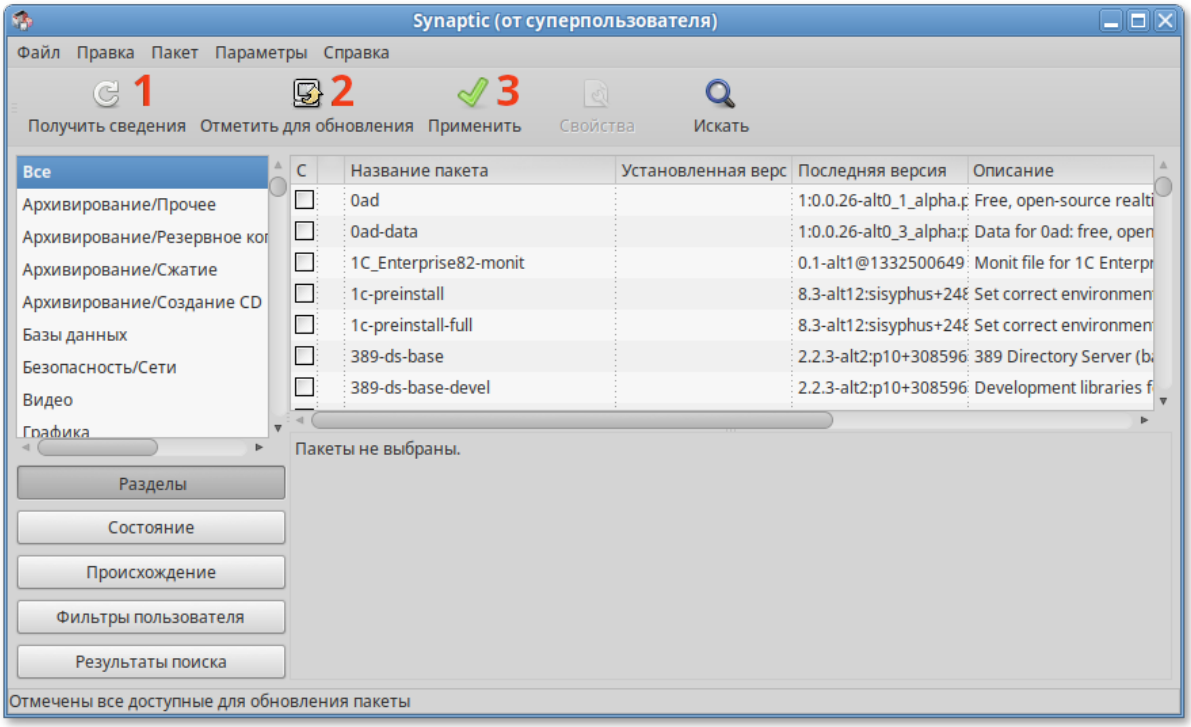
По умолчанию **Synaptic** использует интеллектуальное обновление. Для того чтобы изменить метод обновления системы, откройте диалоговое окно **Параметры** (**Параметры** → **Параметры**) и на вкладке **`Основное`** в списке **`Обновить систему`** выберите требуемый способ.

Для обновления системы необходимо:

1. Нажать кнопку **`Получить сведения`** (**`Ctrl`**+**`R`**), для того чтобы скачать список самых последних версий ПО.

2. Нажать кнопку **`Отметить для обновления`** (**`Ctrl`**+**`G`**), для того чтобы **Synaptic** отметил для обновления все пакеты.

3. Нажать кнопку **`Применить`**:



4. Будет показан список изменений, который произойдет при обновлении пакетов. Тут следует обратить внимание на объём данных, который будет скачан из сети.

   После подтверждения **Synaptic** начнёт загружать файлы, затем начнётся непосредственно установка.

26.2. Обновление ядра ОС

Для обновления ядра ОС см. разделы Обновление ядра ОС и Обновление ядра.

Часть VII. Средства удаленного администрирования

Альт Сервер для Эльбрус в сети организации может быть использован для решения различных задач. Он может предоставлять компьютерам сети общий доступ в Интернет, выступать в роли почтового сервера, файлового хранилища, веб-сервера и т.д. Все эти возможности обеспечиваются соответствующими *службами*, запускаемыми на сервере.

Дальнейшие разделы описывают некоторые возможности использования
Альт Сервер для Эльбрус, настраиваемые в ЦУС.

Важно

Эта и последующие главы рекомендуются к прочтению опытным пользователям и системным администраторам.

Содержание

Глава 27. Вход в систему

Вы можете начать работу по настройке системы сразу после её установки, используя для настройки **Центр управления системой** — веб-ориентированный интерфейс, позволяющий управлять системой с любого компьютера сети (Использование веб-ориентированного центра управления системой).

Глава 28. Настройка подключения к Интернету

Помимо множества различных служб, которые Альт Сервер для Эльбрус может предоставлять компьютерам сети, важно определить, будет ли сервер предоставлять общий доступ в Интернет для компьютеров домена или нет. В зависимости от этого сервер можно рассматривать как:

Сервер без подключения к сети Интернет

Типичный случай — это сервер с одним сетевым интерфейсом (одной сетевой картой), который и связывает его с компьютерами локальной сети. Такой сервер называется также *сервер рабочей группы*.

Шлюз

В этом случае сервер обычно имеет два сетевых интерфейса (например, две сетевые карты), одна из которых служит для подключения к локальной сети, а другая — для подключения к сети Интернет.

Как для обеспечения доступа в сеть Интернет самого Альт Сервер для Эльбрус, так и для настройки общего выхода в Интернет для компьютеров сети необходимо настроить подключение к Интернету на самом сервере. Альт Сервер для Эльбрус поддерживает самые разные способы подключения к сети Интернет:

- Ethernet;
- PPTP;
- PPPoE;
- и т.д.

Для настройки подключения воспользуйтесь одним из разделов ЦУС **Сеть**.

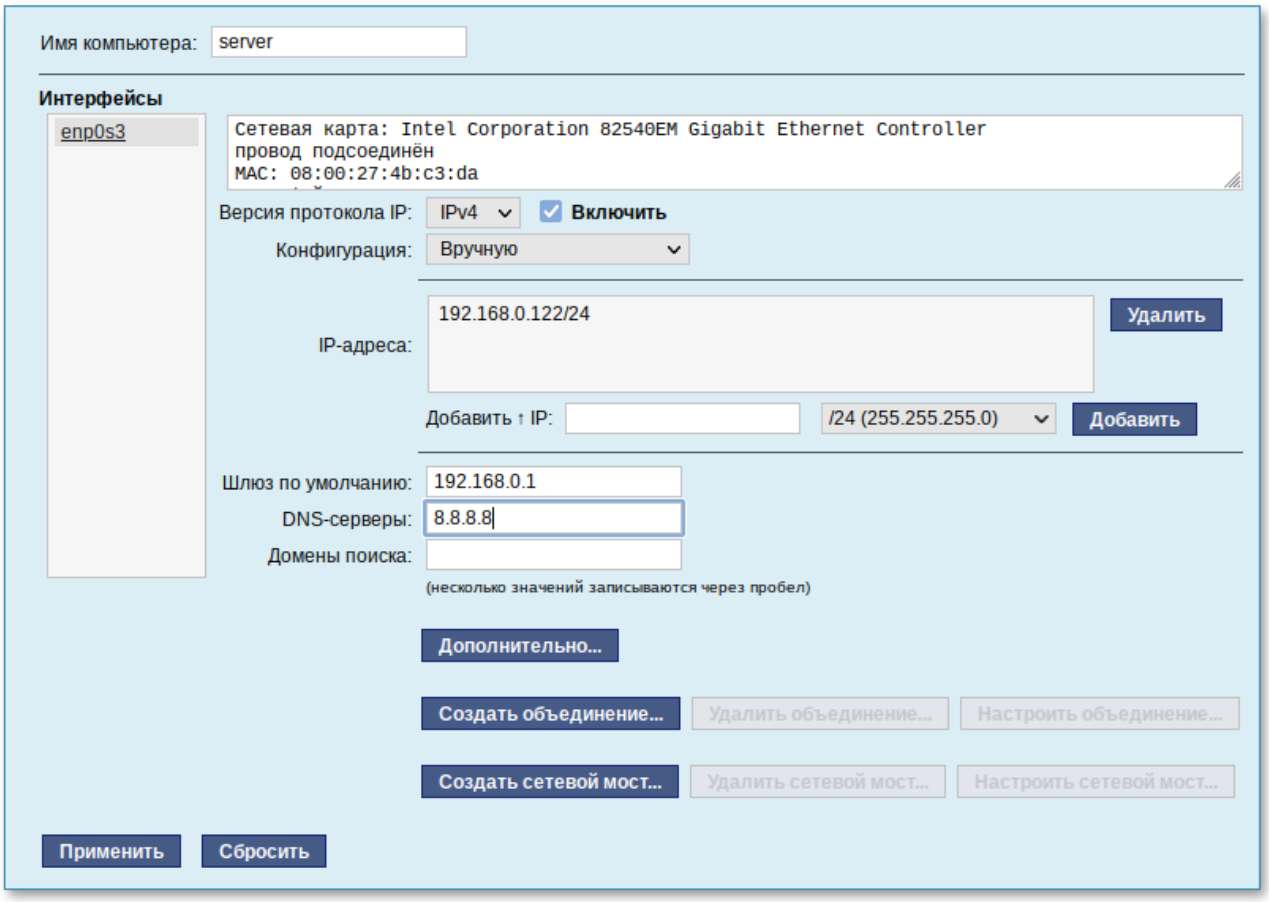
Доступные разделы:

- Ethernet-интерфейсы;
- PPTP-соединения;
- PPPoE-соединения;
- OpenVPN-соединения.

Выберите раздел, соответствующий вашему типу подключения, и приступайте к настройке.

28.1. Конфигурирование сетевых интерфейсов

Конфигурирование сетевых интерфейсов осуществляется в модуле ЦУС **Ethernet-интерфейсы** (пакет *alterator-net-eth*) из раздела **Сеть**:



В модуле **Ethernet-интерфейсы** можно заполнить следующие поля:

- **Имя компьютера** — указать сетевое имя ВК в поле для ввода имени компьютера (это общий сетевой параметр, не привязанный, к какому либо конкретному интерфейсу). Имя компьютера, в отличие от традиционного имени хоста в Unix (hostname), не содержит названия сетевого домена;

- **Интерфейсы** — выбрать доступный сетевой интерфейс, для которого будут выполняться настройки;

- **Версия протокола IP** — указать в выпадающем списке версию используемого протокола IP (IPv4, IPv6) и убедиться, что пункт **Включить**, обеспечивающий поддержку работы протокола, отмечен;

- **Конфигурация** — выбрать способ назначения IP-адресов (службы DHCP, Zeroconf, вручную);

- **IP-адреса** — пул назначенных IP-адресов из поля **Добавить ↑ IP**, выбранные адреса можно удалить нажатием кнопки **Удалить**;

- **Добавить ↑ IP** — ввести IP-адрес вручную и выбрать в выпадающем поле предпочтительную маску сети, затем нажать кнопку **Добавить** для переноса адреса в пул назначенных IP-адресов (поле **IP-адреса**);

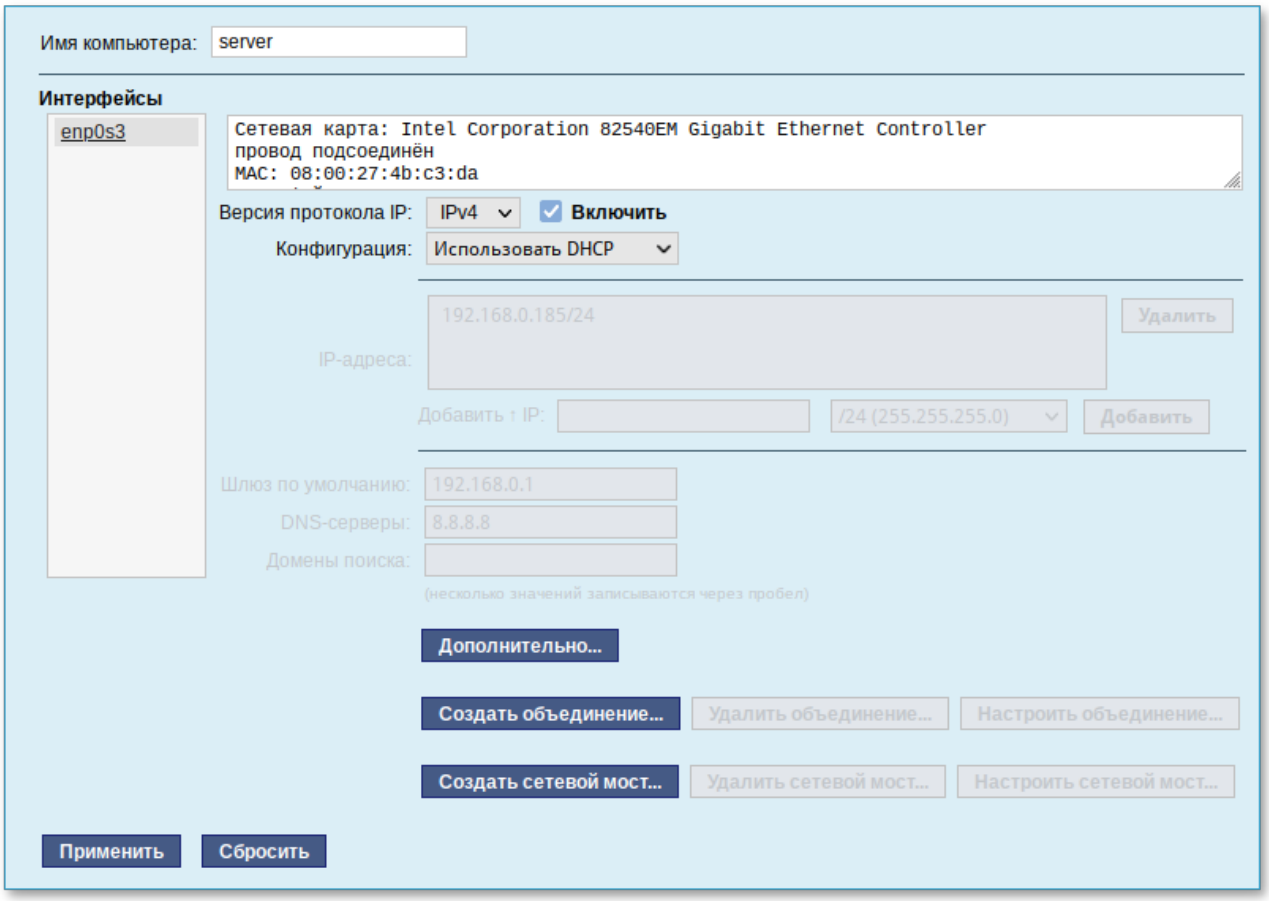
- **Шлюз по умолчанию** — в поле для ввода необходимо ввести адрес шлюза, который будет использоваться сетью по умолчанию;

- **DNS-серверы** — в поле для ввода необходимо ввести список предпочтительных DNS-серверов, которые будут получать информацию о доменах, выполнять маршрутизацию почты и управлять обслуживающими узлами для протоколов в домене;

- **Домены поиска** — в поле для ввода необходимо ввести список предпочтительных доменов, по которым будет выполняться поиск. Если в поле **Домены поиска** перечислить наиболее часто используемые домены (например, domain), то можно пользоваться неполными именами машин (computer вместо computer.domain).

IP-адрес и **Маска сети** — обязательные параметры каждого узла IP-сети. Первый параметр – уникальный идентификатор машины, от второго напрямую зависит, к каким машинам локальной сети данная машина будет иметь доступ. Если требуется выход во внешнюю сеть, то необходимо указать параметр **Шлюз по умолчанию**.

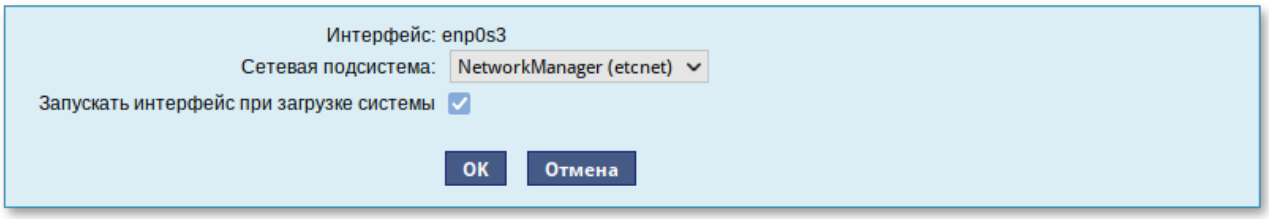
В случае наличия DHCP-сервера можно все вышеперечисленные параметры получить автоматически — выбрав в списке **Конфигурация** пункт **Использовать DHCP**:



Примечание

При переключении конфигурации с **Использовать DHCP** на **Вручную** в поле **IP-адреса** может отображаться IP-адрес, полученный по DHCP. Этот адрес никак не используется в дальнейшей настройке. Необходимо удалить отображаемый IP-адрес и задать адрес вручную, иначе сетевому интерфейсу будет назначен IP-адрес локальной заглушки (например, 127.0.0.2).

Дополнительно для каждого интерфейса можно настроить сетевую подсистему (NetworkManager, Etcnet, systemd-networkd), а также должен ли запускаться данный интерфейс при загрузке системы:



Примечание

Список доступных сетевых подистем зависит от пакетов, выбранных на этапе Установка системы (группа пакетов **Система управления сетевыми интерфейсами**).

В списке **`Сетевая подсистема`** можно выбрать следующие режимы:

Etcnet

В этом режиме настройки берутся исключительно из файлов находящихся в каталоге настраиваемого интерфейса **`/etc/net/ifaces/<интерфейс>`**. Настройки сети могут изменяться либо в ЦУС в данном модуле, либо напрямую через редактирование файлов **`/etc/net/ifaces/<интерфейс>`**.

NetworkManager (etcnet)

В этом режиме **NetworkManager** сам инициирует сеть, используя в качестве параметров — настройки из файлов Etcnet. Настройки сети могут изменяться либо в ЦУС в данном модуле, либо напрямую через редактирование файлов **`/etc/net/ifaces/<интерфейс>`**. В этом режиме можно просмотреть настройки сети, например, полученный по DHCP IP-адрес, через графический интерфейс **NetworkManager**.

NetworkManager (native)

В данном режиме управление настройками интерфейса передаётся **NetworkManager** и не зависит от файлов Etcnet. Управлять настройками можно через графический интерфейс **NetworkManager**. Файлы с настройками находятся в каталоге **`/etc/NetworkManager/system-connections`**. Этот режим особенно актуален для задач настройки сети на клиенте, когда IP-адрес необходимо получать динамически с помощью DHCP, а DNS-сервер указать явно. Через ЦУС так настроить невозможно, так как при включении DHCP отключаются настройки, которые можно задавать вручную.

systemd-networkd

В данном режиме режиме управление настройками интерфейса передаётся службе systemd-networkd. Настройки сети могут изменяться либо в ЦУС в данном модуле (только настройки физического интерфеса), либо напрямую через редактирование файлов **`/etc/systemd/network/<имя_файла>.network`**, **`/etc/systemd/network/<имя_файла>.netdev`**,**`/etc/`**
Данный режим доступен, если установлен пакет *systemd-networkd*;

Не контролируется

В этом режиме интерфейс находится в состоянии DOWN (выключен).

Примечание

После смены сетевой подсистемы с **Etcnet** на **systemd-networkd** может потребоваться вручную отключить службу network и включить systemd-networkd:

```
# systemctl disable --now network && systemctl enable --now systemd-networkd
```

И, наоборот, при смене с **systemd-networkd** на **Etcnet** отключить службу systemd-networkd и включить network:

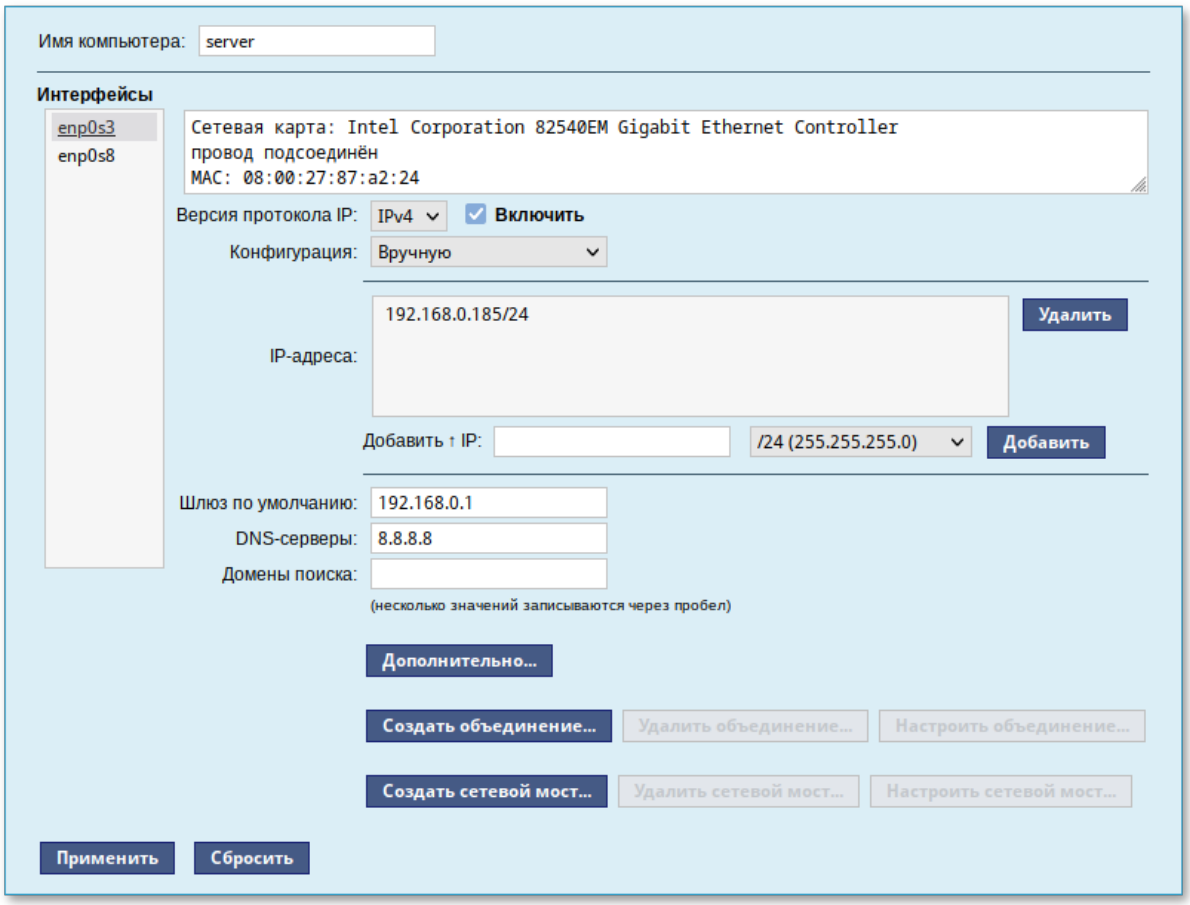
```
# systemctl disable --now systemd-networkd && systemctl enable --now network
```

28.2. Объединение сетевых интерфейсов

Модуль **Объединение интерфейсов** (пакет *alterator-net-bond*) позволяет объединить несколько физических сетевых интерфейсов в один логический. Это позволяет достичь отказоустойчивости, увеличения скорости и балансировки нагрузки.

Для создания объединения интерфейсов необходимо выполнить следующие действия:

1. Нажать кнопку **Создать объединение…**:



2. Переместить сетевые интерфейсы, которые будут входить в объединение, из списка **Доступные интерфейсы** в список **Используемые интерфейсы**.

3. Выбрать режим объединения:

   - **Round-robin** — режим циклического выбора активного интерфейса для исходящего трафика;

   - **Активный-резервный** — активен только один интерфейс, остальные находятся в режиме горячей замены;

   - **XOR** — один и тот же интерфейс работает с определённым получателем, передача пакетов распределяется между интерфейсами на основе формулы *((MAC-адрес источника) XOR (MAC-адрес получателя)) % число интерфейсов*;

   - **Широковещательная** — трафик идёт через все интерфейсы одновременно;

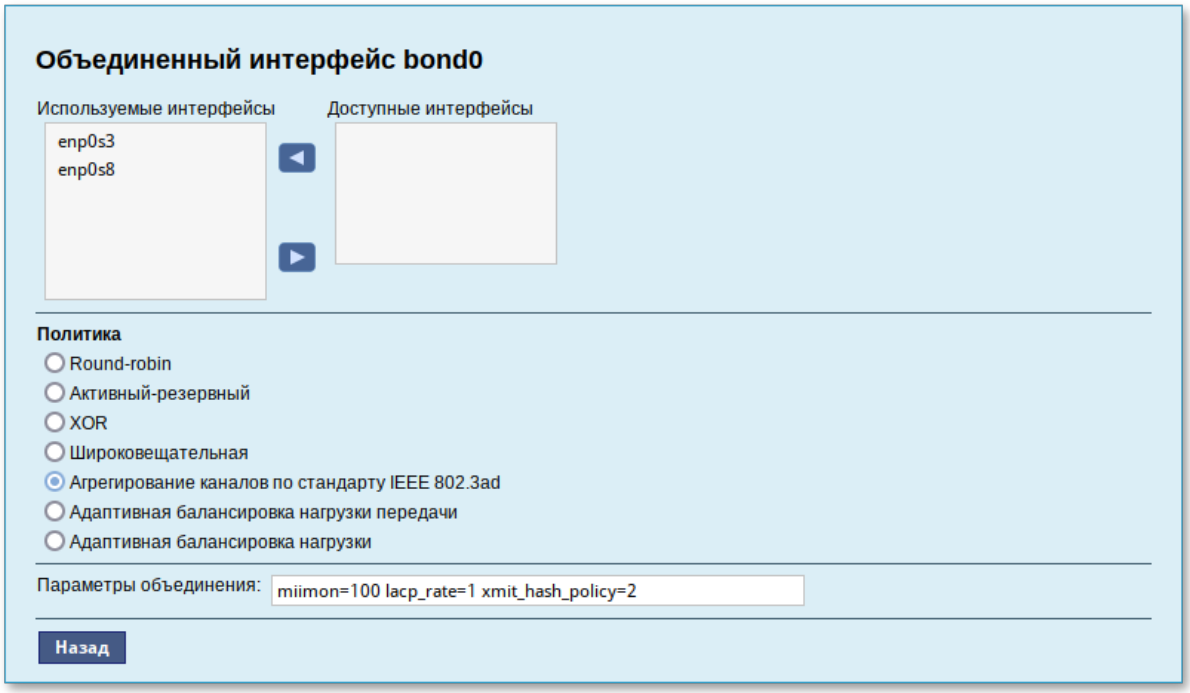
   - **Агрегирование каналов по стандарту IEEE 802.3ad** — в группу объединяются одинаковые по скорости и режиму интерфейсы, все физические интерфейсы используются одновременно в соответствии со спецификацией IEEE 802.3ad. Для реализации этого режима необходима поддержка на уровне драйверов сетевых карт и коммутатор, поддерживающий стандарт IEEE 802.3ad (коммутатор требует отдельной настройки);

   - **Адаптивная балансировка нагрузки передачи** — исходящий трафик распределяется в соответствии с текущей нагрузкой (с учётом скорости) на интерфейсах (для данного режима необходима его поддержка в драйверах сетевых карт). Входящие пакеты принимаются только активным сетевым интерфейсом;

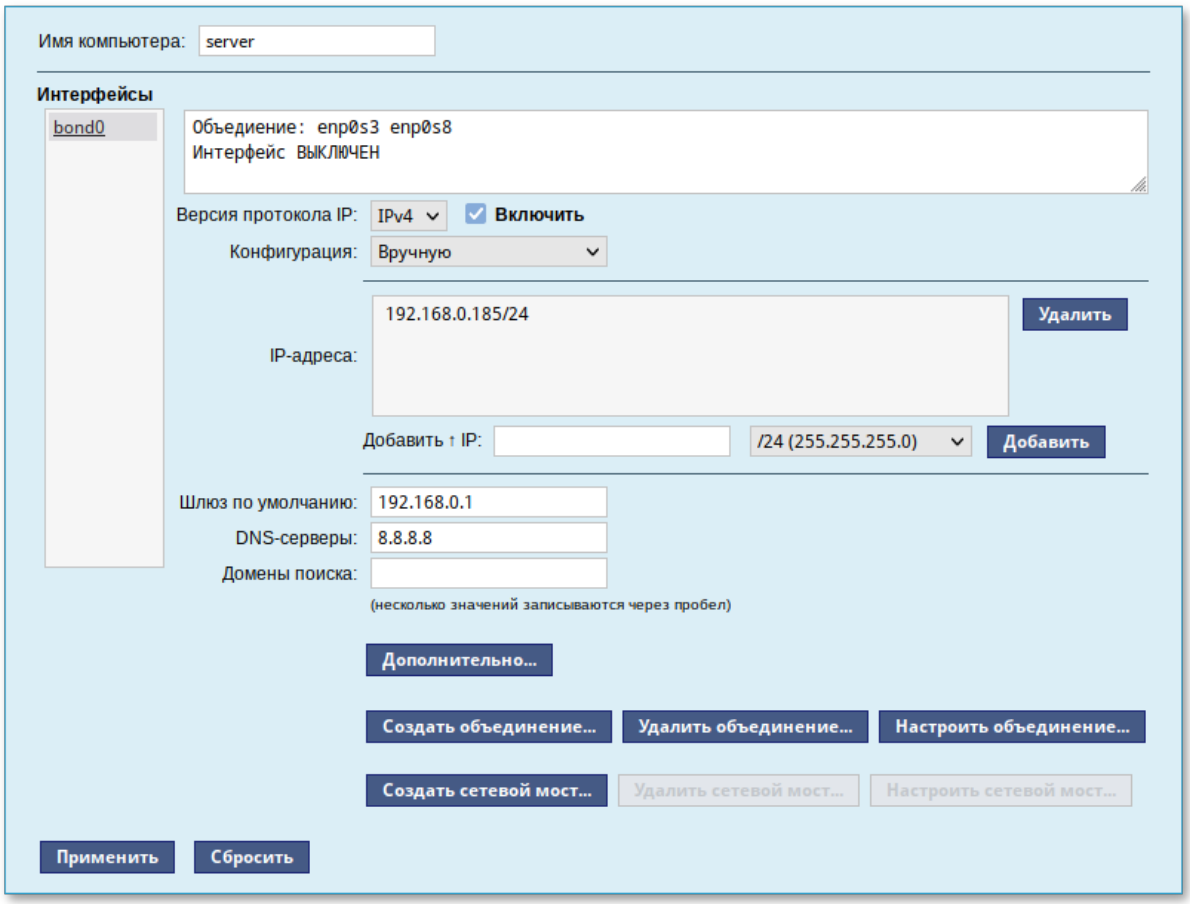
   - **Адаптивная балансировка нагрузки** — включает в себя балансировку исходящего трафика и балансировку на приём (rlb) для IPv4 трафика и не требует применения специальных коммутаторов. Балансировка на приём достигается на уровне протокола ARP путём перехвата ARP ответов локальной системы и перезаписи физического адреса на адрес одного из сетевых интерфейсов (в зависимости от загрузки).

4. Указать, если это необходимо, параметры объединения в поле **Параметры объединения**.

5. Нажать кнопку **Назад**:



6. В результате будет создан агрегированный интерфейс bond0. Для данного интерфейса можно задать IP-адрес и, если необходимо, дополнительные параметры:



7. Нажать кнопку **`Применить`**.

Информацию о получившемся агрегированном интерфейсе можно посмотреть в **`/proc/net/bonding/bond0`**.

Для удаления агрегированного интерфейса необходимо выбрать его в списке **Интерфейсы** и нажать кнопку **Удалить объединение…**.

28.3. Сетевые мосты

Модуль **Сетевые мосты** (пакет *alterator-net-bridge*) позволяет организовать виртуальный сетевой мост.

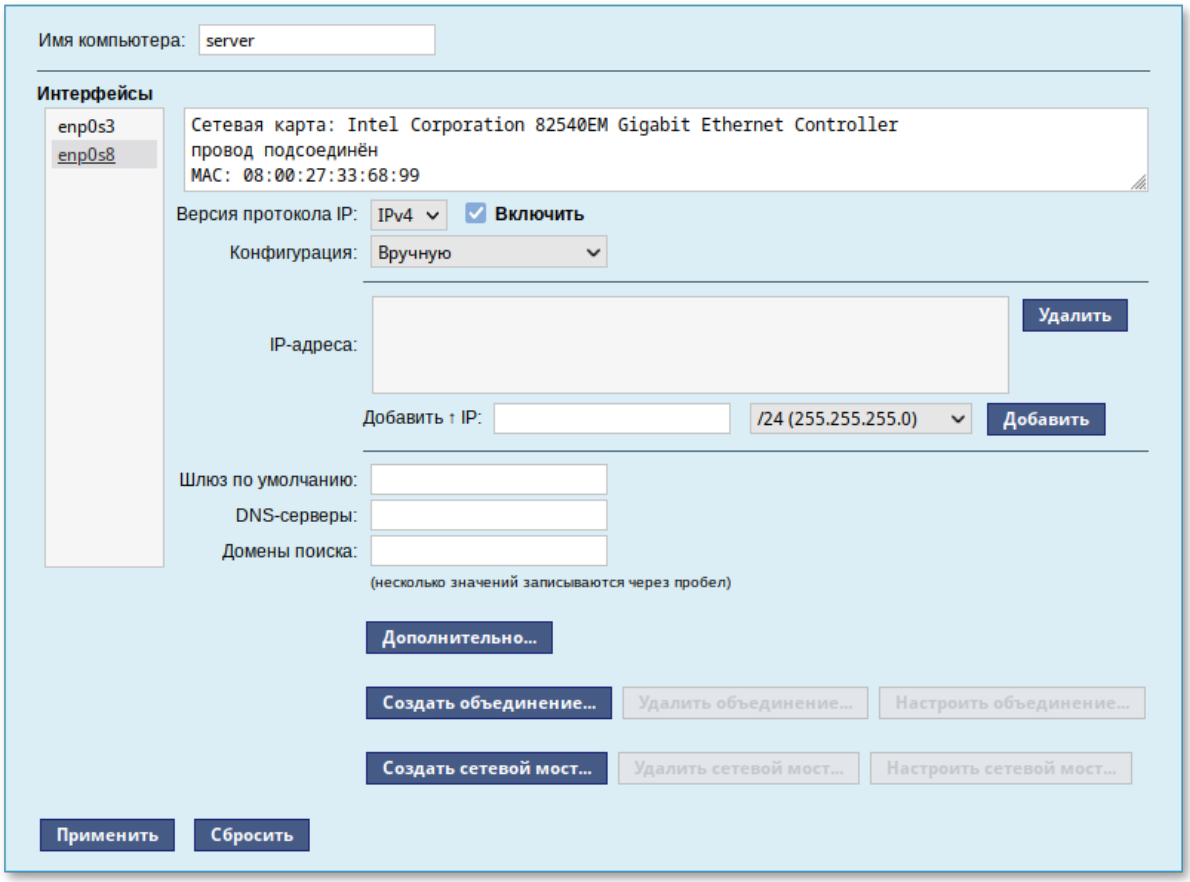
Предупреждение

Если интерфейсы, входящие в состав моста, являются единственными физически подключенными и настройка моста происходит с удалённого узла через эти интерфейсы, то требуется соблюдать осторожность, так как эти интерфейсы перестанут быть доступны.

Для создания Ethernet-моста необходимо выполнить следующие действия:

1. У интерфейсов, которые будут входить в мост, удалить IP-адреса и шлюз по умолчанию (если они были установлены).

2. Нажать кнопку **Создать сетевой мост…**:

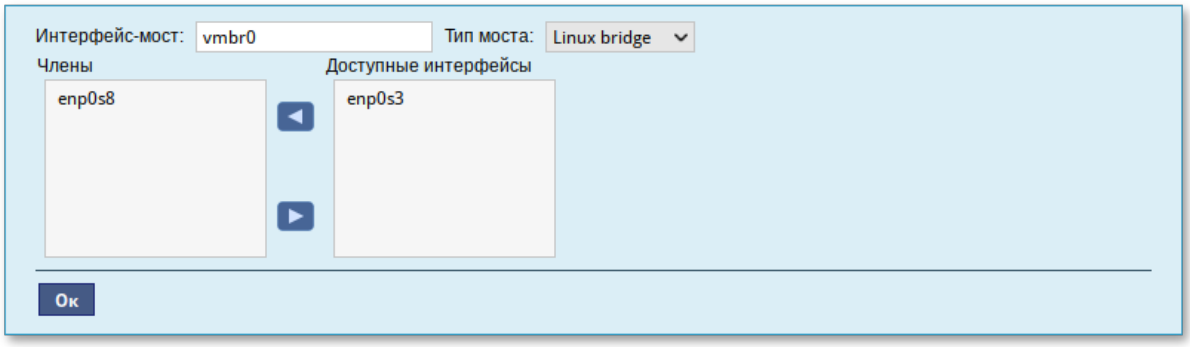


3. В окне **Сетевые мосты** в поле **Интерфейс-мост** ввести имя моста.

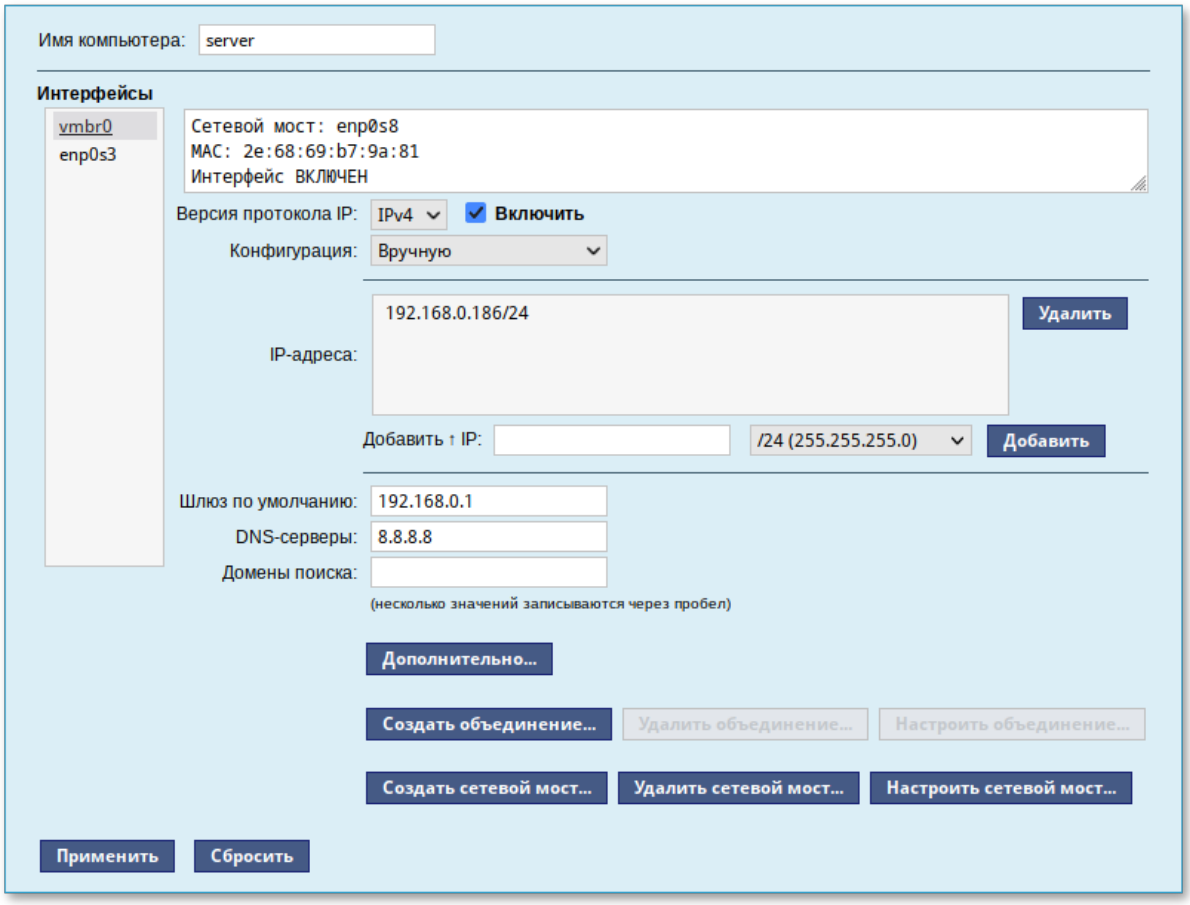
4. В выпадающем списке **Тип моста** выбрать тип моста: **Linux Bridge** (по умолчанию) или **Open vSwitch**.

5. Переместить сетевые интерфейсы, которые будут входить в мост, из списка **Доступные интерфейсы** в список **Члены**.

6. Нажать кнопку **Ок**:



7. В результате будет создан сетевой интерфейс моста (в примере vmbr0). Для данного интерфейса можно задать IP-адрес и, если необходимо, дополнительные параметры:



8. Нажать кнопку **Применить**.

Для удаления интерфейса моста необходимо выбрать его в списке **Интерфейсы** и нажать кнопку **Удалить сетевой мост…**.

28.4. Настройка общего подключения к сети Интернет

Пользователи корпоративных сетей обычно подключаются к сети Интернет через один общий канал. Для организации совместного доступа к сети Интернет стандартными средствами поддерживаются две технологии, которые могут использоваться как по отдельности, так и совместно:

- использование прокси-сервера;
- использование NAT.

Оба способа предполагают, что соединение с Интернет компьютера, через который предполагается настроить общий выход, предварительно сконфигурировано . Сделать это можно в разделе ЦУС **Сеть**.

28.4.1. Прокси-сервер

Отличительной особенностью использования прокси-сервера является то, что, помимо предоставления доступа к веб-сайтам, прокси-сервер кэширует загруженные страницы, а при повторном обращении к ним — отдаёт их из своего кэша. Это может существенно снизить потребление трафика.

У прокси-сервера есть два основных режима работы:

- прозрачный;
- обычный.

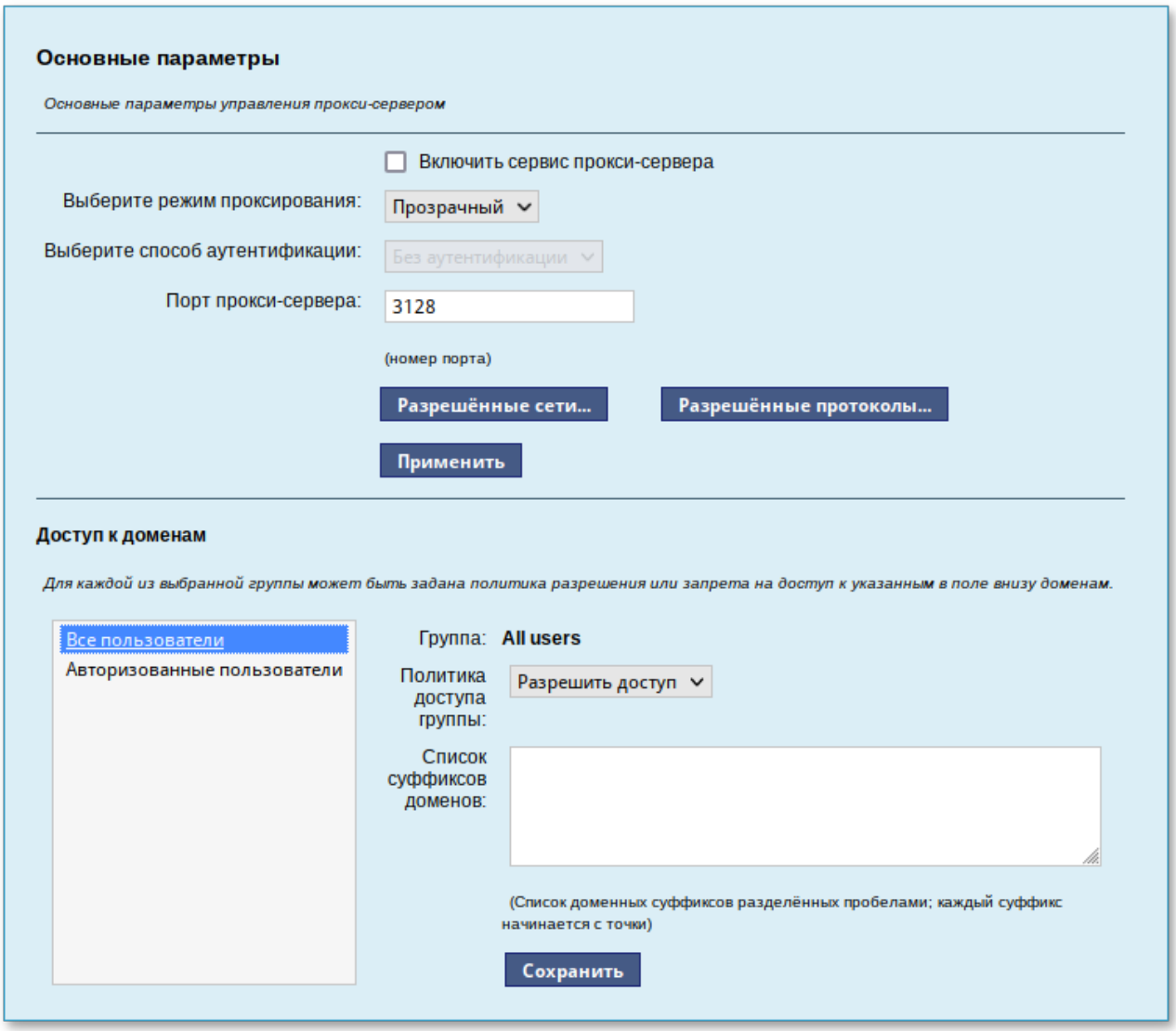
Для работы с прокси-сервером в прозрачном режиме не потребуется специальная настройка рабочих станций. Они лишь должны использовать сервер в качестве шлюза по умолчанию. Этого можно добиться, сделав соответствующие настройки на DHCP-сервере.

Для использования прокси-сервера в обычном режиме потребуется на каждом клиенте в настройках браузера указать данные прокси-сервера (IP-адрес и порт).

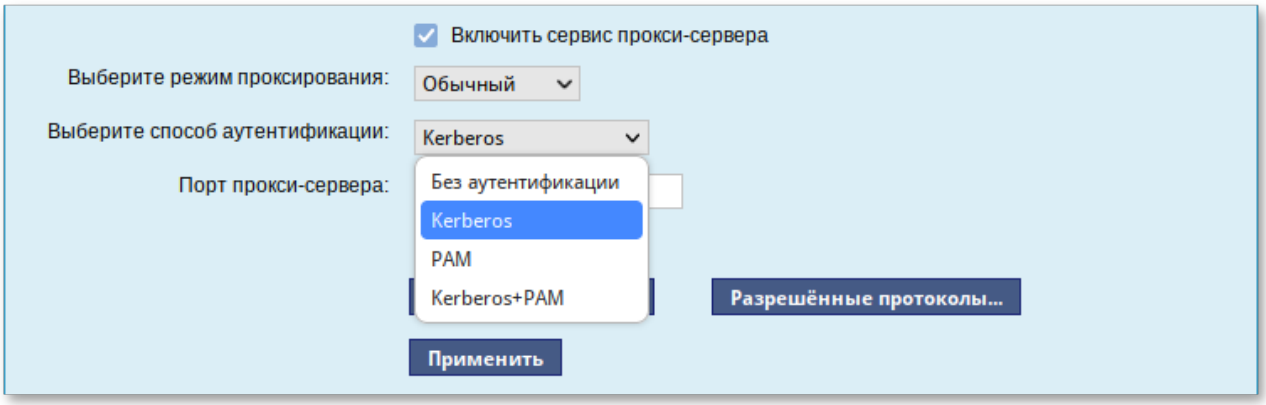
Преимуществом обычного режима работы, требующего перенастройки программ локальной сети, является возможность производить аутентификацию пользователей и контролировать их доступ во внешнюю сеть.

В различных браузерах местоположение формы настройки на прокси-сервер различное. Например, в браузере **Firefox** она доступна через меню **Правка** → **Настройки** → **Основные** → **Настройки сети** кнопка **Настроить…**. Здесь следует выбрать **Ручная настройка прокси** и указать IP-адрес и порт прокси-сервера.

По умолчанию прокси-сервер не предоставляет доступ в Интернет никому кроме себя самого. Список сетей, обслуживаемых прокси-сервером можно изменить, нажав на кнопку «**Разрешённые сети…**» в модуле ЦУС **Прокси-сервер** (пакет *alterator-squid*) из раздела **Серверы**.

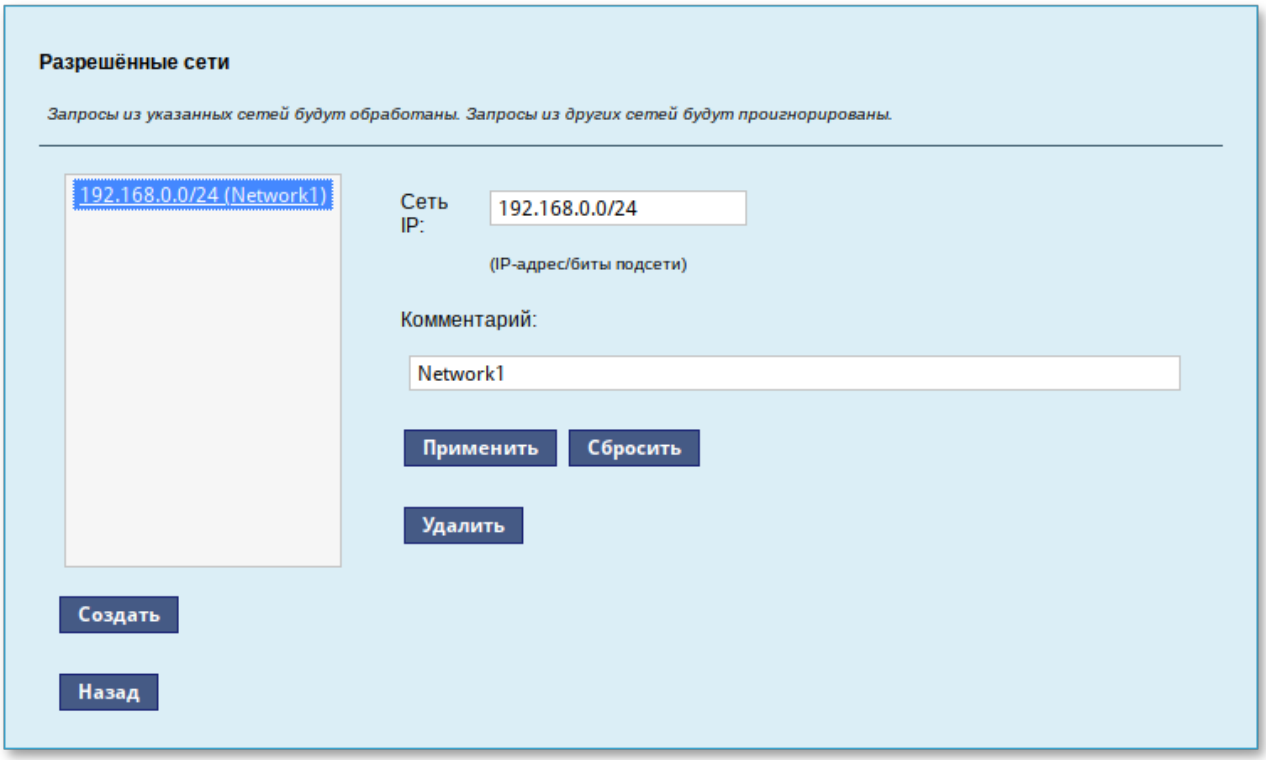


Для того чтобы включить аутентификацию пользователей и контролировать их доступ во внешнюю сеть, необходимо выбрать обычный режим проксирования и способ аутентификации, отличный от **`Без аутентификации`**:

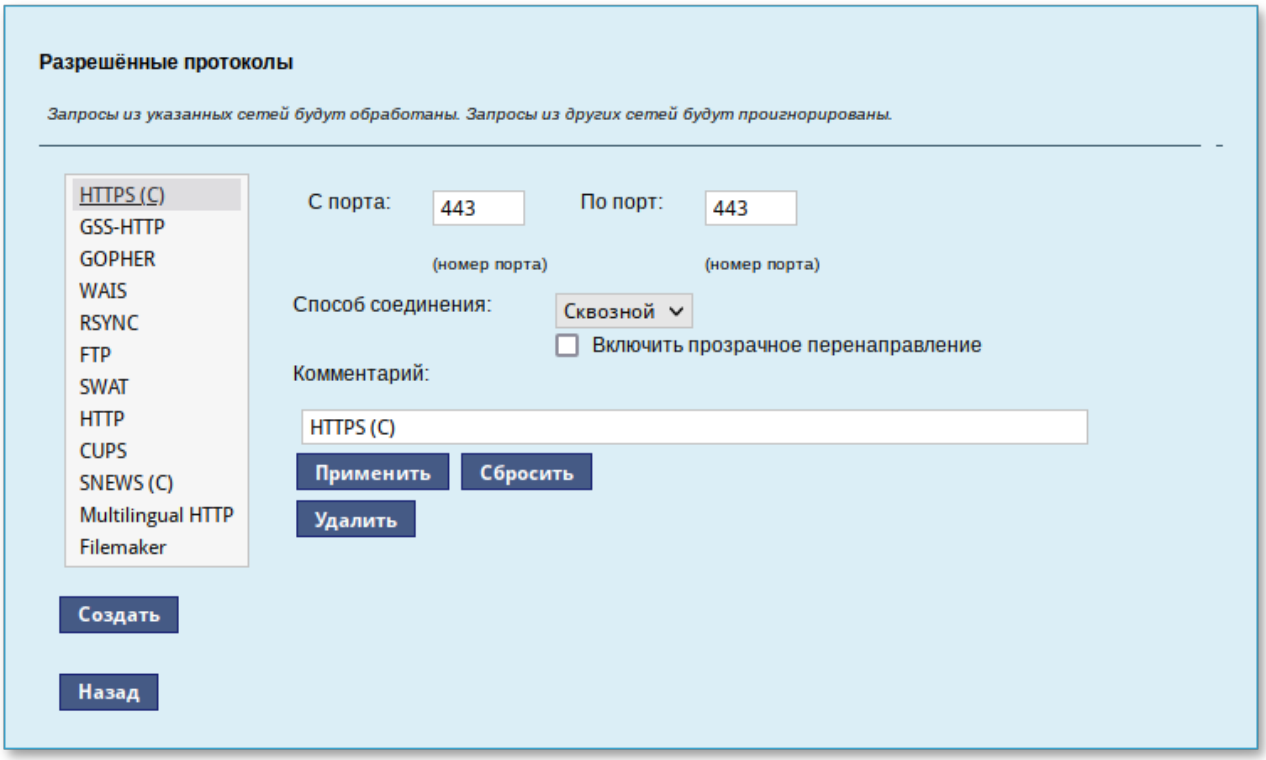


Прокси-сервер принимает запросы из локальной сети и, по мере необходимости, передаёт их во внешнюю сеть. Поступление запроса ожидается на определённом порту, который по умолчанию имеет стандартный номер 3128. Если по каким-то причинам не желательно использовать данный порт, то можно поменять его значение на любое другое.

Перед тем как выполнить перенаправление запроса, прокси-сервер проверяет принадлежность сетевого адрес узла, с которого запрос был отправлен к группе внутренних сетевых адресов. Для того чтобы запросы, отправленные из локальной сети, обрабатывались прокси-сервером, необходимо добавить соответствующую группу адресов (адрес подсети и адресную маску) в список внутренних сетей в разделе **Разрешённые сети**:



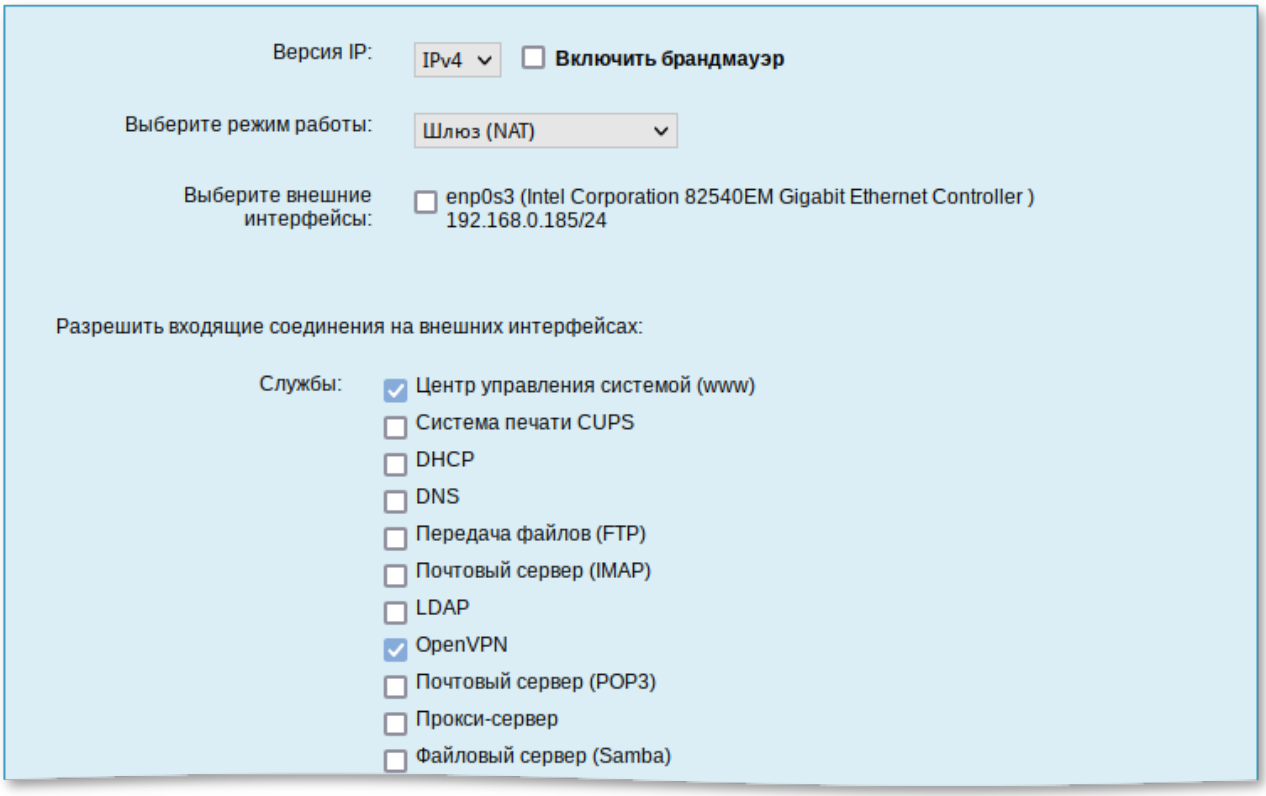
Вторым условием передачи запроса является принадлежность целевого порта к разрешённому диапазону. Посмотреть и отредактировать список разрешённых целевых портов можно в разделе **Разрешённые протоколы**:



28.4.2. NAT

NAT (Network Address Translation, преобразование сетевых адресов) — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Таким образом, компьютеры локальной сети, имеющие IP-адреса, зарезервированные для использования исключительно в локальных сетях, могут использовать общий канал доступа к Интернет (общий внешний IP-адрес). При этом на компьютере-шлюзе, непосредственно подключённом к Интернет, выполняется преобразование адресов.

Настройка NAT осуществляется в модуле ЦУС **Внешние сети** (пакет *alterator-net-iptables*) из раздела **Брандмауэр**. Для минимальной настройки достаточно выбрать режим работы **Шлюз (NAT)**, отметить правильный внешний сетевой интерфейс и нажать на кнопку **Применить**.



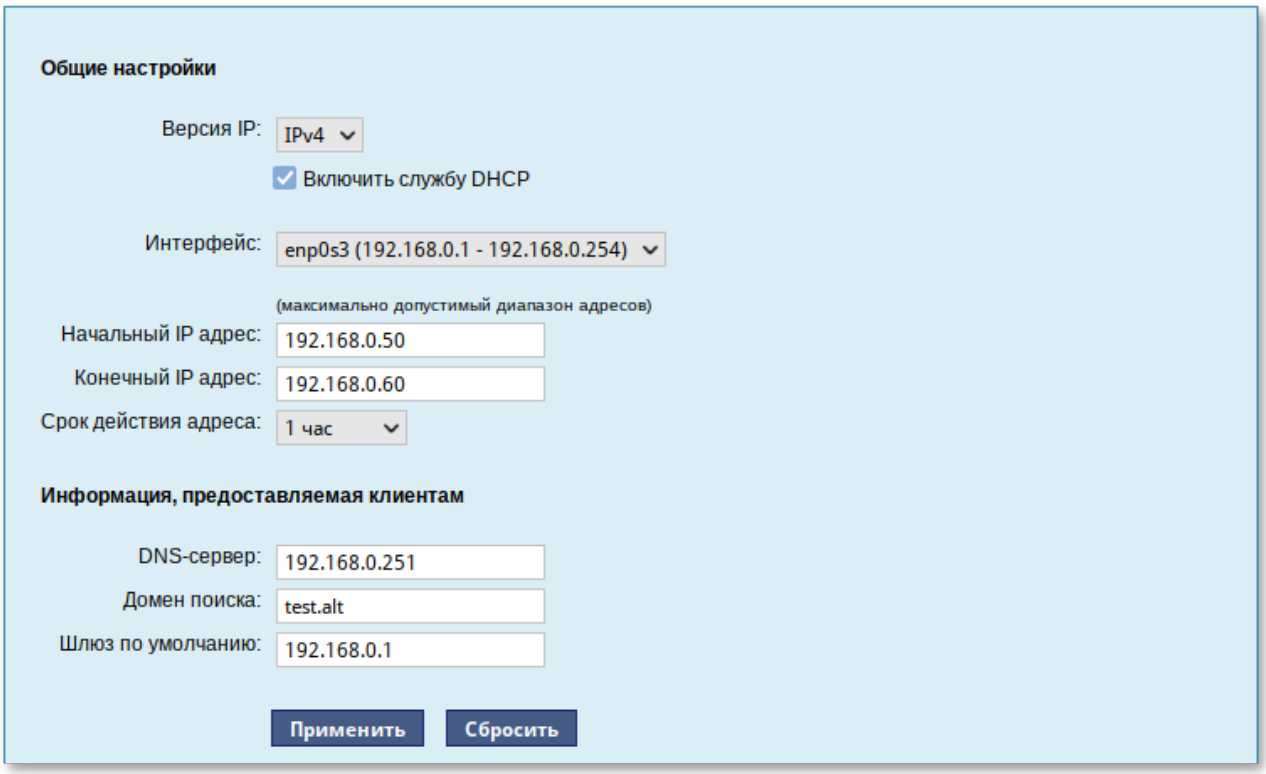
28.5. Автоматическое присвоение IP-адресов (DHCP-сервер)

DHCP (Dynamic Host Configuration Protocol) — протокол, позволяющий клиенту самостоятельно получить IP-адрес из зарезервированного диапазона адресов, а также дополнительную информацию о локальной сети (DNS-сервер сети, домен поиска, шлюз по умолчанию). Это облегчает администрирование клиентских машин, избавляя администратора домена от необходимости вручную настраивать сетевые интерфейсы на компьютерах локальной сети.

Чтобы настраивать DHCP-сервер, на машине должен быть хотя бы один статически сконфигурированный Ethernet-интерфейс.

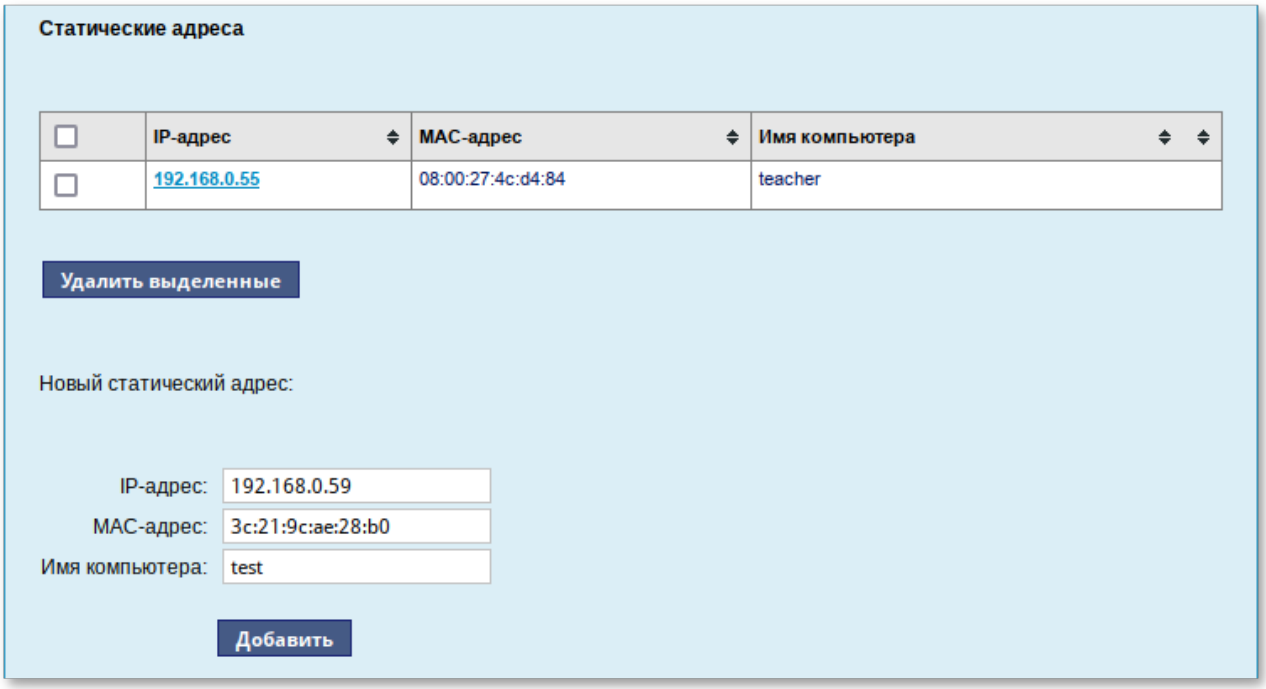
Настройка DHCP-сервера осуществляется в модуле ЦУС **DHCP-сервер** (пакет *alterator-dhcp*) из раздела **Серверы**.

Для включения DHCP-сервера необходимо установить флажок **Включить службу DHCP**, указать начальный и конечный IP-адрес, а также шлюз по умолчанию (обычно это IP-адрес сервера на сетевом интерфейсе, обслуживающем локальную сеть).

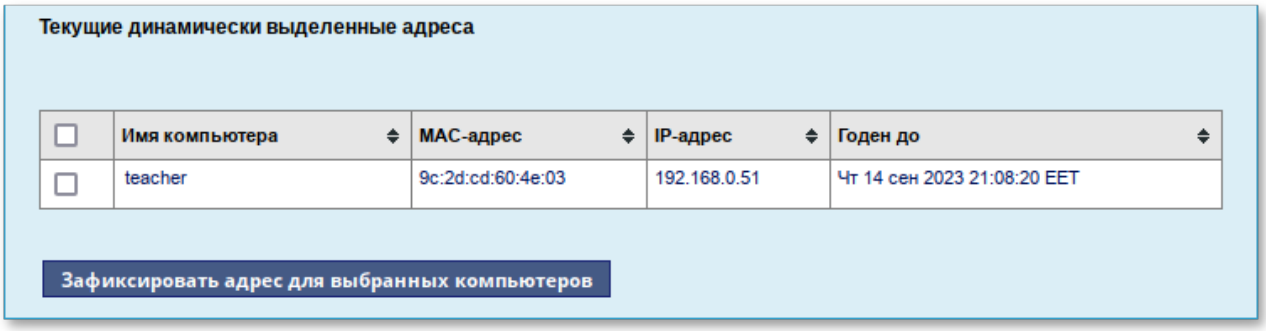


Теперь при включении любой клиентской машины с настройкой **`получение ip и dns автоматически`** будет присваиваться шлюз 192.168.0.1, DNS 192.168.0.251 и адреса начиная с 192.168.0.50 по порядку включения до 192.168.0.60.

Иногда бывает полезно выдавать клиенту один и тот же IP-адрес независимо от момента обращения. В этом случае он определяется по аппаратному адресу (MAC-адресу) сетевой карты клиента. Для добавления своих значений в таблицу соответствия статических адресов введите IP-адрес и соответствующий ему MAC-адрес и нажмите кнопку **`Добавить`**.



Выданные IP-адреса можно увидеть в списке **Текущие динамически выданные адреса**. Здесь также имеется возможность зафиксировать выданные адреса, за данными компьютерами. Для этого необходимо отметить хост, за которым нужно закрепить IP-адрес и нажать кнопку **Зафиксировать адрес для выбранных компьютеров**.



Глава 29. Развертывание доменной структуры

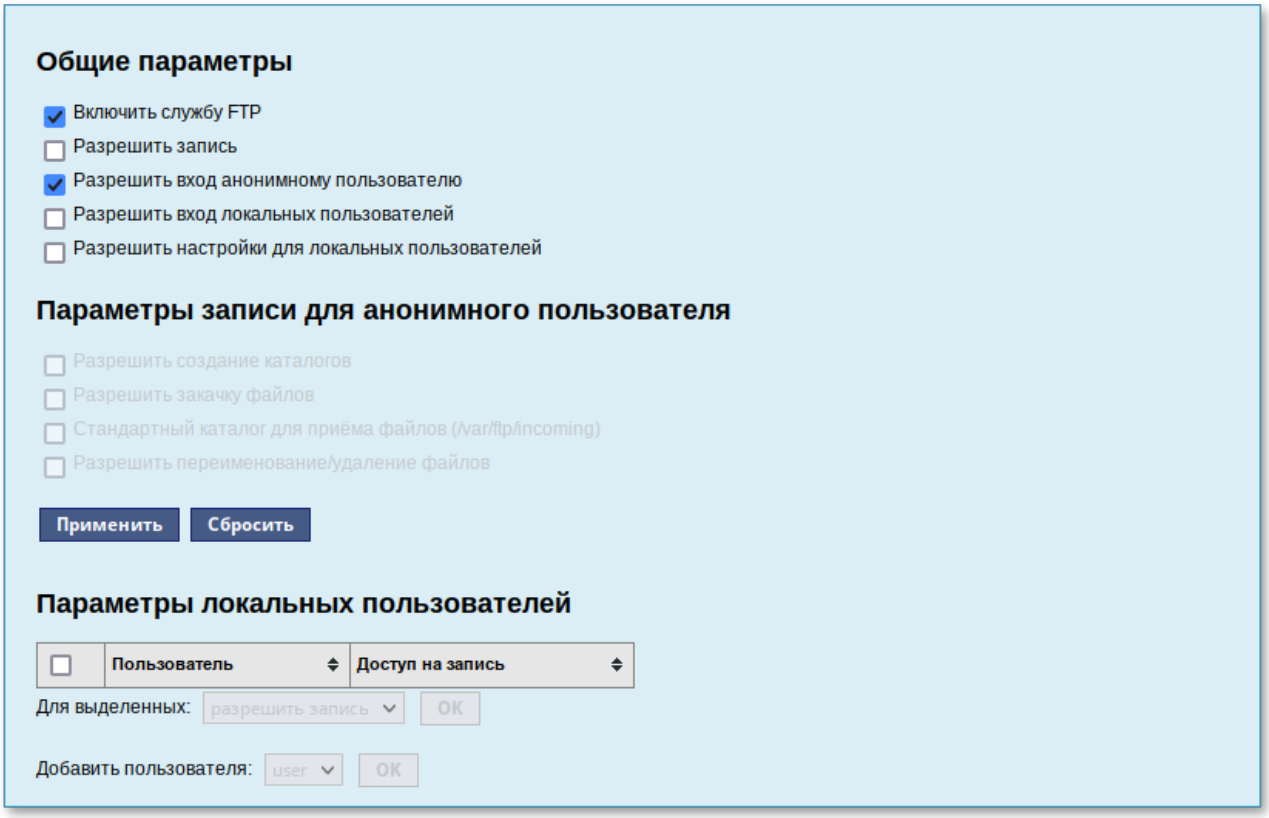
Для развертывания доменной структуры предназначен модуль ЦУС **Домен** из раздела **Система** (пакет *alterator-net-domain*):

Модуль поддерживает следующие виды доменов:

- ALT-домен. Домен, основанный на OpenLDAP и MIT Kerberos. Домен нужно устанавливать только после настройки сервера DHCP. В противном случае придётся выбирать другое имя домена.
- Active Directory. Домен для контроллера домена Samba AD. Рекомендуется для аутентификации рабочих станций под управлением и Windows и Linux.
- DNS. Обслуживание только запросов DNS указанного домена сервисом BIND.

Глава 30. FTP-сервер

Модуль **FTP-сервер** (пакет *alterator-vsftpd*) из раздела **Серверы** предназначен для настройки FTP-сервера (vsftpd).



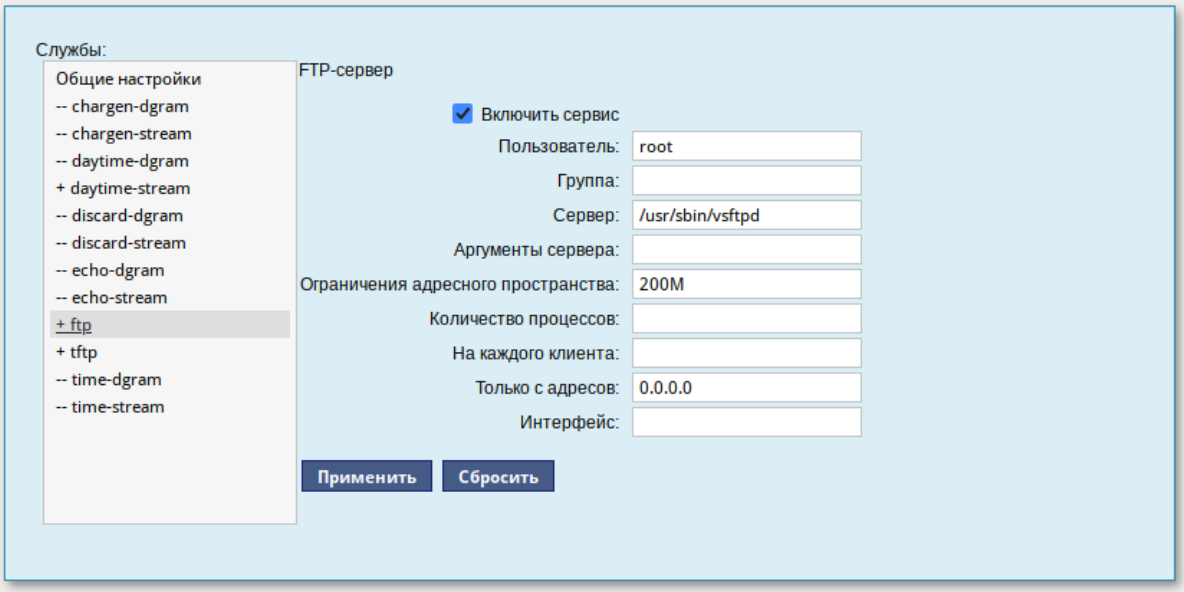
Чаще всего протокол FTP (File Transfer Protocol) используется для организации файлового сервера с анонимным доступом. Возможность анонимного доступа управляется параметром **`Разрешить вход анонимному пользователю`**. Менее распространённый вариант — сервер с возможностью загружать на него файлы, в том числе и анонимным пользователям. Возможность загрузки включается параметром **`Разрешить запись`**. Еще один вариант — сервер, позволяющий локальным пользователям скачивать и загружать файлы из своих домашних каталогов. Этот вариант используется редко, что связано с небезопасностью протокола FTP. Возможность работы с локальными пользователями управляется параметром **`Разрешить вход локальным пользователям`**. Чтобы пользователи могли загружать файлы, требуется включить параметр **`Разрешить запись`**. Разрешение на загрузку файлов можно настраивать индивидуально, для этого необходимо отметить параметр **`Разрешить настройку локальных пользователей`**.

Если вам необходимо создать анонимный FTP-сервер, вы можете использовать vsftpd в сочетании с пакетом anonftp. В целях безопасности сервер по умолчанию сконфигурирован именно для предоставления анонимного доступа. Запрещены любые команды записи, а также доступ локально зарегистрированных пользователей.

При установке пакета *anonftp* автоматически создаётся каталог, который будет корневым при анонимном подключении, — **`/var/ftp`** с необходимыми правами доступа. Владельцем этого каталога является пользователь root, а не псевдопользователь, от имени которого работает vsftpd. Это сделано для обеспечения безопасности FTP-сервера и системы в целом. Группой-владельцем каталога является специальная группа ftpadmin, предназначенная для администраторов FTP-сервера.

Примечание

Многие параметры использования FTP-сервера, в том числе относящиеся к безопасности, могут быть заданы при помощи xinetd. В частности, этот сервер позволяет ограничить количество одновременно выполняемых процессов как по системе в целом, так и для каждого отдельного пользователя, указать пользователя, от имени которого будет выполняться служба, задать приоритет процесса (nice), указать адреса, с которых разрешено подключение к данной службе, а также время доступа и множество других параметров. Указать эти настройки можно в модуле **Службы xinetd** (пакет *alterator-xinetd*) из раздела **Система**. Например, установить неограниченный по адресам доступ можно, указав в поле **Только с адресов** значение 0.0.0.0:



Глава 31. Удостоверяющий центр

Модуль **Удостоверяющий центр** (пакет *alterator-ca*) из раздела **Система** служит для выдачи сертификатов службам на серверах и рабочих станциях.

Для обеспечения безопасности соединения для клиента (в качестве клиентского ПО может выступать, например, веб-браузер) основным является вопрос о принятии сертификата. При принятии сертификата возможны описанные ниже варианты.

Сертификат сервера подписан одним из известных клиенту удостоверяющим центром (УЦ)

В этом случае сертификат принимается и устанавливается безопасное SSL-соединение. Обычно клиентское ПО (например, веб-браузер) содержит список наиболее известных УЦ и предоставляет возможность управления (добавление/удаление) сертификатами таких УЦ.

Сертификат сервера подписан УЦ неизвестным клиенту

В этом случае следует самостоятельно решить вопрос о принятии такого сертификата:

- можно временно (на время одной сессии) принять сертификат сервера;
- можно принять сертификат сервера на постоянной основе;

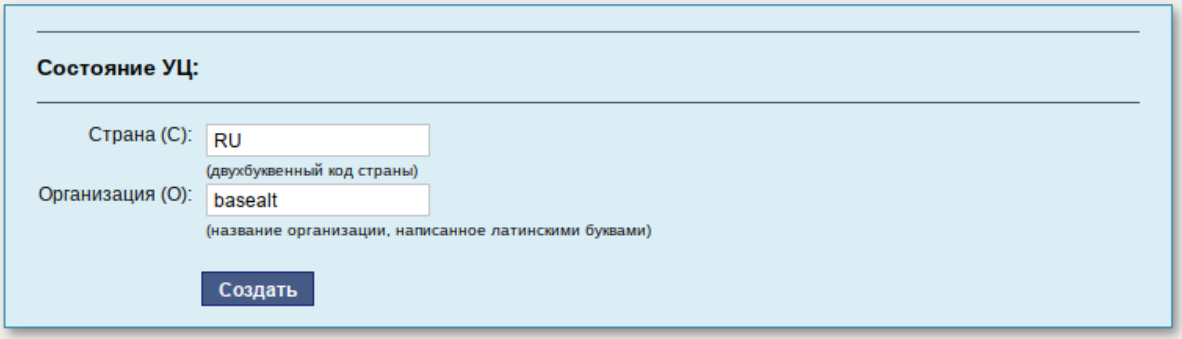
- если вы доверяете УЦ, подписавшему сертификат, можно добавить сертификат самого УЦ к списку известных сертификатов, и таким образом, в дальнейшем все сертификаты, подписанные этим УЦ, будут приниматься автоматически.

Сертификат сервера является самоподписанным

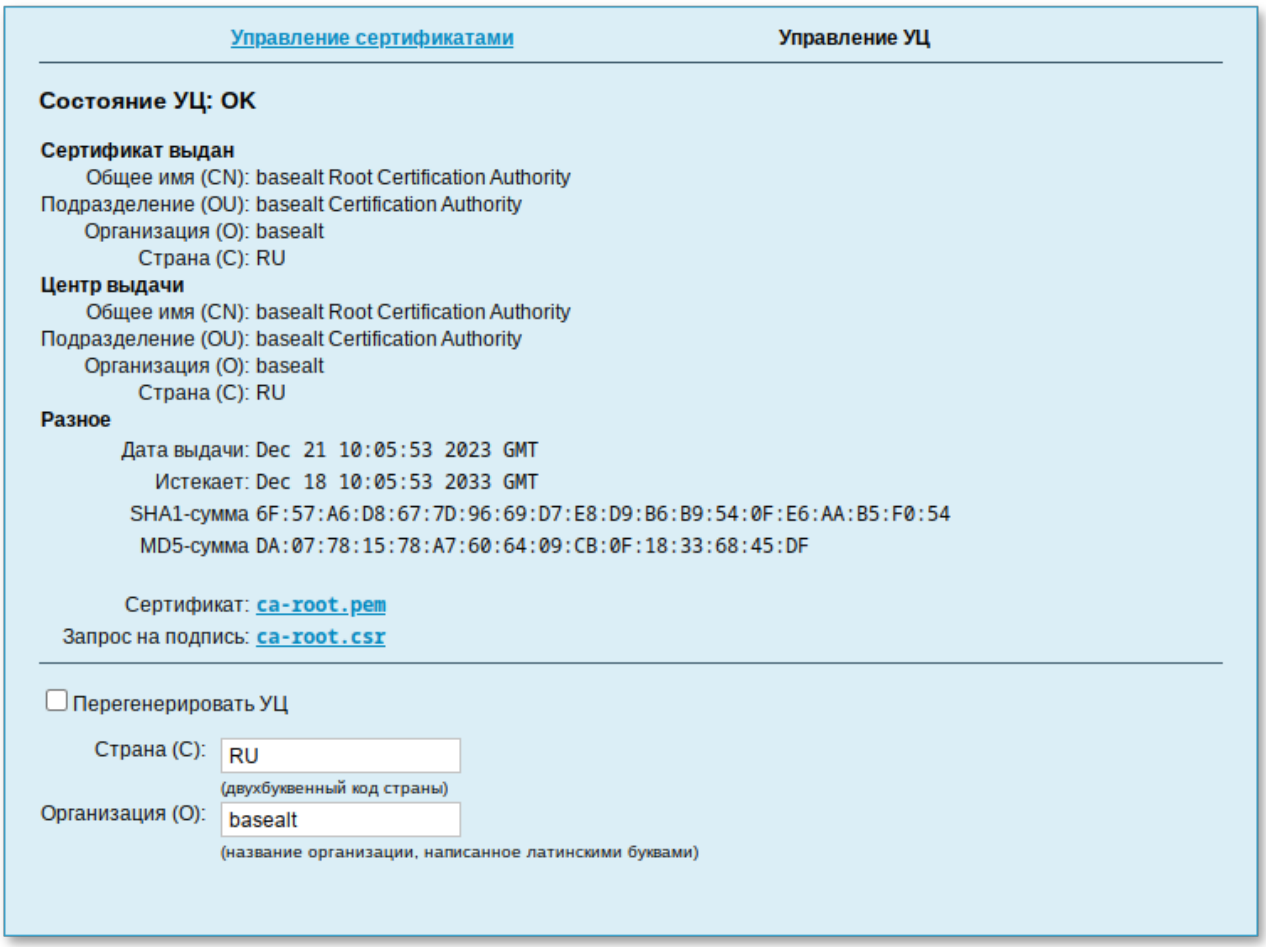
Это случай, когда сертификат сервера не подтверждён вообще никакой третьей стороной. Такие сертификаты используются в локальных сетях, где вы самостоятельно можете проверить аутентичность сервера. В случае самоподписанных сертификатов вы должны самостоятельно убедиться в том, что сервер является тем, за кого себя выдаёт. Сделать это можно, сверив отпечатки полученного сертификата и реально находящегося на сервере.

Примечание

При первом обращении к модулю **Удостоверяющий центр** необходимо создать УЦ, указав страну и организацию:

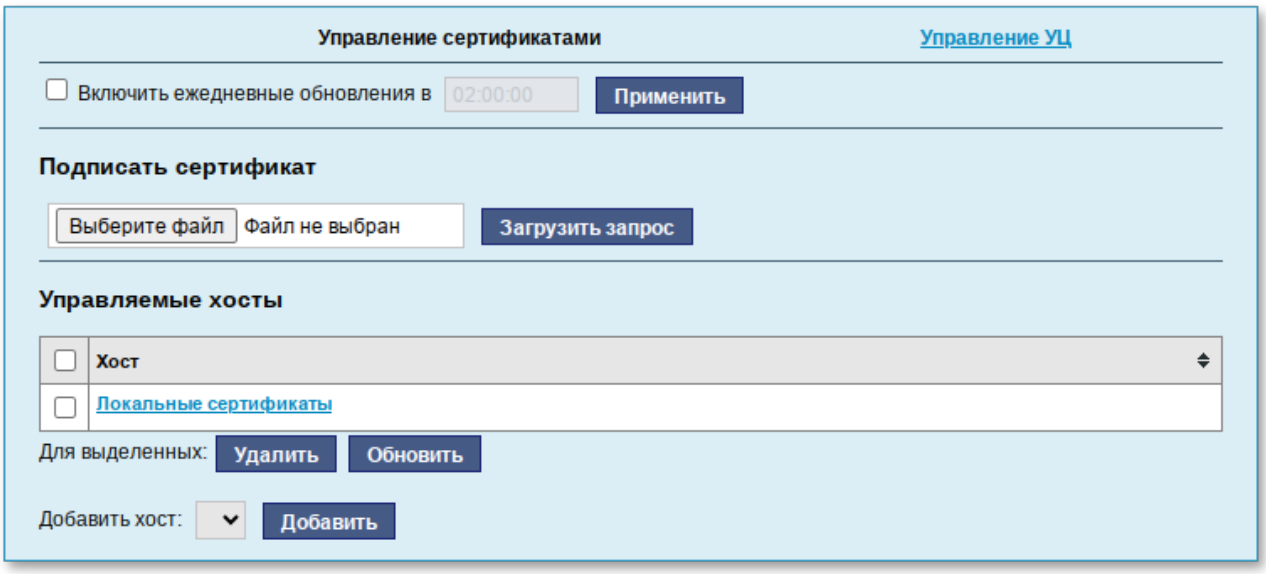


Модуль **Удостоверяющий центр** включает две вкладки: **Управление УЦ** и **Управление сертификатами**.



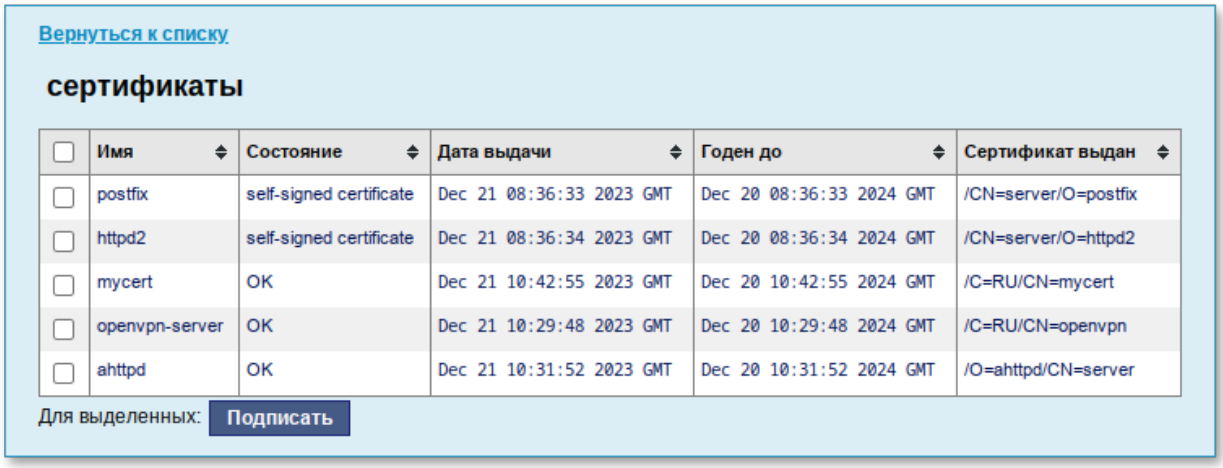
На вкладке **Управление УЦ** можно:

- просмотреть информацию о сертификате УЦ;
- выгрузить для дальнейшего использования сертификат УЦ (файл **ca-root.pem**). Этот файл можно будет добавить к списку УЦ, используемому клиентским ПО, после чего все сертификаты, подписанные данным УЦ будут приниматься автоматически;
- выгрузить, для дальнейшего использования, запрос на подпись сертификата УЦ (файл **ca-root.csr**). Этот запрос можно подписать сторонним УЦ;
- перегенерировать сертификат УЦ с другими параметрами (можно изменить параметры: **Страна (C)** и **Организация (O)**).

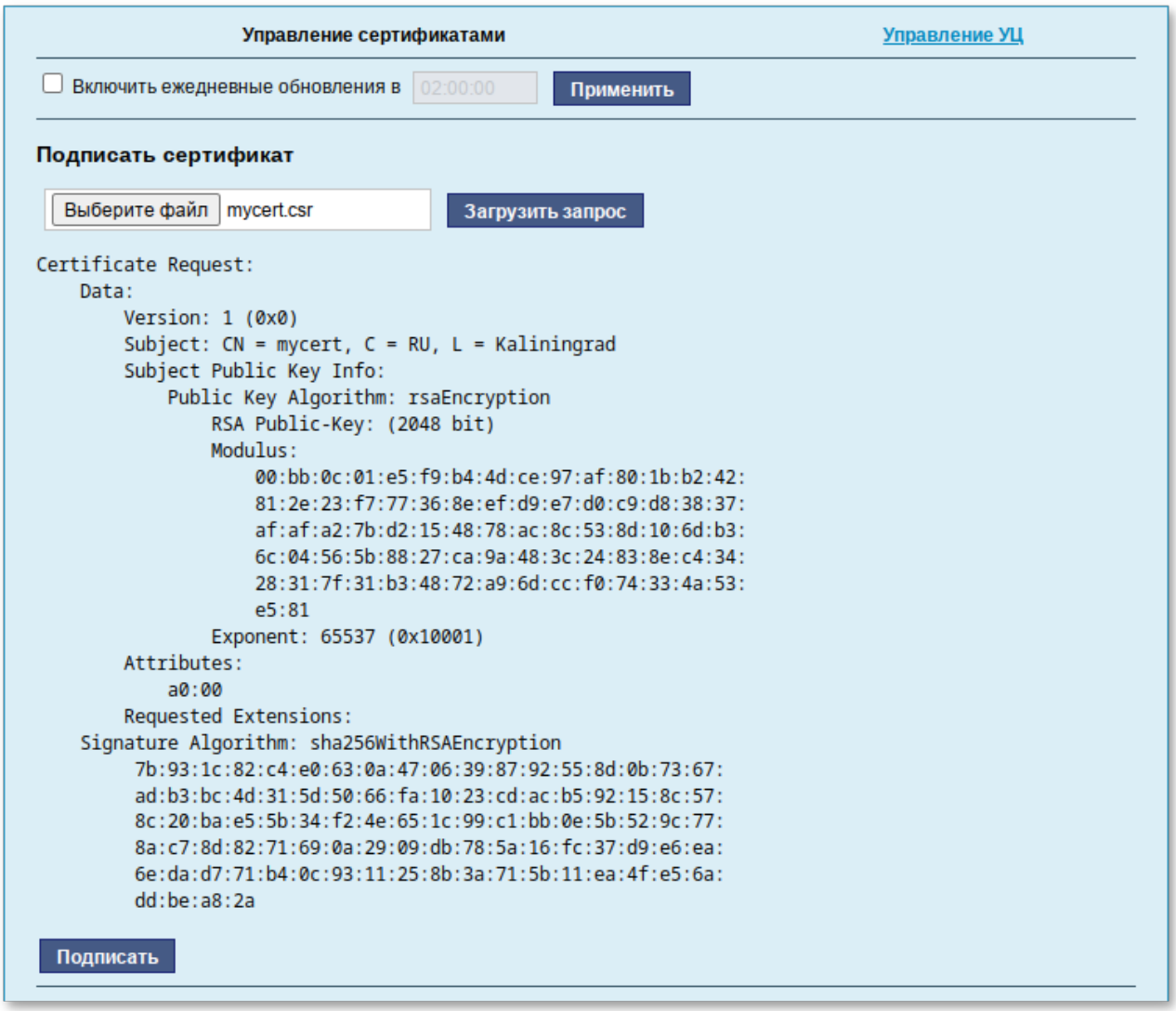


На вкладке **Управление сертификатами** можно:

- настроить ежедневное обновление подписей сертификатов, используемых локальными службами и службами подчинённых серверов;
- подписать произвольный сертификат (запрос на подпись) корневым сертификатом УЦ, настроенным на вкладке **Управление УЦ**;
- просмотреть состояния и подпись локальных сертификатов и сертификатов подчинённых серверов:



Чтобы подписать сертификат необходимо на вкладке **Управление сертификатами** нажать кнопку **Выберите файл**, выбрать файл с запросом на подпись и нажать кнопку **Загрузить запрос**. В результате на экране отобразится запрос на подпись. Далее следует нажать кнопку **Подписать**:



Подписанный сертификат (файл **`output.pem`**) будет загружен в каталог загрузок.

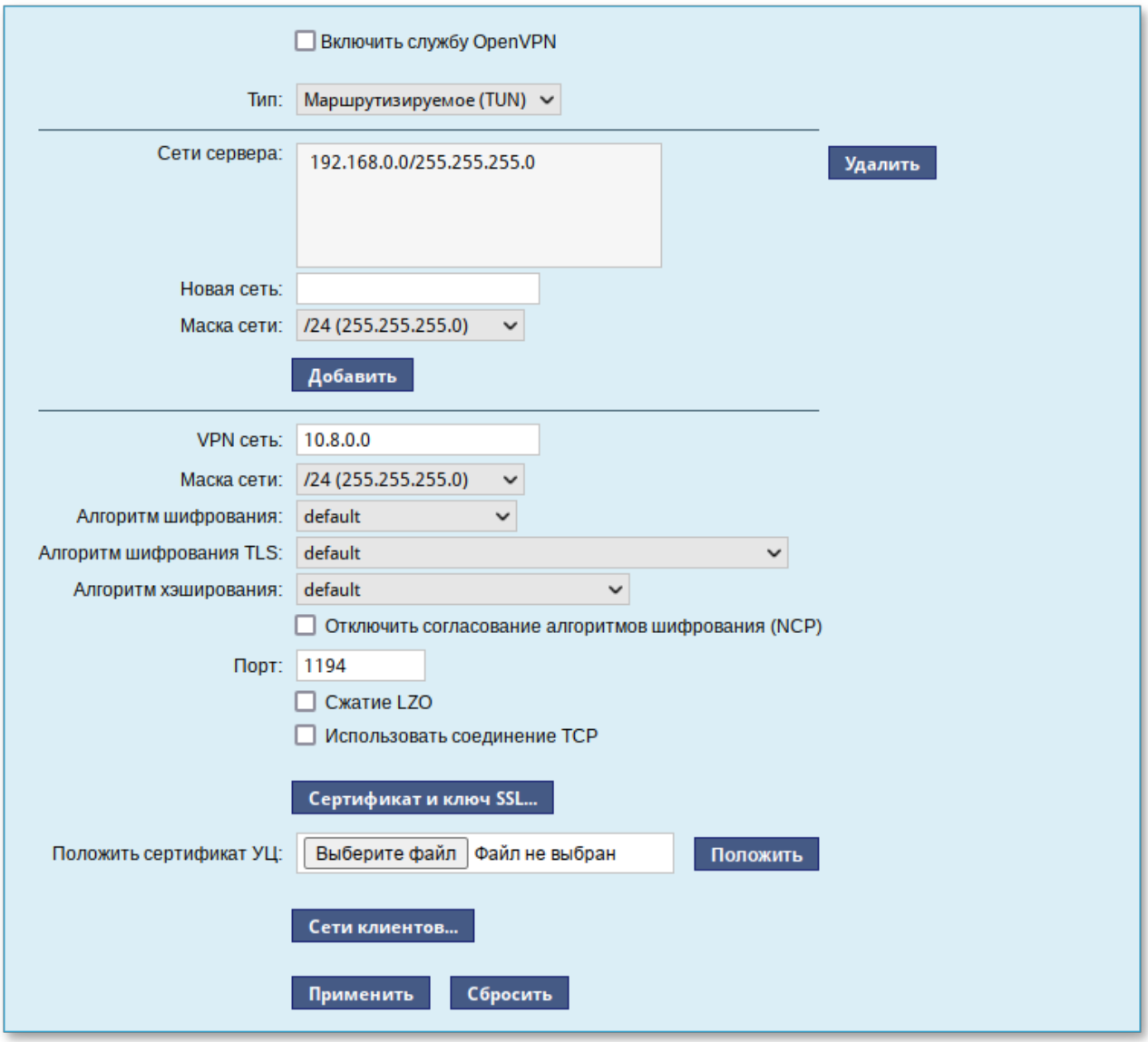
Глава 32. Соединение удалённых офисов (OpenVPN-сервер)

Альт Сервер для Эльбрус предоставляет возможность безопасного соединения удалённых офисов, используя технологию VPN (англ. Virtual Private Network — виртуальная частная сеть), которая позволяет организовать безопасные шифрованные соединения через публичные сети (например, Интернет) между удалёнными офисами или локальной сетью и удалёнными пользователями. Таким образом, вы можете связать два офиса организации, что делает работу с документами, расположенными в сети удалённого офиса, более удобной.

Помимо соединения целых офисов, также существует возможность организовать доступ в офисную сеть для работы в ней извне. Это означает, например, что сотрудник может работать в своём привычном окружении, даже находясь в командировке или просто из дома.

32.1. Настройка OpenVPN-сервера

Для организации VPN соединения на стороне сервера предусмотрен модуль ЦУС **OpenVPN-сервер** (пакет *alterator-openvpn-server*) из раздела **Серверы**.



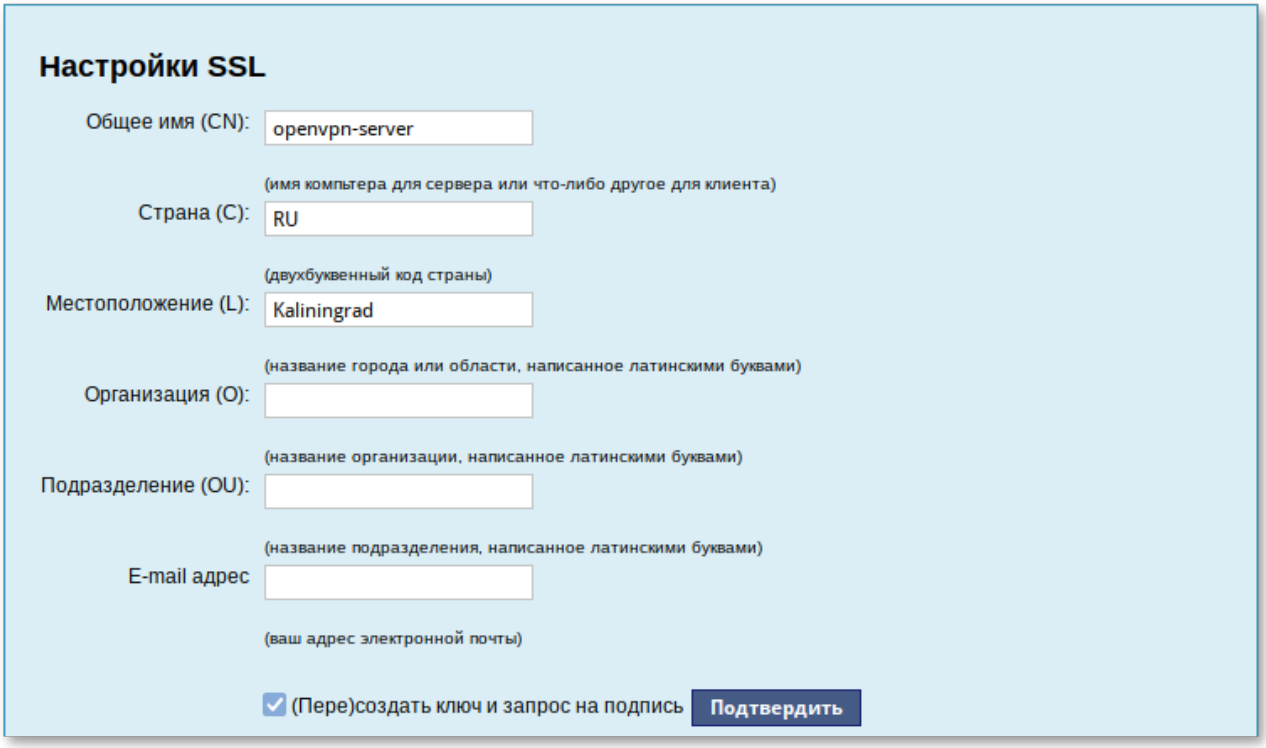
Используя модуль **OpenVPN-сервер** можно:

- включить/отключить OpenVPN-сервер;
- настроить параметры сервера: тип, сети сервера, использование сжатия и т.д.;
- управлять сертификатами сервера;
- настроить сети клиентов.

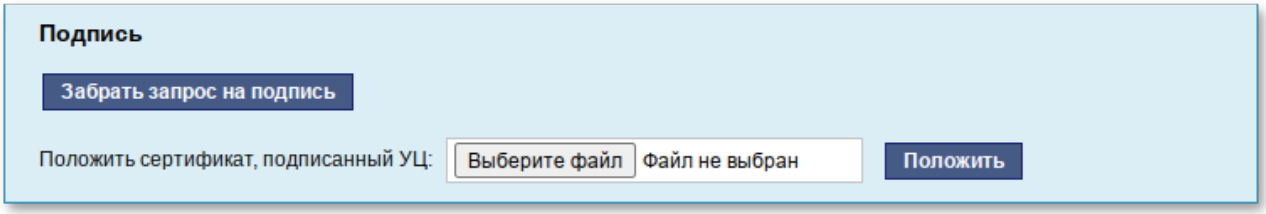
Особое внимание при планировании и настройке подключений следует обратить на используемые сети. Они *не должны* пересекаться.

Для создания соединения необходимо установить флажок **`Включить службу OpenVPN`**, выбрать тип подключения: маршрутизируемое (используется TUN) или через мост (используется TAP), и проверить открываемую по соединению сеть (обычно это локальная сеть в виде IP-адреса и маски подсети).

Для настройки сертификата и ключа ssl необходимо нажать на кнопку **`Сертификат и ключ ssl..`**. Откроется окно модуля **Управление ключами SSL** (пакет *alterator-sslkey*):

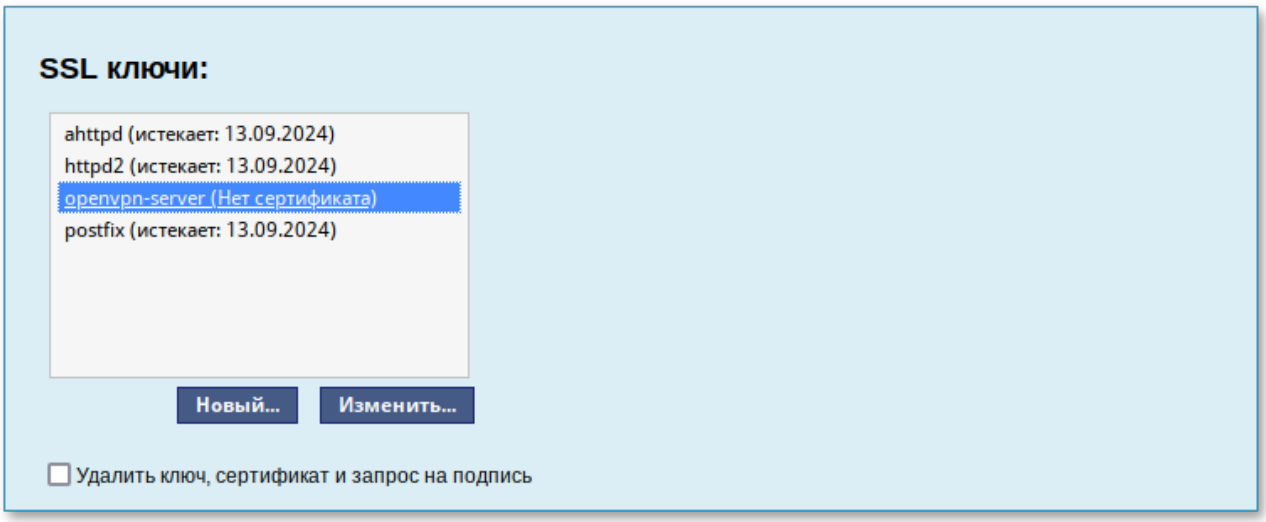


Здесь нужно заполнить поле **`Общее имя (CN)`** и поле **`Страна (C)`** (прописными буквами), отметить пункт **`(Пере)создать ключ и запрос на подпись`** и нажать кнопку **`Подтвердить`**. После чего станет активной кнопка **`Забрать запрос на подпись`**:

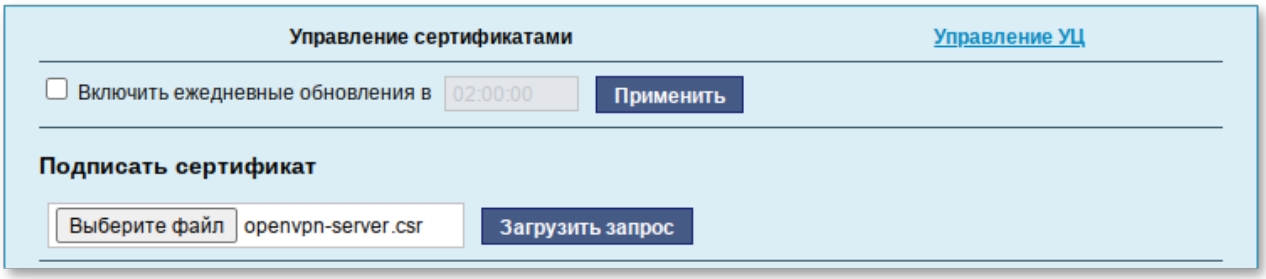


Если нажать на кнопку **`Забрать запрос на подпись`**, появится диалоговое окно с предложением сохранить файл **`openvpn-server.csr`**. Необходимо сохранить этот файл на диске.

В модуле **Управление ключами SSL** появился новый ключ *openvpn-server (Нет сертификата)*:



Чтобы подписать сертификат, необходимо перейти в модуль **Удостоверяющий Центр** → **Управление сертификатами**, нажать кнопку **Выберите файл**, указать путь до полученного файла **`openvpn-server.csr`** и загрузить запрос:



В результате на экране появится две группы цифр и кнопка **`Подписать`**. Необходимо нажать на кнопку **`Подписать`** и сохранить файл **`output.pem`** (подписанный сертификат).

```
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = openvpn-server, C = RU, L = Kaliningrad
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:cf:a0:bc:0c:6c:34:bd:b3:02:a8:c6:ab:75:05:
                    2f:d0:28:67:69:96:25:17:48:2d:cc:c6:68:9c:02:
                    ce:56:a2:ce:22:1b:02:66:4d:56:89:3b:49:b4:6e:
                    23:fe:97:6e:0a:09:bf:ce:8f:5b:5d:f9:71:a6:3d:
                    a6:45:95:5d:48:47:e6:6c:d0:b2:df:2e:8a:7d:41:
                    9a:4d
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
        Requested Extensions:
    Signature Algorithm: sha256WithRSAEncryption
         8a:ba:ef:f1:c8:c2:db:26:b3:c8:cb:c8:4f:d2:ba:57:13:49:
         ac:56:2d:f7:e2:7e:81:22:74:88:00:e0:c3:d1:d2:d8:7b:3a:
         61:0a:2f:37:68:31:4c:8c:d5:2d:da:2c:24:5f:e6:04:19:b3:
         a4:6a:8c:e5:69:5a:19:ff:97:0e:d5:2b:64:aa:e4:57:2f:f2:
         5c:9f:46:58:2a:61:de:4f:87:8c:7b:fe:81:20:98:f4:d9:ea:
         16:01:b5:3e
```

Подписать

Далее в разделе **Управление ключами SSL**, необходимо выделить ключ *openvpn-server (Нет сертификата)* и нажать кнопку **Изменить**. В появившемся окне, в пункте **Положить сертификат, подписанный УЦ** нужно нажать кнопку **Выберите файл**, указать путь до файла **output.pem** и нажать кнопку **Положить**:

Положить сертификат, подписанный УЦ: Выберите файл output.pem Положить

Сертификат успешно загружен

В модуле **Управление ключами SSL**, видно, что изменился ключ *openvpn-server (истекает_и_дата)*. Ключ создан и подписан.

Для того чтобы положить сертификат УЦ, необходимо найти его в модуле **Удостоверяющий Центр**, нажать на ссылку **Управление УЦ** и забрать сертификат, нажав на ссылку **Сертификат: ca-root.pem**:

Сертификат: ca-root.pem
Запрос на подпись: ca-root.csr

В модуле **OpenVPN-сервер**, в графе **Положить сертификат УЦ**: при помощи кнопки **Выберите файл** указать путь к файлу **ca-root.pem** и нажать кнопку **Положить**:

Положить сертификат УЦ: Выберите файл ca-root.pem Положить

Появится сообщение: «Сертификат УЦ успешно загружен».

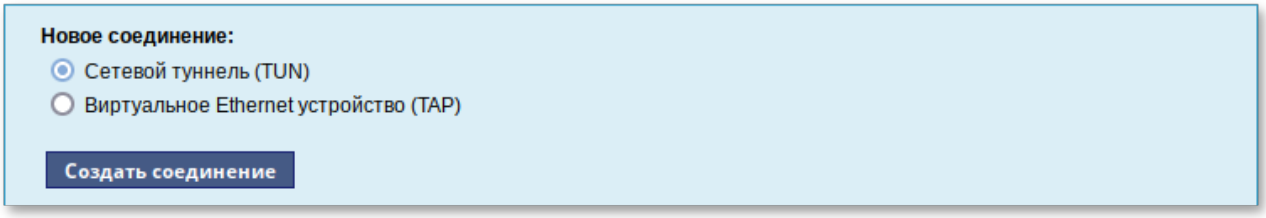
Для включения OpenVPN необходимо отметить пункт **Включить службу OpenVPN** и нажать кнопку **Применить**.

Если необходимо организовать защищённое соединение между двумя локальными сетями, воспользуйтесь модулем **OpenVPN-соединения** (раздел **Сеть**).

32.2. Настройка клиентов

Со стороны клиента соединение настраивается в модуле ЦУС **OpenVPN-соединения** (пакет *alterator-net-openvpn*) из раздела **Сеть**. Доступ к настроенной приватной сети могут получить пользователи, подписавшие свои ключи и получившие сертификат в удостоверяющем центре на том же сервере.

Для создания нового соединения необходимо отметить пункт **Сетевой туннель (TUN)** или **Виртуальное Ethernet устройство (TAP)** и нажать кнопку **Создать соединение**. Должен быть выбран тот же тип, что и на стороне сервера.



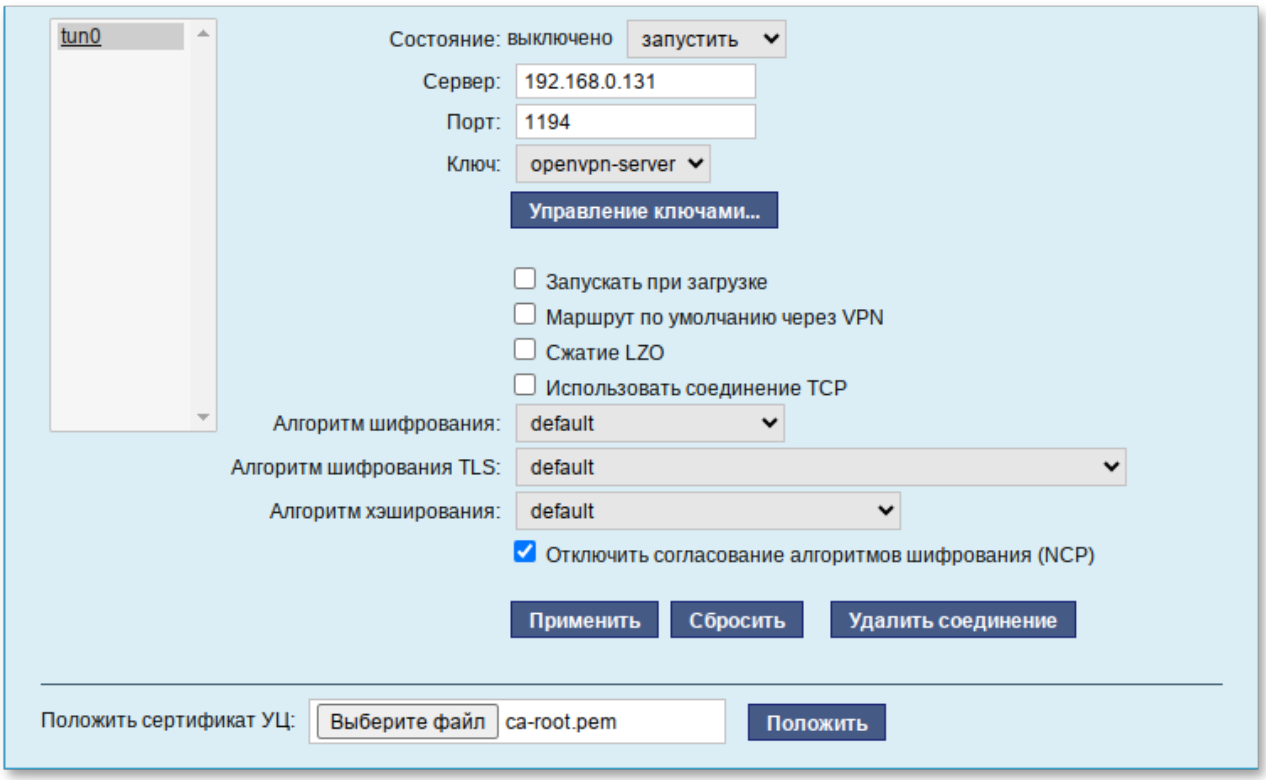
Обратите внимание, что на стороне клиента, должен быть выбран тот же тип виртуального устройства, что и на стороне сервера. Для большинства случаев подходит маршрутизируемое подключение.

Помимо этого нужно создать ключ (например, **openvpn**) в модуле **Управление ключами SSL** и подписать его в модуле Удостоверяющий центр на сервере.

В результате станут доступны настройки соединения. На клиенте в модуле OpenVPN-соединение необходимо указать:

- **Состояние** — «запустить»;
- **Сервер** — IP адрес сервера или домен;
- **Порт** — 1194;
- **Ключ** — выбрать подписанный на сервере ключ.

Для применения настроек, нажать кнопку **Применить**. Состояние с **Выключено** должно поменяться на **Включено**.



Проверить, появилось ли соединение с сервером можно, выполнив команду:

```
$ ip addr
```

должно появиться новое соединение tun0. При обычных настройках это может выглядеть так:

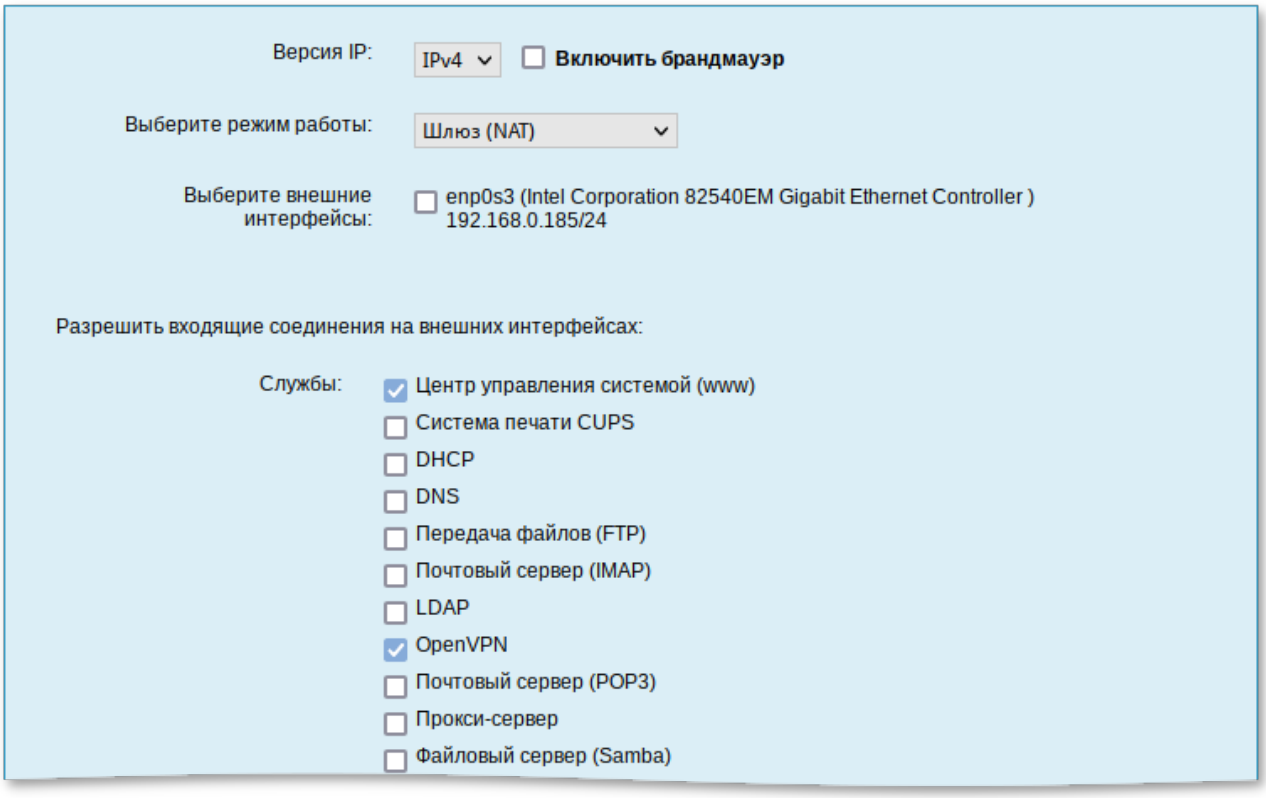
```
tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UNKNOWN group default qlen 500
   link/none
   inet 10.8.0.6 peer 10.8.0.5/32 scope global tun0
```

Глава 33. Доступ к службам сервера из сети Интернет

33.1. Внешние сети

Сервер предоставляет возможность организовать доступ к своим службам извне. Например, можно предоставить доступ к корпоративному веб-сайту из сети Интернет. Для обеспечения такой возможности необходимо разрешить входящие соединения на внешних интерфейсах. По умолчанию такие соединения блокируются.

Для разрешения внешних и внутренних входящих соединений предусмотрен раздел ЦУС **Брандмауэр**. В списке **Разрешить входящие соединения на внешних интерфейсах** модуля **Внешние сети** (пакет *alterator-net-iptables*) перечислены наиболее часто используемые службы, отметив которые, вы делаете их доступными для соединений на внешних сетевых интерфейсах. Если вы хотите предоставить доступ к службе, отсутствующей в списке, задайте используемые этой службой порты в соответствующих полях.



Можно выбрать один из двух режимов работы:

- Роутер. В этом режиме перенаправление пакетов между сетевыми интерфейсами происходит без трансляции сетевых адресов.
- Шлюз (NAT). В этом режиме будет настроена трансляция сетевых адресов (NAT) при перенаправлении пакетов на внешние интерфейсы. Использование этого режима имеет смысл, если у вас настроен, по крайней мере, один внешний и один внутренний интерфейс.

Примечание

В любом режиме включено только перенаправление пакетов с внутренних интерфейсов. Перенаправление пакетов с внешних интерфейсов всегда выключено.

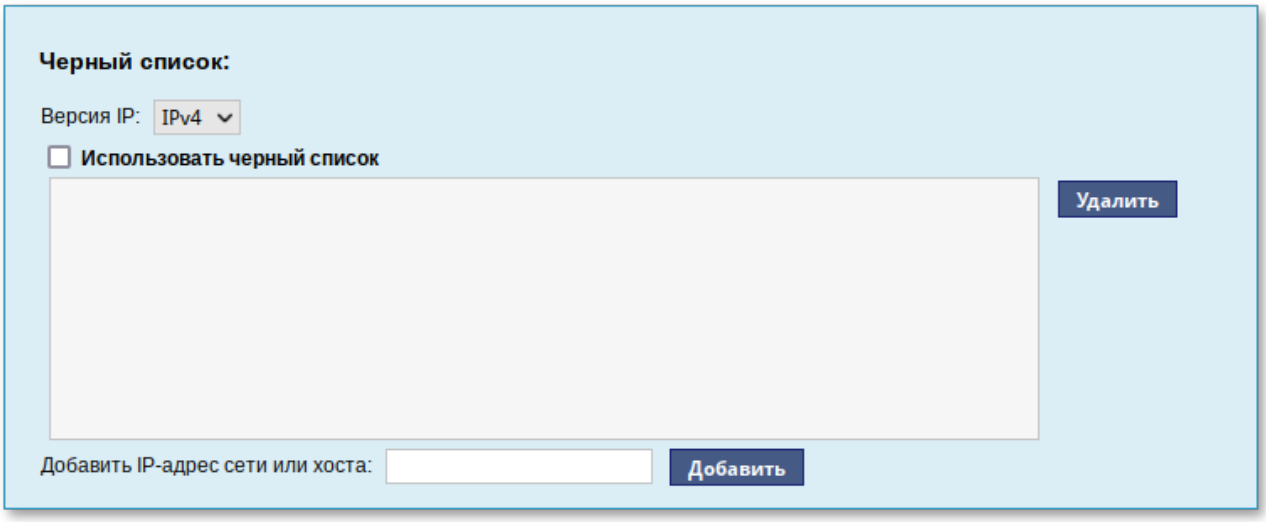
Примечание

Все внутренние интерфейсы открыты для любых входящих соединений.

33.2. Список блокируемых хостов

Модуль ЦУС **Список блокируемых хостов** (пакет *alterator-net-iptables*) предназначен для блокирования любого трафика с указанными узлами. Данный модуль позволяет блокировать любой сетевой трафик с указанных в списке узлов (входящий, исходящий и пересылаемый).

Блокирование трафика с указанных в списке узлов начинается после установки флажка **Использовать чёрный список**.



Для добавления блокируемого узла необходимо ввести IP-адрес в поле **Добавить IP-адрес сети или хоста** и нажать кнопку **Добавить**.

Для удаления узла из списка выберите его и нажмите кнопку **Удалить**.

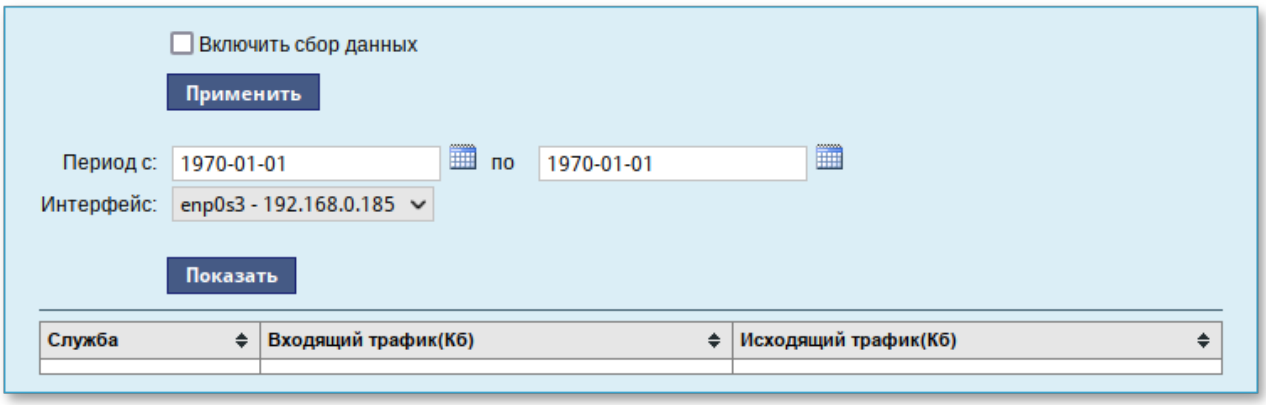
Глава 34. Статистика

34.1. Сетевой трафик

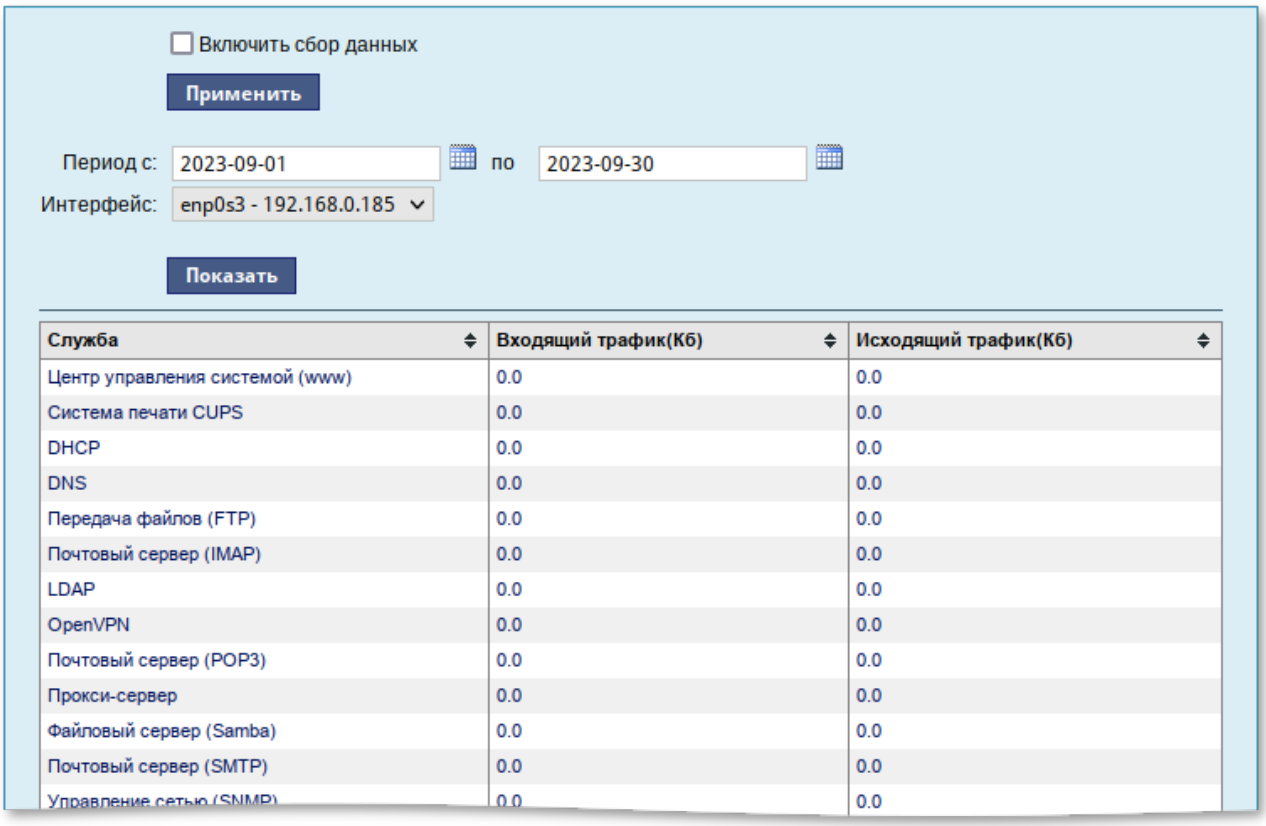
Все входящие и исходящие с сервера сетевые пакеты могут подсчитываться, и выводится по запросу для анализа.

Модуль **Сетевой трафик** (пакет *alterator-ulogd*) из раздела **Статистика** предназначен для просмотра статистики входящих и исходящих с сервера сетевых пакетов. Данный модуль позволяет оценить итоговый объём полученных и переданных данных за всё время работы сервера, за определённый период времени и по каждой службе отдельно.

Для включения сбора данных необходимо установить флажок **Включить сбор данных**, и нажать кнопку **Применить**.



Для просмотра статистики укажите период (в виде начальной и конечной дат). Дата указывается в формате YYYY-MM-DD (год-месяц-день) или выбирается из календаря справа от поля ввода даты. Из списка доступных сетевых интерфейсов необходимо выбрать интересующий и нажать на кнопку **Показать**.



Трафик на указанном интерфейсе за заданный период показывается в виде:

- служба (название протокола);
- входящий трафик в килобайтах;
- исходящий трафик в килобайтах.

Глава 35. Обслуживание сервера

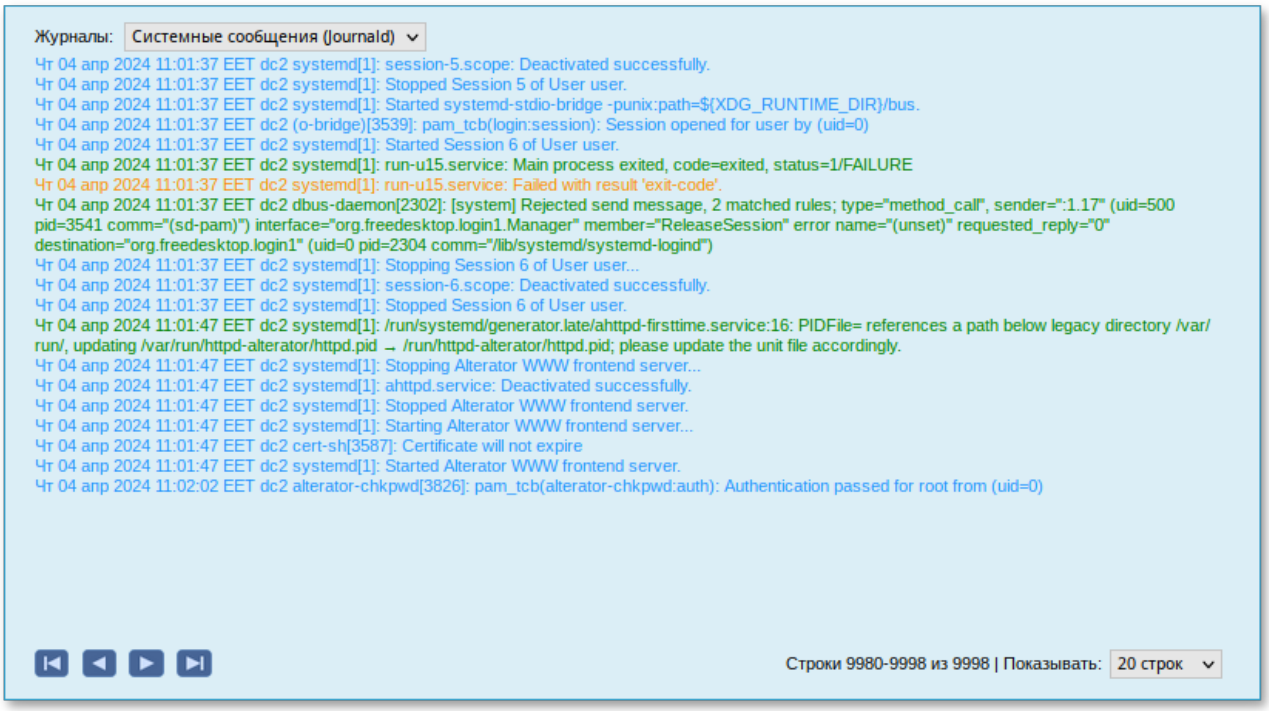
Для безотказной работы всего домена очень важно следить за корректной работой его центрального звена — сервера под управлением Альт Сервер для Эльбрус. Регулярный мониторинг состояния сервера, своевременное резервное копирование, обновление установленного ПО являются важной частью комплекса работ по обслуживанию сервера.

35.1. Мониторинг состояния системы

Для обеспечения бесперебойной работы сервера крайне важно производить постоянный мониторинг его состояния. Все события, происходящие с сервером, записываются в *журналы*, анализ которых помогает избежать сбоев в работе сервера и предоставляет возможность разобраться в причинах некорректной работы сервера.

Для просмотра журналов предназначен модуль ЦУС **Системные журналы** (пакет *alterator-logs*) из раздела **Система**). Интерфейс позволяет просмотреть различные типы журналов с возможностью перехода к более старым или более новым записям.

Различные журналы могут быть выбраны из списка **Журналы**.



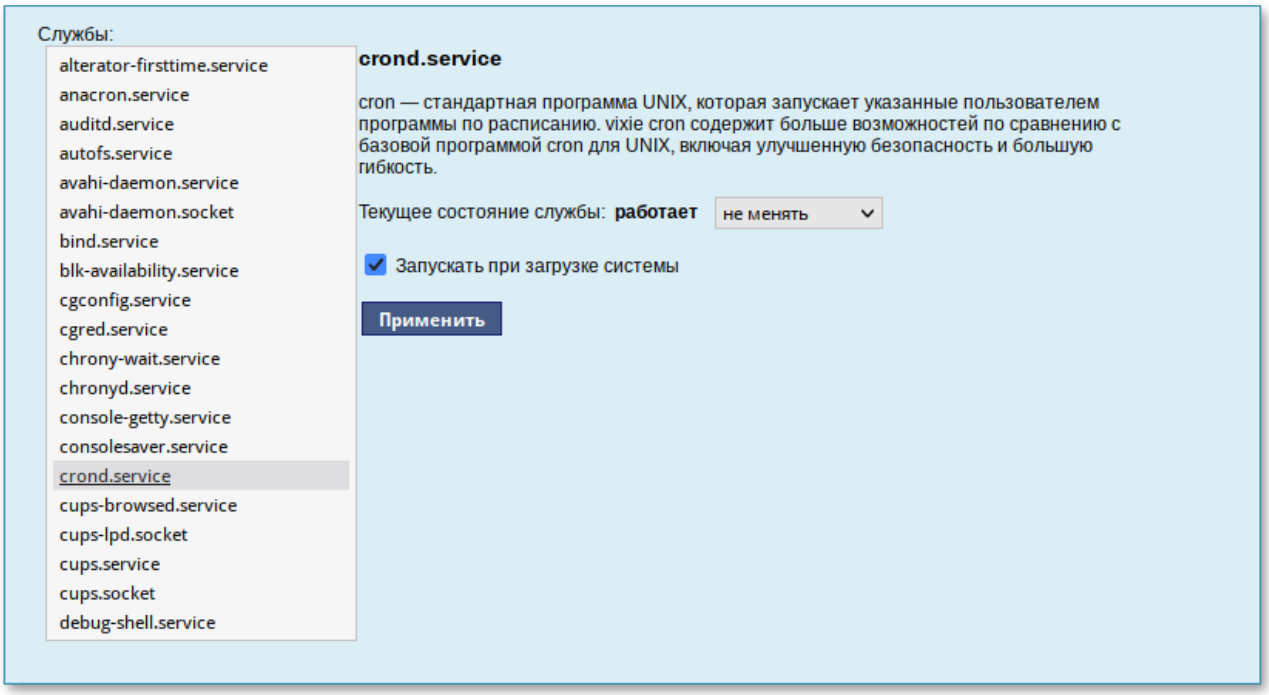
Доступны следующие виды журналов:

- **Брандмауэр** — отображаются события безопасности, связанные с работой межсетевого экрана ОС;
- **Системные сообщения (Journald)** — отображаются события процессов ядра и пользовательской области. У каждого сообщения в этом журнале есть приоритет, который используется для пометки важности сообщений. Сообщения в зависимости от уровня приоритета подсвечиваются цветом.

Каждый журнал может содержать довольно большое количество сообщений. Уменьшить либо увеличить количество выводимых строк можно, выбрав нужное значение в списке **Показывать**.

35.2. Системные службы

Для изменения состояния служб можно использовать модуль ЦУС **Системные службы** (пакет *alterator-services*) из раздела **Система**. Интерфейс позволяет изменять текущее состояние службы и, если необходимо, применить опцию запуска службы при загрузке системы.

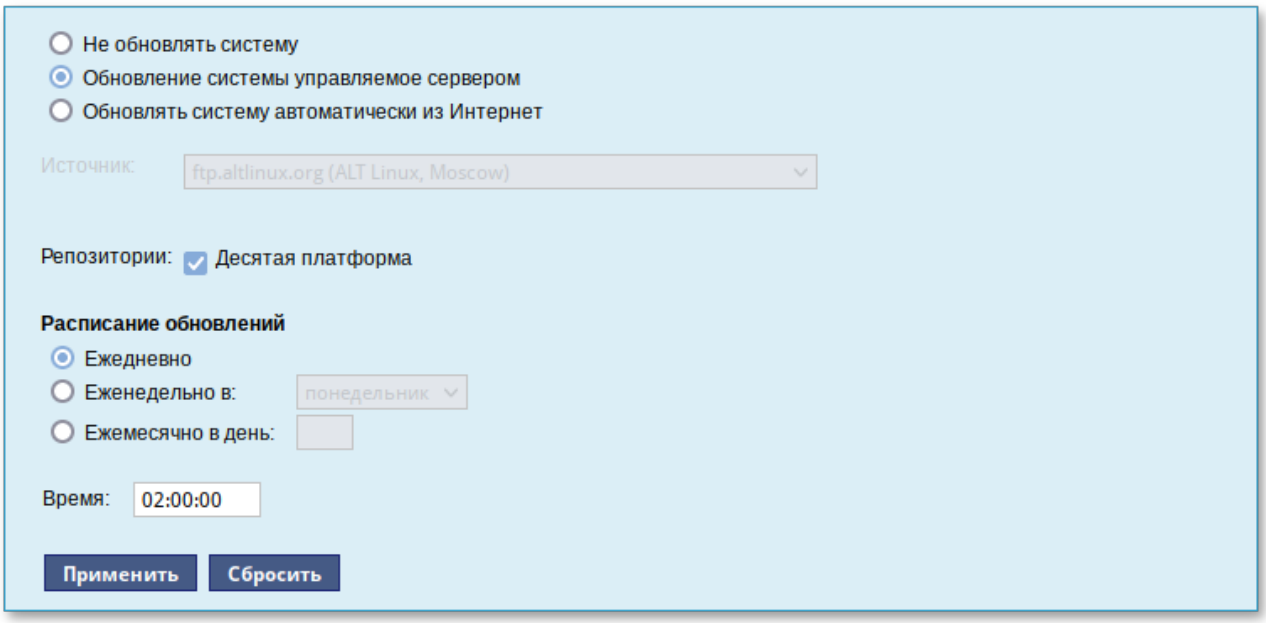


После выбора названия службы из списка отображается описание данной службы, а также текущее состояние: Работает/Остановлена/Неизвестно.

35.3. Обновление системы

После установки системы крайне важно следить за обновлениями ПО. Обновления для Альт Сервер для Эльбрус могут содержать как исправления, связанные с безопасностью, так и новый функционал или просто улучшение и ускорение алгоритмов. В любом случае настоятельно рекомендуется регулярно обновлять систему для повышения надёжности работы сервера.

Для автоматизации процесса установки обновлений предусмотрен модуль ЦУС **Обновление системы** (пакет *alterator-updates*) из раздела **Система**. Здесь можно включить автоматическое обновление через Интернет с одного из предлагаемых серверов или задать собственные настройки.



Источник обновлений указывается явно (при выбранном режиме **Обновлять систему автоматически из сети Интернет**) или вычисляется автоматически (при выбранном режиме **Обновление системы управляемое сервером** и наличии в локальной сети настроенного сервера обновлений).

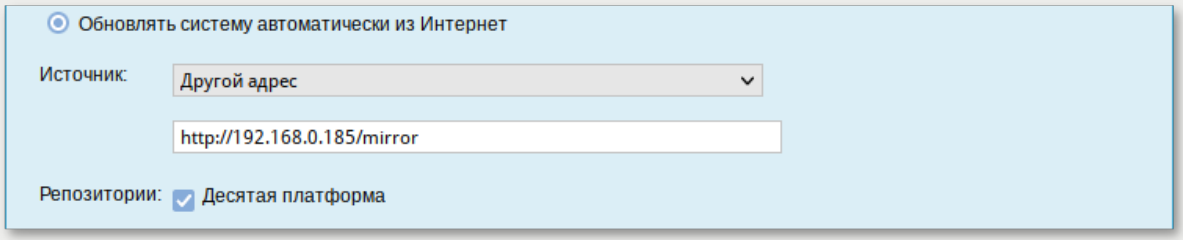
Примечание

Рабочие станции «видят» локальный сервер обновлений, при выборе режима **Обновление системы управляемое сервером**, если они находятся в домене (при этом сервер обновлений должен быть настроен на **Опубликовать как репозиторий для автоматических обновлений**).

Процесс обновления системы будет запускаться автоматически согласно заданному расписанию.

Примечание

Чтобы указать в качестве сервера обновлений локально настроенный источник, необходимо выбрать режим **Обновлять систему автоматически из Интернет**, выбрать в списке **Другой адрес** и указать адрес локального сервера обновлений, например, http://<ip сервера>/mirror:

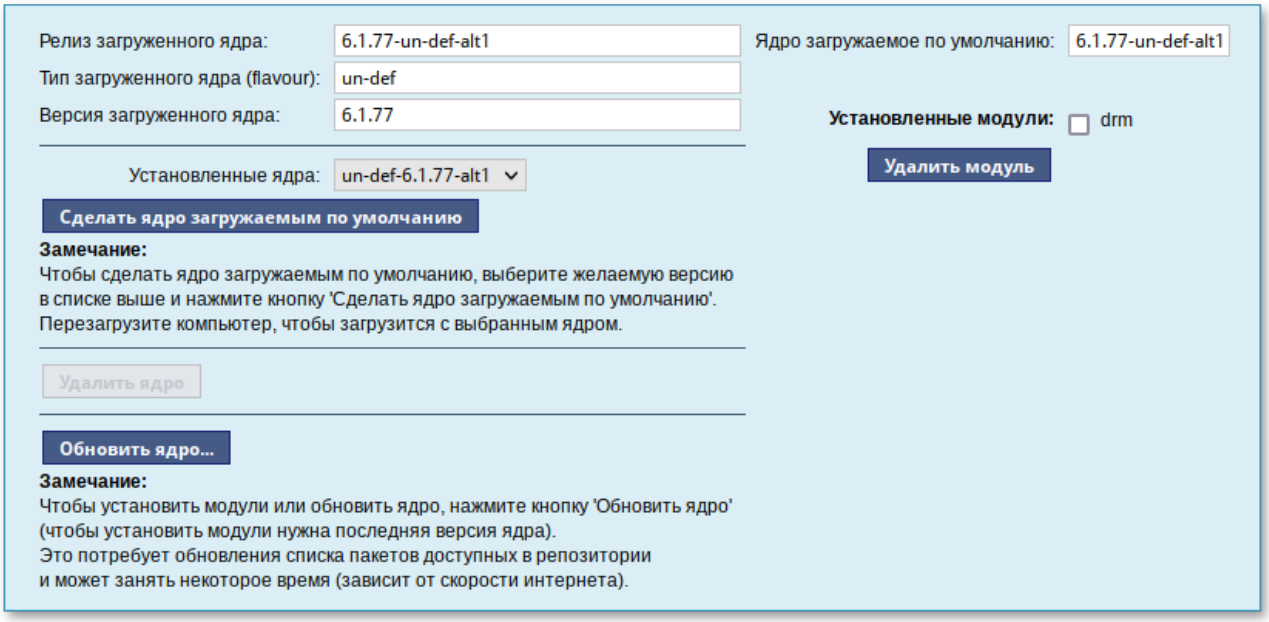


35.4. Обновление ядра ОС

Модуль ЦУС **Обновление ядра** (пакет *alterator-update-kernel*) из раздела **Система** реализует функционал утилиты **`update-kernel`**. Данный модуль предоставляет возможность:

- просматривать список установленных ядер;
- устанавливать, обновлять и удалять ядра;
- задавать ядро, загружаемое по умолчанию;
- устанавливать/удалять отдельные модули ядра.

В главном окне модуля отображается ядро, загруженное по умолчанию, и список установленных модулей ядра:



В дистрибутиве Альт Сервер для Эльбрус можно установить несколько версий ядра одного и того же типа одновременно. После установки или обновления ядра старые ядра не удаляются.

В случае возникновения проблем с новым ядром можно переключиться на установленное ранее. Для этого следует выбрать нужное ядро в списке **`Установленные ядра`** и нажать кнопку **`Сделать ядро загружаемым по умолчанию`**.

Накопленный при обновлениях набор ранее установленных ядер можно удалить для освобождения дискового пространства. Для этого следует выбрать нужное ядро в списке **`Установленные ядра`** и нажать кнопку **`Удалить ядро`**.

Для того чтобы обновить ядро или установить модули ядра, следует нажать кнопку **`Обновить ядро…`**.

Примечание

При нажатии кнопки **`Обновить ядро…`** локальная база данных пакетов будет синхронизирована с удалённым репозиторием, это может занять некоторое время.

Если в системе уже установлено последнее ядро, сообщение об этом появится в открывшемся окне, иначе в этом окне будет показано доступное к установке ядро.

Чтобы обновить ядро, необходимо нажать кнопку **`Обновить ядро`**. Далее следует подтвердить желание обновить ядро нажатием кнопки **`Да`**.

Примечание

Новое ядро загрузится только после перезагрузки системы.

Если с новым ядром что-то пойдёт не так, вы сможете вернуться к предыдущему варианту, выбрав его в начальном меню загрузчика.

Если ядро не требует обновления, в окне **`Доступные модули`** можно отметить модули ядра необходимые к установке и нажать кнопку **`Установить модули`**.

35.5. Обновление систем, не имеющих выхода в Интернет

Для систем, не имеющих прямого выхода в Интернет, рекомендуется установка отдельного сервера обновлений на базе ОС Альт Сервер для Эльбрус, находящегося вне защищенного контура и организация ограниченного доступа к этому серверу.

Модуль ЦУС **Сервер обновлений** (пакет *alterator-mirror*) из раздела **Серверы** предназначен для зеркалирования репозиториев и публикации их для обновлений рабочих станций и серверов.

Сервер обновлений — технология, позволяющая настроить автоматическое обновление программного обеспечения, установленного на клиентских машинах (рабочих местах), работающих под управлением Альт Рабочая станция.

Репозиторий	Источник	Архитектуры	Локальное зеркало	Опубликовано
Стабильная ветка ALT Linux 5.1			☐	☐
Репозиторий обновлений для Альт 8 СП			☐	☐
Десятая платформа	ftp.altlinux.org	x86_64	■ (31 Гб)	☐
Пятая платформа			☐	☐
Шестая платформа			☐	☐
Седьмая платформа			☐	☐
Восьмая платформа			☐	☐
Девятая платформа			☐	☐
Девятая платформа (mipsel)			☐	☐
ALT Linux Sisyphus			☐	☐
ALT Linux Sisyphus (mipsel)			☐	☐
ALT Linux Sisyphus (riscv64)			☐	☐
Публичный бранч TEAM t6			☐	☐
Публичный бранч TEAM t7			☐	☐

Свободное место: 64 Гб

Предупреждение: зеркалирование потребует наличия большого количества места на диске.

- ○ Отключить зеркалирование
- ◉ Зеркалировать ежедневно
- ○ Зеркалировать еженедельно в: понедельник
- ○ Зеркалировать ежемесячно в день: 1

Время: 09:45

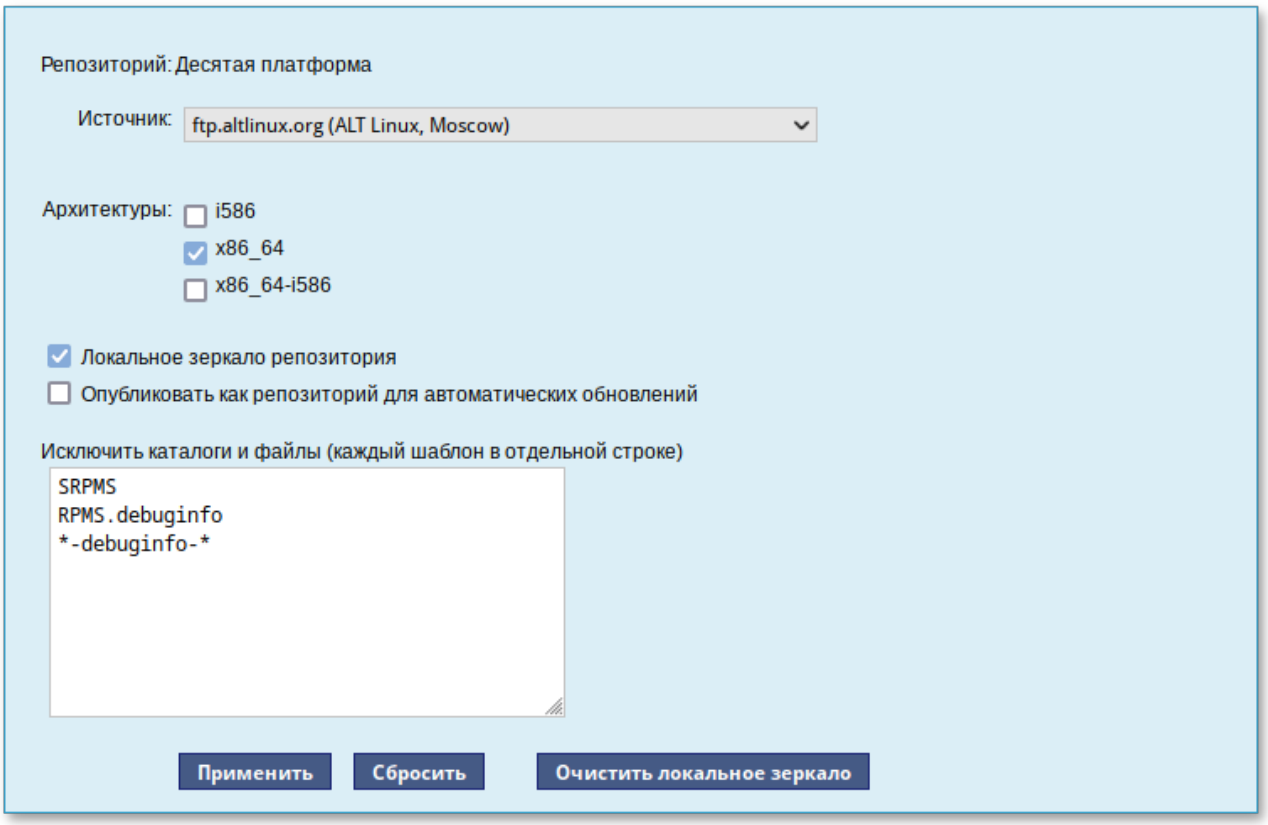
Применить Сбросить

На странице модуля можно выбрать, как часто выполнять закачку пакетов, можно выставить время, когда начинать зеркалирование.

Здесь также можно выбрать репозитории, локальные срезы которых необходимы. При нажатии на название репозитория, появляются настройки этого репозитория. Необходимо выбрать источник (сайт, откуда будет скачиваться репозиторий), архитектуру процессора (если их несколько, то стоит выбрать соответствующие).

Примечание

При выборе любой архитектуры также будет добавлен источник с noarch.



Сервер обновлений предоставляет возможность автоматически настроить обновление клиентских машин в нужном режиме:

Локальное зеркало репозитория

В этом режиме на сервере создаётся копия удалённого репозитория. Загрузка ПО клиентскими машинами может производится с локального сервера по протоколам HTTP, HTTPS, FTP, rsync (для каждого протокола нужно настроить соответствующие службы, ниже приведён пример настройки HTTP- и FTP-сервера). Наличие на локальном сервере зеркала репозитория при большом количестве машин в сети позволяет существенно сэкономить трафик.

Важно

Зеркалирование потребует наличия большого количества места на диске.

Уменьшить размер скачиваемых файлов и занимаемое репозиторием место на диске можно, указав имена каталогов и файлов, которые будут исключены из синхронизации. Например, не скачивать пакеты с исходным кодом и пакеты с отладочной информацией:

```
SRPMS
*-debuginfo-*
```

Шаблоны указываются по одному в отдельной строке. Символ «*» используется для подстановки любого количества символов.

Публикация репозитория

В этом случае публикуется или URL внешнего сервера, содержащего репозиторий или, если включено локальное зеркало репозитория, адрес этого сервера. Такая публикация позволяет клиентским машинам автоматически настроить свои менеджеры пакетов на использование внешнего или локального репозитория.

Со стороны клиентских машин, в этом случае, необходимо настроить модуль **Обновление системы**, отметив в нём **Обновление системы управляемое сервером**.

Настройка локального репозитория заканчивается нажатием на кнопку **Применить**.

Примечание

По умолчанию локальное зеркало репозитория находится в **/srv/public/mirror**. Для того чтобы зеркалирование происходило в другую папку, необходимо эту папку примонтировать в папку **/srv/public/mirror**. Для этого в файл **/etc/fstab** следует вписать строку:

```
/media/disk/localrepo /srv/public/mirror none rw,bind,auto 0 0
```

где **/media/disk/localrepo** — папка-хранилище локального репозитория.

Примечание

Если в каталогах **/srv/public/mirror/<репозиторий>/branch/<архитектура>/base/**. нет файлов **pkglist.*** значит зеркалирование не закончено (т.е. не все файлы загружены на ваш сервер).

35.5.1. Настройка веб-сервера

Установить веб-сервер (в данном примере nginx):

```
# apt-get install nginx
```

Создать файл конфигурации сервера в **/etc/nginx/sites-available.d/repo.conf**:

```
server {
  listen 80;
  server_name localhost .local <ваш ip>;

  access_log /var/log/nginx/repo-access.log;
  error_log /var/log/nginx/repo-error.log;

  location /mirror {
    root /srv/public;
    autoindex on;
   }
}
```

Сделать ссылку в **/etc/nginx/sites-enabled.d/**:

```
# ln -s /etc/nginx/sites-available.d/repo.conf /etc/nginx/sites-enabled.d/
repo.conf
```

Запустить nginx и добавить его в автозагрузку:

```
# systemctl enable --now nginx
```

На клиентских машинах необходимо настроить репозитории. Сделать это можно в программе управления пакетами **Synaptic** (**Параметры** → **Репозитории**) или в командной строке:

```
# apt-repo rm all
# apt-repo add http://<ip сервера>/mirror/p10/branch
```

Проверить правильность настройки репозиториев:

```
# apt-repo
rpm http://192.168.0.185/mirror p10/branch/x86_64 classic
rpm http://192.168.0.185/mirror p10/branch/noarch classic
```

35.5.2. Настройка FTP-сервера

Установить пакеты *vsftpd*, *lftp*, если они еще не установлены:

```
# apt-get install vsftpd lftp
```

Настроить параметры использования vsftpd в файле **/etc/xinetd.d/vsftpd**:

```
# default: off
# description: The vsftpd FTP server.
service ftp
{
    disable = no # включает службу
    socket_type = stream
    protocol = tcp
    wait = no
    user = root
    nice = 10
    rlimit_as = 200M
    server = /usr/sbin/vsftpd
    only_from = 0.0.0.0 # предоставить доступ для всех IP
}
```

Перезапустить xinetd:

```
# systemctl restart xinetd
```

Изменить настройку прав доступа в файле **/etc/vsftpd/conf**:

```
local_enable=YES
```

Создать каталог **/var/ftp/mirror**:

```
# mkdir -p /var/ftp/mirror
```

Примонтировать каталог **/srv/public/mirror** в **/var/ftp/mirror** с опцией **--bind**:

```
# mount --bind /srv/public/mirror /var/ftp/mirror
```

Примечание

Для автоматического монтирования каталога **/srv/public/mirror** при загрузке системы необходимо добавить следующую строку в файл **/etc/fstab**:

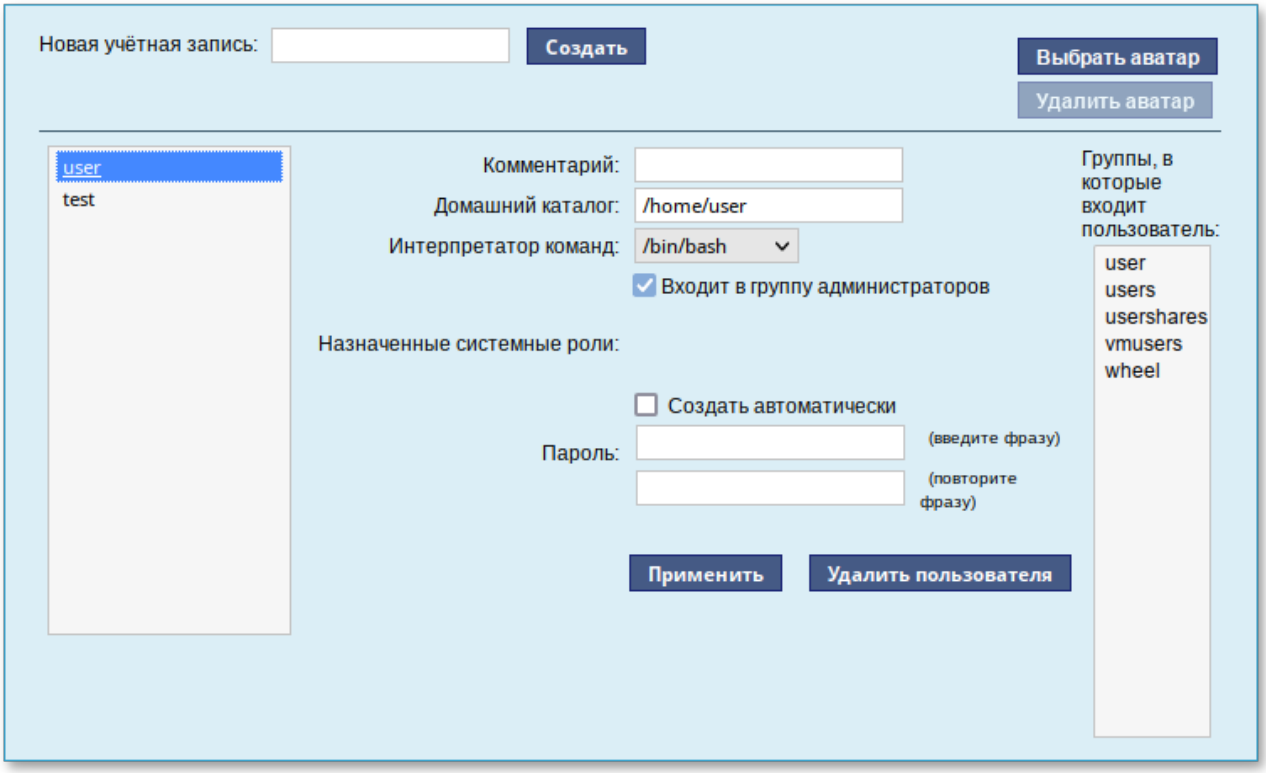
```
/srv/public/mirror /var/ftp/mirror none defaults,bind 0 0
```

На клиентских машинах необходимо настроить репозитории:

```
# apt-repo rm all
# apt-repo add ftp://<ip сервера>/mirror/p10/branch
# apt-repo
rpm ftp://192.168.0.185/mirror p10/branch/x86_64 classic
rpm ftp://192.168.0.185/mirror p10/branch/noarch classic
```

35.6. Локальные учётные записи

Модуль **Локальные учётные записи** (пакет *alterator-users*) из раздела **Пользователи** предназначен для администрирования системных пользователей.



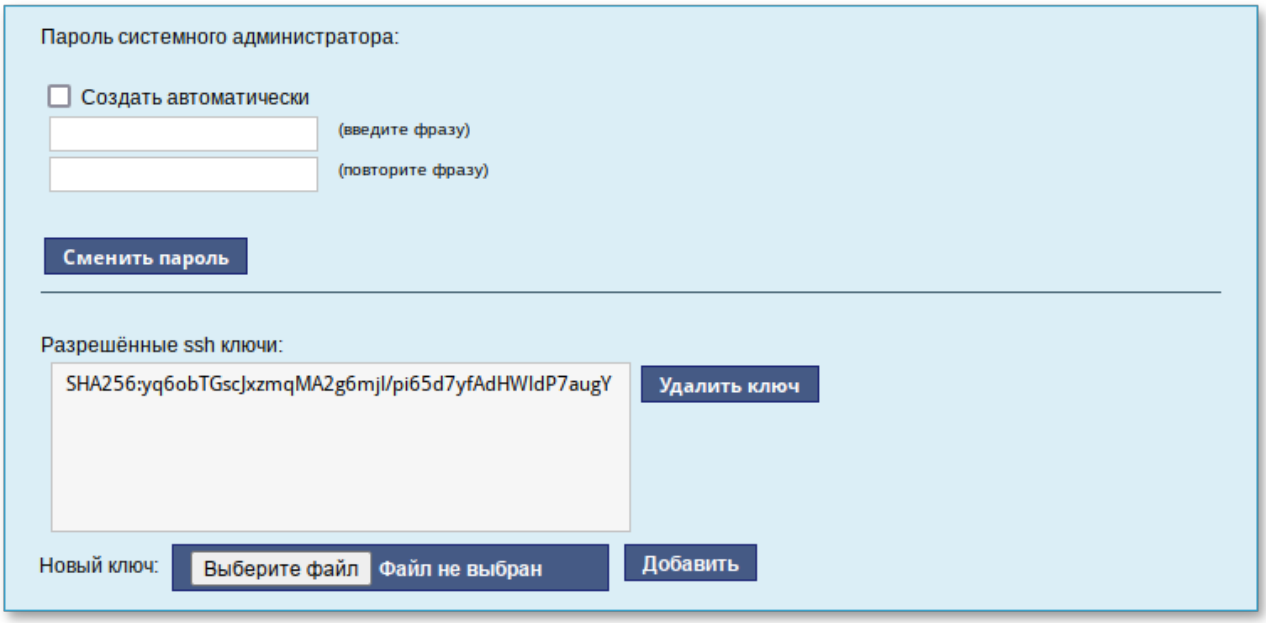
Для создания новой учётной записи необходимо ввести имя новой учётной записи и нажать кнопку **Создать**, после чего имя отобразится в списке слева.

Для дополнительных настроек необходимо выделить добавленное имя, либо, если необходимо изменить существующую учётную запись, выбрать её из списка.

35.7. Администратор системы

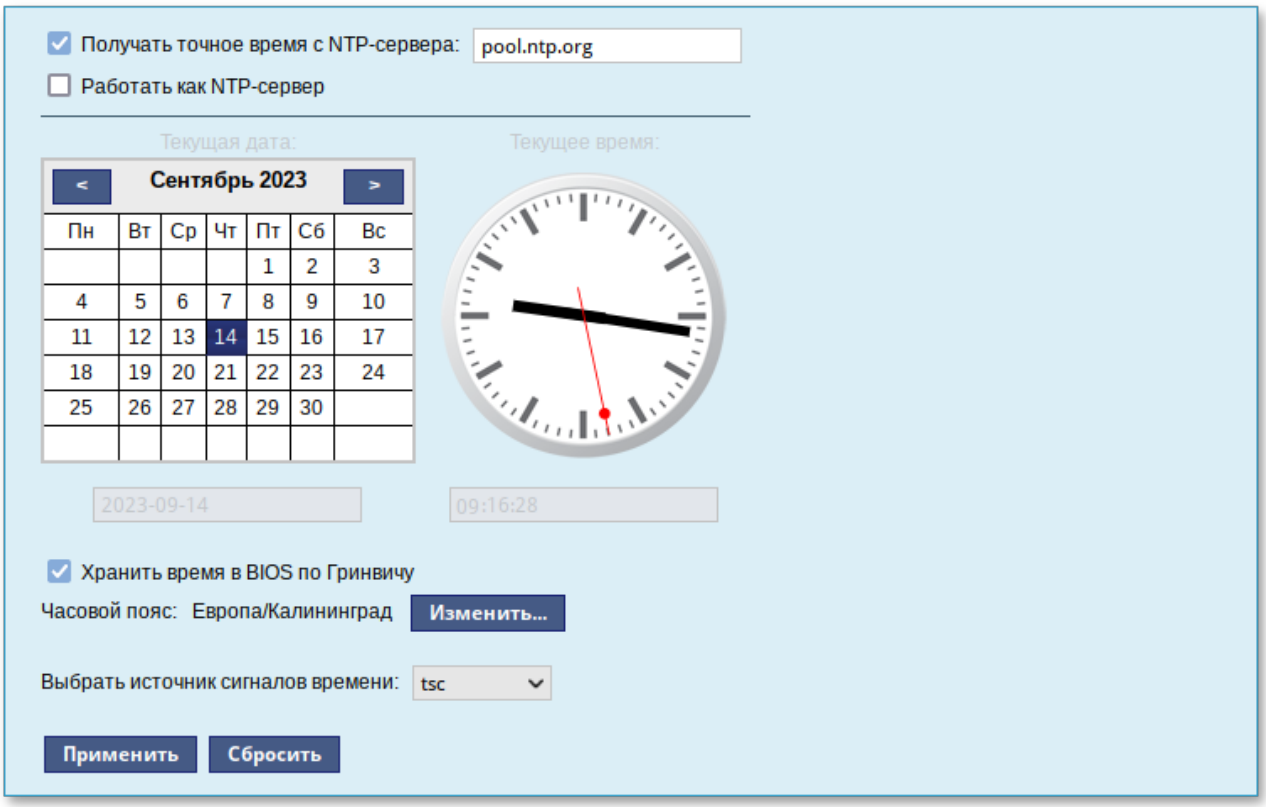
В модуле **Администратор системы** (пакет *alterator-root*) из раздела **Пользователи** можно изменить пароль суперпользователя (root), заданный при начальной настройке системы.

В данном модуле (только в веб-интерфейсе) можно добавить публичную часть ключа RSA или DSA для доступа к серверу по протоколу SSH.



35.8. Дата и время

В модуле **Дата и время** (пакет *alterator-datetime*) из раздела **Система** можно изменить дату и время на сервере, сменить часовой пояс, а также настроить автоматическую синхронизацию часов на самом сервере по протоколу NTP и предоставление точного времени по этому протоколу для рабочих станций локальной сети.



Системное время зависит от следующих факторов:

- часы в BIOS — часы, встроенные в компьютер. Они работают, даже если он выключен;
- системное время — часы в ядре операционной системы. Во время работы системы все процессы пользуются именно этими часами;
- часовые пояса — регионы Земли, в каждом из которых принято единое местное время.

При запуске системы происходит активация системных часов и их синхронизация с аппаратными, кроме того, в определённых случаях учитывается значение часового пояса. При завершении работы системы происходит обратный процесс.

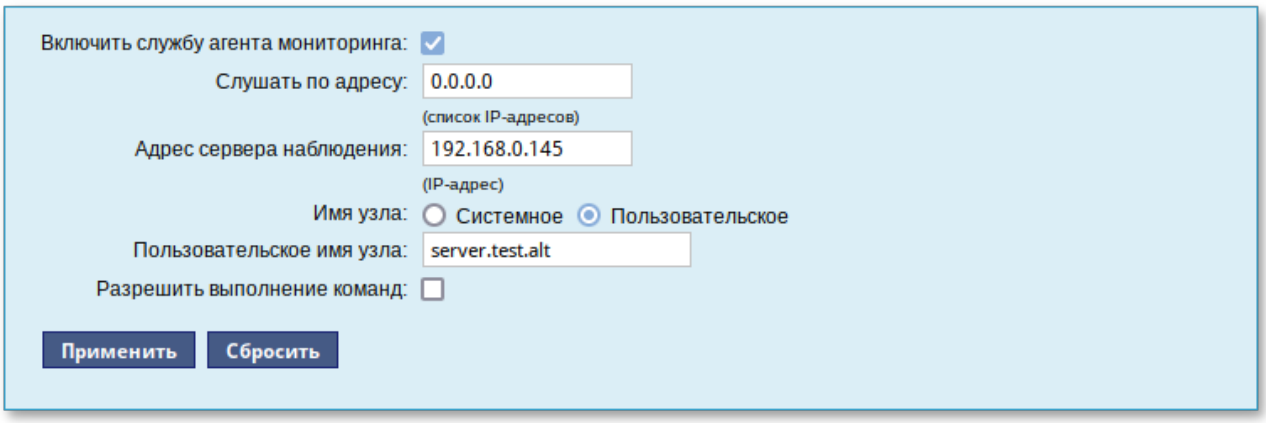
Если настроена синхронизация времени с NTP-сервером, то сервер сможет сам работать как сервер точного времени. Для этого достаточно отметить соответствующий пункт **`Работать как NTP-сервер`**.

Примечание

Выбор источника сигналов времени (источника тактовой частоты) доступен в режиме эксперта.

35.9. Агент наблюдения

Модуль **Агент наблюдения** (пакет *alterator-zabbix-agent*) из раздела **Система** позволяет настроить клиентскую часть системы мониторинга Zabbix.



На странице модуля можно задать следующие параметры:

- **Слушать по адресу** — IP-адрес, который агент должен прослушивать;
- **Адрес сервера наблюдения** — адрес сервера Zabbix, которому разрешено обращаться к агенту;
- **Имя узла** — при выборе пункта **Системное**, узел будет добавлен на сервер Zabbix под системным именем, при выборе пункта **Пользовательское**, имя узла можно указать в поле **Пользовательское имя узла**;
- **Пользовательское имя узла** — имя узла мониторинга, которое будет указано на сервере Zabbix.

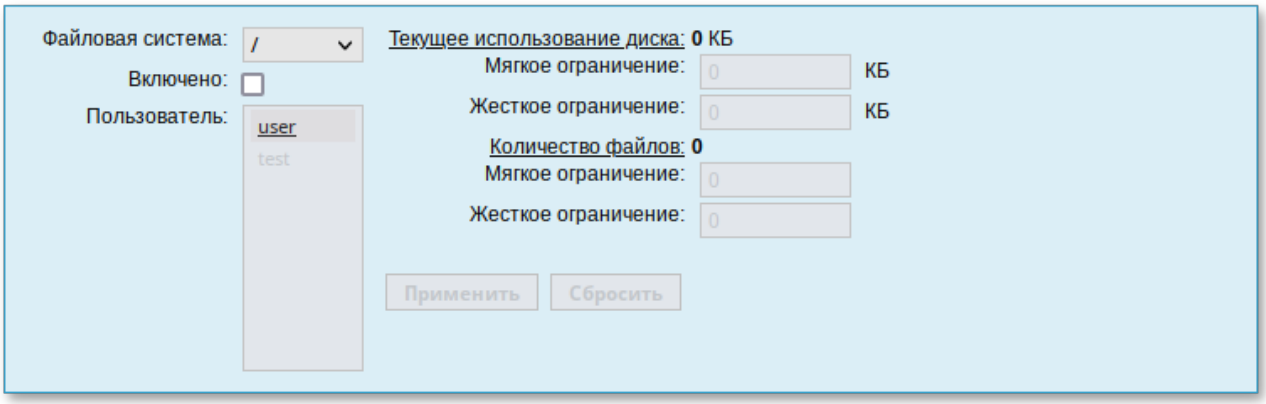
Примечание

Параметр **Разрешить выполнение команд** использовать не рекомендуется.

Чтобы применить настройки и запустить Zabbix-агент, следует отметить пункт **Включить службу агента мониторинга** и нажать кнопку **Применить**.

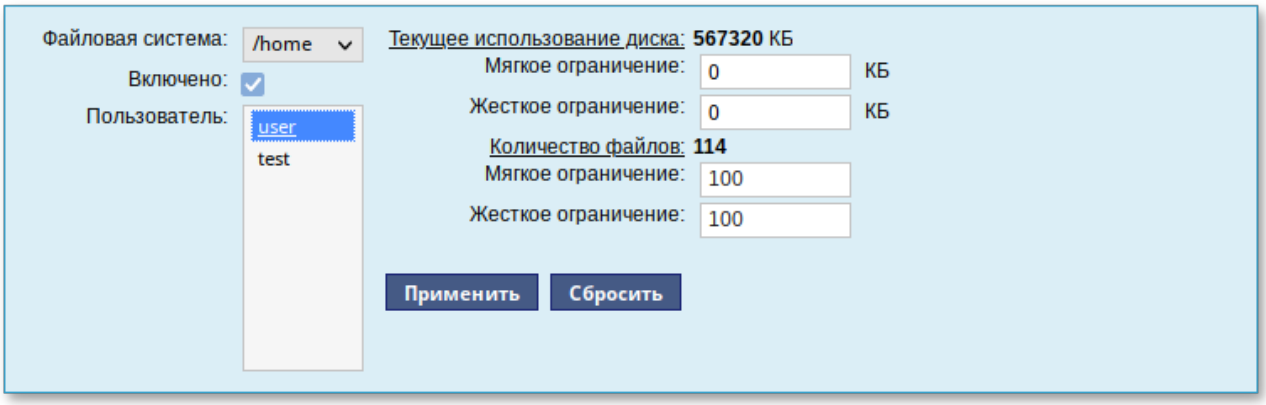
35.10. Ограничение использования диска

Модуль **Использование диска** (пакет *alterator-quota*) в разделе **Пользователи** позволяет ограничить использование дискового пространства пользователями, заведёнными на сервере в модуле **Пользователи**.



Модуль позволяет задать ограничения (квоты) для пользователя при использовании определённого раздела диска. Ограничить можно как суммарное количество килобайт, занятых файлами пользователя, так и количество этих файлов.

Для управления квотами файловая система должна быть подключена с параметрами ***usrquota***, ***grpquota***. Для этого следует выбрать нужный раздел в списке **Файловая система** и установить отметку в поле **Включено**:



Для того чтобы задать ограничения для пользователя, необходимо выбрать пользователя в списке **Пользователь**, установить ограничения и нажать кнопку **Применить**.

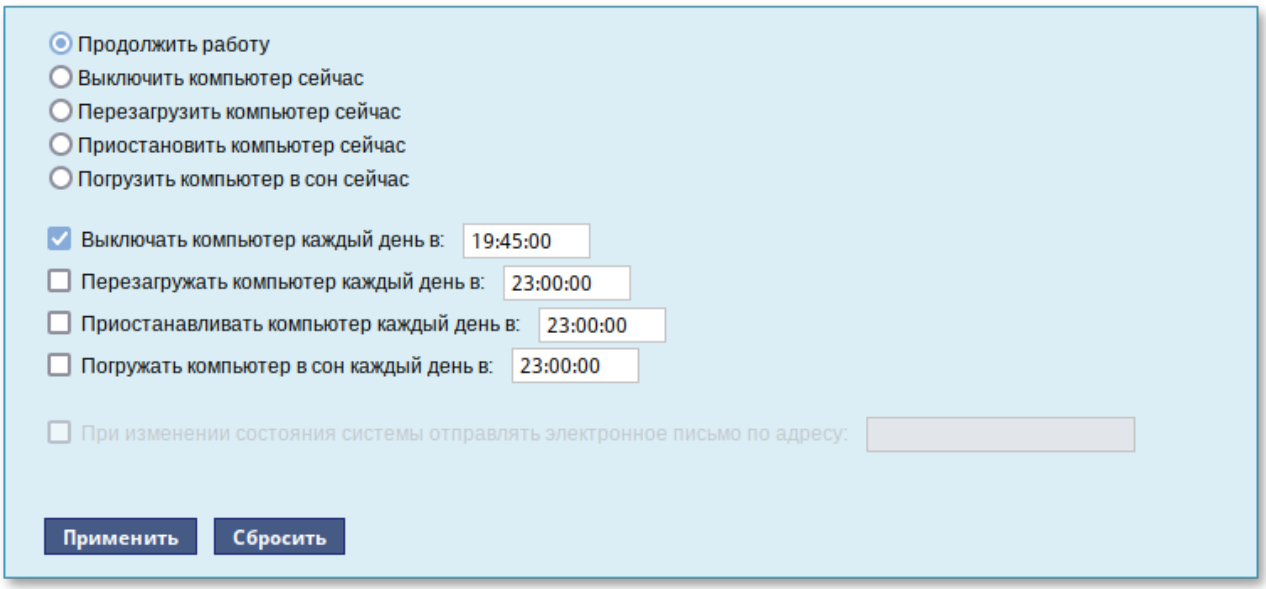
При задании ограничений различают жёсткие и мягкие ограничения:

- **Мягкое ограничение:** нижняя граница ограничения, которая может быть временно превышена. Временное ограничение — одна неделя.
- **Жёсткое ограничение:** использование диска, которое не может быть превышено ни при каких условиях.

Значение 0 при задании ограничений означает отсутствие ограничений.

35.11. Выключение и перезагрузка компьютера

Иногда, в целях обслуживания или по организационным причинам необходимо корректно выключить или перезагрузить сервер. Для этого можно воспользоваться модулем ЦУС **Выключение компьютера** в разделе **Система**.



Модуль **Выключение компьютера** позволяет:

- выключить компьютер;
- перезагрузить компьютер;
- приостановить работу компьютера;
- погрузить компьютер в сон.

Возможна настройка ежедневного применения данных действий в заданное время.

Так как выключение и перезагрузка — критичные для функционирования компьютера операции, то по умолчанию настройка выставлена в значение **Продолжить работу**. Для выключения, перезагрузки или перехода в энергосберегающие режимы нужно отметить соответствующий пункт и нажать **Применить**.

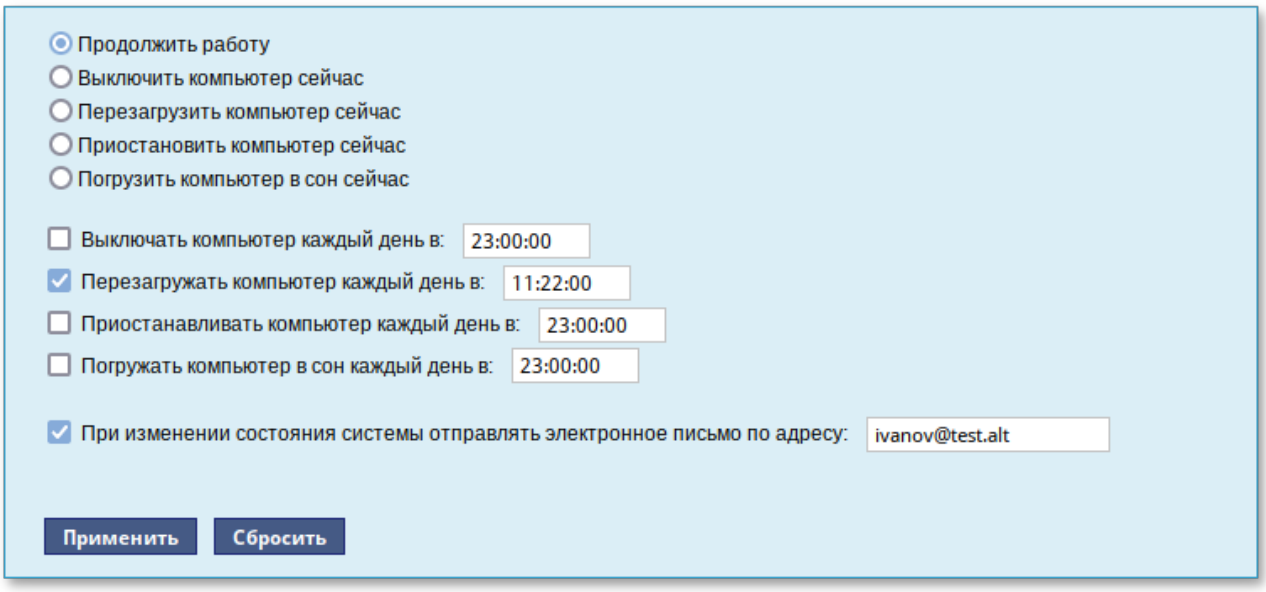
Для ежедневного автоматического выключения компьютера, перезагрузки, а также перехода в энергосберегающие режимы необходимо отметить соответствующий пункт и задать желаемое время. Например, для выключения компьютера следует отметить пункт **Выключать компьютер каждый день в**, задать время выключения в поле ввода слева от этого флажка и нажать кнопку **Применить**.

Примечание

Для возможности настройки оповещений на e-mail, должен быть установлен пакет *state-change-notify-postfix*:

```
# apt-get install state-change-notify-postfix
```

Для настройки оповещений необходимо отметить пункт **При изменении состояния системы отправлять электронное письмо по адресу**, ввести e-mail адрес и нажать кнопку **Применить**:



По указанному адресу, при изменении состоянии системы будут приходить электронные письма. Например, при включении компьютера, содержание письма будет следующее:

```
Thu Sep 14 11:46:59 EET 2023: The server.test.alt is about to start.
```

При выключении:

```
Thu Sep 14 12:27:02 EET 2023: The server.test.alt is about to shutdown.
```

Кнопка **`Сбросить`** возвращает сделанный выбор к безопасному значению по умолчанию: **`Продолжить работу`**, перечитывает расписания и выставляет отметки для ежедневного автоматического действия в соответствие с прочитанным.

Глава 36. Прочие возможности ЦУС

Возможности Альт Сервер для Эльбрус не ограничиваются только теми, что были описаны выше. Вы всегда можете поискать другие модули, предоставляющие прочие возможности для настройки системы в веб-интерфейсе.

Установленные пакеты, которые относятся к ЦУС, можно посмотреть, выполнив команду:

```
rpm -qa | grep alterator*
```

Прочие пакеты для ЦУС можно найти, выполнив команду:

```
apt-cache search alterator*
```

Модули можно дополнительно загружать и удалять как обычные программы:

```
# apt-get install alterator-net-openvpn
# apt-get remove alterator-net-openvpn
```

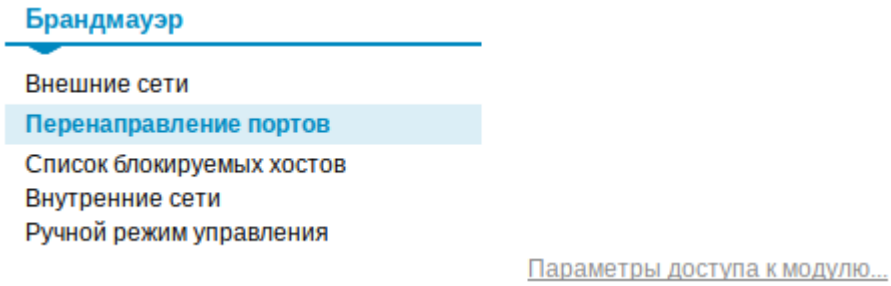
После установки модуля, у которого есть веб-интерфейс, для того чтобы он отобразился в веб-интерфейсе, необходимо перезапустить службу ahttpd:

```
# systemctl restart ahttpd
```

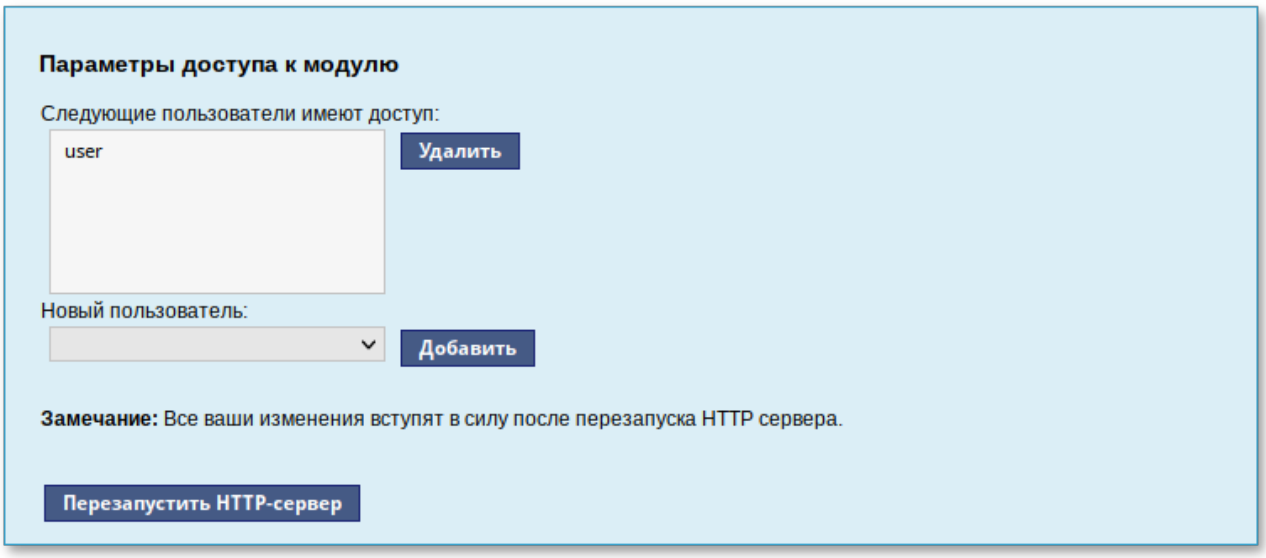
Глава 37. Права доступа к модулям

Администратор системы (root) имеет доступ ко всем модулям, установленным в системе, и может назначать права доступа для пользователей к определенным модулям.

Для разрешения доступа пользователю к конкретному модулю, администратору в веб-интерфейсе ЦУС необходимо выбрать нужный модуль и нажать ссылку **Параметры доступа к модулю**, расположенную в нижней части окна модуля:



В открывшемся окне, в списке **Новый пользователь** необходимо выбрать пользователя, который получит доступ к данному модулю, и нажать кнопку **Добавить**.



Для сохранения настроек необходимо перезапустить HTTP-сервер, для этого достаточно нажать кнопку **Перезапустить HTTP-сервер**.

Для удаления доступа пользователя к определенному модулю, администратору, в окне этого модуля необходимо нажать ссылку **Параметры доступа к модулю**, в открывшемся окне в списке пользователей которым разрешен доступ, должен выбрать пользователя, нажать кнопку **Удалить** и перезапустить HTTP-сервер.

Системный пользователь, пройдя процедуру аутентификации, может просматривать и вызывать модули, к которым он имеет доступ.

Часть VIII. Корпоративная инфраструктура

Содержание

Глава 38. Samba 4 в роли контроллера домена Active Directory

Использование Samba 4 в роли контроллера домена Active Directory позволяет вводить Windows 7/8 в домен без манипуляций с реестром.

Поддерживаются следующие базовые возможности Active Directory:

- аутентификация рабочих станций Windows и Linux и служб;
- авторизация и предоставление ресурсов;
- групповые политики (GPO);
- перемещаемые профили (Roaming Profiles);
- поддержка инструментов Microsoft для управления серверами (Remote Server Administration Tools) с компьютеров под управлением Windows;

- поддержка протоколов SMB2 и SMB3 (в том числе с поддержкой шифрования).

Предупреждение

Samba AD DC конфликтует с OpenLDAP и MIT Kerberos, поскольку эти приложения запускают одни и те же службы на одних тех же, по умолчанию, портах для протоколов LDAP и Kerberos.

Предупреждение

Samba AD DC функционирует на уровне контроллера доменов Windows 2008 R2 . Можно ввести его в домен Windows 2012 как клиента, но не как контроллер домена.

38.1. Установка

Для установки Samba AD DC выполняются следующие шаги:

- Установить пакет *task-samba-dc*, который установит все необходимое:

```
# apt-get install task-samba-dc
```

- Так как Samba в режиме контроллера домена (Domain Controller, DC) использует как свой LDAP, так и свой сервер Kerberos, несовместимый с MIT Kerberos, перед установкой необходимо остановить конфликтующие службы **krb5kdc** и **slapd**, а также **bind**:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl disable $service;
systemctl stop $service; done
```

38.2. Создание нового домена

38.2.1. Восстановление к начальному состоянию Samba

Необходимо очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

Предупреждение

Обязательно удаляйте **`/etc/samba/smb.conf`** перед созданием домена: **`rm -f /etc/samba/smb.conf`**

38.2.2. Выбор имени домена

Имя домена, для разворачиваемого DC, должно состоять минимум из двух компонентов, разделённых точкой. При этом должно быть установлено правильное имя узла и домена для сервера:

- HOSTNAME=dc1.test.alt в **/etc/sysconfig/network**
- ```
  # hostnamectl set-hostname dc1.test.alt
  ```
- ```
  # domainname test.alt
  ```

Примечание

После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

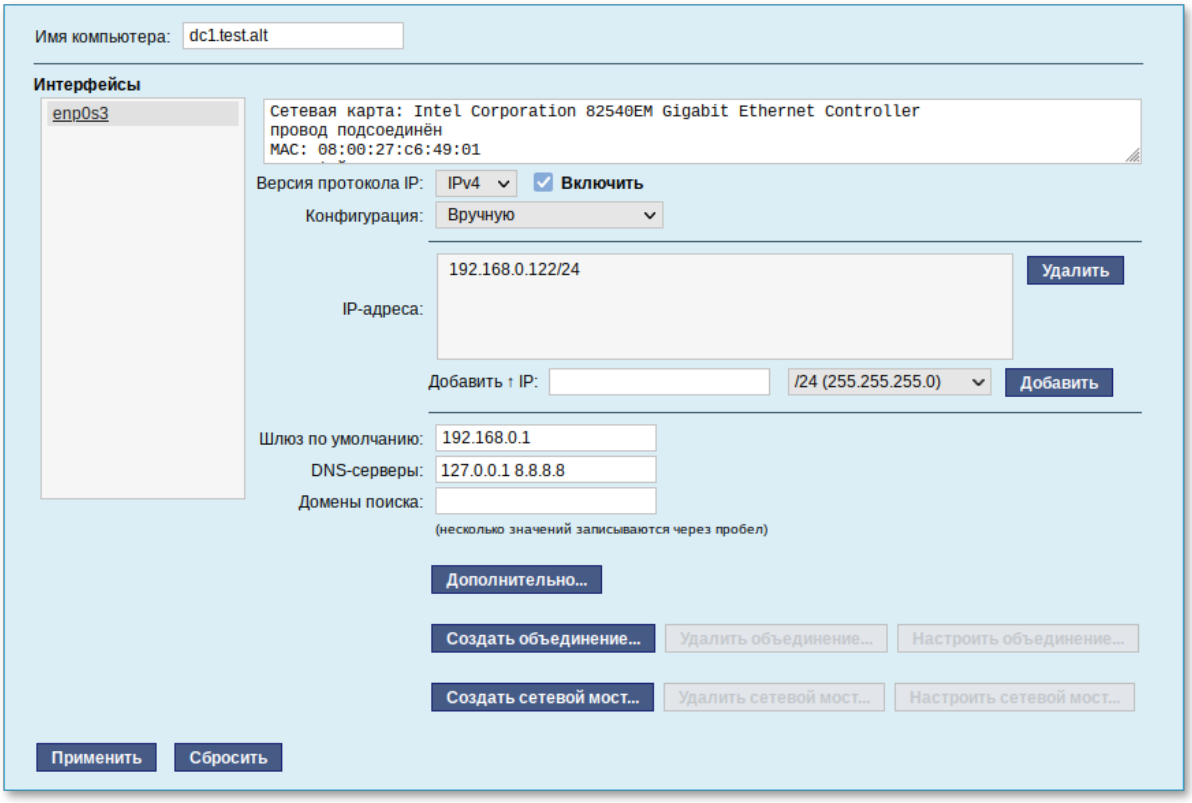
Предупреждение

При указании домена, имеющего суффикс .local, на сервере и подключаемых компьютерах под управлением Linux потребуется отключить службу **avahi-daemon**.

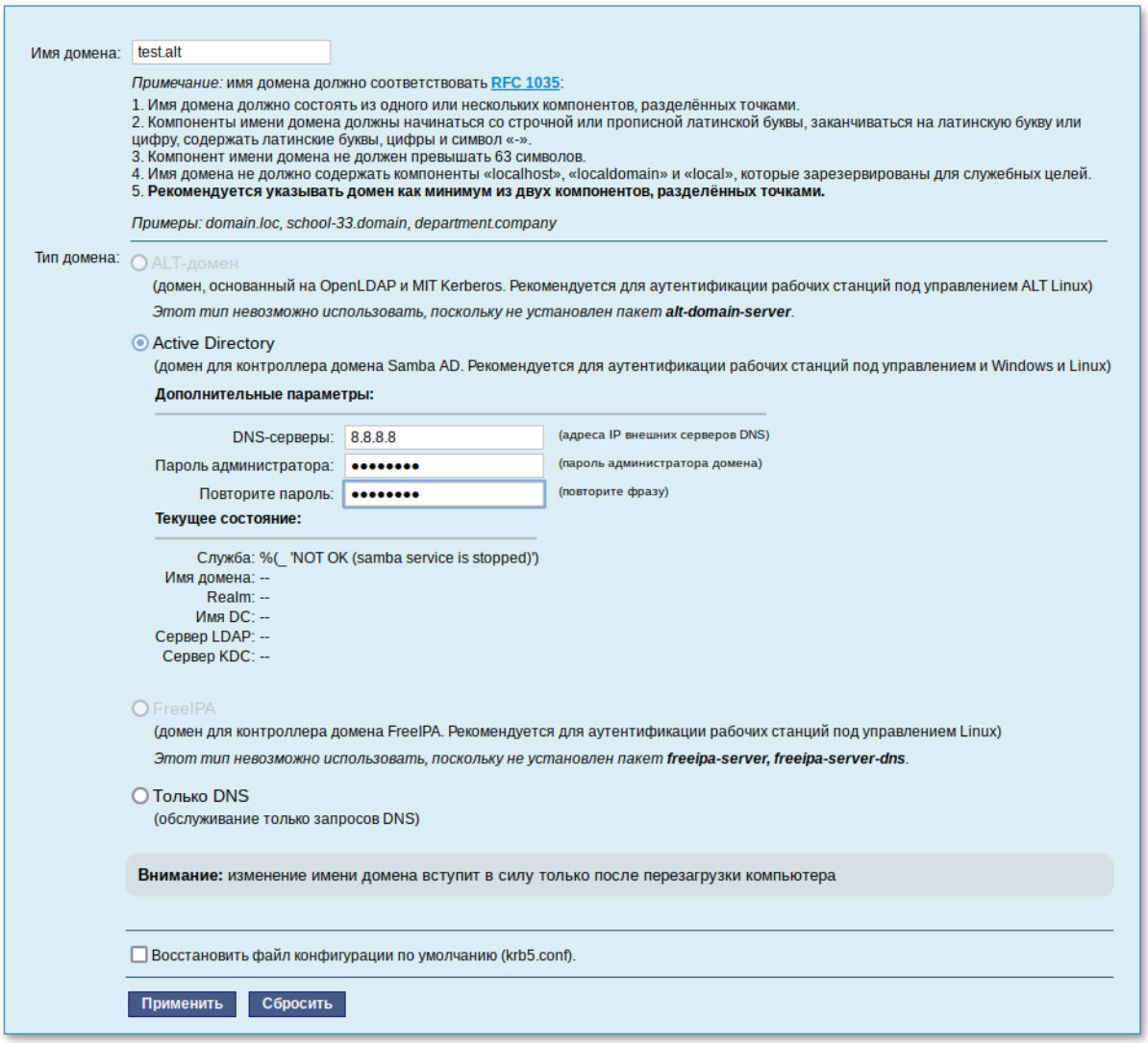
38.2.3. Создание домена в ЦУС

При инициализации домена в веб-интерфейсе ЦУС следует выполнить следующие действия:

1. В модуле Ethernet-интерфейсы указать имя компьютера и DNS 127.0.0.1:



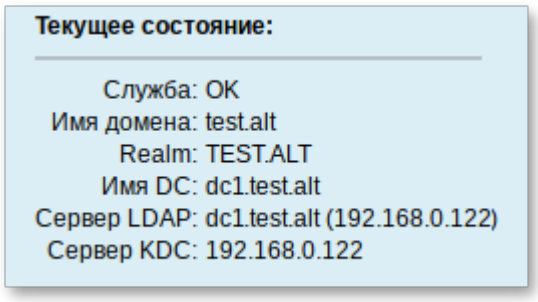
2. В модуле Домен указать имя домена, отметить пункт **`Active Directory`**, указать IP-адреса внешних DNS-серверов, задать пароль администратора домена и нажать кнопку **`Применить`**:



Примечание

Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль, не полностью соответствующий требованиям, это одна из причин завершения развертывания домена ошибкой.

3. После успешного создания домена, будет выведена информация о домене:



4. Перезагрузить сервер.

38.2.4. Создание домена одной командой

Создание контроллера домена test.alt:

```
# samba-tool domain provision --realm=test.alt --domain=test --adminpass='Pa$
$word' --dns-backend=SAMBA_INTERNAL --option="dns forwarder=8.8.8.8" --server-
role=dc
```

где

- --realm — задает область Kerberos (LDAP), и DNS имя домена;
- --domain — задает имя домена (имя рабочей группы);
- --adminpass — пароль основного администратора домена;
- dns forwarder — внешний DNS-сервер;
- --server-role — тип серверной роли.

Примечание

Параметр **`--use-rfc2307`** позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux.

Если уровень домена не указан, то домен разворачивается на уровне 2008_R2. Для разворачивания домена на другом уровне, уровень необходимо явно указать, например:

```
# samba-tool domain provision --realm=test.alt --domain=test --adminpass='Pa$
$word' --dns-backend=SAMBA_INTERNAL --option="dns forwarder=8.8.8.8" --option="ad
dc functional level = 2016" --server-role=dc --function-level=2016
```

Примечание

Если необходим уровень 2012_R2, то следует сначала развернуть домен на уровне 2008_R2, а затем повысить его до 2012_R2 (см. Повышение уровня схемы, функционального уровня домена).

38.2.5. Интерактивное создание домена

Примечание

У Samba свой собственный DNS-сервер. В *DNS forwarder IP address* нужно указать внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена.

Для интерактивного развертывания запустите **samba-tool domain provision**, это запустит утилиту развертывания, которая будет задавать различные вопросы о требованиях к установке. В примере показано создание домена test.alt:

```
# samba-tool domain provision
Realm [TEST.ALT]:
Domain [TEST]:
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) [127.0.0.1]:
8.8.8.8
Administrator password:
Retype password:
Looking up IPv4 addresses
More than one IPv4 address found. Using 192.168.0.122
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=test,DC=alt
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=test,DC=alt
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at /var/lib/
samba/private/krb5.conf
Merge the contents of this file with your system krb5.conf or replace it with
this one. Do not create a symlink!
Once the above files are installed, your Samba4 server will be ready to use
Server Role:           active directory domain controller
Hostname:              dc1
NetBIOS Domain:        TEST
DNS Domain:            test.alt
DOMAIN SID:            S-1-5-21-80639820-2350372464-3293631772
```

При запросе ввода нажимайте **Enter** за исключением запроса пароля администратора («Administrator password:» и «Retype password:»).

Примечание

Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль, не полностью соответствующий требованиям, это одна из причин завершения развертывания домена ошибкой.

38.3. Запуск службы

В файл **/etc/resolvconf.conf** добавить строку:

```
name_servers=127.0.0.1
```

Обновить DNS адреса:

```
# resolvconf -u
```

Установить службу по умолчанию и запустите её:

```
# systemctl enable --now samba
```

38.4. Настройка Kerberos

Внести изменения в файл **/etc/krb5.conf**. Следует раскомментировать строку *default_realm* и содержимое разделов *realms* и *domain_realm* и указать название домена (обратите внимание на регистр символов), в строке *dns_lookup_realm* должно быть установлено значение false:

```
includedir /etc/krb5.conf.d/

[logging]
# default = FILE:/var/log/krb5libs.log
# kdc = FILE:/var/log/krb5kdc.log
# admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_kdc = true
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = TEST.ALT
# default_ccache_name = KEYRING:persistent:%{uid}

[realms]
TEST.ALT = {
  default_domain = test.alt
}

[domain_realm]
dc1 = TEST.ALT
```

Примечание

В момент создания домена Samba конфигурирует шаблон файла **krb5.conf** для домена в каталоге **/var/lib/samba/private/**. Можно просто заменить этим файлом файл, находящийся в каталоге **/etc/**:

```
# cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

38.5. Проверка работоспособности

Просмотр общей информации о домене:

```
# samba-tool domain info 127.0.0.1
Forest           : test.alt
Domain           : test.alt
Netbios domain   : TEST
DC name          : dc1.test.alt
DC netbios name  : DC
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
```

Просмотр предоставляемых служб:

```
# smbclient -L localhost -Uadministrator
Password for [TEST\administrator]:

        Sharename       Type      Comment
        ---------       ----      -------
        sysvol          Disk
        netlogon        Disk
        IPC$            IPC       IPC Service (Samba 4.19.4)
SMB1 disabled -- no workgroup available
```

Общие ресурсы netlogon и sysvol создаваемые по умолчанию нужны для функционирования сервера AD и создаются в **smb.conf** в процессе развертывания/модернизации.

Проверка конфигурации DNS:

- Убедитесь в наличии nameserver 127.0.0.1 в **/etc/resolv.conf**:

```
# cat /etc/resolv.conf
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
search test.alt
nameserver 127.0.0.1

# host test.alt
test.alt has address 192.168.0.122
```

- Проверьте имена хостов:

```
# host -t SRV _kerberos._udp.test.alt.
_kerberos._udp.test.alt has SRV record 0 100 88 dc1.test.alt.
# host -t SRV _ldap._tcp.test.alt.
_ldap._tcp.test.alt has SRV record 0 100 389 dc1.test.alt.
# host -t A dc1.test.alt.
dc1.test.alt has address 192.168.0.122
```

Если имена не находятся, проверьте выключение службы **named**.

Проверка Kerberos (имя домена должно быть в верхнем регистре):

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
```

Просмотр полученного билета:

```
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
01.03.2024 11:50:39  01.03.2024 21:50:39  krbtgt/TEST.ALT@TEST.ALT
        renew until 02.03.2024 11:50:34
```

38.6. Повышение уровня схемы, функционального уровня домена

Для повышения уровня домена необходимо выполнить следующие действия:

1. Указать функциональный уровень AD, который будет поддерживаться контроллером домена в параметре ***ad dc functional level*** файла **/etc/samba/smb.conf**. Возможные значения: 2008_R2, 2012, 2012_R2, 2016.

2. Обновить схему домена, выполнив команду:

   ```
   # samba-tool domain schemaupgrade --schema=<SCHEMA>
   ```

   где SCHEMA — схема, до которой необходимо выполнить обновление (по умолчанию 2019).

3. Подготовить функциональный уровень домена, выполнив команду:

   ```
   # samba-tool domain functionalprep --function-level=<FUNCTION_LEVEL>
   ```

   где FUNCTION_LEVEL — функциональный уровень, к которому нужно подготовиться (по умолчанию 2016).

4. Указать функциональные уровни домена и леса, выполнив команду:

   ```
   # samba-tool domain level raise --domain-level=<DOMAIN_LEVEL> --forest-level=<FOREST_LEVEL>
   ```

где:

- FOREST_LEVEL — уровень работы леса. Возможные значения: 2003, 2008, 2008_R2, 2012, 2012_R2, 2016.
- DOMAIN_LEVEL — уровень работы домена. Возможные значения: 2003, 2008, 2008_R2, 2012, 2012_R2, 2016.

Примечание

При установке значения параметра ***ad dc functional level*** в файле **/etc/samba/smb.conf** вручную, защита от несовпадения функций между контроллерами домена снижается. Поэтому на всех контроллерах домена должна использоваться одна и та же версия Samba, чтобы гарантировать, что поведение, наблюдаемое клиентом, будет одинаковым независимо от того, к какому контроллеру домена осуществляется соединение.

Пример повышения уровня домена до 2016:

- в раздел [global] файла **/etc/samba/smb.conf** добавить строку:

```
ad dc functional level = 2016
```

- перезагрузить службу samba:

```
# systemctl restart samba.service
```

- обновить схему домена:

```
# samba-tool domain schemaupgrade --schema=2019
```

- подготовить функциональный уровень домена:

```
# samba-tool domain functionalprep --function-level=2016
```

- повысить функциональные уровни домена и леса до 2016:

```
# samba-tool domain level raise --domain-level=2016 --forest-level=2016
Domain function level changed!
Forest function level changed!
All changes applied successfully!
```

- убедиться, что уровни домена и леса повышены:

```
# samba-tool domain level show
Domain and forest function level for domain 'DC=test,DC=alt'

Forest function level: (Windows) 2016
Domain function level: (Windows) 2016
Lowest function level of a DC: (Windows) 2016
```

38.7. Управление пользователями

Создать пользователя с паролем:

```
samba-tool user create имя пользователя
samba-tool user setexpiry имя пользователя
```

Удалить пользователя:

```
samba-tool user delete имя пользователя
```

Отключить пользователя:

```
samba-tool user disable имя пользователя
```

Включить пользователя:

```
samba-tool user enable имя пользователя
```

Изменить пароль пользователя:

```
samba-tool user setpassword имя пользователя
```

Просмотреть доступных пользователей:

```
# samba-tool user list
```

Например, создать и разблокировать пользователя ivanov:

```
# samba-tool user create ivanov --given-name='Иван Иванов' --mail-
address='ivanov@test.alt'
# samba-tool user setexpiry ivanov --noexpiry
```

Предупреждение

Не допускайте одинаковых имён для пользователя и компьютера, это может привести к коллизиям (например, такого пользователя нельзя добавить в группу). Если компьютер с таким именем заведён, удалить его можно командой: **`pdbedit -x -m имя`**

38.8. Заведение вторичного DC

Присоединение дополнительного Samba DC к существующему AD отличается от инициализации первого DC в лесу AD.

Все действия выполняются на узле dc2.test.alt (192.168.0.106), если не указано иное.

1. Установить пакет *task-samba-dc*, который установит все необходимое:

```
# apt-get install task-samba-dc
```

2. Остановить конфликтующие службы **krb5kdc** и **slapd**, а также **bind**:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl disable $service;
systemctl stop $service; done
```

3. Очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

4. На Primary Domain Controller (PDC) проверить состояние службы **bind**:

```
# systemctl status bind
```

И, если она была включена, выключить службу **bind** и перезапустить службу **samba**:

```
# systemctl stop bind
# systemctl restart samba
```

5. На PDC завести IP-адрес для dc2:

Предупреждение

Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

```
# samba-tool dns add 192.168.0.122 test.alt DC2 A 192.168.0.106 -
Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

6. На вторичном DC установить следующие параметры в файле конфигурации клиента Kerberos **`/etc/krb5.conf`**):

```
[libdefaults]
default_realm = TEST.ALT
dns_lookup_realm = false
dns_lookup_kdc = true
```

Примечание

На вторичном DC в **/etc/resolv.conf** обязательно должен быть добавлен PDC как nameserver:

```
# echo "name_servers=192.168.0.122" >> /etc/resolvconf.conf
# echo "search_domains=test.alt" >> /etc/resolvconf.conf
# resolvconf -u
# cat /etc/resolv.conf
search test.alt
nameserver 192.168.0.122
nameserver 8.8.8.8
```

7. Для проверки настройки запросить билет Kerberos для администратора домена:

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
```

Предупреждение

Имя домена должно быть указано в верхнем регистре

8. Убедиться, что билет получен:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
01.03.2024 12:43:28  01.03.2024 22:43:28  krbtgt/TEST.ALT@TEST.ALT
         renew until 08.03.2024 12:43:24
```

9. Ввести вторичный DC в домен test.alt в качестве контроллера домена (DC):

```
# samba-tool domain join test.alt DC -Uadministrator --realm=test.alt --
option="dns forwarder=8.8.8.8"
```

Если всё нормально, в конце будет выведена информация о присоединении к домену:

```
Joined domain TEST (SID S-1-5-21-80639820-2350372464-3293631772) as a DC
```

Для получения дополнительной информации можно воспользоваться командой:

```
# samba-tool domain join --help
```

10. Сделать службу **samba** запускаемой по умолчанию и запустить её:

```
# systemctl enable --now samba
```

38.9. Репликация

Предупреждение

Без успешной двунаправленной репликации в течение 14 дней DC исключается из Active Directory

Предупреждение

Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

1. Реплицируем на вторичном DC (с первичного):

```
# samba-tool drs replicate dc2.test.alt dc1.test.alt dc=test,dc=alt -
Uadministrator
```

   Сначала указывается приемник, затем источник, после этого реплицируемая ветка в LDAP.

2. Реплицируем на вторичном DC (на первичный):

```
# samba-tool drs replicate dc1.test.alt dc2.test.alt dc=test,dc=alt -
Uadministrator
```

   Сначала указывается приемник, затем источник, после этого реплицируемая ветка в LDAP.

   Примечание

   Имя домена в именах серверов можно опустить (если они одинаковые).

3. Для просмотра статуса репликации на PDC, запустите на Samba DC:

```
# samba-tool drs showrepl
```

Примечание

Если репликация на Windows не работает, добавьте в Active Directory Sites and Services новое соединение Active Directory. Реплицируйте на DC, подождите минут 5 и пробуйте реплицировать с Samba на Windows.

38.10. Подключение к домену на рабочей станции

38.10.1. Подготовка

Для ввода компьютера в Active Directory потребуется установить пакет *task-auth-ad-sssd* и все его зависимости (если он еще не установлен):

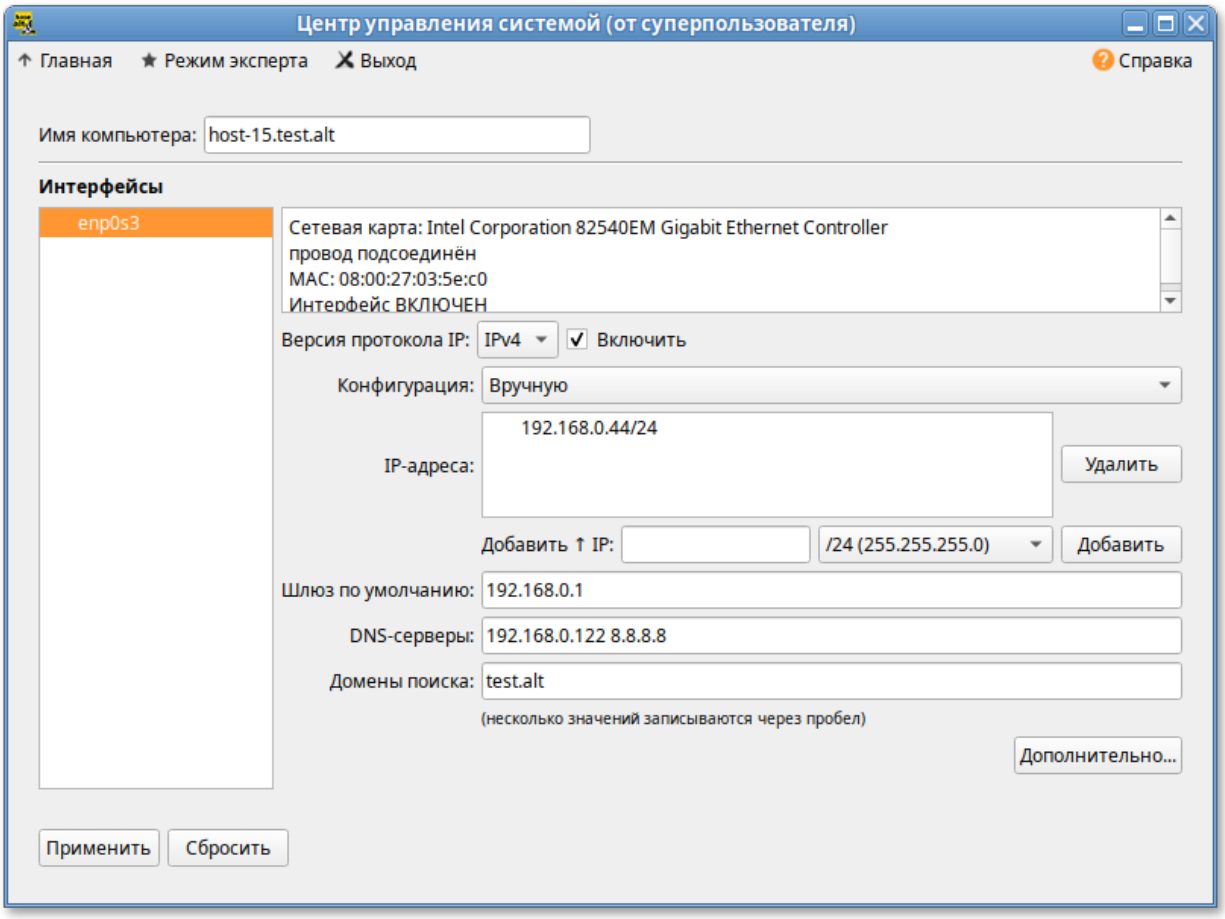
```
# apt-get install task-auth-ad-sssd
```

Синхронизация времени с контроллером домена производится автоматически.

Для ввода компьютера в домен, на нём должен быть доступен сервер DNS, имеющий записи про контроллер домена Active Directory. Ниже приведен пример настройки сетевого интерфейса со статическим IP-адресом. При получении IP-адреса по DHCP данные о сервере DNS также должны быть получены от сервера DHCP.

Настройку сети можно выполнить как в графическом интерфейсе, так и в консоли:

- В Центре управления системой в разделе **Сеть** → **Ethernet интерфейсы** задать имя компьютера, указать в поле **`DNS-серверы`** DNS-сервер домена и в поле **`Домены поиска`** — домен для поиска:



- В консоли:
  - задать имя компьютера:

    ```
    # hostnamectl set-hostname host-15.test.alt
    ```

  - в качестве первичного DNS должен быть указан DNS-сервер домена. Для этого необходимо создать файл **`/etc/net/ifaces/enp0s3/resolv.conf`** со следующим содержимым:

    ```
    nameserver 192.168.0.122
    ```

    где 192.168.0.122 — IP-адрес DNS-сервера домена.

- указать службе resolvconf использовать DNS контроллера домена и домен для поиска. Для этого в файле **/etc/resolvconf.conf** добавить/отредактировать следующие параметры:

```
interface_order='lo lo[0-9]* lo.* enp0s3'
search_domains=test.alt
```

  где enp0s3 — интерфейс на котором доступен контроллер домена, test.alt — домен.

- обновить DNS адреса:

```
# resolvconf -u
```

Примечание

После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

В результате выполненных действий в файле **/etc/resolv.conf** должны появиться строки:

```
search test.alt
nameserver 192.168.0.122
```

38.10.2. Ввод в домен

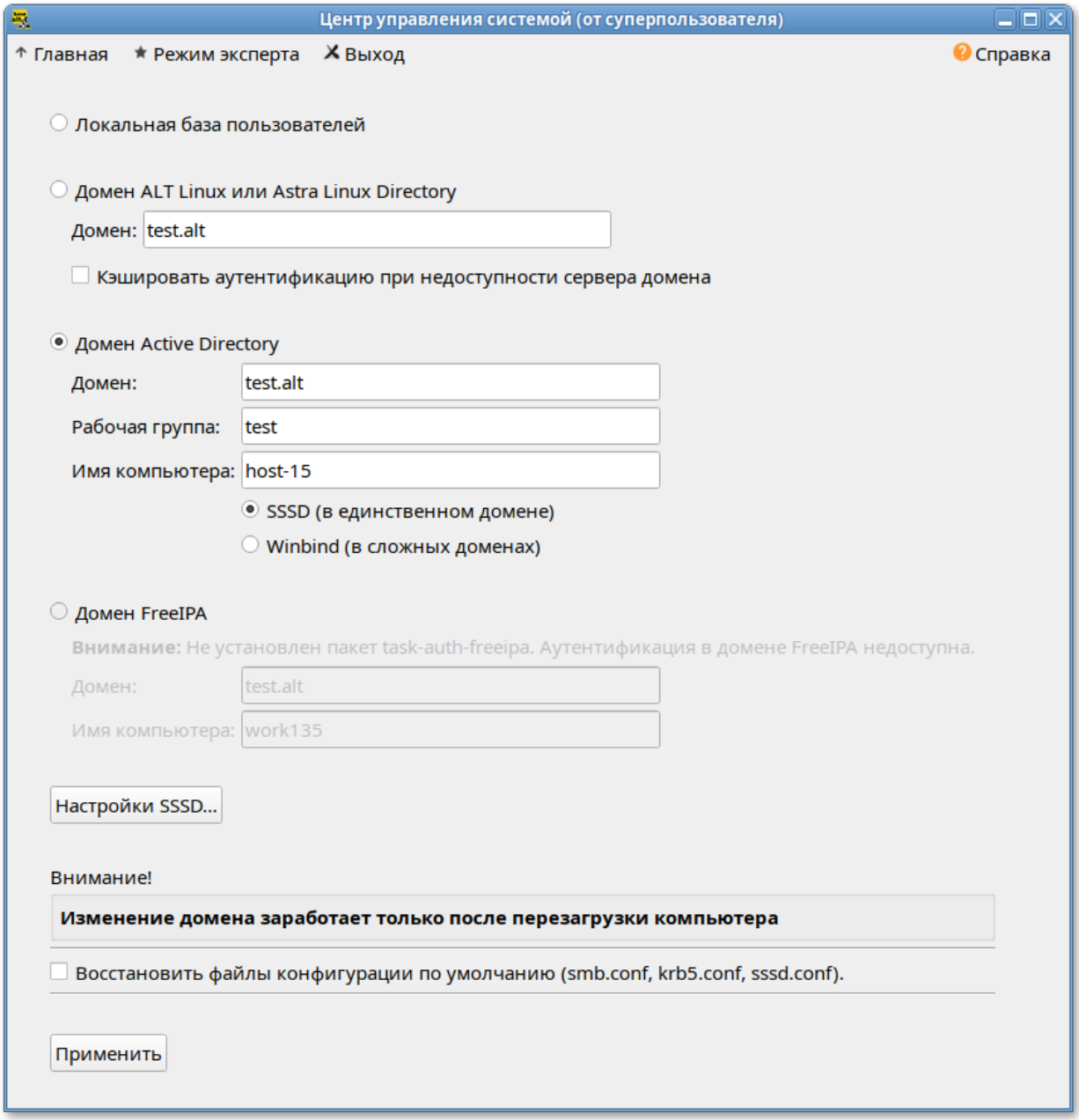
Ввод в домен можно осуществить следующими способами:

- В командной строке:

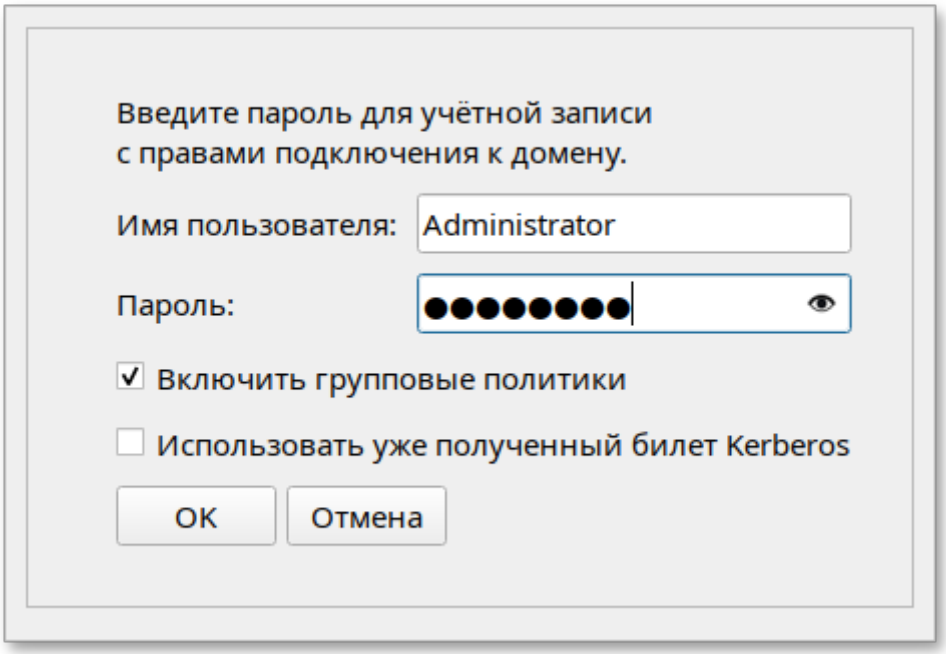
```
# system-auth write ad test.alt host-15 test 'administrator' 'Pa$$word'
Joined 'HOST-15' to dns domain 'test.alt'
```

- В Центре управления системой в разделе **Пользователи** → **Аутентификация**.

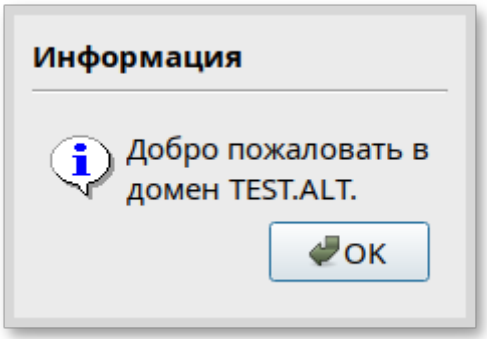
  В открывшемся окне следует выбрать пункт **Домен Active Directory**, заполнить поля и нажать кнопку **Применить**:



В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку **OK**:



При успешном подключении к домену, отобразится соответствующая информация:



Перезагрузить рабочую станцию.

Глава 39. Групповые политики

Групповые политики — это набор правил и настроек для серверов и рабочих станций, реализуемых в корпоративных решениях. В соответствии с групповыми политиками производится настройка рабочей среды относительно локальных политик, действующих по умолчанию. В данном разделе рассмотрена реализация поддержки групповых политик Active Directory в решениях на базе дистрибутивов ALT.

В дистрибутивах ALT для применения групповых политик, на данный момент, предлагается использовать инструмент gpupdate. Инструмент рассчитан на работу на машине, введённой в домен Samba.

Интеграция в инфраструктуру LDAP-объектов Active Directory позволяет осуществлять привязку настроек управляемых конфигураций объектам в дереве каталогов. Кроме глобальных настроек в рамках домена, возможна привязка к следующим группам объектов:

- подразделения (OU) — пользователи и компьютеры, хранящиеся в соответствующей части дерева объектов;
- сайты — группы компьютеров в заданной подсети в рамках одного и того же домена;
- конкретные пользователи и компьютеры.

Кроме того, в самих объектах групповых политик могут быть заданы дополнительные условия, фильтры и ограничения, на основании которых принимается решение о том, как применять данную групповую политику.

Политики подразделяются на политики для компьютеров (Machine) и политики для пользователей (User). Политики для компьютеров применяются на хосте в момент загрузки, а также в момент явного или регулярного запроса планировщиком (раз в час). Пользовательские политики применяются в момент входа в систему.

Групповые политики можно использовать для разных целей, например:

- управления интернет-браузерами Firefox/Chromium/Yandex. Возможно установить при использовании ADMX-файлов Mozilla Firefox (пакет *admx-firefox*), Google Chrome (пакет *admx-chromium*) и Yandex (пакет *admx-yandex-browser*) соответственно;
- установки запрета на подключение внешних носителей;
- управления политиками control (реализован широкий набор настроек). Возможно установить при использовании ADMX-файлов ALT;
- включения или выключения различных служб (сервисов systemd). Возможно установить при использовании ADMX-файлов ALT;
- настройки удаленного доступа к рабочему столу (VNC) и настройки графической среды MATE. Возможно установить при использовании ADMX-файлов ALT;
- настройки среды рабочего стола KDE (экспериментальная политика). Возможно установить при использовании ADMX-файлов ALT;
- подключения сетевых дисков (экспериментальная политика);
- управления общими каталогами (экспериментальная политика);
- генерирования (удаления/замены) ярлыков для запуска программ;
- создания каталогов;
- управления файлами (экспериментальная политика);
- управления сценариями запуска и завершения работы компьютера, входа и выхода пользователя из системы (экспериментальная политика);
- установки и удаления пакетов (экспериментальная политика).

Важно

Модули (настройки), помеченные как экспериментальные, необходимо включать вручную через ADMX-файлы ALT в разделе **Групповые политики**.

39.1. Развертывание групповых политик

Процесс развёртывание групповых политик:

1. Развернуть сервер Samba AD DC (см. Samba 4 в роли контроллера домена Active Directory).

2. Установить административные шаблоны. Для этого:

   - установить пакеты политик *admx-basealt*, *admx-chromium*, *admx-firefox*, *admx-yandex-browser* и утилиту *admx-msi-setup*:

     ```
     # apt-get install admx-basealt admx-chromium admx-firefox admx-yandex-browser admx-msi-setup
     ```

   - скачать и установить ADMX-файлы от Microsoft:

     ```
     # admx-msi-setup
     ```

     Примечание

     По умолчанию, **admx-msi-setup** устанавливает последнюю версию ADMX от Microsoft (сейчас это Microsoft Group Policy — Windows 10 October 2020 Update (20H2)). С помощью параметров, можно указать другой источник:

     ```
     # admx-msi-setup -h
     admx-msi-setup - download msi files and extract them in
     <destination-directory> default value is /usr/share/
     PolicyDefinitions/.
     Usage: admx-msi-setup [-d <destination-directory>] [-s <admx-msi-
     source>]
     Removing admx-msi-setup temporary files...
     ```

   - после установки политики будут находиться в каталоге **/usr/share/PolicyDefinitions**. Необходимо скопировать локальные ADMX-файлы в сетевой каталог sysvol (**/var/lib/samba/sysvol/<DOMAIN>/Policies/**):

     ```
     # samba-tool gpo admxload -U Administrator
     ```

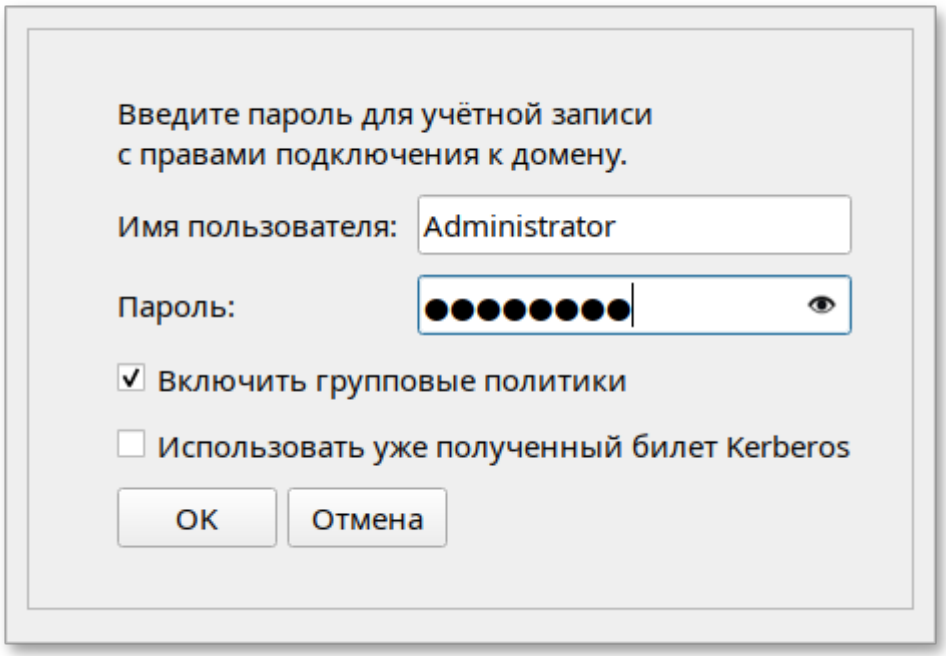
3. Ввести рабочие станции в домен Active Directory (см. Подключение к домену на рабочей станции).

Примечание

Должен быть установлен пакет *alterator-gpupdate*:

```
# apt-get install alterator-gpupdate
```

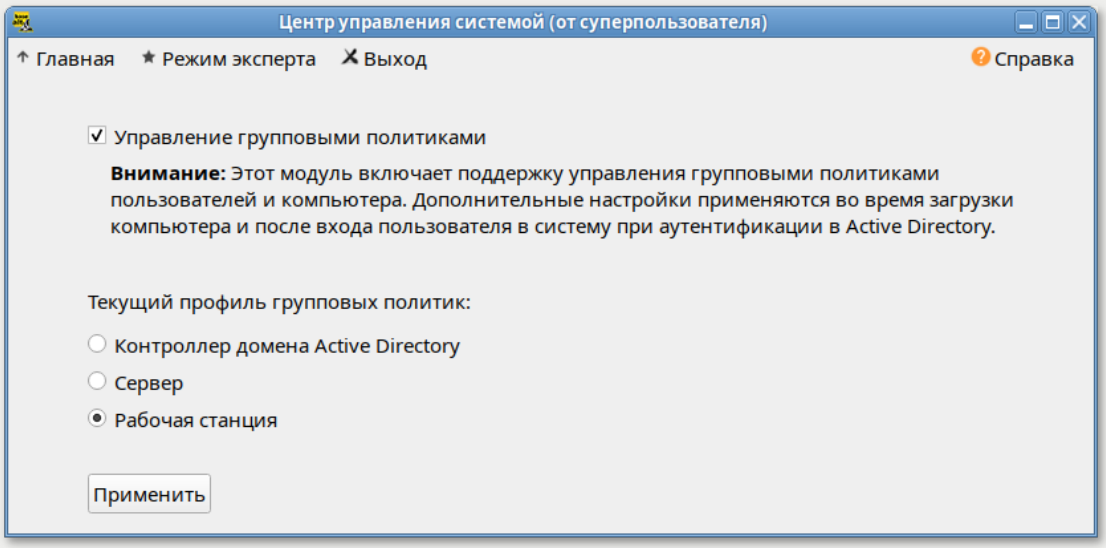
Для автоматического включения групповых политик, при вводе в домен, в окне ввода имени и пароля пользователя, имеющего право вводить машины в домен, отметить пункт **Включить групповые политики**:



Политики будут включены сразу после ввода в домен (после перезагрузки системы).

Примечание

Если машина уже находится в домене, можно вручную включить групповые политики с помощью модуля alterator-gpupdate. Для этого в Центре управления системой в разделе **Система** → **Групповые политики** следует выбрать шаблон локальной политики (**Сервер**, **Рабочая станция** или **Контроллер домена**) и установить отметку в пункте **Управление групповыми политиками**:



4. На рабочей станции, введённой в домен, установить административные инструменты (модуль удаленного управления базой данных конфигурации (ADMC) и модуль редактирования настроек клиентской конфигурации (GPUI)):

```
# apt-get install admc gpui
```

Примечание

В настоящее время GPUI не умеет читать файлы ADMX с контроллера домена. Для корректной работы необходимо установить пакеты admx и файлы ADMX от Microsoft:

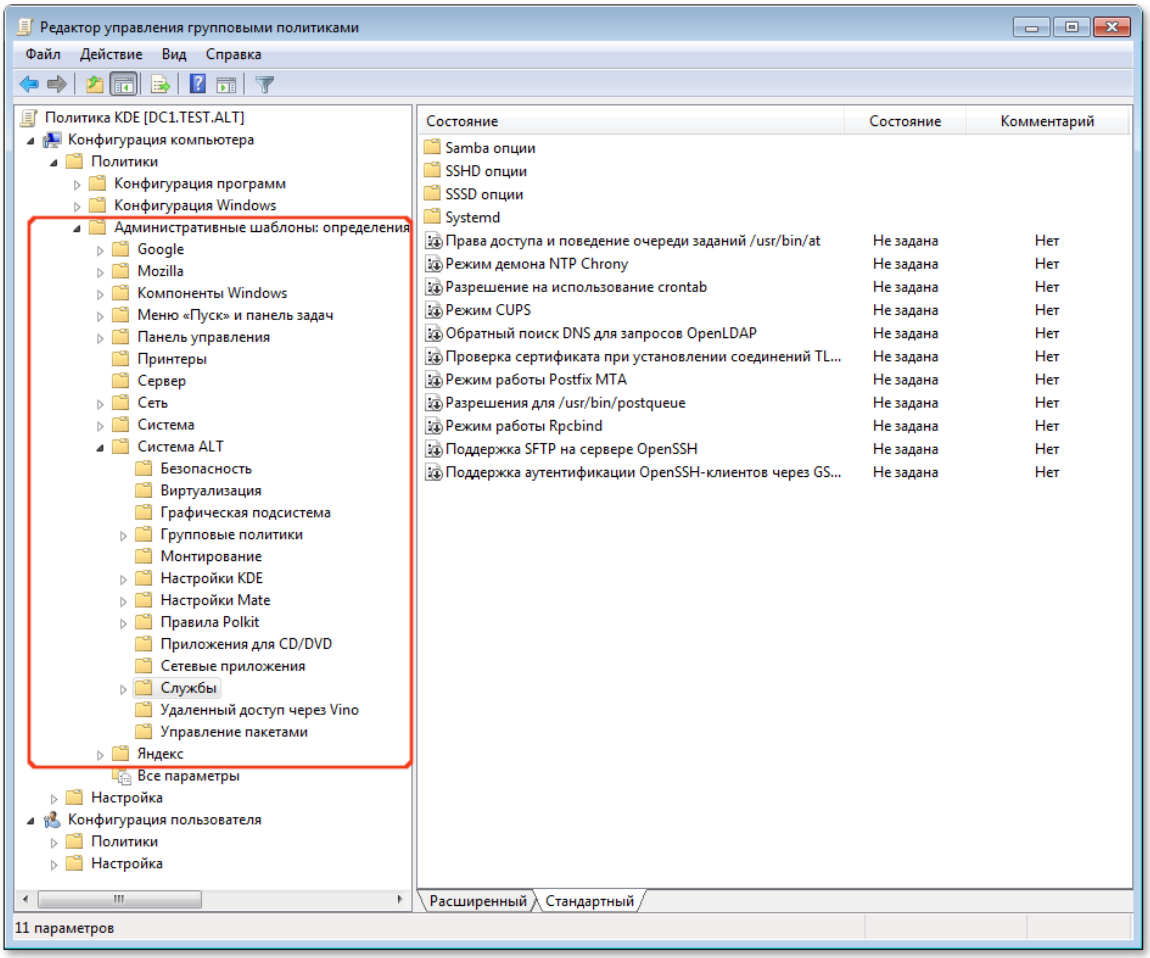
```
# apt-get install admx-basealt admx-chromium admx-firefox admx-yandex-browser admx-msi-setup
# admx-msi-setup
```

5. Настроить, если это необходимо, RSAT на машине с ОС Windows:

   - ввести машину с ОС Windows в домен (управление сервером Samba с помощью RSAT поддерживается из среды до Windows 2012R2 включительно);

- включить компоненты удаленного администрирования (этот шаг можно пропустить, если административные шаблоны были установлены на контроллере домена). Для задания конфигурации с помощью RSAT необходимо установить административные шаблоны (файлы ADMX) и зависящие от языка файлы ADML из репозитория http://git.altlinux.org/gears/a/admx-basealt.git (https://github.com/altlinux/admx-basealt) и разместить их в каталоге **`\\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\PolicyDefinitions`**.

- корректно установленные административные шаблоны будут отображены на машине Windows в оснастке **Редактор управления групповыми политиками** в разделе **Конфигурация компьютера** → **Политики** → **Административные шаблоны** → **Система ALT**:



39.2. Пример создания групповой политики

Для создания групповой политики на машине, введённой в домен, необходимо выполнить следующие шаги:

1. Добавить доменные устройства (компьютеры/пользователи) в подразделение (OU) (инструмент ADMC или оснастка AD «Пользователи и компьютеры»);

2. Создать политику и назначить её на OU (инструмент ADMC или оснастка AD «Управление групповой политикой»);

3. Отредактировать параметры политики (инструмент GPUI или оснастка AD «Редактор управления групповыми политиками»).

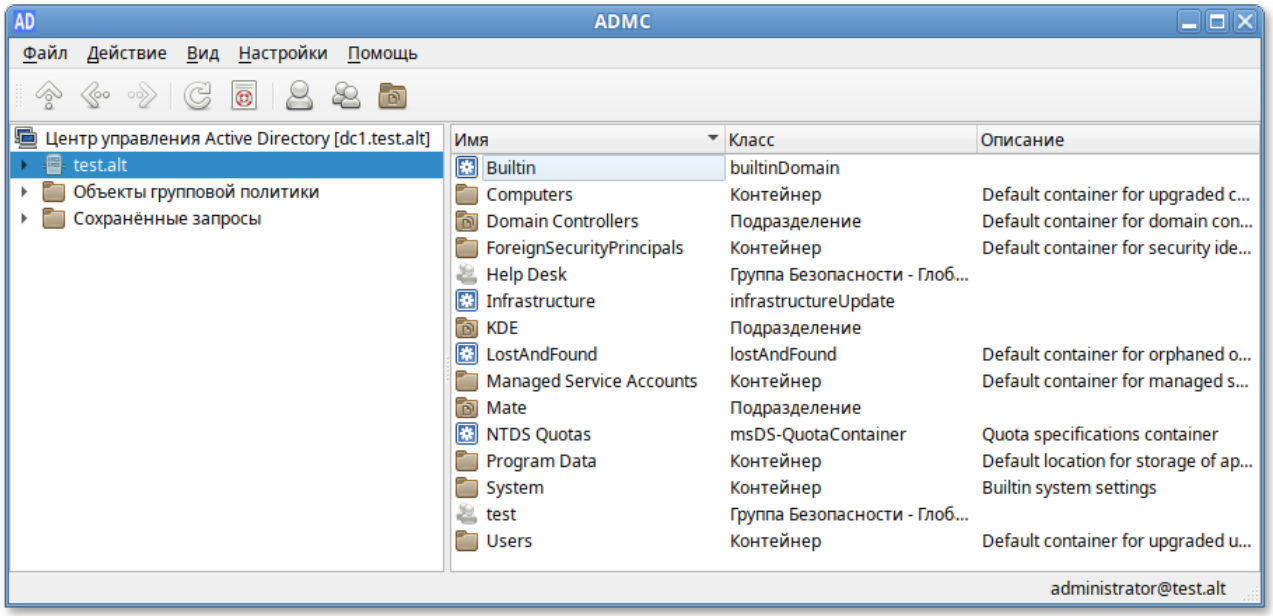
В качестве примера, создадим политику, разрешающую запускать команду **ping** только суперпользователю (root).

Для использования **ADMC** следует сначала получить билет Kerberos для администратора домена:

```
$ kinit administrator
Password for administrator@TEST.ALT:
```

Запустить ADMC можно из меню (**Меню MATE** → **Приложения** → **Системные** → **ADMC**) или командой **admc**:

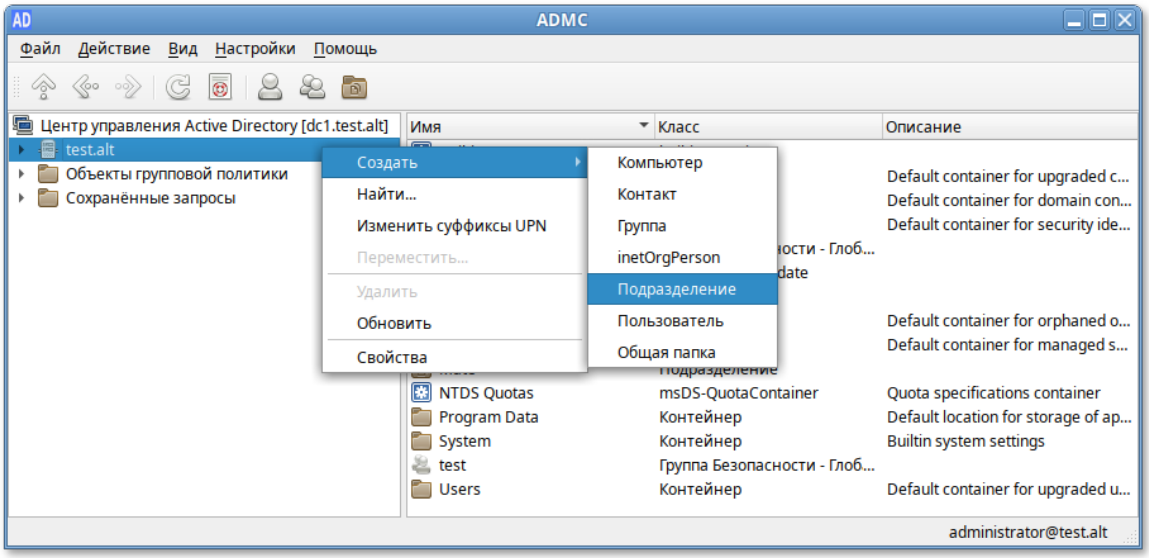
```
$ admc
```



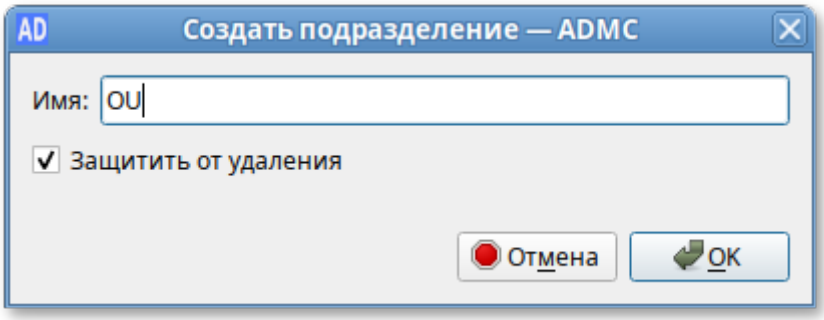
Добавление доменных устройств в группу членства GPO:

1. Создать новое подразделение:

   - в контекстном меню домена выбрать пункт **Создать** → **Подразделение**:



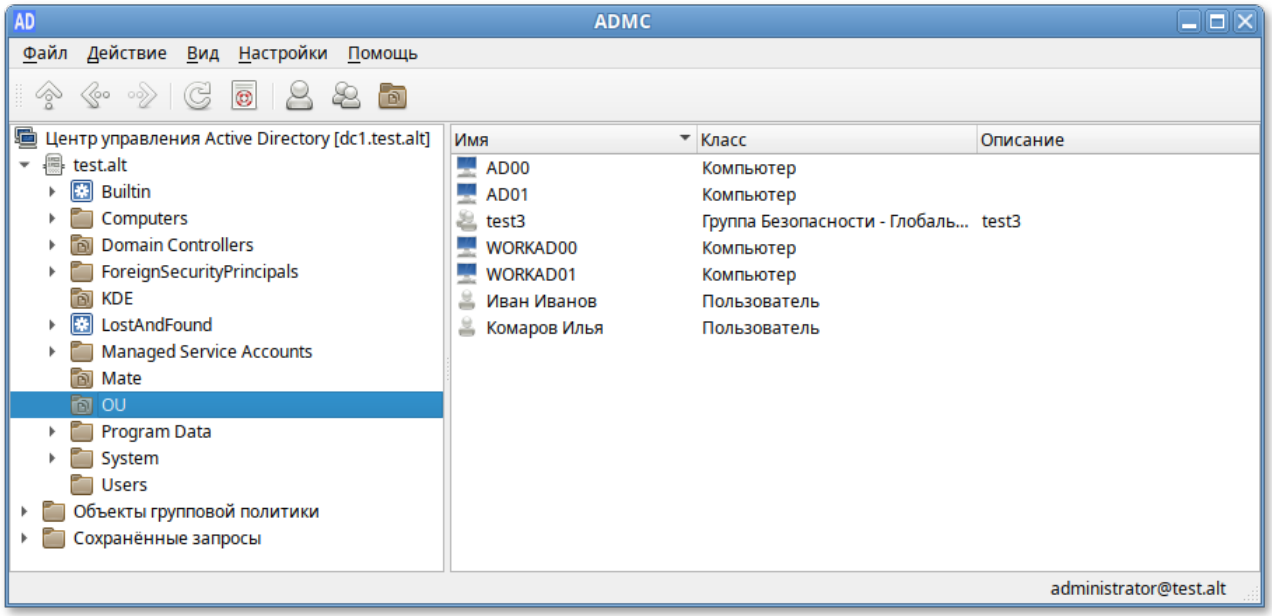
- в открывшемся окне ввести название подразделения (например, OU) и нажать кнопку **OK**:



2. Переместить компьютеры и пользователей домена в созданное подразделение:

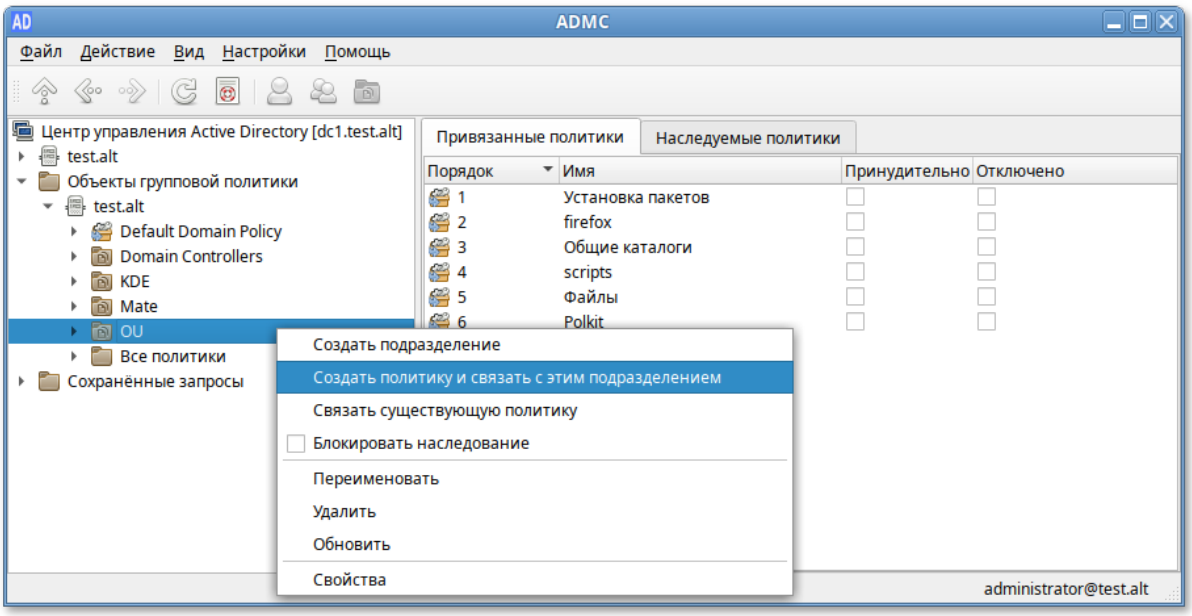
   - в контекстном меню пользователя/компьютера выбрать пункт **Переместить...**;

   - в открывшемся диалоговом окне **Выбор контейнера — ADMC** выбрать контейнер, в который следует переместить учетную запись пользователя.

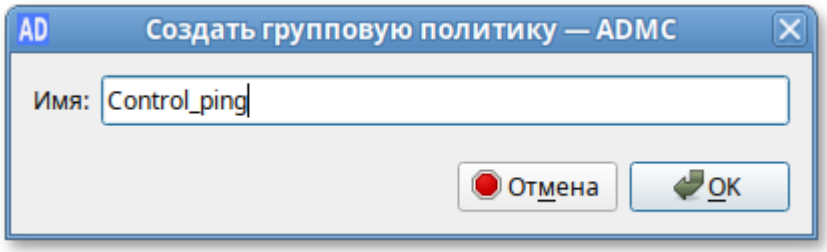


Создание политики для подразделения:

1. В контекстном меню подразделения (в папке **Объекты групповой политики**) выбрать пункт **Создать политику и связать с этим подразделением**:

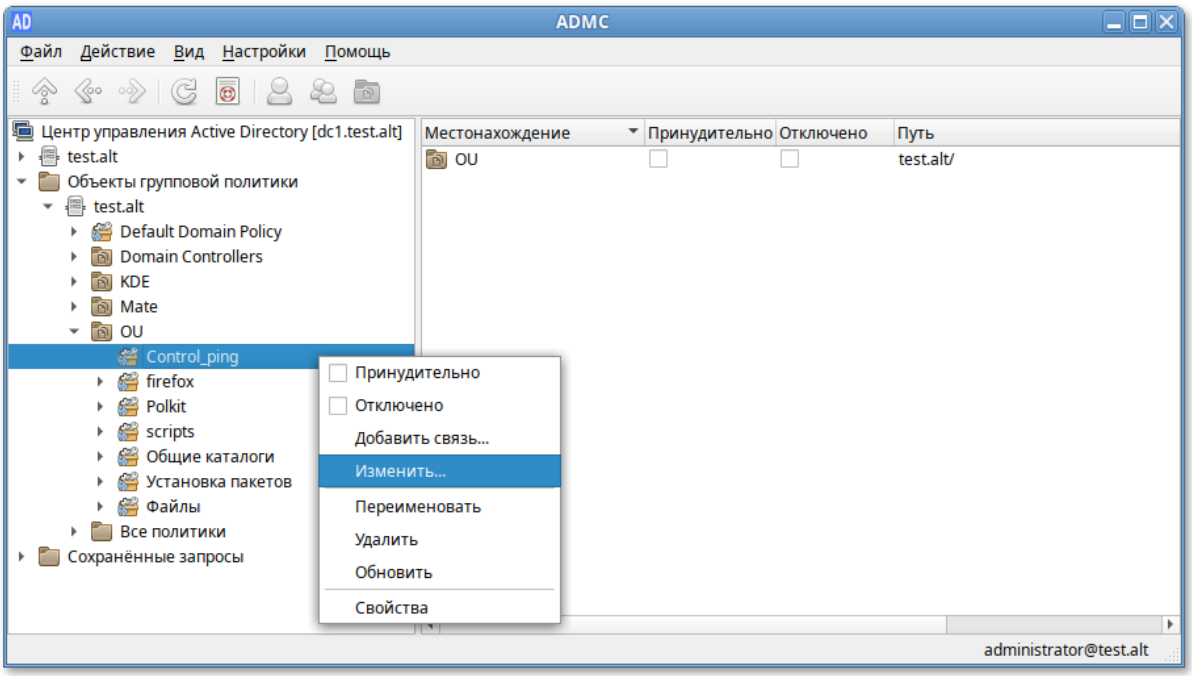


2. В открывшемся окне ввести название политики и нажать кнопку **OK**:

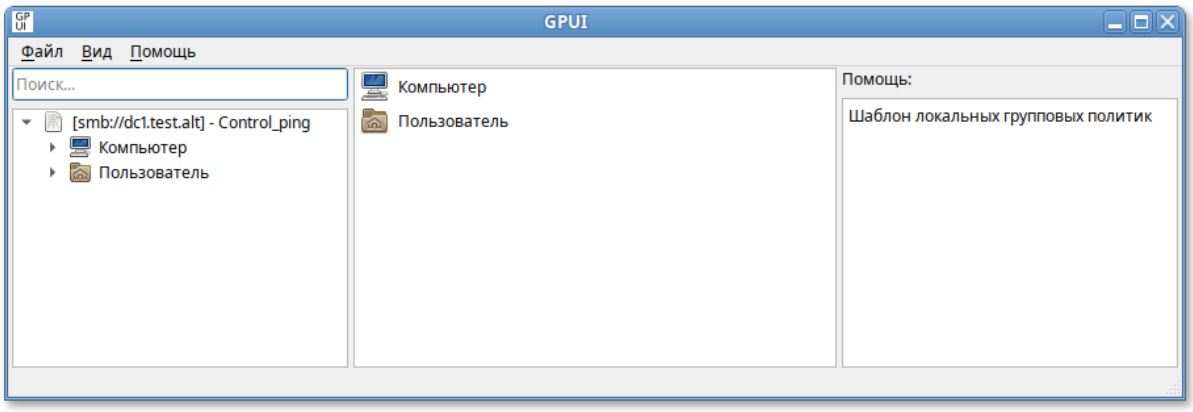


Редактирование настроек групповой политики:

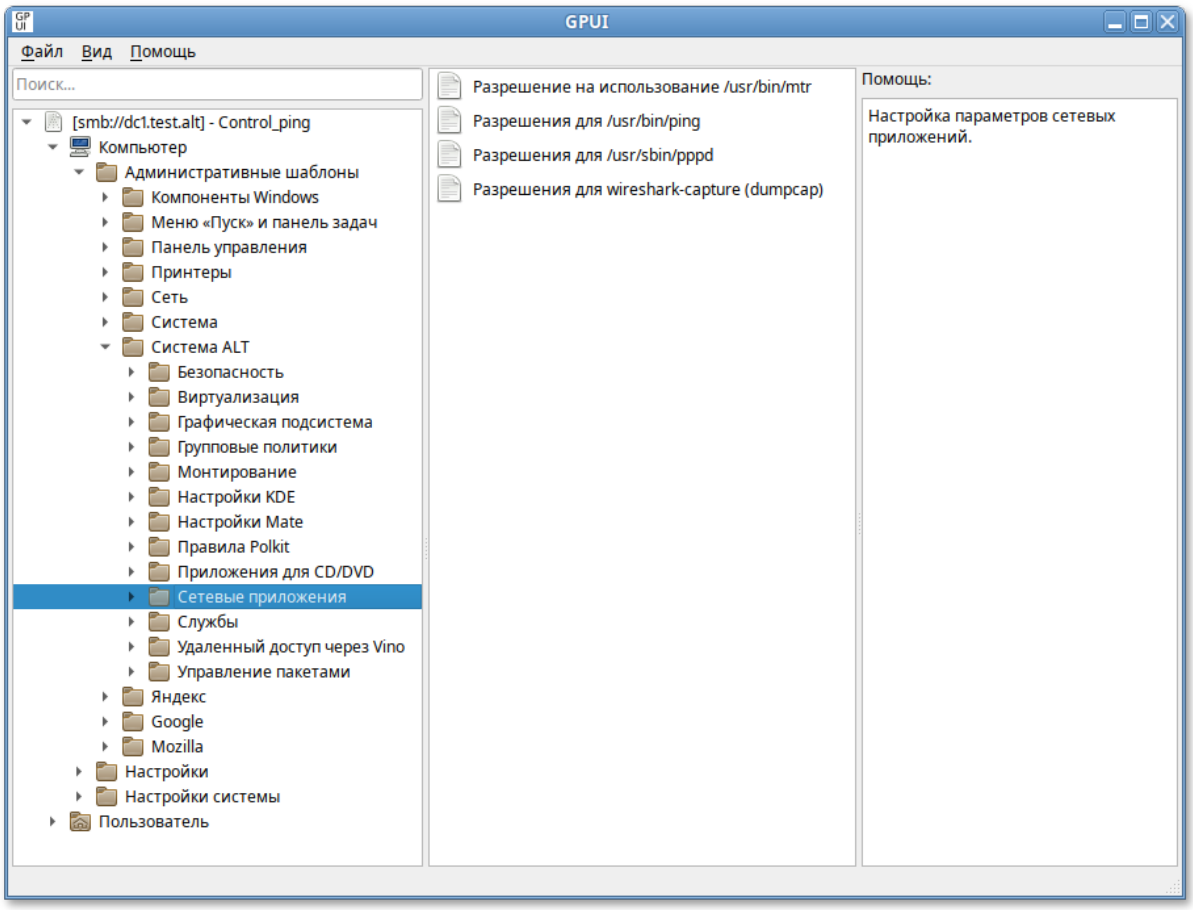
1. В контекстном меню политики выбрать пункт **Изменить…**:



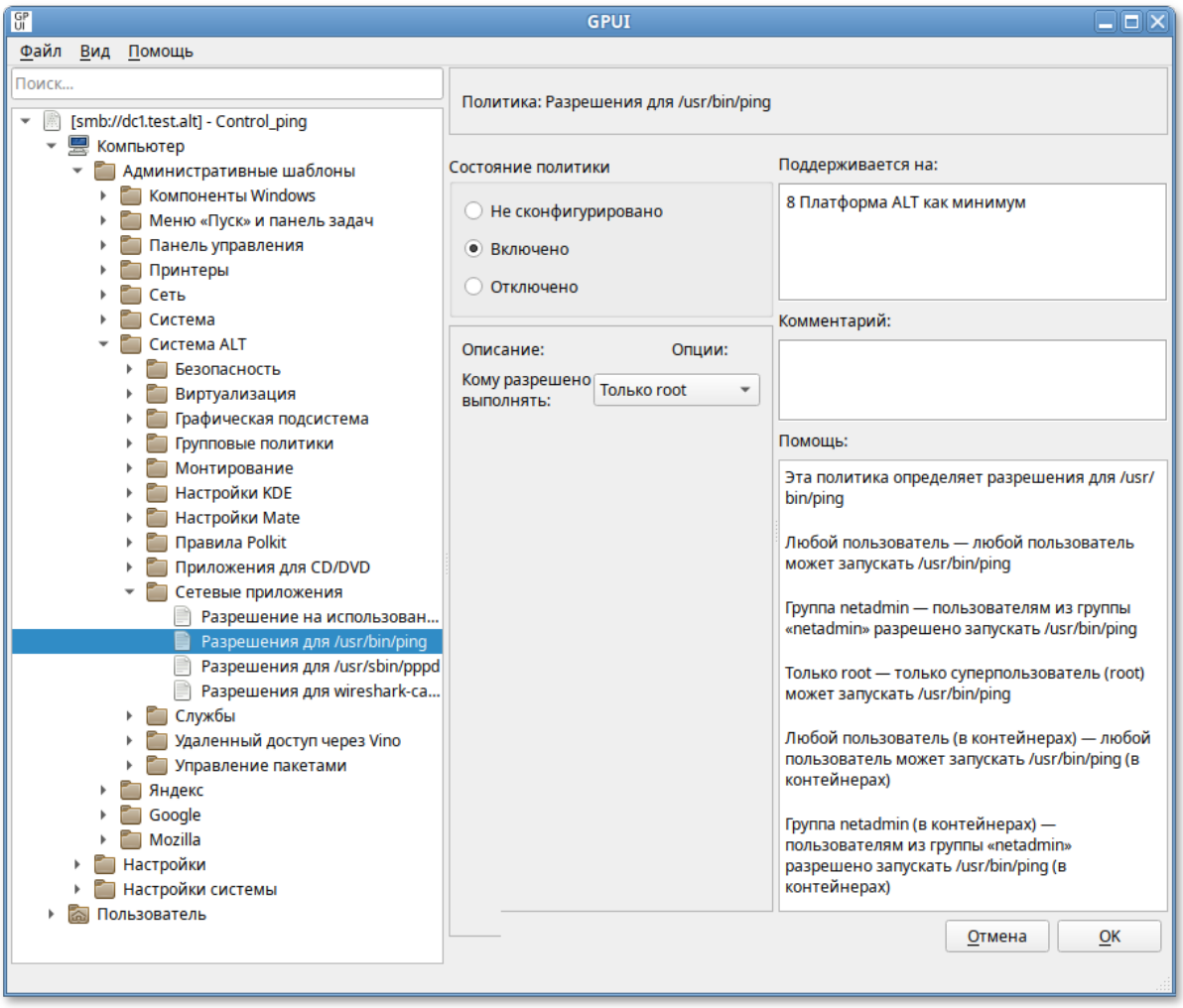
2. Откроется окно редактирования групповых политик (GPUI):



3. Перейти в **Компьютер** → **Административные шаблоны** → **Система ALT**. Здесь есть несколько разделов, соответствующих категориям control. Выбрать раздел **`Сетевые приложения`**, в правом окне редактора отобразится список политик:



4. Щёлкнуть левой кнопкой мыши на политике **`Разрешения для /usr/bin/ping`**. Откроется диалоговое окно настройки политики. Выбрать параметр **`Включено`**, в выпадающем списке **`Кому разрешено выполнять`** выбрать пункт **Только root** и нажать кнопку **`OK`**:



5. После обновления политики на клиенте, выполнять команду **`ping`** сможет только администратор:

```
$ ping localhost
bash: ping: команда не найдена
$ /usr/bin/ping localhost
bash: /usr/bin/ping: Отказано в доступе
# control ping
restricted
```

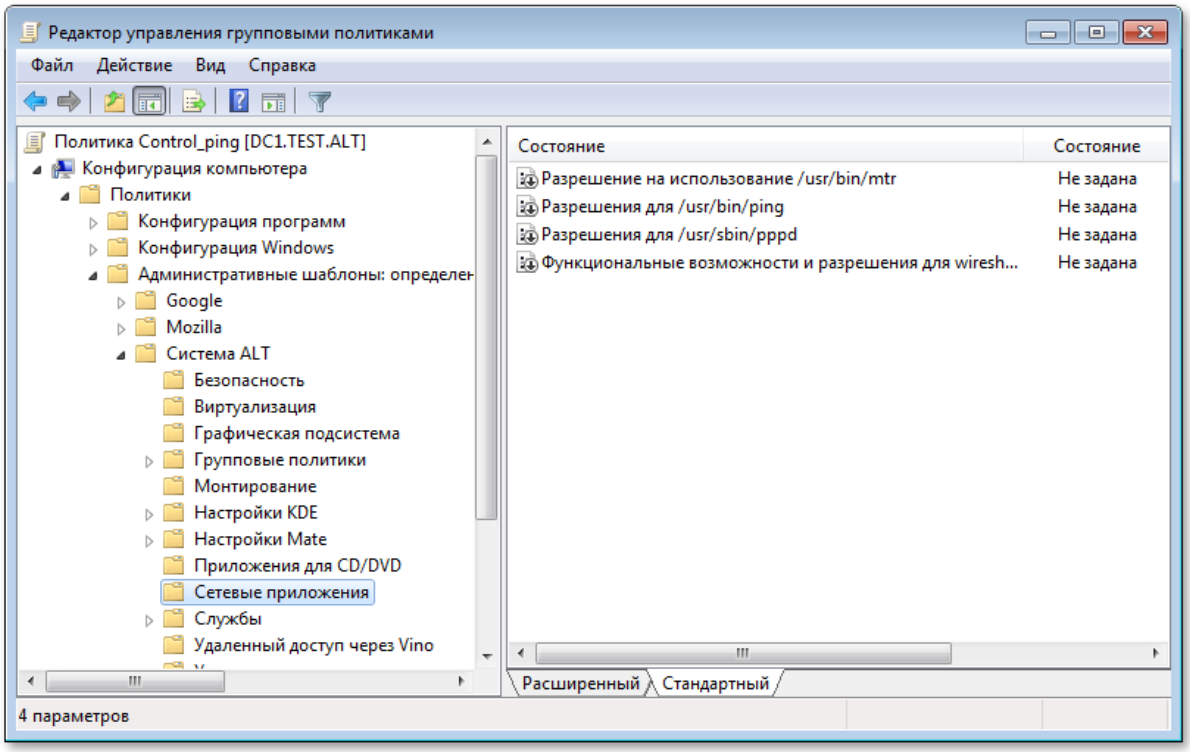
Пример создания групповой политики на машине с ОС Windows:

1. На машине с установленным RSAT открыть оснастку **Управление групповыми политиками** (gpmc.msc).

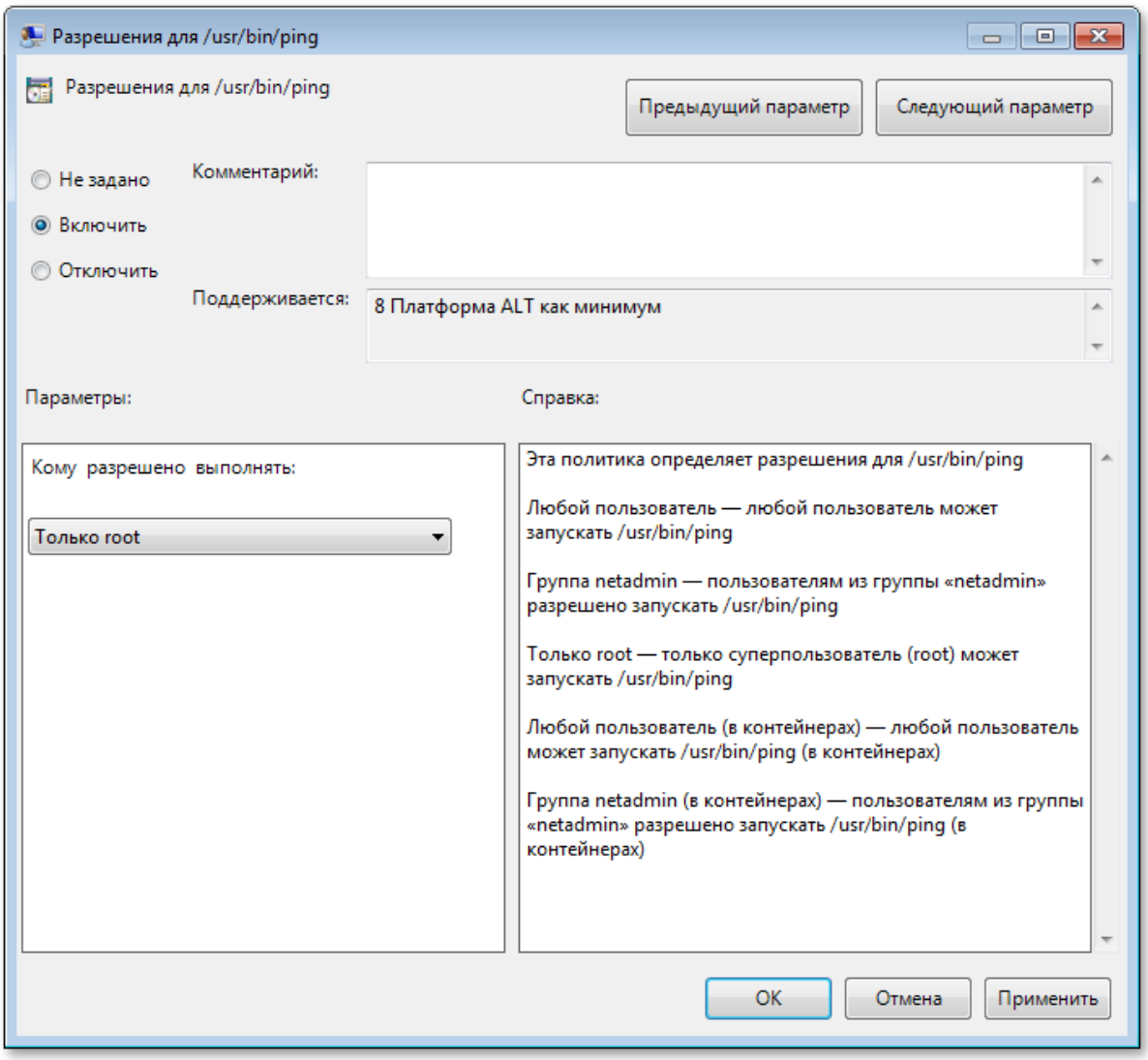
2. Создать новый объект групповой политики (GPO) и связать его с подразделением (OU), в который входят машины или учетные записи пользователей.

3. В контекстном меню GPO, выбрать пункт **Изменить…**. Откроется редактор GPO.

4. Перейти в **Конфигурация компьютера** → **Политики** → **Административные шаблоны** → **Система ALT**. Здесь есть несколько разделов, соответствующих категориям control. Выбрать раздел **`Сетевые приложения`**, в правом окне редактора отобразится список политик:



5. Дважды щелкнуть левой кнопкой мыши на политике **`Разрешения для /usr/bin/ping`**. Откроется диалоговое окно настройки политики. Выбрать параметр **`Включить`**, в выпадающем списке **`Кому разрешено выполнять`** выбрать пункт **Только root** и нажать кнопку **`Применить`**:



Важно

Для диагностики механизмов применения групповых политик на клиенте можно выполнить команду:

```
# gpoa --loglevel 0
```

В выводе команды будут фигурировать полученные групповые объекты. В частности, соответствующий уникальный код (GUID) объекта.

Глава 40. Samba в режиме файлового сервера

Samba — пакет программ, которые позволяют обращаться к сетевым дискам и принтерам на различных операционных системах по протоколу SMB/CIFS. Имеет клиентскую и серверную части.

40.1. Настройка smb.conf

Примечание

После редактирования файла **/etc/samba/smb.conf**, следует запустить команду **testparm** для проверки файла на синтаксические ошибки:

```
# testparm /etc/samba/smb.conf
```

И, в случае отсутствия ошибок, перезапустить службы smb и nmb, чтобы изменения вступили в силу:

```
# systemctl restart smb
# systemctl restart nmb
```

Каждый раздел в файле конфигурации (кроме раздела [global]) описывает общий ресурс. Название раздела — это имя общего ресурса. Параметры в разделе определяют свойства общего ресурса.

Общий ресурс состоит из каталога, к которому предоставляется доступ, а также описания прав доступа, которые предоставляются пользователю.

Разделы — это либо общие файловые ресурсы, либо службы печати. Разделам может быть назначен гостевой доступ, в этом случае для доступа к ним не требуется пароль (для определения прав доступа используется специальная гостевая учетная запись). Для доступа к разделам, к которым запрещен гостевой доступ, потребуется пароль.

Примечание

Samba использует отдельную от системной базу данных пользователей. Для возможности доступа пользователя к папке (если запрещен гостевой доступ) необходимо внести его в базу данных Samba и установить пароль для доступа к общим ресурсам (он может совпадать с основным паролем пользователя). Следует учитывать, что в базу данных Samba можно добавлять только тех пользователей, которые уже есть в системе.

Добавить пользователя в базу данных Samba можно, выполнив команду (должен быть установлен пакет *samba-common-client*):

```
# smbpasswd -a <имя_пользователя>
```

В файле конфигурации есть три специальных раздела: [global], [homes] и [printers]:

Раздел [global]

Параметры в этом разделе применяются к серверу в целом или являются значениями по умолчанию для разделов, и могут быть переопределены в разделе.

Раздел [homes]

Используется для подключения домашних каталогов пользователей. При каждом обращении Samba сначала ищет имя запрошенного ресурса в списке общих ресурсов, и если имя не найдено проверяет наличие в конфигурации секции [homes]. Если такая секция есть, то имя трактуется как имя пользователя, и проверяется по базе данных пользователей сервера Samba. Если имя найдено в базе данных пользователей, то Samba предоставляет в качестве общего ресурса домашний каталог этого пользователя. Аналогичный процесс происходит, если имя запрошенного ресурса — «homes», за исключением того, что имя общего ресурса меняется на имя запрашивающего пользователя.

Раздел [printers]

Если в файле конфигурации имеется раздел [printers], пользователи могут подключаться к любому принтеру, указанному в файле printcap локального хоста.

Примечание

В одноранговой сети (т.е. если Samba используется исключительно как файловый сервер, а не как контроллер домена) для возможности использования файлового ресурса [homes], необходимо добавить каждого локального пользователя в список пользователей Samba, например:

```
# smbpasswd -a user
New SMB password:
Retype new SMB password:
Added user user.
```

Примечание

Если в разделе [homes] указан гостевой доступ (guest ok = yes), все домашние каталоги будут видны всем клиентам без пароля. Если это действительно нужно (хотя маловероятно), разумно также указать доступ только для чтения (read only = yes).

Примечание

Флаг ***browseable*** для домашних каталогов будет унаследован от глобального флага ***browseable***, а не флага ***browseable*** раздела [homes]. Таким образом, установка browseable = no в разделе [homes] скроет общий ресурс [homes], но сделает видимыми все автоматические домашние каталоги.

Описание некоторых параметров:

- ***browseable*** — определяет, отображается ли этот общий ресурс в списке доступных общих ресурсов в сетевом окружении и в списке просмотра (по умолчанию: browseable = yes);
- ***path*** — указывает каталог, к которому должен быть предоставлен доступ;
- ***read only*** — если для этого параметра задано значение «yes», то пользователи службы не могут создавать или изменять файлы в каталоге (по умолчанию: read only = yes);

- ***writable*** — инвертированный синоним для ***read only*** (по умолчанию: writeable = no);
- ***write list*** — список пользователей, которым будет предоставлен доступ для чтения и записи. Если пользователь находится в этом списке, ему будет предоставлен доступ для записи, независимо от того, какой параметр установлен для параметра ***read only***. Список может включать имена групп с использованием синтаксиса @group;
- ***read list*** — список пользователей, которым будет предоставлен доступ только для чтения. Если пользователь находится в этом списке, ему не будет предоставлен доступ для записи, независимо от того, какой параметр установлен для параметра ***read only***. Список может включать имена групп;
- ***guest ok*** — если этот параметр имеет значение «yes», то для подключения к ресурсу не требуется пароль (по умолчанию: guest ok = no);
- ***guest only*** — разрешить только гостевые соединения к общему ресурсу (по умолчанию: guest only = no);
- ***printable*** — если этот параметр имеет значение «yes», то клиенты могут открывать, писать и ставить задания в очередь печати (по умолчанию: printable = no);
- ***map to guest*** — определяет что делать с запросами, которые не удалось аутентифицировать («Never» — запросы с неправильными паролями будут отклонены; «Bad user» — запросы с неправильными паролями будут отклонены, если такое имя пользователя существует;) (по умолчанию: map to guest = Never).

Пример настройки **/etc/samba/smb.conf** для работы Samba в режиме файлового сервера с двумя открытыми для общего доступа ресурсами, домашними каталогами пользователей и принтером (закомментированные параметры действуют по умолчанию):

```
[global]
    workgroup = WORKGROUP
    server string = Samba Server Version %v
    security = user
    log file = /var/log/samba/log.%m
    max log size = 50
    guest ok = yes
    cups options = raw
    map to guest = Bad User
;   idmap config * : backend = tdb

[homes]
    comment = Home Directory for '%u'
    browseable = no
    writable = yes
    guest ok = no

[share]
    comment = Commonplace
    path = /srv/share
    read only = No

[printers]
    comment = All Printers
    path = /var/spool/samba
    browseable = no
;   guest ok = no
;   writable = no
```

```
    printable = yes

# Каталог доступный только для чтения, за исключением пользователей
# входящих в группу "staff"
[public]
    comment = Public Stuff
    path = /home/samba
    public = yes
    writable = yes
    write list = +staff
;   browseable = yes

[Free]
    path = /mnt/win/Free
    read only = no
;   browseable = yes
    guest ok = yes
```

Просмотр ресурсов, доступных пользователю user:

```
# smbclient -L 192.168.0.157 -Uuser
Password for [WORKGROUP\user]:

        Sharename       Type      Comment
        ---------       ----      -------
        share           Disk      Commonplace
        public          Disk      Public Stuff
        Free            Disk
        IPC$            IPC       IPC Service (Samba Server Version 4.19.4)
        user            Disk      Home Directory for 'user'
```

Обращение к домашней папке пользователя выполняется по имени пользователя (например, smb://192.168.0.157/user).

Примечание

Для ознакомления с прочими возможностями, читайте руководство по smb.conf. Для этого используйте команду **man smb.conf**.

40.2. Монтирование ресурса Samba через /etc/fstab

Создать файл **/etc/samba/sambacreds** (например, командой **mcedit /etc/samba/sambacreds**), с содержимым:

```
username=имя_пользователя
password=пароль
```

Для монтирования ресурса Samba в **/etc/fstab** необходимо прописать:

```
//server/public /mnt/server_public cifs users,credentials=/etc/samba/sambacreds 0
0
```

Для защиты информации, права на файл **/etc/samba/sambacreds**, надо установить так, чтобы файл был доступен только владельцу:

```
# chmod 600 /etc/samba/sambacreds
```

и принадлежать root:

```
# chown root: /etc/samba/sambacreds
```

Глава 41. Система мониторинга Zabbix

Zabbix — система мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования.

Для управления системой мониторинга и чтения данных используется веб-интерфейс.

41.1. Установка сервера PostgreSQL

Перед установкой Zabbix должен быть установлен и запущен сервер PostgreSQL, с созданным пользователем zabbix и созданной базой zabbix.

Установить PostgreSQL, Zabbix-сервер и дополнительную утилиту **fping**:

```
# apt-get install postgresql14-server zabbix-server-pgsql fping
```

Подготовить к запуску и настроить службы PostgreSQL, для этого необходимо выполнить следующие действия:

- создать системные базы данных:

  ```
  # /etc/init.d/postgresql initdb
  ```

- включить по умолчанию и запустить службу:

  ```
  # systemctl enable --now postgresql
  ```

- создать пользователя zabbix и базу данных zabbix (под правами root):

```
# su - postgres -s /bin/sh -c 'createuser --no-superuser --no-createdb --no-
createrole --encrypted --pwprompt zabbix'
# su - postgres -s /bin/sh -c 'createdb -O zabbix zabbix'
# systemctl restart postgresql
```

- добавить в базу данные для веб-интерфейса (последовательность команд важна, в разных версиях Zabbix путь будет отличаться, версия помечена звёздочкой):

```
# su - postgres -s /bin/sh -c 'psql -U zabbix -f /usr/share/doc/zabbix-common-
database-pgsql-*/schema.sql zabbix'
# su - postgres -s /bin/sh -c 'psql -U zabbix -f /usr/share/doc/zabbix-common-
database-pgsql-*/images.sql zabbix'
# su - postgres -s /bin/sh -c 'psql -U zabbix -f /usr/share/doc/zabbix-common-
database-pgsql-*/data.sql zabbix'
```

41.2. Установка Apache2

Установить пакеты apache2:

```
# apt-get install apache2 apache2-mod_php8.2
```

Добавить в автозапуск и запустить apache2:

```
# systemctl enable --now httpd2
```

41.3. Установка PHP

Примечание

Начиная с версии php8.0, пакеты модулей именуются следующим образом:

```
php<мажорная>.<минорная версии>-<имя модуля>
```

Из репозитория можно установить и эксплуатировать в одной системе одновременно разные версии php. В данном руководстве в качестве примера используется php8.2.

Установить необходимые пакеты:

```
# apt-get install php8.2 php8.2-mbstring php8.2-sockets php8.2-gd php8.2-
xmlreader php8.2-pgsql php8.2-ldap php8.2-openssl
```

Изменить некоторые опции php в файле **/etc/php/8.2/apache2-mod_php/php.ini**:

```
memory_limit = 256M
post_max_size = 32M
max_execution_time = 600
max_input_time = 600
date.timezone = Europe/Moscow
always_populate_raw_post_data = -1
```

Перезапустить apache2:

```
# systemctl restart httpd2
```

41.4. Настройка и запуск Zabbix-сервера

Внести изменения в конфигурационный файл **`/etc/zabbix/zabbix_server.conf`**:

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=Пароль от базы
```

Добавить Zabbix-сервер в автозапуск и запустить его:

```
# systemctl enable --now zabbix_pgsql
```

41.5. Установка веб-интерфейса Zabbix

Установить метапакеты (из репозитория):

```
# apt-get install zabbix-phpfrontend-apache2 zabbix-phpfrontend-php8.2
```

Включить аддоны в apache2:

```
# ln -s /etc/httpd2/conf/addon.d/A.zabbix.conf /etc/httpd2/conf/extra-enabled/
```

Перезапустить apache2:

```
# systemctl restart httpd2
```

Изменить права доступа к конфигурационному каталогу веб-интерфейса, чтобы веб-установщик мог записать конфигурационный файл:

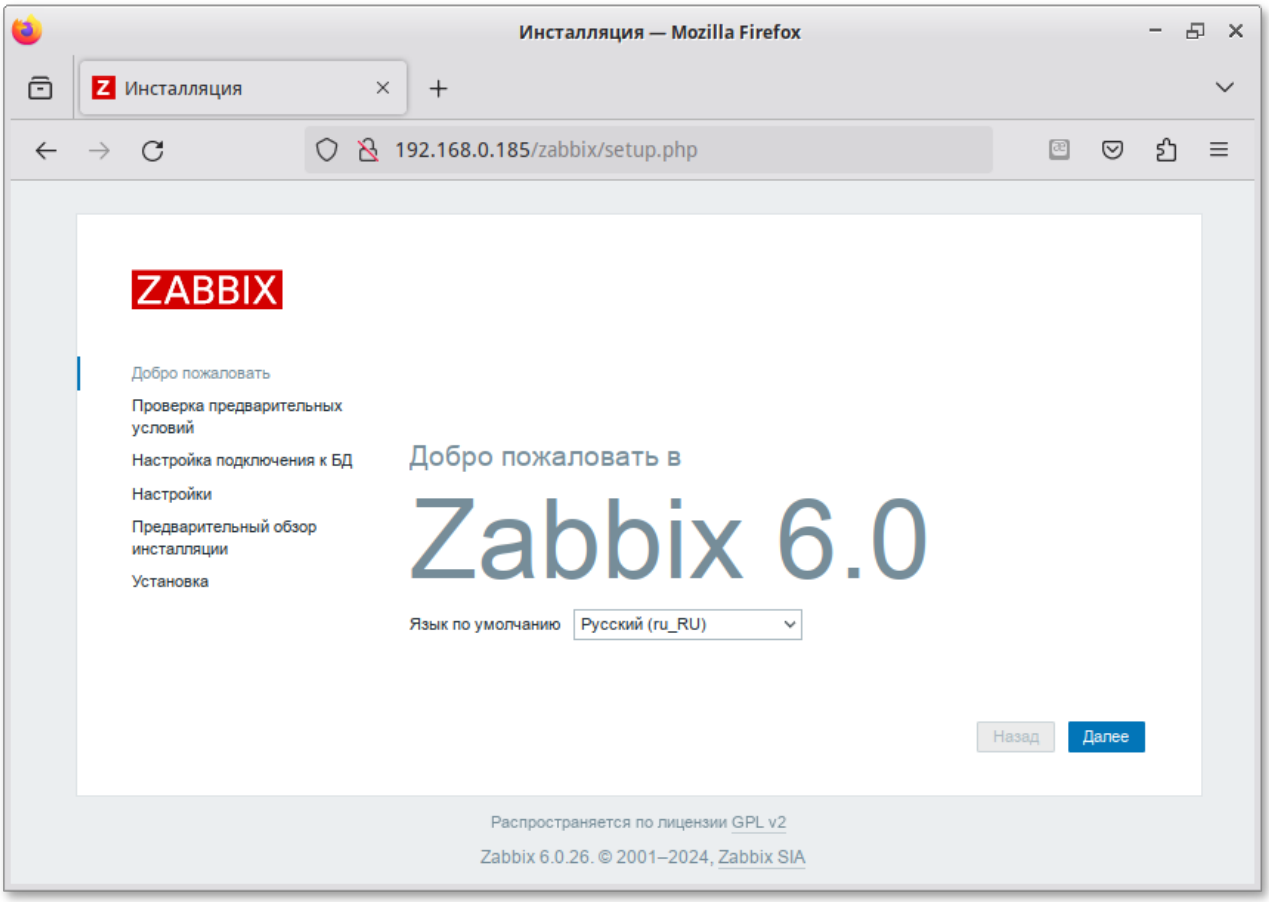
```
# chown apache2:apache2 /var/www/webapps/zabbix/ui/conf
```

В браузере перейти на страницу установки Zabbix сервера:

```
http://<ip-сервера>/zabbix
```

При первом заходе на страницу запустится мастер, который шаг за шагом проверит возможности веб-сервера, интерпретатора PHP и сконфигурирует подключение к базе данных.

На странице также можно выбрать язык установки Zabbix.



Примечание

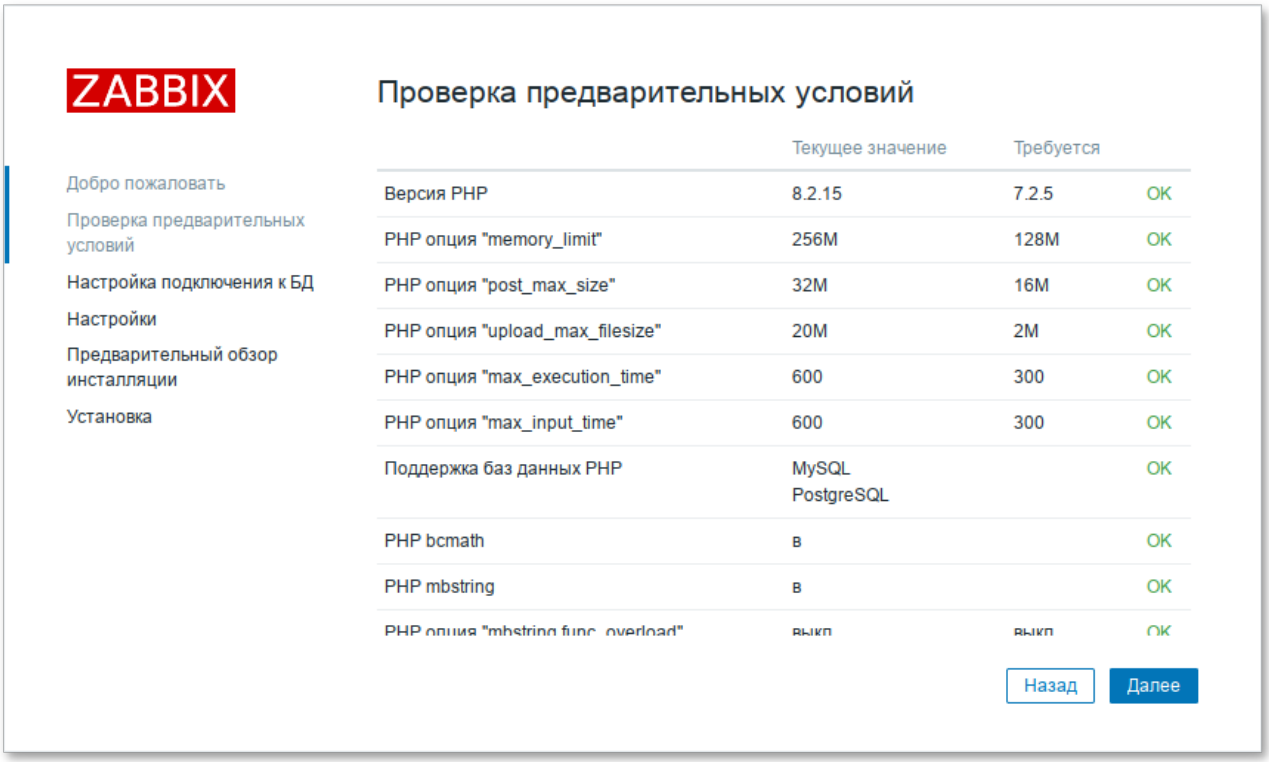
Если при входе на страницу http://<ip-сервера>/zabbix появляется ошибка: доступ запрещен, следует в файле **`/etc/httpd2/conf/sites-available/default.conf`** в секцию <Directory> добавить запись:

```
Require all granted
```

и перезапустить apache2:

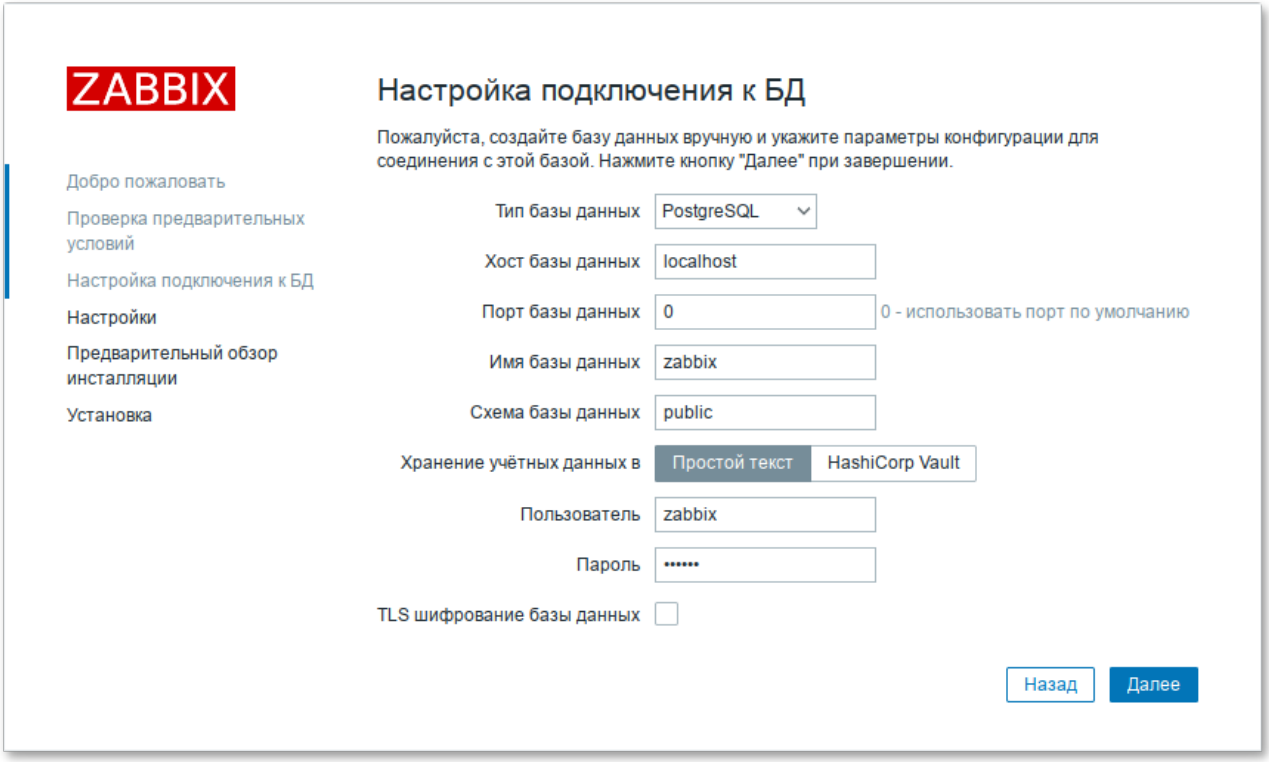
```
# systemctl restart httpd2
```

Для начала установки необходимо нажать кнопку **Далее**, что осуществит переход на страницу проверки предварительных условий.



Необходимо доустановить то, что требуется и перейти на следующую страницу.

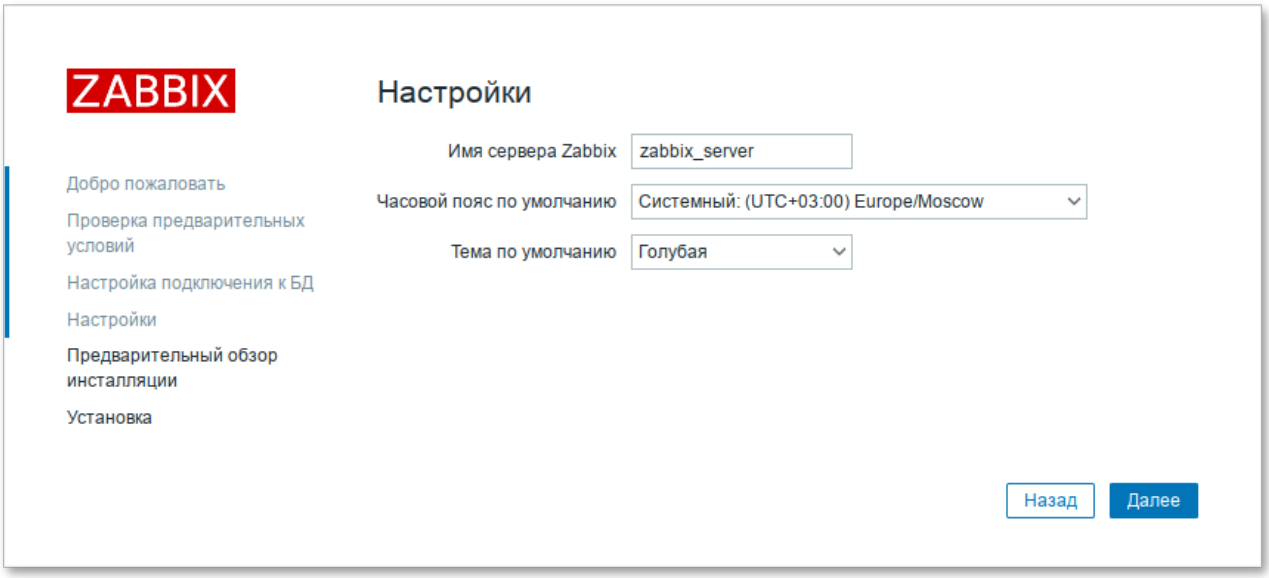
Здесь необходимо ввести параметры подключения к базе данных (параметры подключения нужно указывать такие же, как у сервера Zabbix). По умолчанию в качестве Database schema необходимо указать *public*.



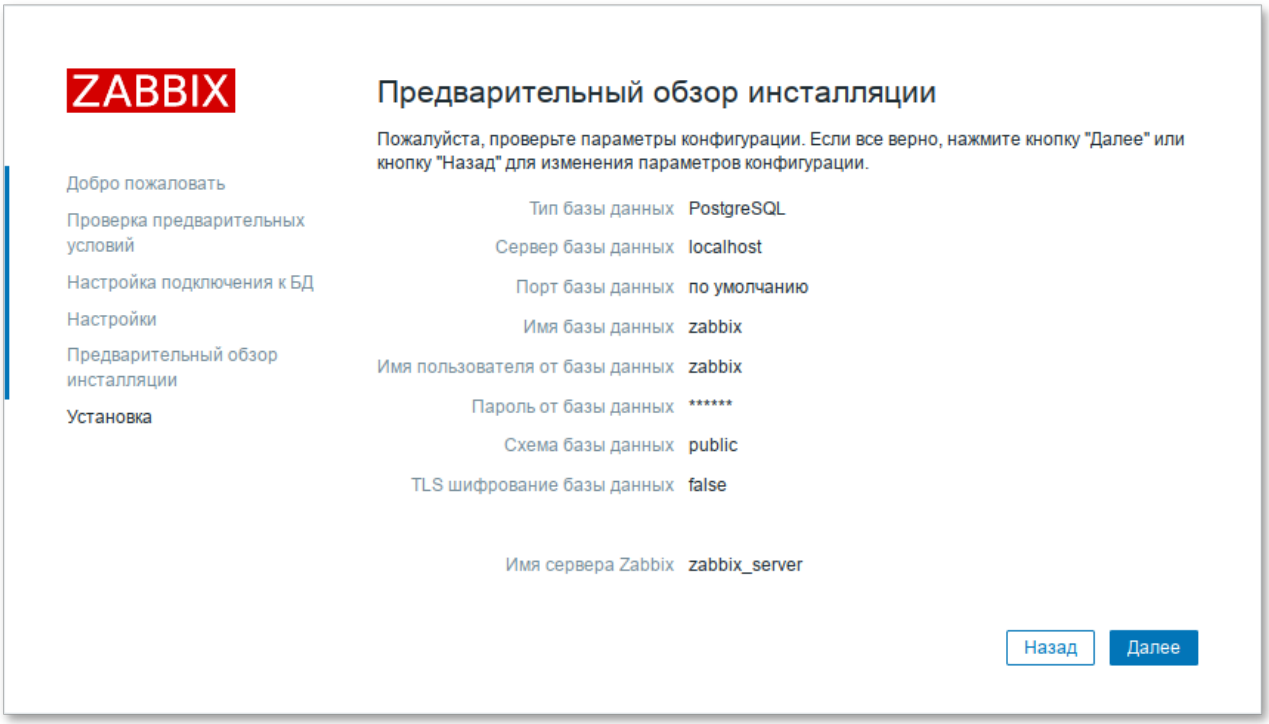
Примечание

Если выбрана опция **TLS шифрование базы данных**, то в форме появятся дополнительные поля для настройки TLS-соединения с базой данных.

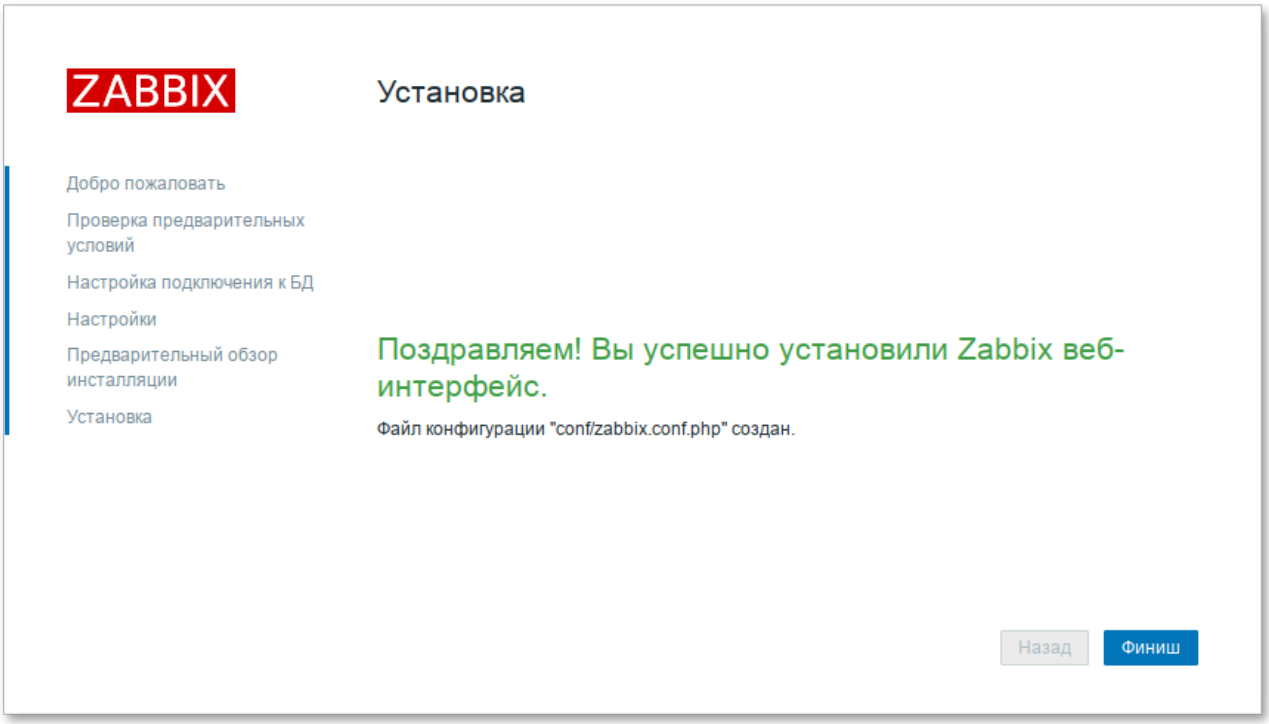
Далее необходимо задать имя сервера и выбрать настройки веб-интерфейса:



На следующей странице следует проверить параметры конфигурации:

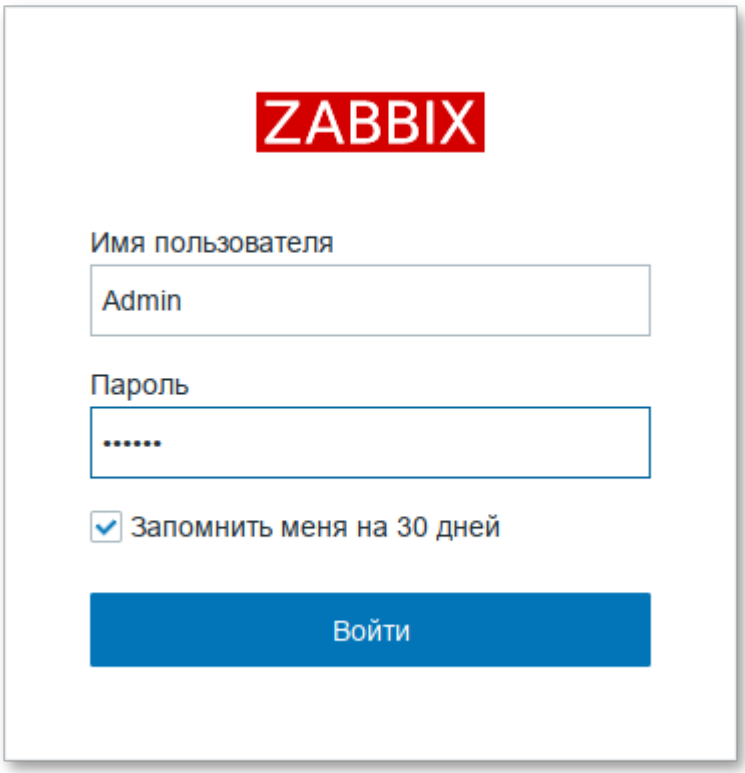


Окончание установки:

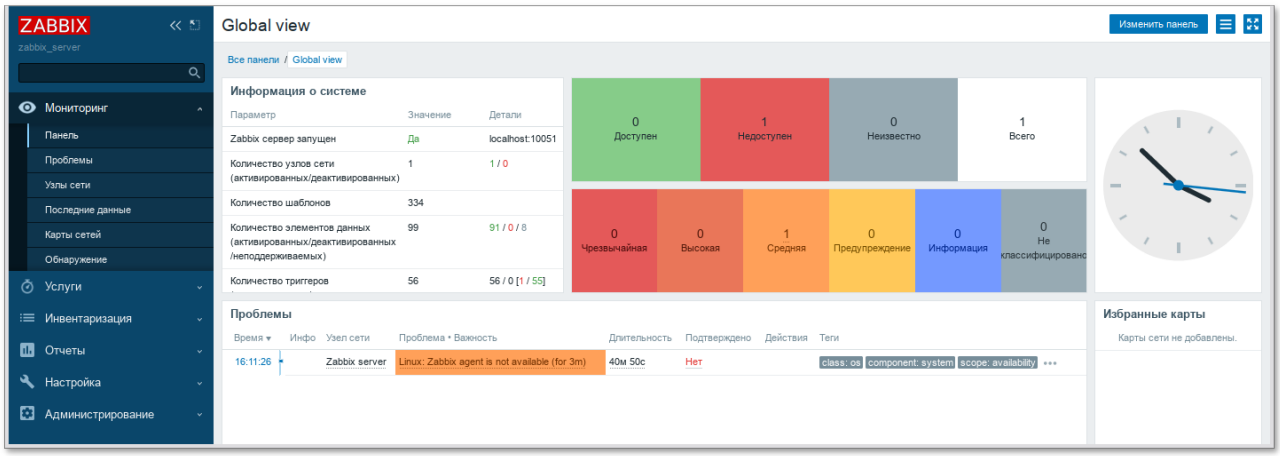


После окончания установки на экране будет отображаться форма входа в интерфейс управления системой мониторинга. Параметры доступа по умолчанию:

```
Логин: Admin
Пароль: zabbix
```

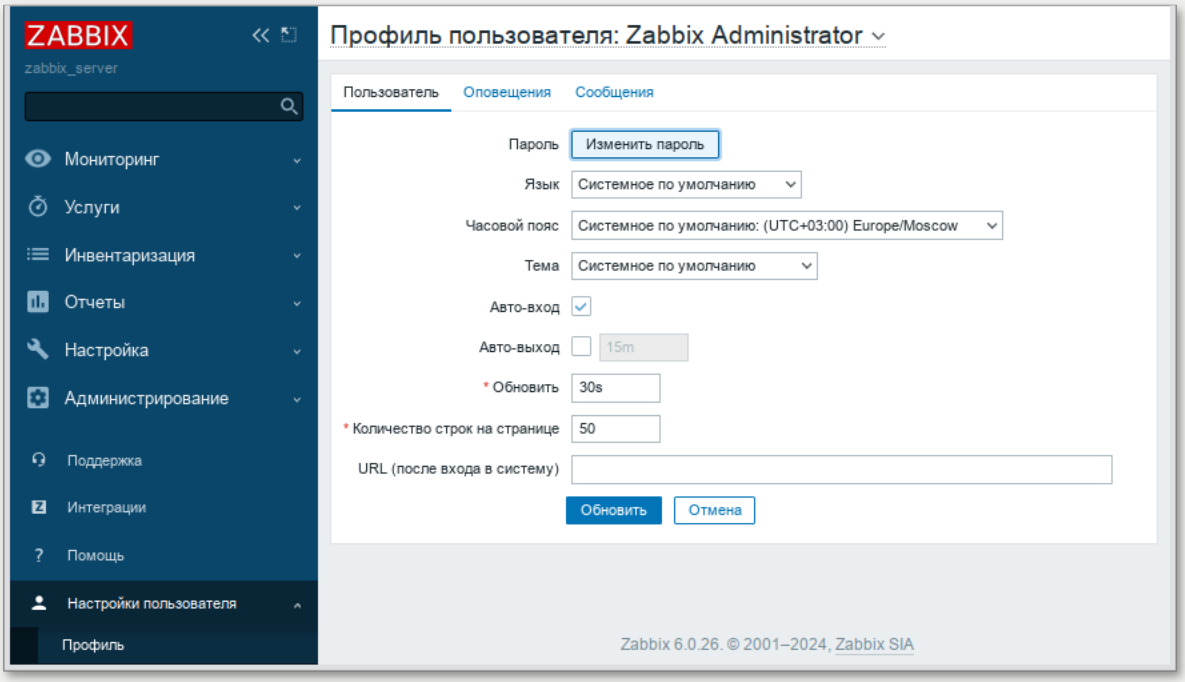


Войдя в систему, нужно сменить пароль пользователя, завести других пользователей и можно начать настраивать Zabbix.



Примечание

В профиле пользователя можно настроить некоторые функции веб-интерфейса Zabbix, такие как язык интерфейса, цветовая тема, количество отображаемых строк в списках и т.п. Сделанные в профиле изменения будут применены только к пользователю, в профиле которого были сделаны эти изменения.



Чтобы собирать информацию с узлов, сервер Zabbix использует информацию, получаемую от агентов. Чтобы добавить новый узел, следует установить на узел, который необходимо мониторить, Zabbix-агент и добавить новый хост на Zabbix-сервере.

41.6. Установка клиента Zabbix

Установить необходимый пакет *zabbix-agent* (из репозитория):

```
# apt-get install zabbix-agent
```

Если Zabbix-агент устанавливается не на сам сервер мониторинга, то в файле конфигурации агента **`/etc/zabbix/zabbix_agentd.conf`** нужно задать следующие параметры:

```
Server=<ip-сервера>
ServerActive=<ip-сервера>
Hostname=comp01.example.test
```

comp01.example.test — имя узла мониторинга, которое будет указано на сервере Zabbix.

Примечание

Если параметр **Hostname** будет пустой или закомментирован, то узел добавится под системным именем.

Добавить Zabbix-агент в автозапуск и запустить его:

```
# systemctl enable --now zabbix_agentd.service
```

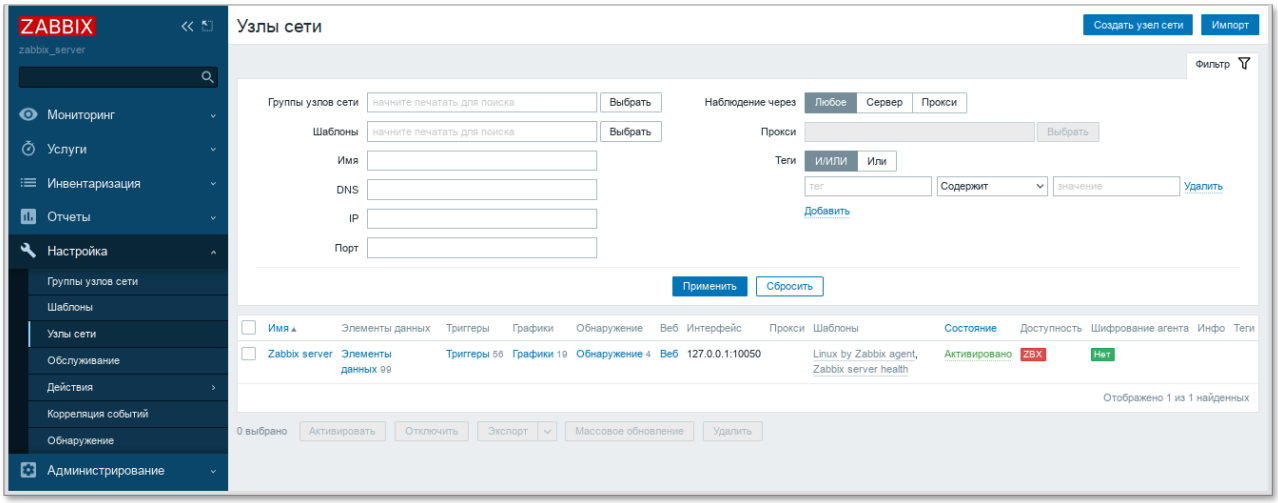
Примечание

Для настройки Zabbix-агента можно воспользоваться модулем Агент наблюдения.

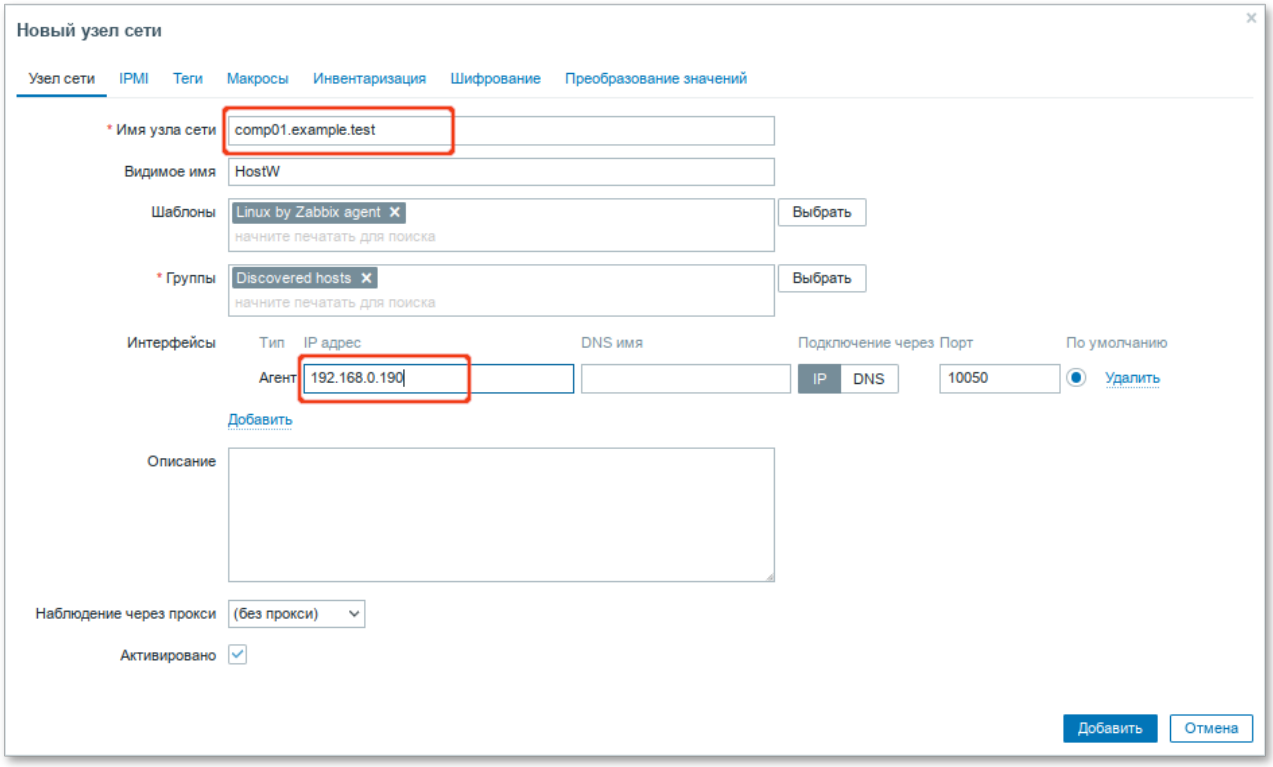
41.7. Добавление нового хоста на сервер Zabbix

Каждый хост необходимо зарегистрировать на сервере Zabbix.

Информация о настроенных узлах сети в Zabbix доступна в разделе **Настройка** → **Узлы сети**. Для добавления нового узла сети следует нажать кнопку **Создать узел сети**:



В открывшемся окне необходимо заполнить поля **Имя узла сети** и **IP адрес** согласно данным добавляемого хоста, выбрать шаблон **Linux by Zabbix agent**, добавить хост в определенную группу (выбрав одну из них из списка, либо создав новую группу) и нажать кнопку **Добавить**:



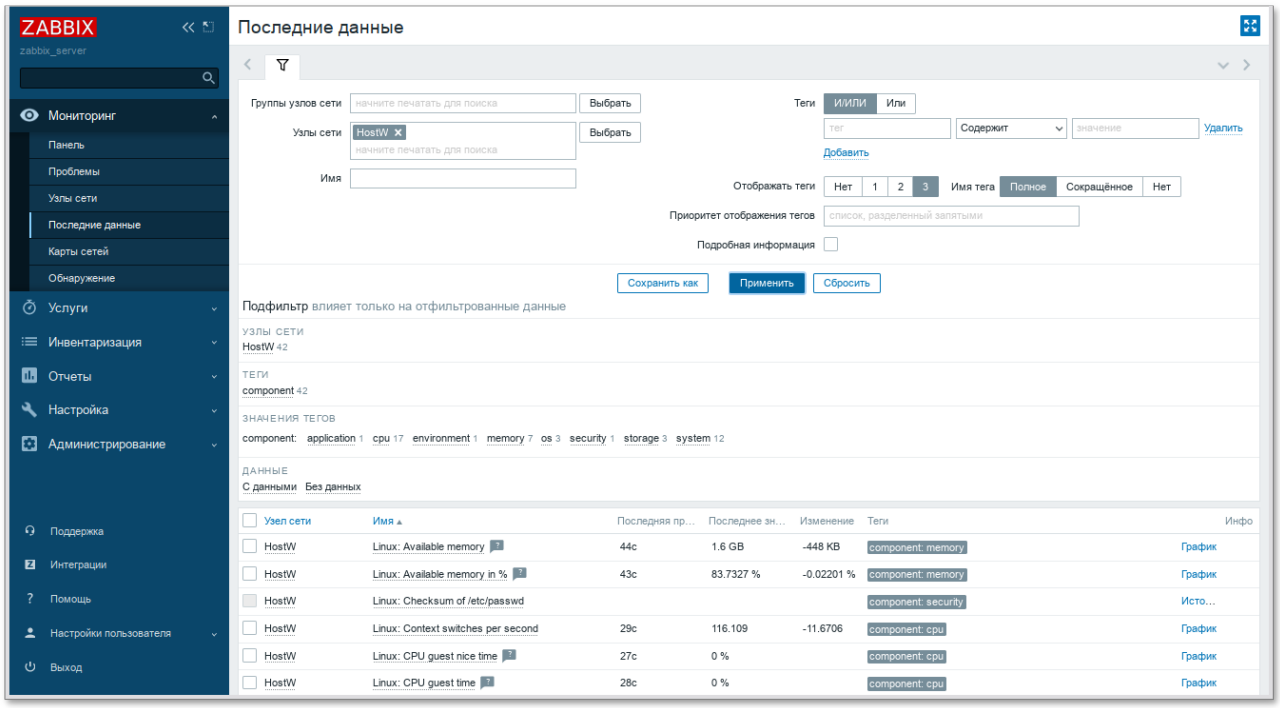
Примечание

В поле **`Имя узла сети`** ставится значение, которое указано в настройках агента (**`/etc/zabbix/zabbix_agentd.conf`**) в поле **`Hostname`**.

Примечание

Все права доступа назначаются на группы узлов сети, не индивидуально узлам сети. Поэтому узел сети должен принадлежать хотя бы одной группе.

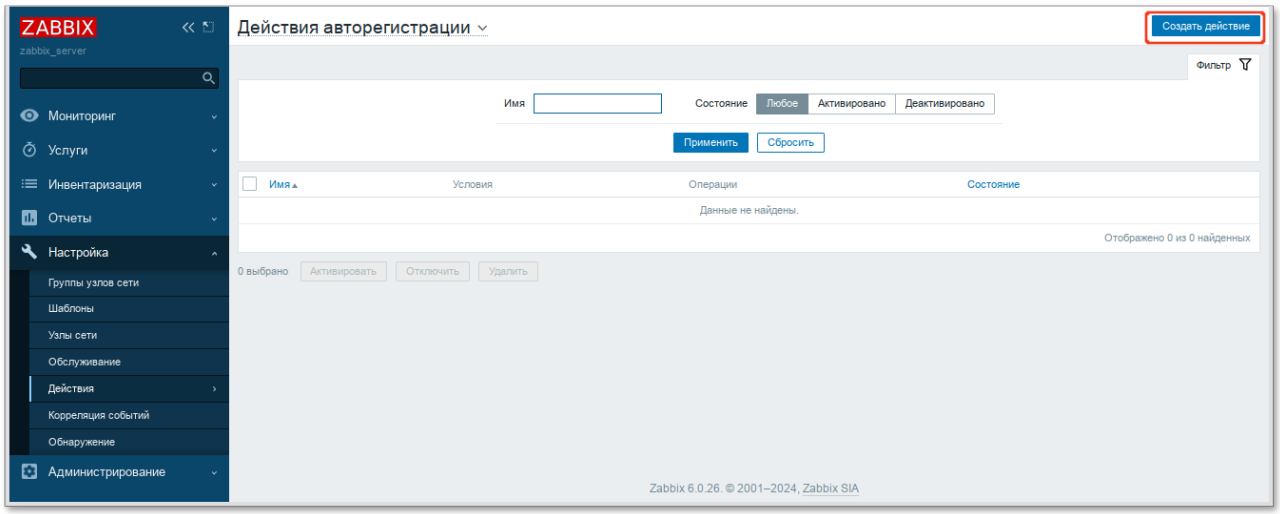
Получение первых данных может занять до 60 секунд. Для того чтобы просмотреть собранные данные, необходимо перейти в **Мониторинг** → **Последние данные**, выбрать в фильтре нужный узел сети и нажать кнопку **`Применить`**:



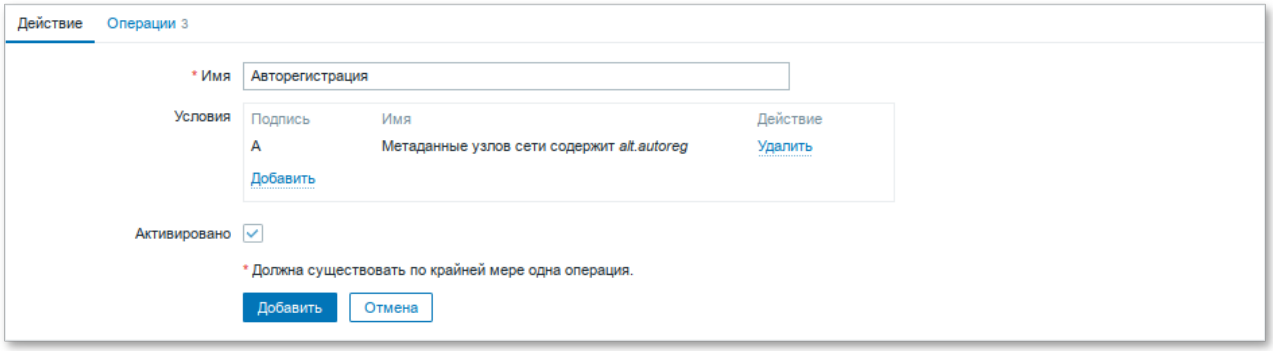
41.8. Авторегистрация узлов

В Zabbix существует механизм, который позволяет Zabbix-серверу начинать мониторинг нового оборудования автоматически, если на этом оборудовании имеется установленный Zabbix-агент. Такой подход позволяет добавлять новые узлы сети на мониторинг без какой-либо настройки Zabbix-сервера вручную по каждому отдельному узлу сети.

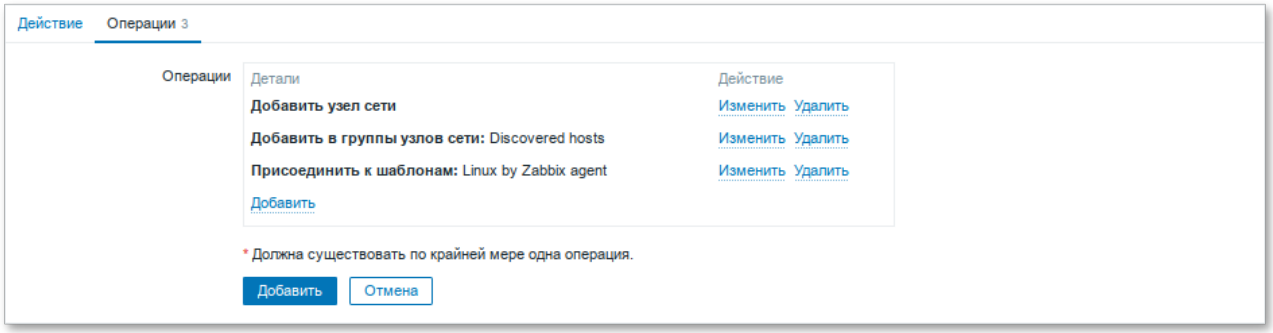
Для настройки авторегистрации необходимо перейти в **Настройка** → **Действия** → **Действия авторегистрации** и нажать кнопку **`Создать действие`**:



На открывшейся странице, на вкладке **Действия** заполнить поле **`Имя`** и добавить условия. В поле **`Условия`** следует задать правила, по которым будут идентифицироваться регистрируемые хосты:



На вкладке **Операции** в поле **Операции** следует добавить правила, которые необходимо применить при регистрации хоста. Пример правил для регистрации узла, добавления его к группе **Discovered hosts** с присоединением к шаблону **Linux by Zabbix agent**:



В конфигурационном файле агента указать следующие значения:

- в параметре **Hostname** — уникальное имя;
- в параметре **ServerActive** — IP-адрес сервера;
- в параметре **HostMetadata** — значение, которое было указано в настройках сервера (HostMetadata=alt.autoreg).

Перезапустить агент.

Глава 42. Nextcloud — хранение документов в «облаке»

Nextcloud — веб-приложение для синхронизации данных, общего доступа к файлам и удалённого хранения документов в «облаке».

Файлы Nextcloud хранятся в обычных структурах каталогов и могут быть доступны через WebDAV, если это необходимо.

Основной сайт проекта: https://nextcloud.com/.

42.1. Установка

Развернуть Nextcloud можно, используя пакет *deploy*:

```
# apt-get install deploy
# deploy nextcloud
```

Примечание

Nextcloud можно установить при установке системы, выбрав для установки пункт **Сервер Nextcloud** (подробнее описано в главе Установка системы).

Если при установке системы доступ к сети отсутствует, то Nextcloud не будет развёрнут. В этом случае развернуть Nextcloud можно, выполнив команду:

```
# deploy nextcloud
```

Для доступа к административным функциям Nextcloud через веб-интерфейс необходимо установить пароль пользователю ncadmin (пароль должен быть достаточно сложным и содержать не менее 10 символов):

```
# deploy nextcloud password=5Z4SAq2U28rWyVz
```

Веб-приложение Nextcloud будет доступно по адресу **https://<сервер>/nextcloud/**. Где «сервер» — localhost или имя, заданное компьютеру при установке системы на этапе Настройка сети.

Примечание

Просмотреть имя компьютера можно, выполнив команду:

```
$ hostname
```

Важно

По умолчанию непоследовательное обновление мажорных версий запрещено (например, с версии 20 сразу до 22), и при попытке доступа к веб-интерфейсу после обновления пакета будет возникать ошибка **Exception: Updates between multiple major versions and downgrades are unsupported**. Для того чтобы обойти эту ошибку, продолжить обновление и получить доступ к веб-интерфейсу, необходимо:

- в файле **/var/www/webapps/nextcloud/config/config.php** в параметре ***version*** изменить старую версию на новую;
- перейти в веб-интерфейс и обновить страницу.

42.2. Настройка Nextcloud

/var/www/webapps/nextcloud/config/config.php — файл конфигурации Nextcloud.

Важно

После внесения изменений в файл конфигурации Nextcloud необходимо перезапустить веб-сервер:

```
# systemctl restart httpd2
```

Настроить кэширование можно, добавив следующие строки в файл конфигурации Nextcloud:

```
'memcache.local' => '\OC\Memcache\Memcached',
'memcache.distributed' => '\OC\Memcache\Memcached',
'memcached_servers' => array(
 array('localhost', 11211),
 ),
```

Примечание

Для возможности настройки кэширования, должны быть установлены пакеты *memcached*, *php8.2-memcached*:

```
# apt-get install memcached php8.2-memcached
```

Служба memcached должна быть добавлена в автозагрузку:

```
# systemctl enable --now memcached
```

После установки Nextcloud отвечает на запросы, сделанные только из localhost. Поэтому необходимо изменить настройки для того, чтобы получить доступ к Nextcloud при использовании доменного имени или IP-адреса сервера. Для этого следует добавить в файл конфигурации в раздел trusted_domains необходимые имена сервера:

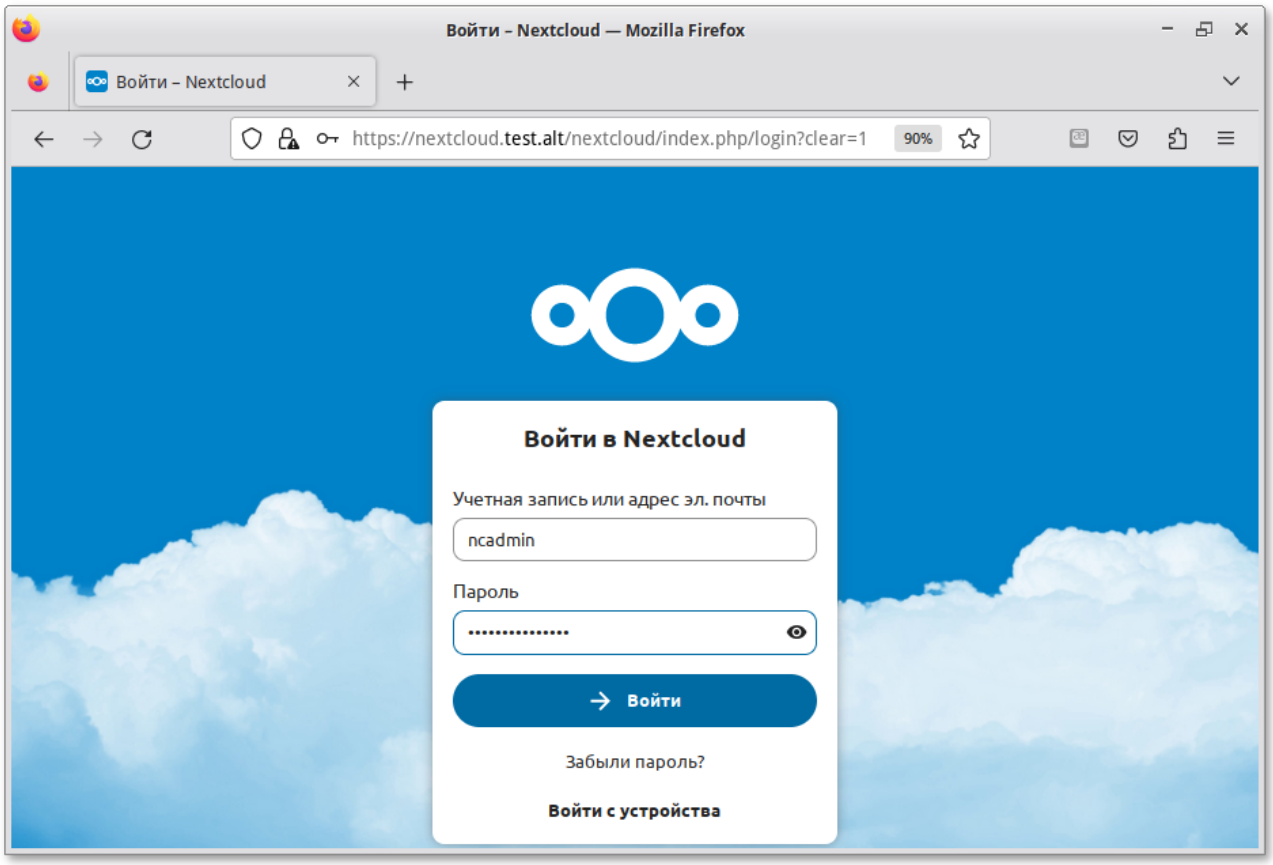
```
'trusted_domains' =>
array (
0 => 'localhost',
1 => 'host-15',
2 => 'nextcloud.test.alt',
),
```

42.3. Работа с Nextcloud

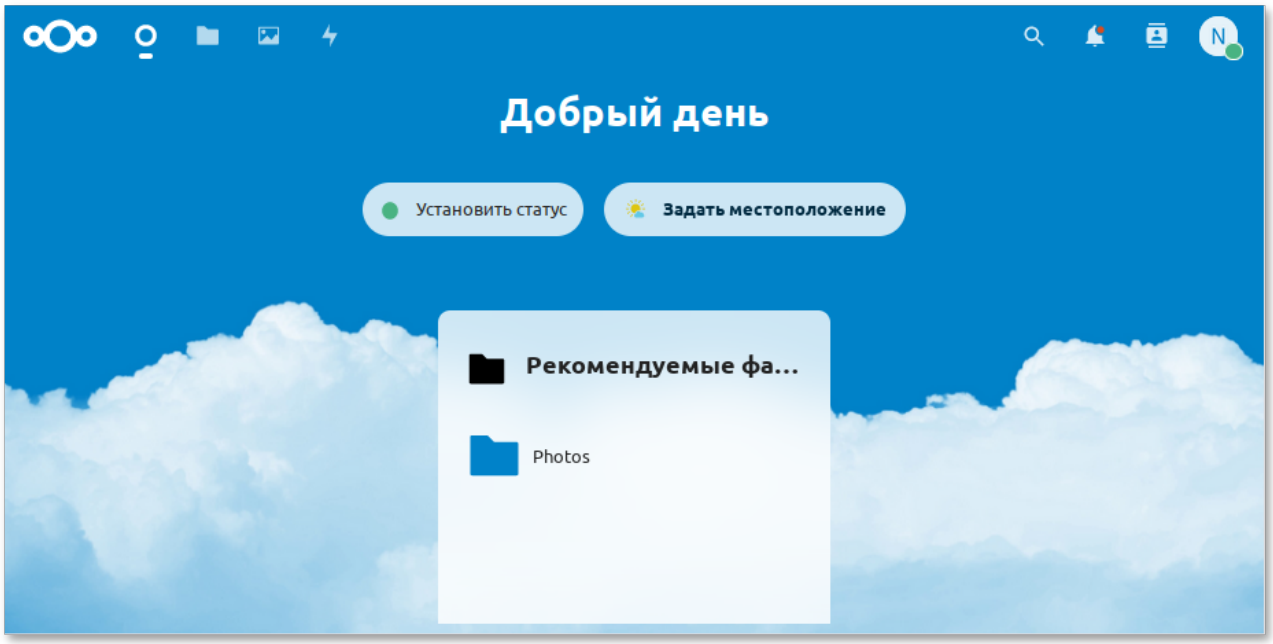
Nextcloud доступен через веб-интерфейс по адресу **https://localhost/nextcloud/** или по имени сервера **https://nextcloud.test.alt/nextcloud/**.

Примечание

Если используется самоподписанный сертификат, то на клиентских машинах потребуется добавлять его в список доверенных.

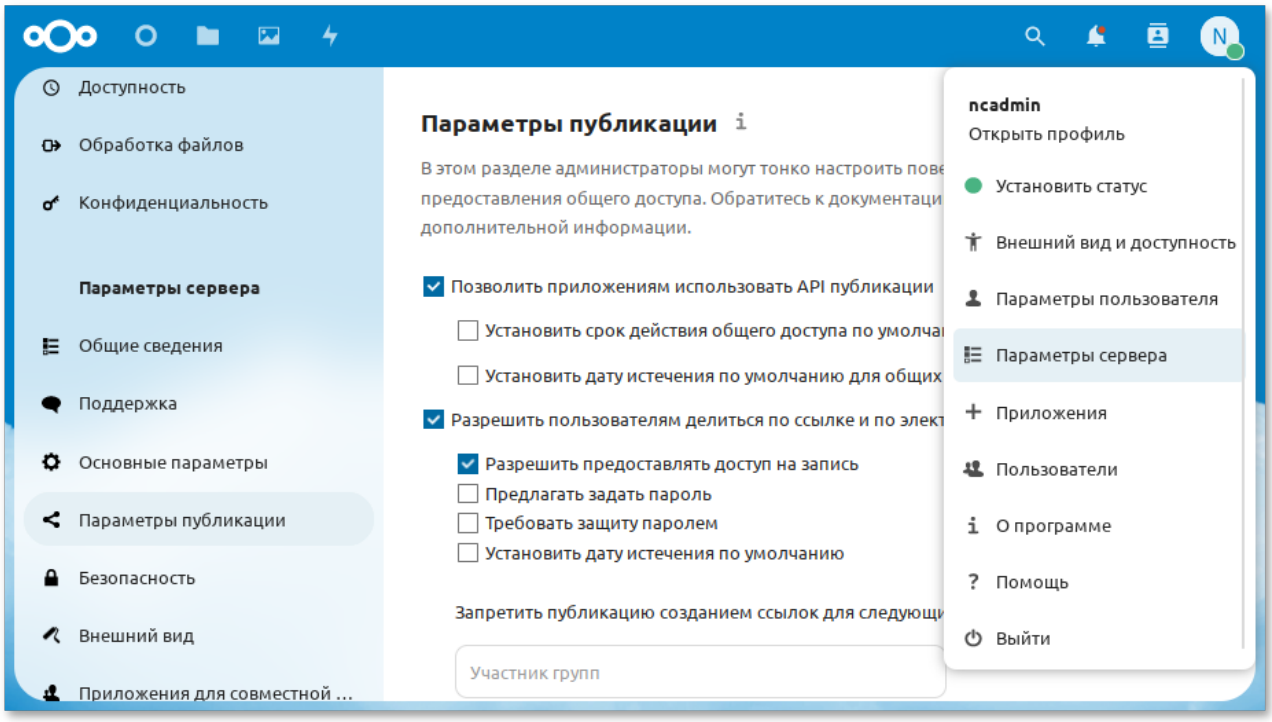


После авторизации открывается панель управления Nextcloud, которую можно настроить (с помощью виджетов) так, как хочет пользователь:



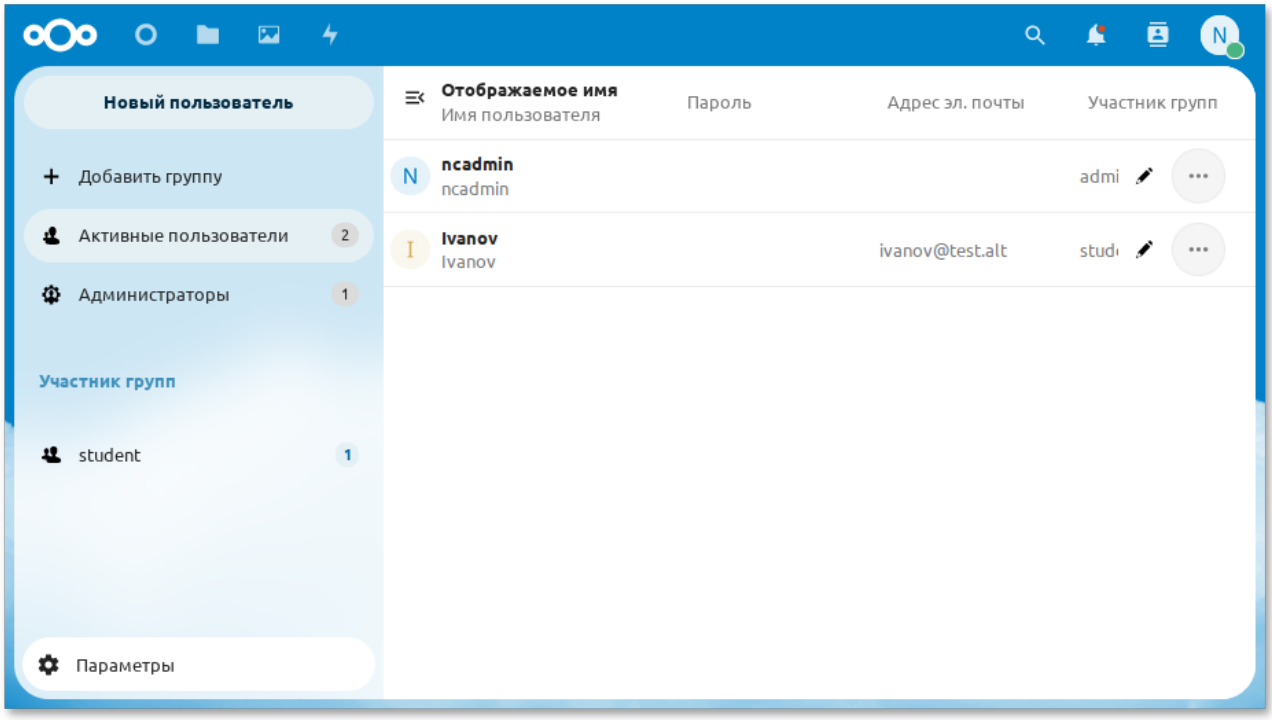
42.3.1. Администрирование

Основные настройки Nextcloud доступны на странице **Параметры сервера**. Открыть которую можно, щелкнув левой кнопкой мыши по логину администратора в правом верхнем углу и выбрав в выпадающем меню строку **Параметры сервера**:

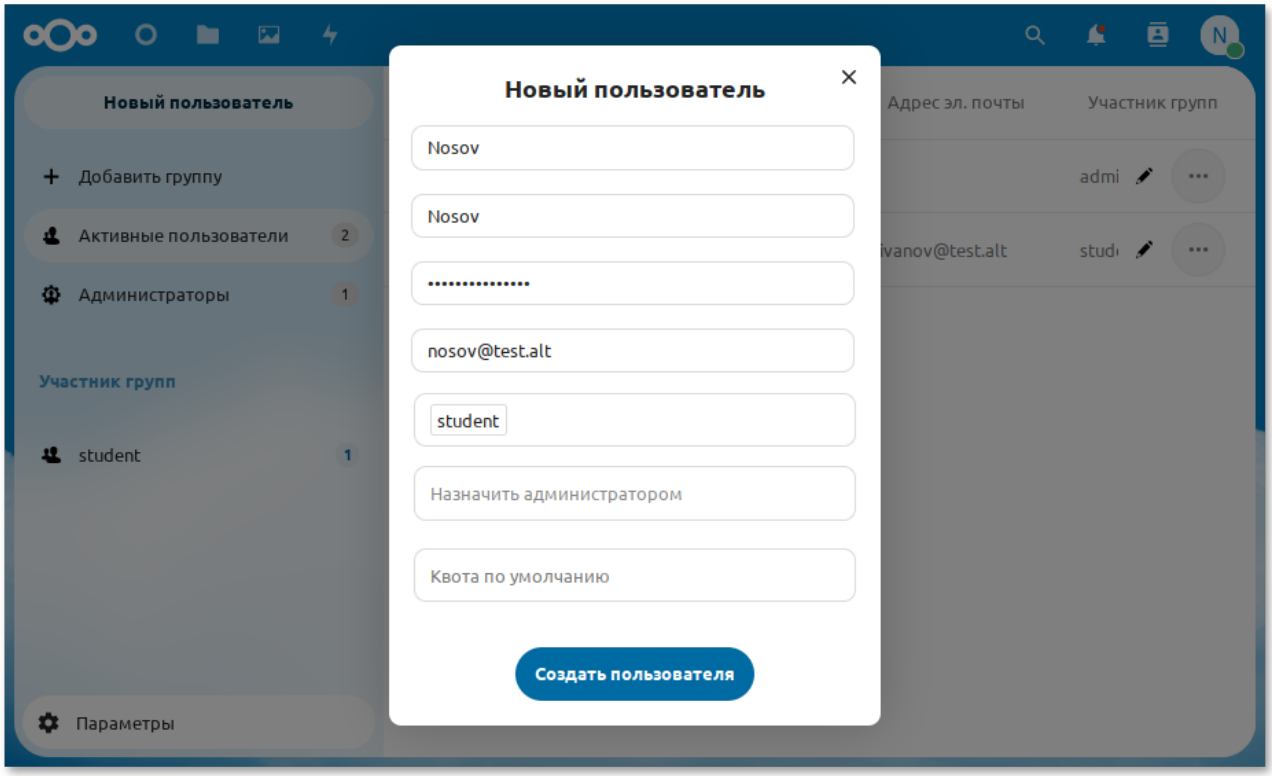


На странице **Активные пользователи** можно:

- просматривать текущих пользователей;
- создавать новых пользователей;
- изменять имена и пароли пользователей;
- просматривать и устанавливать квоты;
- фильтровать пользователей по группам;
- удалять пользователей.

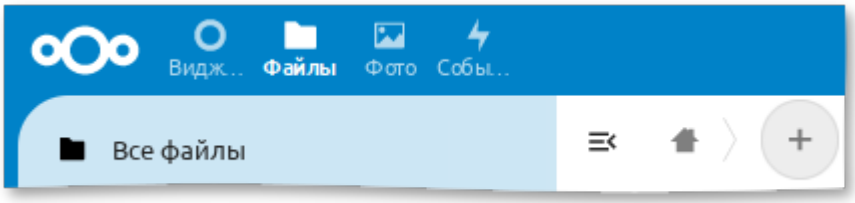


Для создания пользователя, следует нажать кнопку **Новый пользователь**, ввести **Имя пользователя**, **Пароль**, при необходимости указать группу и нажать кнопку **Создать пользователя**:

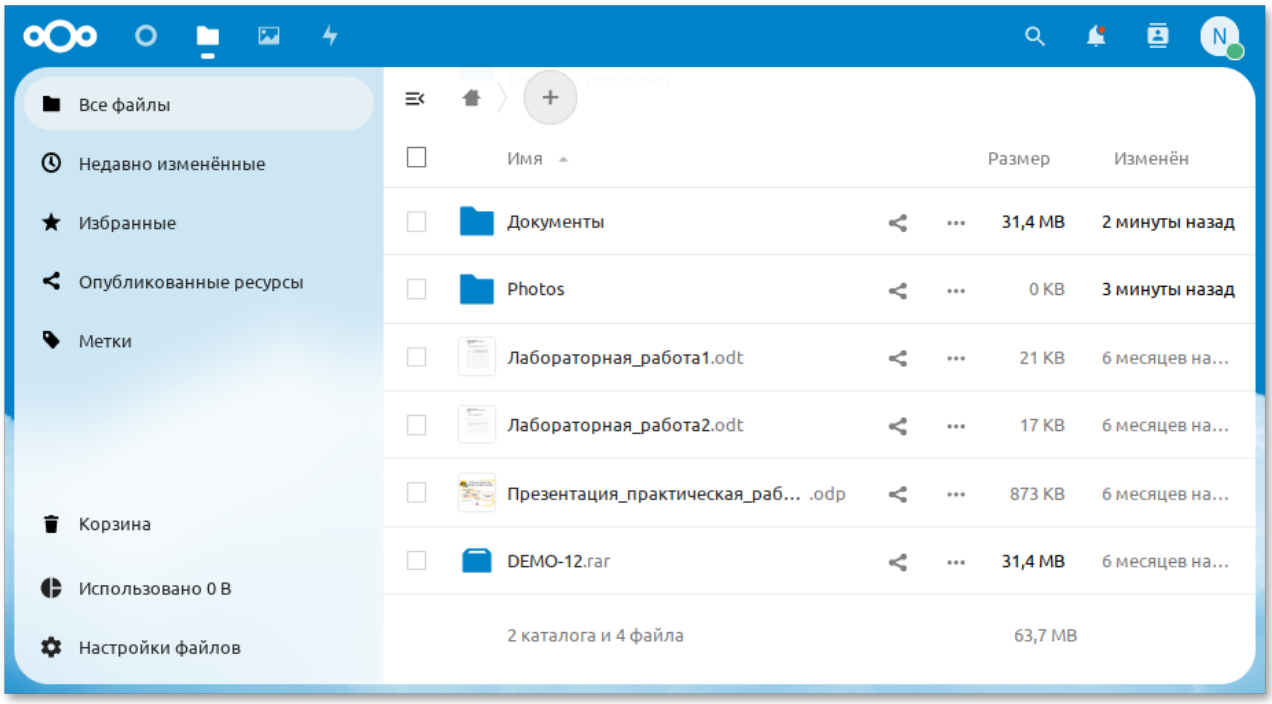


42.3.2. Работа с файлами

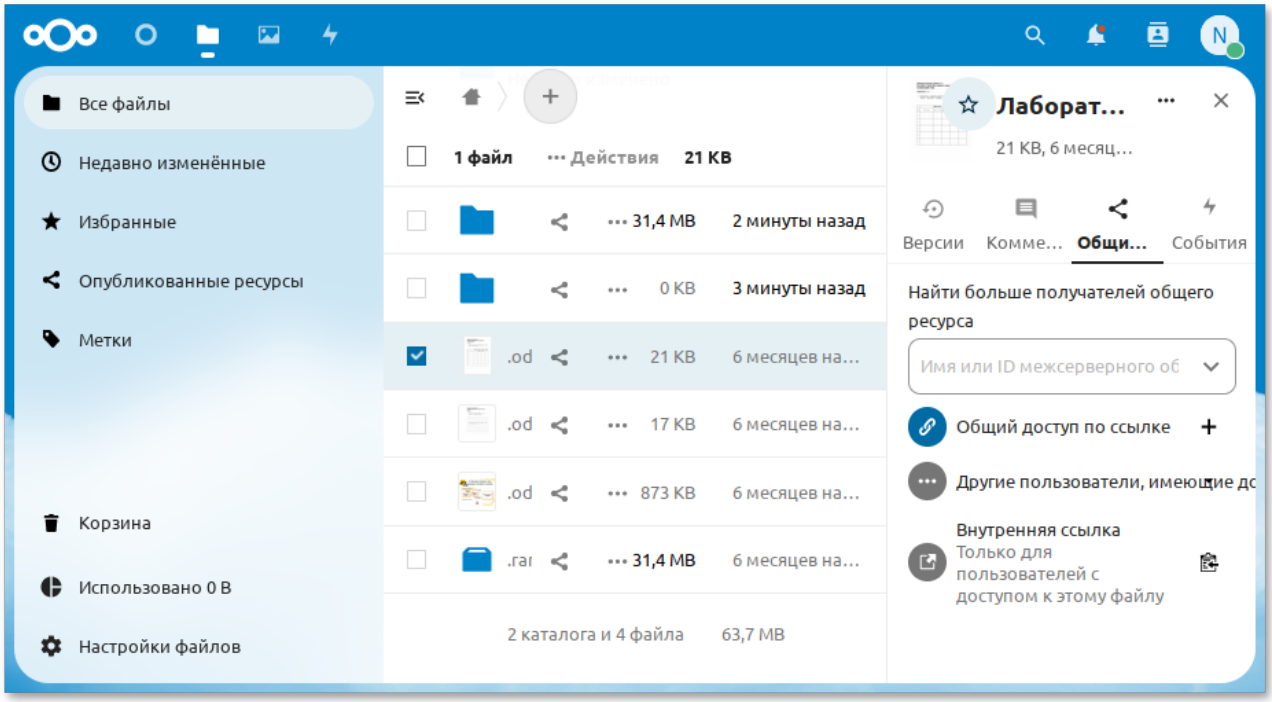
Меню выбора доступных сервисов расположено в левом верхнем углу веб-интерфейса Nextcloud:



При выборе раздела **Файлы** отображается структура каталогов пользователя:



Для того чтобы поделиться файлом или папкой с другими пользователями, необходимо нажать на треугольный значок рядом с названием файла и в открывшемся окне настроить параметры общего доступа:



Поделиться ссылкой может понадобиться в том случае, если необходимо предоставить доступ к файлу или папке людям, которые не входят в число пользователей Nextcloud.

Глава 43. Система резервного копирования UrBackup

UrBackup — это простое в настройке кроссплатформенное клиент-серверное программное обеспечение, позволяющее управлять резервным копированием для компьютеров и операционных систем различных типов. UrBackup позволяет создавать инкрементные и полные резервные копии, как целых разделов, так и отдельных каталогов, с возможностью выбора файлов, которые попадут в архив, а также делать снапшоты разделов жесткого диска.

Примечание

В настоящее время резервные копии образов (снапшоты) работают только с томами в формате NTFS и с клиентами Windows. Резервное копирование образов предназначено в основном для резервного копирования загрузочного тома (C:) систем Windows. Для архивирования других данных следует воспользоваться резервным копированием файлов.

Для управления настройкой резервного копирования и резервными копиями используется веб-интерфейс.

43.1. Установка UrBackup

43.1.1. Сервер UrBackup

Установить сервер UrBackup:

```
# apt-get install urbackup-server
```

Создать каталог для резервных копий:

```
# mkdir -p /mnt/backups/urbackup
```

Каталог должен принадлежать пользователю urbackup и у этого пользователя должны быть права на чтение/запись:

```
# chown -R urbackup:urbackup /mnt/backups/urbackup
```

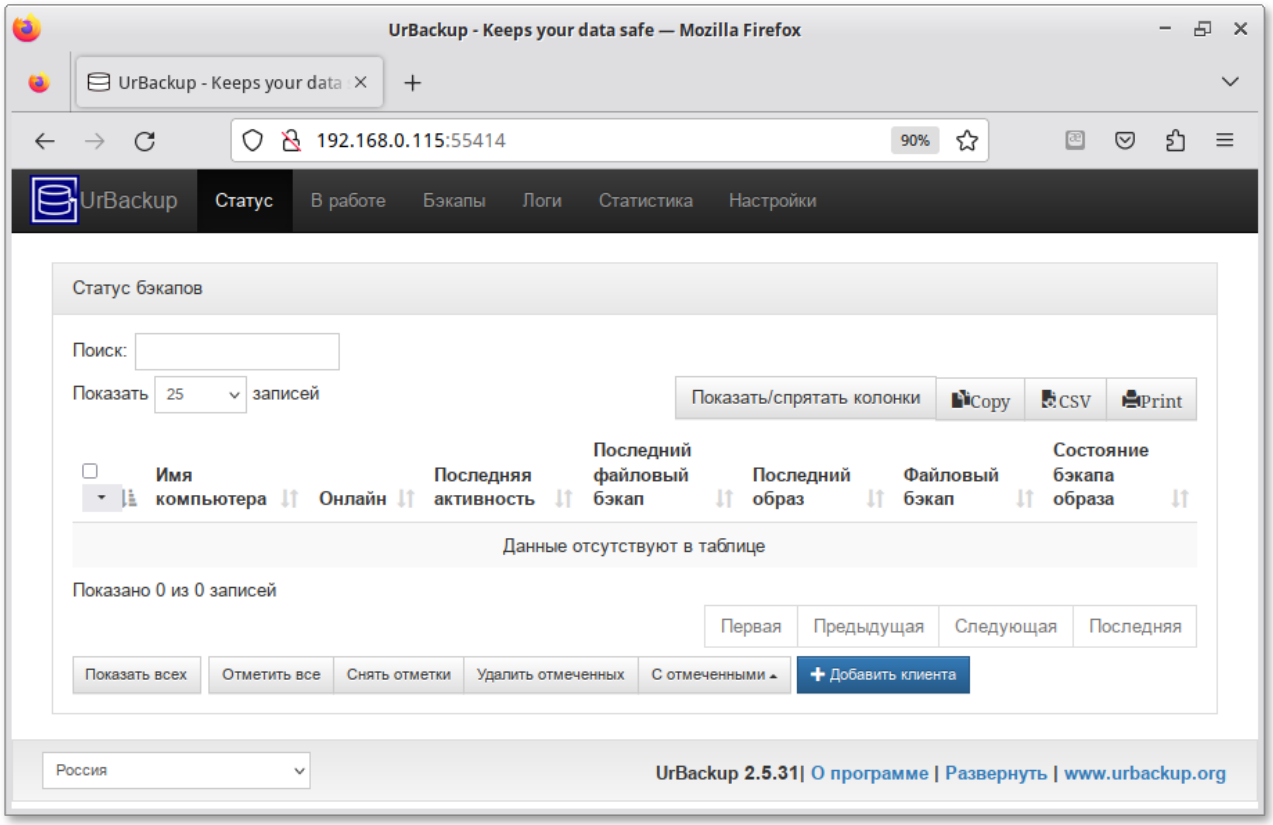
Добавить UrBackup-сервер в автозапуск и запустить его:

```
# systemctl enable --now urbackup-server
```

Примечание

UrBackup по умолчанию прослушивает порты 55413 и 55414.

Веб-интерфейс UrBackup будет доступен по адресу **`http://<ip-сервера>:55414`**:

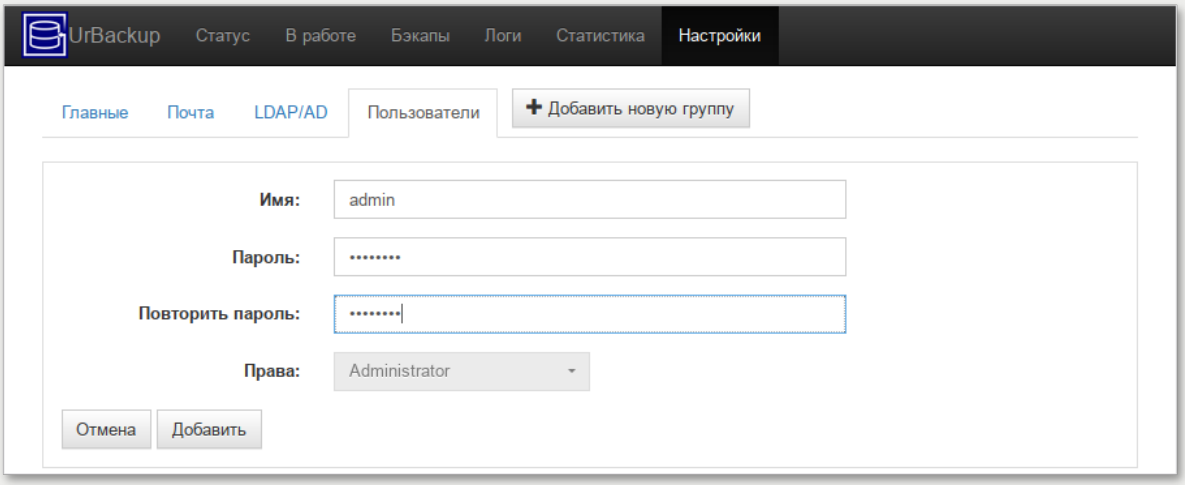


Важно

Если появляется ошибка: «Каталог, где UrBackup будет сохранять резервные копии, недоступен…», следует изменить путь к каталогу резервных копий, выбрав пункт меню **Настройки**, либо изменить права доступа к каталогу.

Примечание

Сразу после установки доступ к веб-интерфейсу UrBackup будет возможен без аутентификации. Чтобы в дальнейшем требовался ввод имени пользователя и пароля необходимо создать администратора (перейти на вкладку **Настройки** → **Пользователи** и нажать кнопку **`Создать`**):



43.1.2. Клиент UrBackup

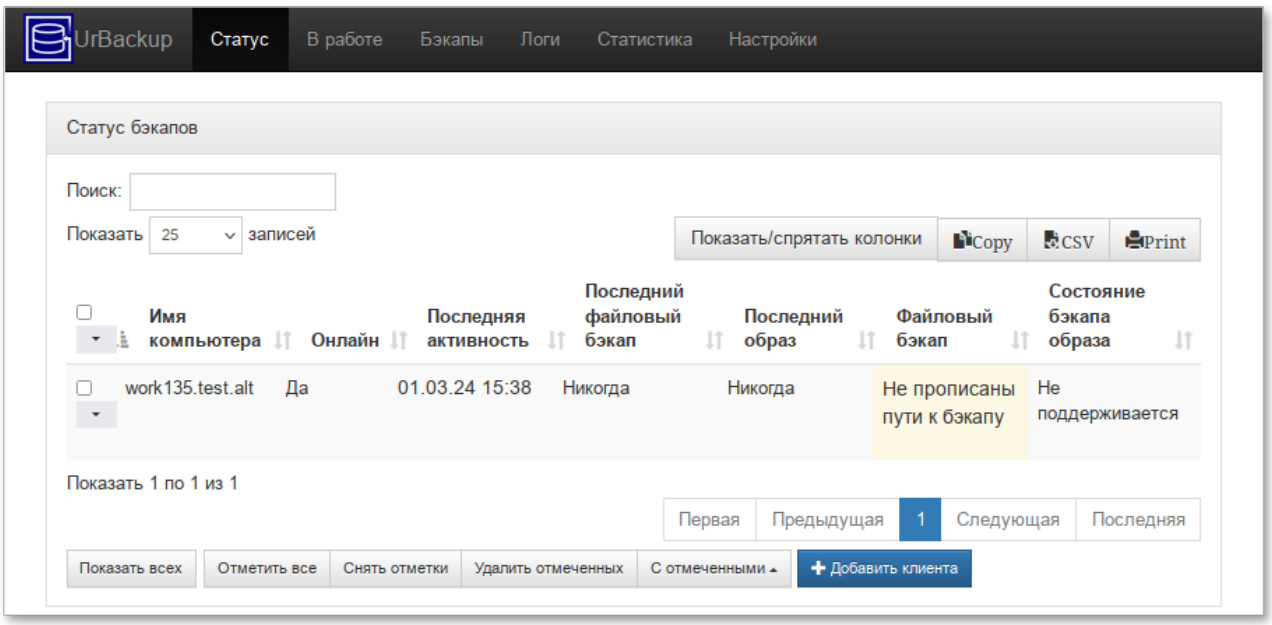
Установить клиент UrBackup:

```
# apt-get install urbackup-client
```

Добавить UrBackup-клиент в автозапуск и запустить его:

```
# systemctl enable --now urbackup-client
```

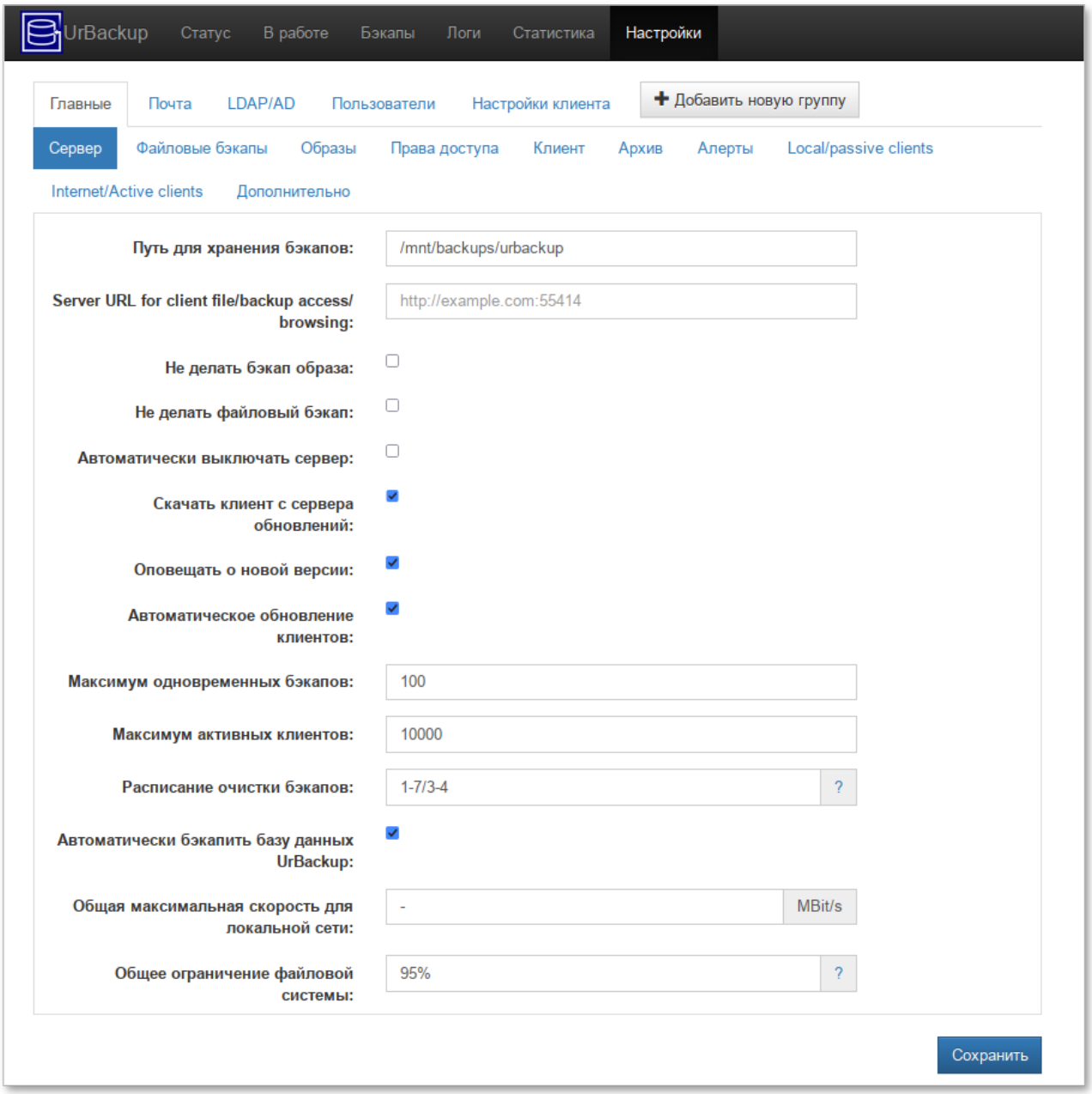
Локальные клиенты будут обнаружены сервером автоматически и появятся в веб-интерфейсе на вкладке **Статус**:



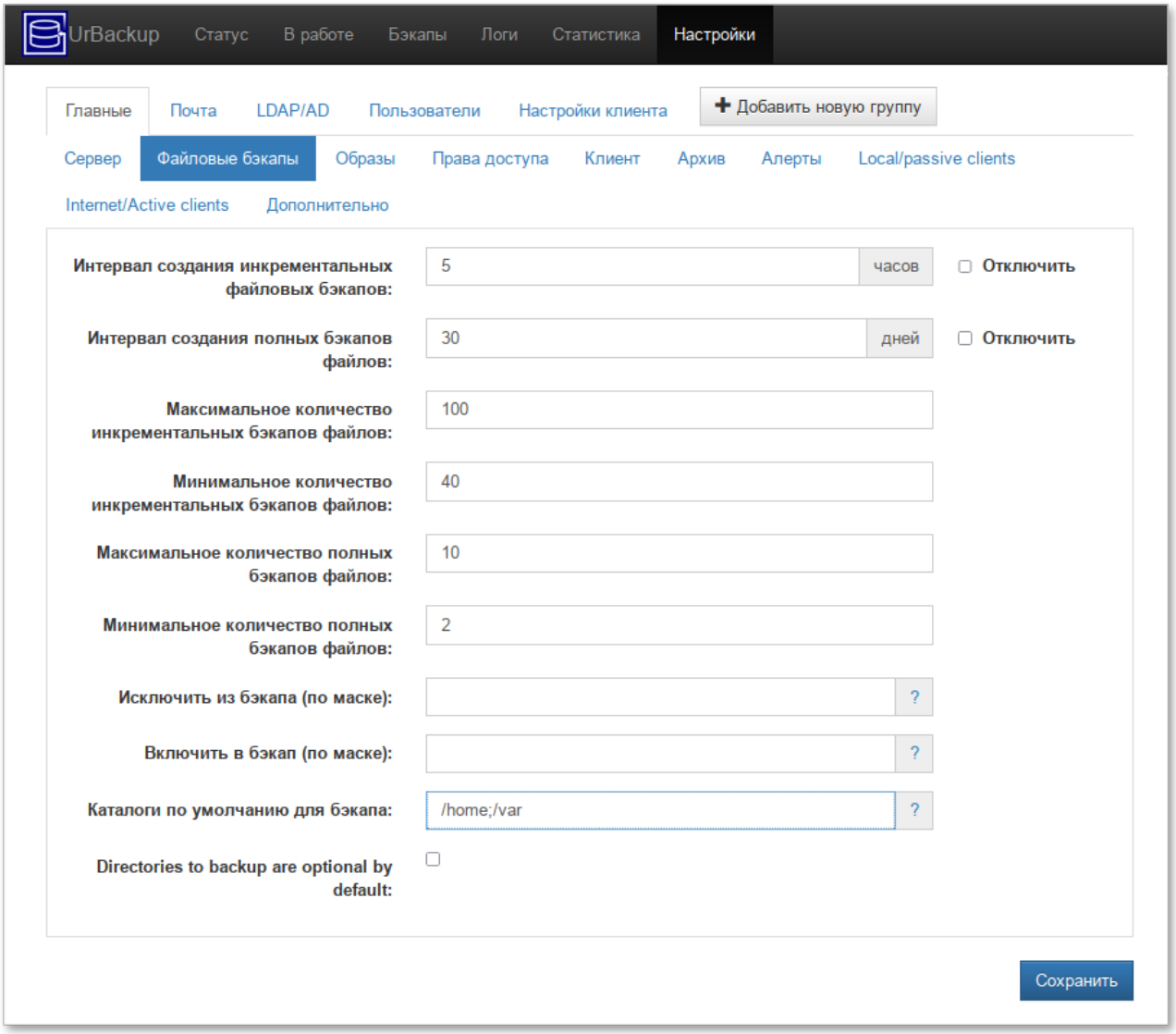
43.2. Настройка резервного копирования

В веб-интерфейсе на вкладке **Настройки** → **Главные** можно изменять настройки UrBackup. Некоторые настройки влияют только на сервер резервного копирования. Остальные настройки влияют и на клиентов резервного копирования, для этих настроек администратор может установить значения по умолчанию или переопределить настройки клиента.

На вкладке **Сервер** можно указать каталог для хранения резервных копий:



На вкладке **Файловые бэкапы** можно указать настройки файловых резервных копий, в том числе каталоги, которые будут включены в резервную копию (каталоги перечисляются через «;»). Здесь также настраиваются интервалы резервного копирования.

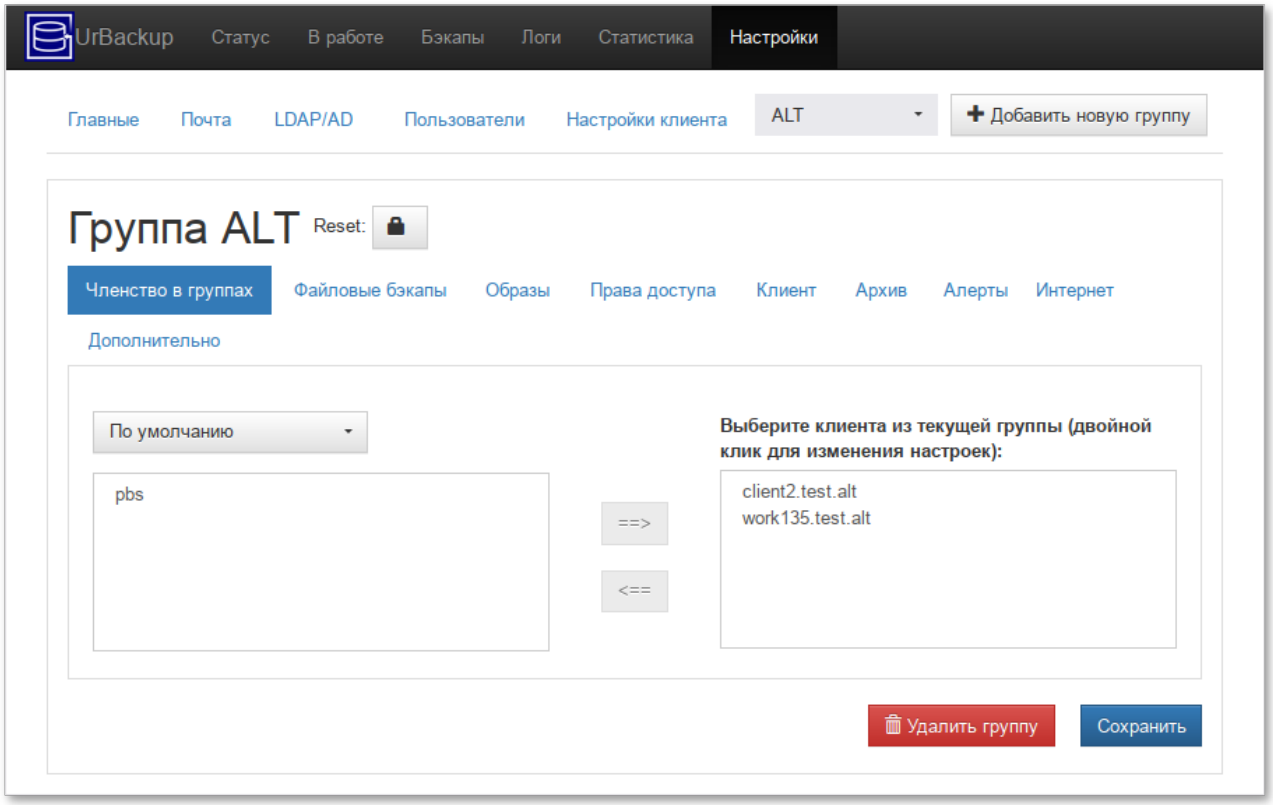


На вкладке **Клиент** (поле **Расписание**) можно установить окно резервного копирования, в пределах которого сервер будет стараться выполнять задания. Начатое задание будет выполняться до завершения, даже если оно не вписывается в указанное время. Примеры окна резервного копирования:

- 1-7/0-24 — резервное копирование может производиться в любое время;
- 1-5/8:00-9:00, 19:30-20:30;6,7/0-24 — резервное копирование в рабочие дни может производиться с 8 до 9 и с 19:30 до 20:30, а в субботу и воскресенье в любое время.

Клиенты могут сами инициировать процесс резервного копирования в любой момент (см. ниже описание утилиты **urbackupclientctl**).

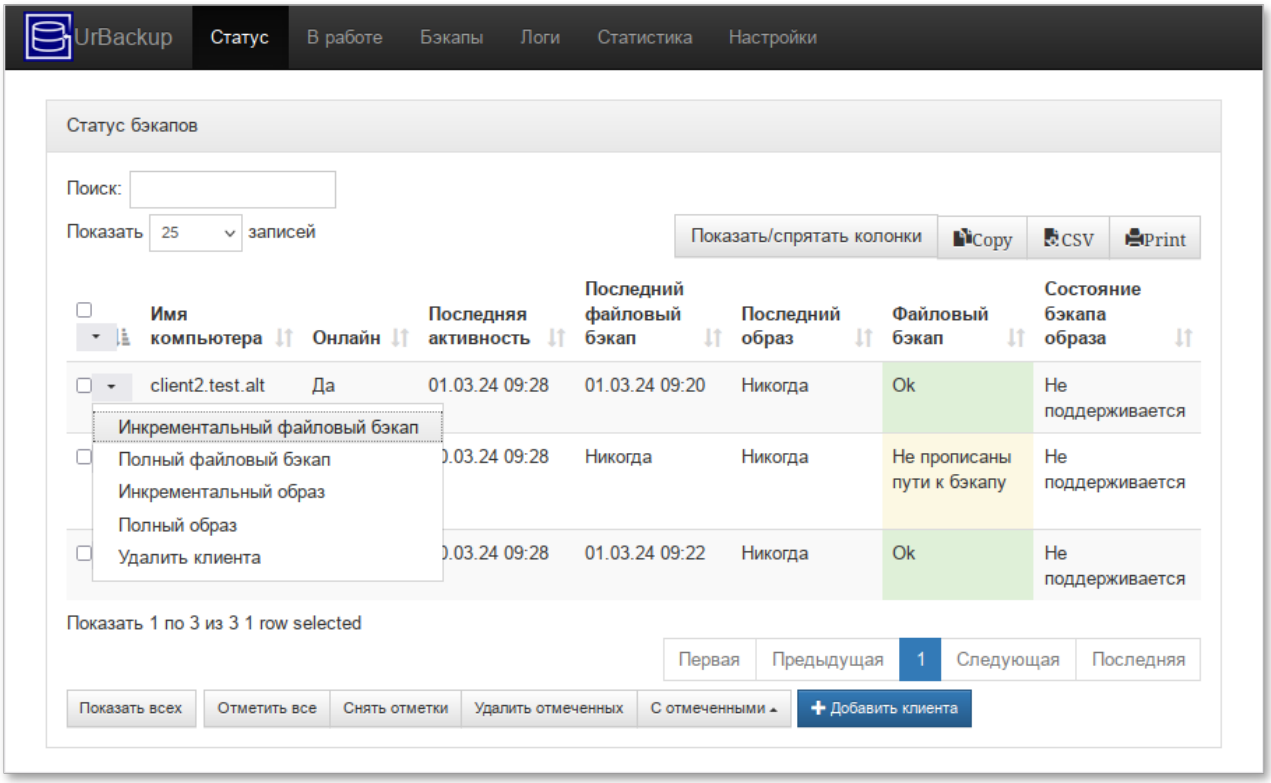
Для более удобного администрирования можно создать несколько групп, распределить клиенты по группам, и задавать настройки отдельно для каждой группы клиентов:



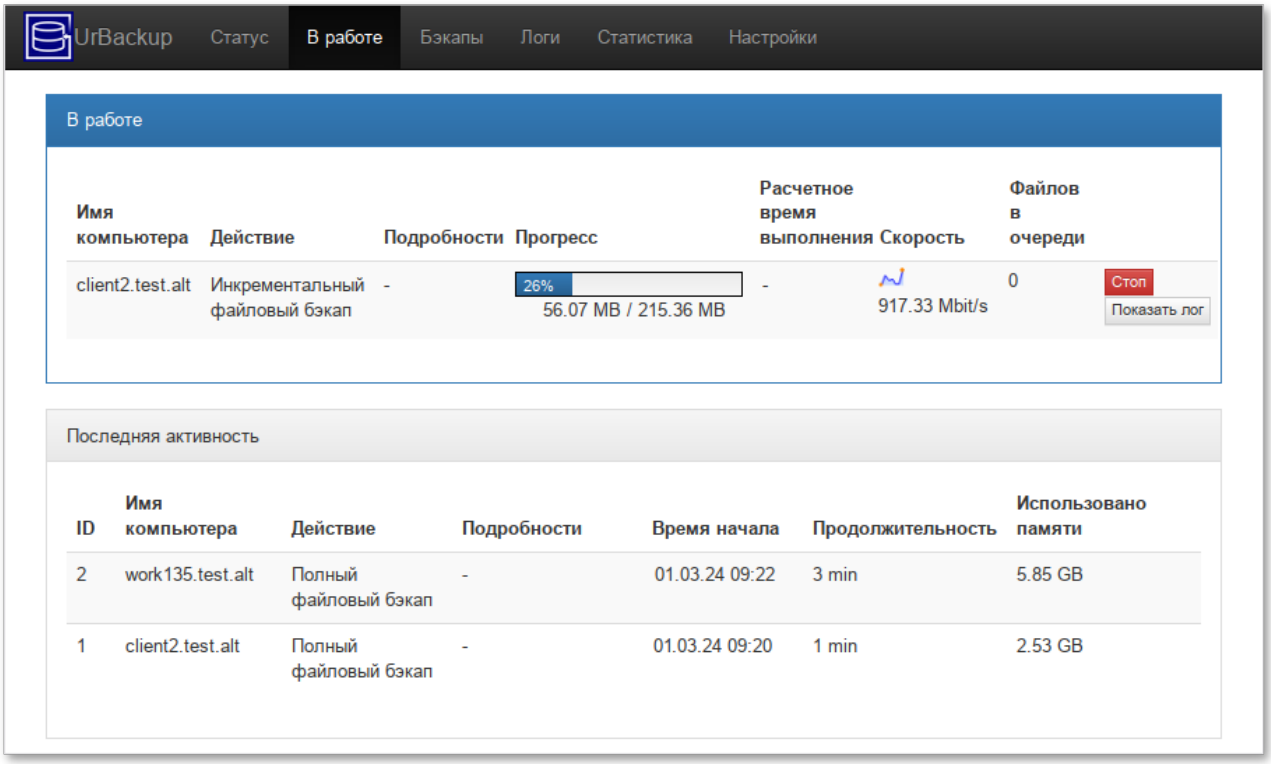
43.3. Создание резервных копий

Инкрементные и полные резервные копии будут создаваться согласно настроенному расписанию.

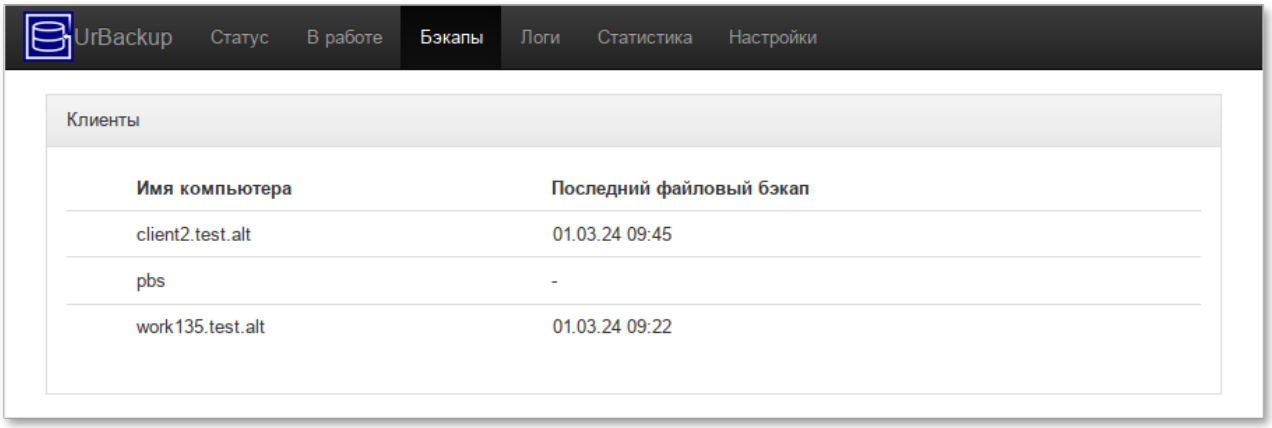
Процесс создания резервной копии можно запустить вручную, отметив клиента и выбрав тип резервной копии в выпадающем списке:



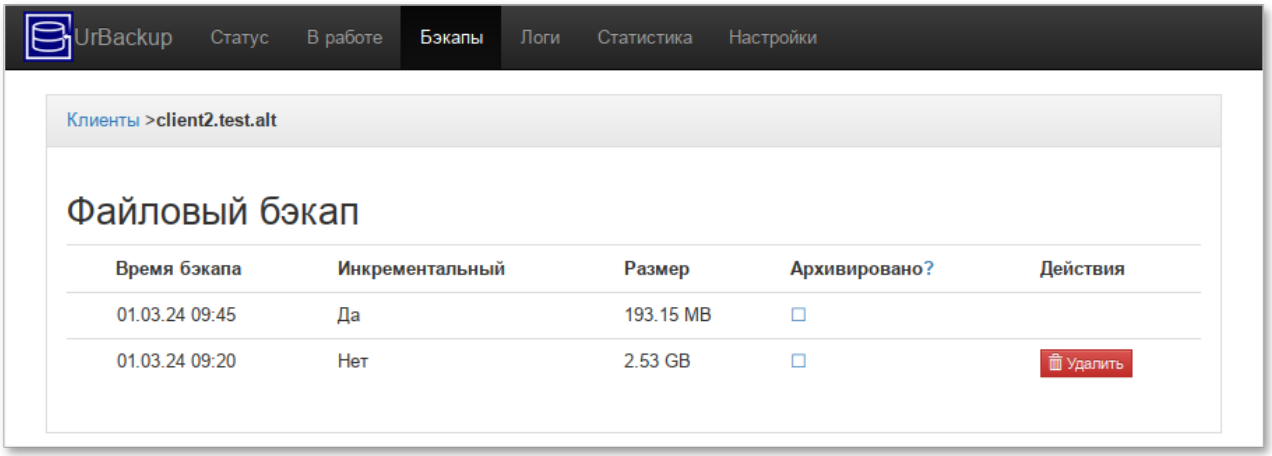
Более подробно отслеживать активность резервного копирования можно на вкладках **В работе**, **Бэкапы**, **Логи**.



Отчёты/содержимое резервных копий можно просмотреть на вкладке **Бэкапы**:



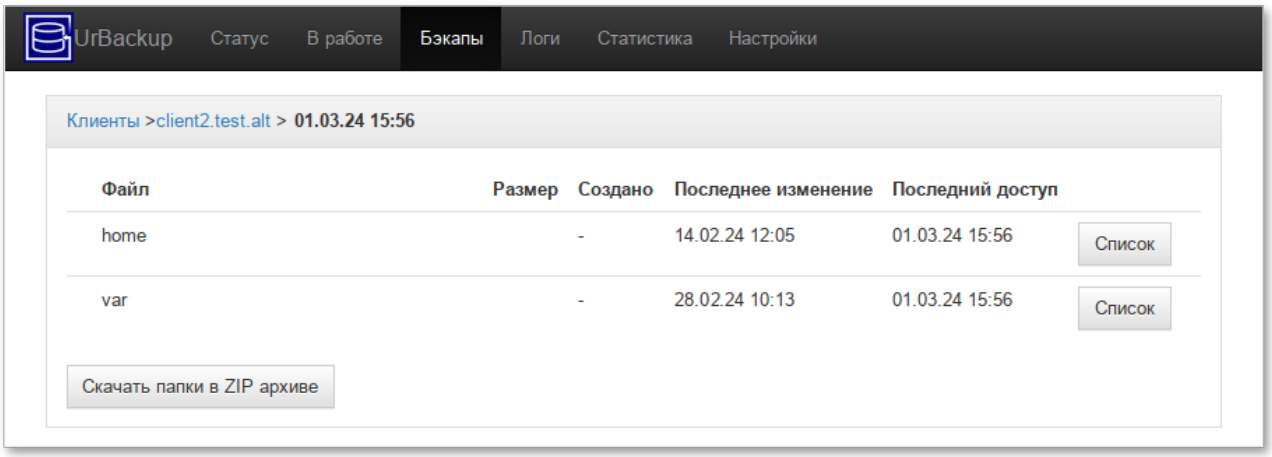
Выбрав клиента, можно просмотреть список его резервных копий:



Примечание

Если отметка в столбце **Архивировано** установлена, резервная копия архивируется. Пока резервная копия заархивирована, её нельзя удалить средствами UrBackup.

Выбрав резервную копию, можно просмотреть её содержимое:



Резервные копии сохраняются в каталоге, который был указан в веб-интерфейсе. В этом каталоге для каждого клиента создается свой подкаталог. Резервные копии файлов находятся в подкаталогах вида <YYMMDD-HHMM>. Каталог **current** является ссылкой на последнюю резервную копию. Резервные копии папок с файлами сохраняются в открытом виде. Образы дисковых разделов хранятся в виде файлов в формате vhdz (имя файла будет иметь вид Image_<Drive>_<YYMMDD-HHMM>.vhdz).

43.4. Утилита urbackupclientctl

Для работы с UrBackup на клиенте предназначена утилита **urbackupclientctl**:

- **urbackupclientctl start** — запустить инкрементное/полное резервное копирование;
- **urbackupclientctl status** — получить текущий статус резервного копирования;
- **urbackupclientctl browse** — просмотр списка резервных копий и файлов в резервных копиях;
- **urbackupclientctl restore-start** — восстановить файлы из резервной копии;
- **urbackupclientctl set-settings** — установить параметры резервного копирования;
- **urbackupclientctl add-backupdir** — добавить новый каталог в список каталогов, для которых выполняется резервное копирование;
- **urbackupclientctl list-backupdirs** — вывести список каталогов, для которых выполняется резервное копирование;
- **urbackupclientctl remove-backupdir** — удалить каталог из списока каталогов, для которых выполняется резервное копирование.

Справку по конкретной команде можно получить, выполнив команду:

```
urbackupclientctl <command> --help
```

Ниже приведены примеры использования утилиты **urbackupclientctl**.

Вывести список резервных копий:

```
$ urbackupclientctl browse
[{
"archived": 0,
"backuptime": 1709304813,
"disable_delete": true,
"id": 3,
"incremental": 0,
"size_bytes": 49182025
}
,{
"archived": 0,
"backuptime": 1709304721,
"id": 2,
"incremental": 0,
"size_bytes": 684214036
}
]
```

Запустить процесс создания полной резервной копии:

```
$ urbackupclientctl start -f
Waiting for server to start backup... done
Preparing... -
Completed successfully.
```

Восстановить файлы из резервной копии:

```
# urbackupclientctl restore-start -b 2
Starting restore. Waiting for backup server...  done
[==============================================================> ] 97% 2.33831 GB/
2.41119 GB at 76.024 KBit/s
Restore completed successfully.
```

Часть IX. Установка пакетов для опытных пользователей

Содержание

Введение

В современных системах на базе Linux существует огромное число общих ресурсов: разделяемых библиотек, содержащих стандартные функции, исполняемые файлы, сценарии и стандартные утилиты и т.д. Этими общими ресурсами пользуются сразу несколько программ. Удаление или изменение версии одного из составляющих систему компонентов может повлечь неработоспособность других, связанных с ним компонентов, или может привести к выводу из строя всей системы. В контексте системного администрирования проблемы такого рода называют нарушением *целостности системы*. Задача администратора — обеспечить наличие в системе согласованных версий всех необходимых программных компонентов (обеспечение целостности системы).

Для установки, удаления и обновления программ, а также поддержания целостности системы в Linux в первую очередь стали использоваться программы *менеджеры пакетов* (например, такие, как **rpm**). С точки зрения менеджера пакетов программное обеспечение представляет собой набор компонентов — программных *пакетов*. Пакеты содержат в себе набор исполняемых программ и вспомогательных файлов, необходимых для корректной работы программного

обеспечения. Менеджеры пакетов облегчают установку программ: они позволяют проверить наличие необходимого для работы устанавливаемой программы компонента подходящей версии непосредственно в момент установки. Менеджеры пакетов производят необходимые процедуры для регистрации программы во всех операционных средах пользователя: сразу после установки программа становится доступна пользователю из командной строки и появляется, если это было предусмотрено, в меню приложений всех графических оболочек.

Часто компоненты, используемые различными программами, выделяют в отдельные пакеты и помечают, что для работы ПО, предоставляемого пакетом A, необходимо установить пакет B. В таком случае говорят, что пакет A *зависит* от пакета B или между пакетами A и B существует *зависимость*.

Отслеживание зависимостей между такими пакетами представляет собой важную задачу для любого дистрибутива. Некоторые компоненты пакетов могут быть взаимозаменяемыми, т.е. может обнаружиться несколько пакетов, предлагающих затребованный ресурс.

Ещё более сложной является задача контроля целостности и непротиворечивости установленного в системе ПО. Представим, что некие программы A и B требуют наличия в системе компонентов C версии 1.0. Обновление версии пакета A, требующее обновления компонентов C до новой версии (например, до версии 2.0, использующей новый интерфейс доступа), влечёт за собой обязательное обновление и программы B.

На практике менеджеры пакетов оказались неспособны эффективно устранить нарушения целостности системы и предотвратить все коллизии при установке или удалении программ. Особенно остро этот недостаток сказался на обновлении систем из централизованного репозитория, в котором пакеты непрерывно обновляются, дробятся на более мелкие и т.п. Именно этот недостаток стимулировал создание систем управления программными пакетами и поддержания целостности ОС.

Для автоматизации и контроля описанных выше процессов стала применяться Усовершенствованная система управления программными пакетами **APT** (от англ. Advanced Packaging Tool). Автоматизация и контроль достигаются путём создания одного или нескольких внешних репозиториев. В них хранятся доступные для установки пакеты программ.

В распоряжении **APT** находятся две базы данных: одна описывает установленные в системе пакеты, вторая — внешний репозиторий. **APT** отслеживает целостность установленной системы и, в случае обнаружения противоречий в зависимостях пакетов, разрешает конфликты, находит пути их корректного устранения, руководствуясь сведениями из внешних репозиториев.

Система **APT** состоит из нескольких утилит. Чаще всего используется утилита управления пакетами **`apt-get`**. Она автоматически определяет зависимости между пакетами и строго следит за её соблюдением при выполнении любой из следующих операций: установка, удаление или обновление пакетов.

Глава 44. Источники программ (репозитории)

Отличие репозиториев, с которыми работает **APT**, от простого набора пакетов — наличие метаинформации. В ней содержится индекс находящихся в репозитории пакетов и сведения о них. Поэтому, чтобы получить всю информацию о репозитории, **APT** достаточно получить его индексы.

APT может пользоваться любым количеством репозиториев одновременно, формируя единую информационную базу обо всех содержащихся в них пакетах. При установке пакетов **APT** обращает внимание только на название пакета, его версию и зависимости. Для **APT** не имеет значения расположение пакета в том или ином репозитории.

Важно

Для одновременного подключения нескольких репозиториев необходимо отслеживать их совместимость друг с другом, т.е. их пакетная база должна отражать один определённый этап разработки. Совместное использование репозиториев, относящихся к разным дистрибутивам, или смешивание стабильного репозитория с нестабильной веткой разработки (Sisyphus) может привести к различным неожиданностям и трудностям при обновлении пакетов.

APT осуществляет взаимодействие с репозиториями при помощи различных протоколов доступа. Наиболее популярные — HTTP и FTP.

Для того чтобы **APT** мог использовать тот или иной репозиторий, информацию о нём необходимо поместить в файл **`/etc/apt/sources.list`**, либо в любой файл **`.list`** (например, ***`mysources`***`.list`) в каталоге **`/etc/apt/sources.list.d/`**. Описания репозиториев заносятся в эти файлы в следующем виде:

```
rpm [подпись] метод:путь база название
rpm-src [подпись] метод:путь база название
```

Здесь:

- rpm или rpm-src — тип репозитория (скомпилированные программы или исходные тексты);
- [подпись] — необязательная строка-указатель на электронную подпись разработчиков. Наличие этого поля подразумевает, что каждый пакет из данного репозитория должен быть подписан соответствующей электронной подписью. Подписи описываются в файле **`/etc/apt/vendor.list`**;
- метод — способ доступа к репозиторию: ftp, http, file, rsh, ssh, cdrom, copy;
- путь — путь к репозиторию в терминах выбранного метода;
- база — относительный путь к базе данных репозитория;
- название — название репозитория.

После редактирования списка репозиториев в **`sources.list`**, необходимо обновить локальную базу данных **APT** о доступных пакетах. Это делается командой **`apt-get update`**.

Если в **`sources.list`** присутствует репозиторий, содержимое которого может изменяться (например, постоянно разрабатываемый репозиторий или репозиторий обновлений по безопасности), то прежде чем работать с **APT**, необходимо синхронизировать локальную базу данных с удалённым сервером командой **`apt-get update`**. Локальная база данных создаётся заново при каждом изменении в репозитории: добавлении, удалении или переименовании пакета.

При установке определённого пакета **APT** производит поиск самой новой версии этого пакета во всех известных ему репозиториях вне зависимости от способа доступа к ним. Так, если в репозитории, доступном в сети Интернет, обнаружена более новая в сравнении с компакт-диском версия программы, то **APT** начнёт загружать соответствующий пакет из сети Интернет. Поэтому, если подключение к сети Интернет отсутствует или ограничено низкой пропускной способностью канала или высокой стоимостью, то следует закомментировать строчки (добавить в начало строки символ #) в **`/etc/apt/sources.list`**, относящиеся к ресурсам в сети Интернет.

Примечание

Репозитории для архитектуры **Эльбрус** могут быть недоступны в сети Интернет публично.

44.1. Редактирование репозиториев

Примечание

О добавлении или удалении репозиториев с использованием графических приложений вы можете почитать в Управление репозиториями.

44.1.1. Утилита apt-repo

Для редактирования репозиториев можно воспользоваться утилитой **`apt-repo`**:

- просмотреть список активных репозиториев:

```
apt-repo
```

- добавить репозиторий в список активных репозиториев:

```
apt-repo add репозиторий
```

- удалить или выключить репозиторий:

```
apt-repo rm репозиторий
```

- обновить информацию о репозиториях:

```
apt-repo update
```

- справка о команде **`apt-repo`**:

```
man apt-repo
```

или

```
apt-repo --help
```

Примечание

Для выполнения большинства команд необходимы права администратора.

Типичный пример использования: удалить все источники и добавить стандартный репозиторий P10 (архитектура выбирается автоматически):

```
# apt-repo rm all
# apt-repo add p10
```

Или то же самое одной командой:

```
# apt-repo set p10
```

44.1.2. Добавление репозитория на сменном носителе

Для добавления в **sources.list** репозитория на сменном диске в **APT** предусмотрена специальная утилита — **apt-cdrom**.

Чтобы добавить запись о репозитории на сменном диске необходимо:

1. Создать каталог для монтирования. Точка монтирования указывается в параметре **Acquire::CDROM::mount** в файле конфигурации **APT** (**/etc/apt/apt.conf**), по умолчанию это **/media/ALTLinux**:

   ```
   # mkdir /media/ALTLinux
   ```

2. Примонтировать носитель в указанную точку:

   ```
   # mount /dev/носитель /media/ALTLinux
   ```

   где **/dev/носитель** — соответствующее блочное устройство (например, **/dev/dvd** — для CD/DVD-диска).

3. Добавить носитель, выполнив команду:

   ```
   # apt-cdrom -m add
   ```

После этого в **sources.list** появится запись о подключённом носителе:

```
rpm cdrom:[ALT for Elbrus 2024-01-19]/ ALTLinux main
```

Примечание

Команду **mount /dev/носитель /media/ALTLinux** необходимо выполнять перед каждой командой **apt-get install имя_пакета**.

44.1.3. Добавление репозиториев вручную

Для изменения списка репозиториев можно отредактировать в любом текстовом редакторе файлы из каталога **/etc/apt/sources.list.d/**.

Примечание

Для изменения этих файлов необходимы права администратора.

В файле ***alt*.list** может содержаться такая информация:

```
rpm file:/srv/repo e2kv4 classic
rpm file:/srv/repo noarch classic
```

По сути, каждая строчка соответствует некому репозиторию. Не активные репозитории — строки, начинающиеся со знака #. Для добавления нового репозитория, достаточно дописать его в этот или другой файл.

После обновления списка репозиториев следует обновить информацию о них (выполнить команду **apt-get update** или **apt-repo update**).

Глава 45. Поиск пакетов

Если точное название пакета неизвестно, то для его поиска можно воспользоваться утилитой **apt-cache**. Данная утилита позволяет искать пакет не только по имени, но и по его описанию.

Команда **apt-cache search *подстрока*** позволяет найти все пакеты, в именах или описании которых присутствует указанная подстрока. Например:

```
$ apt-cache search dictionary
stardict-wn - GCIDE - The Collaborative International Dictionary of English
firefox-ru - Russian (RU) Language Pack for Firefox
gnome-dictionary-applet - GNOME panel applet for gnome-dictionary
gnome-utils - Utilities for the GNOME 2.0 desktop
libgdict - GNOME Dictionary Library.
stardict-mueller7 - V.K. Mueller English-Russian Dictionary, 7 Edition: stardict
format
stardict-slovnyk_be-en - Dictionary: Slovnyk Belarusian-English
stardict-slovnyk_be-ru - Dictionary: Slovnyk Belarusian-Russian
stardict-slovnyk_be-uk - Dictionary: Slovnyk Belarusian-Ukrainian
stardict-slovnyk_cs-ru - Dictionary: Slovnyk Czech-Russian
stardict-slovnyk_en-be - Dictionary: Slovnyk English-Belarusian
stardict-slovnyk_en-ru - Dictionary: Slovnyk English-Russian
stardict-slovnyk_en-uk - Dictionary: Slovnyk English-Ukrainian
stardict-slovnyk_es-ru - Dictionary: Slovnyk Spanish-Russian
stardict-slovnyk_ru-be - Dictionary: Slovnyk Russian-Belarusian
stardict-slovnyk_ru-cs - Dictionary: Slovnyk Russian-Czech
stardict-slovnyk_ru-en - Dictionary: Slovnyk Russian-English
stardict-slovnyk_ru-es - Dictionary: Slovnyk Russian-Spanish
stardict-slovnyk_ru-uk - Dictionary: Slovnyk Russian-Ukrainian
```

```
stardict-slovnyk_uk-be - Dictionary: Slovnyk Ukrainian-Belarusian
stardict-slovnyk_uk-en - Dictionary: Slovnyk Ukrainian-English
stardict-slovnyk_uk-ru - Dictionary: Slovnyk Ukrainian-Russian
words - A dictionary of English words for the /usr/share/dict directory
```

Для того чтобы подробнее узнать информацию о найденном пакете и получить его подробное описание, воспользуйтесь командой **apt-cache show**:

```
$ apt-cache show stardict-mueller7
Package: stardict-mueller7
Section: Text tools
Installed Size: 3095255
Maintainer: Anton V. Boyarshinov <boyarsh@altlinux.ru>
Version: 1.0-alt7
Pre-Depends: rpmlib(PayloadIsLzma)
Depends: stardict (>= 2.4.2)
Provides: stardict-mueller7 (= 1.0-alt7)
Architecture: noarch
Size: 3135276
MD5Sum: ea95c67ca323350b454fbc26533c3548
Filename: stardict-mueller7-1.0-alt7.noarch.rpm
Description: V.K. Mueller English-Russian Dictionary, 7 Edition: stardict format
 Electronic version of V.K. Mueller English-Russian Dictionary, 7 Edition
 in stardict format. You can use it with stardict client.
```

При поиске с помощью **apt-cache** можно использовать русскую подстроку. В этом случае будут найдены пакеты, имеющие описание на русском языке. К сожалению, описание на русском языке в настоящее время есть не у всех пакетов, но наиболее актуальные описания переведены.

Глава 46. Установка или обновление пакета

Важно

Для установки пакетов требуются привилегии администратора.

Установка пакета с помощью APT выполняется командой **apt-get install *имя_пакета***.

Важно

Перед установкой и обновлением пакетов необходимо выполнить команду обновления индексов пакетов:

```
# apt-get update
```

apt-get позволяет устанавливать в систему пакеты, требующие для работы наличие других, пока ещё не установленных пакетов. В этом случае он определяет, какие пакеты необходимо установить. **apt-get** устанавливает их, пользуясь всеми доступными репозиториями.

Установка пакета *stardict-mueller7* командой **apt-get install stardict-mueller7** приведёт к следующему диалогу с **APT** (если пакет еще не установлен):

```
# apt-get install stardict-mueller7
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие НОВЫЕ пакеты будут установлены:
  stardict-mueller7
0 будет обновлено, 1 новых установлено, 0 пакетов будет удалено и 0 не будет
обновлено.
Необходимо получить 0B/3135kB архивов.
После распаковки потребуется дополнительно 3095kB дискового пространства.
Совершаем изменения...
Preparing...                  ######################### [100%]
1: stardict-mueller7          ######################### [100%]
Running /usr/lib/rpm/posttrans-filetriggers
Завершено.
```

Команда

```
apt-get install имя_пакета
```

используется также и для обновления уже установленного пакета или группы пакетов. В этом случае **apt-get** дополнительно проверяет, есть ли обновлённая, в сравнении с установленной в системе, версия пакета в репозитории.

Например, если пакет *stardict-mueller7* установлен и в репозитории нет обновлённой версии этого пакета, то вывод команды **apt-get install stardict-mueller7** будет таким:

```
# apt-get install stardict-mueller7
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Последняя версия stardict-mueller7 уже установлена.
0 будет обновлено, 0 новых установлено, 0 пакетов будет удалено и 2262 не будет
обновлено.
```

При помощи **APT** можно установить и отдельный rpm- пакет, не входящий в состав репозиториев (например, полученный из сети Интернет). Для этого достаточно выполнить команду

```
# apt-get install /путь/к/файлу.rpm
```

При этом **APT** проведёт стандартную процедуру проверки зависимостей и конфликтов с уже установленными пакетами.

Иногда в результате операций с пакетами без использования **APT** целостность системы нарушается, и **apt-get** отказывается выполнять операции установки, удаления или обновления. В этом случае необходимо повторить операцию, задав опцию **-f**, заставляющую **apt-get** исправить нарушенные зависимости, удалить или заменить конфликтующие пакеты. В этом случае необходимо внимательно следить за сообщениями, выводимыми **apt-get**. Любые действия в этом режиме обязательно требуют подтверждения со стороны пользователя.

Глава 47. Удаление установленного пакета

Для удаления пакета используется команда **apt-get remove *имя_пакета***. Для того чтобы не нарушать целостность системы, будут удалены и все пакеты, зависящие от удаляемого. В случае удаления пакета, который относится к базовым компонентам системы, **apt-get** потребует дополнительное подтверждение с целью предотвращения возможной случайной ошибки.

Важно

Для удаления пакетов требуются привилегии администратора.

При попытке с помощью **apt-get** удалить базовый компонент системы, вы увидите следующий запрос на подтверждение операции:

```
# apt-get remove filesystem
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие пакеты будут УДАЛЕНЫ:
  ...
ВНИМАНИЕ: Будут удалены важные для работы системы пакеты
Обычно этого делать не следует. Вы должны точно понимать возможные последствия!
  ...
0 будет обновлено, 0 новых установлено, 2648 пакетов будет удалено и 0 не будет
обновлено.
Необходимо получить 0B архивов.
После распаковки будет освобождено 8994MB дискового пространства.
Вы делаете нечто потенциально опасное!
Введите фразу 'Yes, do as I say!' чтобы продолжить.
```

Предупреждение

Каждую ситуацию, в которой **APT** выдаёт такой запрос, необходимо рассматривать отдельно. Вероятность того, что после выполнения этой команды система окажется неработоспособной, очень велика.

Глава 48. Обновление всех установленных пакетов

Для обновления всех установленных пакетов используются команды:

```
# apt-get update && apt-get dist-upgrade
```

Первая команда (**apt-get update**) обновит индексы пакетов. Вторая команда (**apt-get dist-upgrade**) позволяет обновить только те установленные пакеты, для которых в репозиториях, перечисленных в **/etc/apt/sources.list**, имеются новые версии.

Примечание

Команда (**apt-get dist-upgrade**) обновит систему, но ядро ОС не будет обновлено.

Глава 49. Обновление ядра

Для обновления ядра ОС необходимо выполнить команду:

```
# update-kernel
```

Примечание

Если индексы сегодня еще не обновлялись перед выполнением команды **update-kernel** необходимо выполнить команду **apt-get update**.

Команда **update-kernel** обновляет и модули ядра, если в репозитории обновилось что-то из модулей без обновления ядра.

Новое ядро загрузится только после перезагрузки системы.

Если с новым ядром что-то пойдёт не так, вы сможете вернуться к предыдущему варианту, выбрав его в начальном меню загрузчика.

После успешной загрузки на обновленном ядре можно удалить старое, выполнив команду:

```
# remove-old-kernels
```

Глава 50. Единая команда управления пакетами (epm)

Основное назначение единой команды управления пакетами — унифицировать управление пакетами в дистрибутивах с разными пакетными менеджерами. Утилита **epm** упрощает процедуру управления пакетами, может использоваться в скриптах и установщиках, сервисных программах, в повседневном администрировании различных систем. В **epm** добавлены типовые операции, которые в случае использования apt потребовали бы ввода более одной команды.

Единая команда управления пакетами включает в себя следующую функциональность:

- управление пакетами (установка/удаление/поиск);
- управление репозиториями (добавление/удаление/обновление/список);
- управление системными сервисами (включение/выключение/список).

Список поддерживаемых форматов пакетов: rpm, deb, tgz, tbz, tbz2, apk, pkg.gz.

Примечание

Установка утилиты **epm**, если она еще не установлена, выполняется командой:

```
# apt-get install eepm
```

Подробную информацию об утилите **epm** и её опциях можно получить, выполнив команду:

```
$ epm --help
```

Ниже описаны лишь некоторые возможности утилиты **epm**.

Установка пакета из репозитория или из локального файла в систему:

```
# epm install <имя_пакета>
```

Важно

Если пакет создан сторонним поставщиком, то при его установке командой **epm install** не будут выполнены установочные скрипты из пакета. Это предохраняет систему от повреждения, но может привести к тому, что пакет не заработает. Вернуть стандартное поведение можно добавлением **--scripts**:

```
# epm install --scripts <имя_пакета>
```

Установить сторонние программы безопасным и простым способом:

```
# epm play <имя_программы>
```

Список программ, которые можно установить данной командой, можно просмотреть, выполнив команду:

```
$ epm play
Run with a name of a play script to run:
  anydesk              - Install AnyDesk from the official site
  assistant            - Install Assistant (Ассистент) from the official site
  …
  yandex-browser       - Install Yandex browser from the official site
  yandex-disk          - Install Yandex Disk from the official site
  zoom                 - Install Zoom client from the official site
```

Команда **epm play** требует наличия доступа в сеть Интернет.

Примечание

Для некоторых сторонних rpm-пакетов написаны дополнительные правила для перепаковки (при перепаковке пакета создаётся пакет, учитывающий, что нужно для работы исходного пакета). Установить такие пакеты можно, выполнив команду:

```
# epm install --repack <имя_пакета>
```

Для deb-пакетов ключ **--repack** применяется автоматически.

Удаление пакета из системы:

```
# epm remove <имя_пакета>
```

Поиск пакета в репозитории:

```
# epm search <текст>
```

Получить список установленных пакетов:

```
$ epm list
```

Удалить пакеты, от которых не зависят какие-либо другие пакеты, установленные в системе:

```
# epm autoremove
```

Обновить все установленные пакеты и ядро ОС:

```
# epm full-upgrade
```

Часть X. Основы администрирования Linux

Содержание

Глава 51. Общие принципы работы ОС

51.1. Процессы и файлы

ОС Альт Сервер для Эльбрус является многопользовательской интегрированной системой. Это значит, что она разработана в расчете на одновременную работу нескольких пользователей.

Пользователь может либо сам работать в системе, выполняя некоторую последовательность команд, либо от его имени могут выполняться прикладные процессы.

Пользователь взаимодействует с системой через командный интерпретатор. Командный интерпретатор представляет собой прикладную программу, которая принимает от пользователя команды или набор команд и транслирует их в системные вызовы к ядру системы. Интерпретатор позволяет пользователю просматривать файлы, передвигаться по дереву файловой системы, запускать прикладные процессы. Все командные интерпретаторы UNIX имеют развитый командный язык и позволяют писать достаточно сложные программы, упрощающие процесс администрирования системы и работы с ней.

51.1.1. Процессы функционирования ОС

Все программы, которые выполняются в текущий момент времени, называются процессами. Процессы можно разделить на два основных класса: системные процессы и пользовательские процессы.

Системные процессы — программы, решающие внутренние задачи ОС, например, организацию виртуальной памяти на диске или предоставляющие пользователям те или иные сервисы (процессы-службы).

Пользовательские процессы — процессы, запускаемые пользователем из командного интерпретатора для решения задач пользователя или управления системными процессами. Linux изначально разрабатывался как многозадачная система. Он использует технологии, опробованные и отработанные другими реализациями UNIX, которые существовали ранее.

Фоновый режим работы процесса — режим, когда программа может работать без взаимодействия с пользователем. В случае необходимости интерактивной работы с пользователем (в общем случае) процесс будет «остановлен» ядром, и работа его продолжается только после переведения его в «нормальный» режим работы.

51.1.2. Файловая система ОС

В ОС использована файловая система Linux, которая, в отличие от файловых систем DOS и Windows(™), является единым деревом. Корень этого дерева — каталог, называемый root (рут) и обозначаемый **/**.

Части дерева файловой системы могут физически располагаться в разных разделах разных дисков или вообще на других компьютерах — для пользователя это прозрачно. Процесс присоединения файловой системы раздела к дереву называется монтированием, удаление — размонтированием. Например, файловая система CD-ROM в дистрибутиве монтируется по умолчанию в каталог **/media/cdrom** (путь в дистрибутиве обозначается с использованием **/**, а не ****, как в DOS/Windows).

Текущий каталог обозначается **./**.

51.1.3. Структура каталогов

Корневой каталог **/**:

- **/bin** — командные оболочки (shell), основные утилиты;
- **/boot** — содержит ядро системы;
- **/dev** — псевдофайлы устройств, позволяющие работать с устройствами напрямую. Файлы в **/dev** создаются сервисом **udev**
- **/etc** — общесистемные конфигурационные файлы для большинства программ в системе;
- **/etc/rc?.d**, **/etc/init.d**, **/etc/rc.boot**, **/etc/rc.d** — каталоги, где расположены командные файлы, выполняемые при запуске системы или при смене её режима работы;
- **/etc/passwd** — база данных пользователей, в которой содержится информация об имени пользователя, его настоящем имени, личном каталоге, его зашифрованный пароль и другие данные;

- **/etc/shadow** — теневая база данных пользователей. При этом информация из файла **/etc/passwd** перемещается в **/etc/shadow**, который недоступен для чтения всем, кроме пользователя root. В случае использования альтернативной схемы управления теневыми паролями (TCB), все теневые пароли для каждого пользователя располагаются в каталоге **/etc/tcb/*имя пользователя*/shadow**;
- **/home** — домашние каталоги пользователей;
- **/lib** — содержит файлы динамических библиотек, необходимых для работы большей части приложений, и подгружаемые модули ядра;
- **/lost+found** — восстановленные файлы;
- **/media** — подключаемые носители (каталоги для монтирования файловых систем сменных устройств);
- **/mnt** — точки временного монтирования;
- **/opt** — вспомогательные пакеты;
- **/proc** — виртуальная файловая система, хранящаяся в памяти компьютера при загруженной ОС. В данном каталоге расположены самые свежие сведения обо всех процессах, запущенных на компьютере.
- **/root** — домашний каталог администратора системы;
- **/run** — файлы состояния приложений;
- **/sbin** — набор программ для административной работы с системой (системные утилиты);
- **/selinux** — виртуальная файловая система SELinux;
- **/srv** — виртуальные данные сервисных служб;
- **/sys** — файловая система, содержащая информацию о текущем состоянии системы;
- **/tmp** — временные файлы.
- **/usr** — пользовательские двоичные файлы и данные, используемые только для чтения (программы и библиотеки);
- **/var** — файлы для хранения изменяющихся данных (рабочие файлы программ, очереди, журналы).

Каталог **/usr**:

- **/usr/bin** — дополнительные программы для всех учетных записей;
- **/usr/sbin** — команды, используемые при администрировании системы и не предназначенные для размещения в файловой системе root;
- **/usr/local** — место, где рекомендуется размещать файлы, установленные без использования пакетных менеджеров, внутренняя организация каталогов практически такая же, как и корневого каталога;
- **/usr/man** — каталог, где хранятся файлы справочного руководства **man**;
- **/usr/share** — каталог для размещения общедоступных файлов большей части приложений.

Каталог **`/var`**:

- **`/var/log`** — место, где хранятся файлы аудита работы системы и приложений;
- **`/var/spool`** — каталог для хранения файлов, находящихся в очереди на обработку для того или иного процесса (очереди печати, непрочитанные или не отправленные письма, задачи cron т.д.).

51.1.4. Организация файловой структуры

Система домашних каталогов пользователей помогает организовывать безопасную работу пользователей в многопользовательской системе. Вне своего домашнего каталога пользователь обладает минимальными правами (обычно чтение и выполнение файлов) и не может нанести ущерб системе, например, удалив или изменив файл.

Кроме файлов, созданных пользователем, в его домашнем каталоге обычно содержатся персональные конфигурационные файлы некоторых программ.

Маршрут (путь) — это последовательность имён каталогов, представляющая собой путь в файловой системе к данному файлу, где каждое следующее имя отделяется от предыдущего наклонной чертой (слешем). Если название маршрута начинается со слеша, то путь в искомый файл начинается от корневого каталога всего дерева системы. В обратном случае, если название маршрута начинается непосредственно с имени файла, то путь к искомому файлу должен начаться от текущего каталога (рабочего каталога).

Имя файла может содержать любые символы за исключением косой черты (*/*). Однако следует избегать применения в именах файлов большинства знаков препинания и непечатаемых символов. При выборе имен файлов рекомендуется ограничиться следующими символами:

- **строчные** и **ПРОПИСНЫЕ** буквы. Следует обратить внимание на то, что регистр всегда имеет значение;
- символ подчеркивания (_);
- точка (**.**).

Для удобства работы точку можно использовать для отделения имени файла от расширения файла. Данная возможность может быть необходима пользователям или некоторым программам, но не имеет значение для shell.

51.1.5. Имена дисков и разделов

Все физические устройства вашего компьютера отображаются в каталог **`/dev`** файловой системы дистрибутива (об этом — ниже). Диски (в том числе IDE/SATA/SCSI/SAS жёсткие диски, USB-диски) имеют имена:

- **`/dev/sda`** — первый диск;
- **`/dev/sdb`** — второй диск;
- и т.д.

Диски обозначаются **`/dev/sd`*X***, где *X* — a, b, c, d, e, … в зависимости от порядкового номера диска на шине.

Раздел диска обозначается числом после его имени. Например, **/dev/sdb4** — четвертый раздел второго диска.

51.1.6. Разделы, необходимые для работы ОС

Для работы ОС на жестком диске (дисках) должны быть созданы, по крайней мере, два раздела: корневой (то есть тот, который будет содержать каталог **/**) и раздел для ядра (**/boot**). Если на диске много свободного места, то можно создать отдельные разделы для каталогов **/usr**, **/home**, **/var**.

51.2. Работа с наиболее часто используемыми компонентами

51.2.1. Виртуальная консоль

Система Альт Сервер для Эльбрус предоставляет доступ к виртуальным консолям, с которых можно осуществлять одновременно несколько сеансов работы в системе (login session).

Только что установленная система Альт Сервер для Эльбрус, возможно, предоставляет доступ только к первым шести виртуальным консолям, к которым можно обращаться, нажимая комбинации клавиш **Alt**+**F1** — **Alt**+**F6** (**Ctrl**+**Alt**+**F1** — **Ctrl**+**Alt**+**F6**).

51.2.2. Командные оболочки (интерпретаторы)

Для управления ОС используются командные интерпретаторы (shell).

Зайдя в систему, Вы увидите приглашение — строку, содержащую символ «**$**» (далее этот символ будет обозначать командную строку). Программа ожидает ваших команд. Роль командного интерпретатора — передавать ваши команды операционной системе. По своим функциям он соответствует **command.com** в DOS, но несравненно мощнее. При помощи командных интерпретаторов можно писать небольшие программы — сценарии (скрипты). В Linux доступны следующие командные оболочки:

- **bash** — самая распространенная оболочка под linux. Она ведет историю команд и предоставляет возможность их редактирования;
- **pdksh** — клон korn shell, хорошо известной оболочки в UNIX™ системах.

Проверить, какая оболочка используется в данный момент можно, выполнив команду:

```
$ echo $SHELL
```

Оболочкой по умолчанию является Bash (Bourne Again Shell) — самая распространённая оболочка под Linux, которая ведет историю команд и предоставляет возможность их редактирования. В дальнейшем описании работы с Альт Сервер для Эльбрус будут использоваться примеры с использованием этой оболочки.

51.2.3. Командная оболочка Bash

В Bash имеется несколько приемов для работы со строкой команд. Например, можно использовать следующие сочетания:

- **Ctrl**+**A** — перейти на начало строки;

- **Ctrl**+**U** — удалить текущую строку;
- **Ctrl**+**C** — остановить текущую задачу.

Для ввода нескольких команд одной строкой можно использовать разделитель «**;**». По истории команд можно перемещаться с помощью клавиш **↑** («вверх») и **↓** («вниз»).

Чтобы найти конкретную команду в списке набранных, не пролистывая всю историю, можно нажать **Ctrl**+**R** и начать вводить символы ранее введенной команды.

Для просмотра истории команд можно воспользоваться командой **history**. Команды, присутствующие в истории, отображаются в списке пронумерованными. Чтобы запустить конкретную команду необходимо набрать:

```
!номер команды
```

Если ввести:

```
!!
```

запустится последняя из набранных команд.

В Bash имеется возможность самостоятельного завершения имен команд из общего списка команд, что облегчает работу при вводе команд, в случае, если имена программ и команд слишком длинны. При нажатии клавиши **Tab** Bash завершает имя команды, программы или каталога, если не существует нескольких альтернативных вариантов. Например, чтобы использовать программу декомпрессии **gunzip**, можно набрать следующую команду:

```
gu
```

Затем нажать клавишу **Tab**. Так как в данном случае существует несколько возможных вариантов завершения команды, то необходимо повторно нажать клавишу **Tab**, чтобы получить список имен, начинающихся с **gu**.

В предложенном примере можно получить следующий список:

```
 $  gu
guile gunzip gupnp-binding-tool
```

Если набрать: **n** (**gunzip** — это единственное имя, третьей буквой которого является «**n**»), а затем нажать клавишу **Tab**, то оболочка самостоятельно дополнит имя. Чтобы запустить команду нужно нажать **Enter**.

Программы, вызываемые из командной строки, Bash ищет в каталогах, определяемых в системной переменной **$PATH**. По умолчанию в этот перечень каталогов не входит текущий каталог, обозначаемый **./** (точка слеш) (если только не выбран один из двух самых слабых уровней защиты). Поэтому, для запуска программы из текущего каталога, необходимо использовать команду (в примере запускается команда **prog**):

```
./prog
```

51.2.4. Команда

Простейшая команда состоит из одного «слова», например, команда **`cal`**, выводящая календарь на текущий месяц.

```
$ cal
    Сентябрь 2023
Пн Вт Ср Чт Пт Сб Вс
             1  2  3
 4  5  6  7  8  9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30
```

51.2.5. Команда и параметры

```
$ cal 1 2024
     Январь 2024
Пн Вт Ср Чт Пт Сб Вс
 1  2  3  4  5  6  7
 8  9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 31
```

Команда **`cal 1 2024`** состоит из двух частей — собственно команды **`cal`** и «остального». То, что следует за командой называется *параметрами* (или аргументами) и они вводятся для изменения поведения команды. В большинстве случаев, первое слово считается именем команды, а остальные — её параметрами.

51.2.6. Команда и ключи

Для решения разных задач одни и те же действия необходимо выполнять по-разному. Например, для синхронизации работ в разных точках земного шара лучше использовать единое для всех время (по Гринвичу), а для организации собственного рабочего дня — местное время (с учётом сдвига по часовому поясу и разницы зимнего и летнего времени). И то, и другое время показывает команда **`date`**, только для работы по Гринвичу ей нужен дополнительный параметр ***`-u`*** (он же ***`--universal`***).

```
$ date
Ср 27 сен 2023 18:58:50 EET
$ date -u
Ср 27 сен 2023 16:59:09 UTC
```

Такого рода параметры называются *ключами* или *модификаторами выполнения*. Ключ принадлежит данной конкретной команде и сам по себе смысла не имеет. Этим он отличается от других параметров (например, имён файлов, чисел), имеющих собственный смысл, не зависящий ни от какой команды. Каждая команда может распознавать некоторый набор ключей и соответственно изменять своё поведение. Один и тот же ключ может определять для разных команд совершенно разные значения.

Для формата ключей нет жёсткого стандарта, однако существуют договорённости:

- Если ключ начинается на -, то это *однобуквенный ключ*. За -, как правило, следует один символ, чаще всего буква, обозначающая действие или свойство, которое этот ключ придаёт команде. Так проще отличать ключи от других параметров.
- Если ключ начинается на --, то он называется *полнословным ключом*. Полнословный формат ключа начинается на два знака --, за которыми следует полное имя обозначаемого этим ключом содержания.

Некоторые ключи имеют и однобуквенный, и полнословный формат, а некоторые — только полнословный.

Информацию о ресурсах каждой команды можно получить, используя ключ ***--help***. К примеру, получить подсказку о том, что делает команда **rm**, можно, набрав в терминале **rm *--help***.

51.2.7. Обзор основных команд системы

Все команды, приведенные ниже, могут быть запущены в режиме консоли. Для получения более подробной информации используйте команду **man**. Пример:

```
$ man ls
```

Примечание

Параметры команд обычно начинаются с символа «-», и обычно после одного символа «-» можно указать сразу несколько опций. Например, вместо команды **ls -l -F** можно ввести команду **ls -lF**

Учетные записи пользователей

Команда su

Команда **su** позволяет изменить «владельца» текущего сеанса (сессии) без необходимости завершать сеанс и открывать новый.

Синтаксис:

```
su [ОПЦИИ...] [ПОЛЬЗОВАТЕЛЬ]
```

Команду можно применять для замены текущего пользователя на любого другого, но чаще всего она используется для получения пользователем прав суперпользователя (root).

При вводе команды **su -** будет запрошен пароль суперпользователя (root), и, в случае ввода корректного пароля, пользователь получит права администратора. Чтобы вернуться к правам пользователя, необходимо ввести команду:

```
exit
```

Более подробную информацию о режиме суперпользователя вы можете прочитать в главе Режим суперпользователя.

Команда `id`

Команда **`id`** выводит информацию о пользователе и группах, в которых он состоит, для заданного пользователя или о текущем пользователе (если ничего не указано).

Синтаксис:

```
id [ОПЦИИ...] [ПОЛЬЗОВАТЕЛЬ]
```

Команда `passwd`

Команда **`passwd`** меняет (или устанавливает) пароль, связанный с входным_именем пользователя.

Обычный пользователь может менять только пароль, связанный с его собственным входным_именем.

Команда запрашивает у обычных пользователей старый пароль (если он был), а затем дважды запрашивает новый. Новый пароль должен соответствовать техническим требованиям к паролям, заданным администратором системы.

Основные операции с файлами и каталогами

Команда `ls`

Команда **`ls`** (list) печатает в стандартный вывод содержимое каталогов.

Синтаксис:

```
ls [ОПЦИИ...] [ФАЙЛ...]
```

Основные опции:

- **`-a`** — просмотр всех файлов, включая скрытые;
- **`-l`** — отображение более подробной информации;
- **`-R`** — выводить рекурсивно информацию о подкаталогах.

Команда `cd`

Команда **`cd`** предназначена для смены каталога. Команда работает как с абсолютными, так и с относительными путями. Если каталог не указан, используется значение переменной окружения **`$HOME`** (домашний каталог пользователя). Если каталог задан полным маршрутным именем, он становится текущим. По отношению к новому каталогу нужно иметь право на выполнение, которое в данном случае трактуется как разрешение на поиск.

Синтаксис:

```
cd [-L|-P] [КАТАЛОГ]
```

Если в качестве аргумента задано «-», то это эквивалентно **`$OLDPWD`**. Если переход был осуществлен по переменной окружения **`$CDPATH`** или в качестве аргумента был задан «-» и смена каталога была успешной, то абсолютный путь нового рабочего каталога будет выведен на стандартный вывод.

Примеры:

- находясь в домашнем каталоге перейти в его подкаталог **docs/** (относительный путь):

```
cd docs/
```

- сделать текущим каталог **/usr/bin** (абсолютный путь):

```
cd /usr/bin/
```

- сделать текущим родительский каталог:

```
cd ..
```

- вернуться в предыдущий каталог:

```
cd -
```

- сделать текущим домашний каталог:

```
cd
```

Команда pwd

Команда **pwd** выводит абсолютный путь текущего (рабочего) каталога.

Синтаксис:

```
pwd [-L|-P]
```

Опции:

- **-P** — не выводить символические ссылки;
- **-L** — выводить символические ссылки.

Команда rm

Команда **rm** служит для удаления записей о файлах. Если заданное имя было последней ссылкой на файл, то файл уничтожается.

Предупреждение

Удалив файл, вы не сможете его восстановить!

Синтаксис:

```
rm [ОПЦИИ...] <ФАЙЛ>
```

Основные опции:

- **-f** — никогда не запрашивать подтверждения;

- **-i** — всегда запрашивать подтверждение;
- **-r, -R** — рекурсивно удалять содержимое указанных каталогов.

Пример. Удалить все файлы **html** в каталоге **~/html**:

```
rm -i ~/html/*.html
```

Команда mkdir

mkdir — команда для создания новых каталогов.

Синтаксис:

```
mkdir [-p] [-m права] <КАТАЛОГ...>
```

Команда rmdir

Команда **rmdir** удаляет каталоги из файловой системы. Каталог должен быть пуст перед удалением.

Синтаксис:

```
rmdir [ОПЦИИ...] <КАТАЛОГ...>
```

Основные опции:

- **-p** — удалить каталог и его потомки.

Команда **rmdir** часто заменяется командой **rm -rf**, которая позволяет удалять каталоги, даже если они не пусты.

Команда cp

Команда **cp** предназначена для копирования файлов из одного в другие каталоги.

Синтаксис:

```
cp [-fip] [ИСХ_ФАЙЛ...] [ЦЕЛ_ФАЙЛ...]
```

```
cp [-fip] [ИСХ_ФАЙЛ...] [КАТАЛОГ]
```

```
cp [-R] [[-H] | [-L] | [-P]] [-fip] [ИСХ_ФАЙЛ...] [КАТАЛОГ]
```

Основные опции:

- **-p** — сохранять по возможности времена изменения и доступа к файлу, владельца и группу, права доступа;
- **-i** — запрашивать подтверждение перед копированием в существующие файлы;
- **-r, -R** — рекурсивно копировать содержимое каталогов.

Команда mv

Команда **mv** предназначена для перемещения файлов.

Синтаксис:

```
mv [-fi] [ИСХ_ФАЙЛ...] [ЦЕЛ_ФАЙЛ...]
```

```
mv [-fi] [ИСХ_ФАЙЛ...] [КАТАЛОГ]
```

В первой синтаксической форме, характеризующейся тем, что последний операнд не является ни каталогом, ни символической ссылкой на каталог, **mv** перемещает исх_файл в цел_файл (происходит переименование файла).

Во второй синтаксической форме **mv** перемещает исходные файлы в указанный каталог под именами, совпадающими с краткими именами исходных файлов.

Основные опции:

- **-f** — не запрашивать подтверждения перезаписи существующих файлов;
- **-i** — запрашивать подтверждение перезаписи существующих файлов.

Команда cat

Команда **cat** последовательно выводит содержимое файлов.

Синтаксис:

```
cat [ОПЦИИ...] [ФАЙЛ...]
```

Основные опции:

- **-n, --number** — нумеровать все строки при выводе;
- **-E, --show-ends** — показывать $ в конце каждой строки.

Если файл не указан, читается стандартный ввод. Если в списке файлов присутствует имя «-», вместо этого файла читается стандартный ввод.

Команда head

Команда **head** выводит первые 10 строк каждого файла на стандартный вывод.

Синтаксис:

```
head [ОПЦИИ] [ФАЙЛ...]
```

Основные опции:

- **-n, --lines=[-]K** — вывести первые K строк каждого файла, а не первые 10;
- **-q, --quiet** — не печатать заголовки с именами файлов.

Команда less

Команда **less** позволяет постранично просматривать текст (для выхода необходимо нажать **q**).

Синтаксис:

```
less <ФАЙЛ>
```

Команда grep

Команда **grep** имеет много опций и предоставляет возможности поиска символьной строки в файле.

Синтаксис:

```
grep [шаблон_поиска] <ФАЙЛ>
```

Поиск файлов

Команда find

Команда **find** предназначена для поиска всех файлов, начиная с корневого каталога. Поиск может осуществляться по имени, типу или владельцу файла.

Синтаксис:

```
find [-H] [-L] [-P] [-Оуровень] [-D help|tree|search|stat|rates|opt|exec]
[ПУТЬ…] [ВЫРАЖЕНИЕ]
```

Ключи для поиска:

- **-name** — поиск по имени файла;
- **-type** — поиск по типу f=файл, d=каталог, l=ссылка(lnk);
- **-user** — поиск по владельцу (имя или UID).

Когда выполняется команда **find**, можно выполнять различные действия над найденными файлами. Основные действия:

- **-exec команда \;** — выполнить команду. Запись команды должна заканчиваться экранированной точкой с запятой. Строка «{}» заменяется текущим маршрутным именем файла;
- **execdir команда \;** — то же самое что и **-exec**, но команда вызывается из подкаталога, содержащего текущий файл;
- **-ok команда** — эквивалентно **-exec** за исключением того, что перед выполнением команды запрашивается подтверждение (в виде сгенерированной командной строки со знаком вопроса в конце) и она выполняется только при ответе: «y»;
- **-print** — вывод имени файла на экран.

Путем по умолчанию является текущий подкаталог. Выражение по умолчанию **-print**.

Примеры:

- найти в текущем каталоге обычные файлы (не каталоги), имя которых начинается с символа «~»:

  ```
  find . -type f -name "~*" -print
  ```

- найти в текущем каталоге файлы, измененные позже, чем файл **file.bak**:

```
find . -newer file.bak -type f -print
```

- удалить все файлы с именами **a.out** или ***.o**, доступ к которым не производился в течение недели:

```
find / \( -name a.out -o -name '*.o' \) \ -atime +7 -exec rm {} \;
```

- удалить из текущего каталога и его подкаталогов все файлы нулевого размера, запрашивая подтверждение:

```
find . -size 0c -ok rm {} \;
```

Команда whereis

whereis сообщает путь к исполняемому файлу программы, ее исходным файлам (если есть) и соответствующим страницам справочного руководства.

Синтаксис:

```
whereis [ОПЦИИ...] <ФАЙЛ>
```

Опции:

- **-b** — вывод информации только об исполняемых файлах;
- **-m** — вывод информации только о страницах справочного руководства;
- **-s** — вывод информации только об исходных файлах.

Мониторинг и управление процессами

Команда ps

Команда **ps** отображает список текущих процессов.

Синтаксис:

```
ps [ОПЦИИ...]
```

По умолчанию выводится информация о процессах с теми же действующим UID и управляющим терминалом, что и у подающего команду пользователя.

Основные опции:

- **-a** — вывести информацию о процессах, ассоциированных с терминалами;
- **-f** — вывести «полный» список;
- **-l** — вывести «длинный» список;
- **-p список** — вывести информацию о процессах с перечисленными в списке PID;
- **-u список** — вывести информацию о процессах с перечисленными идентификаторами или именами пользователей.

Команда `kill`

Команда **`kill`** позволяет прекратить исполнение процесса или передать ему сигнал.

Синтаксис:

```
kill [-s] [сигнал] [идентификатор] [...]
```

```
kill [-l] [статус_завершения]
```

```
kill [-номер_сигнала] [идентификатор] [...]
```

Идентификатор — PID ведущего процесса задания или номер задания, предварённый знаком «%».

Основные опции:

- **`-l`** — вывести список поддерживаемых сигналов;
- **`-s сигнал, -сигнал`** — послать сигнал с указанным именем.

Если обычная команда **`kill`** не дает желательного эффекта, необходимо использовать команду **`kill`** с параметром **`-9`** (**`kill -9`** *PID_номер*).

Команда `df`

Команда **`df`** показывает количество доступного дискового пространства в файловой системе, в которой содержится файл, переданный как аргумент. Если ни один файл не указан, показывается доступное место на всех смонтированных файловых системах. Размеры по умолчанию указаны в блоках по 1КБ.

Синтаксис:

```
df [ОПЦИИ] [ФАЙЛ...]
```

Основные опции:

- **`--total`** — подсчитать общий объем в конце;
- **`-h, --human-readable`** — печатать размеры в удобочитаемом формате (например, 1K, 234M, 2G).

Команда `du`

Команда **`du`** подсчитывает использование диска каждым файлом, для каталогов подсчет происходит рекурсивно.

Синтаксис:

```
du [ОПЦИИ] [ФАЙЛ...]
```

Основные опции:

- **`-a, --all`** — выводить общую сумму для каждого заданного файла, а не только для каталогов;

- **-c, --total** — подсчитать общий объем в конце. Может быть использовано для выяснения суммарного использования дискового пространства для всего списка заданных файлов;
- **-d, --max-depth=N** — выводить объем для каталога (или файлов, если указано **--all**) только если она на N или менее уровней ниже аргументов командной строки;
- **-S, --separate-dirs** — выдавать отдельно размер каждого каталога, не включая размеры подкаталогов;
- **-s, --summarize** — отобразить только сумму для каждого аргумента.

Команда which

Команда **which** отображает полный путь к указанным командам или сценариям.

Синтаксис:

```
which [ОПЦИИ] <ФАЙЛ...>
```

Основные опции:

- **-a, --all** — выводит все совпавшие исполняемые файлы по содержимому в переменной окружения **$PATH**, а не только первый из них;
- **-c, --total** — подсчитать общий объем в конце. Может быть использовано для выяснения суммарного использования дискового пространства для всего списка заданных файлов;
- **-d, --max-depth=N** — выводить объем для каталога (или файлов, если указано **--all**) только если она на N или менее уровней ниже аргументов командной строки;
- **-S, --separate-dirs** — выдавать отдельно размер каждого каталога, не включая размеры подкаталогов;
- **--skip-dot** — пропускает все каталоги из переменной окружения **$PATH**, которые начинаются с точки.

Использование многозадачности

Альт Сервер для Эльбрус — это многозадачная система.

Для того чтобы запустить программу в фоновом режиме, необходимо набрать «**&**» после имени программы. После этого оболочка даст возможность запускать другие приложения.

Так как некоторые программы интерактивны — их запуск в фоновом режиме бессмысленен. Подобные программы просто остановятся, если их запустить в фоновом режиме.

Можно также запускать нескольких независимых сеансов. Для этого в консоли необходимо набрать **Alt** и одну из клавиш, находящихся в интервале от **F1** до **F6**. На экране появится новое приглашение системы, и можно открыть новый сеанс. Этот метод также позволяет вам работать на другой консоли, если консоль, которую вы использовали до этого, не отвечает или вам необходимо остановить зависшую программу.

Команда bg

Команда **bg** позволяет перевести задание на задний план.

Синтаксис:

```
bg [ИДЕНТИФИКАТОР ...]
```

Идентификатор — PID ведущего процесса задания или номер задания, предварённый знаком «%».

Команда `fg`

Команда **`fg`** позволяет перевести задание на передний план.

Синтаксис:

```
fg [ИДЕНТИФИКАТОР ...]
```

Идентификатор — PID ведущего процесса задания или номер задания, предварённый знаком «%».

Сжатие и упаковка файлов

Команда `tar`

Сжатие и упаковка файлов выполняется с помощью команды **`tar`**, которая преобразует файл или группу файлов в архив без сжатия (tarfile).

Упаковка файлов в архив чаще всего выполняется следующей командой:

```
tar -cf [имя создаваемого файла архива] [упаковываемые файлы и/или
каталоги]
```

Пример использования команды упаковки архива:

```
tar -cf moi_dokumenti.tar Docs project.tex
```

Распаковка содержимого архива в текущий каталог выполняется командой:

```
tar -xf [имя файла архива]
```

Для сжатия файлов используются специальные программы сжатия: **`gzip`**, **`bzip2`** и **`7z`**.

51.3. Стыкование команд в системе Linux

51.3.1. Стандартный ввод и стандартный вывод

Многие команды системы имеют так называемые стандартный ввод (standard input) и стандартный вывод (standard output), часто сокращаемые до stdin и stdout. Ввод и вывод здесь — это входная и выходная информация для данной команды. Программная оболочка делает так, что стандартным вводом является клавиатура, а стандартным выводом — экран монитора.

Пример с использованием команды **`cat`**. По умолчанию команда **`cat`** читает данные из всех файлов, которые указаны в командной строке, и посылает эту информацию непосредственно в стандартный вывод (stdout). Следовательно, команда:

```
cat history-final masters-thesis
```

выведет на экран сначала содержимое файла **history-final**, а затем — файла **masters-thesis**.

Если имя файла не указано, команда **cat** читает входные данные из stdin и возвращает их в stdout. Пример:

```
cat
Hello there.
Hello there.
Bye.
Bye.
Ctrl-D
```

Каждую строку, вводимую с клавиатуры, команда **cat** немедленно возвращает на экран. При вводе информации со стандартного ввода конец текста сигнализируется вводом специальной комбинации клавиш, как правило, **Ctrl**+**D**. Сокращённое название сигнала конца текста — EOT (end of text).

51.3.2. Перенаправление ввода и вывода

При необходимости можно перенаправить стандартный вывод, используя символ >, и стандартный ввод, используя символ <.

Фильтр (filter) — программа, которая читает данные из стандартного ввода, некоторым образом их обрабатывает и результат направляет на стандартный вывод. Когда применяется перенаправление, в качестве стандартного ввода и вывода могут выступать файлы. Как указывалось выше, по умолчанию, stdin и stdout относятся к клавиатуре и к экрану соответственно. Команда **sort** является простым фильтром — она сортирует входные данные и посылает результат на стандартный вывод. Совсем простым фильтром является команда **cat** — она ничего не делает с входными данными, а просто пересылает их на выход.

51.3.3. Использование состыкованных команд

Стыковку команд (pipelines) осуществляет командная оболочка, которая stdout первой команды направляет на stdin второй команды. Для стыковки используется символ |. Направить stdout команды **ls** на stdin команды **sort**:

```
ls | sort -r
notes
masters-thesis
history-final
english-list
```

Вывод списка файлов частями:

```
ls /usr/bin | more
```

Если необходимо вывести на экран последнее по алфавиту имя файла в текущем каталоге, можно использовать следующую команду:

```
ls | sort -r | head -1 notes
```

где команда **head -1** выводит на экран первую строку получаемого ей входного потока строк (в примере поток состоит из данных от команды **ls**), отсортированных в обратном алфавитном порядке.

51.3.4. Недеструктивное перенаправление вывода

Эффект от использования символа > для перенаправления вывода файла является деструктивным; т.е, команда

```
ls > file-list
```

уничтожит содержимое файла **file-list**, если этот файл ранее существовал, и создаст на его месте новый файл. Если вместо этого перенаправление будет сделано с помощью символов >>, то вывод будет приписан в конец указанного файла, при этом исходное содержимое файла не будет уничтожено.

Примечание

Перенаправление ввода и вывода и стыкование команд осуществляется командными оболочками, которые поддерживают использование символов >, >> и |. Сами команды не способны воспринимать и интерпретировать эти символы.

Глава 52. Средства управления дискреционными правами доступа

52.1. Команда chmod

Команда **chmod** предназначена для изменения прав доступа файлов и каталогов.

Синтаксис:

```
chmod [ОПЦИИ] РЕЖИМ[,РЕЖИМ]... <ФАЙЛ>
```

```
chmod [ОПЦИИ] --reference=ИФАЙЛ <ФАЙЛ>
```

Основные опции:

- **-R** — рекурсивно изменять режим доступа к файлам, расположенным в указанных каталогах;
- **--reference=ИФАЙЛ** — использовать режим файла ИФАЙЛ.

chmod изменяет права доступа каждого указанного файла в соответствии с правами доступа, указанными в параметре режим, который может быть представлен как в символьном виде, так и в виде восьмеричного, представляющего битовую маску новых прав доступа.

Формат символьного режима следующий:

```
[ugoa...][[+-=][разрешения...]...]
```

Здесь разрешения — это ноль или более букв из набора «rwxXst» или одна из букв из набора «ugo».

Каждый аргумент — это список символьных команд изменения прав доступа, разделеных запятыми. Каждая такая команда начинается с нуля или более букв «ugoa», комбинация которых указывает, чьи права доступа к файлу будут изменены: пользователя, владеющего файлом (u), пользователей, входящих в группу, к которой принадлежит файл (g), остальных пользователей (o) или всех пользователей (a). Если не задана ни одна буква, то автоматически будет использована буква «a», но биты, установленные в umask, не будут затронуты.

Оператор «+» добавляет выбранные права доступа к уже имеющимся у каждого файла, «-» удаляет эти права. «=» присваивает только эти права каждому указанному файлу.

Буквы «rwxXst» задают биты доступа для пользователей: «r» — чтение, «w» — запись, «x» — выполнение (или поиск для каталогов), «X» — выполнение/поиск только если это каталог или же файл с уже установленным битом выполнения, «s» — задать ID пользователя и группы при выполнении, «t» — запрет удаления.

Числовой режим состоит из не более четырех восьмеричных цифр (от нуля до семи), которые складываются из битовых масок с разрядами «4», «2» и «1». Любые пропущенные разряды дополняются лидирующими нулями:

- первый разряд выбирает установку идентификатора пользователя (setuid) (4) или идентификатора группы (setgid) (2) или sticky-бита (1);
- второй разряд выбирает права доступа для пользователя, владеющего данным файлом: чтение (4), запись (2) и исполнение (1);
- третий разряд выбирает права доступа для пользователей, входящих в данную группу, с тем же смыслом, что и у второго разряда;
- четвертый разряд выбирает права доступа для остальных пользователей (не входящих в данную группу), опять с тем же смыслом.

Примеры:

- установить права, позволяющие владельцу читать и писать в файл **f1**, а членам группы и прочим пользователям только читать. Команду можно записать двумя способами:

  ```
  $ chmod 644 f1
  $ chmod u=rw,go=r f1
  ```

- позволить всем выполнять файл **f2**:

```
$ chmod +x f2
```

- запретить удаление файла **f3**:

```
$ chmod +t f3
```

- дать всем права на чтение запись и выполнение, а также на переустановку идентификатора группы при выполнении файла **f4**:

```
$ chmod =rwx,g+s f4
$ chmod 2777 f4
```

52.2. Команда chown

Команда **chown** изменяет владельца и/или группу для каждого заданного файла.

Синтаксис:

```
chown [КЛЮЧ]…[ВЛАДЕЛЕЦ][:[ГРУППА]] <ФАЙЛ>
```

```
chown [ОПЦИИ] --reference=ИФАЙЛ <ФАЙЛ>
```

Основные опции:

- **-R** — рекурсивно изменять файлы и каталоги;
- **--reference=ИФАЙЛ** — использовать владельца и группу файла ИФАЙЛ.

Изменить владельца может только владелец файла или суперпользователь.

Владелец не изменяется, если он не задан в аргументе. Группа также не изменяется, если не задана, но если после символьного ВЛАДЕЛЬЦА стоит символ «:», подразумевается изменение группы на основную группу текущего пользователя. Поля ВЛАДЕЛЕЦ и ГРУППА могут быть как числовыми, так и символьными.

Примеры:

- поменять владельца каталога **/u** на пользователя test:

```
chown test /u
```

- поменять владельца и группу каталога **/u**:

```
chown test:staff /u
```

- поменять владельца каталога **/u** и вложенных файлов на test:

```
chown -hR test /u
```

52.3. Команда chgrp

Команда **chgrp** изменяет группу для каждого заданного файла.

Синтаксис:

```
chgrp [ОПЦИИ] ГРУППА <ФАЙЛ>
```

```
chgrp [ОПЦИИ] --reference=ИФАЙЛ <ФАЙЛ>
```

Основные опции:

- **-R** — рекурсивно изменять файлы и каталоги;
- **--reference=ИФАЙЛ** — использовать группу файла ИФАЙЛ.

52.4. Команда umask

Команда **umask** задает маску режима создания файла в текущей среде командного интерпретатора равной значению, задаваемому операндом режим. Эта маска влияет на начальное значение битов прав доступа всех создаваемых далее файлов.

Синтаксис:

```
umask [-p] [-S] [режим]
```

Пользовательской маске режима создания файлов присваивается указанное восьмеричное значение. Три восьмеричные цифры соответствуют правам на чтение/запись/выполнение для владельца, членов группы и прочих пользователей соответственно. Значение каждой заданной в маске цифры вычитается из соответствующей «цифры», определенной системой при создании файла. Например, umask 022 удаляет права на запись для членов группы и прочих пользователей (у файлов, создававшихся с режимом 777, он оказывается равным 755; а режим 666 преобразуется в 644).

Если маска не указана, выдается ее текущее значение:

```
$ umask
0022
```

или то же самое в символьном режиме:

```
$ umask -S
u=rwx,g=rx,o=rx
```

Команда **umask** распознается и выполняется командным интерпретатором bash.

52.5. Команда chattr

Команда **chattr** изменяет атрибуты файлов на файловых системах ext3, ext4.

Синтаксис:

```
chattr [ -RVf ] [+-=aAcCdDeFijmPsStTux] [ -v версия ] <ФАЙЛЫ> …
```

Опции:

- **-R** — рекурсивно изменять атрибуты каталогов и их содержимого. Символические ссылки игнорируются;
- **-V** — выводит расширенную информацию и версию программы;
- **-f** — подавлять сообщения об ошибках;
- **-v версия** — установить номер версии/генерации файла.

Формат символьного режима:

```
+-=aAcCdDeFijmPsStTux
```

Оператор «+» означает добавление выбранных атрибутов к существующим атрибутам; «-» означает их снятие; «=» означает определение только этих указанных атрибутов для файлов.

Символы «aAcCdDeFijmPsStTux» указывают на новые атрибуты файлов:

- ***a*** — только добавление к файлу;
- ***A*** — не обновлять время последнего доступа (atime) к файлу;
- ***c*** — сжатый файл;
- ***C*** — отключение режима «Copy-on-write» для указанного файла;
- ***d*** — не архивировать (отключает создание архивной копии файла командой dump);
- ***D*** — синхронное обновление каталогов;
- ***e*** — включает использование extent при выделении места на устройстве (атрибут не может быть отключён с помощью **chattr**);
- ***F*** — регистронезависимый поиск в каталогах;
- ***i*** — неизменяемый файл (файл защищен от изменений: не может быть удалён или переименован, к этому файлу не могут быть созданы ссылки, и никакие данные не могут быть записаны в этот файл);
- ***j*** — ведение журнала данных (данные файла перед записью будут записаны в журнал ext3/ext4);
- ***m*** — не сжимать;
- ***P*** — каталог с вложенными файлами является иерархической структурой проекта;
- ***s*** — безопасное удаление (перед удалением все содержимое файла полностью затирается «00»);
- ***S*** — синхронное обновление (аналогичен опции монтирования «sync» файловой системы);
- ***t*** — отключает метод tail-merging для файлов;
- ***T*** — вершина иерархии каталогов;

- ***u*** — неудаляемый (при удалении файла его содержимое сохраняется, это позволяет пользователю восстановить файл);
- ***x*** — прямой доступ к файлам (атрибут не может быть установлен с помощью **chattr**).

52.6. Команда lsattr

Команда **lsattr** выводит атрибуты файла расширенной файловой системы.

Синтаксис:

```
lsattr [ -RVadlpv ] <ФАЙЛЫ> …
```

Опции:

- **-R** — рекурсивно изменять атрибуты каталогов и их содержимого. Символические ссылки игнорируются;
- **-V** — выводит расширенную информацию и версию программы;
- **-a** — просматривает все файлы в каталоге, включая скрытые файлы (имена которых начинаются с «.»);
- **-d** — отображает каталоги также, как и файлы вместо того, чтобы просматривать их содержимое;
- **-l** — отображает параметры, используя длинные имена вместо одного символа;
- **-p** — выводит номер проекта файла;
- **-v** — выводит номер версии/генерации файла.

52.7. Команда getfacl

Команда **getfacl** выводит атрибуты файла расширенной файловой системы.

Синтаксис:

```
getfacl [ --aceEsRLPtpndvh ] <ФАЙЛ> …
```

Опции:

- **-a** — вывести только ACL файла;
- **-d** — вывести только ACL по умолчанию;
- **-c** — не показывать заголовок (имя файла);
- **-e** — показывать все эффективные права;
- **-E** — не показывать эффективные права;
- **-s** — пропускать файлы, имеющие только основные записи;
- **-R** — для подкаталогов рекурсивно;

- **-L** — следовать по символическим ссылкам, даже если они не указаны в командной строке;
- **-P** — не следовать по символическим ссылкам, даже если они указаны в командной строке;
- **-t** — использовать табулированный формат вывода;
- **-p** — не удалять ведущие «/» из пути файла;
- **-n** — показывать числовые значения пользователя/группы.

Формат вывода:

```
1: # file: somedir/
2: # owner: lisa
3: # group: staff
4: # flags: -s-
5: user::rwx
6: user:joe:rwx                  #effective:r-x
7: group::rwx                    #effective:r-x
8: group:cool:r-x
9: mask:r-x
10: other:r-x
11: default:user::rwx
12: default:user:joe:rwx#effective:r-x
13: default:group::r-x
14: default:mask:r-x
15: default:oter:---
```

Строки 1 — 3 указывают имя файла, владельца и группу владельцев.

В строке 4 указаны биты setuid (s), setgid (s) и sticky (t): либо буква, обозначающая бит, либо тире (-). Эта строка включается, если какой-либо из этих битов установлен, и опускается в противном случае, поэтому она не будет отображаться для большинства файлов.

Строки 5, 7 и 10 относятся к традиционным битам прав доступа к файлу, соответственно, для владельца, группы-владельца и всех остальных. Эти три элемента являются базовыми. Строки 6 и 8 являются элементами для отдельных пользователя и группы. Строка 9 — маска эффективных прав. Этот элемент ограничивает эффективные права, предоставляемые всем группам и отдельным пользователям. Маска не влияет на права для владельца файла и всех других. Строки 11 — 15 показывают ACL по умолчанию, ассоциированный с данным каталогом.

52.8. Команда setfacl

Команда **setfacl** изменяет ACL к файлам или каталогам. В командной строке за последовательностью команд идет последовательность файлов (за которой, в свою очередь, также может идти последовательность команд и так далее).

Синтаксис:

```
setfacl [-bkndRLPvh] [{-m|-x} acl_spec] [{-M|-X} acl_file] <ФАЙЛ> …
```

```
setfacl --restore=file
```

Опции:

- **-b** — удалить все разрешенные записи ACL;
- **-k** — удалить ACL по умолчанию;
- **-n** — не пересчитывать маску эффективных прав, обычно **setfacl** пересчитывает маску (кроме случая явного задания маски) для того, чтобы включить ее в максимальный набор прав доступа элементов, на которые воздействует маска (для всех групп и отдельных пользователей);
- **-d** — применить ACL по умолчанию;
- **-R** — для подкаталогов рекурсивно;
- **-L** — переходить по символическим ссылкам на каталоги (имеет смысл только в сочетании с **-R**);
- **-P** — не переходить по символическим ссылкам на каталоги (имеет смысл только в сочетании с **-R**);
- **-L** — следовать по символическим ссылкам, даже если они не указаны в командной строке;
- **-P** — не следовать по символическим ссылкам, даже если они указаны в командной строке;
- **--mask** — пересчитать маску эффективных прав;
- **-m** — изменить текущий ACL для файла;
- **-M** — прочитать записи ACL для модификации из файла;
- **-x** — удалить записи из ACL файла;
- **-X** — прочитать записи ACL для удаления из файла;
- **--restore=file** — восстановить резервную копию прав доступа, созданную командой **getfacl –R** или ей подобной. Все права доступа дерева каталогов восстанавливаются, используя этот механизм. В случае если вводимые данные содержат элементы для владельца или группы-владельца, и команда **setfacl** выполняется пользователем с именем root, то владелец и группа-владелец всех файлов также восстанавливаются. Эта опция не может использоваться совместно с другими опциями за исключением опции **--test**;
- **--set=acl** — установить ACL для файла, заменив текущий ACL;
- **--set-file=file** — прочитать записи ACL для установления из файла;
- **--test** — режим тестирования (ACL не изменяются).

При использовании опций **--set**, **-m** и **-x** должны быть перечислены записи ACL в командной строке. Элементы ACL разделяются одинарными кавычками.

При чтении ACL из файла при помощи опций **-set-file**, **-M** и **-X** команда **setfacl** принимает множество элементов в формате вывода команды **getfacl**. В строке обычно содержится не больше одного элемента ACL.

Команда **`setfacl`** использует следующие форматы элементов ACL:

- права доступа отдельного пользователя (если не задан UID, то права доступа владельца файла):

```
[d[efault]:] [u[ser]:]uid [:perms]
```

- права доступа отдельной группы (если не задан GID, то права доступа группы-владельца):

```
[d[efault]:] g[roup]:gid [:perms]
```

- маска эффективных прав:

```
[d[efault]:] m[ask][:] [:perms]
```

- права доступа всех остальных:

```
[d[efault]:] o[ther][:] [:perms]
```

Элемент ACL является абсолютным, если он содержит поле perms и является относительным, если он включает один из модификаторов: «+» или «^». Абсолютные элементы могут использоваться в операциях установки или модификации ACL. Относительные элементы могут использоваться только в операции модификации ACL. Права доступа для отдельных пользователей, группы, не содержащие никаких полей после значений UID, GID (поле perms при этом отсутствует), используются только для удаления элементов.

Значения UID и GID задаются именем или числом. Поле perms может быть представлено комбинацией символов «r», «w», «x», «-» или цифр (0 — 7).

Изначально файлы и каталоги содержат только три базовых элемента ACL: для владельца, группы-владельца и всех остальных пользователей. Существует ряд правил, которые следует учитывать при установке прав доступа:

- не могут быть удалены сразу три базовых элемента, должен присутствовать хотя бы один;
- если ACL содержит права доступа для отдельного пользователя или группы, то ACL также должен содержать маску эффективных прав;
- если ACL содержит какие-либо элементы ACL по умолчанию, то в последнем должны также присутствовать три базовых элемента (т. е. права доступа по умолчанию для владельца, группы-владельца и всех остальных);
- если ACL по умолчанию содержит права доступа для всех отдельных пользователей или групп, то в ACL также должна присутствовать маска эффективных прав.

Для того чтобы помочь пользователю выполнять эти правила, команда **`setfacl`** создает права доступа, используя уже существующие, согласно следующим условиям:

- если права доступа для отдельного пользователя или группы добавлены в ACL, а маски прав не существует, то создается маска с правами доступа группы-владельца;
- если создан элемент ACL по умолчанию, а трех базовых элементов не было, тогда делается их копия и они добавляются в ACL по умолчанию;

- если ACL по умолчанию содержит какие-либо права доступа для конкретных пользователя или группы и не содержит маску прав доступа по умолчанию, то при создании эта маска будет иметь те же права, что и группа по умолчанию.

Пример. Изменить разрешения для файла **test.txt**, принадлежащего пользователю liza и группе docs, так, чтобы:

- пользователь ivan имел права на чтение и запись в этот файл;
- пользователь misha не имел никаких прав на этот файл.

Исходные данные

```
$ ls -l test.txt
-rw-r-r-- 1 liza docs 8 янв 22 15:54 test.txt
$ getfacl test.txt
# file: test.txt
# owner: liza
# group: docs
user::rw-
group::r--
other::r--
```

Установить разрешения (от пользователя liza):

```
$ setfacl -m u:ivan:rw- test.txt
$ setfacl -m u:misha:--- test.txt
```

Просмотреть разрешения (от пользователя liza):

```
$ getfacl test.txt
# file: test.txt
# owner: liza
# group: docs
user::rw-
user:ivan:rw-
user:misha:---
group::r--
mask::rw-
other::r--
```

Примечание

Символ «+» (плюс) после прав доступа в выводе команды **ls -l** указывает на использование ACL:

```
$ ls -l test.txt
-rw-rw-r--+ 1 liza docs 8 янв 22 15:54 test.txt
```

Глава 53. Режим суперпользователя

53.1. Какие бывают пользователи?

Linux — система многопользовательская, а потому пользователь — ключевое понятие для организации всей системы доступа в Linux. Файлы всех пользователей в Linux хранятся раздельно, у каждого пользователя есть собственный домашний каталог, в котором он может хранить свои данные. Доступ других пользователей к домашнему каталогу пользователя может быть ограничен.

Суперпользователь в Linux — это выделенный пользователь системы, на которого не распространяются ограничения прав доступа. Именно суперпользователь имеет возможность произвольно изменять владельца и группу файла. Ему открыт доступ на чтение и запись к любому файлу или каталогу системы.

Среди учётных записей Linux всегда есть учётная запись суперпользователя — **root**. Поэтому вместо «суперпользователь» часто говорят «root». Множество системных файлов принадлежат **root**, множество файлов только ему доступны для чтения или записи. Пароль этой учётной записи — одна из самых больших драгоценностей системы. Именно с её помощью системные администраторы выполняют самую ответственную работу.

53.2. Для чего может понадобиться режим суперпользователя?

Системные утилиты, например, такие, как **Центр управления системой** или **Программа управления пакетами Synaptic** требуют для своей работы привилегий суперпользователя, потому что они вносят изменения в системные файлы. При их запуске выводится диалоговое окно с запросом пароля системного администратора.

53.3. Как получить права суперпользователя?

Для опытных пользователей, умеющих работать с командной строкой, существует два различных способа получить права суперпользователя.

Первый — это зарегистрироваться в системе под именем **root**.

Второй способ — воспользоваться специальной утилитой **`su`** (shell of user), которая позволяет выполнить одну или несколько команд от лица другого пользователя. По умолчанию эта утилита выполняет команду **`sh`** от пользователя **root**, то есть запускает командный интерпретатор. Отличие от предыдущего способа в том, что всегда известно, кто именно запускал **`su`**, а значит, ясно, кто выполнил определённое административное действие.

В некоторых случаях удобнее использовать не **`su`**, а утилиту **`sudo`**, которая позволяет выполнять только заранее заданные команды.

Важно

Для того чтобы воспользоваться командами **su** и **sudo**, необходимо быть членом группы **wheel**. Пользователь, созданный при установке системы, по умолчанию уже включён в эту группу.

В дистрибутивах Альт для управления доступом к важным службам используется подсистема control. control — механизм переключения между неким набором фиксированных состояний для задач, допускающих такой набор.

Команда **control** доступна только для суперпользователя (root). Для того чтобы посмотреть, что означает та или иная политика **control** (разрешения выполнения конкретной команды, управляемой **control**), надо запустить команду с ключом help:

```
# control su help
```

Запустив **control** без параметров, можно увидеть полный список команд, управляемых командой (facilities) вместе с их текущим состоянием и набором допустимых состояний.

53.4. Как перейти в режим суперпользователя?

Для перехода в режим суперпользователя наберите в терминале команду (**минус важен!**):

```
su -
```

Если воспользоваться командой **su** без ключа, то происходит вызов командного интерпретатора с правами **root**. При этом значение переменных окружения, в частности **$PATH**, остаётся таким же, как у пользователя: в переменной **$PATH** не окажется каталогов **/sbin**, **/usr/sbin**, без указания полного имени будут недоступны команды **route**, **shutdown**, **mkswap** и другие. Более того, переменная **$HOME** будет указывать на каталог пользователя, все программы, запущенные в режиме суперпользователя, сохранят свои настройки с правами **root** в каталоге пользователя, что в дальнейшем может вызвать проблемы.

Чтобы избежать этого, следует использовать **su -**. В этом режиме **su** запустит командный интерпретатор в качестве login shell, и он будет вести себя в точности так, как если бы в системе зарегистрировался **root**.

Глава 54. Управление пользователями

54.1. Общая информация

Пользователи и группы внутри системы обозначаются цифровыми идентификаторами — UID и GID, соответственно.

Пользователь может входить в одну или несколько групп. По умолчанию он входит в группу, совпадающую с его именем. Чтобы узнать, в какие еще группы входит пользователь, введите команду **id**, вывод её может быть примерно следующим:

```
uid=500(test) gid=500(test) группы=500(test),16(rpm)
```

Такая запись означает, что пользователь *test* (цифровой идентификатор 500) входит в группы *test* и *rpm*. Разные группы могут иметь разный уровень доступа к тем или иным каталогам; чем в большее количество групп входит пользователь, тем больше прав он имеет в системе.

Примечание

В связи с тем, что большинство привилегированных системных утилит в дистрибутивах Альт имеют не SUID-, а SGID-бит, будьте предельно внимательны и осторожны в переназначении групповых прав на системные каталоги.

54.2. Команда useradd

Команда useradd регистрирует нового пользователя или изменяет информацию по умолчанию о новых пользователях.

Синтаксис:

```
useradd [ОПЦИИ...] <ИМЯ ПОЛЬЗОВАТЕЛЯ>
useradd -D [ОПЦИИ...]
```

Некоторые опции:

- **-b каталог** — базовый каталог для домашнего каталога новой учётной записи;
- **-c комментарий** — текстовая строка (обычно используется для указания фамилии и мени);
- **-d каталог** — домашний каталог новой учётной записи;
- **-D** — показать или изменить настройки по умолчанию для useradd;
- **-e дата** — дата устаревания новой учётной записи;
- **-g группа** — имя или ID первичной группы новой учётной записи;
- **-G группы** — список дополнительных групп (через запятую) новой учётной записи;

- **-m** — создать домашний каталог пользователя;
- **-M** — не создавать домашний каталог пользователя;
- **-p пароль** — зашифрованный пароль новой учётной записи (не рекомендуется);
- **-s оболочка** — регистрационная оболочка новой учётной записи (по умолчанию **/bin/bash**);
- **-u UID** — пользовательский ID новой учётной записи.

Команда **useradd** имеет множество параметров, которые позволяют менять её поведение по умолчанию. Например, можно принудительно указать, какой будет UID или какой группе будет принадлежать пользователь:

```
# useradd -u 1500 -G usershares new_user
```

54.3. Команда passwd

Команда passwd поддерживает традиционные опции **passwd** и утилит **shadow**.

Синтаксис:

```
passwd [ОПЦИИ...] [ИМЯ ПОЛЬЗОВАТЕЛЯ]
```

Возможные опции:

- **-d**, **--delete** — удалить пароль для указанной записи;
- **-f**, **--force** — форсировать операцию;
- **-k**, **--keep-tokens** — сохранить не устаревшие пароли;
- **-l**, **--lock** — блокировать указанную запись;
- **--stdin** — прочитать новые пароли из стандартного ввода;
- **-S**, **--status** — дать отчет о статусе пароля в указанной записи;
- **-u**, **--unlock** — разблокировать указанную запись;
- **-?**, **--help** — показать справку и выйти;
- **--usage** — дать короткую справку по использованию;
- **-V**, **--version** — показать версию программы и выйти.

Код выхода: при успешном завершении **passwd** заканчивает работу с кодом выхода *0*. Код выхода *1* означает, что произошла ошибка. Текстовое описание ошибки выводится на стандартный поток ошибок.

Пользователь может в любой момент поменять свой пароль. Единственное, что требуется для смены пароля — знать текущий пароль.

Только суперпользователь может обновить пароль другого пользователя.

54.4. Добавление нового пользователя

Для добавления нового пользователя используйте команды **useradd** и **passwd**:

```
# useradd test1

# passwd test1
passwd: updating all authentication tokens for user test1.

You can now choose the new password or passphrase.

A valid password should be a mix of upper and lower case letters, digits, and
other characters.  You can use a password containing at least 7 characters
from all of these classes, or a password containing at least 8 characters
from just 3 of these 4 classes.
An upper case letter that begins the password and a digit that ends it do not
count towards the number of character classes used.

A passphrase should be of at least 3 words, 11 to 72 characters long, and
contain enough different characters.

Alternatively, if no one else can see your terminal now, you can pick this as
your password: "Burst*texas$Flow".

Enter new password:
Weak password: too short.
Re-type new password:
passwd: all authentication tokens updated successfully.
```

В результате описанных действий в системе появился пользователь *test1* с некоторым паролем. Если пароль оказался слишком слабым с точки зрения системы, она об этом предупредит (как в примере выше). Пользователь в дальнейшем может поменять свой пароль при помощи команды **passwd** — но если он попытается поставить слабый пароль, система откажет ему (в отличие от *root*) в изменении.

В Альт Сервер для Эльбрус для проверки паролей на слабость используется модуль PAM *passwdqc*.

54.5. Настройка парольных ограничений

Настройка парольных ограничений производится в файле **/etc/passwdqc.conf**.

Файл **passwdqc.conf** состоит из 0 или более строк следующего формата:

```
опция=значение
```

Пустые строки и строки, начинающиеся со знака решетка («#»), игнорируются. Символы пробела между опцией и значением не допускаются.

Опции, которые могут быть переданы в модуль (в скобках указаны значения по умолчанию):
min=N0,N1,N2,N3,N4 (min=disabled,24,11,8,7) — минимально допустимая длина пароля.

Используемые типы паролей по классам символов (алфавит, число, спецсимвол, верхний и нижний регистр) определяются следующим образом:

- тип N0 используется для паролей, состоящих из символов только одного класса;
- тип N1 используется для паролей, состоящих из символов двух классов;
- тип N2 используется для парольных фраз, кроме этого требования длины, парольная фраза должна также состоять из достаточного количества слов;
- типы N3 и N4 используются для паролей, состоящих из символов трех и четырех классов, соответственно.

Ключевое слово disabled используется для запрета паролей выбранного типа N0 — N4 независимо от их длины.

Примечание

Каждое следующее число в настройке «min» должно быть не больше, чем предыдущее.

При расчете количества классов символов, заглавные буквы, используемые в качестве первого символа и цифр, используемых в качестве последнего символа пароля, не учитываются.

`max=N` (max=40) — максимально допустимая длина пароля. Эта опция может быть использована для того, чтобы запретить пользователям устанавливать пароли, которые могут быть слишком длинными для некоторых системных служб. Значение 8 обрабатывается особым образом: пароли длиннее 8 символов, не отклоняются, а обрезаются до 8 символов для проверки надежности (пользователь при этом предупреждается).

`passphrase=N` (passphrase=3) — число слов, необходимых для ключевой фразы (значение 0 отключает поддержку парольных фраз).

`match=N` (match=4) — длина общей подстроки, необходимой для вывода, что пароль хотя бы частично основан на информации, найденной в символьной строке (значение 0 отключает поиск подстроки). Если найдена слабая подстрока пароль не будет отклонен; вместо этого он будет подвергаться обычным требованиям к прочности при удалении слабой подстроки. Поиск подстроки нечувствителен к регистру и может обнаружить и удалить общую подстроку, написанную в обратном направлении.

`similar=permit|deny` (similar=deny) — параметр **`similar=permit`** разрешает задать новый пароль, если он похож на старый (параметр **`similar=deny`** — запрещает). Пароли считаются похожими, если есть достаточно длинная общая подстрока, и при этом новый пароль с частично удаленной подстрокой будет слабым.

`random=N[,only]` (random=42) — размер случайно сгенерированных парольных фраз в битах (от 26 до 81) или 0, чтобы отключить эту функцию. Любая парольная фраза, которая содержит предложенную случайно сгенерированную строку, будет разрешена вне зависимости от других возможных ограничений. Значение **`only`** используется для запрета выбранных пользователем паролей.

enforce=none|users|everyone (enforce=users) — параметр **enforce=users** задает ограничение задания паролей в passwd на пользователей без полномочий root. Параметр **enforce=everyone** задает ограничение задания паролей в passwd и на пользователей, и на суперпользователя root. При значении **none** модуль PAM будет только предупреждать о слабых паролях.

retry=N (retry=3) — количество запросов нового пароля, если пользователь с первого раза не сможет ввести достаточно надежный пароль и повторить его ввод.

Далее приводится пример задания следующих значений в файле **/etc/passwdqc.conf**:

```
min=8,7,4,4,4
enforce=everyone
```

В указанном примере пользователям, включая суперпользователя root, будет невозможно задать пароли:

- типа N0 (символы одного класса) — длиной меньше восьми символов;
- типа N1 (символы двух классов) — длиной меньше семи символов;
- типа N2 (парольные фразы), типа N3 (символы трех классов) и N4 (символы четырех классов) — длиной меньше четырех символов.

54.6. Управление сроком действия пароля

Для управления сроком действия паролей используется команда **chage**.

Примечание

Должен быть установлен пакет *shadow-change*:

```
# apt-get install shadow-change
```

chage изменяет количество дней между сменой пароля и датой последнего изменения пароля.

Синтаксис команды:

```
chage [опции] логин
```

Основные опции:

- **-d**, **--lastday LAST_DAY** — установить последний день смены пароля в LAST_DAY на день (число дней с 1 января 1970). Дата также может быть указана в формате ГГГГ-ММ-ДД;
- **-E**, **-expiredate EXPIRE_DAYS** — установить дату окончания действия учётной записи в EXPIRE_DAYS (число дней с 1 января 1970) Дата также может быть указана в формате ГГГГ-ММ-ДД. Значение ***-1*** удаляет дату окончания действия учётной записи;

- **-I**, **--inactive INACTIVE** — используется для задания количества дней «неактивности», то есть дней, когда пользователь вообще не входил в систему, после которых его учетная запись будет заблокирована. Пользователь, чья учетная запись заблокирована, должен обратиться к системному администратору, прежде чем снова сможет использовать систему. Значение ***-1*** отключает этот режим;

- **-l**, **--list** — просмотр информации о «возрасте» учётной записи пользователя;

- **-m**, **--mindays MIN_DAYS** — установить минимальное число дней перед сменой пароля. Значение ***0*** в этом поле обозначает, что пользователь может изменять свой пароль, когда угодно;

- **-M**, **--maxdays MAX_DAYS** — установить максимальное число дней перед сменой пароля. Когда сумма MAX_DAYS и LAST_DAY меньше, чем текущий день, у пользователя будет запрошен новый пароль до начала работы в системе. Эта операция может предваряться предупреждением (параметр **-W**). При установке значения ***-1***, проверка действительности пароля не будет выполняться;

- **-W**, **--warndays WARN_DAYS** — установить число дней до истечения срока действия пароля, начиная с которых пользователю будет выдаваться предупреждение о необходимости смены пароля.

Пример настройки времени действия пароля для пользователя test:

```
# chage -M 5 test
```

Получить информацию о «возрасте» учётной записи пользователя test:

```
# chage -l test
Последний раз пароль был изменён                          : дек 27, 2023
Срок действия пароля истекает                                     : янв 01, 2024
Пароль будет деактивирован через                          : янв 11, 2024
Срок действия учётной записи истекает                             : никогда
Минимальное количество дней между сменой пароля                   : -1
Максимальное количество дней между сменой пароля         : 5
Количество дней с предупреждением перед деактивацией пароля      : -1
```

Примечание

Задать время действия пароля для вновь создаваемых пользователей можно, изменив параметр ***PASS_MAX_DAYS*** в файле **/etc/login.defs**.

54.7. Настройка неповторяемости пароля

Для настройки неповторяемости паролей используется модуль pam_pwhistory, который сохраняет последние пароли каждого пользователя и не позволяет пользователю при смене пароля чередовать один и тот же пароль слишком часто.

Предупреждение

В данном случае системный каталог станет доступным для записи пользователям группы pw_users (создайте эту группу и включите туда пользователей).

Предупреждение

База используемых паролей ведется в файле **/etc/security/opasswd**, в который пользователи должны иметь доступ на чтение и запись. При этом они могут читать хэши паролей остальных пользователей. Не рекомендуется использовать на многопользовательских системах.

Создайте файл **/etc/security/opasswd** и дайте права на запись пользователям:

```
# install -Dm0660 -gpw_users /dev/null /etc/security/opasswd
# chgrp pw_users /etc/security
# chmod g+w /etc/security
```

Для настройки этого ограничения необходимо изменить файл **/etc/pam.d/system-auth-local-only** таким образом, чтобы он включал модуль pam_pwhistory после первого появления строки с паролем:

```
password        required        pam_passwdqc.so config=/etc/passwdqc.conf
password        required        pam_pwhistory.so debug use_authtok remember=10
retry=3
```

После добавления этой строки в файле **/etc/security/opasswd** будут храниться последние 10 паролей пользователя (содержит хэши паролей всех учетных записей пользователей) и при попытке использования пароля из этого списка будет выведена ошибка:

```
Password has been already used. Choose another.
```

В случае если необходимо, чтобы проверка выполнялась и для суперпользователя root, в настройки нужно добавить параметр ***enforce_for_root***:

```
password        required        pam_pwhistory.so
use_authtok enforce_for_root remember=10 retry=3
```

54.8. Модификация пользовательских записей

Для модификации пользовательских записей применяется утилита **usermod**:

```
# usermod -G audio,rpm,test1 test1
```

Такая команда изменит список групп, в которые входит пользователь *test1* — теперь это *audio*, *rpm*, *test1*.

```
# usermod -l test2 test1
```

Будет произведена смена имени пользователя с *test1* на *test2*.

Команды **`usermod -L test2`** и **`usermod -U test2`** соответственно временно блокируют возможность входа в систему пользователю *test2* и возвращают всё на свои места.

Изменения вступят в силу только при следующем входе пользователя в систему.

При неинтерактивной смене или задании паролей для целой группы пользователей используйте утилиту **`chpasswd`**. На стандартный вход ей следует подавать список, каждая строка которого будет выглядеть как ***`имя:пароль`***.

54.9. Удаление пользователей

Для удаления пользователей используйте **`userdel`**.

Команда **`userdel test2`** удалит пользователя *test2* из системы. Если будет дополнительно задан параметр **`-r`**, то будет уничтожен и домашний каталог пользователя. Нельзя удалить пользователя, если в данный момент он еще работает в системе.

Глава 55. Система инициализации systemd и sysvinit

55.1. Запуск операционной системы

55.1.1. Запуск системы

Алгоритм запуска компьютера приблизительно такой:

1. BIOS компьютера.
2. Загрузчик системы (например, LILO, GRUB или другой). В загрузчике вы можете задать параметры запуска системы или выбрать систему для запуска.
3. Загружается ядро Linux.
4. Запускается на выполнение первый процесс в системе — init.

Ядром запускается самая первая программа в системе **init**. Её задачей является запуск новых процессов и повторный запуск завершившихся. Вы можете посмотреть, где расположился **init** в иерархии процессов вашей системы, введя команду **`pstree`**.

От конфигурации **init** зависит, какая система инициализации будет использована.

55.1.2. Система инициализации

Система инициализации — это набор скриптов, которые будут выполнены при старте системы.

Существуют разные системы инициализации, наиболее популярной системой являются **sysvinit** и ее модификации. **systemd** разрабатывается как замена для **sysVinit**.

В Альт Сервер для Эльбрус используется **systemd**.

55.2. Системы инициализации systemd и sysvinit

55.2.1. sysvinit

System V — классическая схема инициализации, на которой базируются многие дистрибутивы. Привычна и довольно проста для понимания: **init** описывает весь процесс загрузки в своем конфигурационном файле **`/etc/inittab`**, откуда вызываются другие программы и скрипты на определенном этапе запуска.

55.2.2. systemd

systemd является альтернативной системой инициализации Linux, вобравшей в себя достоинства классического **System V init** и более современных **launchd** (OS X), **SMF** (Solaris) и **Upstart** (Ubuntu, Fedora), но при этом лишенной многих их недостатков. Он разрабатывался для обеспечения лучшего выражения зависимостей между службами, что позволяет делать одновременно больше работы при загрузке системы, и уменьшить время загрузки системы.

systemd (system daemon) реализует принципиально новый подход к инициализации и контролю работы системы. Одним из ключевых новшеств этого подхода является высокая степень параллелизации запуска служб при инициализации системы, что в перспективе позволяет добиться гораздо более высокой скорости, чем традиционный подход с последовательным запуском взаимозависимых служб. Другим важным моментом является контроль над точками монтирования (не-жизненно-важные файловые системы можно монтировать только при первом обращении к ним, не тратя на это время при инициализации системы) и устройствами (можно запускать и останавливать определенные службы и при появлении или удалении заданных устройств). Для отслеживания групп процессов используется механизм cgroups, который также может быть использован для ограничения потребляемых ими системных ресурсов.

Удобство **systemd** особенно заметно на компьютерах для домашнего пользования — когда пользователи включают и перезагружают компьютер ежедневно. В отличие от **sysvinit**, подвисание при запуске одного сервиса не приведет к остановке всего процесса загрузки.

55.3. Примеры команд управления службами, журнал в systemd

Обратите внимание, что команды **`service`** и **`chkconfig`** продолжат работать в мире **systemd** практически без изменений. Тем не менее, в этой таблице показано как выполнить те же действия с помощью встроенных утилит **systemctl**.

Таблица 55.1. Команды управления службами

Команды Sysvinit	Команды Systemd	Примечания
service frobozz start	systemctl start frobozz.service	Используется для запуска службы (не перезагружает постоянные)
service frobozz stop	systemctl stop frobozz.service	

Команды Sysvinit	Команды Systemd	Примечания
		Используется для остановки службы (не перезагружает постоянные)
service frobozz restart	systemctl restart frobozz.service	Используется для остановки и последующего запуска службы
service frobozz reload	systemctl reload frobozz.service	Если поддерживается, перезагружает файлы конфигурации без прерывания незаконченных операций
service frobozz condrestart	systemctl condrestart frobozz.service	Перезапускает службу, если она уже работает
service frobozz status	systemctl status frobozz.service	Сообщает, запущена ли уже служба
ls /etc/rc.d/init.d/	systemctl list-unit-files --type=service (preferred) ls /lib/systemd/system/*.service /etc/systemd/system/*.service	Используется для отображения списка служб, которые можно запустить или остановить. Используется для отображения списка всех служб.
chkconfig frobozz on	systemctl enable frobozz.service	Включает службу во время следующей перезагрузки, или любой другой триггер
chkconfig frobozz off	systemctl disable frobozz.service	Выключает службу во время следующей перезагрузки, или любой другой триггер
chkconfig frobozz	systemctl is-enabled frobozz.service	Используется для проверки, сконфигурирована ли служба для запуска в текущем окружении
chkconfig --list	systemctl list-unit-files --type=service(preferred) ls /etc/systemd/system/*.wants/	Выводит таблицу служб. В ней видно, на каких уровнях загрузки они (не)запускаются
chkconfig frobozz --list	ls /etc/systemd/system/*.wants/frobozz.service	Используется, для отображения на каких уровнях служба (не)запускается
chkconfig frobozz --add	systemctl daemon-reload	Используется, когда вы создаете новую службу или модифицируете любую конфигурацию

55.4. Журнал в systemd

В **systemd** включена возможность ведения системного журнала. Для чтения журнала следует использовать команду **`journalctl`**. По умолчанию, больше не требуется запуск службы **syslog**.

Вы можете запускать **`journalctl`** с разными ключами:

- **`journalctl -b`** — покажет сообщения только с текущей загрузки;
- **`journalctl -f`** — покажет только последние сообщения.

Так же вы можете посмотреть сообщения определенного процесса:

- **`journalctl _PID`**=1 — покажет сообщения первого процесса (init).

Для ознакомления с прочими возможностями, читайте руководство по **`journalctl`**. Для этого используйте команду **`man journalctl`**.

Глава 56. Документация

Каждый объект системы Linux обязательно сопровождается документацией, описывающей их назначение и способы использования. От пользователя системы не требуется заучивать все возможные варианты взаимодействия с ней. Достаточно понимать основные принципы её устройства и уметь находить справочную информацию.

Не пренебрегайте чтением документации: она поможет вам избежать многих сложностей, сэкономить массу времени и усилий при установке, настройке и администрировании системы, поможет найти нужное для работы приложение и быстро разобраться в нём.

56.1. Экранная документация

Почти все системы семейства UNIX, включая систему Linux, имеют экранную документацию. Её тексты содержат документацию по системным командам, ресурсам, конфигурационным файлам и т. д., а также могут быть выведены на экран в процессе работы.

56.1.1. man

Для доступа к экранной документации используется команда **`man`** (сокращение от manual). Каждая страница руководства посвящена одному объекту системы. Для того чтобы прочесть страницу руководства по программе, необходимо набрать **`man`** *название_программы*. К примеру, если вы хотите узнать, какие опции есть у команды **`date`**, вы можете ввести команду:

```
$ man date
```

Большинство экранной документации написано для пользователей, имеющих некоторое представление о том, что делает данная команда. Поэтому большинство текстов экранной документации содержит исключительно технические детали команды без особых пояснений. Тем не менее, экранная документация оказывается очень ценной в том случае, если вы помните название команды, но её синтаксис просто выпал у вас из памяти.

Поиск по описаниям **man** осуществляется командой **apropos**. Если вы точно не знаете, как называется необходимая вам программа, то поиск осуществляется по ключевому слову, к примеру, **apropos** *date* или при помощи ввода слова, обозначающего нужное действие, после команды **man -k** (например, **man -k** *copy*). Слово, характеризующее желаемое для вас действие, можно вводить и на русском языке. При наличии русского перевода страниц руководства **man** результаты поиска будут выведены на запрашиваемом языке.

«Страница руководства» занимает, как правило, больше одной страницы экрана. Для того чтобы читать было удобнее, **man** запускает программу постраничного просмотра текстов. Страницы перелистывают пробелом, для выхода из режима чтения описания команд **man** необходимо нажать на клавиатуре **q**. Команда **man man** выдаёт справку по пользованию самой командой **man**.

Документация в подавляющем большинстве случаев пишется на простом английском языке. Необходимость писать на языке, который будет более или менее понятен большинству пользователей, объясняется постоянным развитием Linux. Дело не в том, что страницу руководства нельзя перевести, а в том, что её придётся переводить всякий раз, когда изменится описываемый ею объект! Например, выход новой версии программного продукта сопровождается изменением его возможностей и особенностей работы, а следовательно, и новой версией документации.

Тем не менее, некоторые наиболее актуальные руководства существуют в переводе на русский язык. Свежие версии таких переводов на русский язык собраны в пакете *man-pages-ru*. Установив этот пакет, вы добавите в систему руководства, для которых есть перевод, и **man** по умолчанию будет отображать их на русском языке.

56.1.2. info

Другой источник информации о Linux и составляющих его программах — справочная подсистема *info*. Страница руководства, несмотря на обилие ссылок различного типа, остаётся «линейным» текстом, структурированным только логически. Документ *info* — это настоящий гипертекст, в котором множество небольших страниц объединены в дерево. В каждом разделе документа *info* всегда есть оглавление, из которого можно перейти к нужному подразделу, а затем вернуться обратно (ссылки для перемещения по разделам текста помечены *). Для получения вспомогательной информации о перемещении по тексту используйте клавишу **h**. Полное руководство *info* вызывается командой **info info**. Команда **info**, введённая без параметров, предлагает пользователю список всех документов *info*, установленных в системе.

56.2. Документация по пакетам

Дополнительным источником информации об интересующей вас программе, в основном на английском языке, является каталог **/usr/share/doc** — место хранения разнообразной документации.

Каждый пакет также содержит поставляемую вместе с включённым в него ПО документацию, располагающуюся обычно в каталоге **/usr/share/doc/имя_пакета**. Например, документация к пакету *file-5.44* находится в **/usr/share/doc/file-5.44**. Для получения полного списка файлов документации, относящихся к пакету, воспользуйтесь командой **rpm -qd** *имя_установленного_пакета*.

В документации к каждому пакету вы можете найти такие файлы как **README**, **FAQ**, **TODO**, **ChangeLog** и другие. В файле **README** содержится основная информация о программе — имя и контактные данные авторов, назначение, полезные советы и пр. **FAQ** содержит ответы на часто задаваемые вопросы; этот файл стоит прочитать в первую очередь, если у вас возникли проблемы или вопросы по использованию программы, поскольку большинство проблем и сложностей типичны, вполне вероятно, что в **FAQ** вы тут же найдёте готовое решение. В файле **TODO** записаны планы разработчиков на реализацию той или иной функциональности. В файле **ChangeLog** записана история изменений в программе от версии к версии.

Для поиска внешней информации о программе, например, адреса сайта программы в сети Интернет можно использовать команду **rpm -qi** *имя_установленного_пакета*. В информационном заголовке соответствующего пакета, среди прочей информации, будет выведена искомая ссылка.

56.3. Документация к программам, имеющим графический интерфейс

Каждая программа, имеющая графический интерфейс, как правило, сопровождается справочной информацией, вызываемой из меню программы. Обычно это разделы меню **Справка**.

По обыкновению, это меню предоставляет информацию о программе, её версии, лицензии и авторах. В большинстве случаев, справка содержит встроенное руководство, ссылки на локальные сведения и интернет-страницы документации на официальных сайтах программ (традиционная кнопка **F1**), информацию о сочетании клавиш, а также сообщения о процедурах и отладке в программе.

Часть XI. Техническая поддержка продуктов «Базальт СПО»

Содержание

Глава 57. Покупателям нашей продукции

«Базальт СПО» предоставляет следующие виды технической поддержки:

- Поддержка продукта входит в стоимость лицензии и включает регулярный выпуск обновлений, исправление ошибок, устранение уязвимостей в течение всего срока жизни дистрибутива.

- Поддержка пользователей обеспечивает качественную эксплуатацию продукта. Техническая поддержка эксплуатации продуктов «Базальт СПО» оказывается в объеме SLA. Доступны три уровня SLA («Базовый», «Стандартный» и «Расширенный»).

Право на получение консультационной и технической поддержки вы приобретаете при покупке большинства продуктов торговой марки Альт. Сроки и объём помощи указаны в сертификате технической поддержки.

Условия технической поддержки можно найти на странице сайта «Базальт СПО»: http://www.basealt.ru/support.

Глава 58. Пользователям нашей продукции

Вне зависимости от того, скачали вы или же приобрели наш дистрибутив, задавать вопросы или обсуждать их с сообществом пользователей дистрибутивов «Альт» вы можете на форуме или в списках рассылки.

Помощь сообщества:

- Документация сообщества: https://altlinux.org
- Форум: https://forum.altlinux.org
- Списки рассылки: https://lists.altlinux.org
- Сообщить об ошибке: https://bugs.altlinux.org
- Репозиторий: https://packages.altlinux.org
- Сборочная среда: https://git.altlinux.org
- Telegram-канал сообщества: https://telegram.me/alt_linux

Ресурсы компании «Базальт СПО»:

- Сайт компании: https://www.basealt.ru
- Контакты: https://basealt.ru/contacts
- Новости обновлений безопасности: https://cve.basealt.ru

Форум и списки рассылки читают опытные пользователи, профессиональные системные администраторы и разработчики «Базальт СПО». Сообщество пользователей и специалистов окажет содействие в поиске ответа на ваш вопрос или посоветует выход из сложной ситуации. При обращении к данному виду помощи у вас нет гарантии на полноту и своевременность ответа, но мы стараемся не оставлять без ответа вопросы, задаваемые в списках.