УТВЕРЖДЕН

ЛКНВ.11100-01 90 03-ЛУ

ОПЕРАЦИОННАЯ СИСТЕМА АЛЬТ 8 СП

(ОС Альт 8 СП)

Руководство администратора

ЛКНВ.11100-01 90 03

Листов 1022

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

2024

Литера О

АННОТАЦИЯ

Настоящий документ содержит инструкции по установке и эксплуатации программного изделия (ПИ) «Операционная система Альт 8 СП» ЛКНВ.11100-01, сокращенное наименование – ОС Альт 8 СП, **релиз 10** на процессорах архитектур **64 бит (AMD, Intel)**, **AArch64 (ARMv8)**.

Далее в документе будет использоваться альтернативное наименование ПИ: ОС Альт СП.

Версия: 1.3.

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

Также в документе приведены сведения, которые нужны для выполнения операций администрирования:

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

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение и функции ОС Альт СП

ОС Альт СП представляет собой совокупность интегрированных программ, созданных на основе операционной системы (ОС) Linux.

ОС Альт СП предназначено для группового и корпоративного использования, автоматизации информационных, конструкторских и производственных процессов предприятий (организаций, учреждений) всех возможных типов и направлений.

ОС Альт СП поддерживает клиент-серверную архитектуру и может обслуживать процессы как в пределах одной компьютерной системы, так и процессы на других персональных электронных вычислительных машинах (далее – ПЭВМ) через каналы передачи данных или сетевые соединения.

ОС Альт СП обладает следующими функциональными характеристиками:

- обеспечивает возможность обработки, хранения и передачи информации в защищенной программной среде;
- обеспечивает возможность запуска пользовательского программного обеспечения (далее – ПО) в сертифицированном окружении;
- обеспечивает возможность функционирования в многозадачном режиме (одновременное выполнение множества процессов);
- обеспечивает возможность масштабирования системы: возможна эксплуатация ОС как на одной ПЭВМ, так и в информационных системах различной архитектуры;
- обеспечивает многопользовательский режим эксплуатации;
- обеспечивает поддержку мультипроцессорных систем;
- обеспечивает сетевую обработку данных, в том числе разграничение доступа к сетевым пакетам.

Для поддержки выполнения описанных функций в ОС Альт СП реализованы следующие возможности:

- управление процессами и информационными ресурсами;
- управление системными ресурсами;
- управление памятью;
- управление файлами и внешними устройствами;
- управление доступом к обрабатываемой информации;
- защита хранимых, обрабатываемых и передаваемых информационных ресурсов комплексом средств защиты (далее – КСЗ) ОС;
- администрирование;
- поддержка интерфейса прикладного программирования;
- поддержка пользовательского интерфейса.

1.2. Уровень подготовки администратора

Администратор ОС Альт СП должен иметь базовые знания в областях:

- принципы построения и функционирования современных вычислительных систем, механизмов защиты информации;
- работа с ОС семейства Linux;
- администрирование общесистемного и прикладного ПО;
- настройка средств защиты, используемых в составе ОС Альт СП;
- конфигурирование проводных подключений.

2. СТРУКТУРА ОС АЛЬТ СП

ОС Альт СП состоит из набора компонентов, предназначенных для реализации функциональных задач пользователями (должностными лицами для выполнения определенных должностными инструкциями повседневных действий). ПИ ОС Альт СП поставляется в виде дистрибутива и комплекта эксплуатационной документации.

Структура ОС Альт СП представлена на рис. 1.

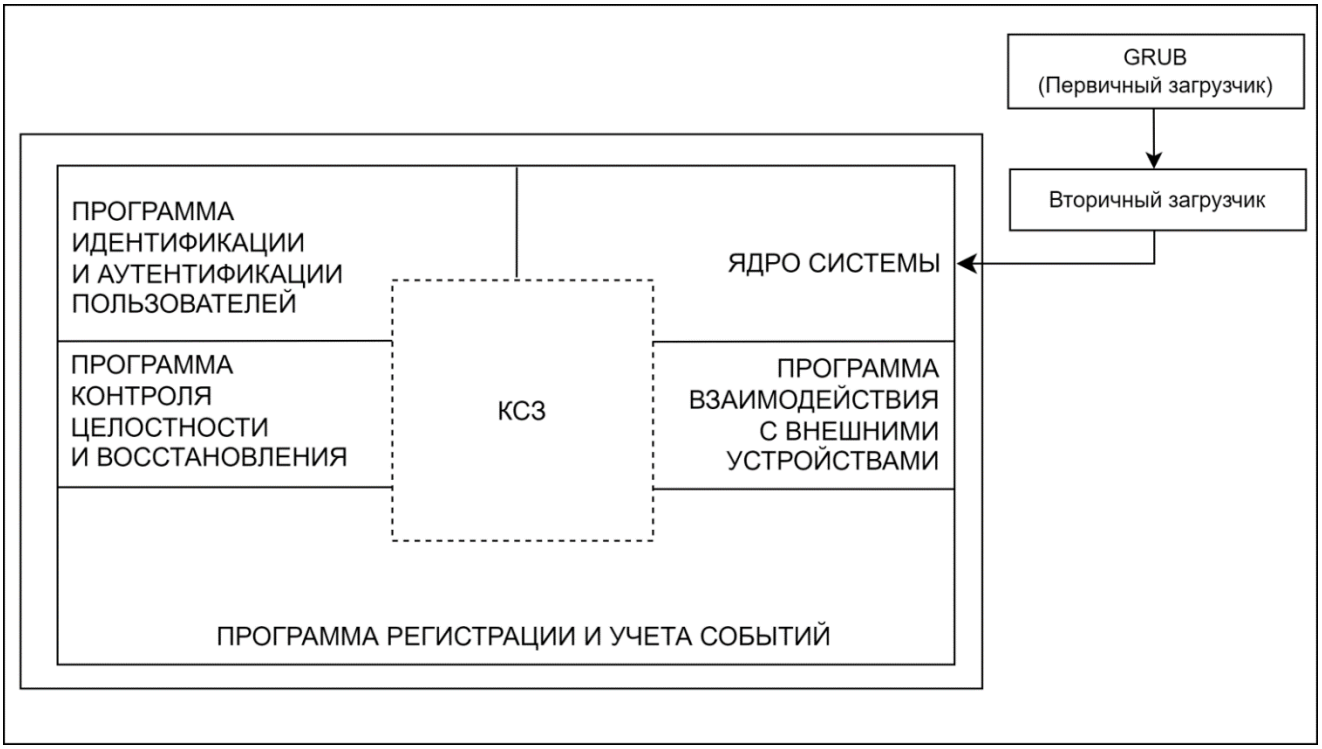


Рис. 1 – Структура ОС Альт СП

В состав ОС Альт СП входят следующие компоненты:

- «Ядро системы»;
- «Программа идентификации и аутентификации пользователей»;
- «Программа контроля целостности и восстановления»;
- «Программа взаимодействия с внешними устройствами»;
- «Программа регистрации и учета событий».

В структуре компонентов ОС Альт СП выделены следующие функциональные элементы:

- ядро ОС;
- КСЗ;
- системные библиотеки;
- серверные программы;
- программы веб-серверов;
- прочие серверные программы;
- интерактивные рабочие среды;
- командные интерпретаторы;
- графическая оболочка MATE;
- системы управления базами данных;
- электронные справочники.

Первичный и вторичный загрузчики ОС обращаются напрямую к ядру ОС, вызывая запуск системных процессов и приложений.

Взаимодействие и обмен информацией в ОС Альт СП контролируются КСЗ, предназначенным для защиты ОС от несанкционированного доступа к обрабатываемой (хранящейся) информации на ПЭВМ.

2.1.1. Ядро ОС Альт СП

Ядро ОС Альт СП управляет доступом к оперативной памяти, сети, дисковым и прочим внешним устройствам. Оно запускает и регистрирует процессы, управляет разделением времени между ними, реализует разграничение прав и определяет политику безопасности, обойти которую, не обращаясь к нему, нельзя.

Ядро работает в режиме «супервизора», позволяющем ему иметь доступ сразу ко всей оперативной памяти и аппаратной таблице задач. Процессы запускаются в «режиме пользователя»: каждый жестко привязан ядром к одной записи таблицы задач, в которой, в числе прочих данных, указано, к какой именно части оперативной памяти этот процесс имеет доступ. Ядро постоянно находится в памяти, выполняя системные вызовы – запросы от процессов на выполнение этих подпрограмм.

2.1.2. КСЗ

КСЗ представляет собой набор специальных программных пакетов, в том числе из состава ядра ОС Альт СП, предназначенных для реализации механизмов безопасности и контроля функционирования ОС Альт СП в целом. Состав и версии пакетов КСЗ уточняйте в зависимости от архитектуры процессора.

* – группа пакетов.

КСЗ включает в себя следующие программные пакеты:

- acl – утилиты, предназначенные для администрирования списков контроля доступа Access Control Lists, которые используются для более точного задания прав доступа к файлам и директориям;
- alterator* – группа пакетов различных модулей системных настроек интерфейса Центра управления системой (ЦУС), предназначены для выполнения наиболее востребованных административных задач;
- apt – средства управления пакетами APT, установка, обновление, разрешение зависимостей RPM пакетов;
- audit – утилиты для хранения и поиска записей аудита, генерируемых подсистемой аудита;
- bacula* – группа пакетов клиент-серверной системы создания и управления резервными копиями данных, а также их резервного восстановления;
- bash – командная оболочка Bourne-Again Shell;
- control – содержит общие интерфейсы управления системным оборудованием, предоставляемые другими пакетами;
- control++ – утилита конфигурирования системы, которая позволяет администратору изменять ограничения системы, устанавливать права доступа;
- coreutils – набор утилит для управления файлами и изменения текстовых файлов;
- corosync – реализует систему взаимодействия для отказоустойчивых кластеров (Сервер 64 бит (AMD, Intel), AArch64 (ARMv8));

- dm-secdel – утилита уничтожения информации, реализует безопасное удаление;
- grub* – модули загрузчика ОС;
- ima-evm* – подсистема контроля целостности GNU/Linux, использует технологии IMA и EVM;
- iptables – используется для настройки, обслуживания и проверки находящихся в ядре Linux таблиц правил фильтрации пакетов IP;
- kernel-image* – ядро ОС Linux, используется для загрузки и запуска системы;
- kernel-modules* – пакеты аппаратных драйверов и библиотек в ядре ОС;
- kubernetes – система с открытым исходным кодом для управления контейнерными приложениями на нескольких хостах; предоставляет базовые механизмы для развертывания, обслуживания и масштабирования приложений;
- libvirt* – набор инструментов для управления виртуализацией;
- lightdm* – менеджер дисплеев, предоставляет графический интерфейс;
- mate-screensaver– хранитель и блокировщик экрана;
- mount – утилита для монтирования файловых систем;
- nagios – система мониторинга служб и сетевой активности;
- nagios-nrpe – сервер выполнения команд системы мониторинга nagios;
- nagstamon – монитор состояний программы nagios;
- nagwad – сервис, генерирующий уведомления от nagios, основанные на записях из журнала аудита;
- openntpd – демон NTP синхронизации времени в локальных системных часах с внешними серверами NTP, а также сам выступает сервером NTP, сообщая свое локальное время по сети другим компьютерам;
- openvpn – VPN с использованием SSL, реализует подключение для удаленных пользователей, телекоммуникации для дома и офиса, безопасные подключения для беспроводных сетей;

- osec – программный комплекс проверки целостности, предназначенный для обнаружения различий между двумя состояниями системы, а также для поиска потенциально опасных файлов;
- pacemaker – менеджер управления ресурсами масштабируемого и высоко доступного кластера (Сервер 64 бит (AMD, Intel), AArch64 (ARMv8));
- libpam0, pam*, pam0* – инструменты системы безопасности, позволяющие администраторам устанавливать политику аутентификации без нужности повторной компиляции программ проверки подлинности;
- passwd – утилита для установки/смены паролей с использованием PAM;
- passwdqc – набор инструментов для контроля сложности паролей и парольных фраз, включающий PAM-модуль, программы и библиотеку;
- podman – модули управления контейнерами, образы контейнеров;
- polkit – это набор инструментов для определения и обработки разрешений. Он используется для того, чтобы позволить непривилегированным процессам контактировать с привилегированными процессами;
- qemu – быстрый эмулятор процессора, использующий динамическую трансляцию для достижения хорошей скорости эмуляции;
- rpm – менеджер пакетов, используемый для сборки, установки, инспекции, проверки, обновления и удаления отдельных программных пакетов;
- rsync – утилита синхронизации файлов по сети, используется в качестве эффективного процесса зеркалирования, т. к. пересылает только различия между файлами, а не файлы целиком;
- secure_delete – набор утилит для безопасного удаления файлов, безопасной очистки от остатков данных неиспользуемого пространства дисков, безопасной очистки разделов подкачки и безопасной очистки неиспользуемой памяти;
- setup – начальный набор конфигурационных файлов;
- sh – командная оболочка Bourne shell;
- shadow – усиливает безопасность системных паролей;

- su – утилита запуска командного интерпретатора от имени другого пользователя;
- sudo – программа, позволяющая делегировать те или иные привилегированные ресурсы пользователям с ведением протокола работы;
- systemd*– менеджер системы и служб в ОС, реализует запуск демонов и отслеживает процессы;
- util-linux – коллекция основных системных утилит;
- vim-console – экранный редактор;
- vlock – программа блокировки сеансов в консоли.

2.1.3. Системные библиотеки

Системные библиотеки – наборы программ (пакетов программ), выполняющие различные функциональные задачи и предназначенные для динамического подключения к работающим программам, которым требуется выполнение этих задач.

2.1.4. Серверные программы и приложения

Серверные программы и приложения предоставляют пользователю специализированные услуги (почтовые службы, хранилище файлов, веб-сервер, система управления базой данных, обеспечение документооборота, хранилище данных пользователей и так далее) в локальной или глобальной сети и обеспечивают их выполнение.

В состав ОС Альт СП включены следующие серверные программы и приложения:

- приложения, обеспечивающие поддержку сетевого протокола DHCP (Dynamic Host Configuration Protocol);
- приложения, обеспечивающие поддержку протокола аутентификации LDAP (Lightweight Directory Access Protocol);
- приложения, обеспечивающие поддержку протоколов FTP, SFTP, SSHD;
- системы управления базами данных;

- программы, обеспечивающие работу SMB-сервера (сервер файлового обмена);
- программы почтового сервера postfix;
- программы прокси-сервера Squid;
- программы веб-сервера apache2;
- программы DNS-сервера.

2.1.5. Прочие системные приложения

Прочие системные приложения – приложения (программы), оказывающие пользователю дополнительные системные услуги при работе с ОС.

В состав ОС Альт СП включены следующие дополнительные системные приложения:

- архиваторы;
- для управления RPM-пакетами;
- резервного копирования;
- мониторинга системы;
- для работы с файлами;
- для настройки системы;
- для настройки параметров загрузки;
- для настройки оборудования;
- для настройки сети.

2.1.6. Программы веб-серверов

Программы веб-серверов участвуют в организации доступа пользователей к сети Интернет. Доступ организуется с помощью клиент-серверной архитектуры.

Клиент, которым обычно является веб-браузер, передает программе веб-сервера запросы на получение ресурсов. В качестве ресурсов могут выступать HTML-страницы, изображения, файлы, медиа-потоки или другие данные, которые требуются клиенту. В ответ веб-сервер передает клиенту запрошенные данные. Обмен происходит по протоколу HTTP.

В состав ОС Альт СП включены программы веб-сервера Apache.

2.1.7. Интерактивные рабочие среды

Интерактивные рабочие среды – программы (пакеты программ), предназначенные для работы пользователя в ОС Альт СП и предоставляющие ему удобный интерфейс для общения с ней.

2.1.8. Командные интерпретаторы

Командные интерпретаторы – специальные программы (терминалы), предназначенные для выполнения различных команд пользователей при работе с ОС Альт СП.

2.1.9. Графическая оболочка MATE

Графическая оболочка MATE – набор программ и технологий, предназначенных для управления ОС Альт СП и предоставляющих пользователю графический интерфейс для работы.

2.1.10. Системы управления базами данных

Системы управления базами данных (далее – СУБД) – приложения, предназначенные для работы с данными, представленными в виде набора записей. СУБД осуществляет поиск, обработку и хранение данных в виде специальных таблиц, являющихся базой данных.

2.1.11. Электронные справочники

Электронные справочники – наборы внутрисистемных справочных страниц, описывающих работу команд и приложений, которые выполнены в виде примеров HOWTOs и справки man.

3. ПОДГОТОВИТЕЛЬНЫЕ ПРОЦЕДУРЫ

3.1. Настройка безопасной конфигурации компьютера

3.1.1. Процедура верификации

Проверка поставленного потребителю дистрибутива производится путем подсчета контрольной суммы с использованием программы фиксации и контроля исходного состояния программного комплекса «ФИКС» (версия 2.0.2)/программы фиксации и контроля целостности информации «ФИКС-UNIX 1.0» по алгоритму «Уровень-3» (при наличии)[1] и сравнения ее с контрольной суммой, указанной в документе «Формуляр. ЛКНВ.11100-01 30 01» и на этикетке ПИ для соответствующей архитектуры.

Администратор имеет возможность верифицировать версию ОС Альт СП, выполнив команду:

```
# cat /root/.install-log/diskinfo
```

3.1.2. Настройка среды функционирования

Для среды функционирования ОС Альт СП (средств вычислительной техники (СВТ)) сформулированы следующие рекомендации:

- обновление установленной системы до ОС Альт СП релиз 10 не допускается. Установка должна производится с удалением всех предыдущих данных со всех разделов диска;
- не допускается использовать аппаратные платформы, включающие в себя базовые системы ввода-вывода (BIOS) или унифицированные расширяемые интерфейсы встроенного ПО (UEFI), содержащие уязвимости, без применения обновлений с закрытием уязвимостей, предоставленных разработчиком данной аппаратной платформы для BIOS или UEFI;
- отключать в BIOS-е Intel SGX;

---

[1] Или с использованием аналогичного ПО, осуществляющего подсчет контрольных сумм по алгоритму ФИКС режим «Уровень-3».

- на серверах отключать системы контроля и управления типа ILO, RSA, iDRAC, ThinkServer EasyManage, AMT, iMana;
- для Intel платформ нужно устранить уязвимости Intel-SA-00086 в Intel Management Engine;
- установка, конфигурирование и управление ОС Альт СП должны выполняться в соответствии с эксплуатационной документацией;
- должна быть обеспечена защита от осуществления действий, направленных на нарушение физической целостности СВТ, на котором функционирует ОС Альт СП;
- должна быть обеспечена доверенная загрузка ОС (блокирование попыток несанкционированной загрузки, контроль доступа субъектов доступа к процессу загрузки, контроль целостности компонентов загружаемой операционной среды);
- должны быть обеспечены ресурсы для выполнения функциональных возможностей безопасности ОС, хранения резервных копий, создаваемых ОС, а также защищенное хранение данных ОС и защищаемой информации;
- должно быть обеспечено ограничение на установку ПО и его компонентов, не задействованных в технологическом процессе обработки информации;
- должен обеспечиваться доверенный маршрут между ОС и пользователями ОС (администраторами, пользователями);
- должен обеспечиваться доверенный канал передачи данных между ОС и средствами вычислительной техники, на которых происходит обработка информации, а также с которых происходит их администрирование;
- должна быть обеспечена невозможность отключения (обхода) компонентов ОС;
- должны быть реализованы меры, препятствующие несанкционированному копированию информации, содержащейся в ОС, на съемные машинные носители информации (или за пределы ИС). В том числе должен осуществляться контроль вноса (выноса) в (из) контролируемую зону (контролируемой зоны) съемных машинных носителей информации;

- должна осуществляться проверка целостности внешних модулей уровня ядра, получаемых от заявителя (разработчика, производителя), перед их установкой в ОС;
- должно быть обеспечено выделение вычислительных ресурсов для процессов в соответствии с их приоритетами;
- персонал, ответственный за функционирование ОС Альт СП, должен обеспечивать функционирование ОС Альт СП, в точности руководствуясь эксплуатационной документацией;
- лица, ответственные за эксплуатацию ОС Альт СП, должны обеспечить, чтобы аутентификационная информация для каждой учетной записи пользователя ОС содержалась в тайне и была недоступна лицам, не уполномоченным использовать данную учетную запись;
- должна обеспечиваться возможность генерации аутентификационной информации соответствующей метрике качества.

3.2. Настройка опций безопасности

Во время установки ОС Альт СП в соответствии с принятыми парольными ограничениями на объекте эксплуатации:

- задать пользователя с паролем, отвечающим требованиям безопасности;
- задать пароль администратора, отвечающий требованиям безопасности;
- установить пароль на загрузчик (при наличии).

Перед началом эксплуатации ОС Альт СП рекомендуется администратору обеспечить выполнение следующих условий:

1) настроить параметры входа пользователя (порядок действий приведен в документе «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03» – далее Руководство по КСЗ):
    - время засыпания (блокирование сеанса доступа см. в п. 6.4);

2) настроить параметры пароля пользователя (порядок действий приведен в Руководстве по КСЗ подразделы «Настройка парольных ограничений», «Управление сроком действия пароля»):
   - сложность пароля;
   - время действия;
3) настроить средства контроля целостности (порядок действий приведен в Руководстве по КСЗ в подразделе «Программный комплекс проверки целостности системы Osec»);
4) настроить параметры запрета удаления файлов (порядок действий приведен п. 18.2 «Модуль AltHa»);
5) настроить сервисы в соответствии с функциональным назначением объекта автоматизации (управление сервисами см. в п. 16.1.1);
6) настроить аудит:
   - создать правила аудита (примеры использования аудита приведены в Руководстве по КСЗ подраздел «Использование аудита»);
7) настроить экспорт аудита на другой компьютер (порядок действий приведен п. 7.6);
8) настроить подключение оповещений администратора (порядок действий приведен п. 7.7);
9) механизм замкнутой программной среды должен быть настроен для работы в штатном режиме пользователя (порядок действий приведен в Руководстве по КСЗ в подразделе «Подсистема IMA/EVM»);
10) с использованием средств управления дискреционными правами разграничения доступа запретить пользователям, не обладающим привилегиями администратора:
    - доступ к библиотеке libpcprofile.so;
    - запуск (использование) средств создания символических ссылок;
11) с использованием средств управления запуском сервисов должна быть отключена служба gpm для поддержки «мыши» в консольном режиме;

12) для защиты от атаки подбора пароля (brute force):
    - внести изменения в файл `/etc/pam.d/sshd` – добавить строку:
    - `auth  required pam_faillock.so authfail deny=3 unlock_time=19`
13) для суперпользователя (root) заблокировать возможность его удаленного входа в ОС посредством включения PAM-модуля `pam_securetty` в файл сценария `/etc/pam.d/common-auth`. Для этого в «Primary block» в указанном файле первой строкой добавить:

    `auth required pam_securetty.so`

3.3. Описание механизмов устранения идентифицированных скрытых каналов

Далее приведены дополнительные рекомендации по настройке механизмов защиты ОС Альт СП для устранения возможных скрытых каналов передачи информации.

Механизмы защиты направлены на ограничение, мониторинг, полное или частичное устранение идентифицированных скрытых каналов, которые могут возникнуть в информационных (автоматизированных) системах вследствие использования в них ОС Альт СП.

1) Исключение возможности работы с общими каталогами с правом записи для пользователей, имеющих разные полномочия доступа.

2) Для противодействия атакам на каналы передачи по времени и памяти администратором безопасности нужно исключить наличие в системе общих для пользователей файловых ресурсов, где размещаются файлы с разными правами дискреционного разграничения доступа, в частности исключить размещение в каталогах файлов, доступ к которым полностью закрыт для конкретных пользователей данного каталога. Также можно монтировать файловую систему без учета времени доступа:

`mount -noatime –nodiratime`

3) На уровне ядра запретить процессам создавать слушающие сокеты, кроме тех, что им действительно нужны, в том числе запрещать слушать на фиксированном порту, а также контролировать частоту создания сокета.

4) Монтировать подсистему `/proc` с флагом `hidepid=2` или `1`. При этом имена процессов других пользователей и другие данные таких процессов будут недоступны вызывающему непривилегированному пользователю.

5) Организовать маскирующие процессы, имитирующие постоянную загрузку процессора. Использовать механизмы ограничения CPU для процессов, гарантирующий время выполнения, одинаковое для всех процессов, такой как cgroups.

6) Для предотвращения Timestamp Evaluation – отключить отметки времени TCP в ОС Альт СП. Для этого выполнить следующие команды:

```
# echo 0 > /proc/sys/net/ipv4/tcp_timestamps
```

```
To make that change permanent though, you need to add the
following line to /etc/sysctl.conf:
net.ipv4.tcp_timestamps = 0
```

также можно настроить правила iptables:

```
iptables -A INPUT -p icmp --icmp-type timestamp-request -j DROP
iptables -A OUTPUT -p icmp --icmp-type timestamp-reply -j DROP
```

7) Для предотвращения ISN Evaluation (оценка временной отметки) – использовать TCP/IP прокси (socks).

8) Для предотвращения TCP URG Pointer (указателя TCP URG) – настроить правила iptables:

```
iptables -N BADFLAGS
iptables -A BADFLAGS -j LOG --log-prefix "BADFLAGS: "
iptables -A BADFLAGS -j DROP
iptables -N TCP_FLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ACK,FIN FIN                  -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ACK,PSH PSH                  -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ACK,URG URG                  -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags FIN,RST FIN,RST              -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags SYN,FIN SYN,FIN              -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags SYN,RST SYN,RST              -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL     ALL                  -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL     NONE                 -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL     FIN,PSH,URG          -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL     SYN,FIN,PSH,URG      -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL     SYN,RST,ACK,FIN,URG  -j BADFLAGS
```

9) Для предотвращения IP ToS Evaluation (Оценки IP-ToS) – настроить способ обслуживания для telnet, ftp-control и ftp-data – выполнить команды:

```
# iptables -A PREROUTING -t mangle -p tcp --sport telnet \
  -j TOS --set-tos Minimize-Delay
# iptables -A PREROUTING -t mangle -p tcp --sport ftp \
```

```
    -j TOS --set-tos Minimize-Delay
  # iptables -A PREROUTING -t mangle -p tcp --sport ftp-data \
    -j TOS --set-tos Maximize-Throughput
```

Эти правила прописываются на удаленном хосте и воздействуют на входящие по отношению к компьютеру пакеты. Для пакетов, отправляемых в обратном направлении, эти флаги устанавливаются автоматически. Настроить их можно, прописав следующие правила:

```
# iptables -A OUTPUT -t mangle -p tcp --dport telnet \
  -j TOS --set-tos Minimize-Delay
# iptables -A OUTPUT -t mangle -p tcp --dport ftp \
  -j TOS --set-tos Minimize-Delay
# iptables -A OUTPUT -t mangle -p tcp --dport ftp-data \
  -j TOS --set-tos Maximize-Throughput
```

Для противодействия данной атаке нужно в командной строке прописать следующие правила:

```
# Разрешить главные типы протокола ICMP
iptables -A OUTPUT -p icmp --icmp-type 0 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 3 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 4 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 11 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 12 -j ACCEPT
```

Типы ICMP-сообщений:

- 0 – echo reply (echo-ответ, пинг);
- 3 – destination unreachable (адресат недосягаем);
- 4 – source quench (подавление источника, просьба посылать пакеты медленнее);
- 5 – redirect (редирект);
- 8 – echo request (echo-запрос, ping);
- 9 – router advertisement (объявление маршрутизатора);
- 10 – router solicitation (ходатайство маршрутизатора);
- 11 – time-to-live exceeded (истечение срока жизни пакета);
- 12 – IP header bad (неправильный IP заголовок пакета);
- 13 – timestamp request (запрос значения счетчика времени);
- 14 – timestamp reply (ответ на запрос значения счетчика времени);
- 15 – information request (запрос информации);

- 16 – information reply (ответ на запрос информации);

- 17 – address mask request (запрос маски сети);

- 18 – address mask reply (ответ на запрос маски сети).

10) Для предотвращения Initial Sequence Number hijacking and spoofing (урона и подделки исходного кода последовательности) – настроить правила iptables:

```
# Защита от спуфинга
iptables -I INPUT -m conntrack --ctstate NEW,INVALID -p tcp  \
 --tcp-flags SYN,ACK SYN,ACK -j REJECT --reject-with tcp-reset
# Защита от SYN-флуда
iptables -A INPUT -p tcp --syn -m limit --limit 10/s  \
 --limit-burst 50 -j ACCEPT
iptables -A INPUT -p udp -m limit --limit 10/s --limit-burst 50 -j \
   ACCEPT
iptables -A INPUT -p icmp -m limit --limit 10/s --limit-burst 50 \
   -j ACCEPT
iptables -A INPUT -j DROP
# Отбрасывать ошибочные пакеты
iptables -A INPUT -m state --state INVALID -j DROP
iptables -I INPUT -m conntrack --ctstate INVALID -j DROP
# Отбрасывать фрагментированные пакеты
iptables -A INPUT -f -j DROP
# Защита от попытки открыть входящее соединение TCP не через SYN
iptables -I INPUT -m conntrack --ctstate NEW -p tcp ! --syn -j DROP
# Защита от Ping of death
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit
   10/s --limit-burst 50 -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
# Защита от некорректных ICMP
iptables -I INPUT -p icmp -f -j DROP
# Отбросить ошибочные пакеты
iptables -A FORWARD -m state --state INVALID -j DROP
iptables -I FORWARD -m conntrack --ctstate INVALID -j DROP
# Отбросить фрагментированные пакеты
iptables -A FORWARD -f -j DROP
# Сбрасывать фрагментированные пакеты
iptables -A OUTPUT -f -j DROP
```

Дополнительно требуется внести правки в `/etc/sysctl.conf`:

```
# vim /etc/systcl.conf


# Отбросить ICMP-редиректы (против атак типа MITM)
net.ipv4.conf.all.accept_redirects=0
net.ipv6.conf.all.accept_redirects=0
# Включить механизм TCP syncookies
net.ipv4.tcp_syncookies=1
# Различные улучшения (защита от спуфинга
# увеличение очереди «полуоткрытых» TCP-соединений и далее):
net.ipv4.tcp_timestamps=0
net.ipv4.conf.all.rp_filter=1
net.ipv4.tcp_max_syn_backlog=1280
kernel.core_uses_pid=1
```

4. ФУНКЦИИ И ЗАДАЧИ АДМИНИСТРИРОВАНИЯ ОС АЛЬТ СП

4.1. Функции администратора

Основными функциями администратора при эксплуатации ОС Альт СП являются:

- ввод в эксплуатацию и эксплуатация в соответствии с указаниями, приведенными в документе «Формуляр. ЛКНВ.11100-01 30 01»;
- соблюдение подготовительных процедур (см. раздел 3);
- установка и настройка ОС Альт СП;
- управление и поддержка функционирования ПЭВМ.

4.2. Задачи администрирования

В состав основных задач администрирования входят следующие:

- установка ОС Альт СП и назначение параметров системы;
- создание загрузочных носителей информации;
- конфигурирование параметров даты и времени, графической среды, средств ввода и вывода;
- настройка и управление системными сервисами и служебными программами;
- настройка и управление работой системы управления пакетами Advanced Packaging Tool (далее – APT);
- обновление ОС и прикладного ПО из ее состава;
- настройка и управление учетными записями и правами доступа пользователей;
- конфигурирование сети `/etc/net` и проверка ее работоспособности;
- настройка FTP-серверов;
- настройка служб DNS;
- настройка серверов электронной почты postfix;
- настройка и управление кэширующими прокси-серверами;

- настройка серверного и клиентского ПО Samba для осуществления связи UNIX-машин с сетями Microsoft и LanManager;
- настройка и управление печатью;
- настройка и управление базами данных.

5. УСТАНОВКА ОС АЛЬТ СП

Обычно для установки дистрибутива используется установочный загрузочный компакт-диск дистрибутива. Если установка производится с компакт-диска, можете сразу перейти к п. 5.3 и п. 5.4.

Для начала процесса установки ПИ ОС Альт СП нужно выбрать способ первоначальной загрузки компьютера (п. 5.3.1).

В случае загрузки с установочного компакт-диска эти две возможности предоставляются самим диском: он является загрузочным и содержит все требуемые для установки файлы. Однако вполне допустим и такой вариант: первоначальная загрузка происходит со специально подготовленного USB-flash-накопителя, а установочные файлы берутся с FTP-сервера сети.

Установка с загрузочного компакт-диска – это один из возможных способов установки системы. Он является самым распространенным способом установки системы, но не работает, например, в случае отсутствия на компьютере CD/DVD-привода. Для таких случаев поддерживаются альтернативные методы установки (см. п. 5.1).

5.1. Запись установочного образа на USB-flash-накопитель

⚠ Запись образа дистрибутива на USB-flash-накопитель приведет к изменению таблицы разделов на носителе, таким образом, если USB-flash-накопитель выполнил функцию загрузочного\установочного устройства и требуется вернуть ему функцию переносного накопителя данных, то нужно удалить все имеющиеся разделы на USB-flash-накопителе и создать нужное их количество заново.

⚠ Для восстановления совместимости USB-flash-накопителя с ОС семейства Windows может понадобиться также пересоздание таблицы разделов (например, при помощи parted). Нужно удалить таблицу GPT и создать таблицу типа msdos. Кроме того, должен быть только один раздел с FAT или NTFS.

Для создания загрузочного USB-flash-накопителя требуется файл ISO-образа установочного носителя информации с дистрибутивом.

ISO-образы установочных носителей информации являются гибридными (Hybrid ISO/IMG), что позволяет записывать их на USB-flash-накопитель.

В ОС Linux для записи образа на USB-flash-накопитель можно воспользоваться любой программой с графическим интерфейсом, например:

- ALT Media Writer (altmediawriter) – может автоматически загружать образы из интернета и записывать их, извлекая сжатые образы (img.xz);
- SUSE Studio Imagewriter.

Или воспользоваться для записи установочного образа утилитой командной строки dd, выполнив с правами пользователя root следующие команды:

```
# dd oflag=direct if=<файл-образа.iso> of=/dev/sdX bs=1M
# sync
```

где:

- `<файл-образа.iso>` – ISO-образ установочного диска с дистрибутивом;
- `/dev/sdX` – устройство, соответствующее USB-flash-накопителю.

Точное обозначение устройства можно узнать, выполнив команду dmesg, после подключения USB-flash-накопителя к компьютеру. Например:

```
$ dmesg | grep disk
[    1.171036] sd 0:0:0:0: [sda] Attached SCSI disk
[    4.755468] sd 1:0:0:0: [sdb] Attached SCSI disk
[53271.629338] sd 5:0:0:0: [sdc] Attached SCSI removable disk
```

USB-flash-накопитель имеет имя устройства sdc. Далее в примере устройство будет называться `/dev/sdc`.

Также просмотреть список доступных устройств можно командой `lsblk` или (если такой команды нет): `blkid`.

Затем для удобства отображения прогресса записи нужно установить пакет pv и запустить команду:

```
# pv <файл-образа.iso> | dd oflag=direct of=/dev/sdX bs=1M;sync
```

⚠ Будьте внимательны при указании имени USB-устройства – запись образа по ошибке на жесткий диск приведет к потере данных на нем.

⚠ Не добавляйте номер раздела, образ пишется на USB-flash-накопитель с самого начала!

⚠ Пока образ не запишется до конца нельзя извлекать USB-flash-накопитель. Определить финал процесса можно по прекращению моргания индикатора USB-устройства либо посредством виджета «Безопасное извлечение съемных устройств». В консоли можно подать команду:

```
$ eject /dev/sdX
```

В среде ОС Windows для создания загрузочного USB-flash-накопителя рекомендуется использовать специализированные программные средства, например: ALT Media Writer, Win32 Disk Imager и другие.

Созданный, описанным выше способом, USB-flash-накопитель является одновременно и загрузочным, и установочным. В результате, установка дистрибутива может быть произведена исключительно с использованием USB-flash-накопителя.

5.2. Установка через VNC

Для управления сетевой установкой следует подключить машину к сети и обеспечить ей получение адреса по DHCP, затем выбрать пункт в меню установки «Установить через VNC ALT SP Server/Workstation (измените пароль и соединитесь)».

После запуска установки по VNC будет запущен сервер VNC (рис. 2) и машина будет ожидать подключения к нему, стандартный пароль для подключения «VNCPWD».

Далее требуется выполнить подключение к данному VNC-серверу и продолжить установку ОС (рис. 3).

```
init-bottom: Root fs is squashfs
init-bottom: Remounting / with Overlayfs
init-bottom: Root FS overlayed with Overlayfs
Spawning init ... done.
Starting systemd-udevd service:                                    [ DONE ]
Populating /dev:                                                   [ DONE ]
Running initinstall script [00-create-missing-symlinks-in-dev.sh]  [ DONE ]
Running initinstall script [01-apt-cache-limit.sh]                 [ DONE ]
Running initinstall script [01-multipath.sh]                       [ DONE ]
Running initinstall script [05-efi.sh]                             [ DONE ]
Running initinstall script [10-disk.sh]                            [ DONE ]
Running initinstall script [10-network.sh]                         [ DONE ]
Running initinstall script [10-vm-profile.sh]                      [ DONE ]
Running initinstall script [10-vt.sh]                              [ DONE ]
Running initinstall script [15-expert.sh]                          [ DONE ]
Running initinstall script [20-bend-license-ru-step.sh]            [ DONE ]
Running initinstall script [20-nodesign.sh]                        [ DONE ]
Running initinstall script [20-pts.sh]                             [ DONE ]
Running initinstall script [25-setup-dhcp.sh]                      [ DONE ]
Running initinstall script [26-metadata-autoinstall.sh]            [ DONE ]
Running initinstall script [27-metadata-install-scripts.sh]        [ DONE ]
Running initinstall script [30-ntp-client.sh]                      [ DONE ]
Running initinstall script [30-turn-grub-password-on.sh]           [ DONE ]
Running initinstall script [40-xorg.sh]                            [ DONE ]
Running initinstall script [50-removable]                          [ DONE ]
Running initinstall script [80-stop-md-dm.sh]                      [ DONE ]
Running initinstall script [85-start-multipath.sh]                 [ DONE ]
Running initinstall script [90-alteratord.sh]                      [ DONE ]
Running initinstall script [90-date.sh]                            [ DONE ]
Running initinstall script [90-pkg.sh]                             [ DONE ]
Running initinstall script [90-remove-unused-officer-steps]        [ DONE ]
Running initinstall script [95-add-remount-step.sh]                [ DONE ]
stored passwd in file: /tmp/vncpasswd
Waiting for network...
** IP(s): 10.140.85.32
** VNC cmdline: vncpassword=VNCPWD

The VNC desktop is:      localhost.localdomain:0
PORT=5900
```

Рис. 2 – Запуск сервера VNC

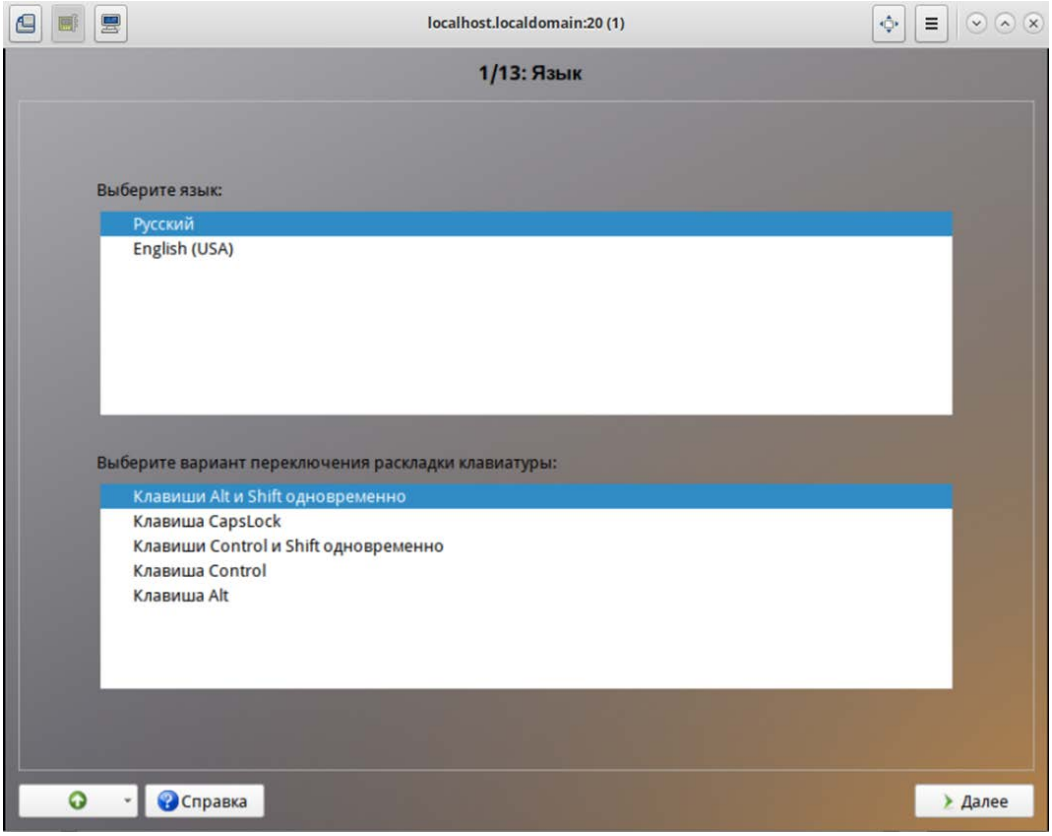


Рис. 3 – Успешное подключение к VNC серверу для дальнейшей установки ОС

5.3. Начало установки: загрузка системы

5.3.1. Способы первоначальной загрузки

Для загрузки компьютера с целью установки системы нужно воспользоваться носителем, содержащим начальный загрузчик. Таким носителем может быть, как сам загрузочный компакт-диск дистрибутива, так и, например, USB-flash-накопитель, который можно сделать загрузочным (см. п. 5.1).

5.3.2. Загрузка системы

Для того чтобы начать обычную установку (при наличии установочного компакт-диска с дистрибутивом и устройства для чтения DVD), нужно загрузиться с компакт-диска, на котором записан дистрибутив.

Примечания:

1.Перед установкой системы нужно выставить точное время в базовой системе ввода-вывода (БСВВ).

2.Может потребоваться включить в БСВВ опцию загрузки с CD/DVD-привода. Способ входа в меню БСВВ и информация о расположении настроек определяется производителем используемого оборудования. За информацией можно обратиться к документации на оборудование.

После загрузки компьютера с установочного компакт-диска или специально подготовленного USB-flash-накопителя (см. п. 5.1) выводится меню, в котором возможно перечисление нескольких вариантов загрузки, зависит от особенностей архитектуры процессора, причем установка системы – это только одна из возможностей (рис. 4):

- «Установить ALT SP Workstation» – установка ОС;
- «Установить через VNC ALT SP Workstation» – установка ОС через VNC;
- «Спасательный LiveCD» – восстановление уже установленной, но так или иначе поврежденной ОС Linux путем запуска небольшого образа ОС в оперативной памяти. Восстановление системы потребует некоторой квалификации. Этот пункт также может быть использован для сбора информации об оборудовании компьютера, которую можно отправить разработчикам, если ОС Альт СП устанавливается и работает неправильно.

Загрузка восстановительного режима заканчивается приглашением командной строки: `[root@localhost /]#`;

- «Изменить язык (нажмите F2)»;

- «UEFI Firmware Settings» – позволяет получить доступ к настройкам UEFI.

Примечание. На данном этапе установки не поддерживается «мышь», поэтому для выбора различных вариантов и опций установки следует воспользоваться клавиатурой.

Примечание. Начальный загрузчик в режиме Legacy показан на рис. 5. Пункт «Загрузка с жесткого диска» позволяет запустить уже установленную на жестком диске операционную систему.

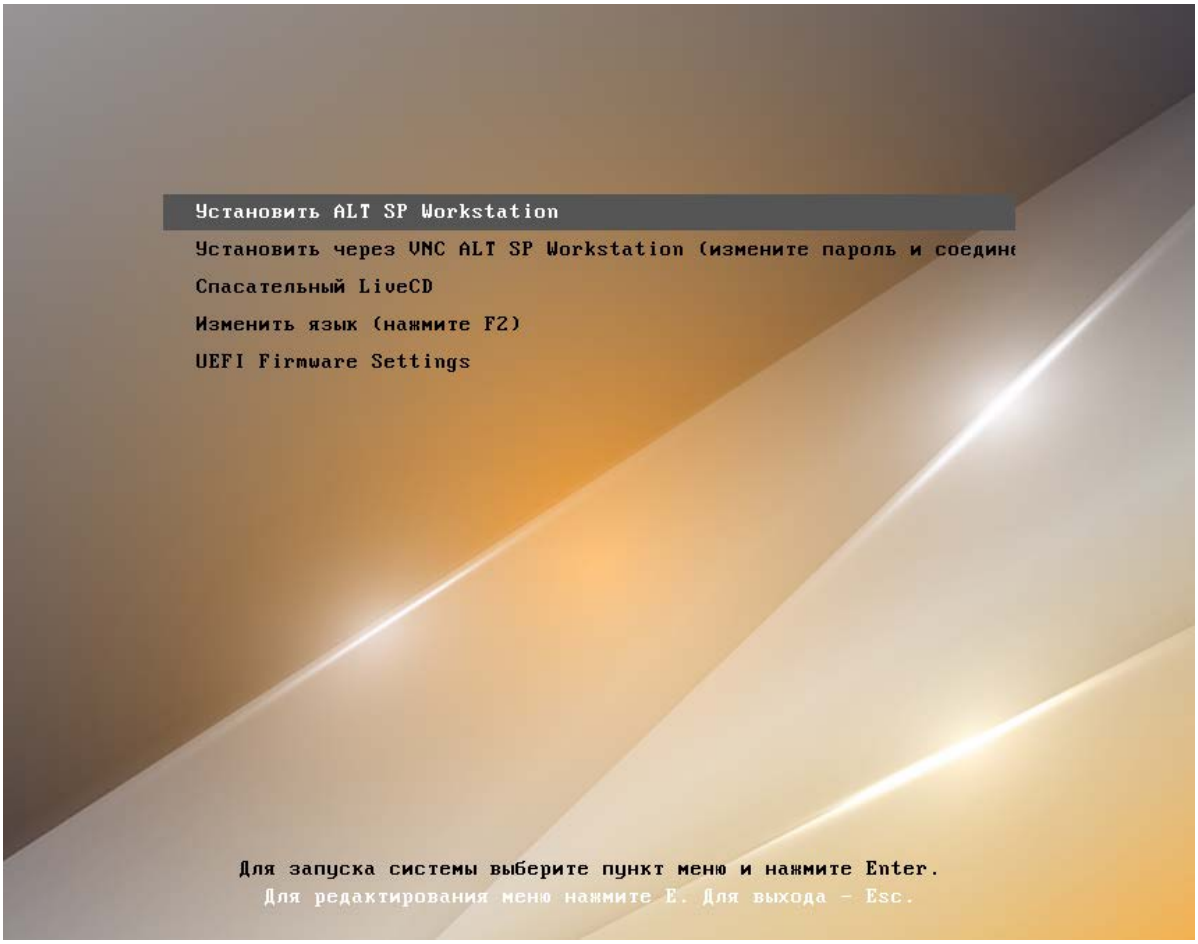


Рис. 4 – Пример загрузки с установочного диска

В строке «Параметры загрузки», меню начального загрузчика, можно вручную задать параметры, передаваемые ядру, например:

- `nomodeset` – не использовать modeset-драйверы для видеокарты;

- `vga=normal` – отключить графический экран загрузки установщика;

- `xdriver=vesa` – явно использовать видеодрайвер vesa. Данным параметром можно явно указать нужный вариант драйвера;
- `acpi=off noapic` – отключение ACPI (управление питанием), если система не поддерживает ACPI полностью.

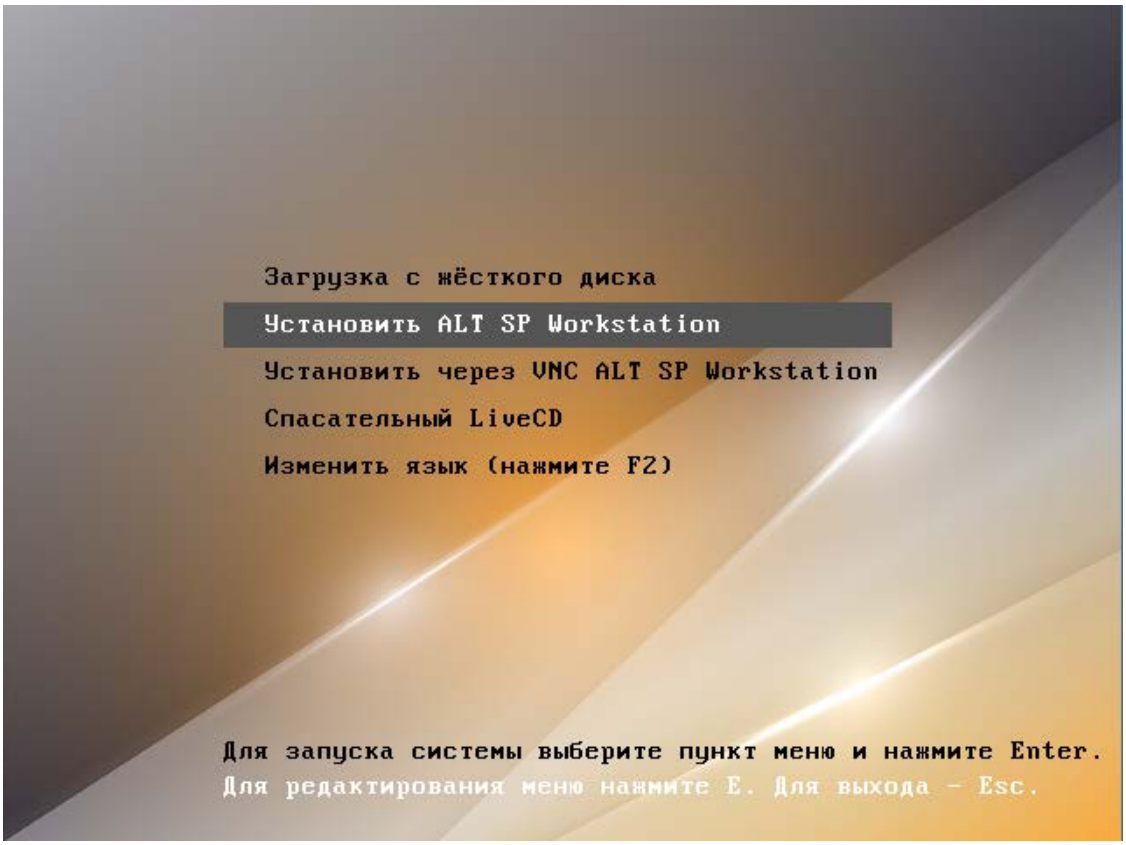


Рис. 5 – Пример загрузки с установочного диска в режиме Legacy

Нажатие клавиши <F2> вызывает переход к окну выбора языка. От выбора языка в загрузчике зависит язык интерфейса загрузчика и программы установки.

Нажатием клавиши <E> можно вызвать редактор параметров текущего пункта загрузки. В открывшемся редакторе (рис. 6) следует найти строку, начинающуюся с `linux /boot/vmlinuz`, в ее конец дописать требуемые параметры, отделив пробелом и нажать <F10>.

Сочетание клавиш <Ctrl>+<Alt>+<F1> – выдает технические сведения о выполнении процесса установки ОС Альт СП.

Чтобы начать процесс установки, нужно клавишами перемещения курсора вверх <↑>, вниз <↓> выбрать пункт меню «Установить ALT SP Workstation» и нажать клавишу <Enter>.

Начальный этап установки не требует вмешательства пользователя: происходит автоматическое определение оборудования и запуск компонентов программы установки. Сообщения о том, что происходит на этом этапе, можно просмотреть, нажав клавишу <ESC>.

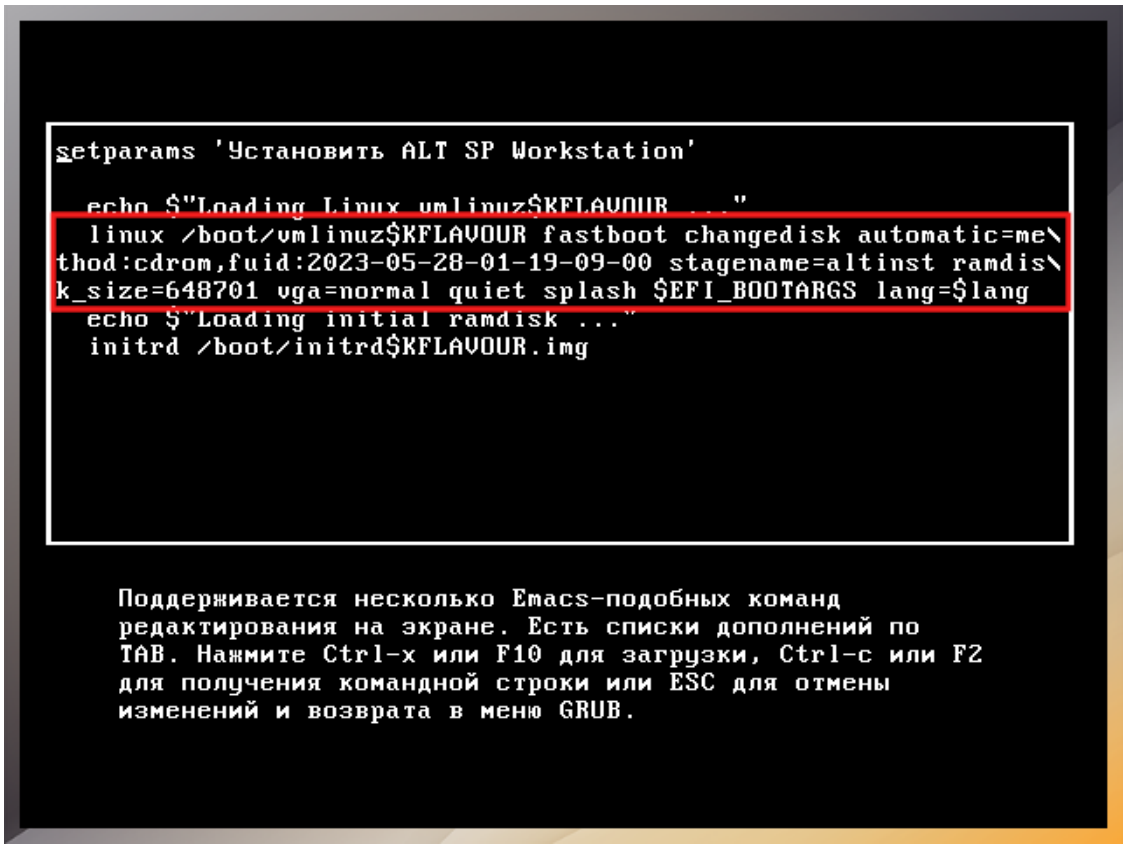


Рис. 6 – Редактор параметров пункта загрузки

Примечание. В начальном загрузчике установлено небольшое время ожидания: если в этот момент не предпринимать никаких действий, то будет загружена та система, которая уже установлена на жестком диске. Если пропустили нужный момент, перезагрузите компьютер и вовремя выберите пункт «Установка».

5.4. Последовательность установки

До того, как будет произведена установка базовой системы на жесткий 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 разделен на шаги; каждый шаг посвящен настройке или установке определенного свойства системы. Шаги нужно проходить последовательно, переход к следующему шагу происходит по нажатию кнопки «Далее». При помощи кнопки «Назад» можно вернуться к уже пройденному шагу и изменить настройки. Однако на этом этапе установки возможность перехода к предыдущему шагу ограничена теми шагами, где нет зависимости от данных, введенных ранее.

В случае отмены установки, нужно нажать на кнопку <Reset> на корпусе системного блока компьютера.

П р и м е ч а н и е . Совершенно безопасно выполнить отмену установки только до шага «Подготовка диска» (см. п. 5.4.4), поскольку до этого момента не производится никаких изменений на жестком диске. Если прервать установку между шагами «Подготовка диска» и «Установка загрузчика» (см. п. 5.4.8), существует вероятность, что после этого с жесткого диска ОС не сможет загрузиться.

Технические сведения о ходе установки можно посмотреть, нажав клавиши <Ctrl>+<Alt>+<F1>, вернуться к программе установки – <Ctrl>+<Alt>+<F7>. По нажатию клавиш <Ctrl>+<Alt>+<F2> откроется отладочная виртуальная консоль.

Каждый шаг сопровождается краткой справкой, которую можно вызвать, нажав <F1>.

Во время установки системы выполняются следующие шаги:

- язык (см. п. 5.4.1);
- подтверждение согласия (см. п. 5.4.2);
- дата и время (см. п. 5.4.3);
- подготовка диска (см. п. 5.4.4);
- перемонтирование (см. п. 5.4.5);
- установка системы (см. п. 5.4.6);
- сохранение настроек (см. 5.4.7);
- установка загрузчика (см. п. 5.4.8);
- настройка сети (см. п. 5.4.9);
- администратор системы (см. п. 5.4.10);
- системный пользователь (см. п. 5.4.11);

- в случае создания LUKS разделов – этап установки пароля на LUKS разделы (см. п. 5.4.12);
- завершение установки (см. п. 5.4.13).

П р и м е ч а н и е . Некоторые шаги при установке могут отсутствовать в связи с особенностями архитектуры процессора.

5.4.1. Язык

Установка начинается с выбора основного языка – языка интерфейса программы установки и устанавливаемой системы (рис. 7).

Также на данном этапе выбирается вариант переключения раскладки клавиатуры. Раскладка клавиатуры – это привязка букв, цифр и специальных символов к клавишам на клавиатуре. Переключение между раскладками осуществляется при помощи специально зарезервированных для этого клавиш.

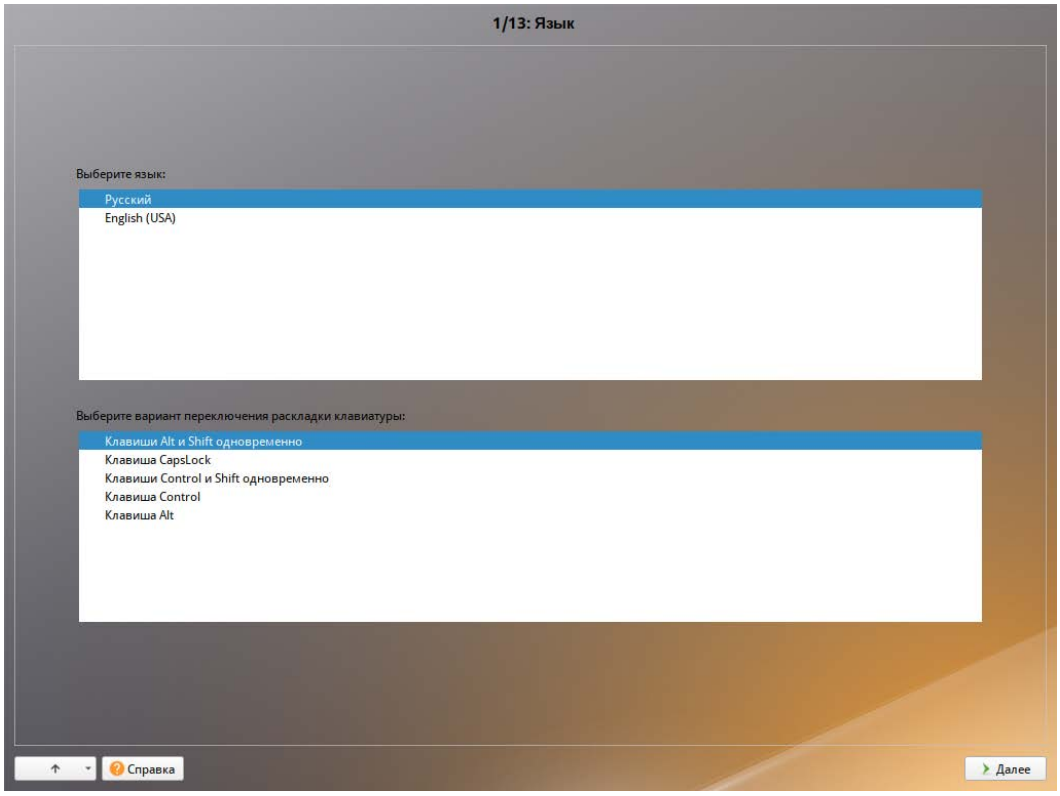


Рис. 7 – Установка. Выбор языка

Для настройки варианта переключения раскладки клавиатуры в пункте «Выберите вариант переключения раскладки клавиатуры:» нужно установить одно из следующих значений (доступно при выборе русского языка, в качестве основного):

- 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.

После завершения настройки основного языка и варианта переключения раскладки клавиатуры нужно нажать на кнопку «Далее».

5.4.2. Подтверждение согласия

После окна выбора языковых параметров ОС Альт СП программа установки переходит к окну «Подтверждение согласия» (рис. 8).

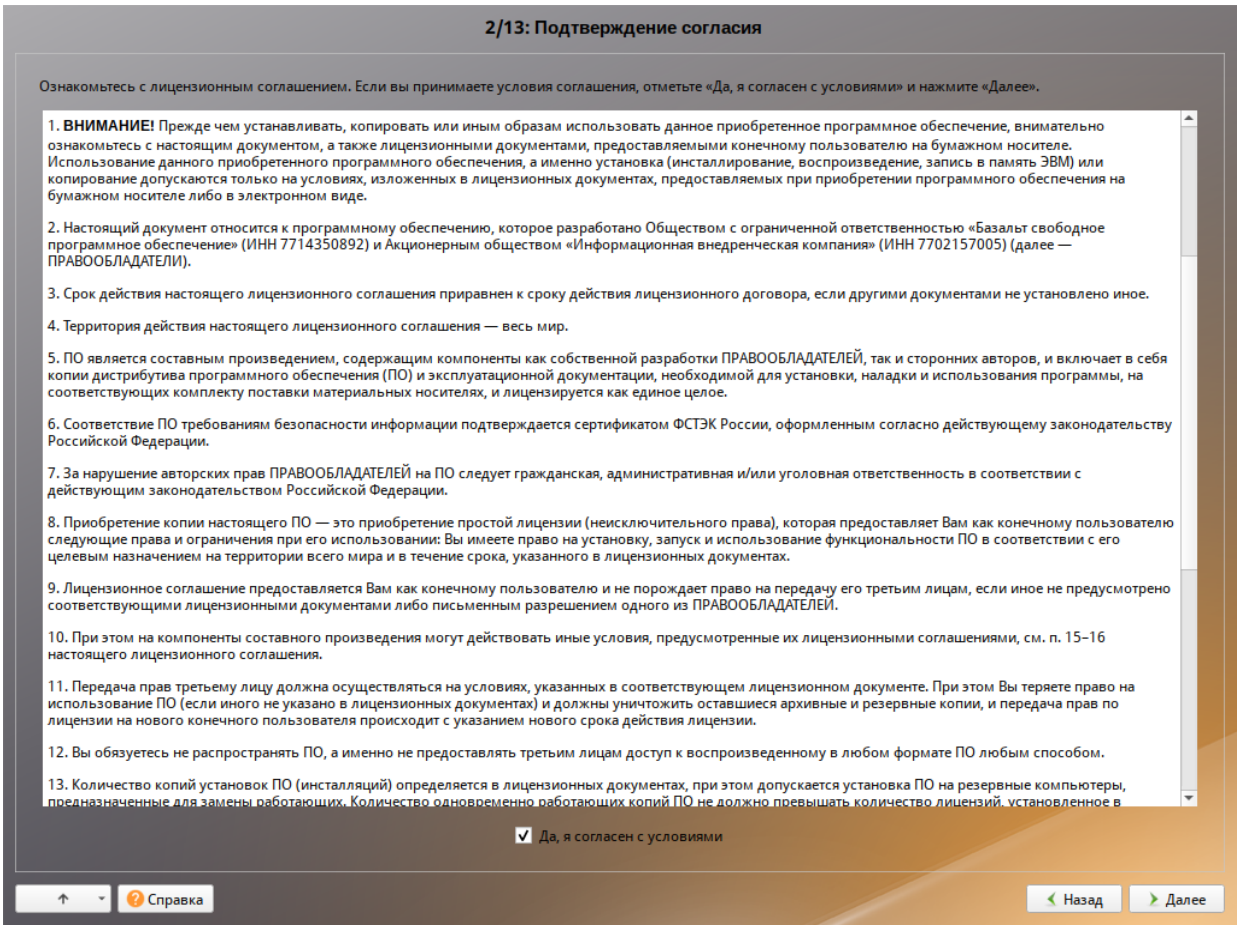


Рис. 8 – Установка. Подтверждение согласия

Перед продолжением установки следует внимательно прочитать условия, регулирующие права владельца экземпляра дистрибутива ОС Альт СП на использование дистрибутива, а также включенных в состав дистрибутива отдельных программ для ЭВМ в установленных условиями пределах.

Для подтверждения согласия следует отметить пункт «Да, я согласен с условиями» и нажать на кнопку «Далее».

5.4.3. Дата и время

После окна «Подтверждения согласия» ОС Альт СП программа установки переходит к окну «Дата и время». На данном этапе выполняется выбор региона и часового пояса (рис. 9).

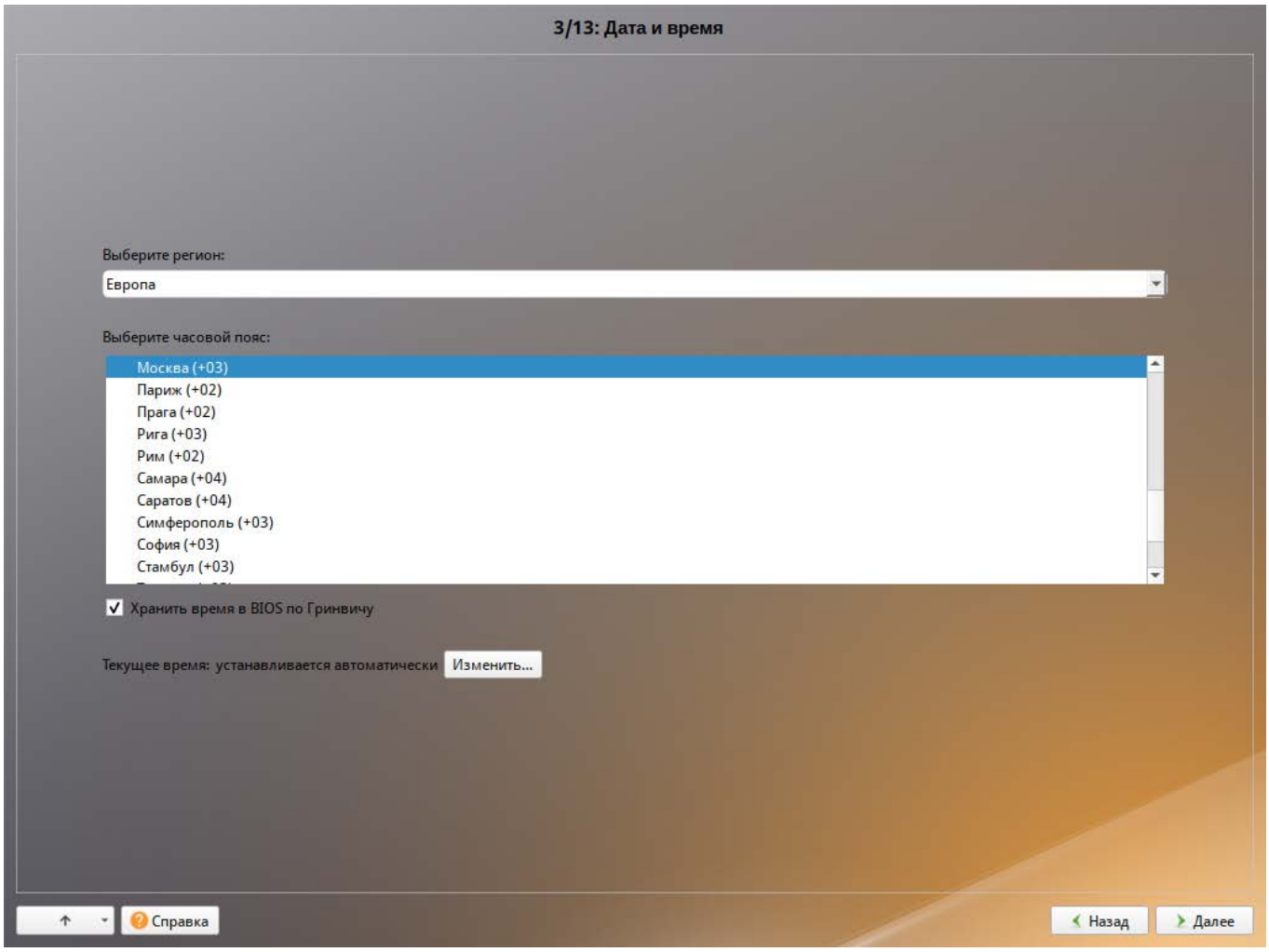


Рис. 9 – Установка. Выбор часового пояса

На этом шаге следует выбрать часовой пояс, по которому нужно установить часы. Для этого в соответствующих списках выберите регион, а затем часовой пояс. 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 на кнопку «Изменить…». Откроется окно ручной настройки системных параметров даты и времени (рис. 10).

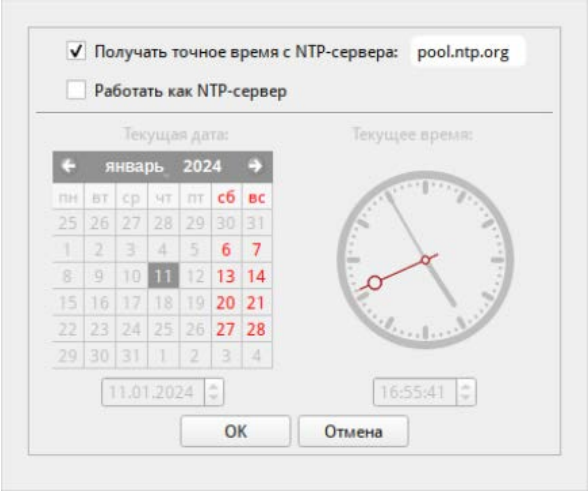


Рис. 10 – Установка. Настройка времени

По умолчанию для синхронизации системных часов (NTP) с удаленным сервером по сети Интернет отмечен пункт «Получать точное время с NTP-сервера» и указан NTP-сервер `pool.ntp.org`.

Для работы компьютера в качестве сервера точного времени внутри локальной сети нужно отметить пункт «Работать как NTP-сервер».

Для сохранения настроек и продолжения установки системы в окне ручной установки даты и времени следует нажать на кнопку «ОК» и затем в окне «Дата и время» нажать на кнопку «Далее».

5.4.4. Подготовка диска

На этом этапе программа установки подготавливает площадку для установки ОС Альт СП, в первую очередь – выделяется свободное место на диске.

Переход к этому шагу может занять некоторое время – период ожидания может быть разным и зависит от производительности компьютера, объема жесткого диска, количества разделов на нем и других параметров.

5.4.4.1. Выбор профиля разбиения диска

После завершения первичной конфигурации загрузочного носителя откроется окно «Подготовка диска» (рис. 11). В списке разделов перечислены уже существующие на жестких дисках разделы (в том числе здесь могут оказаться съемные USB-носители, подключенные к компьютеру в момент установки).

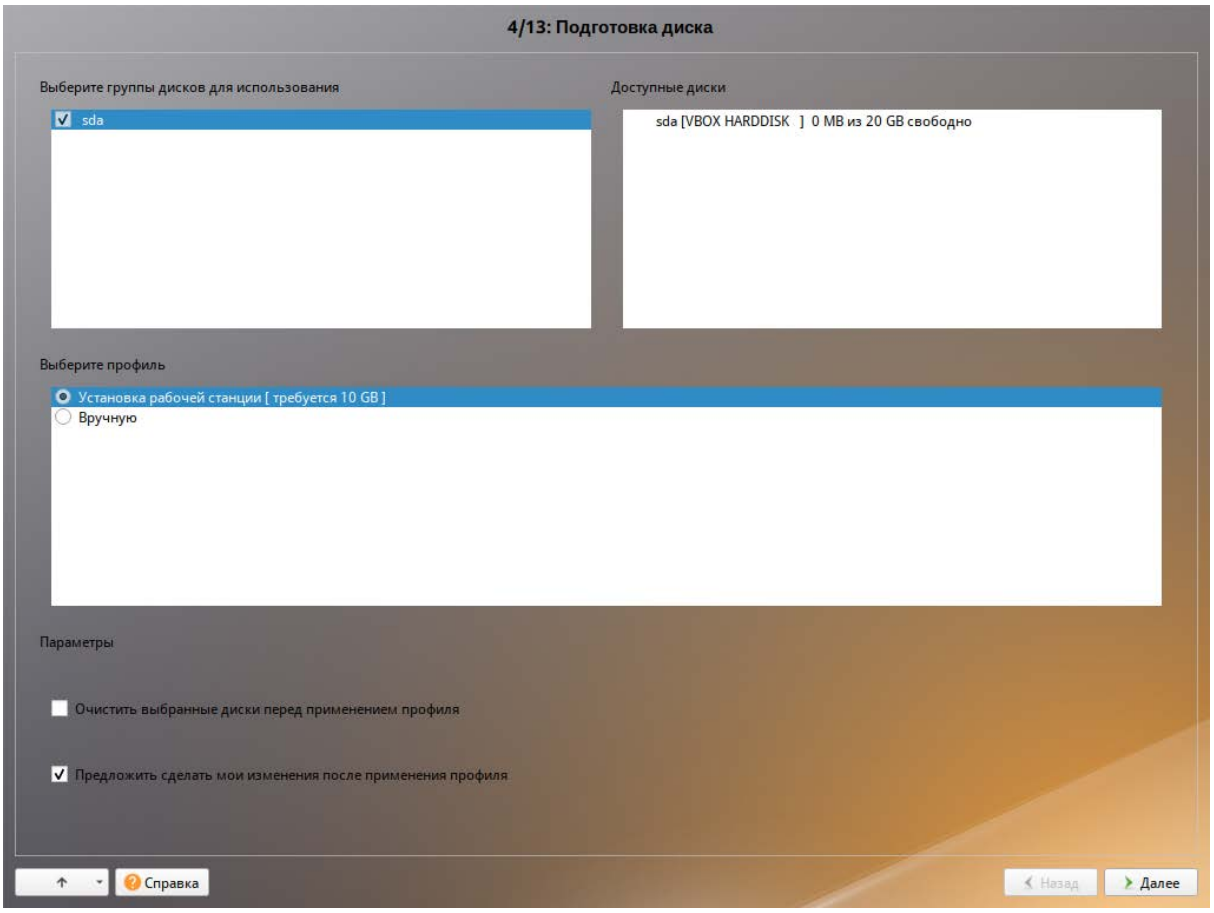


Рис. 11 – Установка. Установка рабочей станции

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/рабочей станции;
- вручную.

Первый профиль предполагает автоматическое разбиение диска.

5.4.4.2. Автоматические профили разбиения диска

Если происходит установка ОС с UEFI, то при разбиении диска будет выделен раздел `/boot/efi`.

Если происходит установка сервера, то при разбиении диска могут быть выделен отдельный раздел для корневой файловой системы. Оставшееся место будет отведено под каталог `/var`.

Если происходит установка рабочей станции, то при разбиении диска будут выделен отдельный раздел для корневой файловой системы. Оставшееся место будет отведено под файловую систему содержащую домашние каталоги пользователей `/home`.

Также перед применением профиля разбиения диска, можно выбрать пункт «Очистить выбранные диски перед применением профиля». Это означает, что все данные будут удалены с диска, после нажатием кнопки «Далее».

Если при применении автоматического профиля разбиения диска доступного места на диске окажется недостаточно, то на экран будет выведено сообщение об ошибке:

```
Невозможно применить профиль, недостаточно места на диске
```

5.4.4.3. Ручной профиль разбиения диска

При нужности 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 разделы самостоятельно или вернуться к шагу выбора профиля и применить автоматический профиль. Выбор этой возможности требует знаний об устройстве диска и технологиях его разбиения.

По нажатию «Далее» будет произведена запись новой таблицы разделов на диск и форматирование разделов. Разделы, только что созданные на диске программой установки, пока не содержат данных и поэтому форматируются без предупреждения. Уже существовавшие, но измененные 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 нужно сохранить, например, со старыми пользовательскими данными (`/home`). Отформатировать можно любые разделы, которые хотите «очистить» (т. е. удалить все данные).

Для того чтобы система правильно работала (в частности могла загрузиться) с UEFI, при ручном разбиении диска надо обязательно сделать точку монтирования `/boot/efi`, в которую нужно смонтировать vfat раздел с загрузочными записями. Если такого раздела нет, то его надо создать вручную. При разбивке жесткого диска в автоматическом режиме такой раздел создает сам установщик. Особенности разбиения диска в UEFI-режиме:

- требуется создать новый или подключить существующий FAT32-раздел с GPT-типом ESP (efi system partition) размером 100 – 500 Мбайт (будет смонтирован в `/boot/efi`);
- может понадобиться раздел типа «bios boot partition» минимального размера, никуда не подключенный и предназначенный для встраивания grub2-efi;
- остальные разделы – и файловая система, и swap – имеют GPT-тип «basic data»; актуальный тип раздела задается отдельно.

5.4.4.4. Дополнительные возможности разбиения диска

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

5.4.4.4.1. Создание программного RAID-массива

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

Для создания RAID-массива нужно два и более жестких 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 жестких дисках;
- создание RAID-массивов на разделах жесткого диска;
- создание файловых систем на RAID-массиве.

П р и м е ч а н и е . Для создания программного RAID-массива может потребоваться предварительно удалить существующую таблицу разделов с жесткого диска.

П р и м е ч а н и е . Системный раздел EFI должен быть физическим разделом в основной таблице разделов диска.

Для настройки параметров нового раздела из состава RAID-массива нужно выбрать неразмеченный диск в окне профиля разбивки пространства «Вручную» и нажать на кнопку «Создать раздел». После этого откроется окно (рис. 12).

Для создания программного массива на GPT-разделах в этом окне нужно настроить следующие параметры:

- «Размер» – в поле нужно указать размер будущего раздела в Мбайт;
- «Смещение» – в поле нужно указать смещение начала данных на диске в Мбайт;
- «Тип раздела» – в выпадающем поле нужно выбрать значение «basic data» для последующего включения раздела в RAID-массивы;
- «Создать том» – следует снять отметку с этого пункта (не создавать том).

П р и м е ч а н и е . В режиме Legacy при создании разделов на жестких дисках для последующего включения их в RAID-массивы следует указать «Тип раздела» для них равным «Linux RAID» (рис. 13).

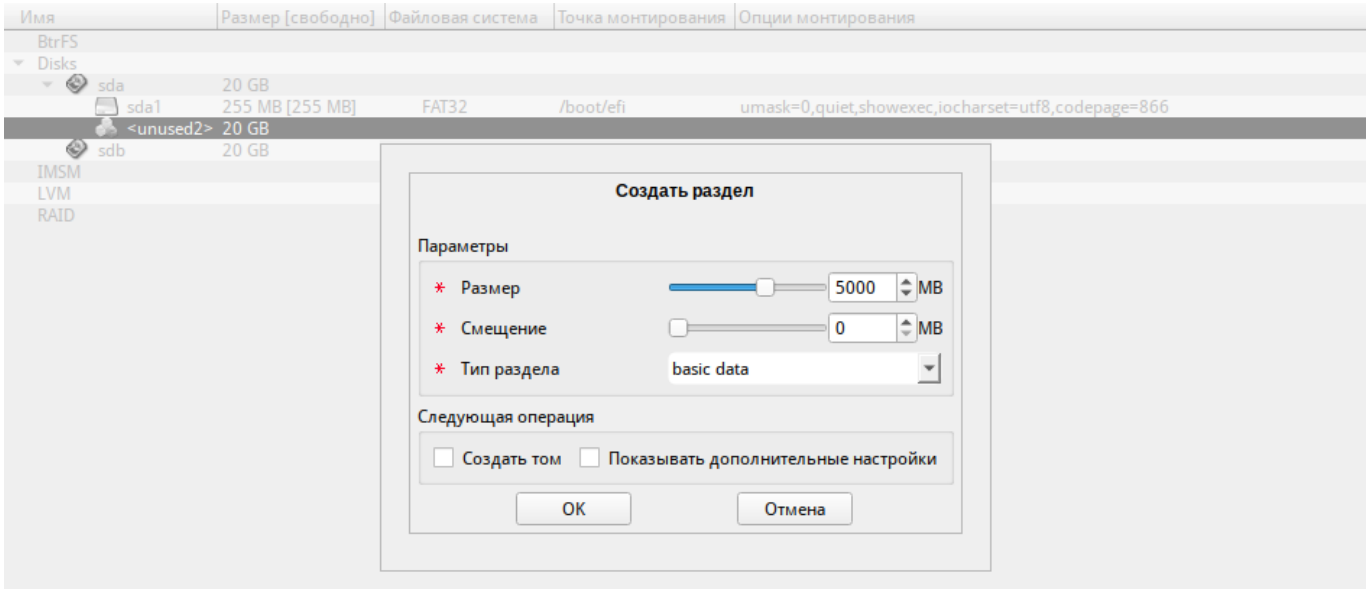


Рис. 12 – Создание раздела программного массива в режиме UEFI

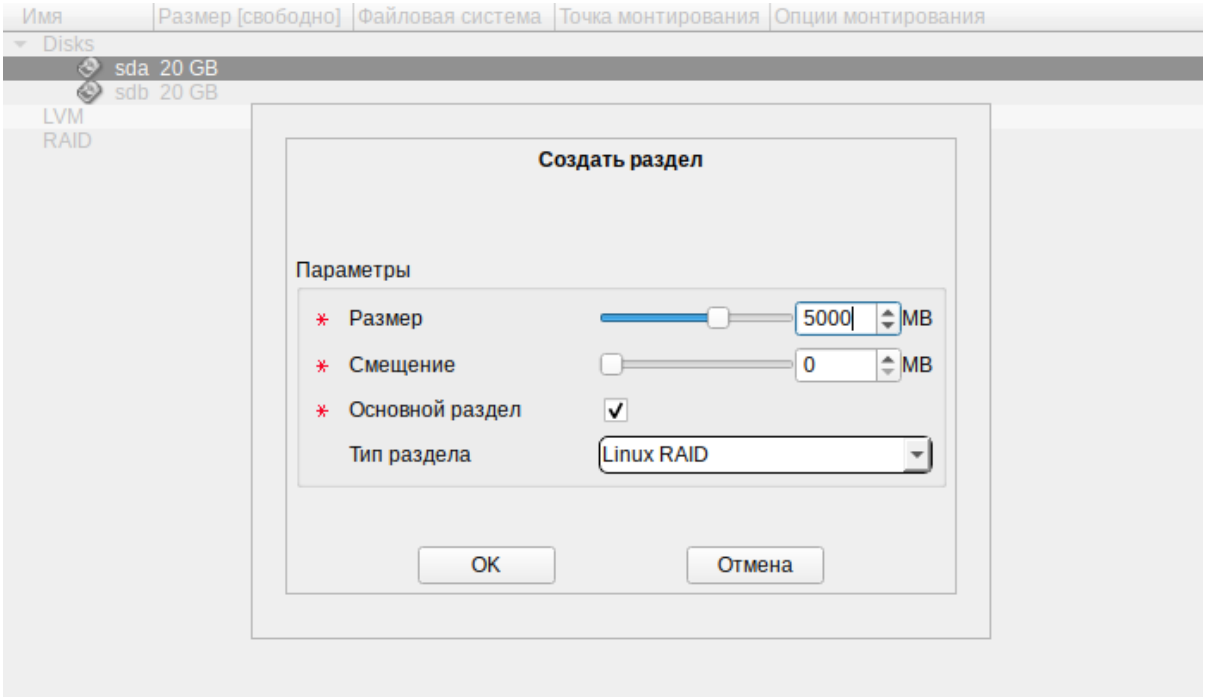


Рис. 13 – Установка. Подготовка диска. Создание раздела Linux RAID

Примечание. Объем результирующего массива может зависеть от размера, включенных в него разделов жесткого диска.

После создания разделов на дисках можно переходить к организации самих RAID-массивов. Для этого в списке следует выбрать пункт «RAID», после чего нажать на кнопку «Создать RAID». Далее мастер предложит выбрать тип массива и указать его участников (рис. 14, рис. 15).

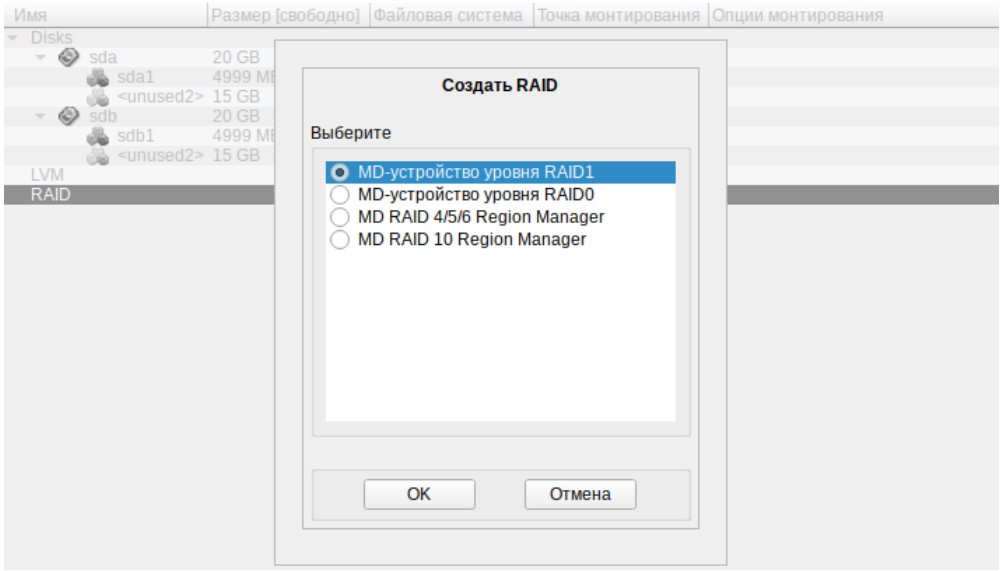


Рис. 14 – Установка. Подготовка диска. Выбор типа RAID-массива

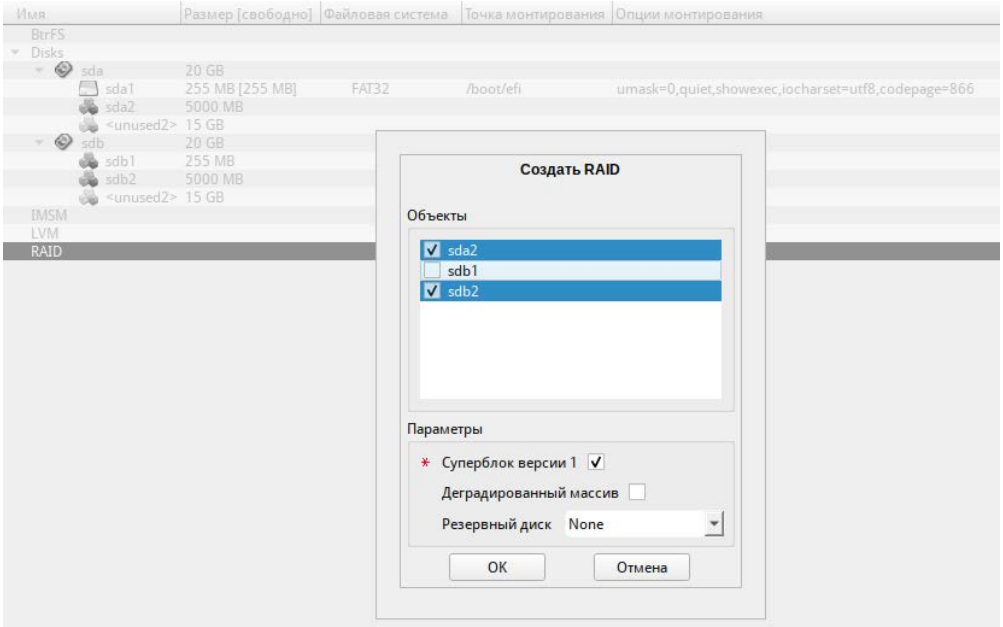


Рис. 15 – Установка. Подготовка диска. Выбор участников RAID-массива

После создания RAID-массивов их можно использовать как обычные разделы на жестких дисках, то есть, на них можно создавать файловые системы или же, например, включать их в LVM-тома.

5.4.4.4.2. 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 можно разбить на следующие шаги:

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

Примечание. Для создания группы томов LVM может потребоваться предварительно удалить таблицу разделов с жесткого диска.

Примечание. Системный раздел EFI должен быть физическим разделом в основной таблице разделов диска.

Для настройки параметров нового раздела нужно выбрать неразмеченный диск в окне профиля разбивки пространства «Вручную» и нажать на кнопку «Создать раздел». После этого откроется окно (рис. 12).

При создании разделов на жестких дисках для последующего включения их в LVM-тома на GPT-разделах в этом окне нужно настроить следующие параметры:

- «Размер» – в поле нужно указать размер будущего раздела в Мбайт;
- «Смещение» – в поле нужно указать смещение начала данных на диске в Мбайт;
- «Тип раздела» – в выпадающем поле нужно выбрать значение «basic data» для последующего включения раздела в RAID-массивы;
- «Создать том» – нужно снять отметку с этого пункта (не создавать том).

Примечание. В режиме Legacy при создании разделов на жестких дисках для последующего включения их в LVM-тома следует указать «Тип раздела» для них, равным «Linux LVM» (рис. 16).

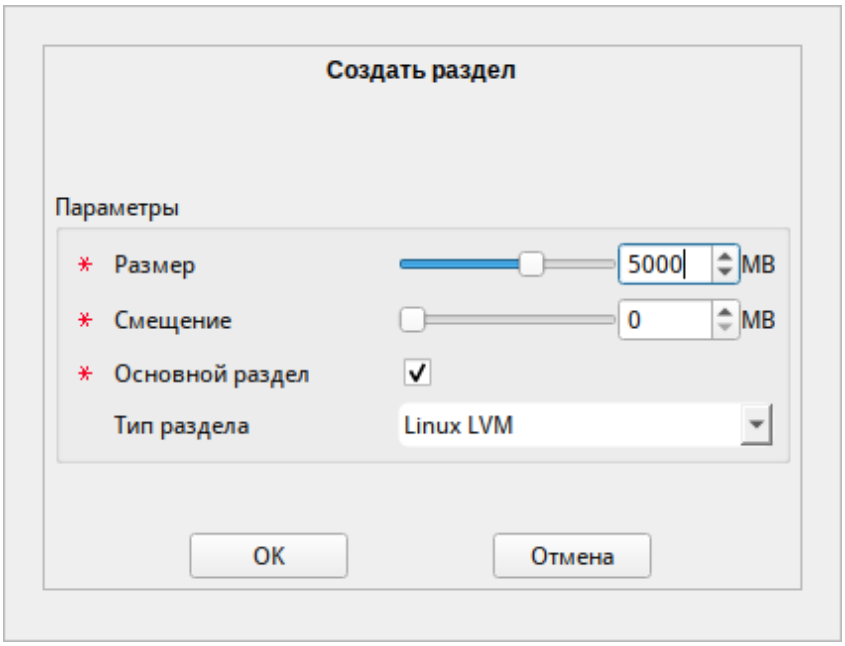


Рис. 16 – Создание раздела Linux LVM в режиме Legacy

Для создания группы томов LVM в списке следует выбрать пункт «LVM», после чего нажать на кнопку «Создать группу томов» (рис. 17).

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

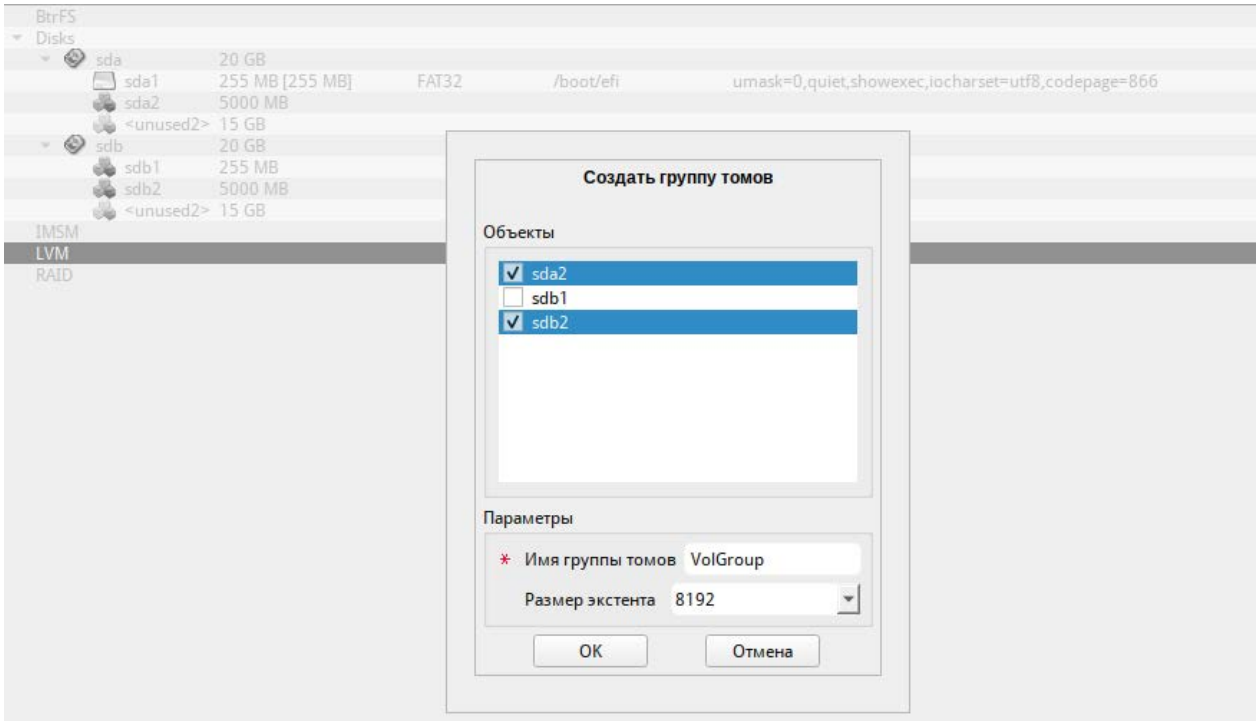


Рис. 17 – Установка. Подготовка диска. Создание группы томов LVM

После создания группы томов LVM ее можно использовать как обычный жесткий диск, то есть внутри группы томов можно создавать тома (аналог раздела на физическом жестком диске) и файловые системы внутри томов (рис. 18).

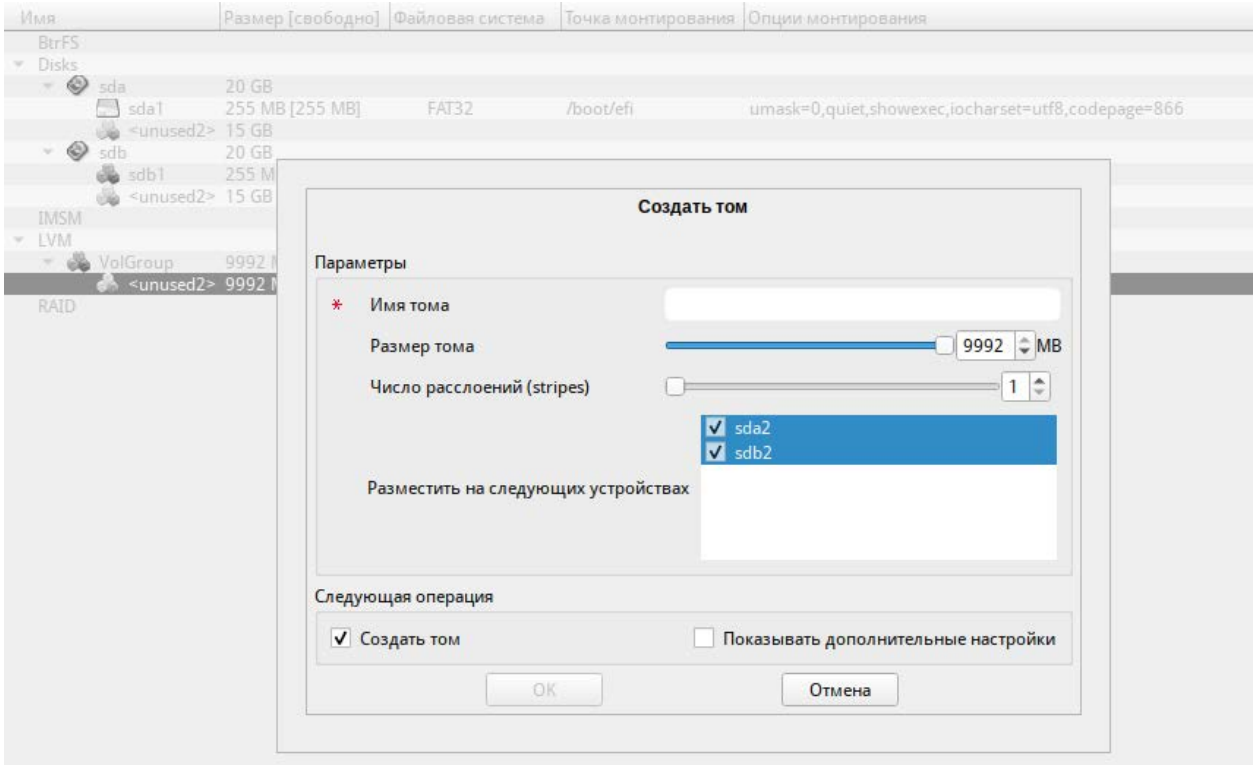


Рис. 18 – Установка. Подготовка диска. Создание тома

5.4.4.4.3. Создание шифруемых разделов

Программа установки ОС Альт СП позволяет создавать шифруемые разделы с использованием встроенных средств маскирования.

Для создания шифруемого раздела и выполнения дальнейшей разметки нужно выбрать требуемый диск и нажать на кнопку «Создать шифруемый раздел».

В открывшемся окне доступны следующие настройки (рис. 19):

- «Размер» – общий размер шифруемого тома;
- «Смещение» – настройка осуществляется с помощью ползунка либо путем ввода значения с клавиатуры (в поле нужно указать смещение начала данных на диске в Мбайт);
- «Основной раздел» – нужно отметить пункт, если раздел является основным для установки ОС;
- «Тип раздела» – в выпадающем поле нужно выбрать значение «Linux»;

- «Создать шифруемый том» – отметить пункт для автоматического перехода к настройке файловой системы на данном разделе;
- «Показывать дополнительные настройки» – отметить пункт для отображения дополнительных настроек при последующей работе с разделом.

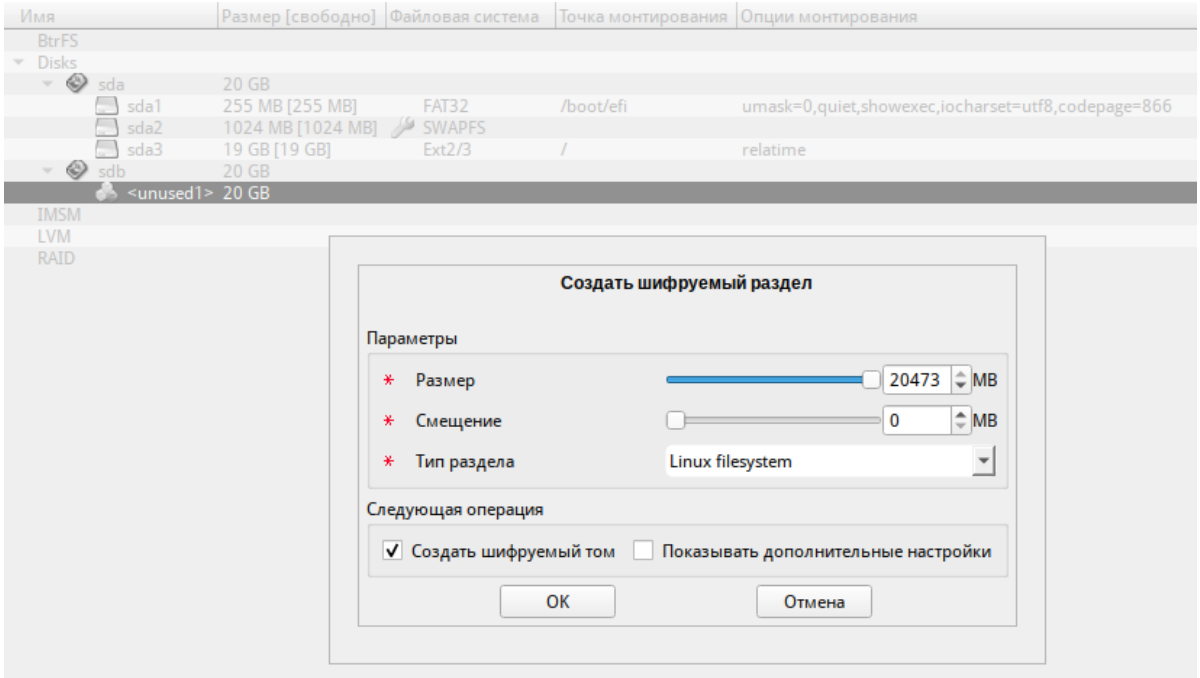


Рис. 19 – Установка. Подготовка диска. Создание кодируемого раздела

После создания шифруемого раздела мастер, как и при создании обычного раздела, предложит создать на нем файловую систему и при нужности потребует указать точку монтирования.

⚠ Установка загрузчика на шифруемый раздел не поддерживается.

Для сохранения всех внесенных настроек и продолжения установки в окне «Подготовка диска» нужно нажать на кнопку «Далее».

5.4.4.4.4. Создание подтомов BtrFS

BtrFS – файловая система, которая может работать с очень большими файлами, имеется поддержка снимков файловой системы (снапшотов), сжатие и подтома.

Подтом (subvolume) не является блочным устройством, но в каждом томе BtrFS создается 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 нужности, например, для `/` и `/home` создаются подтома с именами `@` и `@home`. Для монтирования подтомов нужны определенные параметры вместо корня системы BtrFS по умолчанию:

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

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

Программа установки позволяет создать подтома (subvolume), указав разные точки монтирования.

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

- создание разделов на жестких дисках;
- создание подтомов на разделах жесткого диска.

Для настройки параметров нового раздела нужно выбрать неразмеченный диск в окне профиля разбивки пространства «Вручную» и нажать кнопку «Создать раздел».

При создании раздела на жестком диске следует указать «Тип раздела» равным «Linux-filesystem» или «basic data» (рис. 20).

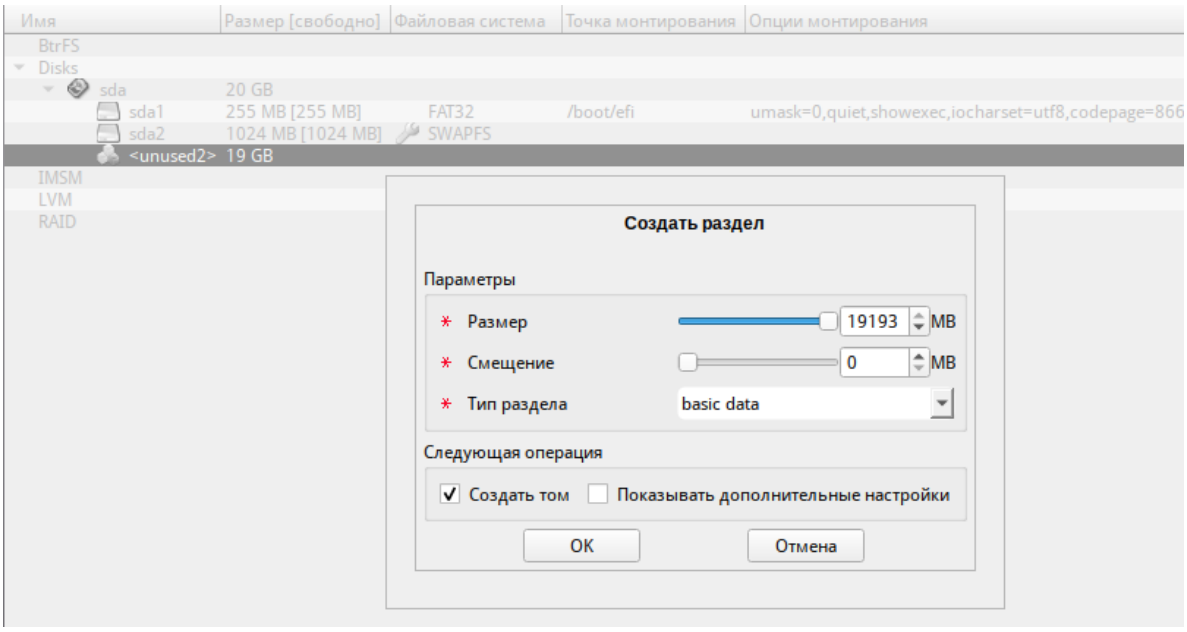


Рис. 20 – Создание раздела с ФС BtrFS в режиме UEFI

П р и м е ч а н и е . В режиме Legacy при создании раздела на жестком диске следует указать «Тип раздела» равным «Linux» (рис. 21).

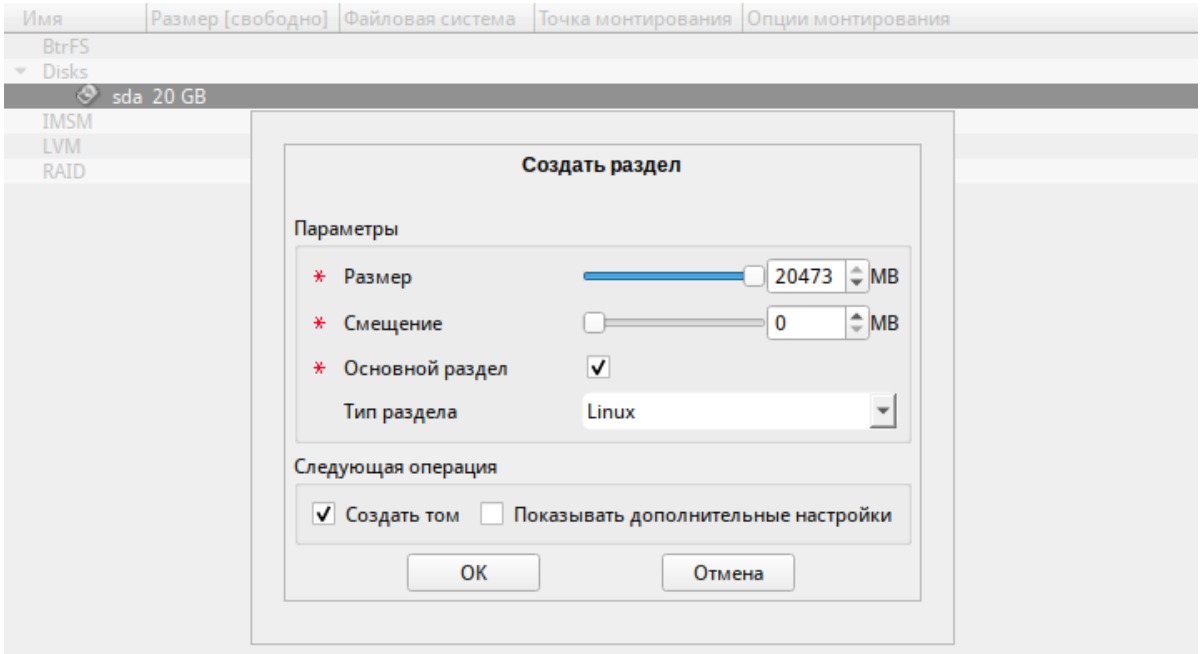


Рис. 21 – Создание раздела с ФС BtrFS в режиме Legacy

На следующем шаге выбрать файловую систему BtrFS (рис. 22).

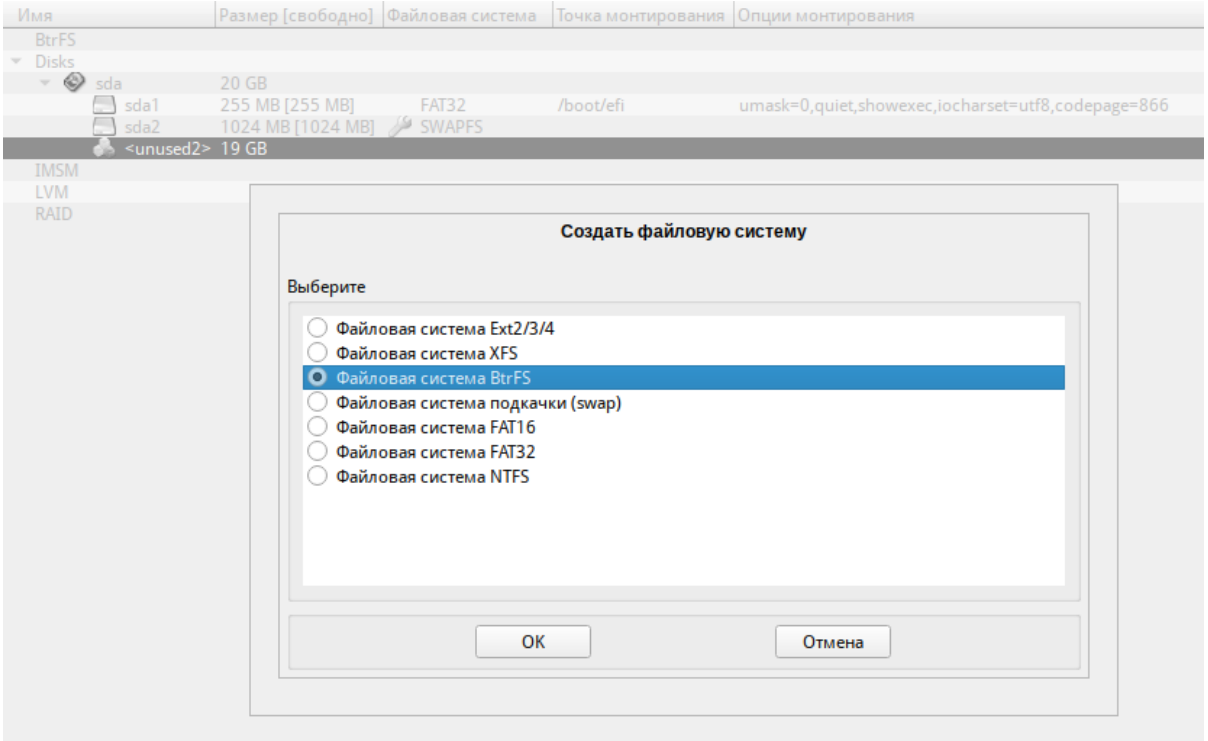


Рис. 22 – Создание раздела с ФС BtrFS

В окне «Изменить точку монтирования» (рис. 23) нажать кнопку «Отмена» (не указывать точку монтирования для раздела).

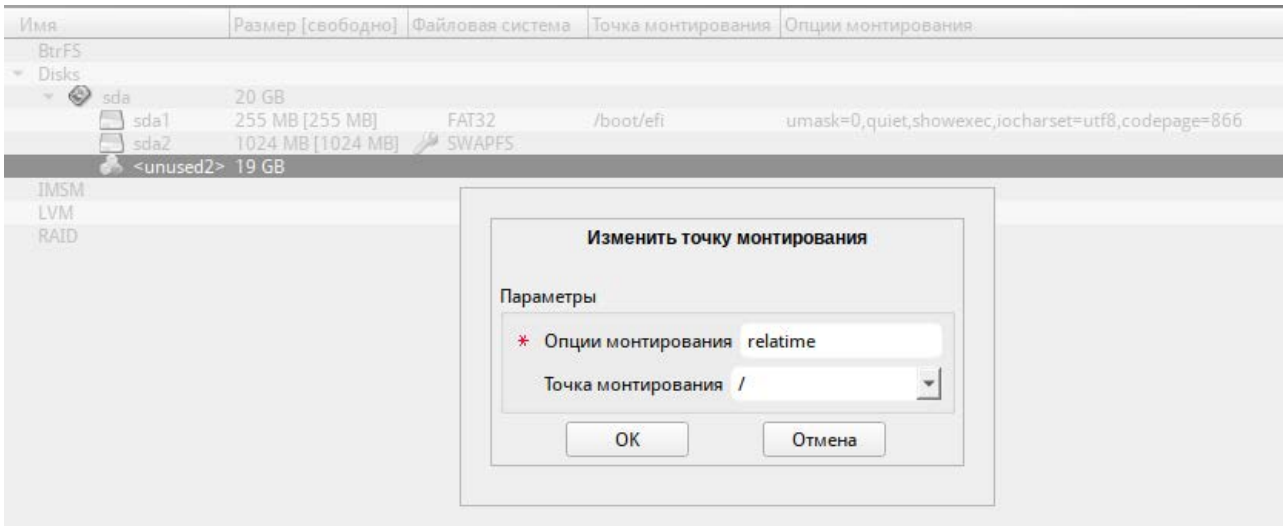


Рис. 23 – Окно «Изменить точку монтирования»

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

В открывшемся окне следует указать имя подтома или путь до него. На рис. 24 показано создание подтома `@home`. Данное действие следует повторить для создания подтома `@`.

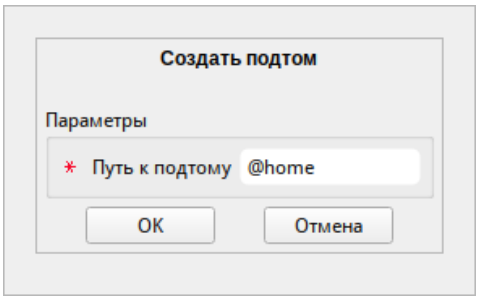


Рис. 24 – Создание подтома

После создания подтомов нужно указать точки монтирования для каждого тома. Для этого выбрать подтом и нажать кнопку «Изменить точку монтирования» (рис. 25).

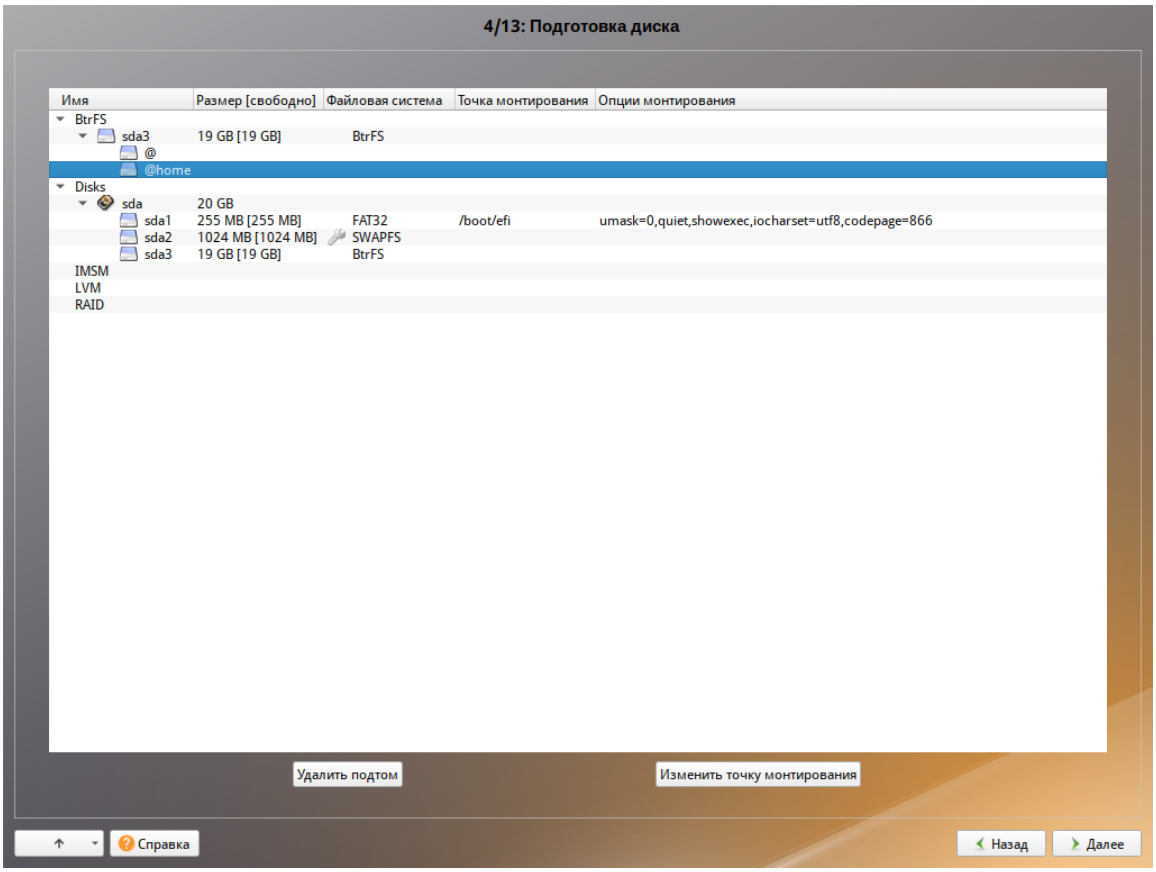


Рис. 25 – Созданные подтома

В открывшемся окне указать точку монтирования (рис. 26).

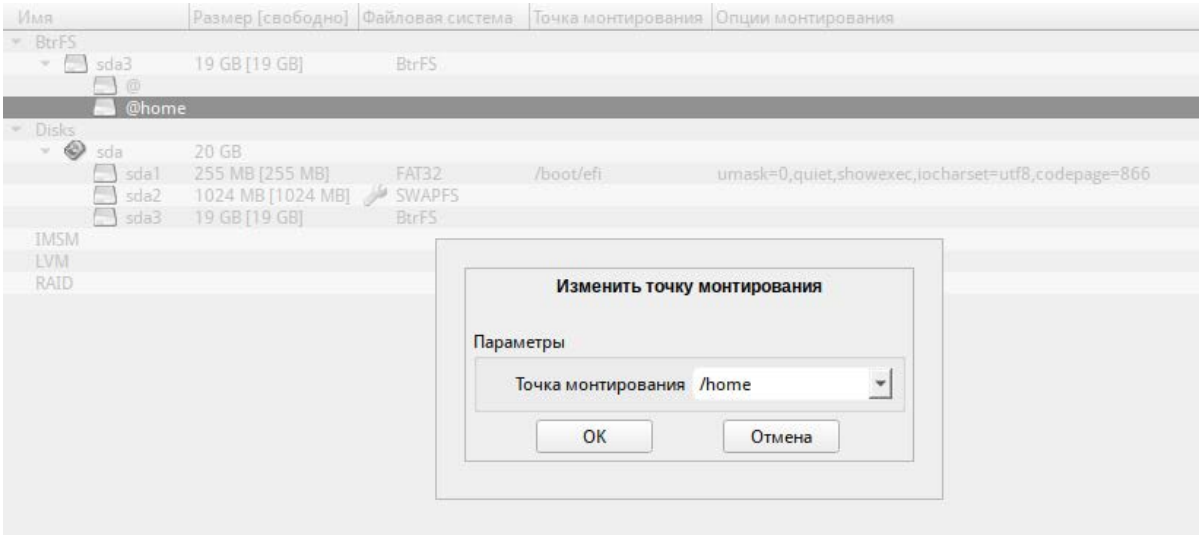


Рис. 26 – Точка монтирования для подтома `@home`

После указания точек монтирования для подтомов можно установить систему как обычно.

5.4.5. Перемонтирование

По завершении этапа подготовки диска начинается шаг перемонтирования. Он проходит автоматически и не требует вмешательства пользователя. На экране отображается индикатор выполнения (рис. 27).

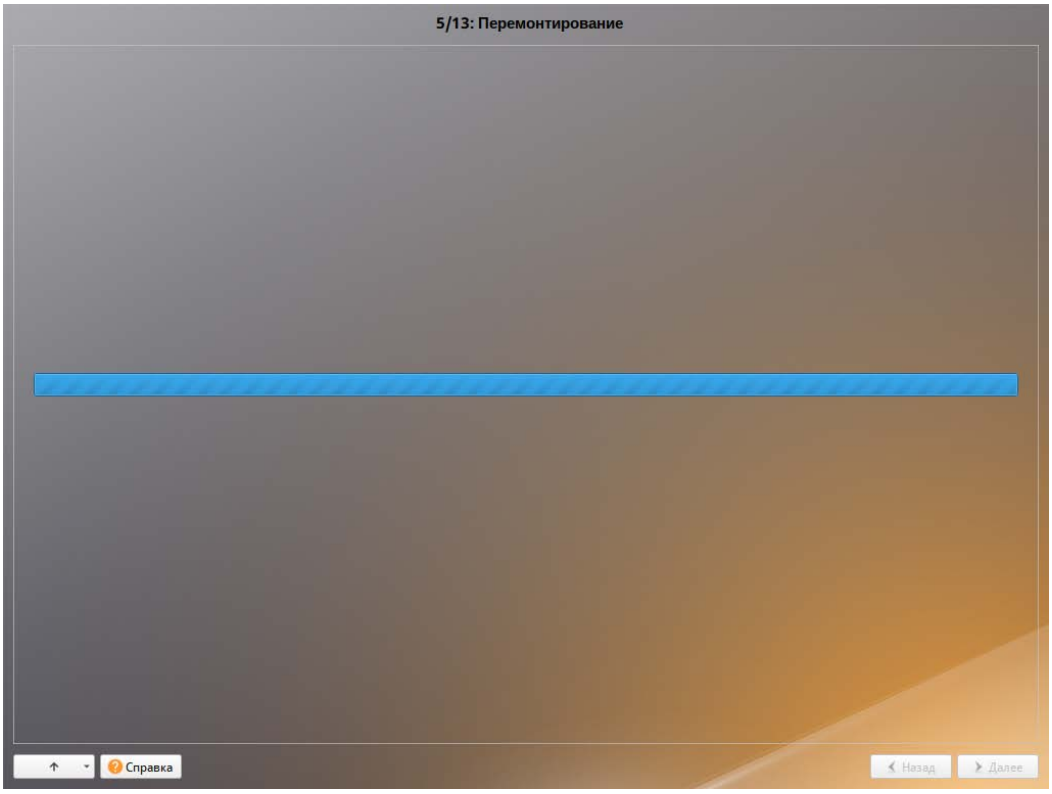


Рис. 27 – Перемонтирование

После сохранения настроек осуществляется автоматический переход к следующему шагу.

5.4.6. Установка системы

На данном этапе происходят распаковка ядра и установка набора программ, которые требуются для работы ОС Альт СП.

Установка происходит автоматически в два этапа (рис. 28):

- получение пакетов;
- установка пакетов.

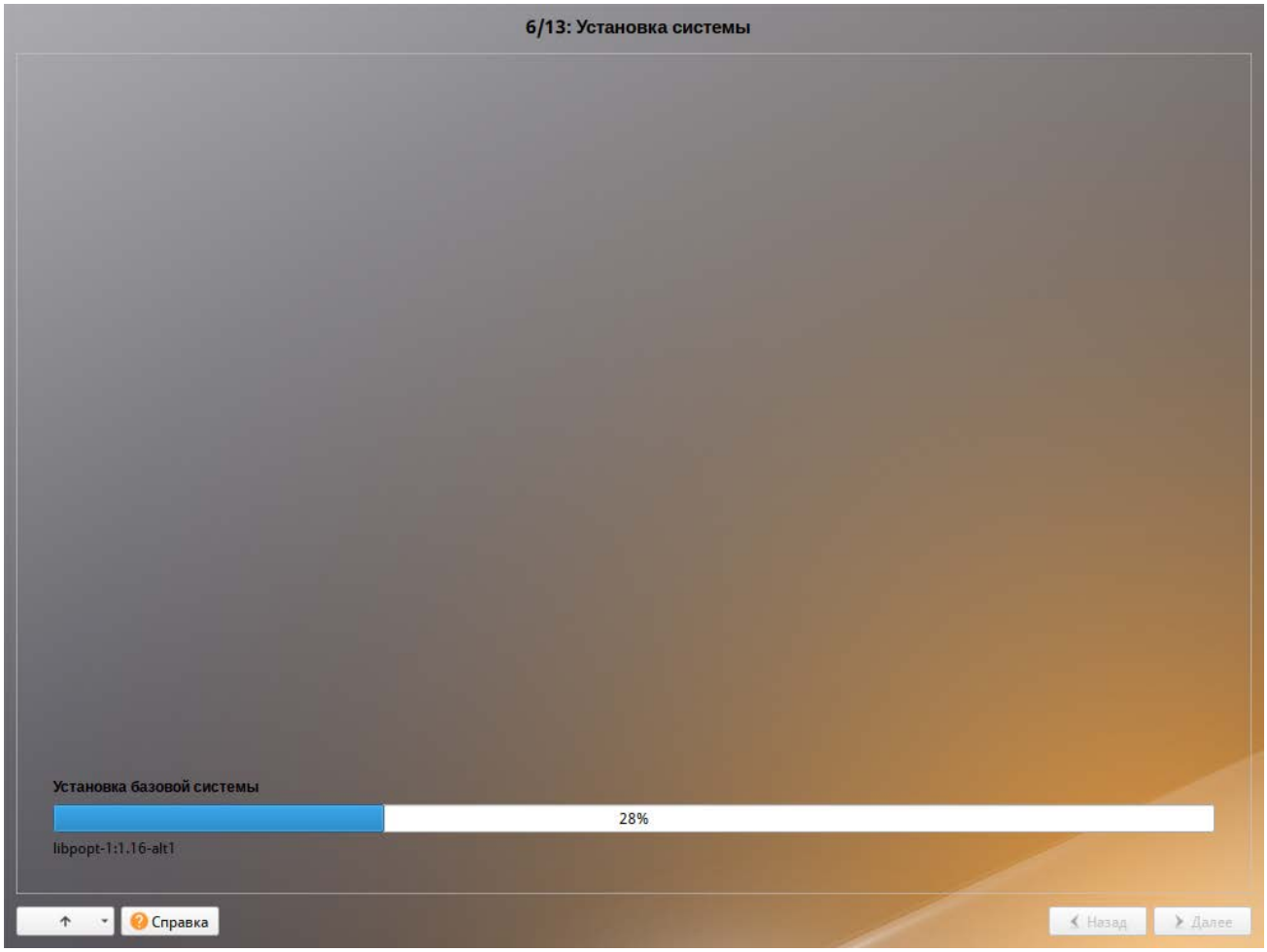


Рис. 28 – Установка. Установка пакетов

Получение пакетов осуществляется с источника, выбранного на этапе начальной загрузки.

5.4.7. 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.

После завершения установки базовой системы выполняется шаг сохранения настроек (рис. 29). Он проходит автоматически и не требует вмешательства пользователя, на экране отображается индикатор выполнения.

Рис. 29 – Установка. Сохранение настроек

На данном этапе производится перенос настроек, выполненных на первых шагах установки, в установленную базовую систему `pool.ntp.o`.

Также производится запись информации о соответствии разделов жесткого диска смонтированным на них файловым системам (заполняется конфигурационный файл `/etc/fstab`).

В список доступных источников программных пакетов добавляется репозиторий, находящийся на установочном лазерном диске – выполняется команда `apt-cdrom add`, осуществляющая запись в конфигурационный файл `/etc/apt/sources.list`.

После сохранения настроек осуществляется автоматический переход к следующему шагу.

5.4.8. Установка загрузчика

Загрузчик ОС – программа, которая позволяет загружать ОС.

Программа установки автоматически определяет, в каком разделе НЖМД следует располагать загрузчик для возможности корректного запуска ОС Альт СП. Модуль установки загрузчика предложит вариант EFI (рис. 30), с которым стоит согласиться.

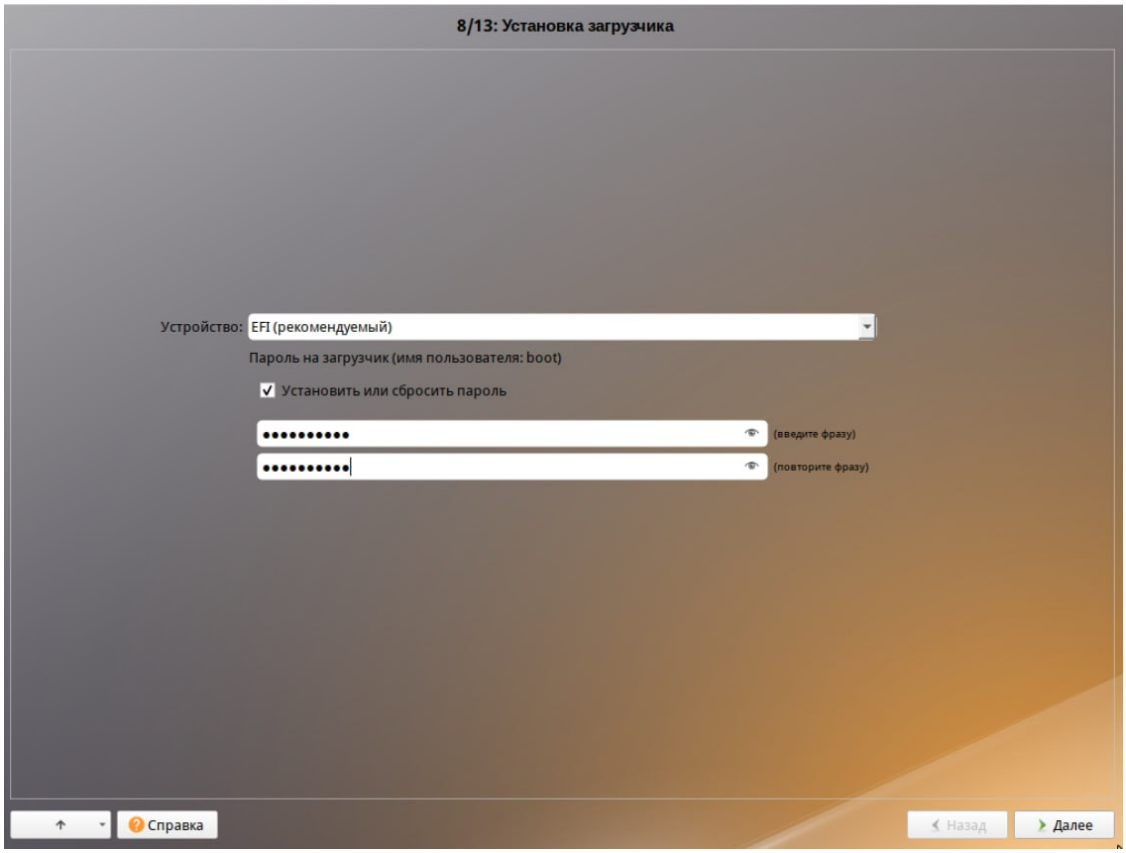


Рис. 30 – Установка. Установка загрузчика

Примечание. Установка загрузчика при установке в режиме Legacy показана на рис. 31.

Положение загрузчика, в случае нужности, можно изменить в выпадающем списке «Устройство:», выбрав другой раздел.

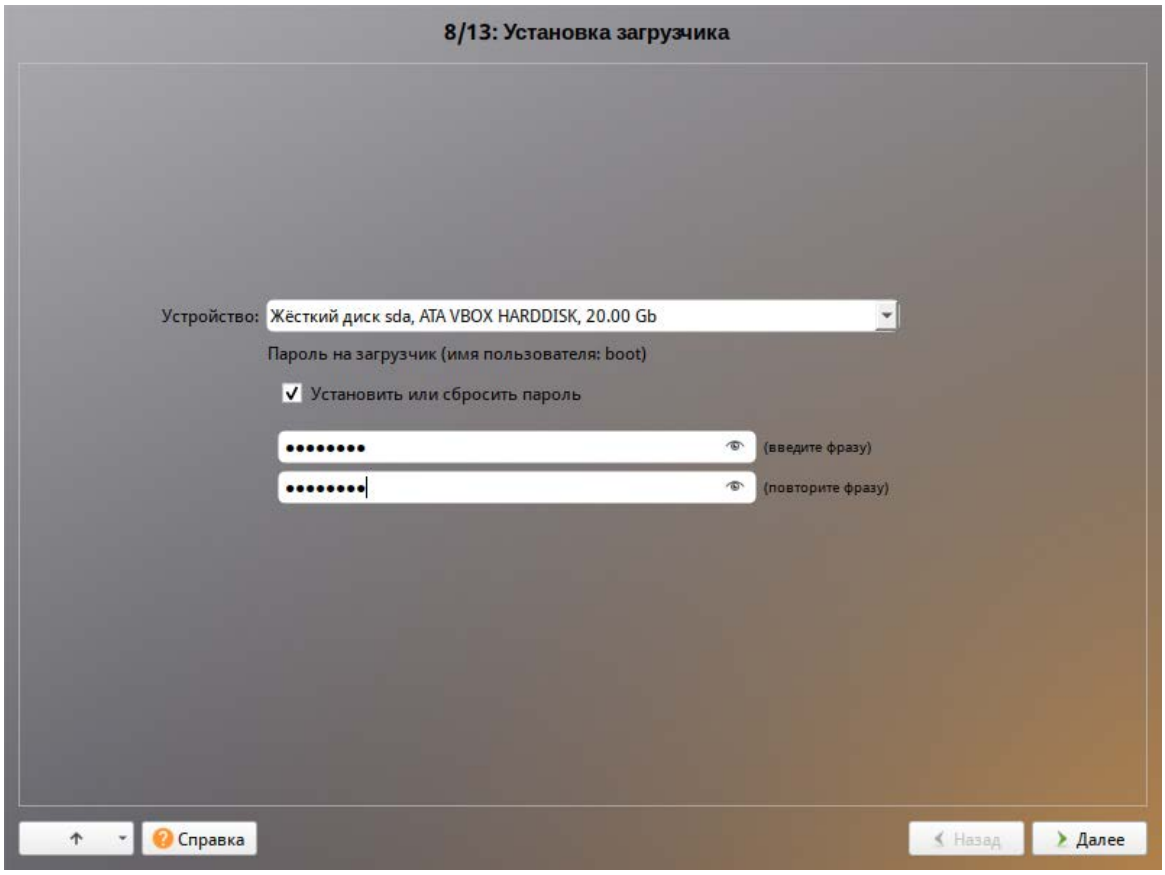


Рис. 31 – Установка загрузчика

Для ограничения доступа к опциям загрузки устанавливается пароль на загрузчик. Чтобы исключить опечатки при вводе пароля, пароль вводится дважды.

Примечание. При нужности изменения опций загрузки при старте компьютера потребуется ввести имя пользователя «boot» и заданный на этом шаге пароль.

ВАЖНО

При установке на EFI выберите в качестве устройства для установки «EFI». Рекомендуется выбрать автоматическое разбиение на этапе разметки диска для создания разделов для загрузки с EFI.

Для подтверждения выбора и продолжения работы программы установки нужно нажать на кнопку «Далее».

5.4.9. Настройка сети

На этом этапе в окне «Настройка сети» нужно задать параметры работы сетевой карты и настройки сети (рис. 32):

- «Имя компьютера:» – указать сетевое имя ПЭВМ в поле для ввода имени компьютера;
- «Интерфейсы:» – выбрать доступный сетевой интерфейс, для которого будут выполняться настройки;
- «Конфигурация:» – выбрать способ назначения IP-адресов (службы DHCP, Zeroconf либо вручную);
- «IP-адреса:» – пул назначенных IP-адресов из поля «IP:», выбранные адреса можно удалить нажатием кнопки «Удалить»;
- «Добавить ↑ IP:» – ввести IP-адрес вручную и выбрать в выпадающем поле предпочтительную маску сети, затем нажать на кнопку «Добавить» для переноса адреса в пул поля «IP-адреса:»;
- «Шлюз по умолчанию:» – в поле для ввода нужно ввести адрес шлюза, который будет использоваться сетью по умолчанию;
- «DNS-серверы:» – в поле для ввода нужно 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 нужно ввести список предпочтительных доменов, по которым будет выполняться поиск.

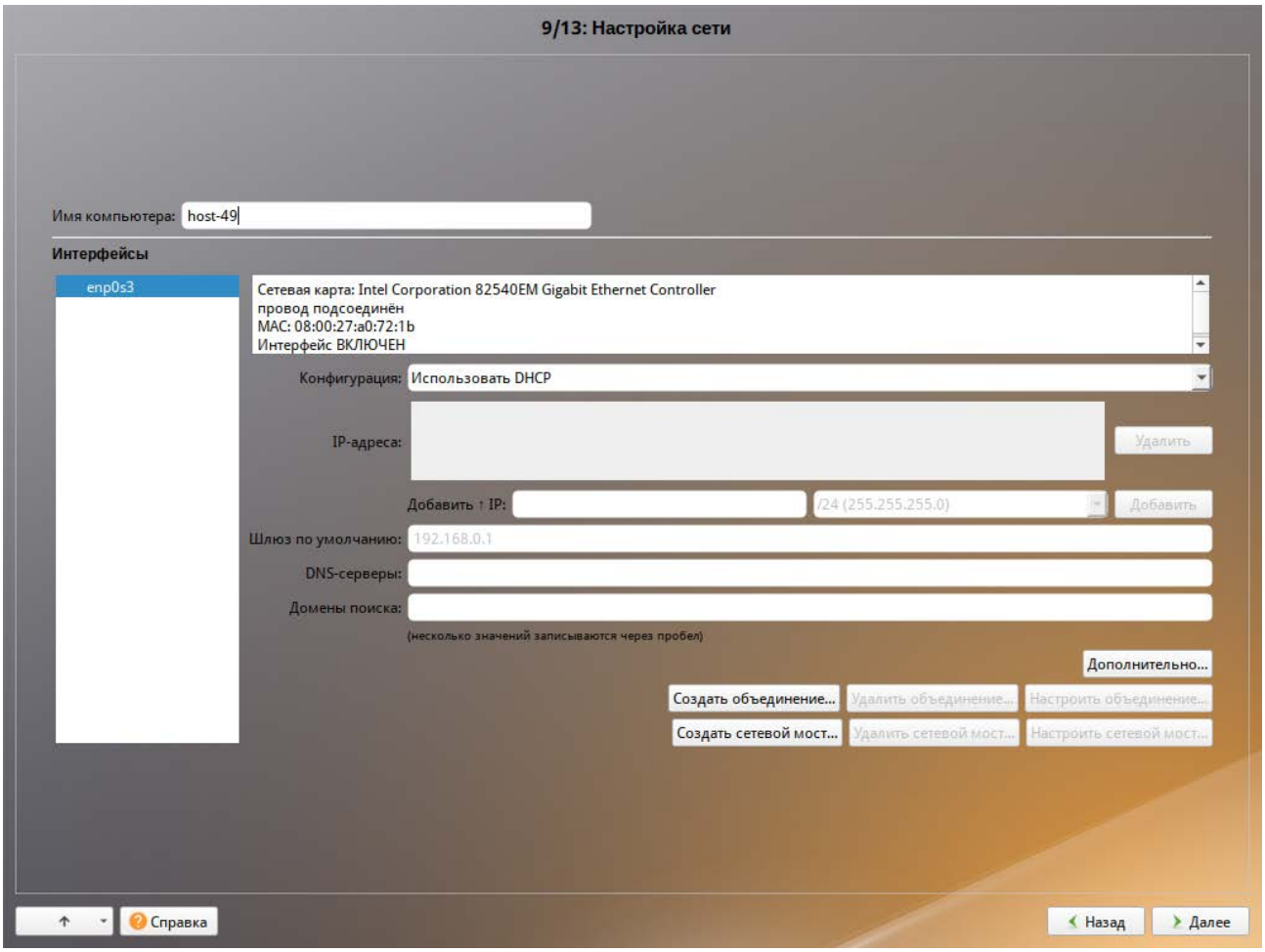


Рис. 32 – Установка. Настройка сети

Конкретные значения будут зависеть от используемого сетевого окружения. Ручного введения настроек можно избежать, если в сети уже есть настроенный DHCP-сервер. В этом случае все нужное сетевые настройки будут получены автоматически.

Для сохранения настроек сети и продолжения работы программы установки нужно нажать на кнопку «Далее».

5.4.10. Администратор системы

На данном этапе загрузчик создает учетную запись администратора (рис. 33). В открывшемся окне нужно ввести пароль учетной записи администратора (root). Чтобы исключить опечатки при вводе пароля, пароль учетной записи вводится дважды.

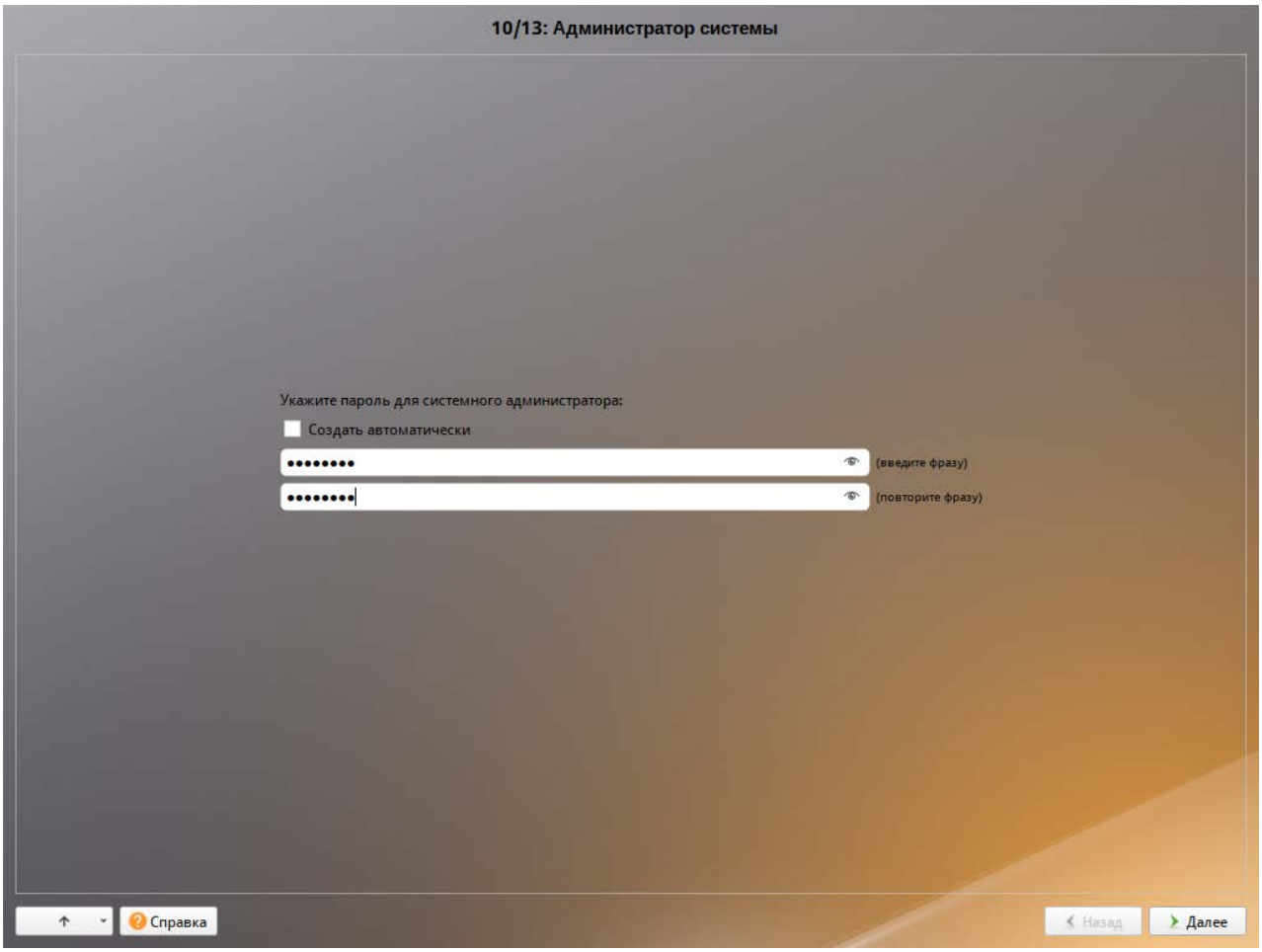


Рис. 33 – Установка. Задание пароля администратора

Для автоматической генерации пароля нужно 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 критичные 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 собственные неосторожные действия от имени root могут иметь катастрофические последствия для всей системы.

ВАЖНО

Запомните пароль root – его нужно будет вводить для получения права изменять настройки системы с помощью стандартных средств настройки ОС. Более подробную информацию о режиме суперпользователя см. в п. 20.2.

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

5.4.11. Системный пользователь

На данном этапе программа установки создает учетную запись системного пользователя (пользователя) ОС Альт СП (рис. 34).

Помимо администратора (root) в систему нужно 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 в окне «Системный пользователь» заполнить следующие поля:

- «Имя:» – имя учетной записи пользователя ОС Альт СП (слово, состоящее только из строчных латинских букв, цифр и символа подчеркивания «_», причем цифра и символ «_» не могут стоять в начале слова, есть также возможность использовать «-». Начинаться имя должно со строчной латинской буквы);
- «Комментарий:» – любой комментарий к имени учетной записи;
- «Пароль:» – пароль учетной записи пользователя (чтобы исключить опечатки при вводе пароля, пароль пользователя вводится дважды).

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

В процессе установки предлагается создать только одну учетную запись пользователя – чтобы от его имени администратор мог выполнять задачи, которые не требуют привилегий администратора (root). Учетные записи для всех прочих пользователей системы можно будет создать в любой момент после ее установки.

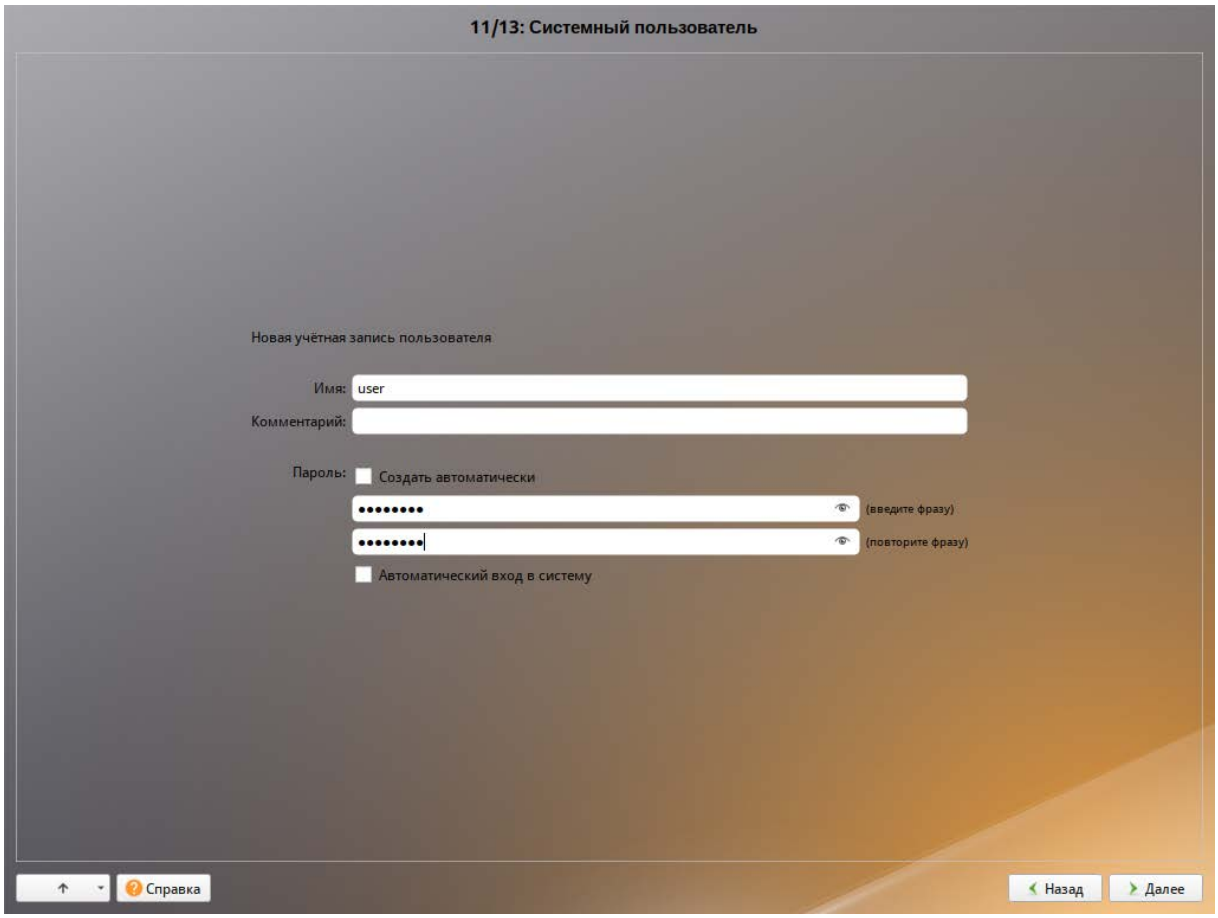


Рис. 34 – Установка. Создание пользователя

5.4.12. Установка пароля на LUKS-разделы

Если на этапе подготовки диска был создан LUKS-раздел, на данном этапе нужно ввести пароль для обращения к этому разделу (рис. 35).

Установленный пароль потребуется вводить для получения доступа к информации на данных разделах.

Примечание. Если кодируемые разделы, не создавались, этот шаг пропускается автоматически.

LUKS надо устанавливать при разметке вручную, удаляя и пересоздавая каждый раздел. LUKS будет требовать пароля при загрузке для каждого раздела.

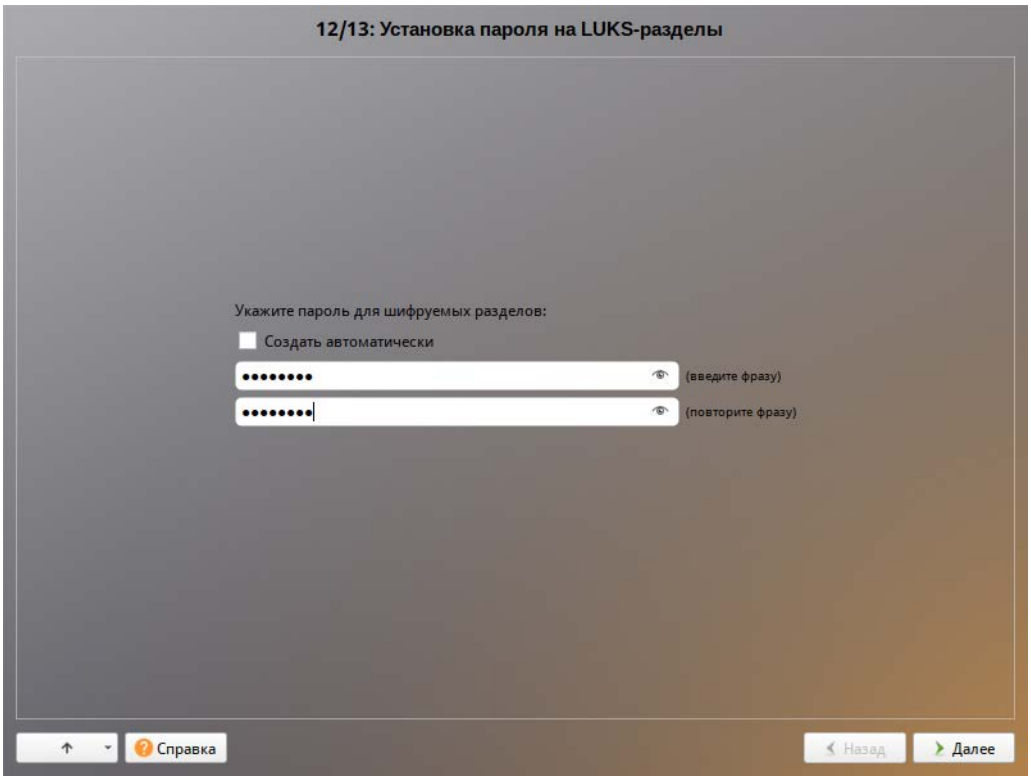


Рис. 35 – Установка. Установка пароля на LUKS-разделы

5.4.13. Завершение установки

На экране последнего этапа установки отображается информация о завершении установки ОС Альт СП (рис. 36).

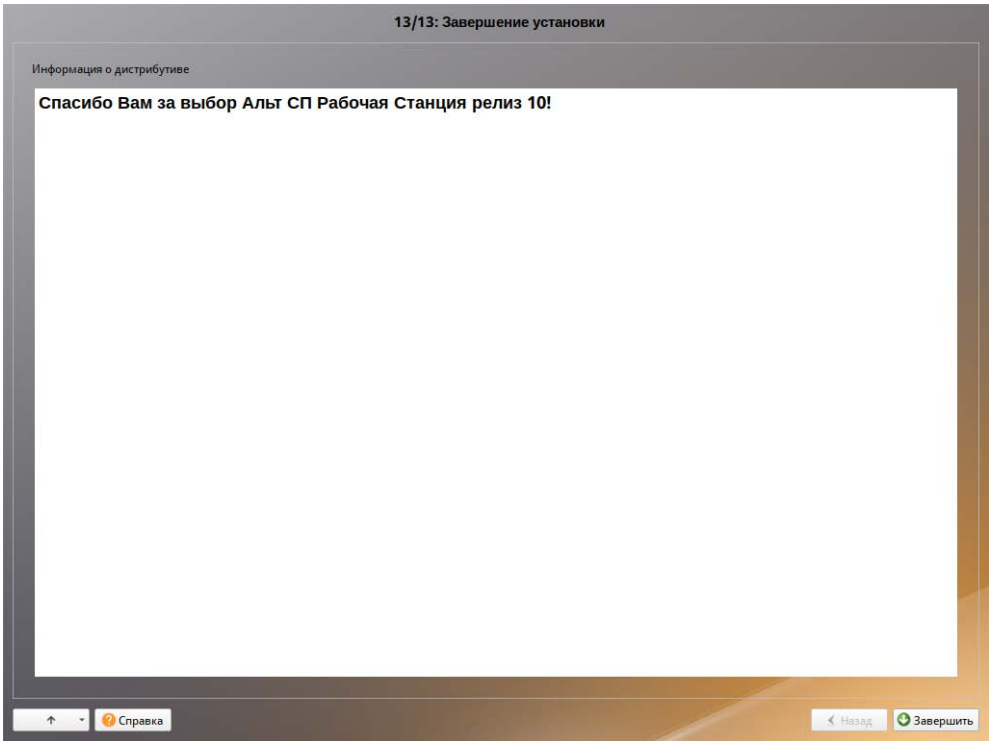


Рис. 36 – Установка. Завершение установки

После нажатия кнопки «Завершить» и перезагрузки компьютера выполняется штатная загрузка установленной ОС.

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

5.5. Автоматическая установка системы (autoinstall)

Возможна установка ОС Альт СП в автоматическом режиме. Для этого нужно иметь установочный диск и доступный по сети (по протоколам HTTP или FTP) каталог с несколькими файлами. Настроить FTP-сервер можно, например, в ЦУС (подробнее см. 8.14).

5.5.1. Файлы автоустановки

Файлы автоустановки:

- pkg-groups.tar – архив, содержащий дополнительные к базовой системе группы пакетов;
- vm-profile.scm – различные варианты автоматической разбивки жесткого диска на языке Scheme;
- autoinstall.scm – сценарий автоматической установки на языке Scheme;
- install-scripts.tar – архив, содержащий дополнительные скрипты для preinstall.d и postinstall.d в одноименных каталогах. Скрипты должны быть исполняемыми. Скрипты из архива заменяют одноименные скрипты инсталлятора.

Файлы, описывающие процесс установки, нужно поместить в каталог, доступный по сети по протоколам HTTP или FTP (например, metadata).

5.5.2. Формат файла `vm-profile.scm`

Файл `vm-profile.scm` содержит сценарий, написанный на языке Scheme. Сценарий описывает формат автоматической разбивки жесткого диска.

Пример файла `vm-profile.scm` с одним профилем (`workstation`) разбивки жесткого диска:

```
((workstation
  (title . "Setup for workstation")
  (action . trivial)
  (actiondata  ("swap" (size 2048000 . 2048000) (fsim . "SWAPFS") (methods plain))
               ("/" (size 40960000 . 40960000 ) (fsim . "Ext4") (methods plain))
               ("/home" (size 20480000 . #t ) (fsim . "Ext4") (methods plain))))
```

В примере указана разбивка:

- подкачка (swap) – 1024 Мбайт;

- корневой раздел (/) – 20 Гбайт;

- `/home` – все остальное, но не меньше 10 Гбайт.

Примечание. Все числа в файле `vm-profile.scm` указываются в виде 512-байтных блоков, поэтому чтобы получить размер в байтах, нужно умножить значения на 512.

Примечание. Добавление записи для `/boot/efi` не требуется – установщик добавит ее сам.

Пример файла `vm-profile.scm` с тремя профилями разбивки жесткого диска:

```
((workstation
  (title . "Setup for workstation")
  (action . trivial)
  (actiondata  ("swap" (size 2048000 . 2048000) (fsim . "SWAPFS") (methods plain))
               ("/" (size 40960000 . 40960000 ) (fsim . "Ext4") (methods plain))
               ("/home" (size 20480000 . #t ) (fsim . "Ext4") (methods plain))))
  (workstation_lvm
  (title . "Setup for workstation LVM")
  (action . trivial)
  (actiondata  ("swap" (size 2048000 . 2048000) (fsim . "SWAPFS") (methods lvm))
               ("/" (size 16384000 . #t) (fsim . "Ext4") (methods lvm))))
  (timeshift
  (title . "Timeshift-compatible setup")
  (action . trivial)
  (actiondata  ("swap" (size 2048000 . 2048000) (fsim . "SWAPFS") (methods plain))
               ("" (size 40632320 . #t) (fsim . "BtrFS") (methods plain) (subvols
("@" . "/") ("@home" . "/home")))))
               )
```

В этом примере указаны профили:

- workstation – подкачка (swap), корневой раздел (`/`) и раздел `/home`;

- workstation_lvm – подкачка (swap) и корневой раздел в томе LVM;

- timeshift – подкачка (swap) и раздел BtrFS с разбивкой на подразделы @ и @home.

Имя профиля указывается в файле autoinstall.scm, например:

```
("/evms/profiles/workstation_lvm" action apply commit #f clearall #t exclude ())
```

5.5.3. Формат файла pkg-groups.tar

Файл pkg-groups.tar представляет собой tar-архив с двумя подкаталогами:

- groups – содержит описание групп программного обеспечения в файлах *.directory;
- lists – содержит файлы со списками пакетов для каждой группы и скрытый файл .base, содержащий список пакетов «базовой системы» (то есть те пакеты, которые устанавливаются в любом случае).

Файл pkg-groups.tar проще всего взять из установочного iso-образа из каталога /Metadata/. При нужности файл можно доработать.

Для изменения списка пакетов:

- распаковать архив, например, выполнив команду:

```
$ tar xf pkg-groups.tar
```

- перейти в подкаталог lists и добавить файл группы. Имена пакетов указываются по одному в каждой строке, например:

```
admc
alterator-gpupdate
gpupdate
local-policy
admx-basealt
samba-dc-common
admx-firefox
admx-chromium
gpui
```

- упаковать архив, например, выполнив команду:

```
$ tar cf pkg-groups.tar lists
```

Имя файла используемой группы затем указывается через пробел в autoinstall.scm:

```
(("pkg-install") action "write" lists "group-1 group-2" auto #t)
```

где group-1 и group-2 – имена файлов со списками пакетов из подкаталога lists.

П р и м е ч а н и е . В качестве источника пакетов при установке выступает сам диск, поэтому указание пакетов, которых нет на диске, приведет к сбою установки.

5.5.4. Формат файла `autoinstall.scm`

Файл `autoinstall.scm` представляет собой командный скрипт для программы установки, написанный с использованием языка программирования Scheme. Каждая строка скрипта – команда для модуля программы установки.

Пример файла `autoinstall.scm`:

```
; установка языка операционной системы (ru_RU)
("/sysconfig-base/language" action "write" lang ("ru_RU"))
; установка переключателя раскладки клавиатуры на Ctrl+Shift
("/sysconfig-base/kbd" language ("ru_RU") action "write" layout "ctrl_shift_toggle")
; установка часового пояса в Europe/Moscow, время в BIOS будет храниться в UTC
("/datetime-installer" action "write" commit #t name "RU" zone "Europe/Moscow" utc #t)
; автоматическая разбивка жесткого диска
("/evms/control" action "write" control open installer #t)
("/evms/control" action "write" control update)
("/evms/profiles/workstation" action apply commit #f clearall #t exclude ())
("/evms/control" action "write" control commit)
("/evms/control" action "write" control close)
; перемонтирование
("/remount-destination" action "write")
; установка пакетов операционной системы
("pkg-init" action "write")
; установка только базовой системы (дополнительные группы пакетов из pkg-groups.tar
указываются по именам через пробел)
("/pkg-install" action "write" lists "" auto #t)
("/preinstall" action "write")
; установка загрузчика GRUB в efi с паролем '123'
("/grub" action "write" device "efi" passwd #t passwd_1 "123" passwd_2 "123")
; настройка сетевого интерфейса на получение адреса по DHCP
("/net-eth" action "write" reset #t)
("/net-eth" action "write" name "enp0s3" ipv "4" configuration "dhcp" default ""
search "" dns "" computer_name "newhost" ipv_enabled #t)
("/net-eth" action "write" commit #t)
; установка пароля суперпользователя root '123'
("/root/change_password" passwd_2 "123" passwd_1 "123")
; задание первого пользователя 'user' с паролем '123'
("/users/create_account" new_name "user" gecos "user" allow_su #t auto #f passwd_1
"123" passwd_2 "123" autologin #f)
```

В данном примере будет выполнена установка системы в минимальном профиле (дополнительное ПО в состав устанавливаемых пакетов включаться не будет). Если, например, нужно установить программы, указанные в файле admc, то нужно указать этот файл в списке устанавливаемых пакетов:

```
("/pkg-install" action "write" lists "admc" auto #t)
```

При установке системы в режиме EFI загрузчик устанавливается в специальный раздел efi. Если установка происходит в режиме Legacy, то загрузчик GRUB нужно установить на первый жесткий диск, например:

```
("/grub" action "write" device "/dev/sda" passwd #t passwd_1 "123"
passwd_2 "123")
```

Пример настройки сетевого интерфейса на статический IP-адрес:

```
("/net-eth" action "write" reset #t)
("/net-eth" action "write" name "enp0s3" ipv "4" configuration
"static" default "192.168.0.1" search "" dns "8.8.8.8" computer_name
"newhost" ipv_enabled #t)
("/net-eth" action "add_iface_address" name "enp0s3" addip
"192.168.0.25" addmask "24" ipv "4")
("/net-eth" action "write" commit #t)
```

где:

- 192.168.0.25 – IP-адрес;
- 192.168.0.1 – шлюз по умолчанию;
- 8.8.8.8 – DNS-сервер;
- newhost – имя хоста.

В конец файла `autoinstall.scm` можно добавить шаг `/postinstall`, который позволяет в конце установки или при первом запуске ОС выполнить команду или скрипт. Например:

```
("/postinstall/firsttime" script "ftp://192.168.0.123/metadata/update.sh")
```

У шага `/postinstall` есть два уровня запуска:

- laststate – скрипт запускается при завершении альтератора (перед перезагрузкой после установки);
- firsttime – скрипт запускается во время первого запуска ОС.

И два метода (method) указания скрипта запуска:

- script – скрипт загружается с сервера и выполняется;
- run – выполняется заданная команда или набор команд (возможно указание перенаправления).

Примеры:

```
("/postinstall/firsttime" script "http://server/script.sh")
("/postinstall/firsttime" run "curl --silent --insecure
http://server/finish")
```

("/postinstall/laststate" script "http://server/script.sh")
("/postinstall/laststate" run "curl --silent --insecure http://server/gotoreboot") два метода (method)

Примечание. На уровне laststate для работы с установленной системой требуется указывать пути с $destdir или выполнять команды через run_chroot:

```
#!/bin/sh

a= . install2-init-functions

run_chroot sh -c "date > /root/STAMP_1"
date > $destdir/root/STAMP_2
```

5.5.5. Формат файла install-scripts.tar

Файл install-scripts.tar представляет собой tar-архив, содержащий дополнительные скрипты.

Скрипты preinstall.d выполняются сразу после установки базовой системы. Как правило, это скрипты для дополнительной настройки базовой системы (перед установкой дополнительного набора ПО) и для переноса настроек из среды инсталлятора. Добавлять сюда свои собственные скрипты стоит только тогда, когда цели четко определены. Скрипты postinstall.d выполняются сразу после последнего шага инсталлятора. Как правило, это скрипты, удаляющие служебные пакеты инсталлятора из базовой системы. Если нужно сделать какие-нибудь специфические настройки системы, то это можно сделать здесь.

Скрипты preinstall.d нужно поместить в каталог preinstall.d, скрипты postinstall.d – в каталог postinstall.d. Упаковать архив можно, выполнив команду:

```
$ tar cf install-scripts.tar preinstall.d postinstall.d
```

Примечание. Данные скрипты выполняются в среде установщика, а не в среде установленной системы. Для работы с установленной системой требуется указывать пути с $destdir или выполнять команды через run_chroot:

```
#!/bin/sh

a= . install2-init-functions

run_chroot sh -c "date > /root/STAMP_1"
date > $destdir/root/STAMP_2
```

5.5.6. Запуск автоматической установки

Для включения режима автоматической установки ядру инсталлятора ОС нужно передать параметр загрузки `ai` (без значения) и параметр `curl` с указанием каталога с установочными файлами. Формат адреса в `curl` должен быть представлен в виде URL. Пример параметров загрузки:

```
ai curl=ftp://<IP-адрес>/metadata/
```

Чтобы начать процесс автоматической установки ОС нужно загрузиться с носителя, на котором записан дистрибутив. Затем клавишами перемещения курсора <↑>, <↓> выбрать пункт меню «Установить ALT SP Workstation…» и нажать клавишу <E>. В открывшемся редакторе следует найти строку, начинающуюся с `linux /boot/vmlinuz`, в ее конец дописать требуемые параметры (рис. 37). После нажатия клавиши <F10> начнется автоматическая установка системы.

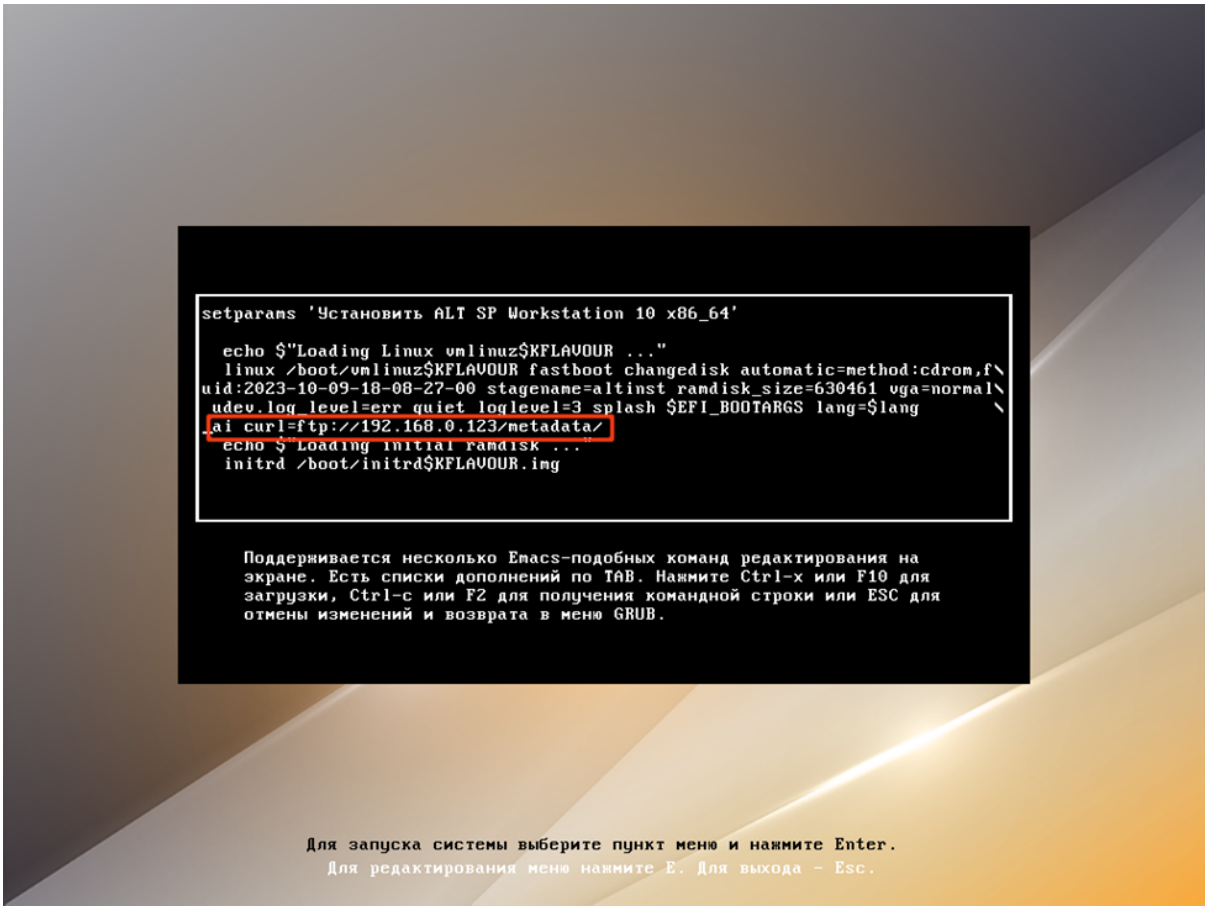


Рис. 37 – Включение режима автоматической установки

Будет запущена автоматическая установка системы.

При невозможности получения файлов из указанного источника по сети, программа установки будет смотреть в следующих местах:

- на диске в каталоге `/Metadata/`;

- в образе установщика в каталоге `/usr/share/install2/metadata/`.

5.6. Обновление системы до актуального состояния

После установки системы лучше сразу обновиться до актуального состояния. Можно не обновлять систему и сразу приступать к работе только в том случае, если не планируется подключение к сети или Интернету и нет нужности устанавливать дополнительные программы.

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

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

П р и м е ч а н и е . Получить права администратора (см. также п. 20.2) можно, выполнив в терминале команду:

```
$ su -
```

или зарегистрировавшись в системе (например, на второй консоли – нажать клавиши <Ctrl>+<Alt>+<F2>) под именем root.

Подробнее про обновление пакетов можно прочитать в п. 17.8, п. 17.9 и п. 17.10 «Обновление ядра».

5.7. Установка графической оболочки на ОС Альт СП Сервер

Стандартная установка варианта исполнения ОС Альт СП Сервер включает базовую систему, работающую в консольном режиме. Для установки графической оболочки, и переключения в графический режим работы следует выполнить следующие команды:

```
# apt-get update
# apt-get install mate-default lightdm-gtk-greeter fonts-ttf-dejavu
# systemctl enable lightdm
# systemctl set-default graphical.target
# reboot
```

После выполнения установки будет выведено сообщение о нарушении целостности. Для восстановления целостности системы, если система контроля целостности IMA/EVM не инициализирована, выполнить команду:

```
# integalert fix
```

5.8. Проблемы при установке системы

Если в системе не произошла настройка какого-либо компонента после стадии установки пакетов, доведите установку до конца, загрузитесь в систему и попытайтесь повторить настройку.

В случае возникновения проблем с установкой, можно вручную задать параметры в строке «Параметры загрузки» (см. рис. 4) меню начального загрузчика:

- xdriver – графический установщик предпринимает попытку автоматического подбора драйвера видеокарты, но иногда это ему не удается. Данным параметром можно явно указать нужный вариант драйвера.

6. НАЧАЛО ИСПОЛЬЗОВАНИЯ ОС АЛЬТ СП

6.1. Запуск ОС

Запуск ОС Альт СП выполняется автоматически после запуска компьютера и отработки набора программ BIOS (БСВВ).

На экране появляется меню, в котором перечислены возможные варианты загрузки ОС (рис. 38, рис. 39).

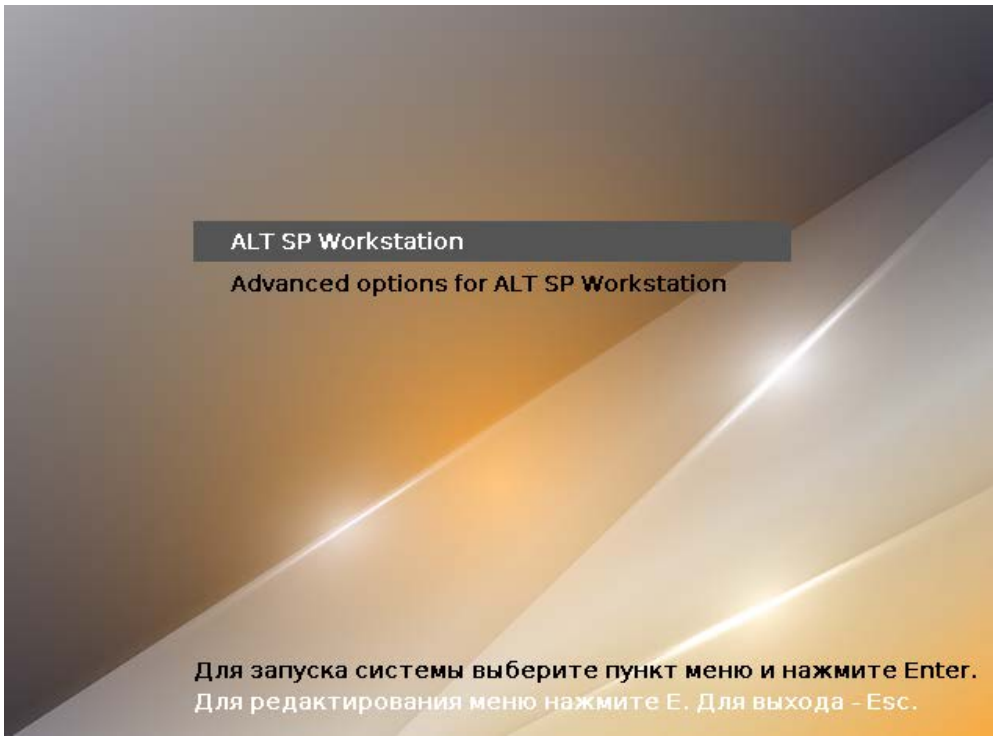


Рис. 38 – Варианты загрузки. Рабочая станция

Рис. 39 – Варианты загрузки. Сервер

По умолчанию, если не были нажаты управляющие клавиши на клавиатуре, загрузка ОС Альт СП продолжится автоматически.

Для выбора дополнительных параметров загрузки нужно выбрать пункт «Дополнительные параметры для ALT SP …» (Advanced options for ALT SP…).

Примечание. Если при установке системы был установлен пароль на загрузчик потребуется ввести имя пользователя «boot» и заданный на шаге «Установка загрузчика» пароль (рис. 40).

Рис. 40 – Пример части окна ввода пароля на загрузчик

Откроется окно с возможностью выбора способа дальнейшей загрузки ОС, например, (рис. 41, рис. 42):

- «ALT SP Workstation 11100-01, vmlinuz»;
- «ALT SP Workstation 11100-01, vmlinuz (recovery mode)»;
- «ALT SP Workstation 11100-01, *».

* – зависит от актуального дистрибутива.

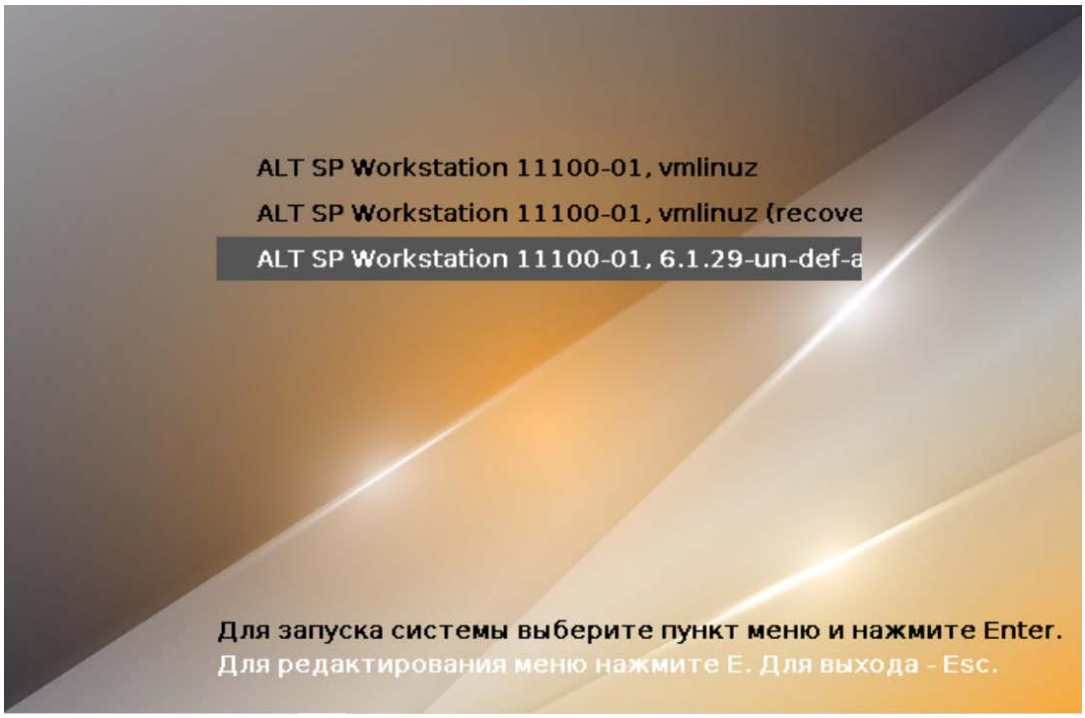


Рис. 41 – Пример окна дополнительные параметры

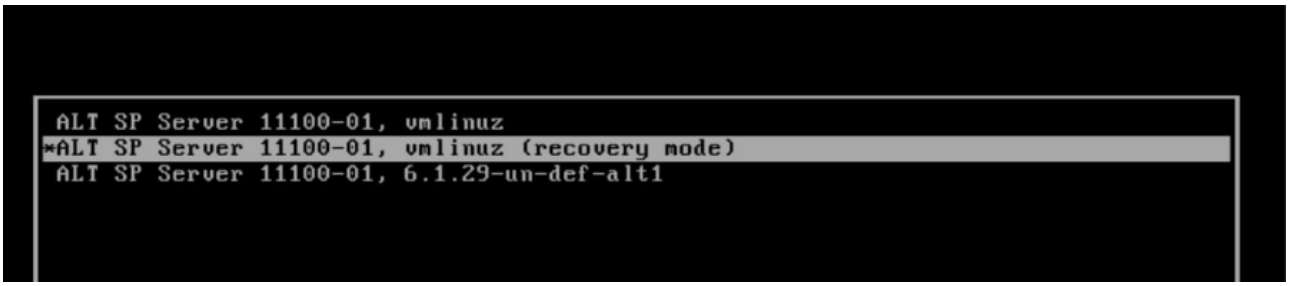


Рис. 42 – Пример окна дополнительные параметры. Сервер

Окно с перечнем дополнительных настроек загрузки (рис. 43) вызывается нажатием клавиши <E>.

П р и м е ч а н и е . Если при установке системы был установлен пароль на загрузчик, то потребуется ввести имя пользователя «boot» и заданный на шаге «Установка загрузчика» пароль (см. рис. 40).

П р и м е ч а н и е . Дополнительные опции загрузчика могут быть добавлены:

- в файле `/etc/sysconfig/grub2` в строке `GRUB_CMDLINE_LINUX_DEFAULT=…`, после следует обновить настройки загрузчика – выполнить команду:
  `# update-grub`

также следует перезагрузить ОС.

В процессе загрузки ОС Альт СП пользователь может следить за информацией процесса загрузки, которая отображает этапы запуска различных служб и программных серверов в виде отдельных строк (рис. 44) на экране монитора.

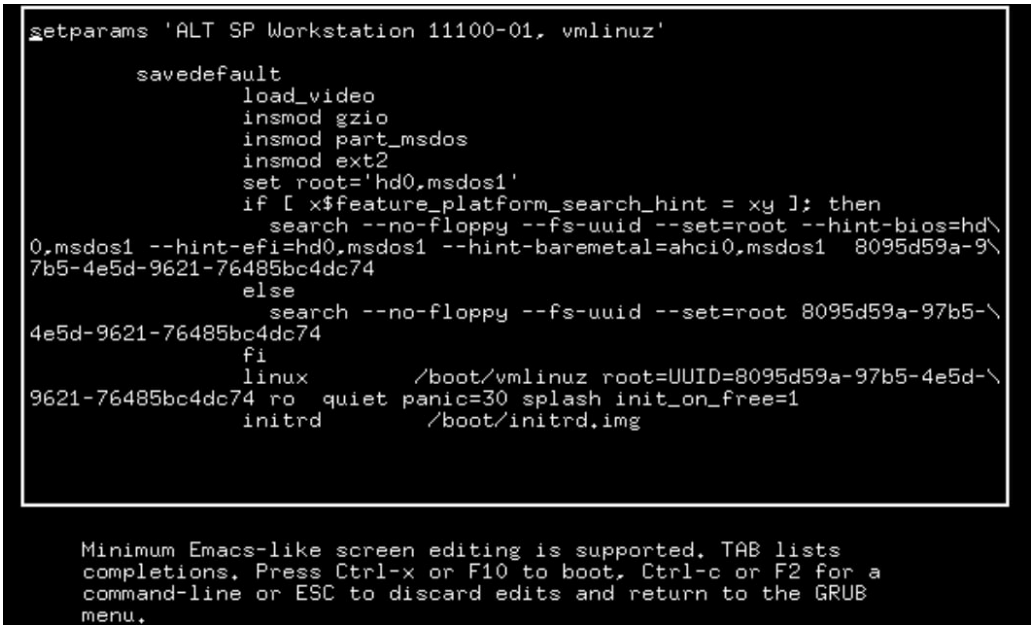


Рис. 43 – Пример окна с перечнем дополнительных настроек загрузчика GRUB

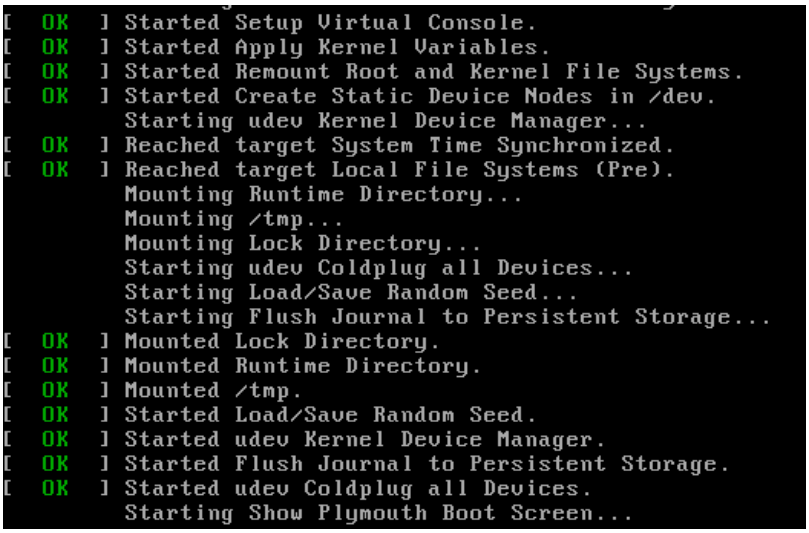


Рис. 44 – Загрузка ОС

При этом каждая строка начинается словом вида [XXXXXXX] (`OK` или `FAILED`), являющегося признаком нормального или ненормального завершения этапа загрузки. Слово `XXXXXXX=FAILED` (авария) свидетельствует о неуспешном завершении этапа загрузки, что требует вмешательства и специальных действий администратора системы.

6.2. Получение доступа к шифруемым разделам

В случае, если был создан шифруемый раздел (см. п. 5.4.4.4.3), потребуется вводить пароль при обращении к этому разделу (рис. 45).

Рис. 45 – Пример запрос пароля для доступа к шифруемым разделам

Если не ввести пароль за отведенный промежуток времени, то загрузка системы завершится ошибкой. В этом случае следует перезагрузить систему, нажав для этого два раза <Enter>, а затем клавиши <Ctrl>+<Alt>+<Delete>.

6.3. Вход в систему

6.3.1. Идентификация и аутентификация в графической оболочке MATE

В состав ОС может входить графическая оболочка MATE. Оболочка состоит из набора различных программ и технологий, используемых для управления ОС и предоставляющих пользователю графический интерфейс для работы в виде оконных менеджеров.

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

Для продолжения работы и входа в ОС Альт СП в графическом режиме нужно выбрать одну из учетных записей, предлагаемых в окне аутентификации. Далее ввести пароль текущей учетной записи и нажать на кнопку «Войти» (рис. 46).

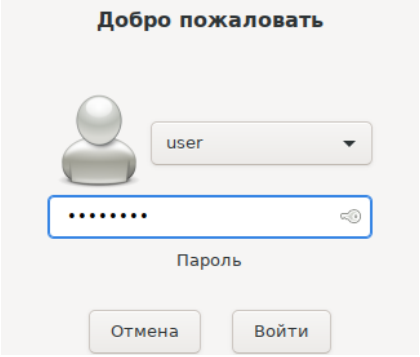


Рис. 46 – Ввод аутентификационных данных в графической оболочке

Для выбора учетной записи, не показанной в списке выбора, нужно раскрыть выпадающий список со значением логина текущей учетной записи и выбрать пункт «Другие…» (рис. 47).

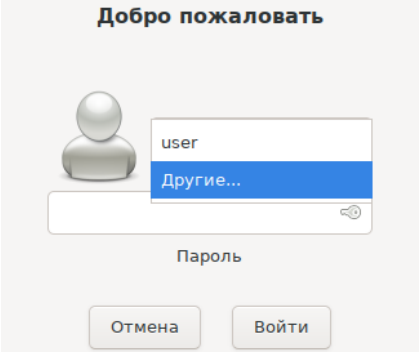


Рис. 47 – Выбор пользователя

После этого откроется окно ввода логина учетной записи (рис. 48), в котором нужно ввести логин учетной записи, и нажать на кнопку «Войти». В следующем окне нужно ввести пароль учетной записи, и нажать на кнопку «Войти» (рис. 47).

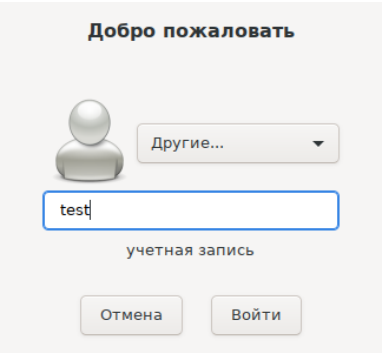


Рис. 48 – Ввод имени учетной записи

В результате успешного прохождения процедуры аутентификации и входа в систему запустится графическая оболочка ОС Альт СП (рис. 49).

Примечание. Работа в системе с использованием учетной записи администратора небезопасна, вследствие этого вход в систему в графическом режиме для администратора (root) запрещен. Попытка зарегистрироваться в системе будет прервана сообщением об ошибке.

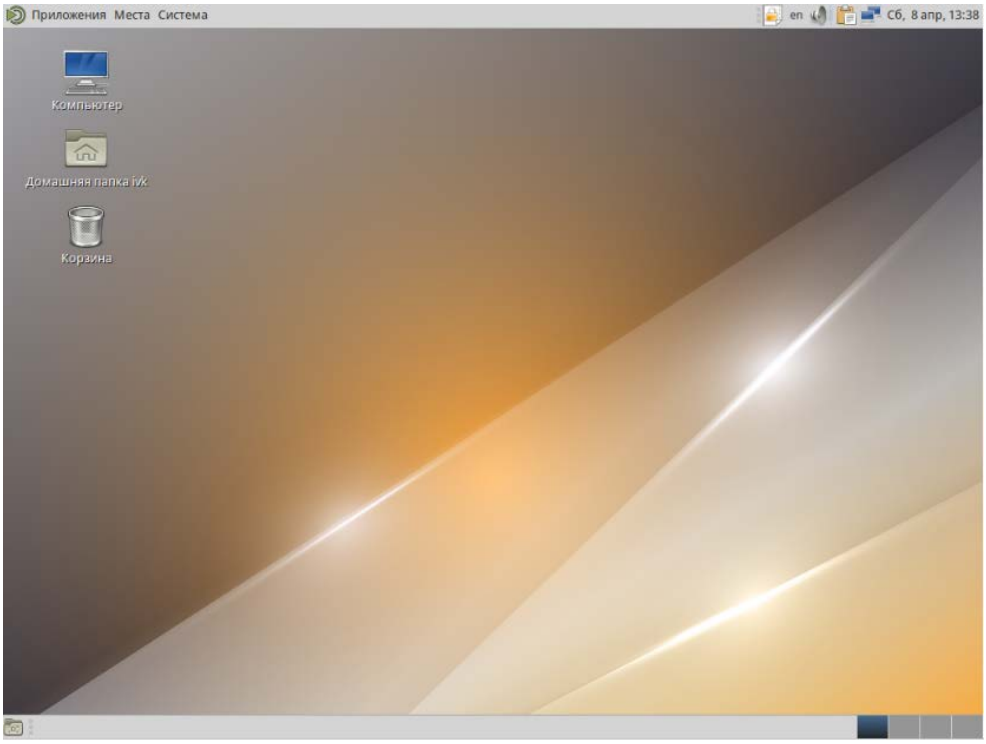


Рис. 49 – Пример графического интерфейса ОС

В случае, если графическая оболочка MATE была включена в состав ОС при установке, однако не стартовала автоматически, ее допускается вызвать вручную из консоли с помощью следующих команд:

```
~/.xinitrc
exec mate-session
```

Далее нужно использовать команду `startx` для запуска MATE.

Подробнее о приложениях для ОС Альт СП Рабочая станция и рабочем столе MATE приведено в документе «Руководство пользователя. ЛКНВ.11100-01 91 03».

6.3.2. Идентификация и аутентификация в консольном режиме

При загрузке в консольном режиме работа загрузчика завершается запросом на ввод логина и пароля учетной записи. В случае нужности перехода на другую консоль нажмите клавиши <Ctrl>+<Alt>+<F2>.

Для продолжения работы в консольном режиме нужно ввести логин учетной записи пользователя и подтвердить его нажатием клавиши <Enter>. Затем ввести пароль и подтвердить его аналогичным образом.

В случае успешного прохождения процедуры аутентификации и входа в систему ОС перейдет к штатному режиму работы и предоставит дальнейший доступ к консоли (рис. 50).

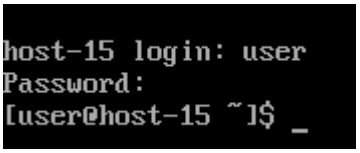


Рис. 50 – Аутентификация пользователя

6.3.3. Виртуальная консоль

В процессе работы ОС Альт СП 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>.

На первых шести виртуальных консолях (от <Ctrl>+<Alt>+<F1> до <Ctrl>+<Alt>+<F6>) пользователь может зарегистрироваться и работать в текстовом режиме. Если была установлена графическая оболочка MATE, она будет загружаться в первой виртуальной консоли. Двенадцатая виртуальная консоль (<Ctrl>+<Alt>+<F12>) выполняет функцию системной консоли – на нее выводятся сообщения о происходящих в системе событиях.

6.4. Блокирование сеанса доступа

6.4.1. Блокирование сеанса доступа после установленного времени бездействия (неактивности) пользователя или по его запросу

После авторизации и загрузки графической рабочей среды MATE, пользователю предоставляется рабочий стол для работы с графическими приложениями.

Для безопасности данных компьютера и, чтобы другие пользователи не могли получить доступ к работающим приложениям, блокируйте свой экран, даже если оставляете компьютер на короткое время.

Заблокировать сеанс доступа можно по запросу пользователя: панель инструментов MATE «Меню» → «Система» → «Заблокировать экран», или вызвать клавишами <Ctrl>+<Alt>+<L>.

Также при работе в графическом режиме блокирование сеанса доступа после установленного времени бездействия происходит посредством срабатывания программы – хранителя экрана (screensaver).

Время бездействия системы устанавливается: панель инструментов MATE «Меню» → «Система» → «Параметры» → «Оформление» → «Хранитель экрана».

Для разблокировки требуется ввести пароль пользователя и нажать на кнопку «Разблокировать».

При заблокированном экране другие пользователи могут входить в систему под своими учетными записями, нажав на экране ввода пароля кнопку «Переключить пользователя».

6.4.2. Блокировка виртуальных текстовых консолей

Программа vlock позволяет заблокировать сеанс при работе в консоли.

Выполнение команды `vlock` без дополнительных параметров заблокирует текущий сеанс виртуальной консоли, без прерывания доступа других пользователей:

```
$ vlock
Блокировка tty2 установлена user.
Используйте Alt-функциональные клавиши для перехода в другие виртуальные консоли.
Пароль:
```

Чтобы предотвратить доступ ко всем виртуальным консолям машины, следует выполнить команду:

```
$ vlock -a
Теперь вывод на консоль полностью заблокирован user.
Пароль:
```

П р и м е ч а н и е . Для разблокировки консоли введите пароль пользователя.

В этом случае `vlock` блокирует текущую активную консоль, а параметр `-a` предотвращает переключение в другие виртуальные консоли.

6.4.3. Настройка блокировки возможности пользователя изменять настройки блокировки системы

Для блокировки возможности пользователя изменять настройки блокировки системы нужно выполнить следующие действия:

1) создать файл `/etc/dconf/profile/user` со следующим содержимым:

```
user-db:user
system-db:local
```

2) создать каталоги `/etc/dconf/db/local.d/` и `/etc/dconf/db/local.d/locks`:

```
# mkdir /etc/dconf/db/local.d/
# mkdir /etc/dconf/db/local.d/locks
```

3) создать файл `/etc/dconf/db/local.d/screensaver`, в который поместить текст:

```
[org/mate/screensaver]
idle-activation-enabled=true
lock-enabled=true
```

4) в файле `/etc/dconf/db/local.d/session` установить время бездействия в минутах:

```
[org/mate/session]
idle-delay=2
```

5) запретить пользователям изменять заставку, для этого создать файл `/etc/dconf/db/local.d/locks/00-screensaver` со следующим содержимым:

```
#prevent users from changing screensaver
/org/mate/screensaver/idle-activation-enabled
/org/mate/screensaver/lock-enabled
/org/mate/desktop/session/idle-delay
```

6) выполнить обновление:

```
# dconf update
```

6.5. Завершение работы ОС

Для корректного завершения работы ОС (перезагрузки) во время ее работы запрещается выключать питание компьютера или перезагружать компьютер нажатием на кнопку «Reset», так как для корректного завершения работы требуется размонтирование файловой системы.

Перед окончанием работы с ОС нужно завершить все работающие программы.

6.5.1. Графический режим

Для завершения сеанса пользователя в графическом режиме выбрать на панели инструментов MATE «Меню» → «Система» → «Завершить сеанс пользователя».

Далее откроется окно, в котором предоставляется выбор дальнейших действий:

- переключить пользователя – сеанс пользователя в графическом режиме блокируется, другой пользователь может войти в систему под своим именем;
- завершить сеанс – выполняется завершение сеанса пользователя в графическом режиме.

Если не производить никаких действий, то сеанс пользователя будет автоматически завершен через 1 минуту.

Также можно воспользоваться комбинацией клавиш <Ctrl>+<Alt>+<Del>, что на рабочей станции приведет к вызову диалога завершения работы системы.

6.5.2. Консольный режим

Завершить сеанс пользователя в консольном режиме можно, выполнив команду `exit`.

6.5.3. Настройки завершения сеанса пользователя

Для каждого пользователя можно настроить автоматическое завершение сеанса, после установленного времени бездействия (неактивности) пользователя.

Для этого нужно создать файл `/etc/logout`, в который поместить допустимое время простоя для каждого пользователя, например:

```
user1 300
user2 200
```

Формат файла `/etc/logout`:

```
<user> <время в секундах от момента последнего действия>
```

П р и м е ч а н и е . Перезагрузите ОС для применения настроек.

6.6. Выключение/перезагрузка компьютера

6.6.1. Графический режим

Для выключения/перезагрузки компьютера следует выбрать на панели инструментов MATE «Меню» → «Система» → «Завершить работу».

Далее откроется окно, в котором предоставляется выбор дальнейших действий:

- ждущий режим – компьютер переводится в режим экономии энергии;
- спящий режим – компьютер переводится в режим энергосбережения, позволяющий отключить питание компьютера, сохранив при этом текущее состояние ОС;
- перезагрузить – выполняется перезапуск ОС;
- выключить – выполняется выключение компьютера.

Если не производить никаких действий, то компьютер будет автоматически выключен через 1 минуту.

Также можно воспользоваться комбинацией клавиш <Ctrl>+<Alt>+<Del>, что на сервере – к перезагрузке системы, при этом нужно дождаться появления на экране сообщения «Reboot» (перезагрузка) и выключить питание системы.

6.6.2. Консольный режим

Перезагрузить систему в консольном режиме можно, выполнив команду:

```
$ systemctl reboot
```

Завершить работу и выключить компьютер (с отключением питания):

```
$ systemctl poweroff
```

Перевести систему в ждущий режим:

```
$ systemctl suspend
```

6.7. Утилита уничтожения информации при удалении – dm-secdel

Операции удаления обычно ограничиваются пометкой блоков данных как «неиспользуемых» в файловой системе. Утилита dm-secdel, так же помечает блоки как не используемые, но заменяет очищение, записью случайных данных в освобождаемые блоки. Таким образом, данные удаляются надежно.

В силу своего абстрактного характера dm-secdel поддерживает множество файловых систем, которые поддерживают опцию `discard` (например, ext3, ext4, xfs, btrfs).

⚠ Следует создать сопоставленное устройство с помощью инструмента secdelsetup. Убедиться, что файловая система (ФС) смонтирована на это, а не основное устройство. Убедиться, что ФС установлена с опцией `-o discard`.

Проверить, смонтирована ли ФС в данный момент с этой опцией, можно посмотрев вывод команды `mount`:

```
/dev/sdd1 on / type ext4 (rw,discard,errors=remount-ro)
```

Не следует включать ведение журнала данных. Обратите внимание, что при удалении файлов командой `rm` удаление будет выполняться асинхронно, поэтому чтобы убедиться, что данные уже удалены следует использовать команду `sync` или опцию монтирования файловой системы `-o sync` до использования команды `rm`.

Если нужно, чтобы имена файлов также были уничтожены, во-первых, следует убедиться, что файловая система создана полностью без ведения журнала (например, `mkfs.ext4 -O ^has_journal`), а во-вторых, удалите сам каталог, тогда его блоки освободятся и будут стерты.

При использовании команды `fstrim` все свободные блоки файловой системы будут отброшены (`discarded`) и, следовательно, также стерты (файловая система должна быть примонтирована с опцией `-o discard`).

Применение:

`secdelsetup <источник-устройство> [маппинг]`

Опции:

1) `-d|--detach <устройство>` – отсоединить устройство;

2) `-D|--detach-all|--stop` – отключить все устройства;

3) `-l|--list` – список активных карт устройства;

4) `-a|--all` – список в другом формате;

5) `--lsblk` – вывод в формате lsblk;

6) `--start` – запускать устройства из secdeltab;

7) `--save` – сохранение активных устройств в secdeltab.

Пример: пусть `/home` находится на устройстве `/dev/sda5`, закомментировать строку с разделом `/home` в файле `/etc/fstab` и выполнить перезагрузку системы.

Проверить наличие журналирования на устройстве, выполнить команду:

```
dumpe2fs /dev/sda5 | grep has_journal
```

Если параметры журналирования найдены, отключить их с помощью команды:

```
tune2fs -O ^has_journal /dev/sda5
```

Создадим для `/dev/sda5` сопоставленное устройство (карта) (по умолчанию задается один проход со случайными битами):

```
# secdelsetup /dev/sda5
```

Пример ожидаемого вывода команды:

```
/dev/mapper/secdel0 is attached to /dev/sda5
```

где `/dev/mapper/secdel0` имя созданного сопоставленного устройства.

В файл /etc/fstab добавить новую строку, указывающую на точку монтирования /home:

```
/dev/mapper/secdel0 /home ext4 noexec,nosuid,relatime,discard 1 2
```

Затем /dev/mapper/secdel0 должно быть смонтировано с параметром -o discard, выполнить команду:

```
# mount /dev/mapper/secdel0 /mnt/test/ -o discard
```

Команда просмотра текущих (существующих) карт:

```
# secdelsetup –all
/dev/mapper/secdel0 /dev/sda5
```

Для хранения конфигурации карт используется файл /etc/secdeltab, который будет автоматически активирован после перезагрузки (системной службой secdeltab.service). Для сохранения текущих карт в файл выполнить команду:

```
# secdelsetup --save
```

Для изменения перезаписи, например, с тремя проходами (первый проход – 1, второй проход случайные биты – R, третий проход – 0) выполнить команду:

```
# secdelsetup /dev/sda5 /dev/mapper/secdel0 1R0
```

Команда отсоединения всех активных карт:

```
# secdelsetup --detach-all
```

Пример ожидаемого вывода команды:

```
detach /dev/mapper/secdel0
```

7. НАСТРОЙКИ СИСТЕМЫ

7.1. Центр управления системой

Для управления настройками установленной системы можно использовать ЦУС (также см. применение ЦУС в документе «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03»).

ЦУС состоит из нескольких независимых диалогов-модулей. Каждый модуль отвечает за настройку определенной функции или свойства системы. Модули настройки сгруппированы по задачам.

Список установленных модулей можно просмотреть, выполнив команду от администратора:

```
# alterator-standalone
```

ЦУС можно использовать для разных целей, например (в скобках указаны имена соответствующих модулей):

- просмотр системных журналов (logs) (п. 8.17.1);
- управление системными службами (services) (п. 8.17.2);
- конфигурирование сетевых интерфейсов (net-eth) (п. 8.5.1);
- настройка межсетевого экрана (net-iptables) (п. 8.15.1);
- настройка ограничений на использование внешних носителей (ports-access, доступно только в веб-интерфейсе) (п. 7.4.4);
- создание, удаление и редактирование учетных записей пользователей (users) (п. 8.17.5);
- изменения пароля администратора системы (root) (п. 8.17.6);
- настройка даты и времени (datetime) (п. 8.17.7);
- настройка ограничений выделяемых ресурсов памяти пользователям (квоты) (quota п. 8.17.8);
- конфигурирование групповых политик (gpupdate) (п. 9.1.3);
- управление выключением удаленного компьютера (ahttpd-power, доступно только в веб-интерфейсе).

Примечание. Соответствующие наименования пакетов ЦУС `alterator-<имя_модуля>`, например, `alterator-net-eth`.

Чтобы исключить возможность несанкционированного доступа к ЦУС по окончанию работы, нужно завершить сеанс, нажав на кнопку «Выход».

7.1.1. Графический интерфейс

Графический интерфейс ЦУС можно запустить следующими способами:

- комбинацией клавиш <ALT>+<F2> открыть окно быстрого запуска приложений и ввести в поле название программы – acc;
- выбрать на панели инструментов MATE «Меню» → «Система» → «Администрирование» → «Центр управления системой»;
- при помощи консоли (приложение «Терминал среды MATE»), в которой нужно ввести команду acc;
- зная имя модуля, запустить графический интерфейс для него, можно также выполнив команду:

```
$ alterator-standalone <имя-модуля>
```

Запуск ЦУС требует прав администратора – введите пароль root (рис. 51).

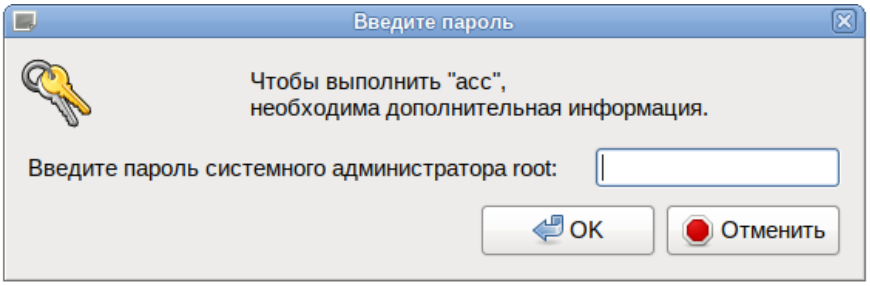


Рис. 51 – Запрос пароля для запуска «Центра управления системой»

После успешного входа откроется окно ЦУС (рис. 52).

Кнопка «Режим эксперта» (рис. 52) 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.

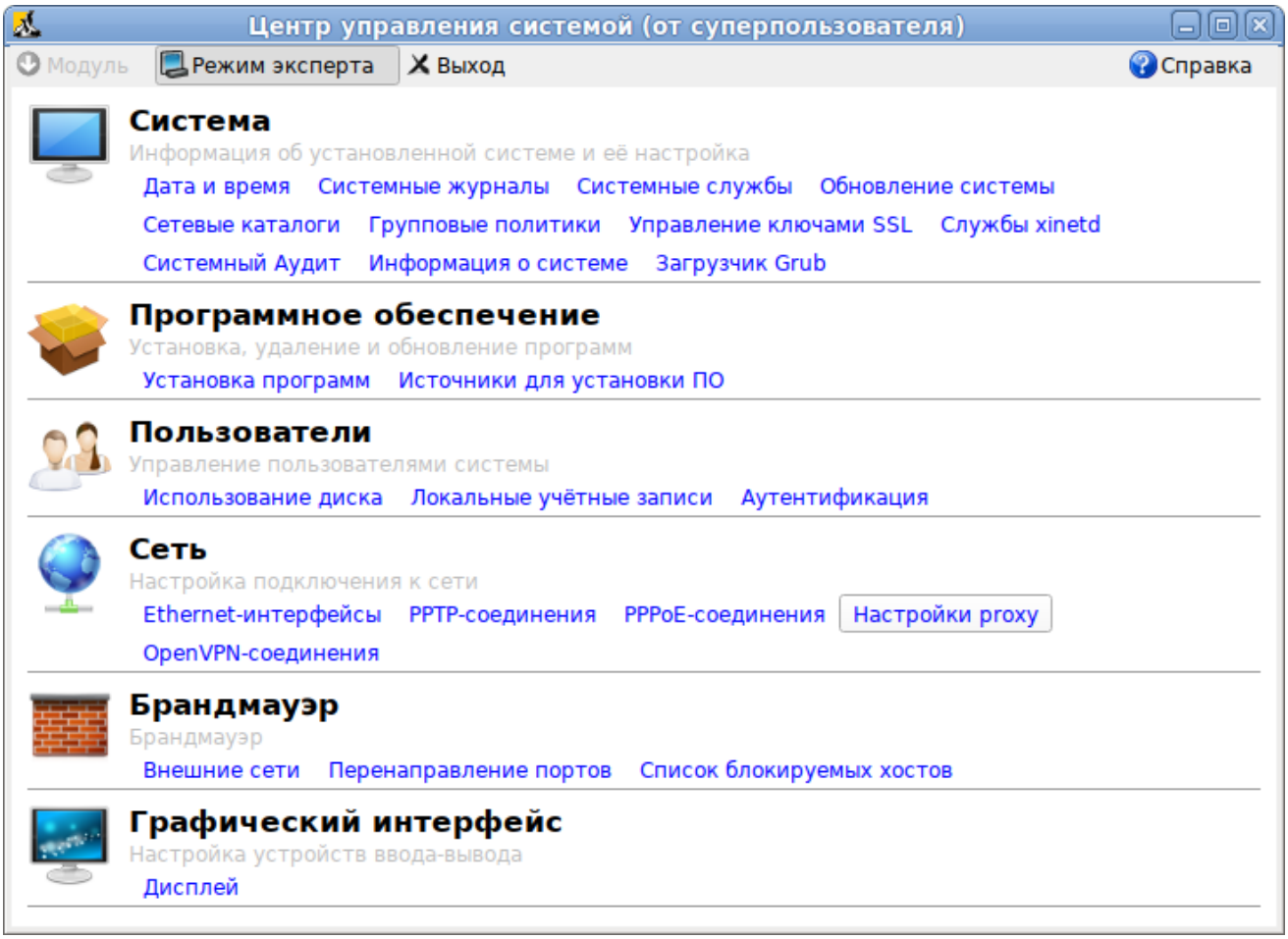


Рис. 52 – Окно «Центр управления системой»

7.1.2. Веб-интерфейс ЦУС

ЦУС имеет веб-ориентированный интерфейс, позволяющий управлять системой с любого компьютера сети.

Для запуска веб-ориентированного интерфейса, должен быть установлен пакет alterator-fbi:

```
# apt-get install alterator-fbi
```

Должен быть запущен сервис ahttpd и alteratord:

```
systemctl enable ahttpd
systemctl start ahttpd
systemctl enable alteratord
systemctl start alteratord
```

Работа с ЦУС может происходить из любого веб-браузера. Для начала работы нужно перейти по адресу `https://localhost:8080/` или `https://IP-адрес:8080/`.

IP-адрес можно узнать, выполнив команду:

```
$ ip addr
```

П р и м е ч а н и е . IP-адрес будет указан после слова inet:

```
inet 192.168.88.211/24 brd 192.168.0.255 scope global eth0
```

Где `192.168.88.211` – IP-адрес.

Для начала работы с ЦУС нужно зарегистрироваться. Запуск ЦУС требует прав администратора (ввести пароль root) (рис. 53). Дополнительно на этапе регистрации можно выбрать язык интерфейса. По умолчанию предлагается язык, определенный настройками веб-браузера.

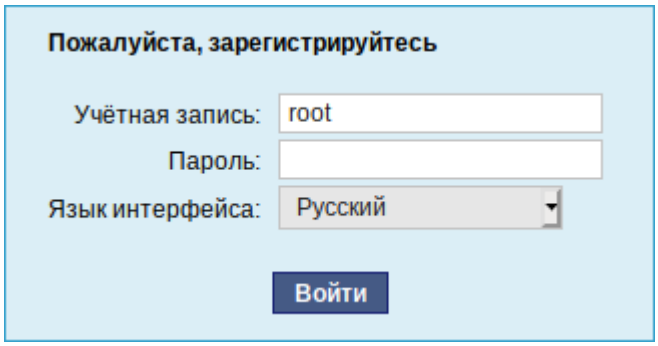


Рис. 53 – Запрос пароля администратора для запуска веб-интерфейса ЦУС

После успешного входа откроется окно «Центра управления системой» (рис. 54).

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.

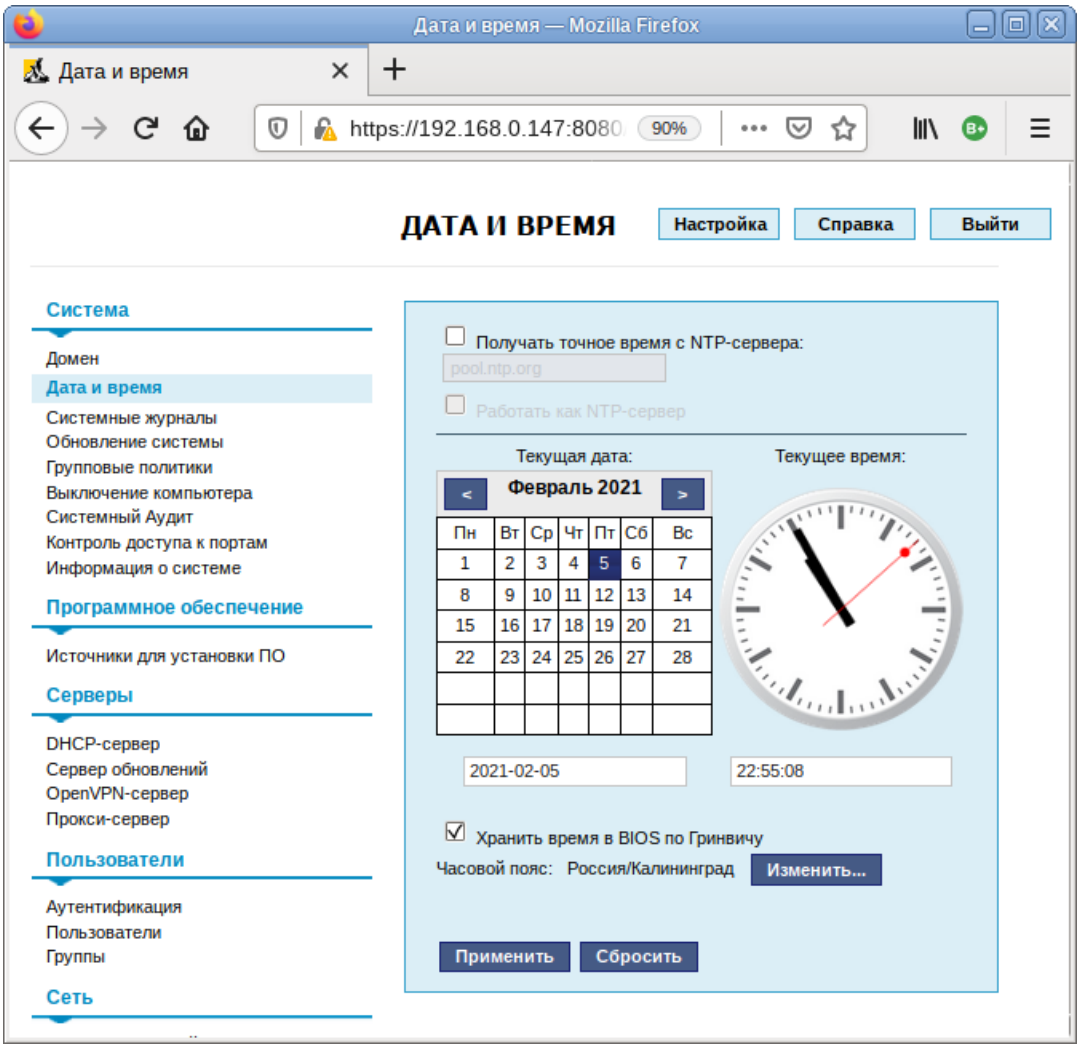


Рис. 54 – Окно веб-интерфейса «Центр управления системой»

ЦУС содержит справочную информацию по модулю, которую можно прочитать, нажав на кнопку «Справка» (см. п. 7.1.5).

⚠ После работы с ЦУС, в целях безопасности, не оставляйте открытым веб-браузер. Обязательно закройте веб-интерфейс – нажать на кнопку «Выйти».

7.1.3. Установка и удаление модулей ЦУС

Состав модулей, предоставляющих различные возможности для настройки системы в веб-интерфейсе, можно изменять.

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

```
# rpm -qa | grep alterator
```

Для поиска прочих пакетов ЦУС выполните 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
```

7.1.4. Права доступа к модулям ЦУС

Администратор 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 нужно выбрать нужный модуль и нажать ссылку «Параметры доступа к модулю», расположенную в нижней части окна модуля (рис. 55).

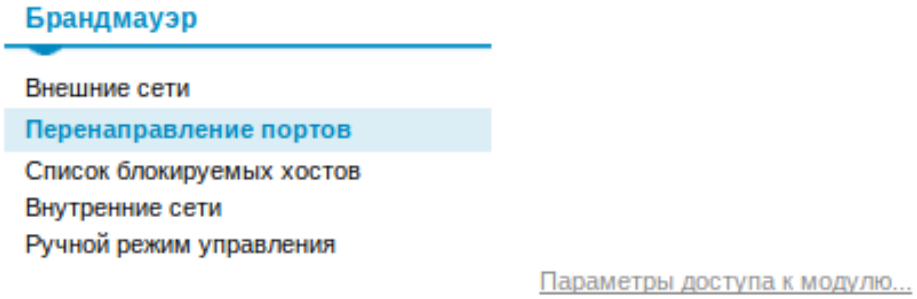


Рис. 55 – Ссылка «Параметры доступа к модулю»

В открывшемся окне, в списке «Новый пользователь» нужно выбрать пользователя, который получит доступ к данному модулю, и нажать на кнопку «Добавить». Для сохранения настроек нужно перезапустить HTTP-сервер, для этого достаточно нажать на кнопку «Перезапустить HTTP-сервер» (рис. 56).

Для удаления доступа пользователя к определенному модулю, администратору, в окне этого модуля нужно нажать ссылку «Параметры доступа к модулю», в открывшемся окне в списке пользователей, которым разрешен доступ, выбрать пользователя, нажать на кнопку «Удалить» (рис. 56) и нажать на кнопку «Перезапустить HTTP-сервер».

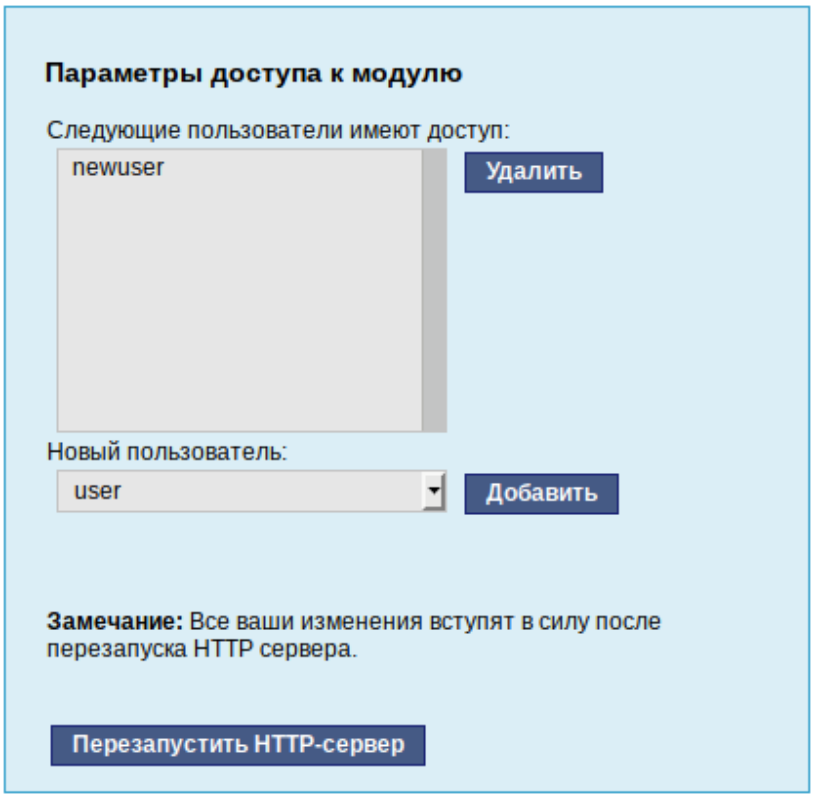


Рис. 56 – Параметры доступа к модулю

Системный пользователь, пройдя процедуру аутентификации (рис. 57), может просматривать и вызывать модули, к которым он имеет доступ (рис. 58).

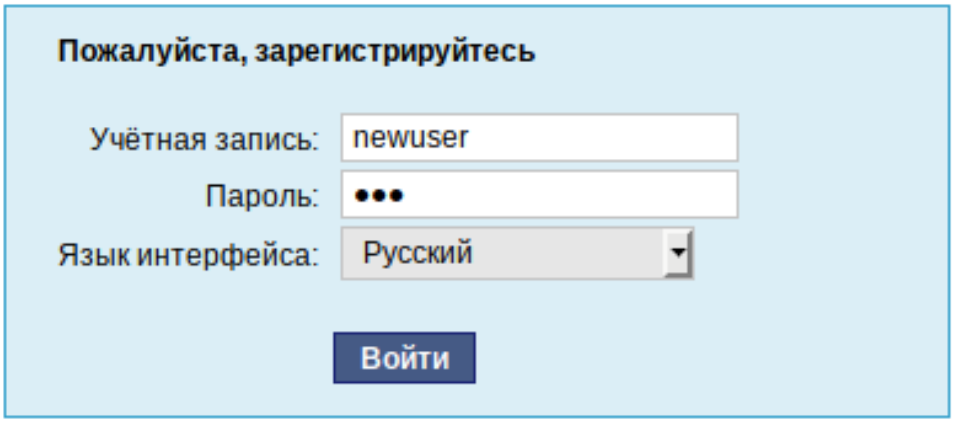


Рис. 57 – Запрос пароля учетной записи пользователя для запуска веб-интерфейса ЦУС

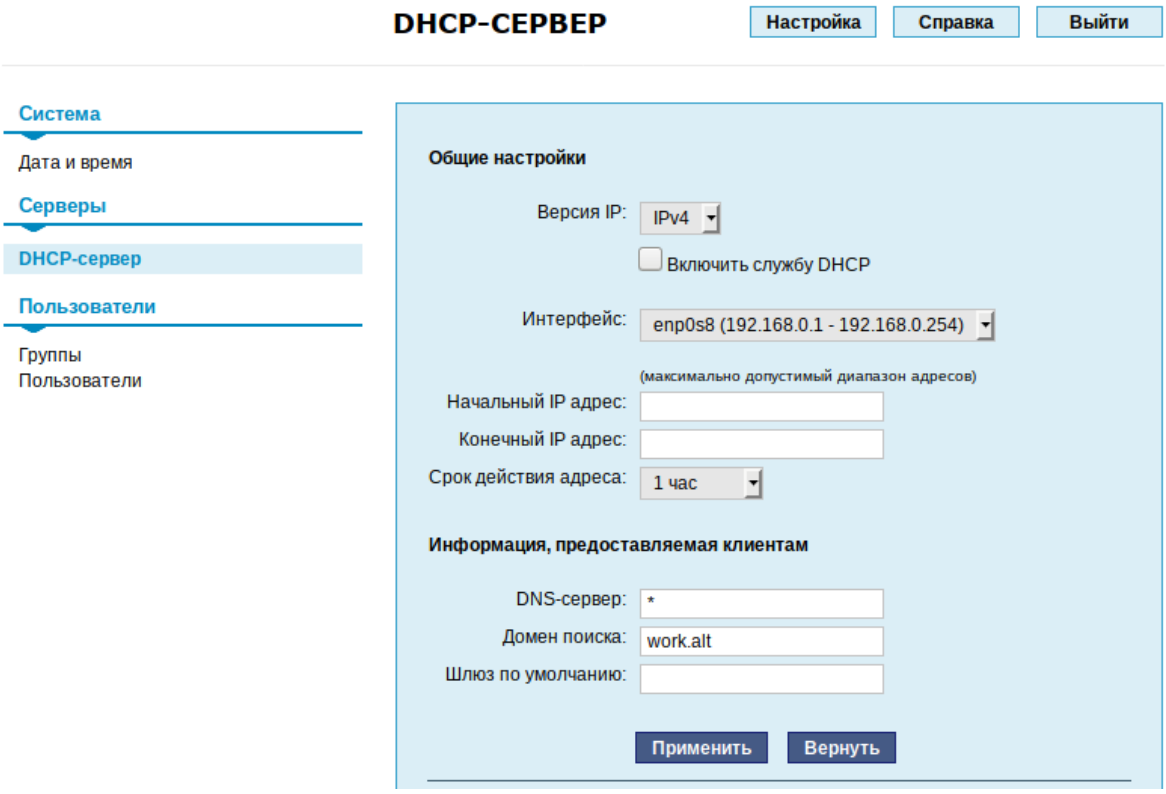


Рис. 58 – Веб-интерфейс ЦУС, запущенный от системного пользователя

7.1.5. Получение справочной информации

Все модули ЦУС содержат встроенную справку, поясняющую назначение конкретного модуля. Справка вызывается кнопкой «Справка» (рис. 59).

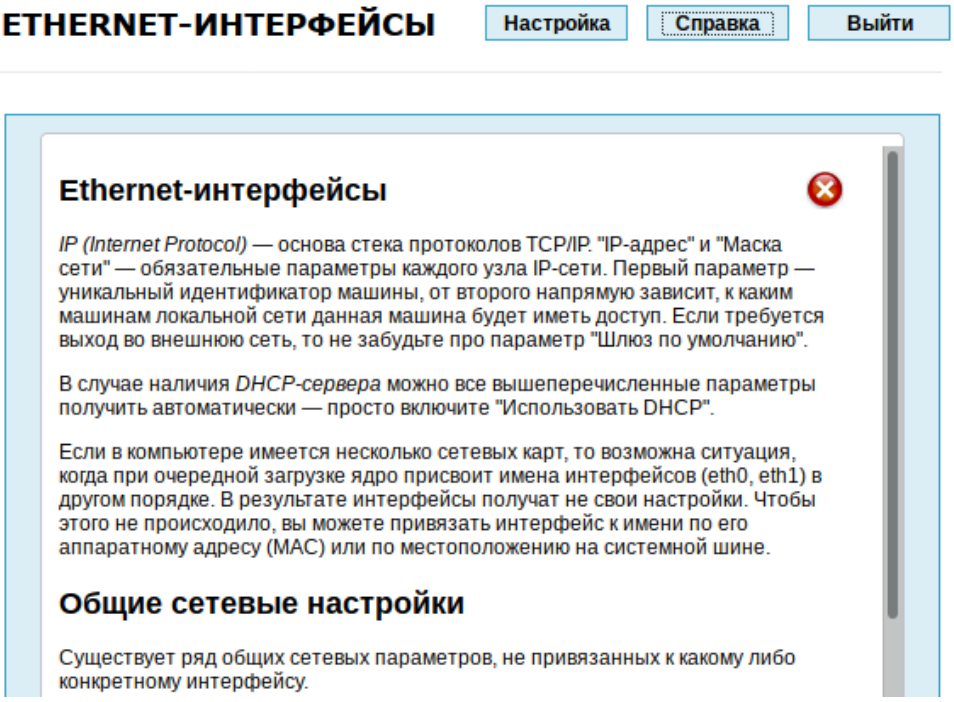


Рис. 59 – Получение справочной информации о модуле ЦУС

7.2. Выбор программ, запускаемых автоматически при входе в систему

Для более удобной работы с системой можно выбрать определенные программы, которые будут запущены автоматически при входе пользователя в систему. Автозапускаемые программы автоматически сохраняют свое состояние и безопасно завершаются сеансовым менеджером при выходе из системы и перезапускаются при входе.

Инструмент настройки сессии позволяет настроить, какие программы будут автоматически запущены при входе в систему. Для запуска инструмента настройки сессии, выбрать на панели инструментов MATE «Меню» → «Система» → «Центр управления» → «Персональные» → «Запускаемые приложения».

7.2.1. Вкладка автоматического запуска программ

Список автоматически запускаемых программ представлен на вкладке «Автоматически запускаемые программы» (рис. 60). Этот список содержит краткое описание каждой программы и отметку, указывающую запускать программу или нет.

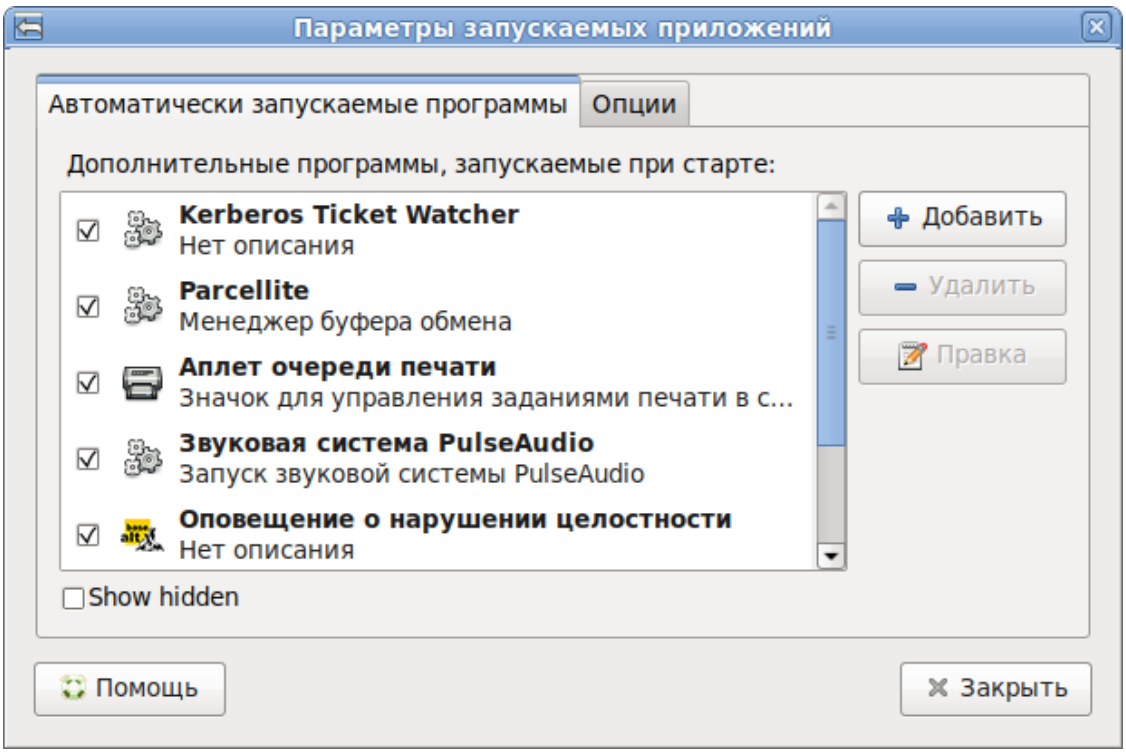


Рис. 60 – Автоматически запускаемые программы

На этой вкладке можно добавлять, удалять и изменять автозапускаемые приложения.

Для добавления новой автоматически запускаемой программы, следует выполнить следующие шаги:

- нажать на кнопку «Добавить». Откроется окно «Новая автоматически запускаемая программа»;
- указать имя программы и команду, которая запустит приложение (рис. 61);
- нажать на кнопку «Добавить».

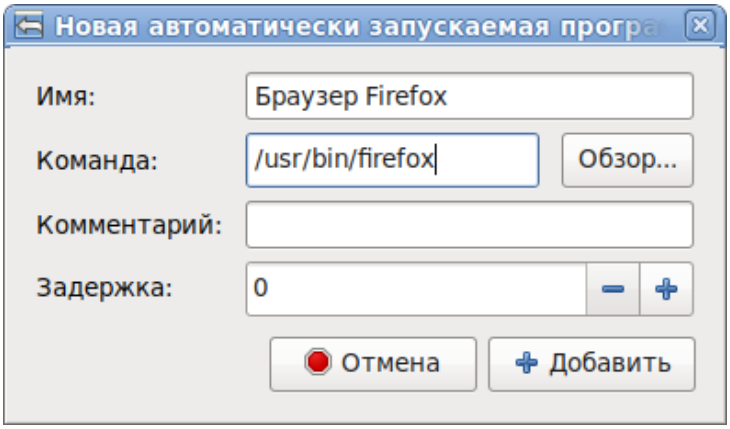


Рис. 61 – Добавление автоматически запускаемой программы

7.2.2. Вкладка настроек сессии

Менеджер сеанса может запомнить, какие приложения были запущены при выходе из системы, и автоматически запустить их при входе в систему. Для того, чтобы это происходило каждый раз при выходе из системы, следует на вкладке «Опции» отметить пункт «Автоматически запоминать запущенные приложения при выходе из сеанса» (рис. 62).

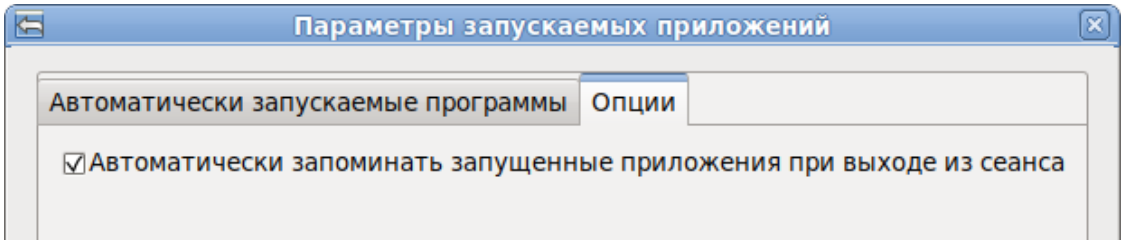


Рис. 62 – Запоминать запущенные приложения при выходе из сеанса

7.3. Задание хешей паролей

В ОС Альт СП реализована возможность хранения аутентификационной информации пользователей, полученной с использованием хеш-функций по ГОСТ Р 34.11–2012.

Для смены алгоритма хеширования, внести изменения в файл `/etc/pam.d/system-auth-local-only` изменить строку:

```
auth required pam_tcb.so shadow fork nullok
```

на

```
auth required pam_tcb.so shadow fork prefix=$2y$ count=8 nullok
```

и строку:

```
password required pam_tcb.so use_authtok shadow fork nullok write_to=tcb
```

на

```
password required pam_tcb.so use_authtok shadow fork prefix=$2y$ count=8 nullok write_to=tcb
```

где в значение `prefix=` подставляется значения для алгоритмов:

- `$gy$` – gost-yescrypt, в соответствии с ГОСТ Р 34.11–2012;

- `$2y$` – алгоритм bcrypt.

Для проверки результата просмотреть текущий хэш паролей пользователя root и произвольного пользователя выполнить команду:

```
cat /etc/tcb/имя_пользователя/shadow
```

Пример ожидаемого результата (bcrypt):

```
root:$2y$08$ClW.L8YyyBhbytvuCIiJS.XbGk8E4bV4S6gDqRH9daEuXYr2Y4a4m:18470::::::
```

Пример ожидаемого результата (gost-yescrypt):

```
root:$gy$jCT$v3mAdHCfMMlPJVvDZNl5I0$qjAbTbqQhl6eO6l7DZnnTW/5ZRmTO.AcZcVYgLyqsz5:18477::::::
```

Выполнить команду просмотра типа хэша пароля пользователя:

```
passwd -S имя_пользователя
```

Результат (bcrypt): `Password set, blowfish mode Y encryption`

Результат (gost-yescrypt): `Password set, gost-yescrypt encryption`

Примечание. Смена алгоритма хеширования происходит при изменении пароля пользователя, например, если истекает срок его действия, или пользователь сменил его. До этого момента алгоритм хеширования остается тем, с которым пароль был задан изначально. Поэтому, перед проверкой изменения алгоритма хэширования, измените пароль пользователя.

7.4. Настройка разграничения доступа к подключаемым устройствам

7.4.1. Общие сведения

В ОС Альт СП осуществляется разграничение доступа к символьным и блочным устройствам, для которых в каталоге `/dev` создаются файлы устройств. Разграничение выполняется с использованием генерации правил менеджера устройств udev.

Примечание. При разграничении доступа к устройствам типа видеокарт, либо сетевых карт, названный метод не используется.

Для решения задачи разграничения доступа к устройствам на основе генерации правил менеджера устройств udev в ОС реализованы:

- средства разграничения доступа к устройствам на основе правил udev;
- средства регистрации устройств.

Средства разграничения доступа к устройствам на основе генерации правил udev обеспечивают дискреционное разграничение доступа пользователей к подключаемым, в первую очередь, через интерфейс USB, устройствам (сканерам, съемным накопителям, видеокамерам).

Средства регистрации устройств обеспечивают учет подключаемых устройств и съемных носителей в системе, установку дискреционных атрибутов доступа пользователей к устройствам и создание дополнительных правил доступа к устройству (например, ограничение на подключение устройства только к определенному USB-порту).

7.4.2. Ограничения при помощи правил udev

Udev – сервис, который подхватывает и конфигурирует внешние устройства, получая уведомления от ядра ОС. Udev гибко настраивается под оборудование и задачи с помощью специальных правил.

Разграничение доступа к устройству осуществляется на основе соответствующего правила для менеджера устройств udev, которое хранится в файле в каталоге `/etc/udev/rules.d`. Файл правил обязательно должен иметь расширение `.rules`.

Далее приведен пример правила для съемного USB-носителя:

```
ENV{ID_SERIAL}=="JetFlash_TS256MJF120_OYLIXNA6", OWNER="user",
GROUP="users"
```

В приведенном примере для съемного USB-носителя с серийным номером `JetFlash_TS256MJF120_OYLIXNA6` разрешено его использование владельцу устройства: пользователю user и пользователям, входящим в группу users.

Типовое правило udev состоит из нескольких пар «ключ – значение», разделенных запятой.

Одни ключи используются для проверки соответствия устройства определенному правилу, в таких ключах используется знак «==» для разделения пары. Следующий пример отражает применение правила только для случая, если значение ключа `SUBSYSTEM` для этого устройства равно «block»:

```
SUBSYSTEM=="block"
```

Другие ключи используются для указания действия, если все условия соответствия выполняются. Для разделения пар в таких ключах используется знак равно «=». Например, в случае с `NAME="mydisk"` правило будет выглядеть следующим образом:

```
SUBSYSTEM=="block", ATTR(size)=="1343153213", NAME="mydisk"
```

Это правило выполнится только для устройства подсистемы block и с размером 1343153213 байт.

Для правил udev существуют следующие ключи соответствия:

- `SUBSYSTEM` – подсистема устройства;
- `KERNEL` – имя, выдаваемое устройству ядром;
- `DRIVER` – драйвер, обслуживающий устройство;
- `ATTR` – sysfs атрибут устройства;
- `SUBSYSTEMS` – подсистема родительского устройства.

Для действий используются ключи:

- `NAME` – установить имя файла устройства;
- `SYMLINK` – альтернативное имя устройства;
- `RUN` – выполнить скрипт при подключении устройства;

- GROUP – группа, у которой есть доступ к файлу;
- OWNER – владелец файла устройства;
- MODE – маска прав доступа.

Ключ ATTR позволяет получить информацию об устройстве. Посмотреть все возможные udev параметры для устройства можно с помощью команды udevadm.

Например, для диска /dev/sda команда просмотра параметров будет выглядеть следующим образом:

```
# udevadm info -a -n sda1
```

Для создания файла с правилами нужно выполнить следующую команду:

```
# touch /etc/udev/rules.d/usb.rules
```

Правило отключения ручного монтирования, для всех пользователей не из группы «plugdev», которое нужно добавить в файл usb.rules, будет выглядеть следующим образом:

```
BUS=="usb", SUBSYSTEM=="block", KERNEL=="sd*", ACTION=="add",
GROUP="plugdev", MODE="660"
```

Правило, которое при подключении USB-устройства запускает скрипт /etc/udev/usb_on.sh, и сделает действия (например, запишет в log-файл информацию), будет выглядеть следующим образом:

```
ACTION=="add", SUBSYSTEM=="block",
ENV{ID_BUS}=="usb|mmc|memstick|ieee1394", RUN+="/bin/bash
/etc/udev/usb_on.sh %E{ID_SERIAL_SHORT} %E{ID_MODEL} %E{ID_VENDOR}"
```

где:

- ACTION – отслеживаемое действие;
- add – подключение устройств;
- remove – отключение;
- ENV – перечень отслеживаемых устройств по типу;
- RUN – исполняемое действие.

Скрипту usb_on.sh udev передает следующие данные:

- %E{ID_SERIAL_SHORT} – серийный номер USB-устройства;
- %E{ID_MODEL} – модель USB-устройства;
- %E{ID_VENDOR} – производитель USB-устройства.

Использование скрипта позволяет выполнять более гибкую настройку правил: можно не только монтировать устройства, но и выполнять другие действия (копировать, менять владельца и так далее). Также допускается задавать тип доступа к информации на носителе, например, «только для чтения».

Далее приводятся примеры оформления других возможных правил для udev:

- отключить все USB-порты:

```
BUS=="usb", OPTIONS+="ignore_device"
```

- отключить все блочные устройства, присоединенные к USB-портам:

```
BUS=="usb", SUBSYSTEM=="block", OPTIONS+="ignore_device"
```

- назначить постоянное имя файлу устройства второго IDE-диска:

```
KERNEL=="sdb", NAME="my_spare"
```

- игнорировать второй USB SCSI/IDE-диск, подключенный по USB:

```
BUS=="usb", KERNEL=="hdb", OPTIONS+="ignore_device"
```

7.4.3. Управление монтированием блочных устройств

При монтировании блочных устройств используется утилита mount, модифицированная для монтирования устройства владельцем или пользователем. В процессе монтирования от имени пользователя ожидается два параметра: конкретное наименование файла устройства и конкретное наименование точки монтирования.

Для предоставления локальным пользователям возможности монтирования ФС съемных накопителей нужно наличие в файле `/etc/fstab` следующей записи:

```
/dev/sdb1 /media/usb     vfat rw,noauto,user 0 0
```

7.4.4. Настройка ограничений в веб-интерфейсе ЦУС (alterator-ports-access)

Настроить ограничения на использование внешних носителей можно в веб-интерфейсе ЦУС (пакет alterator-fbi) (п. 7.1.2) в меню «Система» → пункт «Контроль доступа к портам» (пакет alterator-ports-access) (рис. 63).

Должны быть установлены пакеты alterator-fbi и alterator-ports-access:

```
# apt-get install alterator-fbi
# apt-get install alterator-ports-access
```

Далее нужно запустить службу ahttpd:

```
# systemctl start ahttpd
```

Для определения подключенных USB-устройств в меню «Система» → пункт «Контроль доступа к портам» (рис. 63) нужно нажать на кнопку «Сканировать USB-устройства». Для помещения в таблицу «СПИСОК РАЗРЕШЕННЫХ УСТРОЙСТВ» можно выделить подключенное устройство, которое нужно разрешить в таблице «ПОДКЛЮЧЕННЫЕ USB-УСТРОЙСТВА», и нажать на кнопку «Разрешить выбранное устройство» (рис. 64).

Для исключения устройства из списка разрешенных, нужно выделить правило, разрешающее данное устройство в «СПИСОК РАЗРЕШЕННЫХ УСТРОЙСТВ» и нажать на кнопку «Удалить выбранное правило».

Чтобы отключить поддержку всех USB-устройств кроме заданных, нужно нажать на кнопку «Включить контроль USB-портов».

Примечание. Перед активацией ограничений предварительно разрешите использование USB-портов для клавиатуры и мыши.

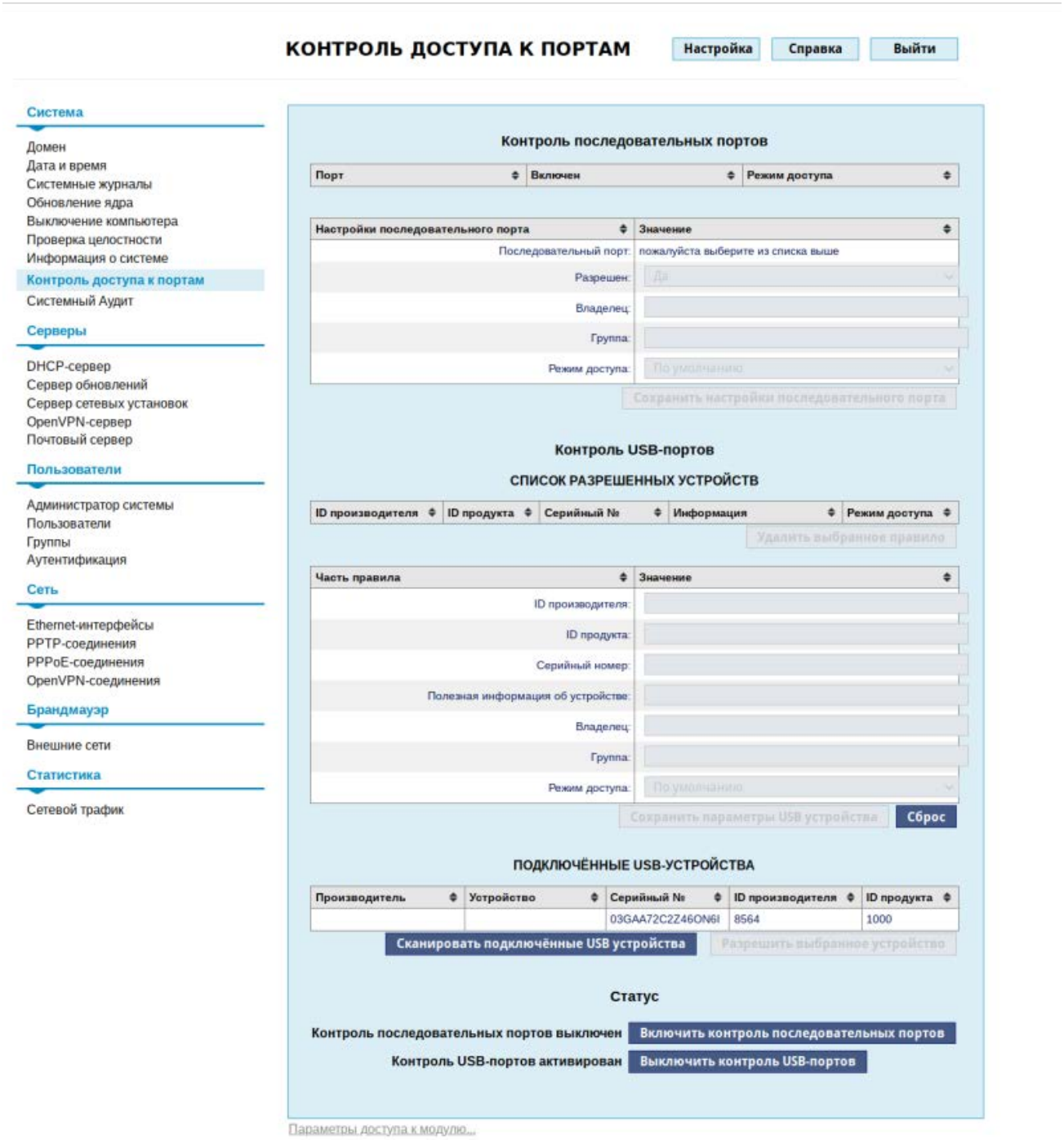


Рис. 63 – Контроль доступа к портам

Рис. 64 – Добавление USB-устройства в список разрешенных устройств

7.5. Настройка фильтрации пакетов с помощью утилиты iptables

Утилита iptables – стандартный интерфейс командной строки для управления фильтрацией сетевых пакетов и сбора статистики сетевого взаимодействия.

Утилита iptables позволяет фильтровать сетевые пакеты по следующим параметрам:

- на основе сетевых адресов отправителя и получателя (IP-адреса, MAC-адреса);
- по протоколам tcp, udp, icmp;
- с учетом входного и выходного сетевого интерфейса;
- на основе используемого порта;
- с учетом даты и времени.

Фильтры состоят из правил. Каждое правило – это строка, содержащая в себе критерии, определяющие, подпадает ли пакет под заданное правило, и действие, которое нужно выполнить в случае удовлетворения критерия.

7.5.1. Устройство фильтра iptables

Для iptables в общем виде правила выглядят так:

```
iptables [-t table] command [match] [target/jump]
```

Если в правило не включается спецификатор `[-t table]`, то по умолчанию предполагается использование таблицы filter, если же предполагается использование другой таблицы, то это требуется указать явно. Спецификатор таблицы так же можно указывать в любом месте строки правила, однако для удобства чтения лучше указывать таблицу в начале правила.

Непосредственно за именем таблицы должна стоять команда управления фильтром. Если спецификатора таблицы нет, то команда всегда должна стоять первой. Команда определяет действие iptables (вставить правило, добавить правило в конец цепочки, или удалить правило). Тело команды в общем виде выглядит так:

```
[команда] [цепочка]
```

Ключ команда указывает на то, что нужно сделать с правилом, например, команда `-A` указывает на то, что правило нужно добавить в конец указанной цепочки.

Цепочка указывает, в какую цепочку нужно добавить правило. Стандартные цепочки – INPUT, OUTPUT, FORWARD, PREROUTING и POSTROUTING. Они находятся в таблицах фильтра. Не все таблицы содержат все стандартные цепочки. Подробнее таблицы и цепочки описаны ниже.

Раздел `[match]` задает критерии проверки, по которым определяется, подпадает ли пакет под действие этого правила или нет. Здесь можно указать самые разные критерии – IP-адрес источника пакета или сети, сетевой интерфейс.

Раздел `[target]` указывает, какое действие должно быть выполнено при условии выполнения критериев в правиле. Здесь можно передать пакет в другую цепочку правил, «сбросить» пакет и забыть про него, выдать на источник сообщение об ошибке и т. д.

Когда пакет приходит на сетевое устройство, он обрабатывается соответствующим драйвером и далее передается в фильтр в ядре ОС. Далее пакет проходит ряд таблиц и затем передается либо локальному приложению, либо переправляется на другую машину (рис. 65).

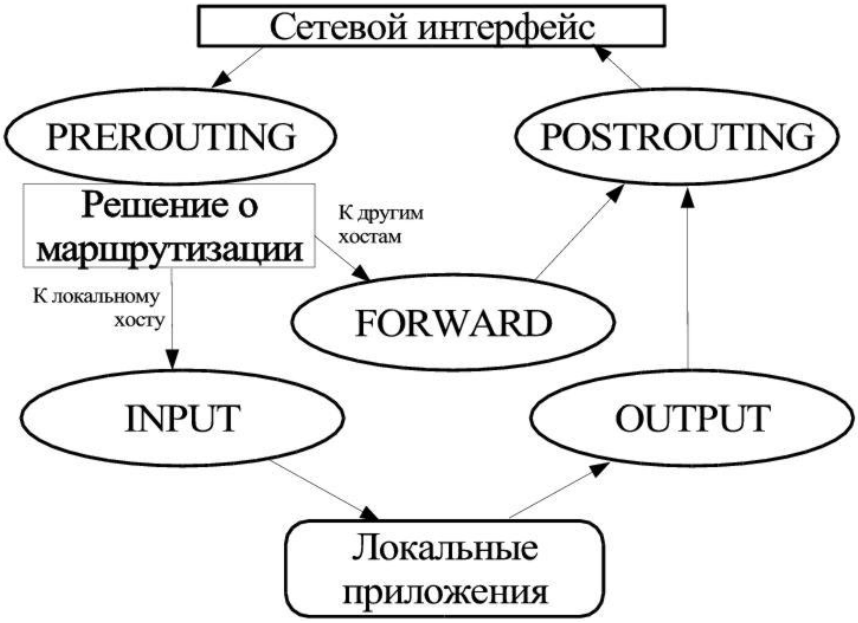


Рис. 65 – Схема движения пакетов в iptables

7.5.2. Встроенные таблицы фильтра iptables

По умолчанию используется таблица filter. Опция `-t` в правиле указывает на используемую таблицу. С ключом `-t` можно указывать следующие таблицы: nat, mangle, filter.

7.5.2.1. Таблица nat

Таблица nat используется главным образом для преобразования сетевых адресов Network Address Translation. Через эту таблицу проходит только первый пакет из потока. Преобразование адресов автоматически применяется ко всем последующим пакетам.

Таблица имеет три цепочки PREROUTING, OUTPUT и POSTROUTING:

- цепочка PREROUTING используется для внесения изменений в пакеты на входе в фильтр;

- цепочка OUTPUT используется для преобразования пакетов, созданных приложениями внутри компьютера, на котором установлен фильтр, перед принятием решения о маршрутизации;
- цепочка POSTROUTING используется для преобразования пакетов перед выдачей их в сеть.

7.5.2.2. Таблица mangle

Таблица mangle используется для внесения изменений в заголовки пакетов. Примером может служить изменение поля TTL, TOS или MARK. Таблица имеет две цепочки PREROUTING и OUTPUT:

- цепочка PREROUTING используется для внесения изменений на входе в фильтр перед принятием решения о маршрутизации;
- цепочка OUTPUT – для внесения изменений в пакеты, поступающие от внутренних приложений. Таблица mangle не должна использоваться для преобразования сетевых адресов (Network Address Translation) или маскарадинга (masquerading), для этих целей используется таблица nat.

7.5.2.3. Таблица filter

Таблица filter используется, главным образом, для фильтрации пакетов.

Таблица имеет три цепочки – FORWARD, INPUT, OUTPUT:

- цепочка FORWARD используется для фильтрации пакетов, идущих транзитом через данный компьютер;
- цепочка INPUT предназначена для обработки входящих пакетов, направляемых локальным приложениям данного компьютера;
- цепочка OUTPUT используется для фильтрации исходящих пакетов, сгенерированных локальными приложениями данного компьютера.

7.5.3. Команды утилиты iptables

В таблице 1 приведены команды, которые используются в iptables.

Т а б л и ц а 1 – Команды утилиты iptables

Команда	Пример	Пояснения
-A, --append	iptables -A INPUT	Добавляет новое правило в конец заданной цепочки
-D, --delete	iptables -D INPUT --dport 80 -j DROP iptables -D INPUT 1	Удаление правила из цепочки. Команда имеет два формата записи, первый – когда задается критерий сравнения с опцией -D (см. первый пример), второй – порядковый номер правила. Если задается критерий сравнения, то удаляется правило, которое имеет в себе этот критерий, если задается номер правила, то будет удалено правило с заданным номером. Счет правил в цепочках начинается с 1
-R, --replace	iptables -R INPUT 1 -s 192.168.0.1 -j DROP	Данная команда заменяет одно правило другим. Используется в основном во время отладки новых правил
-I, --insert	iptables -I INPUT 1 -dport 80 -j ACCEPT	Вставляет новое правило в цепочку. Число, следующее за именем цепочки, указывает номер правила, перед которым нужно вставить новое правило, другими словами число задает номер для вставляемого правила. В примере, указывается, что данное правило должно быть 1-м в цепочке INPUT
-L, --list	iptables -L INPUT	Вывод списка правил в заданной цепочке, в данном примере предполагается вывод правил из цепочки INPUT. Если имя цепочки не указывается, то выводится список правил для всех цепочек. Формат вывода зависит от наличия дополнительных ключей в команде, например, -n, -v, и пр.
-F, --flush	iptables -F INPUT	Удаление всех правил из заданной цепочки (таблицы). Если имя цепочки и таблицы не указывается, то удаляются все правила, во всех цепочках
-Z, --zero	iptables -Z INPUT	Обнуление всех счетчиков в заданной цепочке. Если имя цепочки не указывается, то подразумеваются все цепочки. При использовании ключа -v совместно с командой -L, на вывод будут поданы и состояния счетчиков пакетов, попавших под действие каждого правила. Допускается совместное использование команд -L и -Z. В этом случае будет выдан сначала список правил со счетчиками, а затем произойдет обнуление счетчиков

Окончание таблицы 1

Команда	Пример	Пояснения
-N, --new-chain	iptables -N allowed	Создается новая цепочка с заданным именем в заданной таблице. В приведенном выше примере создается новая цепочка с именем allowed. Имя цепочки должно быть уникальным и не должно совпадать с зарезервированными именами цепочек и действий (DROP, REJECT и т. п.)
-X, --delete-chain	iptables -X allowed	Удаление заданной цепочки из заданной таблицы. Удаляемая цепочка не должна иметь правил и не должно быть ссылок из других цепочек на удаляемую цепочку. Если имя цепочки не указано, то будут удалены все цепочки, определенные командой -N в заданной таблице
-P, --policy	iptables -P INPUT DROP	Определяет политику по умолчанию для заданной цепочки. Политика по умолчанию определяет действие, применяемое к пакетам, не попавшим под действие ни одного из правил в цепочке. В качестве политики по умолчанию допускается использовать DROP, ACCEPT и REJECT
-E, --rename-chain	iptables -E allowed disallowed	Команда -E выполняет переименование пользовательской цепочки. В примере цепочка allowed будет переименована в цепочку disallowed. Эти переименования не изменяют порядок работы, а носят только косметический характер

Команда должна быть указана всегда. Список доступных команд можно просмотреть с помощью команды iptables -h или, что тоже самое, iptables --help. Некоторые команды могут использоваться совместно с дополнительными ключами.

7.5.4. Ключи утилиты iptables

В таблице 2 приводится список дополнительных ключей и описывается результат их действия.

Т а б л и ц а 2 – Ключи утилиты iptables

Ключ	Пример	Пояснения
`-v, --verbose`	`--list`, `--append`, `--insert`, `--delete`, `--replace`	Используется для повышения информативности вывода и, как правило, используется совместно с командой `--list`. В случае использования с командой `--list`, в вывод этой команды включаются: имя интерфейса, счетчики пакетов и байт для каждого правила. Формат вывода счетчиков предполагает вывод кроме цифр числа еще и символьные множители K (x1000), M (x1,000,000) и G (x1,000,000,000). Для того чтобы заставить команду `--list` выводить полное число (без употребления множителей) требуется применять ключ `-x`. Если ключ `-v, --verbose` используется с командами `--append`, `--insert`, `--delete` или `--replace`, то на вывод будет выдан подробный отчет о произведенной операции
`-x, --exact`	`--list`	Для всех чисел в выходных данных выводятся их точные значения без округления и без применения множителей K, M, G
`-n, --numeric`	`--list`	Iptables выводит IP-адреса и номера портов в числовом виде, предотвращая попытки преобразовать их в символические имена
`--line-numbers`	`--list`	Включает режим вывода номеров строк при отображении списка правил
`-c, --set-counters`	`--insert`, `--append`, `--replace`	Используется при создании нового правила для установки счетчиков пакетов и байт в заданное значение. Например, ключ `--set-counters 20 4000` установит счетчик пакетов `= 20`, а счетчик байт `= 4000`
`--modprobe`	Любая команда	Определяет команду загрузки модуля ядра

7.5.5. Основные действия над пакетами в фильтре iptables

В таблице 3 приведены доступные над пакетами действия.

Т а б л и ц а 3 – Действия над пакетами iptables

Действие	Пояснения
ACCEPT	Пакет прекращает движение по цепочке (и всем вызвавшим цепочкам, если текущая цепочка была вложенной) и считается принятым, тем не менее, пакет продолжит движение по цепочкам в других таблицах и может быть отвергнут там
DROP	Отбрасывает пакет и iptables «забывает» о его существовании. Отброшенные пакеты прекращают свое движение полностью
RETURN	Прекращает движение пакета по текущей цепочке правил и производит возврат в вызывающую цепочку, если текущая цепочка была вложенной, или, если текущая цепочка лежит на самом верхнем уровне (например, INPUT), то к пакету будет применена политика по умолчанию

Окончание таблицы 3

Действие	Пояснения
LOG	Служит для журналирования отдельных пакетов и событий. В системный журнал могут заноситься заголовки IP-пакетов и другая интересующая информация
REJECT	Используется, как правило, в тех же самых ситуациях, что и DROP, но в отличие от DROP, команда `REJECT` выдает сообщение об ошибке на хост, передавший пакет
SNAT	Используется для преобразования сетевых адресов (Source Network Address Translation), т. е. изменение исходящего IP-адреса в IP-заголовке пакета
DNAT	Destination Network Address Translation используется для преобразования адреса места назначения в IP-заголовке пакета
MASQUERADE	В основе своей представляет то же самое, что и SNAT только не имеет ключа `--to-source`. Причиной тому то, что маскарадинг может работать, например, с dialup подключением или DHCP, т. е. в тех случаях, когда IP-адрес присваивается устройству динамически. Если используется динамическое подключение, то нужно использовать маскарадинг, если же используется статическое IP-подключение, то лучшим выходом будет использование действия SNAT
REDIRECT	Выполняет перенаправление пакетов и потоков на другой порт той же самой машины. К примеру, можно пакеты, поступающие на HTTP порт перенаправить на порт HTTP proxy. Действие REDIRECT очень удобно для выполнения «прозрачного» проксирования (transparent proxy), когда компьютеры в локальной сети даже не подозревают о существовании прокси
TTL	Используется для изменения содержимого поля «время жизни» (Time To Live) в IP-заголовке. Один из вариантов применения этого действия – это устанавливать значение поля «Time To Live» во всех исходящих пакетах в одно и то же значение. Если установить на все пакеты одно и то же значение TTL, то тем самым можно лишить провайдера одного из критериев определения того, что подключение к Интернету разделяется между несколькими компьютерами. Для примера можно привести число «TTL = 64», которое является стандартным для ядра Linux

7.5.6. Основные критерии пакетов в фильтре iptables

В таблице 4 приведены возможные критерии для фильтрации пакетов в фильтре iptables.

Таблица 4 – Критерии пакетов в фильтре iptables

Критерий	Пояснения
`-p, --protocol`	Используется для указания типа протокола. Примерами протоколов могут быть TCP, UDP и ICMP. Список протоколов можно посмотреть в файле `/etc/protocols`. Прежде всего, в качестве имени протокола в данный критерий можно передавать три вышеупомянутых протокола, а также ключевое слово ALL. В качестве протокола допускается передавать число – номер протокола

Продолжение таблицы 4

Критерий	Пояснения
`-s, --src, --source`	IP-адрес(а) источника пакета. Адрес источника может указываться без маски или префикса (например, 192.168.1.1), тогда подразумевается единственный IP-адрес. Можно указать адрес в виде `address/mask`, например, как 192.168.0.0/255.255.255.0, или более современным способом 192.168.0.0/24, т. е. фактически определяя диапазон адресов. Символ «!», установленный перед адресом, означает логическое отрицание, т. е. `--source ! 192.168.0.0/24` означает любой адрес кроме адресов 192.168.0.x
`-d, --dst, --destination`	IP-адрес(а) получателя. Имеет синтаксис схожий с критерием `--source`, за исключением того, что подразумевает адрес места назначения. Точно так же может определять, как единственный IP-адрес, так и диапазон адресов. Символ «!» используется для логической инверсии критерия
`-i, --in-interface`	Интерфейс, с которого был получен пакет. Использование этого критерия допускается только в цепочках INPUT, FORWARD и PREROUTING, в любых других случаях будет вызывать сообщение об ошибке
`-o, --out-interface`	Задает имя выходного интерфейса. Этот критерий допускается использовать только в цепочках OUTPUT, FORWARD и POSTROUTING, в противном случае будет генерироваться сообщение об ошибке
`-f, --fragment`	Правило распространяется на все фрагменты фрагментированного пакета, кроме первого, сделано это потому, что нет возможности определить исходящий/входящий порт для фрагмента пакета, а для ICMP-пакетов определить их тип. С помощью фрагментированных пакетов могут производиться атаки на межсетевой экран, так как фрагменты пакетов могут не отлавливаться другими правилами
`-sport, --source-port`	Исходный порт, с которого был отправлен пакет. В качестве параметра может указываться номер порта или название сетевой службы. Соответствие имен сервисов и номеров портов можно найти в файле `/etc/services`. При указании номеров портов правила отрабатывают несколько быстрее
`--dport, --destination-port`	Порт, на который адресован пакет. Аргументы задаются в том же формате, что и для `--source-port`
`-tcp-flags`	SYN, ACK, FIN SYN определяет маску и флаги tcp-пакета. Пакет считается удовлетворяющим критерию, если из перечисленных флагов в первом списке в единичное состояние установлены флаги из второго списка. В качестве аргументов критерия могут выступать флаги SYN, ACK, FIN, RST, URG, PSH, а также зарезервированные идентификаторы ALL и NONE. ALL означает ВСЕ флаги, а NONE – НИ ОДИН флаг. Так, критерий `--tcp-flags ALL NONE` означает, что все флаги в пакете должны быть сброшены. Символ «!» означает инверсию критерия. Имена флагов в каждом списке должны разделяться запятыми, пробелы служат для разделения списков
`--icmp-type`	Тип сообщения ICMP определяется номером или именем. Числовые значения определяются в RFC 792. Чтобы получить список имен ICMP значений выполните команду `iptables --protocol icmp --help`. Символ «!» инвертирует критерий, например, `--icmp-type ! 8`

Окончание таблицы 4

Критерий	Пояснения
`--state`	Для использования данного критерия в правиле перед `--state` нужно явно указать `-m state`. Проверяется признак состояния соединения. Можно указывать 4 состояния: INVALID, ESTABLISHED, NEW и RELATED. INVALID подразумевает, что пакет связан с неизвестным потоком или соединением и, возможно содержит ошибку в данных или в заголовке. ESTABLISHED указывает на то, что пакет принадлежит уже установленному соединению, через которое пакеты идут в обоих направлениях. NEW подразумевает, что пакет открывает новое соединение или пакет принадлежит однонаправленному потоку. RELATED указывает на то, что пакет принадлежит уже существующему соединению, но при этом он открывает новое соединение. Примером может служить передача данных по FTP, или выдача сообщения ICMP об ошибке, которое связано с существующим TCP или UDP соединением. Признак NEW – это не то же самое, что установленный бит SYN в пакетах TCP, посредством которых открывается новое соединение, и подобного рода пакеты могут быть потенциально опасны в случае, когда для защиты сети используется один сетевой экран

7.5.7. Модули iptables

Возможности фильтрации пакетов расширяются через модули. Модули подключаются автоматически при выборе протокола (`-p/--protocol`) или вручную опцией `-m/--match`, после которой следует имя подключаемого фильтра и его опции.

Справку по опциям модуля можно получить с помощью ключа `-h/--help`. Допустимо указание нескольких модулей. Результаты фильтрации, выдаваемые модулем, можно инвертировать указав ! перед его именем.

В таблице 5 приведены возможные критерии для фильтрации пакетов в фильтре iptables.

Т а б л и ц а 5 – Модули iptables

Модуль	Опции	Пояснение
connlimit	`[!] --connlimit-above n` — пакет подойдет под описание, если количество одновременных подключений на данный момент больше (меньше), чем `n`; `--connlimit-mask bits` – позволяет задать маску блока адресов	Позволяет задавать возможное количество одновременных подключений к машине от заданного IP или блока адресов. Пример. Допускать не больше 20 соединений на порт 80 с одного хоста `iptables -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 20 -j REJECT --reject-with tcp-reset`

Продолжение таблицы 5

Модуль	Опции	Пояснение
icmp	`--icmp-type [!] тип` – тип ICMP в виде числа или имени в соответствии с `iptables -p icmp –h`	Расширение загружается при указании `--protocol icmp`.
iprange	`[!]--src-range ip-ip` – диапазон IP-адресов отправителя; `[!]--dst-range ip-ip` – диапазон IP-адресов получателя	Выделяет не один адрес, как `--src`, а все адреса от ip1 до ip2

ipv4options (не подключен по умолчанию)	`--flags [!]параметр[,...]` – сопоставляет наличие/отсутствие(!) параметров (по имени или номеру);
	`--any` – хотя бы один `--flags` ipv4 или их комбинация.
	Примеры параметров:
	- `ssrr` – strict source routing – маршрутизация указывается источником;
	- `lsrr` – loose source routing – свободная маршрутизация;
	- `rr` – record-route – запись маршрута;
	- `ra` – оповещения маршрутизатора;
	- `srr` – source-routing – режим маршрутизации;
	- `ts` – timestamp
		Результат теста зависит от параметров заголовка IPv4, таких как параметры маршрутизации, запись маршрута, запрос времени, оповещение маршрутизатора.
		Примеры. Отбрасывать пакеты с флагом `ssrr`:
		`iptables -A INPUT -m ipv4options --flags ssrr -j DROP`
		Отбрасывать пакеты любые пакеты ipv4:
		`iptables -A INPUT -m ipv4options --any -j DROP`

length	`--length [!] размер[:размер]`	Позволяет проверять размеры пакетов (точно или по диапазону)
limit	`--limit частота` – максимальная средняя частота положительных результатов. После числа можно указывать единицы: `/second', `/minute', `/hour', `/day'; значение по умолчанию – `3/hour`. `--limit-burst number` – ограничение на исходное число пропускаемых пакетов (по умолчанию – 5)	Выдает положительный результат с фиксированной частотой. Правило использующее этот модуль будет выполняться до момента достижения лимита (и наоборот, если указан «!»). Может использоваться вместе с целью LOG для получения ограниченного протоколирования
limit	`--limit частота` – максимальная средняя частота положительных результатов. После числа можно указывать единицы: `/second', `/minute', `/hour', `/day'; значение по умолчанию – `3/hour`. `--limit-burst number` – ограничение на исходное число пропускаемых пакетов (по умолчанию – 5)	Выдает положительный результат с фиксированной частотой. Правило использующее этот модуль будет выполняться до момента достижения лимита (и наоборот, если указан «!»). Может использоваться вместе с целью LOG для получения ограниченного протоколирования

Продолжение таблицы 5

Модуль	Опции	Пояснение
limit	`--limit частота` – максимальная средняя частота положительных результатов. После числа можно указывать единицы: `/second', `/minute', `/hour', `/day'; значение по умолчанию – `3/hour`. `--limit-burst number` – ограничение на исходное число пропускаемых пакетов (по умолчанию – 5)	Выдает положительный результат с фиксированной частотой. Правило использующее этот модуль будет выполняться до момента достижения лимита (и наоборот, если указан «!»). Может использоваться вместе с целью LOG для получения ограниченного протоколирования
multiport	`[!]--source-ports port1,port2,port3:port4` – исходный порт равен одному из указанных; `[!]--destination-ports port1,port2,port3:port4` – порт назначения равен одному из указанных; `[!]--ports port1,port2,port3:port4` – исходный и порт назначения и равны одному из указанных	Позволяет указывать в тексте правила несколько (до 15) портов и диапазонов портов (порт:порт). Используется только вместе с `-p tcp` или `-p udp`
state	`--state состояния` – список фильтруемых состояний через запятую (см. таблицу 4)	Проверяется признак состояния соединения (state)
string	`--algo bm|kmp` – стратегия сравнения/поиска (`bm = Boyer-Moore, kmp = Knuth-Pratt-Morris`); `--from позиция` – позиция в данных с которой следует начинать поиск. Значение по умолчанию – 0. `--to позиция` – позиция в данных, при достижении которой следует прекращать поиск. Значение по умолчанию – размер пакета; `--string последовательность` – последовательность символов, которую следует искать в пакете; `--hex-string pattern` – последовательность символов, которую следует искать в пакете (в шестнадцатеричном представлении)	Позволяет выполнять фильтрацию пакетов, основываясь на анализе содержимого области данных пакета

Окончание таблицы 5

Модуль	Опции	Пояснение
tcp	см. таблицу 4	Это расширение загружается при указании `--protocol tcp`
u32	`--u32 "Start&Mask=Range"`	Позволяет извлекать из пакета данные размером до 4 байт, применять к ним операции логического И, сдвига, и проверять принадлежность получающихся данных определенным диапазонам. В простейшей форме, u32 вырезает блок из 4 байт начиная со Start, применяет к ним маску Mask и сравнивает результат с Range-m u32
udp	см. таблицу 4	Это расширение загружается при указании `--protocol udp`

Список доступных модулей можно просмотреть, выполнив команду:

```
# ls /lib/modules/$(uname -r)/kernel/net/netfilter/
```

Загруженные модули iptables можно найти в записи файловой системы proc `/proc/net/ip_tables_matches`:

```
# cat /proc/net/ip_tables_matches
```

Загрузка модуля:

```
# modprobe <модуль>
```

Например:

```
# modprobe xt_limit
# modprobe xt_length
# modprobe xt_u32
```

7.5.8. Использование фильтра iptables

ОС Альт СП уже включает в себя предустановленный iptables. Для его настройки рекомендуется использовать возможности системы настройки сети `/etc/net` (см. п. 8.7).

7.5.9. Примеры команд iptables

Список текущих правил:

```
iptables -nvL --line-numbers
```

Очистка всех правил:

```
iptables -F
```

Очистка правил в цепочке:

```
iptables -F INPUT
```

Удаления пятого правила в цепочке INPUT:

```
iptables -D INPUT 5
```

7.5.9.1. Фильтрация по источнику пакета

Для фильтрации по источнику используется опция `-s`.

Например, запретить все входящие пакеты с узла 192.168.1.95:

```
iptables -A INPUT -s 192.168.1.95 -j DROP
```

Можно использовать доменное имя для указания адреса хоста:

```
iptables -A INPUT -s test.host.net -j DROP
```

Также можно указать целую подсеть:

```
iptables -A INPUT -s 192.168.1.0/24 -j DROP
```

Можно использовать отрицание (знак «!»). Например, все пакеты с хостов отличных от 192.168.1.96 будут уничтожаться:

```
iptables -A INPUT ! -s 192.168.1.96 -j DROP
```

Разрешить трафик по localhost:

```
iptables -A INPUT -i lo -j ACCEPT
```

Записывать в журнал попытки спуфинга с префиксом `"IP_SPOOF A: "` и запретить соединение:

```
iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j LOG --log-prefix "IP_SPOOF A: "
iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
```

7.5.9.2. Фильтрация по адресу назначения

Для фильтрации по адресу назначения используется опция `-d`.

Например, запретить все исходящие пакеты на хост 192.168.1.95:

```
iptables -A OUTPUT -d 192.168.156.156 -j DROP
```

Запретить доступ к ресурсу `vk.com`:

```
iptables -A OUTPUT -d vk.com -j REJECT
```

Как и в случае с источником пакета можно использовать адреса подсети и доменные имена. Отрицание также работает.

7.5.9.3. Фильтрация по протоколу

Опция `-p` указывает на протокол. Можно использовать all, icmp, tcp, udp или номер протокола (из `/etc/protocols`).

Разрешить входящие эхо-запросы:

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

7.5.9.4. Фильтрация по порту источника

Разрешить все исходящие пакеты с порта 80:

```
iptables -A INPUT -p tcp --sport 80 -j ACCEPT
```

Заблокировать все входящие запросы порта 80:

```
iptables -A INPUT -p tcp --dport 80 -j DROP
```

Для указания порта нужно указать протокол (tcp или udp). Можно использовать отрицание.

Открыть диапазон портов:

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 7000:7010 -j ACCEPT
```

7.5.9.5. Фильтрация по порту назначения

Разрешить подключения по HTTP:

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Разрешить подключения по SSH:

```
iptables -A INPUT -p tcp -i eth0 --dport 22 -j ACCEPT
```

Разрешить получать данные от DHCP-сервера:

```
iptables -A INPUT -p UDP --dport 68 --sport 67 -j ACCEPT
```

Разрешить rsync с определенной сети:

```
iptables -A INPUT -i eth0 -p tcp -s 192.168.1.0/24 --dport 873 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 873 -m state --state ESTABLISHED -j ACCEPT
```

Разрешить IMAP/IMAP2 трафик:

```
iptables -A INPUT -i eth0 -p tcp --dport 143 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 143 -m state --state ESTABLISHED -j ACCEPT
```

Разрешить исходящие HTTP, FTP, DNS, SSH, SMTP:

```
iptables -A OUTPUT -p TCP -o eth0 --dport 443 -j ACCEPT
iptables -A OUTPUT -p TCP -o eth0 --dport 80 -j ACCEPT
iptables -A OUTPUT -p TCP -o eth0 --dport 53 -j ACCEPT
iptables -A OUTPUT -p UDP -o eth0 --dport 53 -j ACCEPT
iptables -A OUTPUT -p TCP -o eth0 --dport 25 -j ACCEPT
iptables -A OUTPUT -p TCP -o eth0 --dport 22 -j ACCEPT
iptables -A OUTPUT -p TCP -o eth0 --dport 21 -j ACCEPT
```

Разрешить mysql для локальных пользователей:

```
iptables -I INPUT -p tcp --dport 3306 -j ACCEPT
```

Разрешить CUPS (сервер печати, порт 631) для пользователей внутри локальной сети:

```
iptables -A INPUT -s 192.168.1.0/24 -p udp -m udp --dport 631 -j ACCEPT
iptables -A INPUT -s 192.168.1.0/24 -p tcp -m tcp --dport 631 -j ACCEPT
```

Разрешить синхронизацию времени NTP для пользователей внутри локальной сети:

```
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p udp --dport 123 -j ACCEPT
```

7.5.9.6. Перенаправление портов

Направим трафик с порта 442 на 22, это значит, что входящие ssh-соединения могут быть принятыми с порта 422 и 22:

```
iptables -t nat -A PREROUTING -p tcp -d 192.168.1.15 --dport 422 -j DNAT --to 192.168.1.15:22
```

Также надо разрешить входящие соединения с порта 422:

```
iptables -A INPUT -i eth0 -p tcp --dport 422 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 422 -m state --state ESTABLISHED -j ACCEPT
```

Как и в случае с портом источника нужно указать протокол. Можно использовать отрицание.

7.5.9.7. Ограничение по локальным пользователям

Ограничение по локальным пользователям нельзя поручить внешнему межсетевому экрану, так как он не имеет этой информации.

Отбросить все пакеты, исходящие от процессов пользователя с UID=500:

```
# iptables -A OUTPUT -m owner --uid-owner 500 -j DROP
```

Попытка соединения с удаленным узлом, пользователя с UID=500:

```
# su – test
$ wget ya.ru
--2017-03-07 13:53:14--  http://ya.ru/
Распознается ya.ru (ya.ru)… ошибка: Имя или служба не известны.
wget: не удается разрешить адрес «ya.ru»
```

Попытка соединения с локальным узлом, пользователя с UID=500:

```
# su – test
$ wget localhost
--2017-03-07 13:55:20--  http://localhost/
Распознается localhost (localhost)… 127.0.0.1
Подключение к localhost (localhost)|127.0.0.1|:80... ^C
```

7.5.9.8. Фильтрация по содержимому пакета

Отбросить все пакеты, данные в которых содержат подстроку virus:

```
# iptables -I INPUT -j DROP -p tcp -s 0.0.0.0/0 -m string --algo kmp --string "virus "
```

Записывать в журнал пакеты со строкой secret внутри:

```
# iptables -A INPUT -m string --algo kmp  --string "secret"  -j LOG --log-level info --log-prefix "SECRET "
```

Просмотр журнала:

```
# journalctl |grep SECRET
апр    03    16:47:18    host-15.localdomain    kernel:    SECRET    IN=eth0    OUT=
MAC=08:00:27:d5:f3:78:74:e5:0b:3e:2c:88:08:00   SRC=192.168.3.101   DST=192.168.3.104
LEN=47 TOS=0x00 PREC=0x00 TTL=64 ID=30811 DF PROTO=TCP SPT=53878 DPT=8080 WINDOW=229
RES=0x00 ACK PSH URGP=0
апр    03    16:58:47    host-15.localdomain    kernel:    SECRET    IN=eth0    OUT=
MAC=08:00:27:d5:f3:78:74:e5:0b:3e:2c:88:08:00   SRC=192.168.3.101   DST=192.168.3.104
LEN=47 TOS=0x00 PREC=0x00 TTL=64 ID=38640 DF PROTO=TCP SPT=54510 DPT=8080 WINDOW=229
RES=0x00 ACK PSH URGP=0
```

Статистика правил iptables и счетчики обработанных пакетов в цепочке INPUT:

```
# iptables -nvL INPUT --line-numbers
Chain INPUT (policy ACCEPT 1711 packets, 1400K bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       47 49550 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
STRING match  "virus" ALGO name kmp TO 65535
2        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
STRING match  "virus " ALGO name kmp TO 65535
3       17 66141 LOG        tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
STRING match  "secret" ALGO name kmp TO 65535 LOG flags 0 level 6 prefix "SECRET "
```

7.6. Настройка экспорта аудита на удаленный узел

Для настройки экспорта аудита на удаленный узел нужно настроить OpenVPN-соединение (см. подробнее п. 8.11) между принимающей и передающей стороной, настроить межсетевой экран и внести изменения в конфигурационные файлы аудита.

На принимающей стороне – сервер:

1) скопировать файл `/usr/share/doc/openvpn-*/server.conf` (* – версия openvpn) в директорию `/etc/openvpn/` для его редактирования и последующего запуска сервера VPN;
2) в скопированном на предыдущем этапе файле `server.conf`, проверьте имена и пути файлов сертификата сервера (`.crt`), его ключа (`.key`), а также сертификата CA (`.crt`) и DH (`dh*.pem`), а также закомментировать параметр `proto udp` и раскомментировать `proto tcp`;
3) установить утилиту easy-rsa:

   ```
   # apt-get install easy-rsa
   ```

4) сгенерировать все ключи и сертификаты. Ввести для них пароли:

   ```
   # easyrsa init-pki
   # easyrsa build-ca
   # easyrsa build-server-full server
   # easyrsa build-client-full client1
   # easyrsa gen-dh
   ```

5) перенести полученные ключи и сертификаты в каталог `/etc/openvpn/keys/`.

Настройка OpenVPN-клиента на передающей стороне:

1) скопировать из `/usr/share/doc/openvpn-*/client.conf` (* – версия openvpn) в директорию `/etc/openvpn/` для его редактирования и последующего запуска клиента VPN;
2) скопировать раннее сгенерированные ключи и сертификаты в директорию `/etc/openvpn/keys/` и указать их в `client.conf`;
3) открыть `client.conf` найти строку `remote` и изменить ее на:

   `remote 10.10.3.87 1194`

   где `10.10.3.87` – это IP-адрес сервера на внешнем интерфейсе принимающей стороны.

Также, закомментировать параметр `proto udp` и раскомментировать `proto tcp`.

Отредактировать конфигурационные файлы аудита:

- на принимающей стороне в файле `/etc/audit/auditd.conf` исправить параметр `tcp_listen_port=1060`;
- на передающей стороне в файле `/etc/audit/audisp-remote.conf` исправить параметры:

  ```
  remote_server = 10.8.0.1
  port = 1060
  #queue_error_action
  ```

  где `10.8.0.1` – IP-адрес сервера vpn на созданном интерфейсе-туннеле принимающей стороны;
- на передающей стороне изменить параметр: `active = yes` в файле `/etc/audit/plugins.d/au-remote.conf`;
- перезапустить систему на принимающей и передающей сторонах.

Запустить сервер на принимающей стороне:

```
# openvpn /etc/openvpn/server.conf
```

Запустить OpenVPN-клиент на передающей стороне:

```
# openvpn /etc/openvpn/client.conf
```

Команды установки правила пропуска tcp пакетов с портом назначения 1060 только через устройство vpn (например, tun0) на принимающей стороне:

```
# iptables –A INPUT –p tcp --dport 1060 –i tun0 –j ACCEPT
# iptables –A INPUT –p tcp --dport 1060 –j DROP
```

Для проверки аудита передающей стороны на принимающей стороне выполнить команду:

```
# ausearch -hn имя_передающей_стороны
```

Если ничего не отображается, то, возможно, было указано неверное имя передающей стороны. Для проверки, что лог приходит, можно, например, авторизоваться на передающей стороне, а затем проверить лог на принимающей стороне командой:

```
# ausearch -m USER_AUTH
```

Имя передающей стороны будет указано в параметре `hostname` лога.

7.7. Настройка системы сигнализации на основе nagios

Главной задачей системы мониторинга является оповещение администратора безопасности, о том, что поведение наблюдаемых объектов изменилось. Также оповещения должны отсылаться, когда состояние объекта возвращается в норму. Nagios позволяет использовать в качестве инструмента оповещения программы, разработанные пользователями.

Система сигнализации состоит из сервера мониторинга (управляющей машины) и удаленных узлов с датчиками мониторинга (управляемые машины).

На управляющей машине должны работать:

- nagios – осуществляет наблюдение, оповещение администратора, контроль состояния узлов, сервисов. (см. п. 7.7.1 и п. 7.7.3);
- apache2 – позволяет использовать веб-браузер для управления интерфейсом nagios, nagiosdigger;
- nagstamon (п. 7.7.5) – это монитор состояний и управлений отслеживаемых узлов, сервисов;
- nagiosdigger – это веб-интерфейс ведения журналов, производимых nagios.

На управляемых машинах должны работать:

- nagwad – осуществляет мониторинг journald и генерирует предупреждение на основе сообщений журнала (см. п. 7.7.2);
- nagios-nrpe – это агент мониторинга nagios, позволяющий запускать плагины на наблюдаемых хостах (см. п. 7.7.2).

7.7.1. Настройка сервера мониторинга

7.7.1.1. Установка пакета nagios

В качестве сервера мониторинга (управляющей машины) используется ОС Альт СП Рабочая станция с установленной группой пакетов «Рабочее место контролера событий безопасности».

Группа пакетов «Рабочее место контролера событий безопасности» включает в себя установку следующих пакетов: nagios-full, nagios-www-apache2, nagios-addons-nrpe, nagwad-templates, nagwad-actions, apache2-mod_ssl, nagiosdigger, perl-DBD-mysql.

Группа пакетов «Датчики системы сигнализации» включает в себя установку пакетов: nagwad и nagios-npre.

7.7.2. Настройка удаленных узлов (клиенты)

Расширение NRPE предназначено для выполнения плагинов Nagios на удаленных машинах. Основная задача – позволить Nagios контролировать «локальные» ресурсы (например, загрузку процессора, использование памяти) на удаленных машинах. Поскольку эти ресурсы обычно не подвергаются воздействию внешних машин, то на удаленных машинах должен быть установлен агент, такой как NRPE (рис. 66).

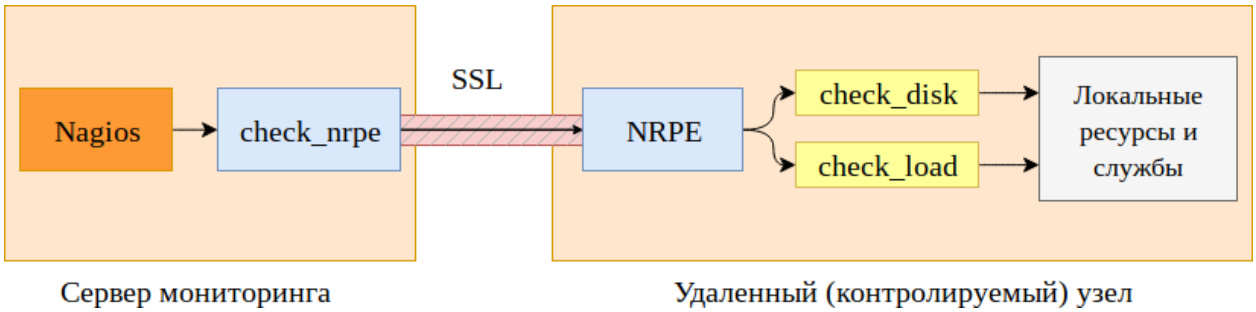


Рис. 66 – Взаимодействие сервера мониторинга с удаленным узлом

На удаленном хосте, за которым нужно наблюдать, установить пакеты группы «Датчики системы сигнализации» (вариант исполнения Рабочая станция) nagwad и nagios-nrpe, и добавить их в автозагрузку:

```
# apt-get install nagwad
# apt-get install nagios-nrpe
```

1) Привести к указанному виду содержимое конфигурационного файла `/etc/audit/rules.d/50-nagwad.rules`:

```
-w /etc/passwd -p wa -k usergroup-change
-w /etc/group -p wa -k usergroup-change

# blacklist
-a always,exit -S execve -F exit=-EACCES -F perm=x -F success=0 -F uid=0 -F key=blacklistau
-a always,exit -S execve -F exit=-EPERM -F perm=x -F success=0 -F uid=0 -F key=blacklistau
-a always,exit -S execve -F exit=-EACCES -F perm=x -F success=0 -F uid=<указать_UID_нужного_пользователя> -F key=blacklistau
-a always,exit -S execve -F exit=-EPERM -F perm=x -F success=0 -F uid=<указать_UID_нужного_пользователя> -F key=blacklistau
```

Примечания:

1. При добавлении дополнительных правил в файл учитывайте архитектуру системы (`arch`), см. примеры правил аудита в документе «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03».

2. Для каждого пользователя (UID) нужно создавать отдельные правила или можно указать, например, `uid>=500` для отслеживания действий всех пользователей системы с UID удовлетворяющим значению.

2) В директорию `/etc/nagwad/` добавить конфигурационный файл `audit.regexp` со следующим содержимым:

```
open-eacces
open-eperm
exec-eacces
exec-eperm
```

3) В директорию `/etc/nagwad/` добавить конфигурационный файл `blacklist.regexp` со следующим содержимым:

```
blacklistau
```

4) В конфигурационном файле `/etc/cups/cups-files.conf` установить:

```
AccessLog syslog
```

А в главном конфигурационном файле `/etc/cups/cupsd.conf` повысить уровень сообщений о нарушении доступа с `warn` до `info`:

```
LogLevel info
```

Затем в этом же файле ограничить доступ к операциям печати, например, разрешив их конкретному пользователю:

```
<Limit Create-Job Print-Job Print-URI Validate-Job>
  Require user имя-пользователя
  Order deny,allow
</Limit>
```

Подробнее о написании политик доступа к печати см. https://www.cups.org/doc/policies.html.

5) Содержимое файла `/etc/nagios/nrpe-commands/nagwad.cfg` привести к следующему виду:

```
command[check_audit]=/usr/lib/nagios/plugins/check_nagwad 'audit'
command[check_authdata]=/usr/lib/nagios/plugins/check_nagwad 'authdata'
command[check_login]=/usr/lib/nagios/plugins/check_nagwad 'login'
command[check_devices]=/usr/lib/nagios/plugins/check_nagwad 'device'
command[check_print]=/usr/lib/nagios/plugins/check_nagwad 'print'
command[check_osec]=/usr/lib/nagios/plugins/check_osec
command[check_blacklist]=/usr/lib/nagios/plugins/check_nagwad 'blacklist'
```

Файл конфигурации NRPE содержит несколько определений команд, которые можно использовать для мониторинга этой машины. Можно редактировать определения команд, добавлять новые команды и т. д. редактируя конфигурационный файл NRPE с помощью текстового редактора.

`command[check_audit]=/usr/lib/nagios/plugins/check_nagwad` – для сигнализации о попытках НСД к защищаемой в ОС информации о попытках несанкционированного запуска программ пользователями ОС.

`command[check_authdata]=/usr/lib/nagios/plugins/check_nagwad` – для сигнализации о попытках несанкционированного изменения полномочий пользователей в ОС, а также изменения, добавления и удаления учетных данных пользователей.

`command[check_blacklist]=/usr/lib/nagios/plugins/check_nagwad` – для сигнализации о попытках несанкционированного запуска программ пользователями ОС.

`command[check_osec]=/usr/lib/nagios/plugins/check_osec` – для сигнализации о нарушении целостности КСЗ и (или) объектов контроля целостности нужно, предварительно настроить подсистему контроля целостности osec.

`command[check_devices]=/usr/lib/nagios/plugins/check_nagwad` – для сигнализации о попытках подключения к СВТ незарегистрированных устройств ввода-вывода информации или о попытках ввода/вывода информации с/на неучтенные устройства ввода-вывода, в том числе съемные носители информации.

Службы, которые используют команды из файла `/etc/nagios/nrpe-commands/nagwad.cfg`, прописаны в `/etc/nagios/templates/50-nagwad.cfg` (пакет nagwad-templates, вариант исполнения Рабочая станция).

6) IP-адрес сервера мониторинга Nagios нужно добавить в файл конфигурации `/etc/nagios/nrpe.cfg` – измените следующие строки:

```
server_address=0.0.0.0
allowed_hosts=192.168.7.100 #сервер мониторинга с Nagios
```

7) В файле `/etc/nagios/send_nsca.cfg` установить:

```
host_address=192.168.7.100 #сервер мониторинга с Nagios
```

8) В файл `/etc/pam.d/system-auth` заменить строку:

```
auth    include    system-auth-common
```

- для блокировки пользователя без возможности разблокирования учетной записи через время (разблокировать может только root) на строку:

  ```
  auth    required    pam_faillock.so authfail deny=4 audit
  ```

- для установки времени разблокировки учетной записи, например, через 100 с на строку:

  ```
  auth    required    pam_faillock.so    authfail    deny=4
  unlock_time=100 audit
  ```

9) Добавить службы в автозапуск, используя следующие команды:

```
systemctl enable osec.timer
systemctl enable nagwad
systemctl enable xinetd
systemctl enable nrpe
```

10) Перезагрузить ОС.

Лог событий хранится в `/var/log/nagwad/`.

7.7.3. Добавление удаленных узлов для мониторинга (сервер)

Для добавления удаленных узлов, на сервере мониторинга (управляющая машина, на которой работает nagios):

- установить пакет для БД, далее в настройках используется пакет mariadb-server (вариант исполнения ОС Альт СП Сервер);
- создать определения узла и служб nagios для мониторинга удаленного хоста;
- создать определение nagios для использования плагина check_nrpe.

Прежде чем контролировать службу, сначала нужно определить хост, который связан с этой услугой. Можно поместить определения хостов в любом конфигурационном файле объекта, указанном в директиве `cfg_file` или помещенном в каталог, указанный в директиве `cfg_dir`. Лучше создать новый шаблон для каждого типа узла, который планируется контролировать.

Добавление удаленных узлов для мониторинга выполняется в следующей последовательности:

1) Для каждого наблюдаемого узла в директории `/etc/nagios/objects` нужно создать его конфигурационный файл. Например, для узла `nagios-node`, имеющего IP-адрес 192.168.7.100, нужно создать файл `/etc/nagios/objects/nagios-node.cfg` со следующим содержимым:

```
define host {
    host_name   nagios-node
    use         linux-server
    alias       nagios-node
    address     192.168.7.100
    hostgroups  nagwad-nodes
}
```

При необходимости можно выбрать другое имя файла. Критически важным является указание `hostgroups nagwad-nodes`.

Все проверки, которые обеспечивает пакет nagwad и описаны в шаблоне `/etc/nagios/templates/50-nagwad.cfg` будут выполняться именно для этой группы хостов.

После того, как определение было добавлено для узла, который будет контролироваться, нужно определить службы, которые должны контролироваться, на этом узле. Как и определения хостов, определения служб могут быть помещены в любой конфигурационный файл объекта.

В `/etc/nagios/templates/50-nagwad.cfg` для мониторинга на удаленном узле, например, для отслеживания попыток несанкционированного запуска программ пользователями ОС:

```
define service {
    name                blacklist-event
    hostgroup_name      nagwad-nodes
    use                 generic-service
    service_description blacklist_whitelist
    check_command       check_nrpe!check_blacklist
}
```

где:

- `blacklist-event` – имя проверки;
- `blacklist_whitelist` – описание проверки;
- `check_blacklist` – имя файла-паттерна для поиска событий.

Примечание. В дальнейшем, при добавлении новых событий для отслеживания осуществляйте на сервере мониторинга перезагрузку сервиса: `systemctl restart nagios`.

Запустить службу mariadb командой `systemctl start mariadb`. Далее подключиться к СУБД командой `mysql` и ввести следующие команды:

```
CREATE DATABASE nagiosdigger;
EXIT;
```

Будет создана БД для хранения статистики нарушений с именем nagiosdigger. Затем ввести следующую команду (оболочки):

```
cat /usr/share/doc/nagiosdigger-0.9/create_tables_mysql.sql | mysql -B nagiosdigger
```

где `0.9` – пример версии nagiosdigger.

После ее выполнения в БД nagiosdigger будут созданы все таблицы.

Следом, нужно снова подключиться к СУБД командой `mysql` и ввести следующие команды:

```
GRANT INSERT,SELECT ON nagiosdigger.logs TO nagioslogs@localhost
IDENTIFIED BY 'пароль';
FLUSH PRIVILEGES;
EXIT;
```

указав в качестве пароля желаемый пароль для доступа к БД статистики нарушений.

Для того, чтобы собирающее статистику нарушений ПО имело возможность чтения и записи статистики нарушений, использованный при конфигурации БД пароль нужно прописать в конфигурационный файл `/etc/nagios/nagiosdigger/config.ini` (строка `dbi_pass`).

Включить копирование записей о событиях в БД, записав в конфигурационный `/etc/nagios/nagios.cfg` строку:

```
global_service_event_handler=nagiosdigger-service-handler
```

1) Импортировать в БД статистику нарушений, имеющуюся в журнале Nagios, ввести команду:

```
cat /var/log/nagios/nagios.log | sort | nagiosdigger-import
```

2) Добавить службы в автозапуск, используя следующие команды:

```
systemctl enable xinetd
systemctl enable mariadb
systemctl enable nagios
systemctl enable httpd2
```

3) Для обеспечения удаленного доступа пользователя root на наблюдаемые узлы, выполнить от его имени следующие команды (предварительно на управляемой машине должны быть выполнены команды `echo “PermitRootLogin yes” >> /etc/openssh/sshd_config` и `service sshd restart`):

```
ssh-keygen  # однократно
ssh-copy-id <IP_адрес_узла> # для каждого наблюдаемого узла
```

4) Запустить программу Nagstamon (см. п. 7.7.5), нажать на кнопку «Создать сервер», в появившемся диалоговом окне ввести параметры для доступа к локальному серверу Nagios. По умолчанию установлен пароль nagios; поменять его можно с помощью команды:

```
htpasswd /etc/nagios/nagios.web-users <имя_пользователя>
```

и ввести новый пароль.

5) В настройках программы Nagstamon выбрать «Actions» и установить «Connection method» в положение «IP resolved by hostname».

6) В настройках программы Nagstamon выбрать «Actions/New action», задать тип действия «Command», имя `NSCA_shell` и команду:

```
xvt -- ssh -t root@$ADDRESS$ -- nsca-shell \"$SERVICE$\"
```

Там же добавить еще одну команду с именем `Lock_host` и команду:

```
ssh root@$ADDRESS$ -- /bin/openvt -wfs -- vlock -a
```

7) Перезагрузить ОС.

8) Для удаления сигнализации события, нужно на управляемой машине перенести содержимое `/var/log/nagwad/<имя_события>` в `/var/log/nagwad/<имя_события>.archived/`.

7.7.4. Тестирование системы мониторинга

Нужно убедиться, что плагин `check_nrpe` может обмениваться данными с демоном NRPE на удаленном узле:

```
/usr/lib/nagios/plugins/check_nrpe -H 192.168.7.101
```

где `192.168.7.101` – IP-адрес удаленного хоста, на котором установлен NRPE.

Если плагин возвращает ошибку, нужно проверить следующее:

- между удаленным узлом и сервером мониторинга нет межсетевого экрана, который блокирует связь;
- демон NRPE правильно установлен и запущен на удаленном узле;
- на удаленном узле нет правил локального брандмауэра, которые не позволяют подключаться серверу мониторинга.

Проверить состояние сигнализатора на управляемом узле можно, выполнив на нем через ssh команду:

```
# systemctl status nagwad
```

Проверить конфигурационные файлы Nagios можно командой:

```
# /usr/sbin/nagios -v /etc/nagios/nagios.cfg
```

Исправьте ошибки, если они есть. Если ошибок нет, перезапустите Nagios:

```
# systemctl restart nagios
```

В течение нескольких минут Nagios должен получить текущую информацию о состоянии удаленной машины.

После запуска служб можно проверить работу Nagios Core веб-сервером. Для этого в адресной строке веб-браузера введите адрес:

```
localhost/nagios
```

Если все настроено верно, после ввода аутентификационных данных (по умолчанию nagios/nagios) будет загружена начальная страница Nagios (рис. 67). На странице Host Detail будут показаны узлы, за которыми ведется наблюдение и их состояние (рис. 68).

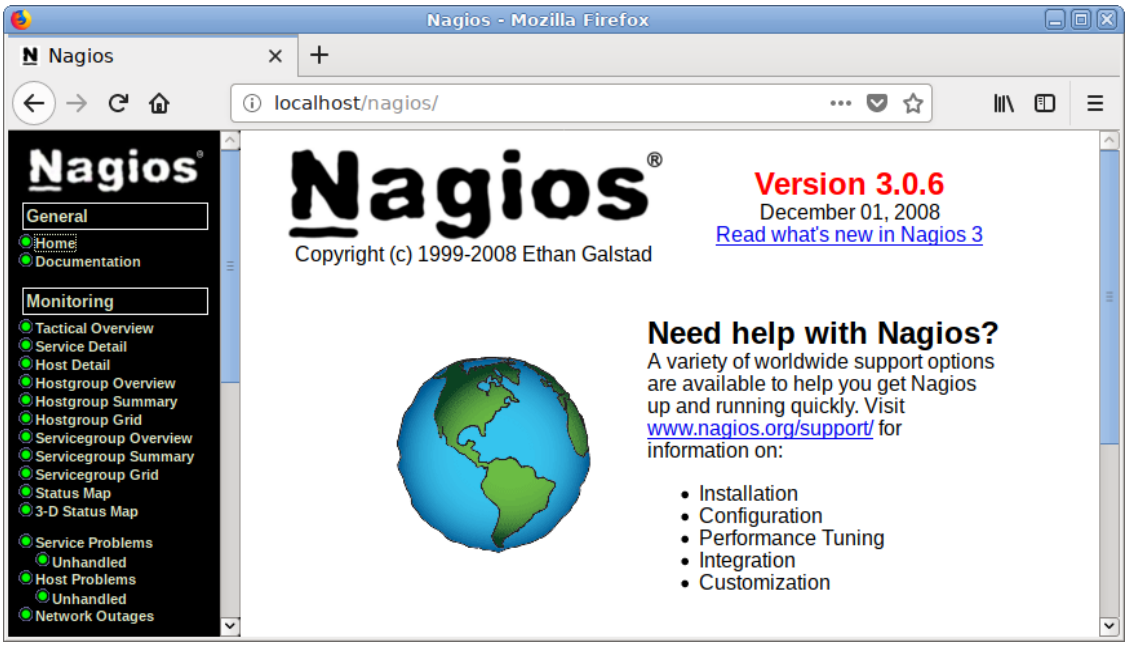


Рис. 67 – Работа с Nagios в веб-браузере

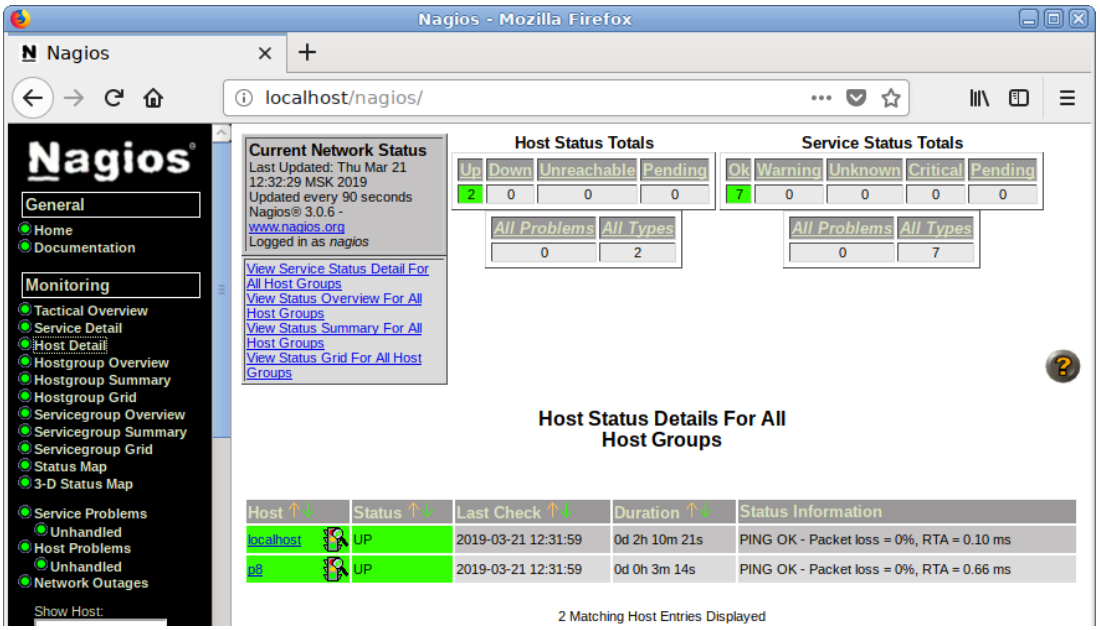


Рис. 68 – Список узлов

7.7.5. Nagstamon

Nagstamon – утилита, которая может подключаться к серверам мониторинга, например, к nagios, для того, чтобы обеспечить в режиме реального времени информацию о состоянии узлов и служб. Nagstamon в виде небольшой настраиваемой строчки может висеть в любом месте экрана, отображая количество проблем в сети. Детальный список проблем можно получить при наведении на нее мышкой.

Пакет nagstamon (входит в состав варианта исполнения Рабочая станция, если он еще не установлен) следует установить на сервере мониторинга:

```
# apt-get install nagstamon
```

При первом запуске Nagstamon («Приложения» → «Системные» → «Nagstamon») появляется диалоговое окно, в котором нужно настроить хотя бы один монитор для проверки (рис. 69):

- тип сервера мониторинга: Nagios;
- URL-адрес главной страницы монитора: `http://localhost/nagios/`;
- URL-адрес монитора CGI: `http://localhost/nagios/`;
- имя пользователя: nagios;
- пароль: nagios;

- прокси (Use proxy), если нужно.

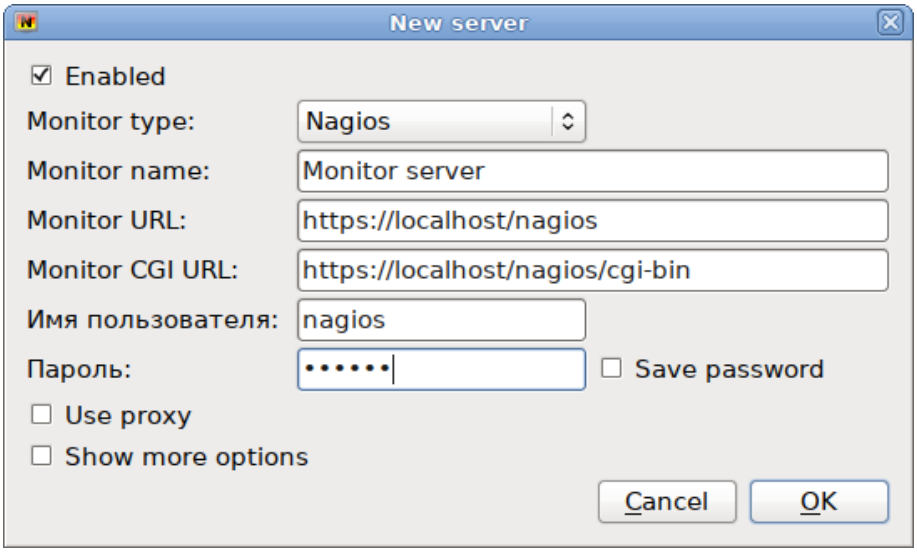


Рис. 69 – Настройка сервера мониторинга

Каталог `config` по умолчанию находится в `$HOME/.nagstamon`.

Nagstamon находится на рабочем столе в виде перемещаемой строки состояния или полноэкранного режима, где представлено краткое описание (рис. 70) критических, предупреждающих, неизвестных, недостижимых и недоступных узлов и сервисов. При касании указателем мыши уведомления, выводится подробный отчет о состоянии (рис. 71). Пользователи также могут получать звуковые сигналы.

Рис. 70 – Уведомление о критической ошибке

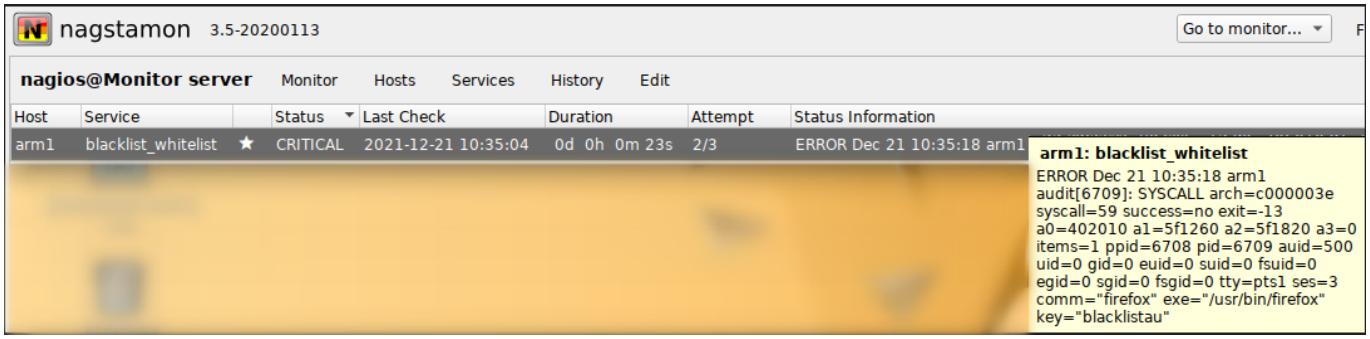


Рис. 71 – Просмотр отчета об ошибке

Nagstamon позволяет пользователю определять действия, предпринимаемые для отказавших узлов и служб. Также есть встроенные действия:

- Monitor – открыть страницу узла/службы в веб-интерфейсе монитора;
- Recheck – снова проверить состояние узла/службы;
- Acknowledge – позволяет признать проблему с узлом/службой;
- Downtime – позволяет настроить обслуживание службы/узла.

С удаленными узлами и службами можно устанавливать соединение через SSH, RDP, VNC или выполнить любые самоопределяемые действия.

В качестве примера создать действие, которое будет проверять доступность узла, командой `ping`. Для этого из контекстного меню выбрать пункт «Edit action» (Редактировать действие) (рис. 72). В открывшемся окне нужно нажать на кнопку «New action…» (Новое действие).

Существует три типа действий:

- Browser – открыть веб-браузер с определенным URL-адресом;
- Command – вызов внешней команды с некоторыми связанными аргументами;
- URL – вызывать любой URL в фоновом режиме с аргументами, например, действие CGI.

Команды и URL-вызовы могут быть построены с использованием некоторых переменных-заполнителей.

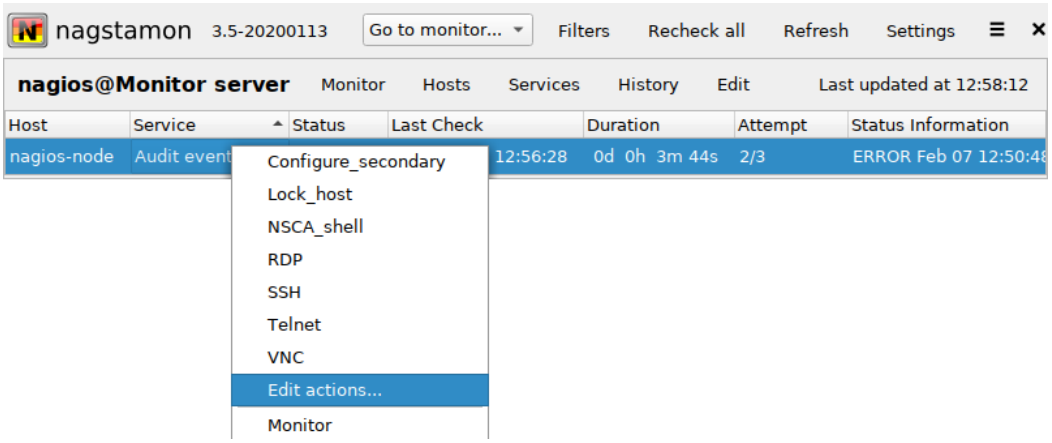


Рис. 72 – Контекстное меню Nagstamon

Регулярными выражениями можно отфильтровать узлы и службы, чтобы меню действий оставалось как можно более удобным. Для сохранения изменений нужно нажать на кнопку «OK».

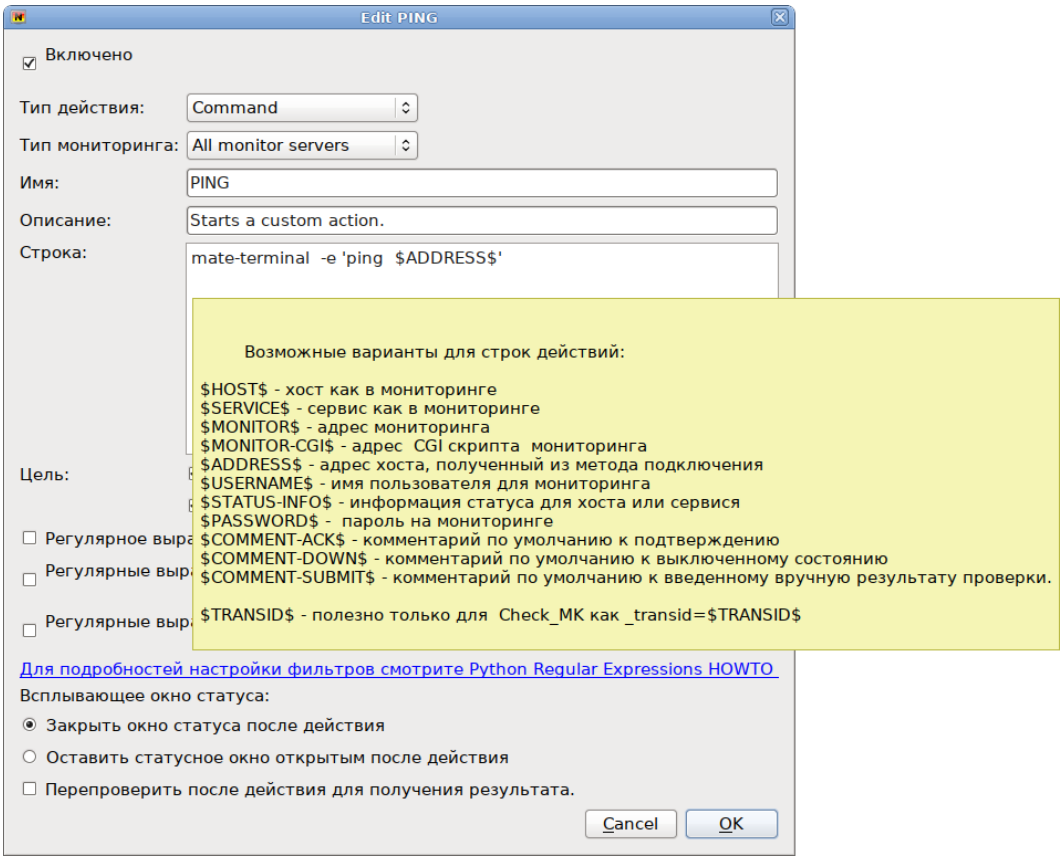


Рис. 73 – Добавление нового действия

7.8. ГОСТ в OpenSSL

7.8.1. Поддержка шифрования по ГОСТ в OpenSSL

Для включения поддержки шифрования ГОСТ в OpenSSL нужно выполнить следующие действия:

1) установить пакет:

```
# apt-get install openssl-gost-engine
```

2) изменить конфигурационный файл OpenSSL, выполнив команду:

```
# control openssl-gost enabled
```

3) проверить, доступны ли шифры ГОСТ для OpenSSL:

```
$ openssl ciphers|tr ':' '\n'|grep GOST
GOST2012-GOST8912-GOST8912
GOST2001-GOST89-GOST89
```

7.8.2. Создание ключей

Пример генерации закрытого ключа с алгоритмом ГОСТ-2012:

```
$ openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:TCA -out ca.key
```

Пример создания сертификата на 365 дней (`ca.cer`):

```
$ openssl req -new -x509 -md_gost12_256 -days 365 -key ca.key -out ca.cer \
-subj "/C=RU/ST=Russia/L=Moscow/O=SuperPlat/OU=SuperPlat CA/CN=SuperPlat CA Root"
```

Проверка сертификата (`ca.cer`):

```
$ openssl x509 -in ca.cer -text -–noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            70:66:39:34:7b:4b:55:52:89:64:83:66:1c:63:ff:fb:90:2e:2e:3b
        Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)
        Issuer: C = RU, ST = Russia, L = Moscow, O = SuperPlat, OU = SuperPlat CA, CN = SuperPlat CA Root
        Validity
            Not Before: Jun 15 10:08:24 2020 GMT
            Not After : Jun 15 10:08:24 2021 GMT
        Subject: C = RU, ST = Russia, L = Moscow, O = SuperPlat, OU = SuperPlat CA, CN = SuperPlat CA Root
        Subject Public Key Info:
            Public Key Algorithm: GOST R 34.10-2012 with 256 bit modulus
                Public key:
                   X:24529B83573322D0F2B5A75DD20D31DCD3B84AA7E69AF5035E228AC46705798A
                   Y:3E4F9142B640EBCAA8C76A6EE13B431E452337ADC10E52D3E4D3E8C9745AAE16
                Parameter set: GOST R 34.10-2012 (256 bit) ParamSet A
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                BD:E6:E8:74:62:82:EE:F1:9F:FE:C1:48:73:A1:F3:0B:E0:4C:D2:0F
            X509v3 Authority Key Identifier:
                keyid:BD:E6:E8:74:62:82:EE:F1:9F:FE:C1:48:73:A1:F3:0B:E0:4C:D2:0F

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)
         2d:6c:71:78:da:fe:9c:70:75:81:82:c5:4e:1e:10:19:8a:bb:
         9f:12:6a:02:6c:d5:12:43:20:3e:01:4f:b1:a2:13:ba:44:11:
         b5:e6:9d:82:49:98:f5:24:49:c4:fb:ff:a2:ea:18:0a:72:57:
         d7:7b:cc:6a:66:0b:d8:7e:2a:10
```

8. СРЕДСТВА УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ, ОРГАНИЗАЦИЯ СЕТЕВОЙ ИНФРАСТРУКТУРЫ С ПОМОЩЬЮ СЕРВЕРА

Последующие пункты рекомендуются к прочтению опытным пользователям и системным администраторам.

8.1. Вход в систему

Для начала работы по настройке системы сразу после ее установки, нужно использовать веб-ориентированный интерфейс ЦУС (см. п. 7.1.2), позволяющий управлять выбранным компьютером с любого другого в сети.

8.2. Развертывание офисной ИТ-инфраструктуры

8.2.1. Подготовка

Перед началом развертывания офисной ИТ-инфраструктуры нужно провести детальное планирование. Конкретные решения в каждом случае будут продиктованы спецификой требований, предъявляемых к офисной ИТ-инфраструктуре. При этом важно понимать принципы взаимодействия компьютеров в сети и роль каждого конкретного компьютера: главный сервер, подчиненный сервер или компьютер-клиент (рабочее место).

Ключевым понятием для работы сети, построенной на базе ОС Альт СП, является домен.

8.2.2. Домен

Под доменом понимается группа компьютеров с разными ролями. Каждый сервер обслуживает один домен – группу компьютеров одной сети, имеющую единый центр и использующую единые базы данных для различных сетевых служб.

С помощью домена можно:

- вести централизованную базу пользователей и групп;
- аутентифицировать пользователей и предоставлять им доступ к сетевым службам без повторного ввода пароля;

- использовать единую базу пользователей для файлового сервера, прокси-сервера, веб-приложений;
- автоматически подключать файловые ресурсы с серверов, анонсированных по Zeroconf;
- использовать тонкие клиенты, загружаемые по сети и использующие сетевые домашние каталоги;
- аутентифицировать пользователей как на «ALT-домен», так и на Microsoft Windows.

Примечание. Не следует путать это понятие с другими доменами: почтовыми доменами, доменными именами (DNS), Windows-доменами.

8.2.3. Сервер, рабочие места и аутентификация

Важно понимать роль, которая будет отводиться ОС Альт СП в домене. Именно сервер (например, под управлением ОС Альт СП Сервер) будет являться центральным звеном сети, контролируя доступ к ресурсам сети и предоставляя различные службы для клиентских машин. Все службы, предоставляемые серверами, используются рабочими местами.

Таким образом, можно выделить:

1) Сервер (компьютер под управлением ОС Альт СП Сервер).

   Сервер осуществляет контроль доступа к ресурсам сети, содержит централизованную базу данных пользователей и удостоверяющий центр для выдачи сертификатов службам на серверах и рабочих местах.

2) Рабочее место.

   Рабочие места – это клиентские, по отношению к серверам, компьютеры, непосредственно использующиеся для работы пользователей.

   Наибольший эффект от использования ОС Альт СП Сервер достигается при использовании его вместе с рабочими местами под управлением ОС Альт СП Рабочая станция. Они уже содержат все нужное для интеграции в сеть с ОС Альт СП Сервер, в качестве рабочих мест могут использоваться и другие ОС, возможно, на стороне компьютера-клиента потребуется дополнительная настройка.

Для доступа к ресурсам сети (например, общим файлам, расположенным на сервере, либо получения доступа в сеть Интернет) пользователю, работающему на клиентском компьютере, нужно авторизоваться на сервере – ввести свои данные (имя и пароль). После проверки аутентификации главным сервером, пользователь получает определенный администратором домена объем прав доступа к ресурсам сети.

3) Авторизация.

Типичный пример – офисное рабочее место, постоянно находящееся в локальной сети. В этом случае аутентификация в домене происходит непосредственно в момент регистрации пользователя на рабочем месте (с доменными аутентификационными данными).

Рабочие места под управлением ОС Альт СП Рабочая станция позволяют легко настроить такой способ аутентификации. Для этого в ЦУС (раздел «Аутентификация» см. п. 8.4.5) на рабочей станции, нужно выбрать домен, управляемый ОС Альт СП Рабочая станция.

8.3. Развертывание доменной структуры

Для развертывания доменной структуры предназначен модуль ЦУС «Домен» из раздела «Система» (пакет alterator-net-domain).

Модуль поддерживает следующие виды доменов:

1) ALT-домен – домен, основанный на OpenLDAP и MIT Kerberos. Рекомендуется для аутентификации рабочих станций под управлением дистрибутивов ALT. Домен нужно устанавливать только после настройки сервера DHCP. В противном случае придется выбирать другое имя домена;
2) Active Directory – домен для контроллера домена Samba AD. Рекомендуется для аутентификации рабочих станций под управлением и Windows и Linux (см. п. 10.2);
3) FreeIPA – домен для контроллера домена FreeIPA. Рекомендуется для аутентификации рабочих станций под управлением Linux (см. п. 12);

4) DNS – обслуживание только запросов DNS указанного домена сервисом Bind (см. п. 13) (рис. 74).

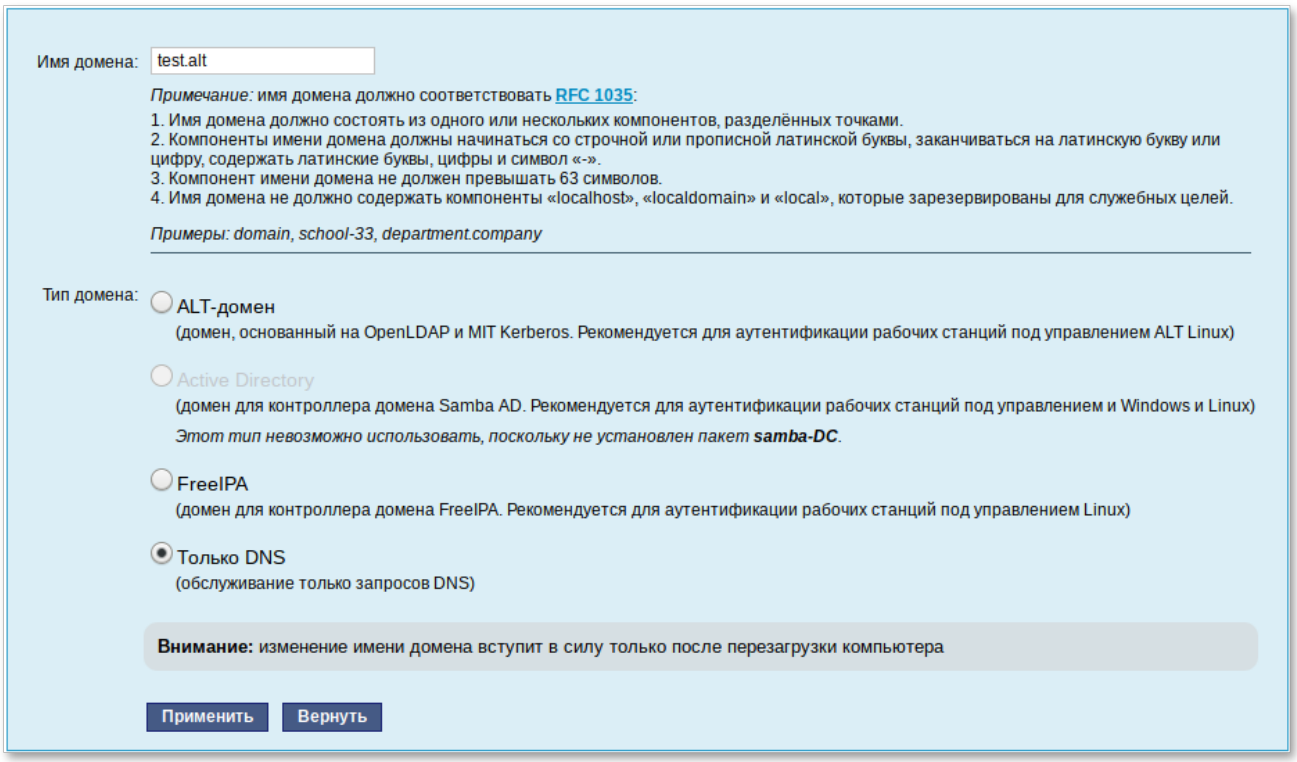


Рис. 74 – Виды доменов

8.4. Централизованная база пользователей

Основной идеей домена является единая база учетных записей. При такой организации работы пользователям требуется лишь одна единственная учетная запись для доступа ко всем разрешенным администратором сети ресурсам. Наличие в сети единой централизованной базы пользователей позволяет значительно упростить работу, как самих пользователей, так и системных администраторов.

8.4.1. Создание учетных записей пользователей

Централизованная база пользователей создается на главном сервере. Наполнить ее учетными записями можно воспользовавшись модулем ЦУС «Пользователи» (пакет alterator-ldap-users) из раздела «Пользователи» (рис. 76).

Для выбора источника данных о пользователях, нужно нажать на кнопку «Выбор источника», выбрать источник и нажать на кнопку «Применить» (рис. 75).

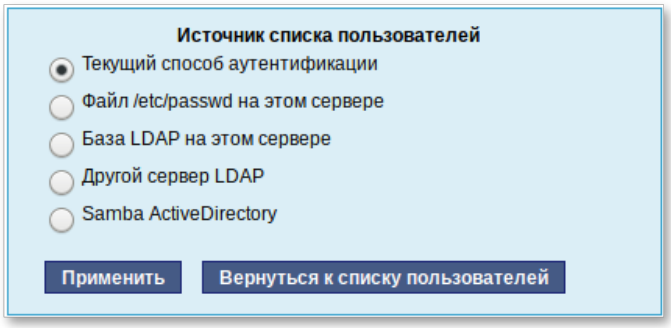


Рис. 75 – Источник списка пользователей

Возможные варианты источника данных о пользователях:

- текущий метод аутентификации (выбирается в модуле «Аутентификация» см. п. 8.4.5);
- файл `/etc/passwd` (выбран по умолчанию);
- локальная база LDAP;
- база LDAP на другом сервере;
- локальная база Samba DC.

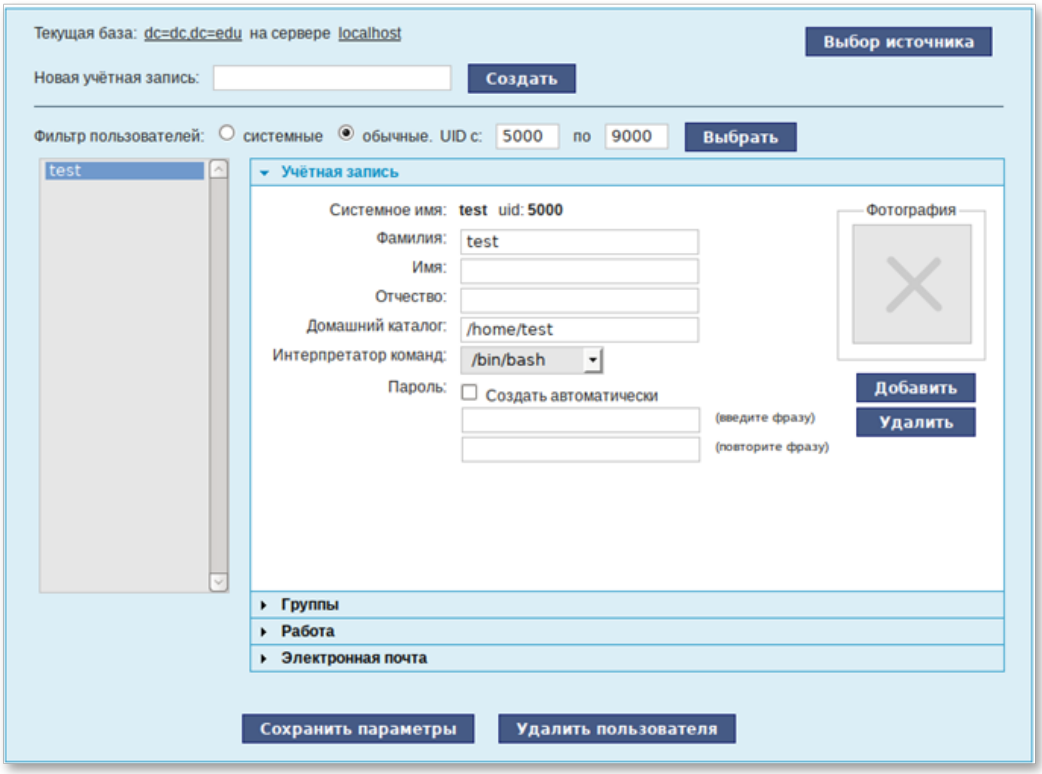


Рис. 76 – Создание учетной записи пользователя в модуле «Пользователи»

Для создания новой учетной записи нужно ввести имя новой учетной записи и нажать на кнопку «Создать», после чего имя отобразится в списке слева. Для дополнительных настроек нужно выделить существующую учетную запись, выбрав ее из списка. Список доступных полей зависит от выбранного источника данных о пользователях.

После создания учетной записи пользователя не забудьте присвоить учетной записи пароль. Этот пароль и будет использоваться пользователем для регистрации в домене. После этого на рабочих местах под управлением ОС Альт СП Рабочая станция, на которых для аутентификации установлен этот домен, можно вводить это имя пользователя и пароль.

8.4.2. Объединение пользователей в группы

Пользователи могут быть объединены в группы. Это может быть полезно для более точного распределения полномочий пользователей. Например, члены группы wheel могут получать полномочия администратора на локальной машине, выполнив команду:

```
$ su -
```

Настройка групп производится в модуле ЦУС «Группы» (пакет alterator-ldap-groups) из раздела «Пользователи». С помощью данного модуля можно (рис. 77):

- просматривать актуальный список групп и список пользователей, входящих в каждую группу;
- создавать и удалять группы;
- добавлять и удалять пользователей в существующие группы;
- привязывать группу к системным группам и группам Samba.

Для выбора источника списка групп, нажмите кнопку «Выбор источника» (рис. 77) и выберите источник (рис. 78).

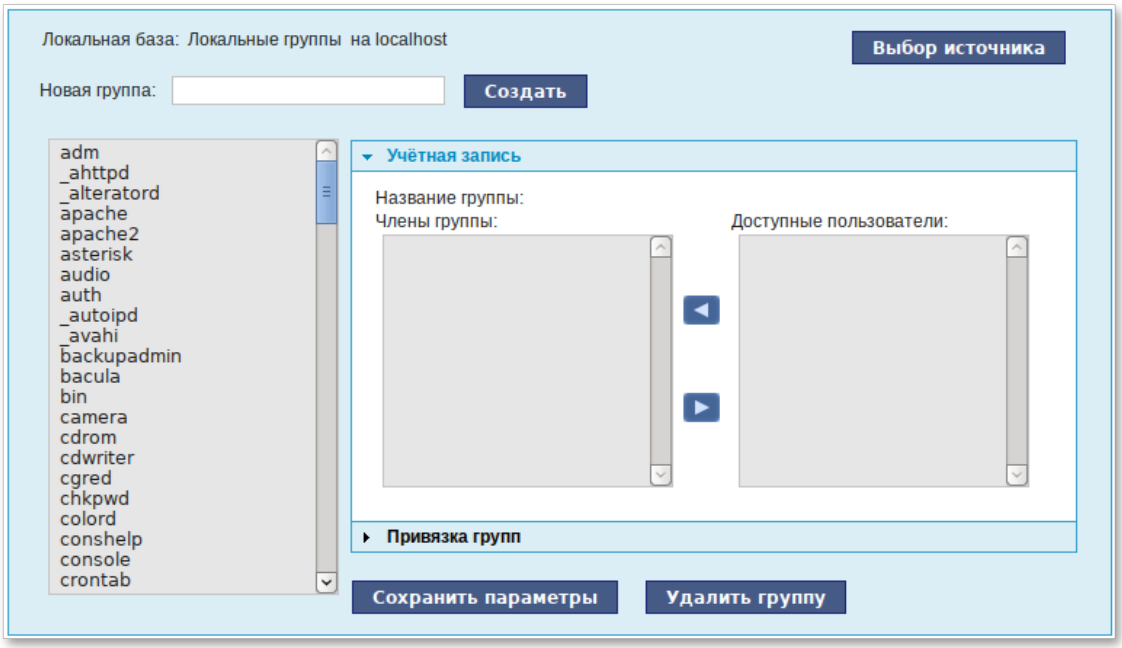


Рис. 77 – Локальная база. Выбор источника

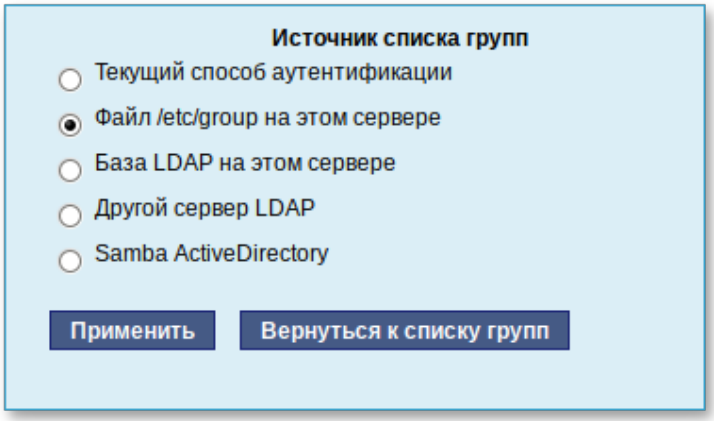


Рис. 78 – Источник списка групп

Возможные варианты источника данных о пользователях:

- текущий метод аутентификации (выбирается в модуле «Аутентификация» см. п. 8.4.5);
- файл `/etc/group` (выбран по умолчанию);
- локальная база LDAP;
- база LDAP на другом сервере;
- локальная база Samba DC.

Для создания новой группы нужно ввести название группы и нажать на кнопку «Создать», после чего имя отобразится в списке слева.

8.4.3. Настройка учетной записи

Во вкладке «Учетная запись» (модуль ЦУС «Группы» пакет alterator-groups) можно настроить принадлежность учетной записи группам (рис. 79).

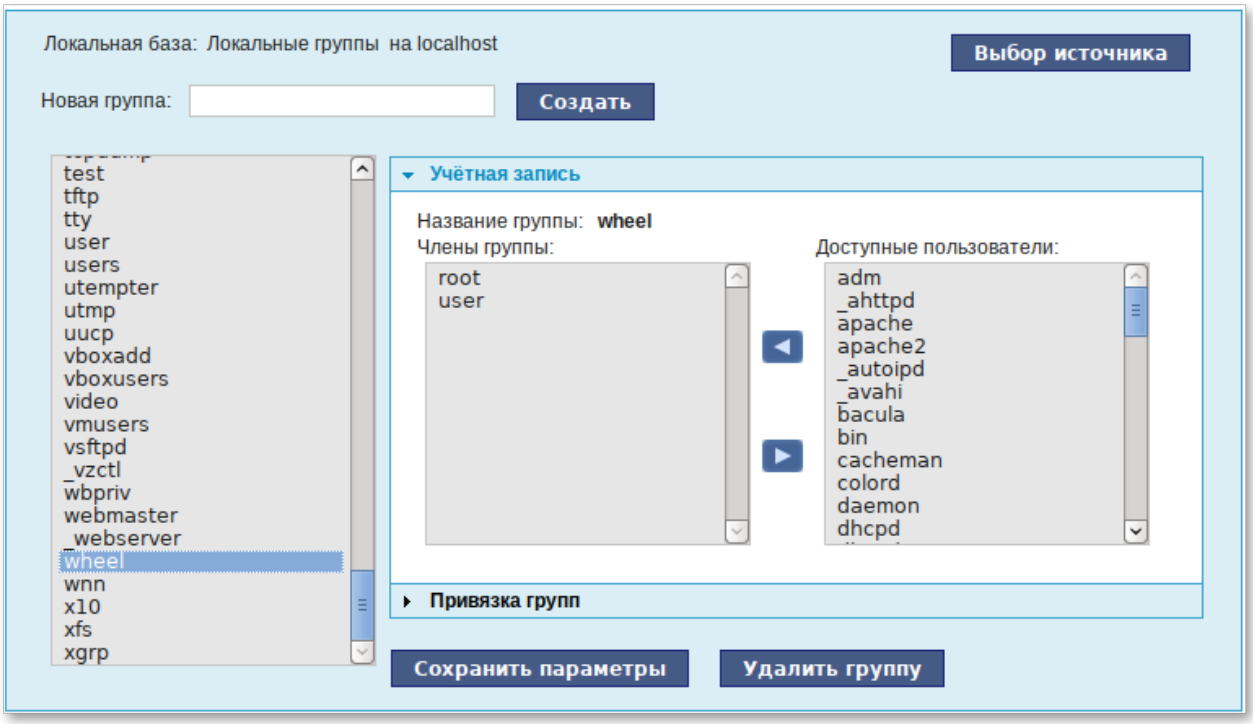


Рис. 79 – Локальная база. Учетная запись

Для этого нужно в списке групп выделить группу, к которой нужно добавить (удалить) пользователей. В списке «Члены группы» отображается информация о членах выделенной группы. В списке «Доступные пользователи» отображается список пользователей системы. Для включения пользователя в группу нужно выбрать пользователя в списке «Доступные пользователи» и нажать на кнопку ◀. Для исключения пользователя из группы нужно выбрать пользователя в списке «Члены группы» и нажать на кнопку ▶.

8.4.4. Привязка групп

Во вкладке «Привязка групп» (модуль ЦУС «Группы») можно привязать группу к системной группе или к группе Samba (рис. 80).

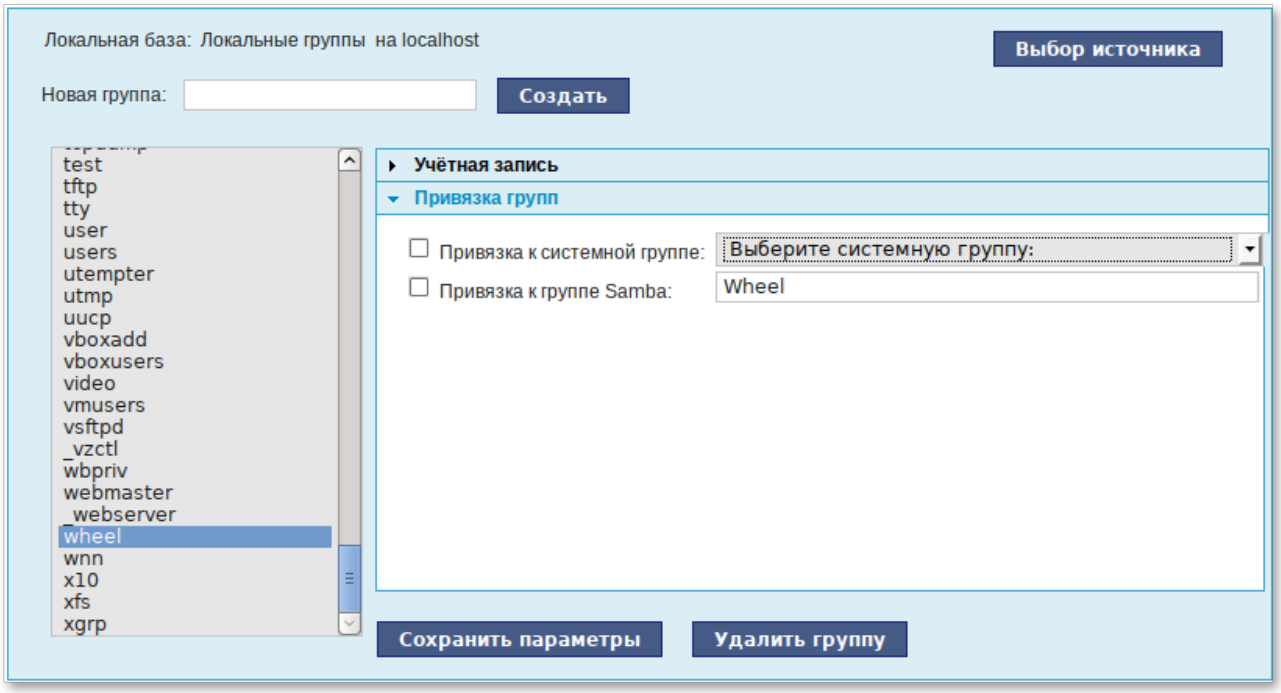


Рис. 80 – Локальная база. Привязка групп

Привязка к системной группе позволяет включать доменных пользователей в системные группы при регистрации на рабочей станции.

Примечание. Некоторые системные группы на сервере и на рабочей станции имеют разные идентификаторы (GID). Проверьте GID используемых системных групп на сервере и на рабочих станциях (в файле `/etc/group`).

8.4.5. Настройка рабочей станции

Настройка рабочих станций для использования централизованной аутентификации производится в ЦУС (графический интерфейс) в разделе «Аутентификация» (пакет alterator-auth) (рис. 81).

После выбора домена (см. п. 8.2.2), для полного вступления изменений с силу нужно перезагрузить систему.

После перезагрузки у пользователя появится возможность авторизоваться с использованием централизованной аутентификации.

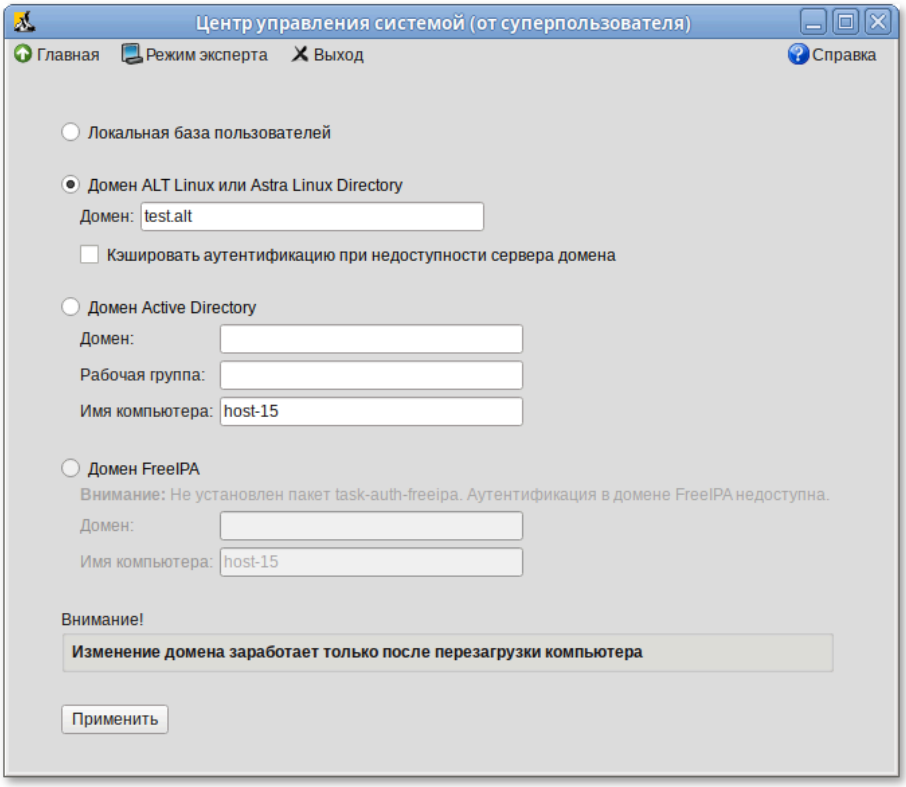


Рис. 81 – Центр управления системой

8.5. Настройка подключения к Интернету

Помимо множества различных служб, которые ОС Альт СП 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 – 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 сервера, так и для настройки общего выхода в Интернет для компьютеров сети нужно настроить подключение к Интернету на самом сервере.

ОС Альт СП поддерживает самые разные способы подключения к сети Интернет:

- Ethernet (см. п. 8.5.1);
- PPTP (см. п. 8.7.4);
- PPPoE (см. п. 8.7.4);
- и т. д.

Для настройки подключения можно воспользоваться одним из разделов ЦУС «Сеть»:

- Ethernet-интерфейсы (см. п. 8.5.1);
- PPTP-соединения;
- PPPoE-соединения;
- OpenVPN-соединения (см. п. 8.11.2).

8.5.1. Конфигурирование сетевых интерфейсов

Конфигурирование сетевых интерфейсов осуществляется в модуле ЦУС «Ethernet-интерфейсы» (пакет alterator-net-eth) из раздела «Сеть» (рис. 82).

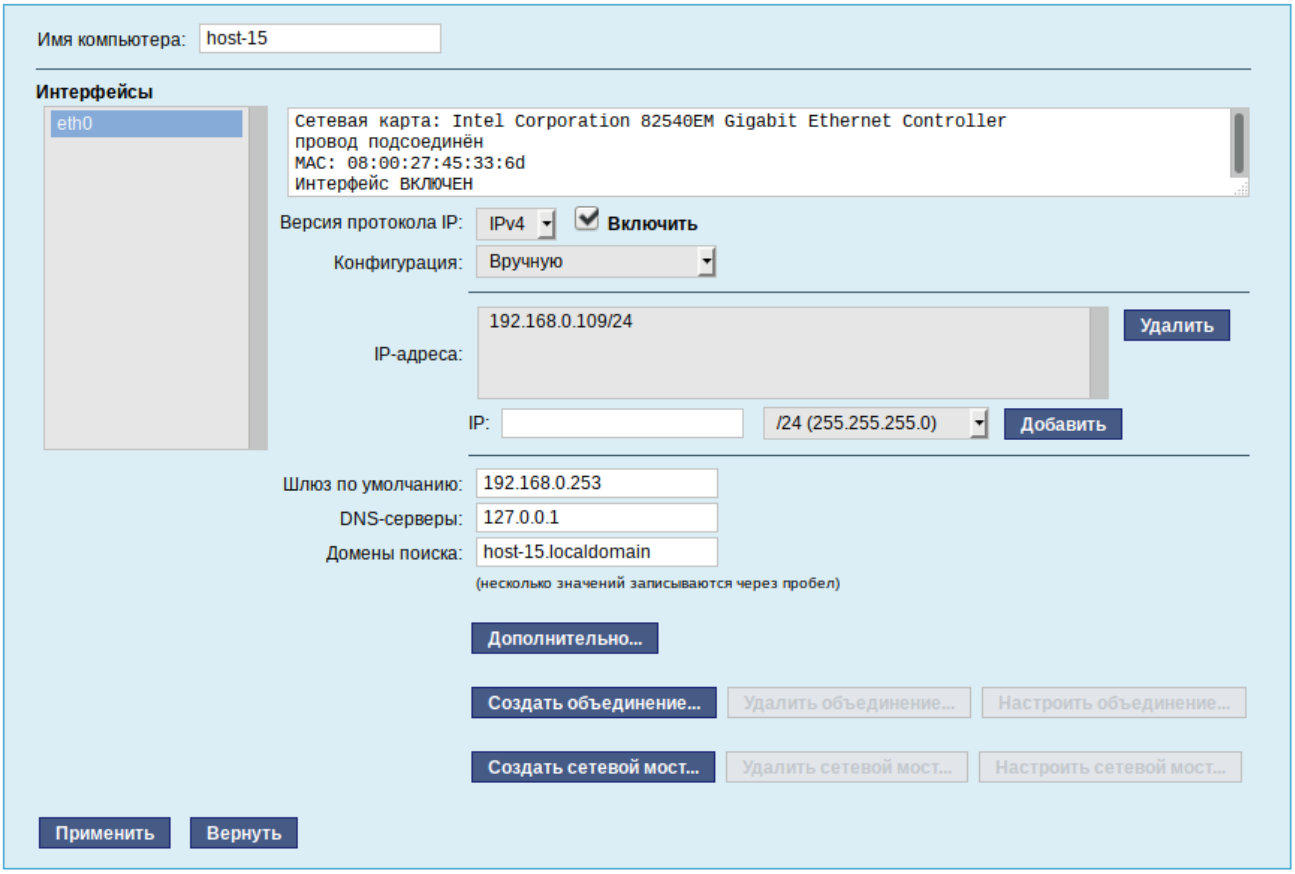


Рис. 82 – Настройка модуля «Ethernet-интерфейсы»

В модуле «Ethernet-интерфейсы» можно заполнить следующие поля:

- «Имя компьютера» – указать сетевое имя ПЭВМ 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 «IP», выбранные адреса можно удалить нажатием кнопки «Удалить»;
- «IP» – ввести IP-адрес вручную и выбрать в выпадающем поле предпочтительную маску сети, затем нажать на кнопку «Добавить» для переноса адреса в пул поля «IP-адреса»;
- «Шлюз по умолчанию» – в поле для ввода нужно ввести адрес шлюза, который будет использоваться сетью по умолчанию;
- «DNS-серверы» – в поле для ввода нужно 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 нужно ввести список предпочтительных доменов, по которым будет выполняться поиск.

«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 нужно указать параметр «Шлюз по умолчанию».

В случае наличия DHCP-сервера (см. п. 8.5.3) можно все вышеперечисленные параметры получить автоматически – выбрав в списке «Конфигурация» пункт «Использовать DHCP» (рис. 83).

Если в компьютере имеется несколько сетевых карт, то возможна ситуация, когда при очередной загрузке ядро присвоит имена интерфейсов (eth0, eth1) в другом порядке. В результате интерфейсы получат не свои настройки. Чтобы этого не происходило, можно привязать интерфейс к имени по его аппаратному адресу (MAC) или по местоположению на системной шине.

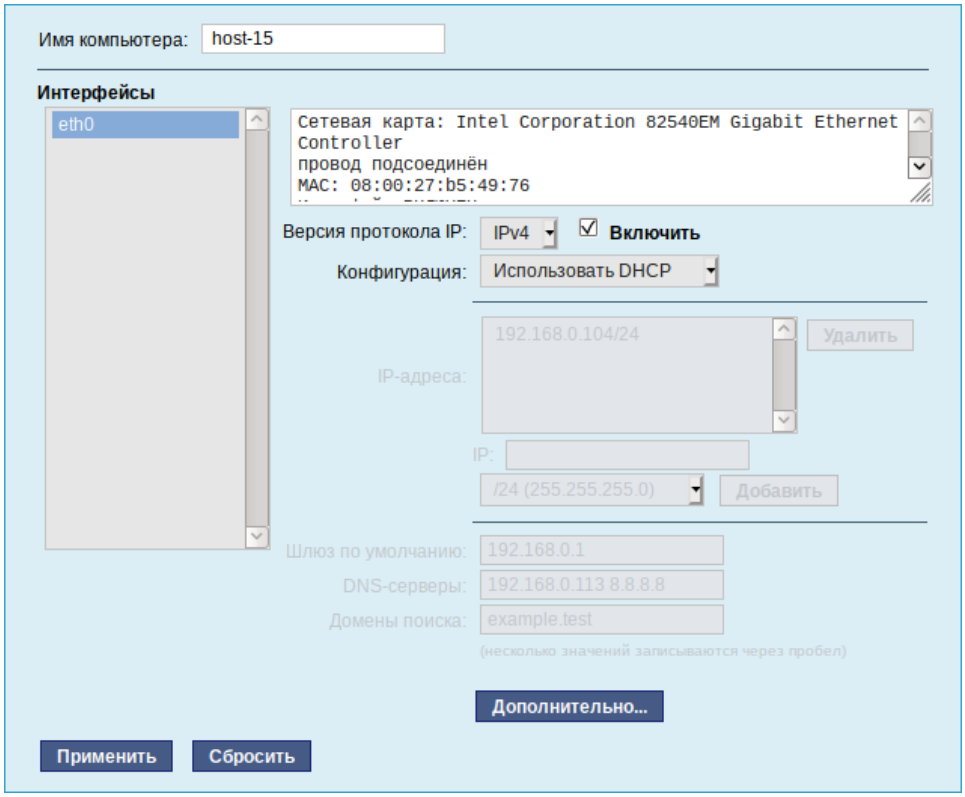


Рис. 83 – Автоматическое получение настроек от DHCP-сервера

Дополнительно для каждого интерфейса можно настроить сетевую подсистему (NetworkManager, Etcnet), а также должен ли запускаться данный интерфейс при загрузке системы (рис. 84).

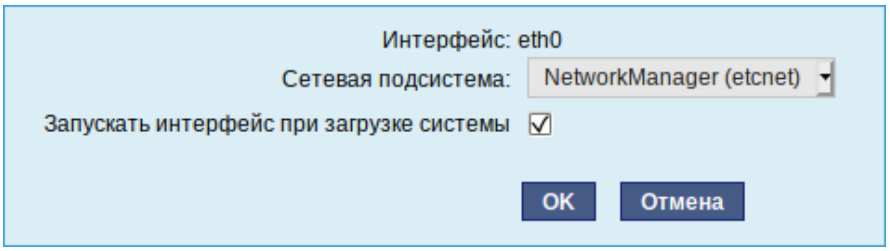


Рис. 84 – Выбор сетевой подсистемы

В списке «Сетевая подсистема» (рис. 84) 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 передается NetworkManager и не зависит от файлов Etcnet. Управлять настройками можно через графический интерфейс NetworkManager. Файлы с настройками находятся в директории /etc/NetworkManager/system-connections. Этот режим особенно актуален для задач настройки сети на клиенте, когда IP-адрес нужно 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;
- Не контролируется – в этом режиме интерфейс находится в состоянии DOWN (выключен).

8.5.2. 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 (п. 8.5.2.1);
- использование NAT (п. 8.5.2.2).

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

8.5.2.1. 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 – отдает 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 специальная настройка рабочих станций не потребуется. 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 веб-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 веб-браузерах местоположение формы настройки на прокси-сервер различное.

По умолчанию прокси-сервер не предоставляет доступ в Интернет никому кроме себя самого. Список сетей, обслуживаемых прокси-сервером можно изменить, нажав на кнопку «Разрешенные сети…» в модуле ЦУС «Прокси-сервер» (пакет alterator-squid) из раздела «Серверы» (рис. 85).

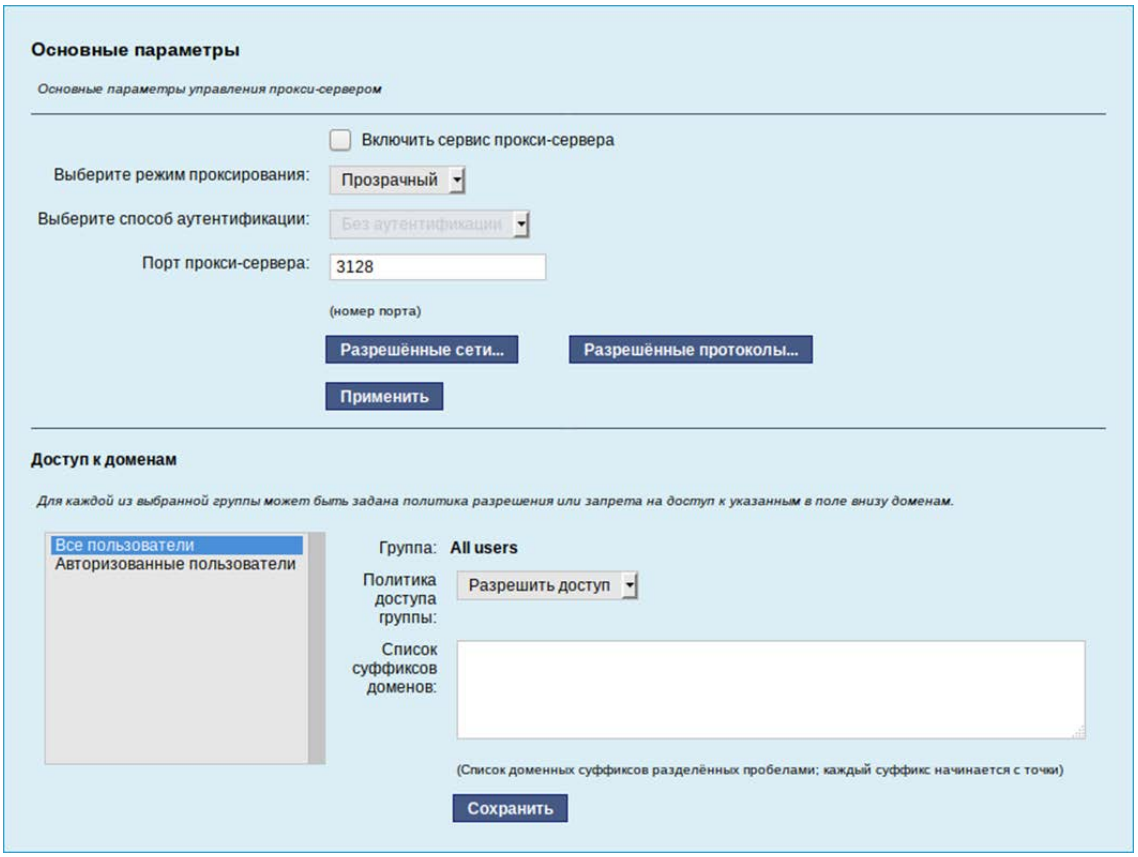


Рис. 85 – Модуль «Прокси-сервер»

Примечание. См. также описание настроек прокси-сервера Squid в п. 8.13.

Для того чтобы включить аутентификацию пользователей и контролировать их доступ во внешнюю сеть, нужно выбрать обычный режим проксирования и способ аутентификации, отличный от «Без аутентификации» (рис. 86).

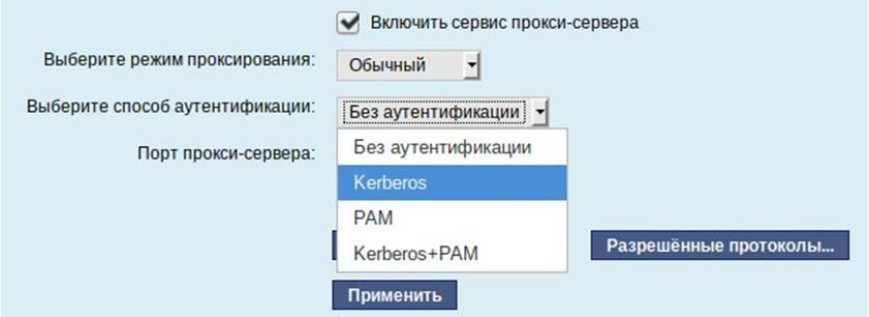


Рис. 86 – Настройка аутентификации пользователей

Прокси-сервер принимает запросы из локальной сети и, по мере нужности, передает их во внешнюю сеть. Поступление запроса ожидается на определенном порту, который по умолчанию имеет стандартный номер `3128`. Если по каким-то причинам нежелательно 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, нужно добавить соответствующую группу адресов (адрес подсети и адресную маску) в список внутренних сетей в разделе «Разрешенные сети» (рис. 87).

Вторым условием передачи запроса является принадлежность целевого порта к разрешенному диапазону. Посмотреть и отредактировать список разрешенных целевых портов можно в разделе «Разрешенные протоколы» (рис. 88).

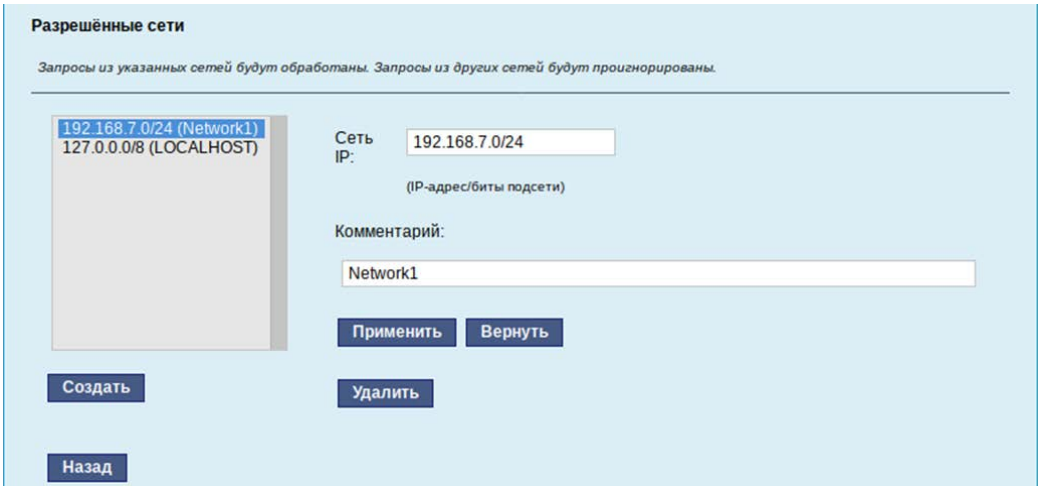


Рис. 87 – Настройка списка внутренних сетей

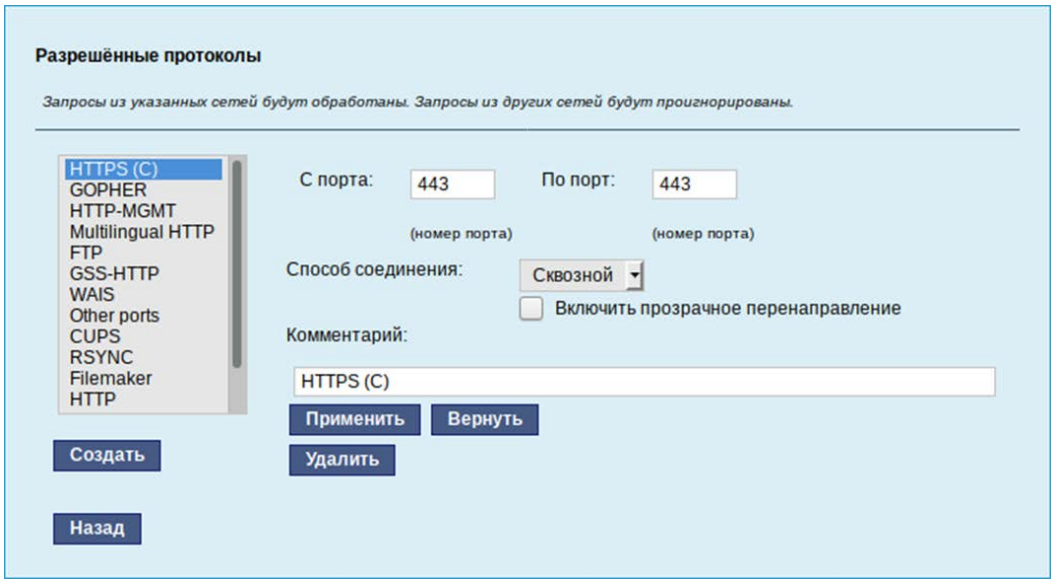


Рис. 88 – Настройка списка разрешенных целевых портов

Прокси-сервер позволяет вести статистику посещений страниц в Интернете. Она доступна в модуле ЦУС «Прокси-сервер» (пакет alterator-squidmill) в разделе «Статистика» (п. 8.16). Основное предназначение статистики – просмотр отчета об объеме полученных из Интернета данных в привязке к пользователям (если включена аутентификация) или к IP-адресам клиентов.

Примечания:

1. Статистика не собирается по умолчанию. Включить ее сбор следует в модуле ЦУС «Прокси-сервер» (раздел «Статистика» п. 8.16). Для этого отметьте «Включить сбор данных прокси-сервера» и нажмите кнопку «Применить».

2. Для учета пользователей в статистике нужно добавить хотя бы одно правило, например, запрет не аутентифицированных пользователей. Только после этого в статистике появятся пользователи.

8.5.2.2. 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 сети Интернет (общий внешний IP-адрес). При этом на компьютере-шлюзе, непосредственно подключенном к сети Интернет, выполняется преобразование адресов.

Настройка NAT осуществляется в модуле ЦУС «Внешние сети» (пакет alterator-net-iptables) из раздела «Брандмауэр» (см. п. 8.15.1). Для минимальной настройки достаточно выбрать режим работы Шлюз (NAT), отметить правильный внешний сетевой интерфейс (рис. 89) и нажать на кнопку «Применить».

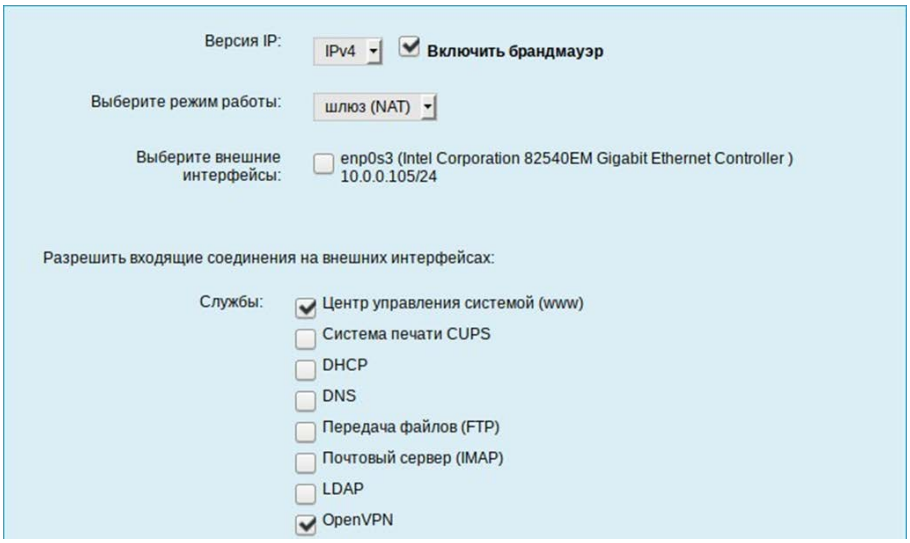


Рис. 89 – Настройка NAT в модуле «Внешние сети»

8.5.3. 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).

Чтобы настраивать DHCP-сервер, на машине должен быть хотя бы один статически сконфигурированный Ethernet-интерфейс (см. п. 8.5.1).

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

Для включения DHCP-сервера нужно установить флаг «Включить службу DHCP» (рис. 90), указать начальный и конечный IP-адрес, а также шлюз по умолчанию (обычно, это IP-адрес сервера на сетевом интерфейсе, обслуживающем локальную сеть).

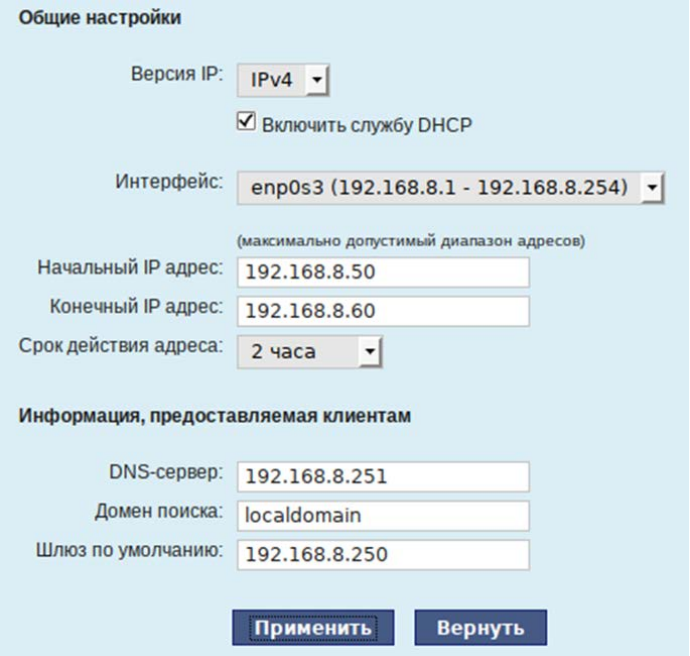


Рис. 90 – Настройка модуля DHCP-сервер

Теперь при включении любой клиентской машины с настройкой «получение IP и DNS автоматически» будет присваиваться шлюз `192.168.8.250`, DNS `192.168.8.251` и адреса начиная с `192.168.8.50` по порядку включения до `192.168.8.60`.

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 следует ввести IP-адрес и соответствующий ему MAC-адрес и нажать на кнопку «Добавить» (рис. 91).

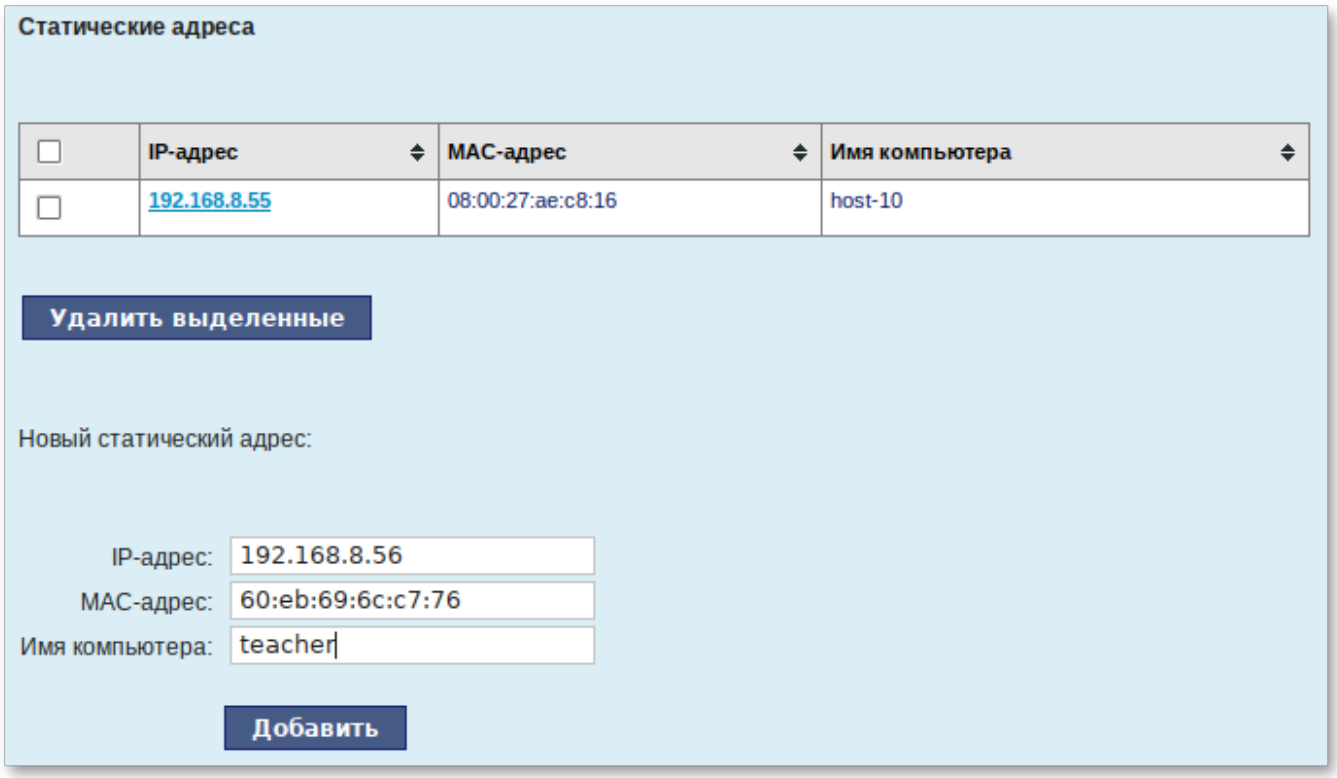


Рис. 91 – Привязка IP-адреса к MAC-адресу

Выданные IP-адреса можно увидеть в списке «Текущие динамически выданные адреса» (рис. 92). Также имеется возможность зафиксировать выданные адреса, за данными компьютерами. Для этого нужно отметить хост, за которым нужно закрепить IP-адрес и нажать на кнопку «Зафиксировать адрес для выбранных компьютеров».

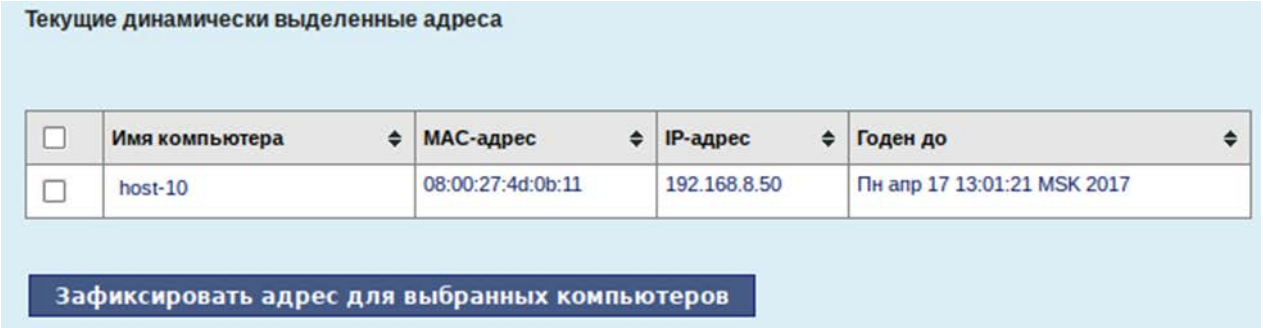


Рис. 92 – Список динамически выданных адресов

8.6. Настройка сети – NetworkManager

Программа NetworkManager (рис. 93) позволяет подключаться к различным типам сетей: проводные, беспроводные, мобильные, VPN и DSL, а также сохранять эти подключения для быстрого доступа к сети, чтобы в дальнейшем подключиться автоматически.

При нажатии левой кнопкой мыши на значок NetworkManager в трее, появится меню, в котором можно выбрать одну из доступных Wi-Fi сетей и подключиться к ней. Из этого меню так же можно отключить активное Wi-Fi соединение.

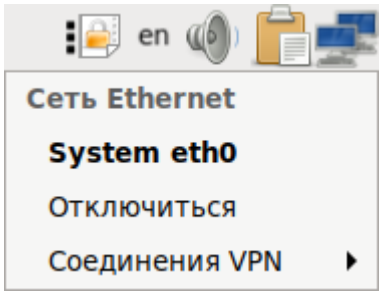


Рис. 93 – Меню NetworkManger при нажатии левой кнопки мыши

При нажатии правой кнопкой мыши на значок NetworkManager (рис. 94), появится меню, из которого можно получить доступ к изменению некоторых настроек, также можно узнать версию программы, посмотреть сведения о соединении, изменить соединения (например, удалить Wi-Fi сеть, чтобы не подключаться к ней автоматически).

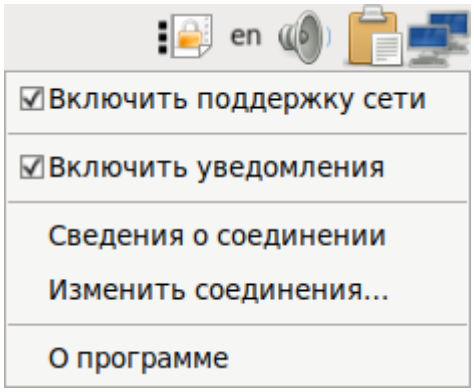


Рис. 94 – Меню NetworkManger при нажатии правой кнопки мыши

8.7. Настройка сети – набор пакетов `/etc/net`

Набор пакетов `/etc/net` – это система конфигурации сети в ОС семейства Linux, которая позволяет администратору произвести настройки сети.

8.7.1. Устройство `/etc/net`

`/etc/net` интегрирован в ОС Альт СП в виде пакетов:

- etcnet – базовые сценарии;
- etcnet-full – виртуальный пакет с зависимостями на все пакеты, которые могут использоваться сценариями `/etc/net`, с указанием их точных версий;
- etcnet-defaults-desktop – умолчания для рабочей станции;
- etcnet-defaults-server – умолчания для сервера.

Переменные sysctl в ОС Альт СП конфигурируются в следующих местах:

- `/etc/sysctl.conf` (глобальные системные);
- `/etc/net/sysctl.conf` (общие сетевые в /etc/net);
- `/etc/net/ifaces/*/sysctl.conf*` (частные для конкретных интерфейсов или их типов в `/etc/net`).

8.7.1.1. Организация опций `/etc/net` по умолчанию

Методология работы `/etc/net` предусматривает несколько шагов наследования опций, первый из которых – загрузка опций по умолчанию. Для их хранения предназначен каталог `/etc/net/options.d`, из которого будут последовательно прочитаны все файлы. В этом каталоге содержится файл `/etc/net/options.d/00-default`, содержащий значения по умолчанию, а также файл `/etc/net/options.d/50-ALTLinux-server` со специфичными для дистрибутива значениями.

Для изменения набора функций по умолчанию допускается создать файл с еще более высоким номером и определить настройки умолчания для своей системы. В результате такого подхода:

- не изменяются файлы с опциями, принадлежащие пакету. Это делает обновление пакета намного более корректным;
- можно легко увидеть, какие опции переопределяются на каждом этапе.

8.7.1.2. Интерфейсы lo, default и unknown

Сразу после установки пакета etcnet в каталоге `/etc/net/ifaces` (в котором хранятся конфигурации интерфейсов) создаются три каталога:

- lo;
- default;
- unknown.

Интерфейс lo – стандартная «петля» (loopback), которая должна быть во всякой Linux-системе, поэтому конфигурация для него включена по умолчанию. В остальном он ничем не отличается от любого другого интерфейса и конфигурируется точно так же файлами `options` и `ipv4address`.

Интерфейс `default` – специальный каталог, файлы в котором обрабатываются следующим образом:

- `resolv.conf` – если присутствует, то копируется в `/etc/resolv.conf`;
- `options` – файл опций, читается после опций по умолчанию;
- `options-<вид интерфейса>` – файл содержит опции, специфичные для данного вида интерфейсов. Некоторые из них не обязательны и позволяют использовать особенности данного вида интерфейсов, например, LINKDETECT в options-eth; другие обязательны;
- `sysctl.conf-<вид интерфейса>` – файл с переменными sysctl, которые нужно изменить. Файл `sysctl.conf-dvb` отключает `return path filter`, что нужно в случае асимметричной маршрутизации;
- `iplink-<вид интерфейса>` – файл с командами iplink, специфичными для данного вида;
- `selectprofile` – если этот файл исполняемый, то он будет вызван из сценариев ifup/ifdown, setup/shutdown для того, чтобы вернуть на стандартном выводе имя профиля, которое нужно использовать. Это позволяет автоматически переключать профили в зависимости от каких-либо условий. В поставку включен пример сценария: `/etc/net/scripts/contrib/selectprofile`;
- `fw` – каталог с настройками сетевого экрана по умолчанию.

Интерфейс unknown – специальная конфигурация, которая будет использована в том случае, когда /etc/net выполняет настройку hotplug-интерфейса, для которого не существует каталога конфигурации. Она будет работать только в том случае, если включена опция ALLOW_UNKNOWN.

8.7.1.3. Сценарии конфигурации сети и hotplug-интерфейсы

8.7.1.3.1. Сценарии конфигурации сети

Существует несколько сценариев конфигурации сети.

Первый сценарий – выполнение service network start при старте системы или вручную. При этом требуется только сформировать погруппные (потиповые) списки интерфейсов, подлежащих обработке, и последовательно выполнить требуемые действия. Модули ядра при этом загружаются сценариями /etc/net, при этом имена модулей берутся из опции MODULE (в этой опции можно в кавычках перечислить несколько имен, и они будут последовательно загружены). Этот метод часто используется на практике и лучше всего подходит для маршрутизаторов. Преимущество метода в том, что вся информация сконцентрирована в одном месте – каталоге /etc/net. Если опция MODULE не определена, то будет предпринята попытка загрузки по имени интерфейса, подразумевая, что файл /etc/modules.conf заполнен правильно.

Второй сценарий – реакция на событие ifplugd. В части загрузки модуля этот сценарий не отличается от первого.

Третий сценарий – реакция на появление или исчезновение сменного устройства. Для обработки таких событий предназначены сценарии /etc/net/scripts/{ifup,ifdown}-removable, которые вызываются из сценариев пакетов hotplug и pcmcia-cs. Сложность заключается в том, что для сменных PCMCIA-карт вызовы могут дублироваться: для одного и того же события первый раз ifup-removable будет вызван из hotplug, второй – из pcmcia-cs. Кроме того, hotplug также реагирует на загрузку модулей ядра для обычных карт PCI и, более того, включает сценарии, которые пытаются загружать модули самостоятельно.

В этом контексте /etc/net получает слишком много вызовов от hotplug и по

умолчанию их игнорирует (USE_HOTPLUG=no).

8.7.1.3.2. hotplug-интерфейсы

Для настройки сменной карты в файле options нужно задать следующий параметр:

USE_HOTPLUG=yes

После этого /etc/net при получении события от hotplug будет автоматически вызывать управляющий модуль устройства при его подключении и выгружать из памяти в случае отсоединения устройства.

Примечание. Съемные интерфейсы будут пропущены при обычном старте сети, так как их присутствие ОС определяет только после получения вызова от hotplug.

В случае, если нужно вручную расконфигурировать hotplug-интерфейс до его извлечения, допускается использовать команду ifdown. Для повторной конфигурации интерфейса нужно подключить его к ПЭВМ еще раз.

Также существует опция USE_PCMCIA. В случае, если события для интерфейса и карты генерирует демон pcmcia-cs, то нужно ее включить. Также, если события генерируются только hotplug, то рекомендуется использовать опцию USE_HOTPLUG.

8.7.2. Быстрая настройка сетевого интерфейса стандарта Ethernet

Для настройки сетевого интерфейса стандарта Ethernet следует выполнить следующие шаги:

1) узнать имя сетевого интерфейса:

```
$ ip link show
```

Примечание. Если система не загрузила модуль ядра для сетевой карты автоматически, то его следует загрузить вручную. Для определения модуля можно использовать команду lspci. Чтобы загрузить модуль вручную можно использовать команду modprobe, например: modprobe e1000;

2) создать каталог конфигурации интерфейса /etc/net/ifaces/<название интерфейса>, в котором будут храниться файлы с настройками;

3) в каталоге конфигурации сетевого интерфейса создать файл options и записать в этот файл строку:

```
MODULE=<имя модуля>
```

На данном этапе работу с файлом options можно завершить;

4) выяснить, какой IP-адрес должен быть назначен интерфейсу. Если сетевой интерфейс конфигурируется по DHCP), то в файл `/etc/net/ifaces/eth0/options` следует записать строку:

```
BOOTPROTO=dhcp
```

и перейти к шагу 7).

Примечания:

1. В ряде случаев в файле options может понадобиться запись:
   `DHCP_HOSTNAME=<имя машины без домена>`
2. В конце файла options нужно наличие пустой строки.
3. У сетевого интерфейса существуют два взаимосвязанных атрибута:
   - IP-адрес;
   - сетевая маска (mask).

5) текущие значение адреса можно просмотреть командой:

```
$ ip address show
```

Вероятнее всего интерфейс-петля lo (loopback) уже сконфигурирован с адресом 127.0.0.1/8 (что эквивалентно IP-адресу 127.0.0.1 и маске подсети 255.0.0.0). /8 означает длину префикса CIDR (Classless InterDomain Routing). Для задания IP-адреса и маски подсети интерфейса eth0 нужно создать файл `/etc/net/ifaces/eth0/ipv4address`, в который следует записать IP-адрес с длиной маски, например:

```
10.0.0.20/24
```

6) выяснить адрес шлюза (маршрут по умолчанию). Создать файл `/etc/net/ifaces/<название интерфейса>/ipv4route`, в который записать строку:

```
default via <ip-шлюза>
```

7) убедиться, что все выполнено правильно, выполнив команду:

```
# systemctl restart network
```

На данном этапе сетевой интерфейс должен быть успешно сконфигурирован.

В случае, если интерфейс был сконфигурирован с помощью DHCP-сервера, но адрес не был назначен, то следует искать сообщение от DHCP-сервера в файле `/var/log/messages`.

8.7.3. Настройка ifplugd

Для корректного использования ifplugd нужно выполнить команду:

```
# systemctl disable ifplugd
```

Затем назначить переменную USE_IFPLUGD в файлах options соответствующих интерфейсов (/etc/net/ifaces/<имя_интерфейса>/options).

8.7.4. Настройка PPtP-интерфейса и PPPoE-интерфейса

В /etc/net введена опция PPPTYPE для единообразной настройки интерфейсов PPP, PPPoE и PPtP.

PPPTYPE может принимать следующие значения:

- dialup – обычный PPP-интерфейс;
- pppoe – интерфейс PPPoE;
- pptp – интерфейс PPtP.

Для PPPTYPE=pppoe нужно в опции HOST указывать имя Ethernet-интерфейса, через который будет производиться работа PPPoE. В дальнейшем, этот интерфейс будет настраиваться автоматически.

Для PPPTYPE=pptp нужно в опции PPTP_SERVER указывать имя хоста или IP-адрес PPtP-сервера, к которому будет производиться подключение. Кроме того, в большинстве случаев нужно указать в опции REQUIRES интерфейс, через который будет достижим хост, указанный в PPTP_SERVER.

Для настройки PPPoE-соединения нужно выполнить следующие действия:

1) создать каталог конфигурации PPP-интерфейса, например, /etc/net/ifaces/ppp5 (допускается задавать имена PPP-интерфейса вида pppN, pppNN, pppNNN, где N – любая цифра от 0 до 9);
2) создать файл с опциями /etc/net /etc/net/ifaces/ppp5/options следующего содержания:

```
PPPTYPE=dialup
PPPPERSIST=on
PPPMAXFAIL=0
HOST=eth0
```

3) создать файл с опциями `pppd` `/etc/net/ifaces/ppp5/pppoptions` следующего содержания:

```
defaultroute
mtu 1476
usepeerdns
user ppp_username
password ppp_password
nomppe
```

8.7.5. Команды сервиса network

У сервиса network имеется ряд команд:

- start – запустить все стационарные интерфейсы. hotplug-интерфейсы будут сконфигурированы при поступлении соответствующего вызова от hotplug;
- startwith <имя профиля> – старт с указанным именем профиля, а не определенным автоматически;
- stop – остановить все стационарные интерфейсы. hotplug-интерфейсы будут расконфигурированы при поступлении соответствующего вызова от hotplug;
- stopwith <имя профиля> – стоп с указанным именем профиля, а не определенным автоматически;
- restart – эквивалентно «stop» с последующим «start», как и в большинстве других сервисов;
- restartwith <имя профиля> – рестарт в контексте указанного профиля, эквивалентно stopwith <имя профиля> и startwith <имя профиля>;
- switchto <имя профиля> – переключение в указанный профиль, эквивалентно stop и startwith <имя профиля>;
- reload – семантически обозначает «актуализировать текущую конфигурацию». Для всех сконфигурированных в настоящий момент интерфейсов будет выполнена реконфигурация при наличии конфигурации;
- check – автоматическая проверка конфигурационной базы.

8.7.6. Протоколы конфигурации адресов

Опция `BOOTPROTO` позволяет управлять назначением адресов и маршрутов сетевого интерфейса. Управление выполняется с помощью следующих команд:

- static – адреса и маршруты будут взяты из ipv4address/ipv6address и ipv4route/ipv6route;
- dhcp – интерфейс будет сконфигурирован по DHCP;
- dhcp6 – интерфейс будет сконфигурирован по DHCPv6;
- ipv4ll – интерфейс будет сконфигурирован с помощью IPv4LL (link-local), ранее известному как ZCIP (zeroconf IP), это значит, что из сети 169.254.0.0/16 будет подобран еще не использованный адрес и назначен на интерфейс.

Существует несколько комбинированных способов:

- dhcp-static – если конфигурация по DHCP не удалась, конфигурировать методом static;
- dhcp6-static – если конфигурация по DHCPv6 не удалась, конфигурировать методом static;
- dhcp-ipv4ll – если конфигурация по DHCP не удалась, конфигурировать методом ipv4ll;
- dhcp-ipv4ll-static – если конфигурация по DHCP не удалась, конфигурировать методом ipv4ll.

8.7.7. Расширенные возможности `/etc/net`

8.7.7.1. Несколько IP-адресов или маршрутов на одном интерфейсе

В файл `ipv4address` можно помещать произвольное количество IP-адресов по одному адресу на каждой строке. То же самое относится к статическим маршрутам и файлу `ipv4route`.

`/etc/net` не анализирует содержимое этих файлов, а формирует на основе каждой строки командную строку для утилиты ip. Это означает, что можно помещать в этих файлах произвольные поддерживаемые ip опции и они будут обработаны. Например, в файле `ipv4route` можно поместить строку:

```
10.0.1.0/24 via 10.0.0.253 metric 50 weight 5 table 100
```

8.7.7.2. Зависимости между интерфейсами

У интерфейсов vlan, bond, bri, teql входящих в группу зависимых физических, должна быть определена опция `HOST` со списком интерфейсов, которые требуются для инициализации текущего интерфейса. Если хост-интерфейс не сконфигурирован при поднятии зависимого интерфейса, то это будет исправлено.

Кроме обязательной для определенных интерфейсов опции `HOST`, может быть задана и необязательная для всех остальных интерфейсов опция `REQUIRES`. Интерфейсы, перечисленные в этой опции, будут считаться зависимостями текущего интерфейса. Например, по умолчанию попытка сконфигурировать интерфейс А, который зависит от Б и В, приведет сначала к конфигурации Б и В. Аналогично, при расконфигурации Б или В сначала будет расконфигурирован А.

Зависимость одного интерфейса от другого не всегда формальна. Например, в сценарии ifup-pre одного интерфейса может использоваться команда, которая потребует разрешения DNS-имени, которое может быть разрешено только с помощью `resolv.conf`, инсталлируемого другим интерфейсом. Или это может быть PPPoE/PPtP-интерфейс, требующий Ethernet-интерфейс для работы.

8.7.7.3. Пользовательские сценарии post и pre

Существует возможность поместить в каталог конфигурации интерфейса файлы, которые будут выполнены в определенные моменты. Для этого они должны быть исполняемыми и называться следующим образом:

- ifup-pre – для выполнения перед конфигурированием интерфейса;
- ifup-post – для выполнения после конфигурирования интерфейса. Например, можно запустить почтовую систему;
- ifdown-pre – для выполнения перед расконфигурированием интерфейса. Например, можно остановить почтовую систему;
- ifdown-post – для выполнения после расконфигурирования интерфейса.

8.7.7.4. Управление канальными параметрами интерфейсов

Если поместить в конфигурационный каталог интерфейса файл `iplink`, в котором в каждой строке будут записаны команды режима link утилиты ip, то они будут выполнены при конфигурации интерфейса.

Например, если нужно, чтобы интерфейс eth0 имел MAC-адрес `aa:bb:cc:dd:ee:ff` и MTU 200 байт, то в файл `/etc/net/ifaces/eth0/iplink` нужно поместить следующее:

```
address aa:bb:cc:dd:ee:ff
mtu 200
```

8.7.7.5. Управление физическими параметрами интерфейсов

Если поместить в конфигурационный каталог интерфейса файл `ethtool`, в котором будет строка с параметрами программы ethtool, то она будет выполнена при конфигурации интерфейса.

Например, если есть нужность, чтобы интерфейс eth0 имел скорость 10 Мбит/с и авто-согласование скорости было отключено, то в файл `/etc/net/ifaces/eth0/ethtool` нужно поместить следующую строку:

```
speed 10 autoneg off
```

8.7.7.6. Настройка Ethernet-моста

Etcnet использует утилиту brctl для настройки Ethernet-моста (далее – моста). В случае, если интерфейсы, входящие в состав моста, единственные физически подключенные, и настройка моста происходит с удаленного узла через эти интерфейсы, то требуется соблюдать осторожность, поскольку эти интерфейсы перестанут быть доступны.

В случае ошибки в конфигурации, потребуется физический доступ к серверу. Для страховки перед перезапуском сервиса network можно открыть еще одну консоль и запустить там, например, команду:

```
sleep 500 &&reboot
```

Для настройки моста нужно завести каталог `/etc/net/ifaces/<имя_моста>` и создать там файлы со следующими данными:

- brctl:

```
stp AUTO on
```

- ipv4address:

```
192.168.100.200/24
```

- options:

```
TYPE=bri
HOST='eth0 tap0'
BOOTPROTO=static
```

Содержимое файла `brctl` передается утилите brctl. AUTO означает, что скрипт `setup-bri` самостоятельно определит имя bridge-интерфейса.

IP-адрес для интерфейса, будет взят из ipv4address.

В опции `HOST` файла `options` нужно указать те интерфейсы, которые будут входить в мост. Если в него будут входить интерфейсы, которые до этого имели IP-адрес (например, eth0), то этот адрес должен быть удален (например, можно закомментировать содержимое файла `ifaces/eth0/ipv4address`).

При старте сети сначала поднимаются интерфейсы, входящие в мост, затем сам мост (автоматически). Для назначения адреса мосту можно так же использовать DHCP (`BOOTPROTO=dhcp`).

8.7.7.7. Настройка VLAN

Для настройки 802.1q VLAN (например, id 4094 на eth0) следует, создав каталог `ifaces/eth0.4094`, поместить в него файлы со следующим содержимым:

- ipv4address:

```
192.168.100.200/24
```

- options:

```
TYPE=vlan
HOST=eth0
VID=4094
BOOTPROTO=static
```

Содержимое переменных `HOST` и VID будет передано утилите vconfig; использование файла `vlantab` необязательно (и не рекомендуется по причине невозможности использовать ifup для отдельного интерфейса).

Следует обратить внимание, что 4094 является верхней допустимой границей идентификатора валидного VLAN, а 4095 используется технически в процессе

отбрасывания трафика по неверным VLAN. (следует отметить, что это не ограничение Linux: в стандарте под VID отведено 12 бит).

Для настройки Q-in-Q интерфейса, например, `eth0.123.513` (дважды тегированный трафик: внешняя метка – 123, внутренняя – 513) следует файл `options` в каталоге `ifaces/eth0.123.513` заполнить следующим образом:

```
TYPE=vlan
HOST=eth0.123  # «родительский» интерфейс;
VID=513
VLAN_REORDER_HDR=0
BOOTPROTO=static
```

Родительский интерфейс должен быть сконфигурирован (можно с или без BOOTPROTO, с или без ipv4address).

Таким образом, можно каскадировать интерфейсы как «угодно глубоко» (Q-in-Q-in-Q-in-Q...). Нужно только учитывать, что длина имени интерфейса ограничена (16-ю символами).

8.7.7.8. Настройка tun/tap интерфейса

Etcnet поддерживает простое создание интерфейсов типа tun/tap. Это виртуальный тип интерфейсов для передачи пакетов между ядром и программами, который не передает данных через физические устройства. tun – это интерфейс типа point-to-point, работающий с кадрами IP. tap – интерфейс типа ethernet, работающий с кадрами ethernet. Потребуется использование утилиты tunctl, находящейся в одноименном пакете. Пусть требуется создать и настроить tun/tap интерфейс, например, с именем tap0. Для этого:

1) создать каталог интерфейса `/etc/net/ifaces/tap0`;
2) создать в каталоге интерфейса `/etc/net/ifaces/tap0` файл настройки `options` со следующим содержанием:

```
TYPE=tuntap
TUNTAP_USER=combr
```

`TUNTAP_USER` – аккаунт или цифровой id пользователя, которому будут даны права на использование интерфейса tap0 (устройство `/dev/net/tun`). Этот параметр будет передан утилите tunctl как аргумент опции `-u`.

Для создания интерфейса через `/dev/net/tun` требуется привилегия `CAP_NET_ADMIN`. В общем случае, данная привилегия назначена для учетной записи root, и обычный пользователь, имеющий доступ к `/dev/net/tun`, может использовать только уже созданные интерфейсы, к которым разрешен доступ для его UID.

8.7.7.8.1. Настройка и использование IP-туннелей

IP-туннели – средство, позволяющее расширить возможности IP-сетей. Поддерживаются IP-туннели трех видов: IPIP, GRE и SIT.

Каждый вид туннеля по степени сложности организации предназначен для решения задач разных уровней:

- туннели IPIP – самые простые;
- туннели SIT предназначены для транспортировки пакетов IPv6 через сети IPv4;
- туннели GRE (general incapsulation) обычно используются в маршрутизаторах Cisco.

По туннелям типа GRE могут передаваться «broadcast» и «multicast» пакеты. Кроме того, эти туннели поддерживают контрольные суммы и контроль упорядоченности пакетов. Также GRE-туннели обладают опциональным атрибутом key в виде произвольного 4-байтового числа, который позволяет конфигурировать несколько GRE туннелей между одной парой IP-адресов несущей сети (в отличие от IPIP-туннелей, с которыми это невозможно).

Тип туннеля определяется опцией `TUNTYPE` (ipip, gre, sit). По умолчанию `TUNTYPE=ipip`. Кроме типа туннеля для конфигурации всегда требуется адрес удаленного хоста и почти всегда – локальный адрес. Эти адреса определяются опциями `TUNREMOTE` и `TUNLOCAL` соответственно. В некоторых случаях локальный адрес можно не указывать. В этом случае опция `TUNLOCAL` все равно обязательна, но принимает значение any.

Не забудьте назначить туннельному интерфейсу адреса и маршруты в соответствующих файлах.

Далее, в качестве примера, выполняется конфигурация GRE-туннеля между 10.0.1.2 и 10.0.2.3 с двумя ключами для исходящих и входящих пакетов, проверкой очередности пакетов, TTL-8 и вычислением контрольных сумм. Туннель должен использовать только определенный интерфейс. Пусть имя создаваемого туннеля будет mytunnel.

Нужно сделать следующие операции:

1) создать каталог туннеля `/etc/net/ifaces/mytunnel`;
2) создать в каталоге туннеля файл настроек `options` `/etc/net/ifaces/mytunnel/options`;
3) отредактировать файл настроек `options`:

```
TYPE=iptun
TUNTYPE=gre
TUNLOCAL=10.0.1.2
TUNREMOTE=10.0.2.3
TUNTTL=8
HOST=eth0
TUNOPTIONS='seq ikey 2020 okey 2030 csum'
```

При настройке VPN-подключения часто не учитывают, что при использовании опции `pppd 'defaultroute'` маршрут по умолчанию после подключения будет изменен. При этом, если VPN-сервер находится в другой, отличной от клиента, сети, то после подключения (и изменения маршрута по умолчанию) VPN-сервер становится недоступным, следовательно, недоступными становятся все внешние адреса, и подключение, как правило, прекращается по тайм-ауту.

Решением служит указание отдельного маршрута на VPN-сервер (или его сеть). Для этого нужно прописать (в примере – для маршрута через eth0) в `/etc/net/ifaces/eth0/ipv4route` строку вида:

```
10.0.1.0/24 via 10.0.0.1
```

В данном примере подразумевается, что VPN-сервер находится в сети 10.0.1.0/24 (например, имеет адрес 10.0.1.1), клиент – в сети 10.0.0.0/24 (и имеет адрес, например, 10.0.0.10), а маршрутизатор имеет адрес 10.0.0.1.

Теперь, при использовании опции `'defaultroute'` для pppd (которая указывает, что нужно изменить на вновь созданное подключение маршрут по

умолчанию), даже после замены маршрута по умолчанию новым, сеть 10.0.1.0, в которой в нашем примере и находится VPN-сервер, останется доступной.

Как более точечный вариант можно использовать скрипты `ifup-pre` и `ifdown-post` в каталоге конфигурируемого PPP-интерфейса.

Например:

```
#!/bin/sh
# sample /etc/net/ifaces/ppp0/ifup-pre; replace variables
yourself
ip route add VPN_SERVER via DEF_GW
#!/bin/sh
# sample /etc/net/ifaces/ppp0/ifdown-post; replace variables
yourself
ip route del VPN_SERVER via DEF_GW
```

Далее нужно подставить нужные IP-адреса вместо `VPN_SERVER` и `DEF_GW` (не сеть, где VPN-сервер, а ее /32 префикс CIDR) и выполнить команду:

```
chmod +x ifup-pre ifdown-post
```

8.7.7.9. Сложная маршрутизация

Под «сложной маршрутизацией» подразумевается наличие нескольких таблиц маршрутизации. Для их использования нужно сконфигурировать правила ядра. В правилах по умолчанию можно увидеть следующее:

```
# ip rule show
0: from all lookup local
32766: from all lookup main
32767: from all lookup default
```

Для настройки «сложной маршрутизации» нужно выполнить следующие операции:

1) сами таблицы определены в файле `/etc/iproute2/rt_tables`. Для создания конфигурации «сложной маршрутизации» нужно вначале «создать» нужные таблицы в этом файле (если хотите использовать имена таблиц, а не числа);

2) нужно заполнить таблицы. В конфигурационном каталоге интерфейса в файле ipv4route нужно добавить маршрутные записи, не забывая указать tableXX. Важно учитывать, что если строка начинается с режима iproute (add, del, replace, append, change), то по умолчанию будет использован режим `DEFAULT_IPV4ROUTE_CMD` (append);
3) определить правила в файле `ipv4rule`. Если строка не начинается с операции `del` или `add`, то нужный режим будет подставлен автоматически. Это подходит для тех случаев, когда при «поднятии» интерфейса нужно добавить правила, а при «опускании» – удалить. Возможность указывать `del` или `add` реализована для обратных случаев: если при «поднятии» интерфейса нужно удалить правила, а при «опускании» – добавить. В этом случае `add` и `del` будут в нужный момент автоматически заменены на `del` и `add`.

8.7.7.10. Простое переключение маршрутов

При нужности настроить второй маршрут по умолчанию через беспроводной интерфейс, в обход работы основного проводного сетевого интерфейса, но с меньшей метрикой, чем у проводного интерфейса используется простое переключение маршрутов.

В этом случае при настройке Wi-Fi маршрут настроится по умолчанию:

- для ethernet-интерфейса файл настроек `/etc/net/ifaces/eth0/ipv4route` будет следующим:
  `default via 192.168.3.254 metric 10`
- для Wi-Fi-интерфейса файл настроек `/etc/net/ifaces/wlan0/ipv4route` таким:
  `default via 192.168.123.1 metric 5`

8.7.7.11. Настройка Wi-Fi

Большинство беспроводных интерфейсов сейчас представлено в системе как интерфейсы Ethernet. Соответственно беспроводной интерфейс будет иметь `TYPE=eth`.

Чтобы интерфейс нормально функционировал, нужно кроме загрузки модуля с параметрами, воспользоваться утилитами iwconfig из пакета wireless-tools или wpa_supplicant из такого же пакета.

Для автоматического запуска беспроводной сети с помощью wpa_supplicant достаточно добавить файл `/etc/net/ifaces/eth0/wpa_supplicant.conf`:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
eapol_version=1
ap_scan=1
fast_reauth=1
network={
    ssid="homenet"
    key_mgmt=WPA-PSK
    pairwise=CCMP
    psk="this is my mega secret password string to wpa supplicant"
}
```

и перезагрузить систему.

После этого сервис network должен переключиться на работу с wpa_supplicant.

Сразу после загрузки интерфейс будет сконфигурирован и подключен к сети.

Если настроено получение параметров по DHCP – они будут получены автоматически.

Для подключения к сети достаточно добавить ssid и psk, однако можно добавить и другие параметры.

Например:

- proto – выбор поддерживаемых протоколов, например, WPA или RSN;
- bssid – Basic Service Set Identifier, идентификатор точки доступа в беспроводной сети.

  Например, bssid=00:11:D8:22:AD:0D.Bssid можно использовать вместо ssid, тогда psk должен был записан в виде строки из 64 символов в шестнадцатеричной системе. Получить эту строку можно с помощью wpa_passphrase:

  ```
  # wpa_passphrase <SSID> <password>
  ```
- priority – приоритет подключения к сети. Может записываться как положительное значение (например, 2), так и отрицательное (-999).

В качестве дополнительных параметров можно прописать в `/etc/net/ifaces/wlan0/options` параметры загружаемых драйверов и модулей:

```
module=ipw2200
WPA_DRIVER=wext
```

Еще один способ настройки интерфейса через wpa_supplicant:

1) установить пакет wpa_supplicant:

```
# apt-get install wpa_supplicant
```

2) включить сервис:

```
# systemctl enable wpa_supplicant
# systemctl start wpa_supplicant
```

3) добавить файл `/etc/wpa_supplicant/wpa_supplicant-wlan0.conf`:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
eapol_version=1
ap_scan=1
fast_reauth=1
network={
    ssid="homenet"
    key_mgmt=WPA-PSK
    pairwise=CCMP
    psk="this is my mega secret password string to wpa supplicant"
}
```

4) поднять интерфейс wlan0:

```
# systemctl start wpa_supplicant@wlan0
# systemctl enable wpa_supplicant@wlan0
```

5) для получения параметров по DHCP выполнить команду:

```
# dhcpcd wlan0
```

При таких настройках интерфейс будет автоматически запускаться после перезагрузки, но параметры по DHCP нужно будет получать каждый раз заново.

8.7.7.12. Использование автодополнения в `sysctl.conf`

В конфигурационном каталоге интерфейса может находиться файл `sysctl.conf`, в котором можно перечислить переменные sysctl. Переменные могут быть как общесистемными, так и относящимися к интерфейсу. Естественно, запись в `sysctl.conf` настроек вида `net.ipv4.conf.eth0.log_martians = 1` достаточно неудобна, а при переименовании интерфейса велик риск не отредактировать файл `sysctl.conf` соответствующим образом.

Эта проблема решается следующим способом: производится запись в файл только имени переменной и значение, а система `/etc/net` сама найдет путь к этой переменной и вызовет sysctl с полным именем.

Пример содержания файла `sysctl.conf`:

```
log_martians=1
rp_filter=1
```

8.7.7.13. Профили конфигурации

8.7.7.13.1. Определение профилей

Профиль – именованный вариант конфигурации, в той или иной степени изменяющий базовую конфигурацию системы. Профили могут быть применены, например, для конфигурации ноутбука в разных сетевых окружениях, или при подготовке новой или тестовой конфигурации с возможностью быстрого возврата к старой. Практически профили реализуются следующим образом: для какого-либо из файлов, составляющих общесистемную конфигурацию или конфигурацию интерфейса, создается альтернативный вариант, который отличается добавлением в конце названия файла знака «#» и имени профиля.

Например, пусть единственное отличие между профилями заключается в том, какой модуль ядра будет загружен для интерфейса eth0. В этом случае файл `/etc/net/ifaces/eth0/options` нужно скопировать в `/etc/net/ifaces/eth0/options#profile1` и изменить значение переменной `MODULE` в одном из них. Далее при использовании конфигурации по умолчанию будет использован файл `options`, а при использовании профиля profile1 – файл `options#profile1`.

Профили могут использоваться также и для отключения каких-то параметров конфигурации. Например, если используется файл `ipv4route` для установки маршрутов для интерфейса, то можно создать файл нулевого размера `ipv4route#profile2`, чтобы при использовании профиля profile2 никаких маршрутов не конфигурировалось.

8.7.7.13.2. Выбор профиля при загрузке

Если при загрузке системы ядру был передан параметр `netprofile`, то его значение будет использовано как имя профиля по умолчанию. Это может быть использовано для создания собственных пунктов меню загрузчиков LILO и GRUB с заранее определенным профилем сетевой конфигурации. Заданный таким образом профиль может быть далее переопределен другими методами.

Следует понимать разницу между различными конфигурациями и различными результатами применения одной конфигурации. Например, если в двух разных сетях используется DHCP, то смысла в разных профилях конфигурации нет.

Для загрузчика grub2 нужно добавить новый пункт меню (пример пункта меню можно найти в конце файла `/boot/grub/grub.cfg`) в файл `/etc/grub.d/40_custom` и для обновления конфигурации grub запустить команду:

```
grub-mkconfig -o /boot/grub/grub.cfg
```

Использование этого метода удобно, если смена сетевого окружения происходит синхронно с загрузкой системы.

8.7.7.13.3. Выбор профиля по умолчанию

Если требуется, чтобы определенный профиль конфигурации использовался по умолчанию, то нужно записать его название в файл `/etc/net/profile`. Этот метод имеет приоритет над параметром ядра `netprofile`. Использование такого способа выбора профиля целесообразно, когда переключение между конфигурациями происходит реже, чем перезагрузка системы.

8.7.7.13.4. Смена профиля во время работы

Если требуется переконфигурировать сеть без перезагрузки или редактирования файла `/etc/net/profile`, то следует использовать параметры сервиса network (см. п. 8.7.5).

Пример подключения профиля с помощью сервиса network:

```
# /etc/rc.d/init.d/network restartwith имя_профиля
```

Этот метод имеет приоритет над профилем по умолчанию и профилем, выбранным при загрузке. Целесообразно его использовать, если смена сетевого окружения происходит чаще, чем перезагрузка системы.

8.7.7.13.5. Определение профиля во время конфигурации интерфейса

Если в каталоге конфигурации интерфейса существует исполняемый файл ненулевого размера с именем `selectprofile`, то этот файл будет выполнен и первое слово первой строки его стандартного вывода использовано как имя профиля, которое должно быть использовано для конфигурации данного интерфейса. Этот метод имеет приоритет над всеми остальными методами.

Исходной задачей, требующей такого решения, являлось конфигурирование беспроводного интерфейса в зависимости от доступных точек доступа.

Следует учитывать, что число вызовов файла `selectprofile` может меняться в зависимости от контекста и время его выполнения может быть различным, поэтому при написании такого файла следует учитывать, что первым параметром будет являться имя текущего сценария. В настоящее время это могут быть `ifup*`, `ifdown*`, `setup*` и `shutdown*`. Для приведенного выше примера имеет смысл реагировать только на вызовы из ifup или ifup-common.

8.7.8. Настройка межсетевого экрана в `/etc/net`

`/etc/net` содержит поддержку управления межсетевым экраном (firewall). В данный момент поддерживается iptables, ip6tables, ipset и ebtables. Реализация основана на группировке таблиц и цепочек в таблицах. Таблицы могут быть только системные, цепочки же, кроме системных, могут быть заданы пользователем.

Ниже приведены файлы и каталоги, используемые для настройки межсетевого экрана.

`/etc/net/ifaces/default/fw/options` – файл с настройками межсетевого экрана по умолчанию:

1) `FW_TYPE` – тип межсетевого экрана. Здесь можно указать только iptables, другие типы пока не поддерживаются;
2) `IPTABLES_HUMAN_SYNTAX` – включает или отключает использование поддержки удобочитаемого синтаксиса правил для iptables. Значение: `yes` или `no`;

3) IPTABLES_SYSTEM_CHAINS – список системных цепочек в таблицах. Все цепочки, не указанные здесь, будут автоматически создаваться и удаляться. Значение: названия цепочек (все названия чувствительны к регистру!), разделенные пробелом;
4) IPTABLES_INPUT_POLICY – действие по умолчанию для пакетов, попадающих в системную цепочку INPUT таблицы filter. Значение: одно из ACCEPT, DROP, QUEUE или RETURN;
5) IPTABLES_FORWARD_POLICY – действие по умолчанию для пакетов, попадающих в системную цепочку FORWARD таблицы filter. Значение: одно из ACCEPT, DROP, QUEUE или RETURN;
6) IPTABLES_OUTPUT_POLICY – действие по умолчанию для пакетов, попадающих в системную цепочку OUTPUT таблицы filter. Значение: одно из ACCEPT, DROP, QUEUE или RETURN;
7) IPTABLES_RULE_EMBEDDING – способ добавления нового правила в цепочку. Значение: APPEND или INSERT, что означает добавление в конец списка правил или, соответственно, в начало.

/etc/net/ifaces/default/fw/iptables/filter, /etc/net/ifaces/default/fw/iptables/nat, /etc/net/ifaces/default/fw/iptables/mangle – каталоги, соответствующие таблицам iptables. В каталогах создаются файлы, соответствующие системным или пользовательским цепочкам, в которых уже и прописываются сами правила iptables.

/etc/net/ifaces/default/fw/iptables/loadorder, /etc/net/ifaces/default/fw/tablename/loadorder – если такой файл существует и не пуст, то обработка таблиц и (или) цепочек в таблице происходит в том порядке, который указан в файле (по одному значению на строку). Все таблицы и цепочки, которые не указаны, обрабатываться не будут.

/etc/net/ifaces/default/fw/iptables/modules – список модулей ядра, которые нужно загрузить перед запуском межсетевого экрана. При остановке эти модули выгружаются. /etc/net/ifaces/default/fw/iptables/syntax – описание

замен при использовании удобочитаемого синтаксиса правил iptables.

8.7.8.1. Алгоритм работы сетевого экрана

Алгоритм работы сетевого экрана:

1) при запуске службы network, виртуальный интерфейс default:

- если опция `CONFIG_FW` (в файле `/etc/net/ifaces/default/options`) не установлена в `yes`, то ничего не делает и происходит выход из процедуры запуска сетевого экрана, иначе переходим к следующему пункту;
- считывается файл настроек:
`/etc/net/ifaces/default/fw/iptables/options`;
- до настройки любого интерфейса и обработки значений sysctl устанавливаются действия по умолчанию (policy) для системных цепочек таблицы filter;
- считывается файл со списком модулей ядра `/etc/net/ifaces/default/fw/iptables/modules`, и все указанные в нем модули (по одному на строку) загружаются. При отсутствии файла никакие модули не загружаются;
- создаются все пользовательские цепочки во всех таблицах (пользовательскими считаются все цепочки, не указанные в переменной `IPTABLES_SYSTEM_CHAINS`);
- считывается файл `/etc/net/ifaces/default/fw/iptables/loadorder`, и в указанном в нем порядке происходит обработка таблиц iptables. При отсутствии файла обработка происходит в соответствии с сортировкой названий таблиц по имени;
- считывается файл `/etc/net/ifaces/default/fw/iptables/tablename/loadorder` в каждой обрабатываемой таблице, и происходит обработка и загрузка правил для каждой цепочки в порядке, указанном в файле. При отсутствии файла обработка опять же происходит в соответствии с

сортировкой по имени;

- если опция `IPTABLES_HUMAN_SYNTAX` установлена в `yes`, то считывается и обрабатывается файл с «синтаксисом» `/etc/net/ifaces/default/fw/iptables/syntax`;
- файл с правилами обрабатывает построчно (одно правило на строку); если указана опция `IPTABLES_HUMAN_SYNTAX`, то правило обрабатывается интерпретатором в соответствии с синтаксисом и превращается в реальные опции для команды iptables, после чего запускается iptables с этими параметрами; иначе правило без обработки передается iptables;

2) при «поднятии» любого интерфейса, кроме default – выполняются все подпункты пункта 1), только все файлы и каталоги ищутся в каталоге текущего интерфейса;
3) при «опускании» любого интерфейса, кроме default – все подпункты пункта 1) выполняются в обратном порядке, все правила удаляются из цепочек в обратном порядке, все модули ядра выгружаются в обратном порядке. Все файлы и каталоги ищутся в каталоге текущего интерфейса;
4) при остановке службы network виртуальный интерфейс default – все подпункты пункта 1) выполняются в обратном порядке, все правила из всех цепочек удаляются командой `iptables -F`, все модули выгружаются в обратном порядке, все пользовательские цепочки удаляются.

Действия по умолчанию (policy) для системных цепочек устанавливается в ACCEPT.

8.7.8.2. Правила для iptables

Правила для iptables можно писать с помощью синтаксиса, подобного синтаксису ipfw и других.

Сделано это с помощью простой замены слов на опции iptables. Сами замены описаны в файле `/etc/net/ifaces/default/fw/iptables/syntax`, там также описано некоторое количество вспомогательных слов, так что правила можно писать практически на английском литературном. Синтаксис правила можно

совмещать (то есть использовать и заданный в «etcnet» синтаксис, и реальные опции команды iptables (см. подробнее п. 7.5)).

Во всех правилах нельзя использовать названия цепочки и (или) таблицы. Они будут добавляться автоматически.

В правилах можно использовать любые переменные окружения, выполнять любые команды `shell` (они должны быть указаны в одну строку).

Переменная `$NAME` содержит имя текущего интерфейса. Переменные `$IPV4ADDRESS` и `$IPV6ADDRESS` содержат массив IPv4/IPv6 адресов текущего интерфейса (это обычные «bash arrays», можно обращаться к ним по индексу: `${IPV4ADDRESS[2]}` или просто `$IPV4ADDRESS` для первого значения). Для удобства можно использовать файлы `options`, в которых прописывать какие-либо переменные, к примеру, адреса gateway, ISP, сетей и т. д.

Во всех файлах можно использовать комментарии (строка должна начинаться с символа #).

Нет необходимости копировать все файлы настроек в каталог каждого интерфейса. Сначала будут считаны настройки виртуального интерфейса default, а уже потом у текущего интерфейса, соответственно, можно переопределять только требуемые для настройки параметры.

Описания всех правил в настройках виртуального интерфейса default достаточно для поднятия простого сетевого экрана. При наличии же большого количества правил и интерфейсов есть смысл разделить логически все правила по каждому интерфейсу (опять же, не будет нагружаться процессор без нужности, если интерфейс, к которому относится много правил, сейчас не «поднят»).

В начале каждого правила можно указать, что с этим правилом делать. Может быть одно из трех значений:

1) `-A` – добавление в конец списка правил (при включенном удобочитаемом синтаксисе соответствует команде `append`);
2) `-I [num]` – добавление в начало списка правил; если указан необязательный параметр num, то правило будет вставлено в строку правил с таким номером (iptables считает несуществующий номер строки ошибкой

и добавляет правило). При включенном удобочитаемом синтаксисе соответствует команде `insert [num]`);

3) `-D` – удаление правила из списка правил (соответственно, при «остановке» интерфейса правило наоборот будет добавлено). При включенном удобочитаемом синтаксисе соответствует команде `delete`.

Если никакое действие не указано, то правила добавляются в цепочку в соответствии со значением переменной `IPTABLES_RULE_EMBEDDING`.

Если изменяется какое-то правило в конфигурационных файлах при уже загруженных правилах iptables, то для того, чтобы в памяти не остались старые правила, нужно или выгрузить все правила для текущего интерфейса (если настраивается для конкретного интерфейса, а не для default) перед изменением файлов или после изменения использовать команду `/etc/net/scripts/contrib/efw default restart` (она полностью удалит все правила, однако, пользовательские цепочки других интерфейсов не будут затронуты), и далее загрузить заново правила для нужного или всех интерфейсов.

8.7.8.3. Примеры

Пример настройки сетевого экрана в etcnet (файл – содержание):

Файл `/etc/net/ifaces/eth0/fw/options`:

```
# Our WAN IP address
WAN_IP=5.6.7.8
# First net
NET1=1.2.3.0/24
# Second net
NET2=4.3.2.0/24
# Friend net
FRIEND_NET=5.6.7.0/24
```

Файл `/etc/net/ifaces/eth0/fw/iptables/filter/INPUT`:

```
accept all from any to $IPV4ADDRESS
jump-to COUNT-CHAIN if marked as 0x11
```

Файл `/etc/net/ifaces/eth0/fw/iptables/filter/FORWARD`:

```
jump-to FRIEND-NET if from $FRIEND-NET
append drop tcp from net $NET1 to net $NET2
delete drop udp from $NET1 to $NET2
insert reject udp to $WAN_IP
drop icmp to $(somescript.sh)
```

Файл `/etc/net/ifaces/eth0/fw/iptables/filter/FRIEND-NET`:

```
policy reject
```

Файл `/etc/net/ifaces/eth0/fw/iptables/mangle/PREROUTING`:

```
insert 2 tcp mark as 0x10 if from-iface $NAME and dport is 22
tcp mark as 0x11 if from net $NET1 and from-iface $NAME
```

Файл `/etc/net/ifaces/eth0/fw/iptables/nat/POSTROUTING`:

```
snat-to $WAN_IP if marked as 0x10
```

8.7.8.4. Утилиты

В `scripts/contrib` находятся вспомогательные утилиты.

Скрипт `efw` предназначен для ручного управления сетевым экраном.

Синтаксис:

```
efw –ips[et]|[--ipt[ables]|--ip6t[ables]|--ebt[ables]|--no-ips[et]|--no-ipt[ables]|
--no-ip6t[ables]|--no-ebt[ables]] [iface] [table|settype] [chain|set] <action> [правило или опции для action]
```

Параметры:

1) `--ipset` – обработать только ipset;
2) `--iptables` – обработать только iptables;
3) `--ip6tables` – обработать только ip6tables;
4) `--ebtables` – обработать только ebtables;
5) `--no-iptables` – обработать все типы за исключением iptables;
6) `--no-ip6tables` – обработать все типы за исключением ip6tables;
7) `--no-ebtables` – обработать все типы за исключением ebtables;
8) `iface` – `'default'` (по умолчанию), имя интерфейса или `'all'` для всех интерфейсов;
9) `table` – `'mangle'` (только для iptables и ip6tables), 'broute' (только для ebtables), `'filter'` (по умолчанию), `'nat'` или `'all'` для всех таблиц;
10) `chain` – системная либо пользовательская цепочка (чувствительно к регистру!) или `'all'` для всех цепочек;
11) `action` – `'start'`, `'stop'`, `'restart'`, `'load'`, `'unload'`, `'reload'`, `'flush'`, `'show|list'`, `'count|counters'`, `'rule'`, `'new|create'`, `'remove|delete'`, `'zero'`, `'policy'`, `'rename'`.

Действия (action):

1) start – обработать все таблицы и цепочки для заданного интерфейса (даже если задано конкретное имя цепочки либо таблицы);
2) stop – обработать все таблицы и цепочки для заданного интерфейса (даже если задано конкретное имя цепочки либо таблицы);
3) restart – равносильно сначала 'stop' затем 'start';
4) load – загрузить правила для заданного интерфейса, таблицы и цепочки;
5) unload – выгрузить правила для заданного интерфейса, таблицы и цепочки;
6) reload – равносильно сначала 'unload' затем 'load';
7) flush – очистить правила для заданного интерфейса, таблицы и цепочки;
8) show – показать правила для заданного интерфейса, таблицы и цепочки;
9) list – тоже что и 'show';
10) count – показать значения счетчиков для заданной таблицы и цепочки;
11) counters – тоже что и 'count';
12) rule – разобрать правило и передать его в iptables и (или) ip6tables и (или) ebtables;
13) new – создать новую цепочку;
14) create – тоже что и 'new';
15) remove – удалить цепочку;
16) delete – тоже что и 'remove';
17) zero – очистить счетчики пакетов и байтов в цепочке;
18) policy – задать политику для цепочки;
19) rename – переименовать цепочку.

Опции для действий show и list:

1) -n или numeric – цифровой вывод IP-адресов, портов и сервисов;
2) -v или verbose – детальный вывод правил;
3) -x или exact – не округлять числа;
4) --line-numbers или lines – показать номера каждой строки.

На данный момент скрипт `efw` «умеет» частично «угадывать» интерфейс, таблицу и цепочку (если их не передали в командной строке) и все действия, кроме `counters`. Так же поддерживается маска «all» для интерфейсов, таблиц и цепочек.

Примеры команд:

Выгрузить (flush) все правила из всех цепочек всех таблиц, удалить цепочки, пользователем, выгрузить все загруженные модули:

```
/etc/net/scripts/contrib/efw default stop
```

Выгрузить (путем удаления каждого правила в обратном порядке) все правила из цепочки FORWARD таблицы filter для интерфейса eth0:

```
/etc/net/scripts/contrib/efw eth0 FORWARD unload
```

Загрузить все правила для всех цепочек во всех таблицах всех интерфейсов:

```
/etc/net/scripts/contrib/efw all all all load
```

Обработать правило и добавить его во все цепочки таблицы filter:

```
/etc/net/scripts/contrib/efw default filter all rule accept all from any
```

Если изменяется какое-либо правило в конфигурационных файлах при уже загруженных правилах iptables, то для того, чтобы в памяти не остались старые правила, нужно:

- вариант 1: выгрузить все правила для текущего интерфейса (если настраивается для конкретного интерфейса, а не default) перед изменением файлов;
- вариант 2: после изменения использовать команду efw default restart (она полностью удалит все правила, однако, пользовательские цепочки других интерфейсов не будут затронуты), и далее загрузить заново правила для требуемого или всех интерфейсов.

Таким образом, наиболее используемой командой при изменении конфигурации сетевого экрана является:

```
/etc/net/scripts/contrib/efw default stop;
/etc/net/scripts/contrib/efw all start
```

8.8. Сетевая установка ОС на рабочие места

Одной из удобных возможностей ОС Альт СП при разворачивании инфраструктуры является сетевая установка. При помощи нее можно производить установку ОС Альт СП не с компакт-диска дистрибутива, а загрузив инсталлятор по сети.

8.8.1. Подготовка сервера

Перед началом установки рабочих станций следует произвести предварительную настройку сервера: задать имя сервера (модуль «Ethernet-интерфейсы» в ЦУС п. 8.5.1), включить DHCP-сервер (модуль «DHCP-сервер» (см. п. 8.5.3)), задать имя домена.

Примечание. При сетевой установке с сервера будут переняты настройки домена, и будет включена централизованная аутентификация. Если устанавливается ОС Альт СП с компакт-диска, то настройку домена и аутентификации надо будет производить отдельно на каждом компьютере.

Перед активацией сетевой установки потребуется импортировать установочный компакт-диска дистрибутива ОС Альт СП, предварительно вставив его в DVD-привод сервера, либо используя образ диска, расположенный на файловой системе на сервере. В разделе «Сервер сетевых установок» (пакет alterator-netinst), укажите откуда импортировать новый образ и нажмите кнопку «Добавить» (рис. 95).

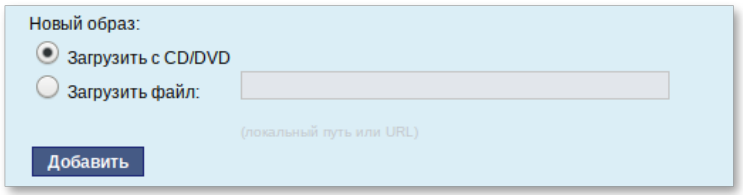


Рис. 95 – Загрузка CD/DVD

Процесс добавления занимает какое-то время. Пожалуйста, дождитесь окончания этого процесса (рис. 96).

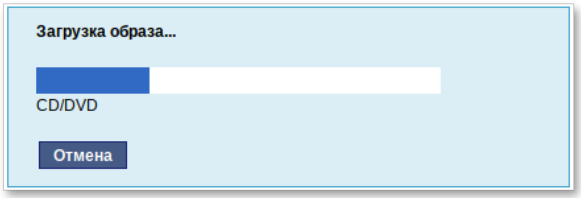


Рис. 96 – Процесс загрузки образа

После добавления образа он появится в списке «Доступные образы дисков». Выберите из этого списка один из образов и нажмите кнопку «Выбрать» (рис. 97). На этом подготовка сервера к сетевой установке рабочих станций завершена.

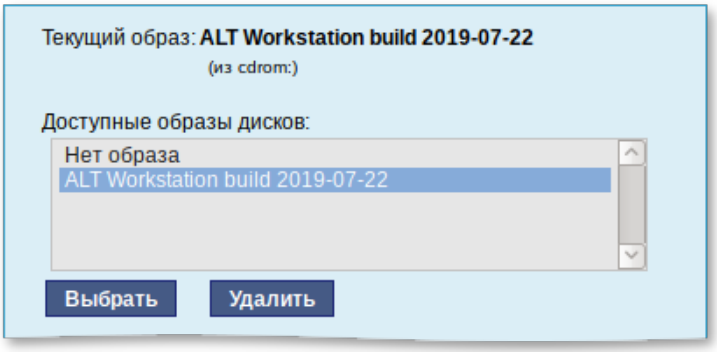


Рис. 97 – Выбор доступного образа диска

Далее нужно выбрать направление соединения. Удаленный доступ к компьютеру может быть двух видов (рис. 98):

- со стороны клиента – во время установки администратор может с помощью VNC-клиента подключиться к компьютеру, на которой производится установка, зная его IP-адрес и заданный пароль;
- со стороны сервера – во время установки с каждого компьютера инициируется подключение к запущенному на заданном компьютере VNC-клиенту. Компьютер-приемник соединений задается IP-адресом или именем.

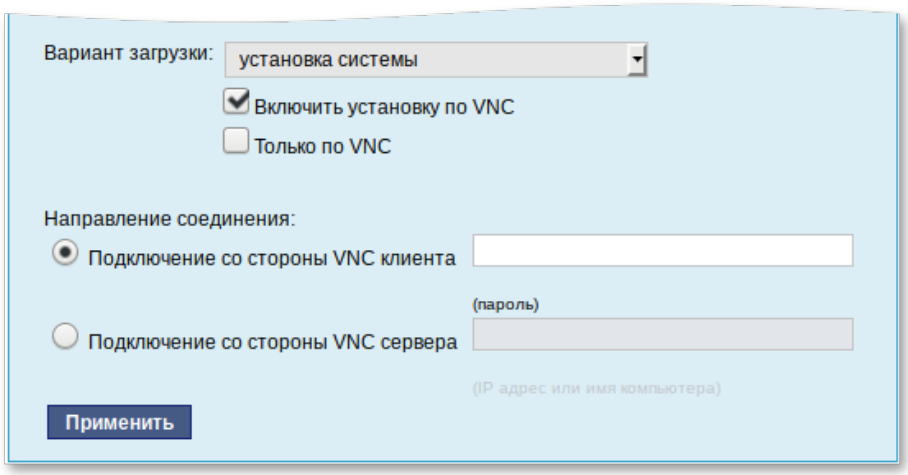


Рис. 98 – Виды удаленного доступа к компьютеру

В случае, когда работа с аппаратной подсистемой ввода-вывода невозможна (например, если клавиатура, мышь или монитор отсутствуют), можно использовать вариант «Только по VNC».

Если нужно управлять установкой удаленно, отметьте пункт «Включить установку по VNC» и пункт «Подключение со стороны VNC сервера» раздела «Направление соединения», и там укажите адрес компьютера, с которого будет происходить управление. Для приема подключения можно запустить, например, `vncviewer -listen`.

⚠ Не забудьте отключить сетевую установку по окончании процесса установки ОС на рабочих станциях. Это можно сделать, выбрав в списке «Доступные образы дисков» пункт «Нет образа» и подтвердив действие нажатием кнопки «Выбрать».

За дополнительной информацией по настройке обращайтесь к встроенной справке соответствующих модулей ЦУС (п. 7.1.5).

8.8.2. Подготовка рабочих станций

Для сетевой установки следует обеспечить возможность загрузки по сети рабочих станций, на которых будет производиться установка ОС.

Большинство современных материнских плат имеют возможность загрузки по сети, однако она по умолчанию может быть отключена в BIOS (БСВВ). Различные

производители материнских плат дают разные названия данной возможности, например: «Boot Option ROM» или «Boot From Onboard LAN».

Примечание. Некоторые материнские платы позволяют выбрать источник загрузки во время включения компьютера. Эта возможность может называться, например, «Select boot device» или «Boot menu».

Последовательность установки при установке с компакт-диска и при сетевой установке не отличаются друг от друга. Подробный о процессе см. в разделе 5 «Установка ОС Альт СП».

8.9. Сервер электронной почты (SMTP, POP3/IMAP)

8.9.1. Сервер электронной почты

ОС Альт СП Сервер может служить как почтовым сервером, обслуживающим определенный домен, так и посредником (шлюзом) для пересылки почты. Почтовый сервер отвечает, как за отправку писем (SMTP-сервер см. п. 8.10.3) исходящих от почтовых клиентов рабочих станций, так и за предоставление им входящей почты (Сервер POP3/IMAP см. п. 8.9.3).

Для настройки параметров работы сервера предусмотрен модуль ЦУС «Почтовый сервер» (пакет alterator-postfix-dovecot) из раздела «Серверы» (рис. 99).

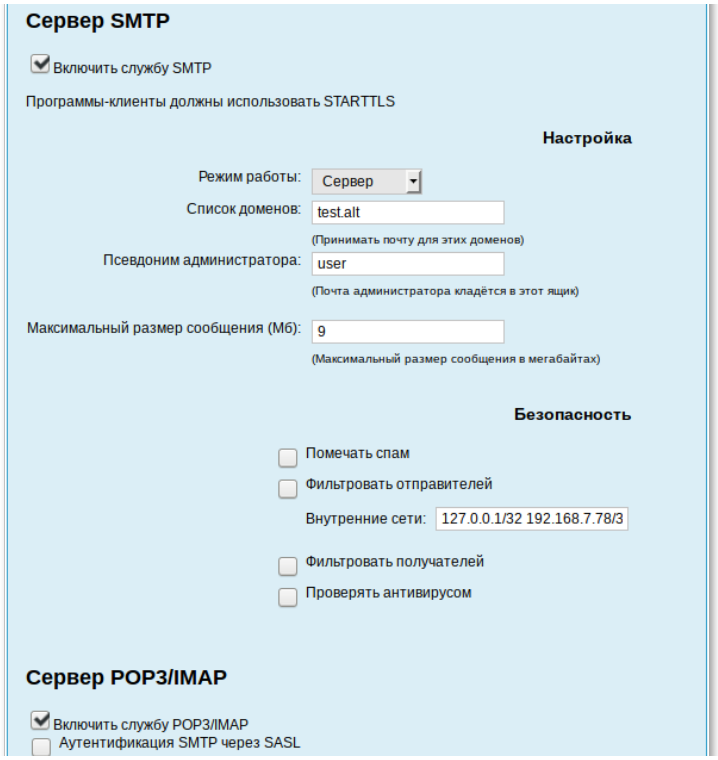


Рис. 99 – Настройка параметров работы сервера

8.9.2. Сервер SMTP

Сервер SMTP отвечает за отправку сообщений и может работать в двух режимах:

1) посредник – в этом режиме исходящая почта пересылается для дальнейшей отправки на указанный сервер;
2) сервер – в этом режиме сервер доставляет почту самостоятельно.

8.9.3. Сервер POP3/IMAP

Сервер POP3/IMAP используется для доступа пользователей к электронной почте на сервере.

Для доступа к службам POP3 и IMAP пользователь должен включить в своем почтовом клиенте аутентификацию и указать свое имя и пароль.

Выбор конкретного используемого протокола для получения почты зависит от предпочтений пользователя.

1) POP – при проверке почты почтовым клиентом почта передается на клиентскую машину, где и сохраняется. Возможность просмотра принятой/отправленной почты при этом существует даже если клиент не имеет соединения с сервером;
2) IMAP – все сообщения хранятся на сервере. Почтовый клиент может просматривать их только при наличии соединения с сервером.

Помимо включения/отключения служб, модуль ЦУС «Почтовый сервер» позволяет произвести дополнительные настройки: фильтрацию спама, настройку параметров аутентификации и т. д.

8.10. Сервер электронной почты postfix

Postfix представляет собой агент передачи электронной почты и позволяет организовать обмен почтой внутри локальной сети, а также с внешней сетью.

Для расширения возможностей postfix используется ряд дополнений, выделенных в отдельные пакеты, полный список которых можно получить с помощью следующей команды:

```
$ apt-cache search ^postfix-
```

Настройка сервера электронной почты postfix осуществляется с помощью конфигурационных файлов, хранящихся в каталоге `/etc/postfix`. Основные параметры определяются в файле конфигурации `main.cf`. В файле `main.cf` указываются только параметры, выставленные администратором, и некоторые из значений по умолчанию, которые администратору с большой вероятностью нужно будет изменить. Значения по умолчанию для всех остальных параметров перечислены в файле `main.cf.default` (этот файл не следует редактировать, он служит только для справок).

Если конфигурация была изменена при запущенной службе postfix, новые настройки нужно активизировать командой: `# service postfix reload`

Postfix сохраняет все сообщения в журнале `mail.log`, расположенном в каталоге `/var/log/`. Сообщения об ошибках и предупреждения сохраняются отдельно в журналы `mail.err` и `mail.warn` соответственно.

Запуск postfix осуществляется с помощью следующей команды:

```
# postfix start
```

8.10.1. Утилиты командной строки

Postfix поставляется с набором утилит командной строки, которые помогают решать административные задачи. Они выполняют разнообразные функции (обращение к картам, просмотр файлов очередей, постановка сообщений в очередь и извлечение из очереди, изменение конфигурации).

Команда `postfix` останавливает, запускает и перезагружает конфигурацию с помощью параметров `stop`, `start` и `reload`.

Команда `postalias` создает индексированную карту псевдонимов из файла псевдонимов и работает аналогично команде `postmap`, при этом уделяя особое внимание нотации в файле псевдонимов (ключ и значение разделяются двоеточием).

Команда `postcat` выводит содержимое сообщения, находящегося в почтовой очереди. Для того чтобы прочитать сообщение, находящееся в очереди, нужно знать идентификатор очереди. Для получения списка идентификаторов очередей следует выполнить следующую команду:

```
# mailq
```

После получения идентификатора очереди нужно указать его в качестве параметра команды postcat для просмотра содержимого файла следующим образом:

```
# postcat -q <идентификатор очереди>
```

Основная задача команды postmap заключается в построении индексированных карт на основе обычных текстовых файлов.

Для того чтобы создать карту /etc/postfix/virtual.db на основе /etc/postfix/virtual, нужно выполнить следующую команду:

```
# postmap hash:/etc/postfix/virtual
```

Также команда postmap обеспечивает возможность тестирования карт любого вида, поддерживаемых конфигурацией postfix.

Команда postdrop считывает почту из стандартного ввода и записывает результат в каталог maildrop (программа работает в связке с утилитой sendmail).

Команда postkick отправляет запрос демону postfix по локальному транспортному каналу, делая межпроцессное взаимодействие postfix доступным для сценариев оболочки и других программ.

Команда postlock предоставляет монопольный доступ к файлам mbox, в которые выполняет запись postfix, а затем исполняет команду, удерживая блокировку.

Команда postlog позволяет внешним программам, таким как сценарии командного интерпретатора, писать сообщения в журнал электронной почты (представляет собой postfix-совместимый интерфейс регистрации).

Команда postqueue представляет собой пользовательский интерфейс для очередей postfix, предоставляющий возможности, обычно доступные в рамках выполнения команды sendmail.

Команда postqueue с параметром -f просит диспетчер очередей доставить всю стоящую в очереди почту вне зависимости от места назначения:

```
# postqueue -f
```

Команда postqueue с параметром -p выводит содержимое очереди:

```
# postqueue -p
```

Команда postqueue с параметром -s domain пытается доставить всю стоящую в очереди почту для домена domain:

```
# postqueue -s example.com
```

Команда postsuper обслуживает задания внутри очередей postfix (в отличие от postqueue, эта команда доступна только пользователю с идентификатором root, и она может быть выполнена, когда сервер не запущен).

8.10.2. Первичная настройка

В первую очередь после установки postfix нужно настроить параметры, отвечающие за домен и имя сервера. Чтобы установить значение параметра myhostname, нужно отредактировать конфигурационный файл main.cf. (для параметра myhostname нужно ввести полностью определенное доменное имя хоста):

```
myhostname = mail.example.com
```

Postfix может автоматически получить значение mydomain после того, как параметр myhostname настроен, для этого postfix отбрасывает первую часть значения myhostname до первой точки включительно:

```
mydomain = example.com
```

Далее нужно указать домен, с которого отправляется локальная почта. Postfix будет добавлять значение из mydomain к любому адресу, если он задан не полностью. Для этого нужно в конфигурационном файле main.cf для параметра myorigin установить следующее значение:

```
myorigin = $mydomain
```

Примечание. Сообщение от процесса cron пользователю root получит адрес root@$mydomain, которое будет преобразовано в root@example.com.

Далее нужно указать домены, для которых данный сервер является конечной точкой доставки электронной почты. Для того чтобы postfix принимал любую почту, адресованную в домен example.com нужно в файл конфигурации внести следующие изменения:

```
mydestination = $mydomain
```

Домены, для которых сервер получает почту, отличные от значения mydomain и не сконфигурированные как виртуальные домены postfix, нужно перечислить с помощью параметра `mydestination`, либо в дополнительном файле, на который ссылается этот параметр.

Адресаты указываются через запятую следующим образом:

```
mydestination =
$mydomain,
$myhostname
```

Аналогичным образом параметр `mynetworks` описывает блоки IP-адресов, которые считаются внутренними и с которых разрешен прием исходящих сообщений.

После внесения изменений в конфигурацию postfix для применения новых настроек нужно перезапустить службу postfix:

```
# service postfix reload
```

8.10.3. Работа в режиме SMTP-сервера

После установки служба postfix функционирует в режиме local, в котором сервер электронной почты postfix не принимает соединения из внешней сети, ограничиваясь приемом локальных соединений посредством сокетов семейства UNIX (UNIX-domain socket).

Для настройки возможности приема сообщений по протоколу SMTP или ESMTP, как из внешней сети, так из внутренней, нужно переключить службу postfix в режим работы server с помощью следующей команды:

```
control postfix server
```

Рабочие станции в локальной сети или машины в сети провайдера, отделенной от внешней сети, должны перенаправлять исходящую почту на почтовый сервер, обслуживающий данную сеть.

Для того чтобы postfix отправлял почту из локальной сети на SMTP-сервер провайдера, нужно для параметра relayhost установить следующее значение:

```
relayhost = [smtp.provider.net]
```

8.10.4. SMTP-аутентификация

SMTP-аутентификация обеспечивает идентификацию клиентов независимо от их IP-адресов и позволяет серверу пересылать сообщения от почтовых клиентов, чьи IP-адреса не входят в список доверенных. Postfix реализует SMTP-аутентификацию при помощи протокола SASL (Simple Authentication and Security Layer) и использует библиотеки Cyrus-SASL.

Для защиты соединений используется протокол SSL/TLS (для включения поддержки нужно установить пакет postfix-tls).

Для проверки поддержки SMTP-аутентификации postfix нужно от имени от имени администратора (root) выполнить следующую команду:

```
ldd ‘postconf h daemon_directory’/smtpd
```

Если в выводе команды присутствует строка `libsasl.so.2`, значит, пакет postfix был собран с поддержкой SASL.

8.10.4.1. Настройки SMTP-аутентификации на сервере

Настройка SMTP-аутентификации на сервере осуществляется в несколько этапов:

1) включение SMTP-аутентификации на серверной части;
2) настройка механизмов SASL, которые будут предоставляться клиентам;
3) настройка поддержки SMTP-аутентификации для нестандартных почтовых клиентов;
4) настройка области (realm), которую postfix будет передавать библиотеке SASL;
5) определение разрешения на пересылку в postfix.

Чтобы включить SMTP-аутентификацию, нужно в конфигурационный файл `main.cf` добавить следующую запись:

```
smtpd_sasl_auth_enable = yes
```

8.10.4.1.1. Настройка механизмов SASL

Управление предоставляемыми механизмами осуществляется с помощью параметра `smtpd_sasl_security_options`, в котором через запятые следует указать список из одного или более значений:

1) `noanonymous` – значение параметра, позволяющее включить проверку сервером верительных данных клиента (список значений параметра `smtpd_sasl_security_options` всегда должен включать в себя значение `noanonymous`);
2) `noplaintext` – значение параметра, позволяющее исключить использование всех механизмов открытого текста, таких как PLAIN и LOGIN (значение, рекомендуемое для использования, так как отправляемые открытым текстом верительные данные могут быть легко перехвачены в сети);
3) `noactive` – значение параметра, исключающее использование механизмов SASL, которые восприимчивы к активным атакам);
4) `nodictionary` – значение параметра, исключающее все механизмы, не устойчивые к атакам по словарю (атаки, осуществляемые методом полного перебора паролей);
5) `mutual_auth` – значение параметра, позволяющее включить поддержку только механизмов, обеспечивающих взаимную аутентификацию (сервер аутентифицирует себя для клиента).

8.10.4.1.2. Настройка SMTP-аутентификации для нестандартных почтовых клиентов

Для настройки альтернативной нотации для устаревших клиентов, не распознающих SMTP-аутентификацию по стандарту RFC 2222, но распознающих более раннюю нотацию, использованную в черновом варианте этого стандарта (где между командой `AUTH` и названиями механизмов стоял не пробел, а знак равенства), нужно в конфигурационном файле `main.cf` установить параметр `broken_sasl_auth_clients`:

```
broken_sasl_auth_clients = yes
```

8.10.4.1.3. Настройка области SASL

Для аутентификации клиента сервер postfix отправляет службе паролей Cyrus SASL область аутентификации (realm) вместе с верительными данными клиента. Такая нужность определяется версией Cyrus SASL и выбором службы. Для указания области аутентификации в файле `main.cf` используется параметр `smtpd_sasl_local_domain`. По умолчанию этот параметр пуст и должен оставаться пустым, если только не используется вспомогательный плагин, которому действительно требуется область аутентификации.

8.10.4.1.4. Настройка разрешений на пересылку

Для разрешения пересылки для клиентов, прошедших аутентификацию SASL, нужно добавить параметр `permit_sasl_authenticated` в список ограничений `smtpd_recipient_restrictions` своей конфигурации следующим образом:

```
smtpd_recipient_restrictions =
[...]
permit_sasl_authenticated,
permit_mynetworks,
reject_unauth_destination
[...]
```

Нужно поместить ключевое слово `permit_sasl_authenticated` достаточно близко к началу списка ограничений, чтобы аутентифицированный клиент не был случайно отвергнут из-за несоответствия какому-то другому правилу (например, `reject_unauth_destination`).

8.10.4.2. Настройка SMTP-аутентификации на стороне клиента

Для настройки SMTP-аутентификации для клиента нужно выполнить следующее:

1) запросить у удаленного сервера список поддерживаемых механизмов аутентификации;
2) включить SMTP-аутентификацию на клиентской части;
3) предоставить файл для хранения верительных данных;
4) настроить postfix на работу с файлом верительных данных;
5) отключить ненадежные механизмы аутентификации.

Клиентская ПЭВМ должна поддерживать механизмы аутентификации, поддерживаемые сервером. Для получения списка механизмов аутентификации нужно подключиться к почтовому серверу и отправить приветствие `EHLO` с помощью следующих команд:

```
$ telnet mail.remoteexample.com 25
EHLO mail.example.com
```

По умолчанию SMTP-аутентификация на стороне клиента выключена. Для того чтобы включить SMTP-аутентификацию нужно в конфигурационный файл `main.cf` добавить следующую запись:

```
smtp_sasl_auth_enable = yes
```

После включения аутентификации на клиентской ПЭВМ нужно сообщить серверу postfix, где следует искать данные, которые нужны для аутентификации, и какой из механизмов (из предлагаемых удаленным сервером) postfix может использовать.

8.10.4.2.1. Хранение верительных данных

Нужно подготовить данные, которые клиент postfix будет использовать для того, чтобы аутентифицировать себя на сервере, для этого следует создать от имени root файл карты `/etc/postfix/sasl_passwd` (если он еще не существует) с помощью следующей команды:

```
# touch /etc/postfix/sasl_passwd
```

Далее нужно отредактировать этот файл, поместив полностью определенное доменное имя почтового сервера, который требует аутентификации, с левой стороны, а разделенную двоеточием пару «имя пользователя – пароль» – с правой. Для имен пользователей `mail.example.com` и `relay.another.example.com`, а также соответствующих паролей файл `sasl_passwd` будет выглядеть следующим образом:

```
mail.example.com test:testpass
relay.another.example.com username:password
```

После редактирования файла `sasl_passwd` нужно изменить права на него так, чтобы читать его мог только пользователь root (в файле хранится конфиденциальная

информация, которая не должна быть доступна локальным пользователям), для этого нужно использовать команды chown и chmod:

```
# chown root:root /etc/postfix/sasl_passwd && chmod 600
/etc/postfix/sasl_passwd
```

Затем нужно преобразовать файл карты в индексированную карту для быстрого доступа postfix (нужно выполнять при каждом изменении файла sasl_passwd) с помощью следующей команды:

```
# postmap hash:/etc/postfix/sasl_passwd
```

8.10.4.2.2. Настройка postfix для использования верительных данных

Нужно сообщить клиенту postfix, где хранится созданная карта верительных данных аутентификации, для этого нужно в параметре smtp_sasl_password_maps в файле main.cf указать полный путь к файлу sasl_passwd, указывая при этом (с помощью спецификатора hash:), что значения карты хранятся в хеш-файле, например:

```
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
```

8.10.4.2.3. Отключение некоторых механизмов аутентификации

Для отключения использования ненадежных механизмов следует указать в параметре smtp_sasl_security_options список (через запятую) типов механизмов, которые клиент не может использовать. По умолчанию параметр smtp_sasl_security_options установлен в значение «noanonymous», но по возможности (если сервер поддерживает механизм с шифрованием, такой как DIGEST-MD5 или CRAM-MD5) следует также отключить использование механизмов открытого текста. Для этого нужно добавить в файл main.cf следующую строку:

```
smtp_sasl_security_options = noanonymous, noplaintext
```

8.10.5. Триггеры ограничений

Ограничения позволяют почтовому серверу принять или отвергнуть сообщения на основе данных SMTP-соединения между клиентом и сервером. Информация, полученная из этого диалога, позволяет postfix наложить или отменить ограничения на клиента (отправителя и получателя).

Postfix поддерживает следующие триггеры:

1) smtpd_client_restrictions – триггер применяется к IP-адресу или имени хоста клиента либо к ним обоим (по умолчанию postfix разрешает подключение любому клиенту);
2) smtpd_helo_restrictions – триггер применяется к аргументу HELO/EHLO клиента и к IP-адресу и (или) имени хоста клиента (по умолчанию допускается любой аргумент HELO/EHLO);
3) smtpd_sender_restrictions – набор триггеров, который относится к частям конверта (Postfix применяет его к отправителю конверта, аргументу HELO/EHLO и клиенту, по умолчанию любому отправителю конверта разрешено отправлять сообщения);
4) smtpd_recipient_restrictions – триггер применяется к получателям конверта, отправителю конверта, аргументу HELO/EHLO и к IP-адресу и (или) имени хоста клиента (по умолчанию postfix допускает любых получателей для клиентов, которые определены в параметре конфигурации mynet-works, для остальных же разрешены получатели в доменах из relay_domains и mydomains);
5) smtpd_data_restrictions – триггер выявляет клиенты, которые отправляют содержимое письма прежде, чем postfix ответит на команду DATA (Postfix выполняет это посредством трассировки DATA, когда клиент отправляет команду на сервер, по умолчанию ограничения нет);
6) smtpd_etrn_restrictions – специальный триггер может ограничить клиенты, которые могут запрашивать у postfix очистку очереди сообщений (по умолчанию всем клиентам разрешено выдавать команду ETRN).

В postfix существуют несколько видов ограничений, которые можно разбить на четыре группы:

1) общие ограничения;
2) переключаемые ограничения;
3) настраиваемые ограничения;
4) дополнительные параметры контроля спама.

Общие ограничения выполняют следующие команды:

1) `permit` – разрешает запрос;
2) `defer` – откладывает запрос;
3) `reject` – отвергает запрос;
4) `warn_if_reject` – содействует последующим ограничениям (если ограничение после `warn_if_reject` решает отвергнуть запрос, то postfix записывает в журнал сообщение `reject_warning`);
5) `reject_unauth_pipelining` – отвергает запрос, когда клиент отправляет команды SMTP раньше времени, еще не зная о том, действительно ли postfix поддерживает конвейерную обработку команд `ESMTP` (таким образом, достигается противодействие программам массовой рассылки, которые некорректно используют конвейерную обработку команд `ESMTP` для ускорения доставки).

Переключаемые ограничения работают как переключатели, при активации которых они проверяют выполнение некоторого условия. К переключаемым ограничениям относятся следующие:

1) `smtpd_helo_required` – ограничение, требующее от клиентов отправки команды `HELO` (или `EHLO`) в начале сеанса SMTP (наличия команды `HELO/EHLO` требуют RFC 821 и RFC 2821);
2) `strict_rfc821_envelopes` – ограничение, регулирующее степень терпимости postfix к ошибкам в адресах, указанных в команде `MAIL FROM` (отправитель конверта) или RCPT TO;
3) `disable_vrfy_command` – SMTP-команда `VRFY` позволяет клиентам проверять существование получателя (ограничение позволяет отменить команды `VRFY`);
4) `allow_percent_hack` – ограничение, регулирующее преобразование из формы «user%domain» в «user@domain»;
5) `swap_bangpath` – ограничение, контролирующее преобразование из формы «site!user» в «user@site» (нужно, если ПЭВМ подключена к сети UUCP).

Настраиваемые ограничения представляют собой карты, которые работают как фильтры. В каждой записи карты ключ является фильтром, а значение – тем действием, которое нужно выполнить при совпадении:

1) `HELO` (`EHLO`) имя хоста – ограничения, относящиеся к именам хостов, которые клиенты могут отправлять с командой `HELO` или `EHLO`;
2) имя хоста/адрес клиента – ограничения, определяющие клиенты, которые могут устанавливать SMTP-соединения с почтовым сервером;
3) адрес отправителя – ограничения, определяющие адреса отправителей (конвертов), которые postfix разрешает для использования в командах `MAIL FROM`;
4) адрес получателя – ограничения, определяющие адреса получателей (конвертов), которые postfix разрешает для использования в командах `RCPT TO`;
5) `ETRN!команды` – ограничение, накладываемое на клиенты, которые могут выдавать команды `ETRN`;
6) проверка заголовка – ограничение, регулирующее заголовки сообщений;
7) проверка тела – ограничения, накладываемые на текст, который может появляться в строках тела сообщения;
8) черные списки DNSBL – черные списки, ограничивающие соединения от IP-адресов (клиентов), которые включены в черные списки DNSBL;
9) черные списки RHSBL – черные списки, запрещающие те домены отправителей (конверта), которые присутствуют в черных списках RHSBL.

Дополнительные параметры контроля спама поддерживают другие ограничения или возможности, не входящие в функциональность postfix по умолчанию:

1) `default_rbl_reply` – создает шаблон ответа по умолчанию, который будет использоваться при блокировании запроса SMTP-клиента ограничением `reject_rbl_client` или `reject_rhsbl_sender`;

2) `permit_mx_backup_networks` – ограничивает использование функции контроля за пересылкой `permit_mx_backup` теми адресатами, у которых основные хосты MX входят в указанный список сетей;
3) `rbl_reply_maps` – определяет таблицы поиска и шаблоны ответов DNSBL, индексированные по имени домена DNSBL;
4) `relay_domains` – указывает postfix на нужность приема почты для этих доменов несмотря на то, что данный сервер не является местом их конечного назначения;
5) `smtpd_sender_login_maps` – определяет пользователя, которому разрешено использовать определенный адрес `MAIL FROM`.

В postfix по умолчанию встроен набор ограничений. Для того чтобы посмотреть список ограничений нужно выполнить следующую команду:

```
# postconf -d smtpd_recipient_restrictions
```

Для включения режима фильтрации почты в postfix в зависимости от наличия в них нежелательной информации (спам) нужно выполнить следующую команду:

```
control postfix filter
```

8.10.6. Алиасы и преобразование адресов

В postfix для передачи сообщений электронной почты используются алиасы, которые позволяют создавать псевдонимы для длинных или плохо запоминаемых адресов электронной почты. Настройка алиасов в postfix осуществляется с помощью таблиц aliases.

При установке postfix в таблице создается алиас на имя пользователя root: вся корреспонденция, предназначенная администратору и поступающая на другие системные адреса, будет отправляться на имя реального пользователя, который осуществляет функции администратора.

Рабочий образ таблицы строится с помощью следующей команды:

```
newaliases
```

а также при актуализации всех изменений посредством следующей команды:

```
service postfix reload
```

При отправке сообщения postfix формирует адрес отправителя автоматически из имени учетной записи пользователя и значения собственного домена (или значения «myorigin»). Преобразование адресов отправителей в глобальные адреса задаются в таблице типа canonical:

```
sender_canonical_maps = cdb:/etc/postfix/sender_canonical
```

Аналогичная таблица recipient_canonical и соответствующий параметр `recipient_canonical_maps` могут быть использованы для преобразования адресов назначения.

8.10.7. Настройка ограничений размера почтового ящика и отправляемого сообщения

По умолчанию размер файла почтового ящика при локальной доставке ограничен 51 200 000 байтами. Это ограничение можно изменить с помощью параметра `mailbox_size_limit`.

Например, снять ограничение можно установив этот параметр в 0:

```
mailbox_size_limit = 0
```

Также можно установить требуемый размер, указав в значении параметра величину:

```
mailbox_size_limit = <размер почтового ящика в байтах>
```

Для настройки размера отправляемого сообщения используется параметр `message_size_limit`:

```
message_size_limit = <размер сообщения в байтах>
```

Для настройки виртуальных аккаунтов используется параметр `virtual_mailbox_limit`:

```
virtual_mailbox_limit= <размер почтового ящика виртуального
аккаунта в байтах>
```

8.11. Соединение удаленных офисов (OpenVPN)

ОС Альт СП предоставляет возможность безопасного соединения удаленных офисов используя технологию VPN (англ. Virtual Private Network – виртуальная частная сеть), которая позволяет организовать безопасные шифрованные соединения через публичные сети (например, Интернет) между удаленными

офисами или локальной сетью и удаленными пользователями. Таким образом, можно связать различные офисы организации, что, делает работу с документами, расположенными в сети удаленного 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 своем привычном окружении, даже находясь в командировке или просто из дома.

8.11.1. Общие сведения об OpenVPN

OpenVPN – свободная реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами, находящимися за NAT-firewall, без нужности изменения их настроек.

Для обеспечения безопасности управляющего канала и потока данных OpenVPN использует библиотеку OpenSSL. Это позволяет задействовать весь набор алгоритмов шифрования, доступных в данной библиотеке. Также может использоваться пакетная авторизация HMAC, для обеспечения большей безопасности, и аппаратное ускорение для улучшения производительности шифрования. Эта библиотека использует OpenSSL, а точнее протоколы SSLv3/TLSv1.2.

Аутентификация в OpenVPN возможна несколькими способами:

- статическим ключом, распространяемым на каждого клиента;
- парой логин/пароль (как через самописный скрипт, так и с помощью плагинов: PAM, RADIUS и других);
- с использованием SSL-сертификатов;
- двухфакторная аутентификация (с использованием смарт-карт).

Размещение файлов OpenVPN:

- `/var/lib/openvpn/` – корневой каталог после инициализации демона (chroot);

- `/var/lib/openvpn/etc/openvpn/ccd` – каталог, в котором размещаются файлы особых параметров для подключаемых клиентов (Client Config Directory);
- `/var/lib/openvpn/cache` – рабочий каталог, является текущим для работы демона после инициализации (в него демон записывает файлы, у которых не указан путь, обычно это ipp и status);
- `/etc/openvpn/` – каталог с файлами настройки;
- `/etc/openvpn/ccd` – символическая ссылка на `/var/lib/openvpn/etc/openvpn/ccd` (файлы доступны и до, и после chroot). Требуется для отладки, когда openvpn запускается без chroot;
- `/etc/openvpn/keys/` – каталог для хранения ключей (информации ограниченного доступа).

8.11.2. Настройка OpenVPN-сервера в ЦУС

Для организации VPN соединения на стороне сервера предусмотрен модуль ЦУС «OpenVPN-сервер» (пакет alterator-openvpn-server) из раздела «Серверы» (рис. 100).

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 нужно установить флаг «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 нужно нажать на кнопку «Сертификат и ключ ssl..». Откроется окно модуля «Управление ключами SSL» (пакет alterator-sslkey) (рис. 101).

Здесь нужно заполнить поле «Общее имя (CN)» и поле «Страна (C)» (прописными буквами), отметить пункт «(Пере)создать ключ и запрос на подпись» и нажать на кнопку «Подтвердить». После чего станет активной кнопка «Забрать запрос на подпись» (рис. 102).

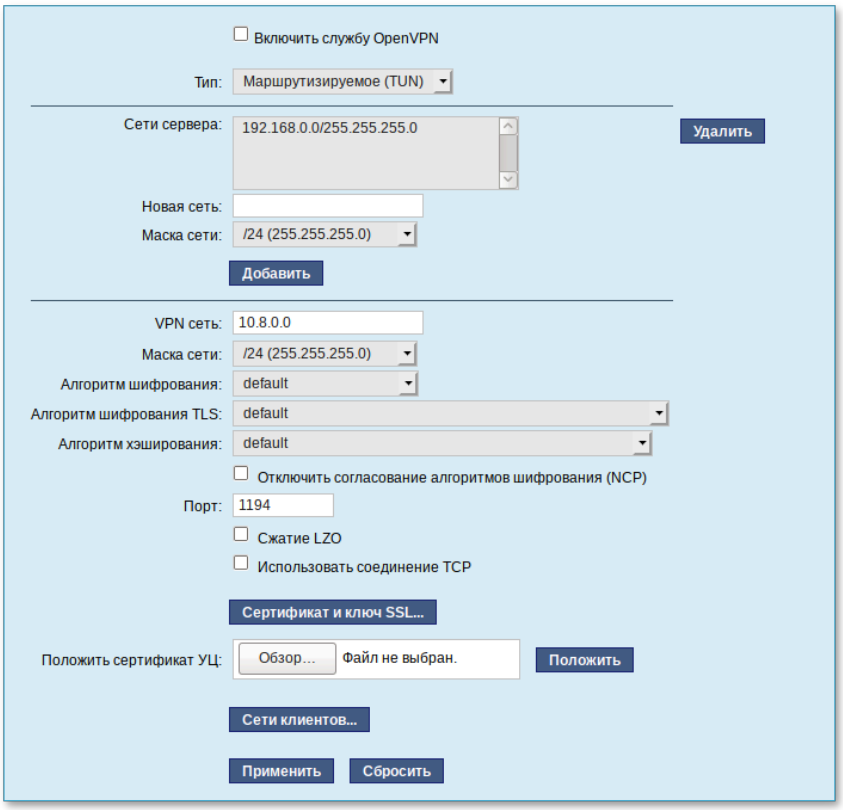


Рис. 100 – Модуль «OpenVPN-сервер»

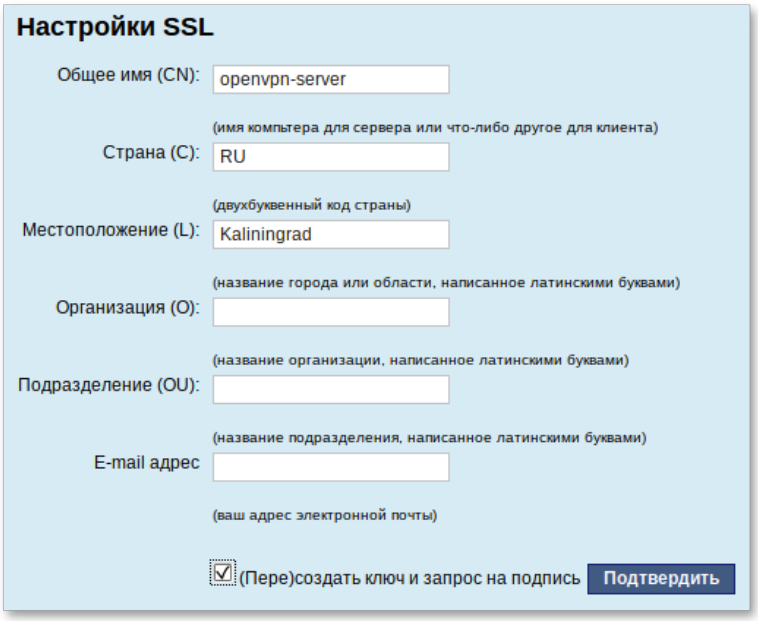


Рис. 101 – Настройки SSL

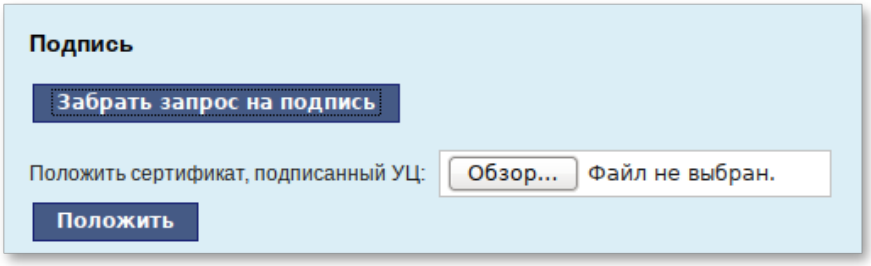


Рис. 102 – Кнопка «Забрать запрос на подпись»

Если нажать на кнопку «Забрать запрос на подпись» (рис. 102), появится диалоговое окно с предложением сохранить файл `openvpn-server.csr`. Нужно сохранить этот файл на диске.

В модуле «Управление ключами SSL» появился новый ключ «openvpn-server (Нет сертификата)» (рис. 103).

Чтобы подписать сертификат, нужно перейти в модуль «Удостоверяющий Центр» → «Управление сертификатами», нажать на кнопку «Обзор», указать путь до полученного файла `openvpn-server.csr` и загрузить запрос (рис. 104).

П р и м е ч а н и е . Для доступа к модулям «Управление ключами SSl»» и «Удостоверяющий Центр» необходимо переключиться в режим эксперта.

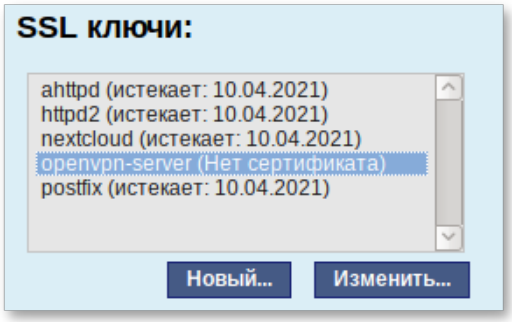


Рис. 103 – SSL ключи

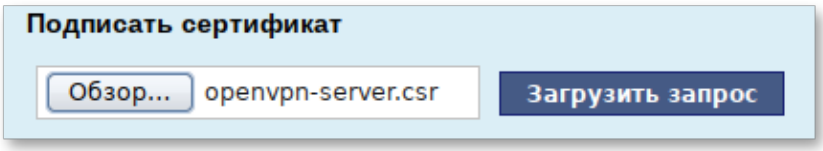
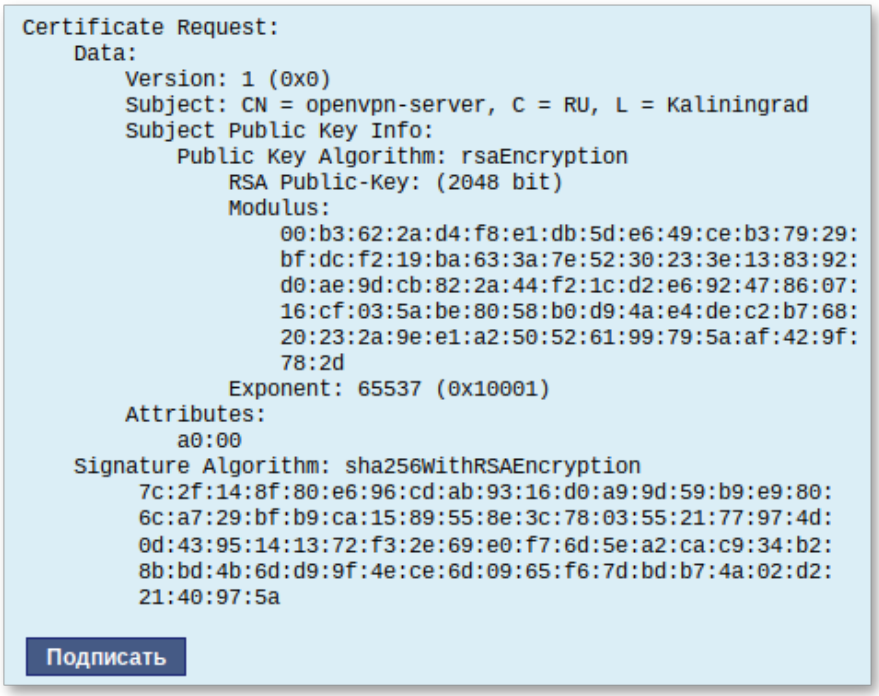


Рис. 104 – Кнопка «Подписать сертификат»

В результате на экране появится две группы цифр и кнопка «Подписать». Нужно нажать на кнопку «Подписать» и сохранить файл `output.pem` (подписанный сертификат) (рис. 105).



```
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:b3:62:2a:d4:f8:e1:db:5d:e6:49:ce:b3:79:29:
                    bf:dc:f2:19:ba:63:3a:7e:52:30:23:3e:13:83:92:
                    d0:ae:9d:cb:82:2a:44:f2:1c:d2:e6:92:47:86:07:
                    16:cf:03:5a:be:80:58:b0:d9:4a:e4:de:c2:b7:68:
                    20:23:2a:9e:e1:a2:50:52:61:99:79:5a:af:42:9f:
                    78:2d
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         7c:2f:14:8f:80:e6:96:cd:ab:93:16:d0:a9:9d:59:b9:e9:80:
         6c:a7:29:bf:b9:ca:15:89:55:8e:3c:78:03:55:21:77:97:4d:
         0d:43:95:14:13:72:f3:2e:69:e0:f7:6d:5e:a2:ca:c9:34:b2:
         8b:bd:4b:6d:d9:9f:4e:ce:6d:09:65:f6:7d:bd:b7:4a:02:d2:
         21:40:97:5a
```


Рис. 105 – Подписание сертификата

Далее в разделе «Управление ключами SSL», нужно выделить ключ «openvpn-server (Нет сертификата)» и нажать на кнопку «Изменить». В появившемся окне, в пункте «Положить сертификат, подписанный УЦ» нужно нажать на кнопку «Обзор», указать путь до файла `output.pem` и нажать на кнопку «Положить» (рис. 106).

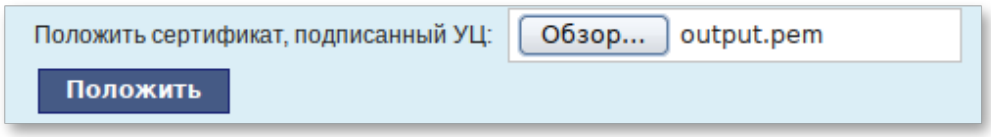


Рис. 106 – Кнопка «Положить»

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

Для того чтобы положить сертификат удостоверяющего центра (УЦ), нужно найти его в модуле «Удостоверяющий Центр» ЦУС, нажать на ссылку «Управление УЦ» и забрать сертификат, нажав на ссылку «Сертификат: ca-root.pem» (рис. 107).

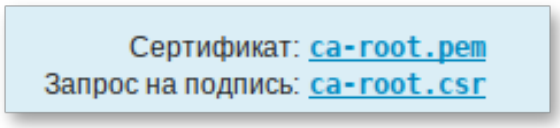


Рис. 107 – Ссылка «Сертификат»

В модуле «OpenVPN-сервер», в графе «Положить сертификат УЦ:» при помощи кнопки «Обзор» указать путь к файлу `ca-root.pem` и нажать на кнопку «Положить» (рис. 108).

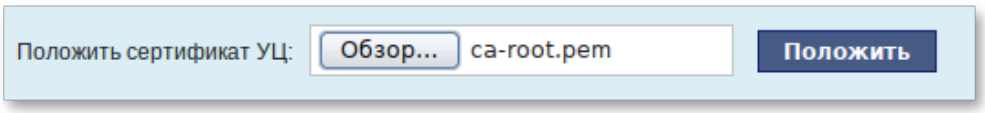


Рис. 108 – Графа «Положить сертификат УЦ:»

Появится сообщение: «Сертификат УЦ успешно загружен».

Для включения OpenVPN нужно отметить пункт «Включить службу OpenVPN» и нажать на кнопку «Применить».

Если нужно организовать защищенное соединение между двумя локальными сетями, воспользуйтесь модулем «OpenVPN-соединения» (раздел «Сеть») (п. 8.11.3).

8.11.3. Настройка клиентов в ЦУС

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 нужно отметить пункт «Сетевой туннель (TUN)» или «Виртуальное Ethernet устройство (TAP)» и нажать на кнопку «Создать соединение» (рис. 109).

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 и подписать SSL ключ клиента в удостоверяющем центре сервера (модуль «Удостоверяющий Центр» (пакет alterator-ca) из раздела «Система»). Процесс подписания аналогичен подписанию запроса для сервера.

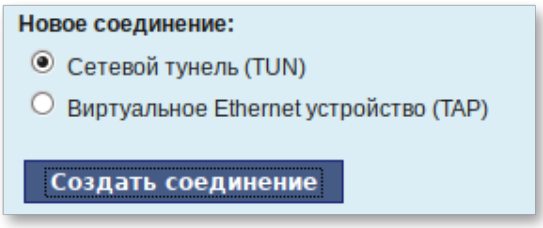


Рис. 109 – Вкладка «Новое соединение»

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

- состояние – «запустить»;
- сервер – IP-адрес сервера или домен;

- порт – 1194;

- ключ – выбрать подписанный на сервере ключ.

Для применения настроек, нажать на кнопку «Применить» (рис. 110). Состояние с «Выключено» должно поменяться на «Включено».

Проверить, появилось ли соединение с сервером можно командой:

```
ip addr
```

должно появиться новое соединение tun1. При обычных настройках это может выглядеть так:

```
tun1: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 100
    link/[none]
    inet 10.8.0.6 peer 10.8.0.5/32 scope global tun0
```

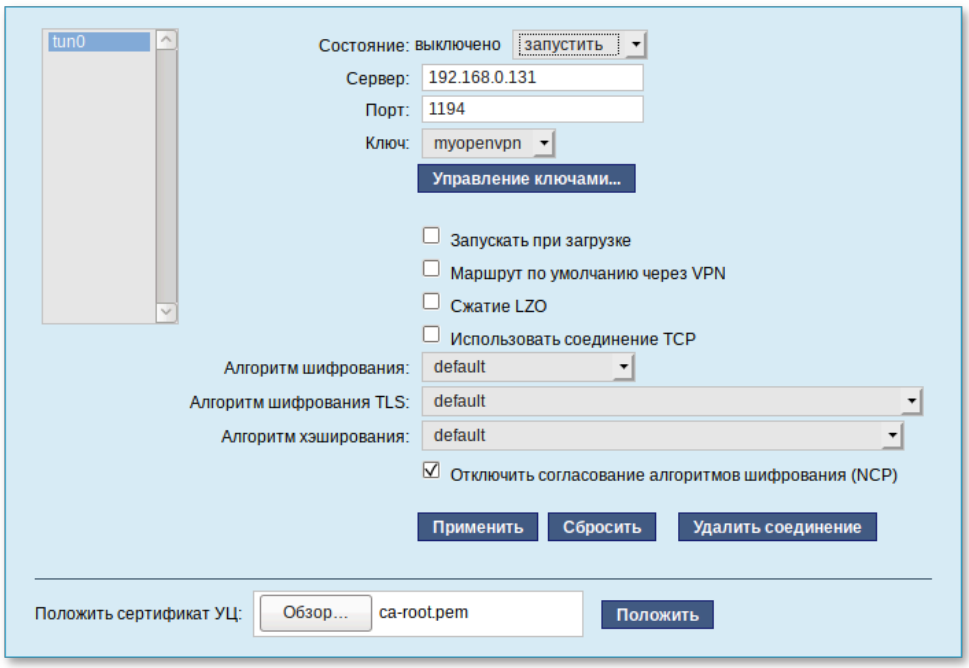


Рис. 110 – Применение настроек

8.11.4. Конфигурирование openvpn

Каждый файл конфигурации по маске `/etc/openvpn/*.conf` является конфигурацией отдельного экземпляра демона openvpn. Для имени экземпляра берется имя файла без суффикса `.conf`.

Настройки стартового скрипта располагаются в файле /etc/sysconfig/openvpn, по умолчанию он устанавливает следующие переменные окружения:

```
CHROOT=yes
OPENVPNUSER=openvpn
OPENVPNGROUP=openvpn
MANUAL=""
```

Стартовый скрипт /etc/init.d/openvpn может запускать и останавливать как все экземпляры демона, так и каждый по отдельности. Значение переменной MANUAL в /etc/sysconfig/openvpn указывает экземпляры, которые не нужно запускать при старте системы (и при запуске стартового скрипта без параметра).

Для запуска openvpn можно использовать следующие команды:

```
# service openvpn start
```

или

```
# systemctl start openvpn
```

Если есть экземпляры, которые запускать не нужно, их можно вписать в переменную MANUAL в /etc/sysconfig/openvpn. Переменные записываются как названия конфигурационных файлов без *.conf.

При запуске сервиса, демон openvpn запускается, читает файл конфигурации из /etc/openvpn/, читает оттуда же файлы dh, ca и ключи. Этот каталог доступен демону только при его запуске.

Далее демон выполняет chroot в /var/lib/openvpn/ и cd в /var/lib/openvpn/cache, понижает привилегии до пользователя openvpn, затем инициализирует работу с сетью.

Таким образом, файл конфигурации должен быть размещен в /etc/openvpn, все ключи – в /etc/openvpn/keys, файлы настроек клиентов – в /etc/openvpn/ccd/ или /var/lib/openvpn/etc/openvpn/ccd/.

Важно правильно указать права доступа. Ключи должны быть доступны только администратору, конфигурации клиентов должны быть доступны на чтение пользователю openvpn:

```
# chown root:root /etc/openvpn/keys/* ; chmod 600 /etc/openvpn/keys/*
```

```
# chown root:openvpn /var/lib/openvpn/etc/openvpn/ccd/* ; chmod 640 /var/lib/openvpn/etc/openvpn/ccd/*
```

В файле конфигурации должны быть указаны:

- `ifconfig-pool-persist` и `status` – без полного пути либо с путем `/cache/`;
- `ca, dh, cert, key` – с путем `/etc/openvpn/keys/`;
- `client-config-dir /etc/openvpn/ccd`.

Далее приводится пример конфигурации в файле `server.conf`:

```
$ cat /etc/openvpn/server.conf
port 1194
proto udp
dev tun
ca /etc/openvpn/keys/admin.ca
dh /etc/openvpn/keys/dh4096.pem
cert /etc/openvpn/keys/server.crt
key /etc/openvpn/keys/server.key
comp-lzo
server 192.168.254.0 255.255.255.0
tls-server
cipher AES-256-CBC
verb 3
mute 10
keepalive 10 60
user nobody
group nogroup
persist-key
persist-tun
status server_status.log
ifconfig-pool-persist server_ipp.txt
verb 3
management localhost 1194
push "route 192.168.1.0 255.255.255.0"
client-config-dir /etc/openvpn/ccd
route 192.168.2.0 255.255.255.0
route 192.168.3.0 255.255.255.0
```

8.11.5. Создание ключей для OpenVPN туннеля средствами утилиты openssl

Для создания туннеля средствами утилиты openssl нужно выполнить следующие действия:

1) проверить наличие в системе установленного пакета openssl с помощью следующей команды:

```
# rpm -qa openssl
```

2) для возможности подписывать любые сертификаты, нужно открыть файл `/var/lib/ssl/openssl.cnf` и изменить значение параметра policy на следующее:

```
policy = policy_anything
```

Кроме этого, в файле `/var/lib/ssl/openssl.cnf` нужно проверить параметры `keyUsage` и `extendedKeyUsage` в секции `[usr_cert]`:

- для сервера должны быть указаны следующие расширения:

  ```
  keyUsage = nonRepudiation, digitalSignature, keyEncipherment
  extendedKeyUsage = TLS Web Server Authentication
  ```

- для клиента:

  ```
  keyUsage = digitalSignature
  extendedKeyUsage = TLS Web Client Authentication
  ```

Если предполагается, что ПЭВМ будет являться и сервером, и клиентом, можно записать расширения следующим образом:

```
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = TLS Web Server Authentication,TLS Web Client Authentication
```

Эти расширения будут добавлены в момент подписи сертификата. Без них у клиента могут возникнуть проблемы с проверкой сертификатов, и он не сможет подключиться к VPN-серверу;

3) создать папку:

```
# mkdir -p /root/CA/demoCA
```

4) перейти в каталог:

```
# cd /root/CA
```

5) создать в каталоге `/root/CA` следующие папки и файлы:

```
# mkdir -p ./demoCA/newcerts
# touch ./demoCA/index.txt
# echo '01' > ./demoCA/serial
# echo '01' > ./demoCA/crlnumber
```

где:

- `demoCA/newcerts` – каталог сертификатов;

- `demoCA/index.txt` – текстовый файл, база с действующими и отозванными сертификатами;
- `demoCA/serial` – файл индекса для базы ключей и сертификатов;
- `demoCA/crlnumber` – файл индекса для базы отозванных сертификатов;

6) создать «самоподписанный» сертификат `my-ca.crt` и закрытый ключ `my-ca.pem`, которыми будут заверяться/подписываться ключи и сертификаты клиентов, желающих подключиться к серверу, с помощью следующей команды:

```
# openssl req -new -x509 -keyout my-ca.pem -out my-ca.crt
```

где:

- `-req` – запрос на создание сертификата;
- `-x509` – создать самоподписанный сертификат стандарта X.509;
- `-keyout` – записать закрытый ключ в файл;
- `-out` – записать сертификат в файл;

7) ввести пароль для закрытого ключа и ответить на запросы о владельце ключа;

8) создать пару «ключ-сертификат» для сервера и каждого клиента, желающего подключиться к серверу, с помощью следующей команды:

```
# openssl req -new -nodes -keyout server.pem -out server.crs
```

где `-nodes` – означает, что шифровать закрытый ключ не нужно;

9) подписать запрос на сертификат своим «самоподписанным» my-ca.crt сертификатом и ключом my-ca.pem с помощью следующей команды:

```
# openssl ca -cert my-ca.crt -keyfile my-ca.pem -days 3650 -in server.crs -out server.crt
```

где:

- `-cert` – корневой сертификат удостоверяющего центра;
- `-keyfile` – секретный ключ удостоверяющего центра;

10) после получения связки «ключ-сертификат» для сервера server сгенерировать запрос на сертификат для пользователя:

```
# openssl req -new -nodes -keyout user_1.pem -out user_1.crs
```

11) подписать запрос на сертификат своим my-ca.crt сертификатом и ключом my-ca.pem:

```
# openssl ca -cert my-ca.crt -keyfile my-ca.pem -days 365 -in user_1.crs -out user_1.crt
```

12) задать параметры Диффи-Хеллмана для сервера:

```
# openssl dhparam -out server.dh 2048
```

13) удалить файлы запросов на сертификаты:

```
# rm *.crs
```

14) проверить состав каталога /root/CA (состав файлов должен соответствовать приведенному ниже):

```
# ls -l
итого 40
drwxr-xr-x 3 root root 4096 авг 26 15:07 demoCA
-rw-r--r-- 1 root root 1123 авг 26 14:47 my-ca.crt
-rw-r--r-- 1 root root 1834 авг 26 14:47 my-ca.pem
-rw-r--r-- 1 root root 4202 авг 26 14:58 server.crt
-rw-r--r-- 1 root root 424 авг 26 15:14 server.dh
-rw-r--r-- 1 root root 1708 авг 26 14:52 server.pem
-rw-r--r-- 1 root root 4190 авг 26 15:07 user_1.crt
-rw-r--r-- 1 root root 1708 авг 26 15:05 user_1.pem
```

15) разместить ключи и сертификаты в каталогах сервера и клиента следующим образом:

- my-ca.crt – для сервера и клиентов;
- my-ca.pem – только для подписи сертификатов (лучше хранить на отдельном от OpenVPN сервера компьютере);
- my-ca.crt, server.crt, server.dh, server.pem – для сервера OpenVPN;
- my-ca.crt, user_1.crt, user_1.pem – для клиента OpenVPN;

16) для новых клиентов создать новые ключи и отдать комплектом my-ca.crt, новый_сертификат.crt, новый_ключ.pem;

17) в конфигурационном файле OpenVPN сервера поместить ссылки на эти ключи:

```
ca /root/CA/my-ca.crt
cert /root/CA/server.crt
key /root/CA/server.pem
dh /root/CA/server.dh
```

18) в конфигурационном файле OpenVPN клиента поместить ссылки на эти ключи:

```
ca /etc/net/ifaces/tun0/my-ca.crt
cert /var/lib/ssl/certs/user_1.crt
key /var/lib/ssl/private/user_1.pem
```

19) просмотреть базу ключей:

```
# cat /root/CA/demoCA/index.txt
V 250823115811Z 01 unknown /C=RU/CN=vpn-server
V 160825120737Z 02 unknown /C=RU/CN=user_1
```

где `V` – действующий (валидный) ключ.

8.11.6. Создание списка отзыва сертификатов

Для создания списка отзыва сертификатов нужно выполнить следующие действия:

1) выполнить следующую команду:

```
# openssl ca -cert my-ca.crt -keyfile my-ca.pem -gencrl -out crl.pem
```

2) просмотреть содержимое файла `crl.pem` с помощью следующей команды:

```
# openssl crl -noout -text -in crl.pem
```

3) отозвать сертификат `user_1.crt`:

```
# openssl ca -cert my-ca.crt -keyfile my-ca.pem -revoke user_1.crt -out crl.pem
```

4) обновить список (обязательно после каждого отзыва сертификата):

```
# openssl ca -cert my-ca.crt -keyfile my-ca.pem -gencrl -out crl.pem
```

5) просмотреть `crl.pem`:

```
# openssl crl -noout -text -in crl.pem
```

6) поместить файл `crl.pem` в каталог `/var/lib/openvpn`.

8.11.7. Создание ключей для OpenVPN туннеля средствами Easy-Rsa скриптов

Для работы с утилитой Easy-Rsa нужно установить пакет easy-rsa с помощью следующей команды:

```
# apt-get install easy-rsa
```

Далее нужно выполнить поиск по ключевому слову "easyrsa*", чтобы посмотреть, куда выполнялась установка утилиты:

```
# find / -name "easyrsa*"
/usr/bin/easyrsa
/usr/share/easyrsa3
```

В OpenSSL есть пример файла openssl.cnf, который находится в соответствующей папке. По умолчанию утилита openssl обращается к файлу /var/lib/ssl/openssl.cnf.

В файле конфигурации есть несколько полезных параметров – например, местонахождение серийных номеров и списка отозванных сертификатов (Certificate Revocation List).

Однако некоторые записи из раздела CA_default ссылаются на директории и файлы, которые, в случае их отсутствия, могут привести к проблемам при развертывании центра сертификации. В связи с этим нужно создать все требуемые файлы и папки перед тем, как подписывать CSR. В составе OpenSSL включена утилита CA.pl, которая упрощает процесс подготовки директорий и файлов.

В каталоге /usr/share/easyrsa3 находятся следующие файлы:

```
openssl-easyrsa.cnf vars.example x509-types
```

Файл openssl-easyrsa.cnf, является конфигуратором для утилиты openssl, запущенной через скрипты easy-rsa. Программа упрощает процесс создания инфраструктуры каталогов PKI.

Нужно перейти в каталог, в котором будет создаваться инфраструктура каталогов для ключей и сертификатов, с помощью следующей команды:

```
# cd /root
```

Затем нужно создать структуру каталогов с помощью следующей команды:

```
# easyrsa init-pki
```

В текущей директории будет создан каталог pki с вложенными каталогами для ключей и запросов.

Дальнейшие действия также нужно выполнять в текущей директории, иначе утилита будет выводить ошибки из-за отсутствия pki каталога в текущей директории при запуске easyrsa команды.

8.11.7.1. Создание ключей центра сертификации с помощью Easy-Rsa скриптов

Для создания ключей центра сертификации нужно создать корневой сертификат. Для этого нужно запустить easyrsa с помощью следующей команды:

```
# easyrsa build-ca
```

Далее будет выведен процесс генерации, в ходе которого нужно указать сложный пароль и Common Name сервера, например, CA-ORG:

```
Generating a 2048 bit RSA private key
.....................................................+++
.....................................................+++
writing new private key to '/root/pki/private/ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
...
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:CA-ORG
CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/root/pki/ca.crt
```

Затем нужно создать ключи Диффи-Хелмана:

```
# easyrsa gen-dh
```

Создание ключа занимает некоторое продолжительное время. Далее нужно проверить содержание каталога `pki` с помощью следующей команды:

```
# ls -l ./pki
```

Содержание каталога должно соответствовать приведенному ниже:

```
итого 28
-rw------- 1 root root 1151 авг 27 09:32 ca.crt
drwx------ 2 root root 4096 авг 27 09:32 certs_by_serial
-rw------- 1 root root 424 авг 27 09:38 dh.pem
-rw------- 1 root root 0 авг 27 09:32 index.txt
drwx------ 2 root root 4096 авг 27 09:32 issued
drwx------ 2 root root 4096 авг 27 09:32 private
drwx------ 2 root root 4096 авг 27 09:28 reqs
-rw------- 1 root root 3 авг 27 09:32 serial
```

где:

- `ca.crt` – сертификат корневого центра сертификации;

- `dh.pem` – ключ Диффи-Хелмана;

- `./private/ca.key` – секретный ключ центра сертификации.

8.11.7.2. Создание ключей сервера с помощью Easy-Rsa скриптов

Создать запрос на сертификат для сервера OVPN. Сертификат будет не зашифрован (запаролен), за это отвечает параметр nopass, иначе при каждом старте OpenVPN будет запрашивать этот пароль:

```
easyrsa gen-req vpn-server nopass
```

Скопировать полученные ключи в рабочий каталог openvpn и в конфигурации сервера указать полный путь к ключам:

```
cp ./pki/ca.crt /etc/openvpn/keys
cp ./pki/issued/vpn-server.crt /etc/openvpn/keys
cp ./pki/private/vpn-server.key /etc/openvpn/keys
cp ./pki/dh.pem /etc/openvpn/keys
```

Для создания пары ключ/сертификат минуя создание запросов и подписи нужно выполнить команду:

`easyrsa build-server-full vpn-server nopass` – без пароля.

`easyrsa build-server-full vpn-server` – с паролем.

8.11.7.3. Создание клиентских ключей с помощью Easy-Rsa скриптов

Процесс создания ключей клиентам аналогичен созданию ключей для сервера. Создание запроса запароленного ключа для клиента (потребуется вводить при каждом подключении) с именем `User` выполняется с помощью следующей команды:

```
easyrsa gen-req User
```

Создание запроса без парольного ключа для клиента выполняется с помощью следующей команды:

```
easyrsa gen-req User nopass
```

Создание ключа пользователя выполняется с помощью следующей команды:

```
easyrsa sign-req client User
```

Создание ключа пользователя с ограничением действия сертификата в 90 дней (после истечения срока можно только перевыпустить) выполняется с помощью следующей команды:

```
# easyrsa sign-req client User -days 90
```

Передача файлов клиенту выполняется с помощью следующей команды:

```
./pki/issued/User.crt
./pki/private/User.key
./pki/ca.crt
```

Копирование файлов с одного компьютера на другой можно выполнить с помощью утилиты scp и команд:

```
scp /pki/issued/User.crt user@<ip-address>:/<path>
scp /pki/private/User.key user@<ip-address>:/<path>
scp /pki/ca.crt user@<ip-address>:/<path>
```

где `<path>` путь сохранения файлов.

Для создания пары ключ/сертификат минуя создание запросов и подписи нужно выполнить команду:

`easyrsa build-client-full User nopass` – без пароля

`easyrsa build-client-full User` – с паролем

8.11.8. Отзыв сертификатов

Генерация файла отозванных ключей выполняется с помощью следующей команды:

```
# easyrsa gen-crl
```

Сделать символическую ссылку в каталог с ключами:

```
# ln -s /root/pki/crl.pem /var/lib/openvpn
```

В файл конфигурации openvpn сервера добавить строку:

```
# crl-verify crl.pem
```

Отзыв сертификата пользователя User выполняется с помощью следующей команды:

```
# easyrsa revoke User
```

Каждый раз при отзыве сертификата нужно обновлять `crl.pem`, чтобы внести в него изменения:

```
# easyrsa gen-crl
```

Одноименный файл ключа не может быть создан, пока не отозван старый. Для исключения возможности mitm атаки служит параметр `remote-cert-tls server`. Список валидных и отозванных сертификатов можно посмотреть в файле `./pki/index.txt`. Начало строки описания каждого сертификата начинается с букв V или R, что значит Valid и Revoked (действующий и отозванный).

8.12. Настройка удаленного подключения

Для получения удаленного доступа к другим ПЭВМ и предоставления такого доступа в ОС Альт СП используется протокол SSH (Secure Shell).

SSH реализует соединение с удаленным компьютером, защищающее от следующих угроз:

- прослушивание данных, передаваемых по этому соединению;
- манипулирование данными на пути от клиента к серверу;
- подмена клиента, либо сервера, путем манипулирования IP-адресами, DNS, либо маршрутизацией.

SSH обладает следующими возможностями:

- сжатие передаваемых данных;
- туннелирование каналов внутри установленного соединения – в том числе соединений с X-сервером;
- широкая распространенность: существуют реализации SSH для самых различных аппаратных платформ и ОС.

OpenSSH – реализация SSH, входящая в состав дистрибутива. Эта реализация включает в себя следующие программы и утилиты:

- клиентские программы ssh, scp и sftp (используются для запуска программ на удаленных серверах и копирования файлов по сети);
- серверные программы sshd, sftp-server (используются для предоставления доступа по протоколу SSH);
- вспомогательные программы scp, rescp, ssh-keygen, ssh-add, ssh-agent, ssh-copy-id, ssh-keyscan.

8.12.1. OpenSSH, сервер протокола SSH (sshd)

OpenSSH Daemon (sshd) – программа-сервер, обслуживающая запросы программы-клиента ssh. Вместе эти программы заменяют rlogin и rsh и обеспечивают защищенную и кодированную связь между двумя непроверенными компьютерами через незащищенную сеть.

sshd – это служба, принимающая запросы на соединения от клиентов. Для каждого нового соединения создается (с помощью вызова «fork») новый экземпляр службы. Ответвленный экземпляр обрабатывает обмен ключами, кодирование, аутентификацию, выполнение команд и обмен данными.

Параметры определяются при помощи ключей командной строки или файла конфигурации (по умолчанию – `sshd_config`). Ключи командной строки имеют больший приоритет, чем значения, указанные в файле конфигурации. При получении сигнала отбоя SIGHUP перечитывает свой файл конфигурации путем запуска собственной копии с тем же самым именем, с которым был запущен, например, `/usr/sbin/sshd`.

Синтаксис команды:

`sshd [-46Ddeiqt] [-b длина ключа_1] [-f файл конфигурации] [-g время_задержки_регистрации] [-h файл_ключа_хоста] [-k частота_генерации_ключа] [-o директива] [-p порт] [-u длина]`

Доступны ключи, приведенные в таблице 6.

Т а б л и ц а 6 – Ключи команды sshd

Ключ	Описание
`-4`	Использовать только адреса IPv4
`-6`	Использовать только адреса IPv6
`-b длина_ключа_1`	Определяет число битов в ключе сервера протокола версии 1 (по умолчанию 1024)
`-D`	Не переходить в фоновый режим и не становиться службой. Это упрощает слежение за экземпляром sshd
`-d`	Режим отладки. Сервер посылает расширенную отладочную информацию в файл журнала событий системы и не переходит в фоновый режим работы. Сервер не создает дочерних процессов и обрабатывает только одно соединение. Параметр предназначен только для отладки работы сервера. Несколько параметров `-d` указанных один за другим, повышают уровень отладки. Максимум – это 3
`-e`	Направлять вывод в консоль (stderr) вместо механизма журналирования событий системы
`-f файл_конфигурации`	Определяет имя файла конфигурации (по умолчанию – `/etc/openssh/sshd_config`). Не работает, если нет файла конфигурации
`-g время_задержки_регистрации`	Определяет период, в течение которого клиент должен себя идентифицировать (по умолчанию – 120 секунд). Если клиент не смог идентифицировать себя в течение этого времени, экземпляр сервера прекращает свою работу. Значение равное нулю отменяет ограничение на время ожидания
`-h файл_ключа_хоста`	Определяет файл, из которого будет считан ключ хоста. Этот параметр должен быть указан, если запущен не от имени пользователя с идентификатором root (так как обычно стандартные файлы хоста доступны для чтения только пользователю с идентификатором root). Стандартное расположение файла – `/etc/openssh/ssh_host_key` для протокола версии 1, и `/etc/openssh/ssh_host_dsa_key`, `/etc/openssh/ssh_host_ecdsa_key` и `/etc/openssh/ssh_host_rsa_key` для протокола версии 2. Можно иметь несколько ключей хоста для разных версий протокола и алгоритмов генерации ключей
`-i`	Позволяет уведомить программу о том, что она запускается службой inetd. Обычно sshd не запускается из inetd, так как требуется генерировать ключ сервера до ответа клиенту, а это может отнять десятки секунд. Клиент будет вынужден ожидать слишком долго, если ключ будет повторно генерироваться каждый раз. Однако, при малых размерах ключа (например, 512), использование из inetd может быть оправдано

Окончание таблицы 6

Ключ	Описание
`-k частота_генерации_ключа`	Определяет, как часто будет регенерироваться ключ сервера протокола версии 1 (по умолчанию 3600 секунд – один раз в час). Значение ноль означает, что ключ никогда не будет регенерирован
`-o директива`	Позволяет указывать директивы в формате файла конфигурации, например, такие, для которых нет соответствующего ключа командной строки. Директивы файла конфигурации описаны в sshd_config
`-p порт`	Порт, на котором сервер будет ожидать соединения (по умолчанию – 22). Возможно указание нескольких ключей с разными портами. Если данный ключ указан, параметр Port файла конфигурации игнорируется, однако порты, указанные в `ListenAddress` имеют больший приоритет, чем указанные в командной строке
`-q`	Не заносить в системный журнал регистрации событий никакой информации. В обычном режиме в нем фиксируется подключение, аутентификация и разрыв каждого соединения.
`-t`	Режим тестирования. Выполняется только проверка соответствия файла конфигурации и готовность ключей. Полезно для проверки состояния службы после обновления, при котором были изменены файлы конфигурации
`-u длина`	Размер поля в структуре utmp хранящей имя удаленного хоста. Если разрешенное имя хоста превышает указанное значение, то взамен будет использован десятичное представление IP-адреса через точку. Это позволяет уникально идентифицировать машины со слишком длинными именами. Указание `-u0` включает использование в файле utmp IP-адресов во всех случаях. При этом будет производить DNS-запросы только если это явно требуется конфигурацией (`from="pattern-list"`) или механизмом аутентификации (либо `RhostsRSAAuthentication` либо `HostbasedAuthentication`). Использование DNS также обязательно в случае задания параметрам `AllowUsers` и `DenyUsers` значения в формате `USER@HOST`

8.12.1.1. Аутентификация

Служба OpenSSH SSH поддерживает версии протокола SSH 1 и 2. При этом использование протокола версии 1 крайне не рекомендуется. Запретить использование одного протокола версии 1 можно, указав в параметре `Protocol` файла `/etc/openssh/sshd_config`:

```
Protocol 2
```

Протокол 2 поддерживает ключи DSA, ECDSA и RSA; протокол 1 поддерживает только ключи RSA. Независимо от протокола, каждый подключающийся хост имеет собственный, обычно 2048-битный идентифицирующий его ключ.

Для протокола версии 1 подтверждение субъекта сервера обеспечивается 768-битным ключом, который генерируется при запуске сервера. Ключ генерируется заново каждый час, при условии его использования, и не хранится на диске. При получении запроса на подключение со стороны клиента служба посылает в ответ свой открытый ключ и свои ключи. Клиент сравнивает ключ хоста RSA со своими данными, чтобы убедиться в том, что это тот же сервер. Затем клиент генерирует 256-битное произвольное число, шифрует его при помощи обоих ключей (своего и сервера) и отправляет результат серверу. Это число становится ключом сеанса, и с его помощью выполняется кодирование всех последующих данных, по согласованному методу – Blowfish или 3DES (клиент выбирает метод из предложенных сервером). В настоящее время по умолчанию используется 3DES.

Для протокола версии 2 подтверждение субъекта сервера обеспечивается по схеме Диффи-Хеллмана, в результате которой также получается общий ключ сеанса. Дальнейший обмен данными шифруется симметричным кодом, 128-битным AES, Blowfish, 3DES, CAST128, Arcfour, 192-битным AES или 256-битным AES, который выбирает клиент из предложенных сервером. Кроме того, целостность передаваемых данных обеспечивается кодом подтверждения подлинности сообщения (hmac-md5, hmac-sha1, umac-64, hmac-ripemd160, hmac-sha2-256 или hmac-sha2-512).

Далее, сервер и клиент переходят в режим аутентификации. Клиент пытается аутентифицировать себя по своему хосту, открытому ключу, паролю или с помощью беспарольного механизма («вызов-ответ»).

Независимо от типа аутентификации служба проверяет доступность соответствующей учетной записи в системе. Так, она может быть заблокирована посредством добавления ее в параметр `DenyUsers` или ее группы в `DenyGroups`. Для

запрета только аутентификации по паролю укажите в файле passwd 'NP' или '*NP*'.

После успешной аутентификации себя клиентом связь переходит в режим подготовки сеанса. В этот момент клиент может запросить такие вещи, как выделение псевдо-терминала, перенаправление соединения X11, перенаправление соединения TCP/IP или перенаправление соединения агента аутентификации через защищенный канал.

Наконец, клиент запрашивает оболочку или выполнение команды, после чего стороны входят в режим сеанса. В этом режиме, каждая из сторон в любой момент может пересылать данные и эти данные будут переданы оболочке или команде на стороне сервера и на пользовательский терминал соответственно.

По завершении работы пользовательской программы и закрытии всех перенаправленных X11 и других соединений сервер посылает клиенту команду со статусом выхода и сеанс завершается.

8.12.1.2. Вход в систему

После успешной аутентификации пользователя выполняются следующие действия:

- если регистрация в системе произведена на терминале (tty) и не указана никакая команда, то отображается время последнего входа в систему и содержимое файла /etc/motd (если только это не отключено в файле конфигурации или ~/.hushlogin);
- если регистрация в системе произведена на терминале, записывается время регистрации;
- проверяется /etc/nologin если он присутствует, выводится его содержимое и завершается работа (исключение – root);
- осуществляется переход к выполнению с правами обычного пользователя;
- устанавливаются значения основных переменных среды;
- интерпретируется файл ~/.ssh/environment, если таковой имеется, и пользователям разрешено изменять среду;
- происходит переход в домашний каталог пользователя;

- если имеется файл `~/.ssh/rc`, то производится его выполнение, а если нет и имеется `/etc/openssh/sshrc`, то выполняется он, в противном случае выполняется xauth. Файлам rc на стандартный ввод передается протокол аутентификации X11 и cookie;
- запускается оболочка пользователя или выполняется указанная команда.

8.12.1.3. SSHRC

Если файл `~/.ssh/rc` существует, он будет выполняться после файлов определения переменных среды, но перед запуском оболочки пользователя или команды. Если используется подмена X11, то на его стандартный ввод будет передана пара «proto cookie», также ему будет доступна переменная среды DISPLAY. Сценарий должен вызывать xauth самостоятельно для добавления cookie X11.

Основная цель этого файла состоит в выполнении процедур инициализации, прежде, чем станет доступным основной каталог пользователя. AFS – пример такой среды.

Этот файл будет, содержать блок аналогичный следующему:

```
if read proto cookie && [ -n "$DISPLAY" ]; then
if [ `echo $DISPLAY | cut -c1-10` = 'localhost:' ]; then
# X11UseLocalhost=yes
echo add unix:`echo $DISPLAY |
cut -c11-` $proto $cookie
else
# X11UseLocalhost=no
echo add $DISPLAY $proto $cookie
fi | xauth -q -
fi
```

Если этот файл отсутствует, то выполняется `/etc/openssh/sshrc`, а если отсутствует и он, то для добавления cookie используется xauth.

8.12.1.4. Формат файла authorized_keys

Параметр `AuthorizedKeysFile` файла конфигурации определяет путь к файлу с открытыми ключами. Значение по умолчанию – `~/.ssh/authorized_keys` и `~/.ssh/authorized_keys2`. Каждая строка файла содержит один ключ (пустые строки или строки, начинающиеся с символа «#» считаются комментариями и

игнорируются). Открытые ключи протокола 1 (RSA) состоят из следующих полей, разделенных пробелами: параметры, битность, порядок, модуль, комментарий. Открытые ключи протокола версии 2 состоят из полей: параметр, тип ключа, ключ в виде base64, комментарий. Поля параметров необязательны; их отсутствие определяется наличием в начале строки цифры (поле параметра никогда не начинается с цифры). Поля битности, порядка, модуля и комментарии определяют ключ RSA; поле комментария не используется (но может быть удобно пользователю для отметки ключа). Для протокола версии 2 типом ключа является ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-dss или ssh-rsa.

Строки в этих файлах, обычно имеют длину в несколько сотен байт (из-за размера открытого ключа RSA) и могут достигать длины в 8 килобайт (таким образом, максимальный размер ключа DSA – 8 килобит, а RSA – 16 килобит). Очевидно, не стоит вводить их вручную. Вместо этого следует скопировать файл `identity.pub`, `id_dsa.pub` или `id_rsa.pub` и отредактировать их.

Минимальная длина модуля RSA независимо от протокола составляет 768 бит.

Параметры (если таковые имеются) состоят из разделенных запятой определений. Для указания пробелов следует воспользоваться двойными кавычками. Поддерживаются следующие определения параметров (регистра названий параметров не учитывается):

- `command="команда"` – выполнять команду при каждом использовании данного ключа для аутентификации. Команда, передаваемая пользователем, будет игнорироваться. Команда выполняется на псевдо-терминале, если последний запрашивается клиентом; в противном случае она выполняется без терминала. Если требуется «чистый» 8-битный канал, запрашивать псевдо-терминал или указывать no-pty нельзя. В команду может быть включена кавычка, предваренная обратной косой чертой. Данный параметр полезен для ограничения использования определенных RSA-ключей. Примером может служить ключ, по которому можно выполнять удаленные операции резервного копирования и ничего более. Учтите, что клиент по-прежнему может запросить перенаправление TCP и (или) X11, если только

это не запрещено явно. Команда, запрашиваемая клиентом, заносится в переменную SSH_ORIGINAL_COMMAND. Заметьте, что данный параметр относится к выполнению оболочки, команды или подсистемы;

- `environment="ПЕРЕМЕННАЯ=значение"` – добавить переменную в среду (или переопределить ее значение) при регистрации в системе с использованием данного ключа. Допускается указание нескольких таких директив. По умолчанию изменение переменных среды таким образом отключено. За его включение отвечает параметр PermitUserEnvironment. Этот параметр отключается автоматически при включении UseLogin;
- `From="список-шаблонов"` – если параметр определен, то в дополнение к прохождению аутентификации по открытому ключу каноническое имя удаленного хоста должно соответствовать одному из шаблонов в списке (шаблоны указываются через запятую). Цель этого параметра – увеличение степени защиты: если частный ключ хоста каким-либо образом удастся похитить, то он позволит злоумышленнику войти в систему из любой точки мира. Этот дополнительный параметр делает использование ворованных ключей более затруднительным (кроме перехвата ключа, требуется взлом серверов имен и (или) маршрутизаторов). Смотрите секцию `ШАБЛОНЫ` в `ssh_config`;
- `no-agent-forwarding` – запретить перенаправление агента аутентификации при аутентификации данным ключом;
- `no-port-forwarding` – запретить перенаправление TCP/IP при аутентификации данным ключом. Любой запрос на перенаправление порта приведет к получению клиентом сообщения об ошибке. Это может быть использовано, например, вместе с параметром command;
- `no-pty` – запретить назначение терминала (запросы на назначение псевдо-терминала не будут удовлетворены);
- `no-X11-forwarding` – запретить перенаправление X11 при аутентификации данным ключом. Любой запрос на перенаправление порта возвратит клиенту сообщение об ошибке;

- `permitopen="хост:порт"` – для функции перенаправления данных с локального клиентского порта на порт удаленной системы (выполняемого при указании `ssh -L`) ограничить набор возможных целей для перенаправления указанной машиной и портом. Для указания адресов IPv6 можно использовать альтернативный синтаксис: хост/порт. Допускается указание нескольких целей через запятую. Значение параметра не интерпретируется как шаблон (т. е. является литеральным);
- `tunnel="n"` – принудительно использовать устройство tun на сервере. Без этого параметра при запросе клиентом туннеля используется ближайшее доступное для этого устройство.

Пример файла `authorized_keys`:

```
# допустимы комментарии только на всю строку
ssh-rsa AAAAB3Nza...LiPk== user@example.test
from="*.sales.example.test,!pc.sales.example.test" ssh-rsa
AAAAB2...19Q== test@example.test
command="dump /home",no-pty,no-port-forwarding ssh-dss
AAAAC3...51R== example.test
permitopen="192.0.2.1:80",permitopen="192.0.2.2:25" ssh-dss
AAAAB5...21S==
tunnel="0",command="sh /etc/netstart tun0" ssh-rsa AAAA...==
user@example.test
```

8.12.1.5. Формат файла ssh_known_hosts

В файлах `/etc/openssh/ssh_known_hosts` и `~/.ssh/known_hosts` хранятся открытые ключи всех машин, с которыми когда-либо устанавливалась связь. Глобальный файл должен быть подготовлен администратором (это необязательно), пользовательский файл поддерживается автоматически: каждый раз, когда поступает запрос на соединение от неизвестной машины, ее ключ автоматически заносится в пользовательский файл.

Каждая строка в этом файле содержит следующие поля: имена хостов, битность, порядок, модуль, комментарий. Поля разделены пробелами.

Имена хостов – это разделенный запятыми список шаблонов (символы подстановки – ('*' и '?'); каждый шаблон сопоставляется с каноническим именем машины (при аутентификации клиента) или с именем, которое указано

пользователем (при аутентификации сервера). Этот шаблон может также быть предварен знаком '!' для обозначения отрицания: если имя машины соответствует отрицаемому шаблону, оно будет отвергнуто (этой строкой) даже если оно соответствует другому шаблону в этой же строке. Также можно, заключив имя хоста или IP-адрес в квадратные скобки – '[' и],' – через ':' указать нестандартный порт.

Вместо имен хостов можно записывать их хеши. Это позволит скрыть их от злоумышленника в случае попадания файла в его руки. Для различия хешей от имен хостов первые предваряются символом '|'. На одной строке может быть не больше одного хеша, операция отрицания в этом случае не доступна.

Разрядность, порядок и модуль копируются из ключа хоста RSA, например, `/etc/openssh/ssh_host_key.pub` Необязательное поле комментария занимает всю оставшуюся часть строки и игнорируется.

Комментариями также считаются пустые и строки, начинающиеся с «#».

Идентификация машины принимается, если любая совпавшая строка содержит правильный ключ. Таким образом, можно (хотя это не рекомендуется) иметь несколько строк или различных ключей для одного и того же хоста. Это неизбежно случается при помещении в файл кратких форм имен хостов из различных доменов. В файлах может содержаться противоречивая информация. Идентификация принимается, если адекватная информация имеется в любом из них.

Заметьте, что строки в этих файлах, обычно имеют длину в несколько сотен символов и, очевидно, не стоит вводить имена хостов вручную. Вместо этого их можно сгенерировать при помощи сценария оболочки или взять из файла `/etc/ssh/ssh_host_key.pub`, добавив вначале имя хоста.

Пример файла `ssh_known_hosts`:

```
# допустимы явные комментарии только на всю строку
closenet,...,192.0.2.53 1024 37 159...93 closenet.example.test
cvs.example.test,192.0.2.10 ssh-rsa AAAA1234.....=
# хеш имени хоста
|1|JfKTdBh7rNbXkVAQCRp4OQoPfmI=|USECr3SWf1JUPsms5AqfD5QfxkM=  ssh-
rsa
AAAA1234.....=
```

8.12.1.6. Файлы

~/.hushlogin – позволяет отключить вывод времени последнего входа в систему и содержимого файла /etc/motd, если в файле конфигурации включены соответственно PrintLastLog и PrintMotd. Файл не влияет на вывод содержимого Banner.

~/.rhosts – используется для аутентификации по хосту. На некоторых машинах, если каталог пользователя находится на разделе NFS, для того чтобы он был доступен пользователю root, он должен быть доступен для чтения всем. Файл должен принадлежать пользователю и не должен быть доступен для записи другим. Рекомендуемый набор прав доступа в общем случае – чтение/запись для пользователя и недоступность для других.

~/.shosts – аналогичен файлу .rhosts, но позволяет проводить аутентификацию на основе хоста, не разрешая вход в систему с помощью rlogin/rsh.

~/.ssh/authorized_keys – содержит список открытых ключей (DSA/ECDSA/RSA), которые могут быть использованы для регистрации данного пользователя. Формат файла описан выше. Этот файл не очень важен для злоумышленника, но мы рекомендуем сделать его доступным только пользователю (чтение/запись).

Если этот файл, каталог ~/.ssh или домашний каталог пользователя доступны для записи другим пользователям, этот файл может быть изменен или заменен любым пользователем системы, имеющим сколько угодно мало прав. В этом случае sshd не будет использовать этот файл, если только параметр StrictModes не имеет значение «no». Установить рекомендуемый набор прав доступа можно командой chmodgo-w ~/ ~/.ssh ~/.ssh/authorized_keys.

~/.ssh/environment – этот файл (при его наличии) считывается в среду при регистрации в системе. Он может содержать только пустые строки, строки комментария (начинающиеся с «#»), и определения значений переменных в виде: переменная=значение. Правом на запись этого файла должен обладать только

пользователь; он не должен быть доступен остальным. Задание переменных среды отключено по умолчанию, за что отвечает параметр `PermitUserEnvironment`.

`~/.ssh/known_hosts` – список адресов, к которым когда-либо подключался пользователь, и которые отсутствуют в общесистемном файле, и соответствующих им открытых ключей. Формат файла описан выше. Файл должен быть доступен для записи только владельцу и администратору. Он может также быть доступен для чтения всем остальным, но это не обязательно.

`~/.ssh/rc` – сценарий инициализации, запускаемый перед запуском оболочки пользователя или команды. Этот файл должен быть доступен для записи только пользователю и не должен быть вообще доступен другим.

`/etc/hosts.allow` и `/etc/hosts.deny` – данные о разрешении и запрете соединений с хостами для надстроек TCP.

`/etc/hosts.equiv` – используется для аутентификации на основе хоста. Должен быть доступен для записи только root.

`/etc/openssh/moduli` – модули для схемы Диффи-Хеллмана.

`/etc/motd` – содержимое файла отображается программой login после того, как осуществлен успешный вход в систему, перед запуском команды интерпретатора.

`/etc/nologin` – если существует, подключение будет разрешено только пользователю с идентификатором root. Любому, кто пытается войти в систему, будет показано содержимое этого файла, и запросы на регистрацию в качестве не пользователя с идентификатором root будут отвергнуты. Этот файл должен быть доступен для чтения всем.

`/etc/shosts.equiv` – аналогичен `hosts.equiv`, но позволяет проводить аутентификацию на основе хоста, не разрешая вход в систему с помощью `rlogin/rsh`.

`/etc/openssh/ssh_known_hosts` – общесистемный список известных хостов и их ключей. Этот файл должен составляться администратором. В него следует включать открытые ключи всех компьютеров организации. Формат файла описан

выше. Файл должен быть доступен всем для чтения и владельцу/администратору для записи.

`/etc/openssh/ssh_host_key`, `/etc/openssh/ssh_host_dsa_key`, `/etc/openssh/ssh_host_ecdsa_key`, `/etc/openssh/ssh_host_rsa_key` – содержат частные ключи хостов. Файлы должны принадлежать root, и быть доступными только для него. Не запустится если эти файлы доступны для чтения кому-либо кроме пользователя с идентификатором root.

`/etc/openssh/ssh_host_key.pub`, `/etc/openssh/ssh_host_dsa_key.pub`, `/etc/openssh/ssh_host_ecdsa_key.pub`, `/etc/openssh/ssh_host_rsa_key.pub` – содержат открытые ключи хостов. Должны быть доступны всем для чтения и только пользователю с идентификатором root для записи. Содержимое файлов должно соответствовать содержимому соответствующих файлов с частными ключами. Эти файлы не используются программой и предназначены для копирования пользователем в файлы known_hosts. Эти файлы создаются командой ssh-keygen.

`/etc/openssh/sshd_config` – конфигурация службы sshd.

`/etc/openssh/sshrc` – аналогичен `~/.ssh/rc`, позволяет задавать инициализационный сценарий глобально для всех пользователей. Должен быть доступен всем для чтения и только root для записи.

`/var/empty` – каталог `chroot` используемый при отделении полномочий на предаутентификационном этапе. В папке не должно быть никаких файлов, она должна принадлежать только root и не должна быть доступна другим для записи.

`/var/run/sshd.pid` – идентификатор процесса, ожидающего запросов на подключение (если одновременно работает несколько экземпляров служб для нескольких портов, в него записывается идентификатор экземпляра, запущенного последним). Содержимое этого файла может не быть защищено и может быть доступно всем.

8.12.2. SSHD_CONFIG

8.12.2.1. Описание файла конфигурации

Служба sshd считывает данные о конфигурации из файла `/etc/openssh/sshd_config` (или из файла, указанного в командной строке при помощи параметра `-f`). Файл содержит пары «параметр-значение», по одной на строку. Пустые строки и строки, начинающиеся с «#» интерпретируются как комментарии. В случае, если аргументы содержат пробелы, они должны быть заключены в двойные кавычки (”).

Файл `/etc/openssh/sshd_config` должен быть доступен для записи только пользователю root, и рекомендуется делать его доступным для чтения всем.

В таблице 7 приведены описания возможных параметров (регистр имен аргументов учитывается, регистр имен параметров – нет).

Т а б л и ц а 7 – Описание параметров

Параметр	Описание
AcceptEnv	Список переменных среды, которые, будучи заданы клиентом, будут копироваться в environ сеанса. Соответствующая настройка на стороне клиента выполняется параметром SendEnv и описана в ssh_config. Переменные указываются по имени, допускаются символы подстановки «*» и «?» Несколько переменных среды можно указывать через пробелы или в нескольких параметрах AcceptEnv. Данный параметр введен для предотвращения обхода ограничений среды пользователя посредством изменения значений переменных среды. По умолчанию не принимаются никакие переменные среды
AddressFamily	Семейство адресов, которое должна использовать служба sshd. Допустимые значения: «any» «inet» (только IPv4) и «inet6» (только IPv6). Значение по умолчанию – «any»
AllowGroups	Список шаблонов имен групп через пробел. Если параметр определен, регистрация в системе разрешается только тем пользователям, чья главная или вспомогательная группы соответствуют какому-либо из шаблонов. Допустимы только имена групп. По умолчанию разрешена регистрация в системе для членов всех групп. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups
AllowTcpForwarding	Определяет, будет ли разрешено перенаправление TCP. Значение по умолчанию – «yes». Отключение пересылки TCP не увеличит уровень защищенности системы, пока пользователям не запрещен доступ к командной оболочке, так как они всегда могут установить свои собственные перенаправления
AllowUsers	Список имен пользователей через пробел. Если параметр определен, регистрация в системе будет разрешена только пользователям, чьи имена соответствуют одному из шаблонов. Допустимы только имена пользователей; числовой идентификатор пользователя не распознается. По умолчанию разрешена регистрация в системе для всех пользователей. Если шаблон указывается в форме ПОЛЬЗОВАТЕЛЬ@ХОСТ, его две части проверяются отдельно, таким образом, разрешая доступ только пользователям с указанными именами, подключающимся с указанных хостов. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups
AuthorizedKeysFile	Файл с открытыми ключами, которые могут быть использованы для аутентификации пользователей. Допустимо указание шаблонов, они преобразуются при настройке соединения: %% заменяется на символ '%', %h заменяется на домашний каталог идентифицируемого пользователя, %u – на имя пользователя. После преобразования AuthorizedKeysFile интерпретируется либо как абсолютный путь, либо как путь относительно домашнего каталога пользователя. Значение по умолчанию: /etc/openssh/authorized_keys/%u /etc/openssh/authorized_keys2/%u .ssh/authorized_keys .ssh /authorized_keys2.

Продолжение таблицы 7

Параметр	Описание
Banner	Содержимое указанного файла будет отправлено удаленному пользователю прежде, чем будет разрешена аутентификация. Этот параметр доступен только с протоколом версии 2. По умолчанию не выводится никакой информации
ChallengeResponseAuthentication	Определяет, разрешается ли беспарольная аутентификация «вызов-ответ». Поддерживаются все схемы аутентификации login.conf. Значение по умолчанию – «no»
Ciphers	Допустимые для протокола версии 2 шифры. Несколько кодов указываются через запятую. Поддерживаются следующие шифры: «3des-cbc», «aes128-cbc», «aes192-cbc», «aes256-cbc», «aes128-ctr», «aes192-ctr», «aes256-ctr», «arcfour128», «arcfour256», «arcfour», «blowfish-cbc» и «cast128-cbc». Значение по умолчанию: - aes256-ctr,aes192-ctr,aes128-ctr,arcfour256, arcfour128; - blowfish-cbc,aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc;cast128-cbc, arcfour
ClientAliveCountMax	Количество запросов, проверяющих доступность клиента, которые могут оставаться без ответа. Если предел достигнут, sshd отключит клиента и завершит сеанс. Запросы client alive отличаются от TCPKeepAlive. Данные запросы отправляются через защищенный канал и поэтому не могут быть подменены. Параметр TCPKeepAlive допускает возможность подмены данных. Механизм client alive полезен, если поведение клиента или сервера зависит от активности соединения. Значение по умолчанию – 3. Если ClientAliveInterval равно 15, а для ClientAliveCountMax оставлено значение по умолчанию, не отвечающие клиенты SSH будут отключаться приблизительно через 45 секунд. Данный параметр относится только к протоколу версии 2
ClientAliveInterval	Время бездействия со стороны клиента в секундах, после которого sshd отправляет через защищенный канал запрос отклика клиенту. Значение по умолчанию – 0, что означает, что клиенту не будут направляться такие запросы. Этот параметр применим только с протоколом версии 2
Compression	Разрешить сжатие сразу, после аутентификации или вообще запретить его. Допустимые значения – «yes», «delayed» и «no». Значение по умолчанию – «delayed»
DenyGroups	Список шаблонов имен групп через пробел. Если параметр определен, регистрация в системе пользователям, чья главная или вспомогательная группа соответствуют содержащимся в списке шаблонам, не разрешается. Допустимы только имена групп. По умолчанию регистрация в системе разрешена для всех групп. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups

Продолжение таблицы 7

Параметр	Описание
DenyUsers	Список имен пользователей через пробел. Если параметр определен, регистрация в системе пользователей, чьи имена соответствуют одному из шаблонов, будет запрещена. Допустимы только имена пользователей; числовой идентификатор пользователя не распознается. По умолчанию разрешена регистрация в системе для всех пользователей. Если шаблон указывается в форме ПОЛЬЗОВАТЕЛЬ@ХОСТ, его две части проверяются отдельно, таким образом, запрещается доступ только пользователям с указанными именами, подключающимся с указанных хостов. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups
ForceCommand	Выполнять указанную команду после регистрации пользователя в системе, игнорируя команду, запрашиваемую им. Команда запускается оболочкой пользователя с ключом -c. Это относится к выполнению оболочки, команды или подсистемы, обычно применяется внутри блока Match. Команда, запрошенная пользователем, помещается в переменную среды SSH_ORIGINAL_COMMAND
GatewayPorts	Определяет, разрешено ли удаленным машинам подключение к портам, выделенным для туннелирования трафика клиентов. По умолчанию sshd делает доступными порты, используемые для туннелирования инициируемого сервером, только для кольцевого (loopback) адреса, то есть удаленные машины подключаться к перенаправляемым портам не могут. С помощью данного параметра можно исправить такое положение дел. Значение «no» разрешает туннелирование только в рамках данной системы, «yes» разрешает туннелирование для хостов, соответствующих шаблону, а «clientspecified» позволяет клиенту самостоятельно выбирать адрес для туннелирования. Значение по умолчанию – «no»
GSSAPIAuthentication	Допускать аутентификацию по GSSAPI. Значение по умолчанию – «no» Данный параметр относится только к протоколу версии 2
GSSAPICleanupCredentials	Очищать ли кэш аутентификационных данных клиента при завершении сеанса. Значение по умолчанию – «yes» Данный параметр относится только к протоколу версии 2
HostbasedAuthentication	Допускать аутентификацию по хостам, т. е. аутентификацию по rhosts или /etc/hosts.equiv в сочетании с открытым ключом клиента. Этот параметр схож с RhostsRSAAuthentication и применим только к протоколу версии 2. Значение по умолчанию – «no»
HostbasedUsesNameFromPacketOnly	Отключить выполнение запросов имени хоста при обработке файлов ~/.shosts, ~/.rhosts и /etc/hosts.equiv в рамках аутентификации по хосту (HostbasedAuthentication). При значении «yes» для сравнения будет использоваться имя, указанное клиентом, а не имя которое может быть получено стандартными средствами соединения TCP. По умолчанию – «no»

Продолжение таблицы 7

Параметр	Описание
HostKey	Файл с частными ключами хоста. Значение по умолчанию – /etc/ssh/ssh_host_key для протокола 1, и /etc/ssh/ssh_host_dsa_key, /etc/ssh/ssh_host_ecdsa_key и /etc/ssh/ssh_host_rsa_key для протокола 2. sshd не будет принимать файлы частных ключей доступные для чтения всей группе или вообще всем пользователям. Можно указывать несколько файлов с ключами хоста. Ключи «rsa1» используются для протокола версии 1, ключи «dsa», «ecdsa» и «rsa» – для версии 2 протокола SSH
IgnoreRhosts	Не учитывать содержимое файлов .rhosts и .shosts при аутентификации RhostsRSAAuthentication и HostbasedAuthentication. При этом будут учитываться только /etc/hosts.equiv и /etc/openssh/shosts.equiv. Значение по умолчанию – «yes»
IgnoreUserKnownHosts	Не учитывать содержимое файла ~/.ssh/known_hosts при RhostsRSAAuthentication или HostbasedAuthentication. Значение по умолчанию – «no»
KerberosAuthentication	Определяет, дозволена ли аутентификация Kerberos. Проверять ли пароль, указанный пользователем для аутентификации PasswordAuthentication в Kerberos KDC. Это может быть либо в форме тикетов Kerberos или, если PasswordAuthentication установлена в «yes», пароль, предоставленный пользователем, будет утвержден через Kerberos KDC. Для использования этого параметра серверу нужна Kerberos servtab, которая разрешит проверку субъекта KDC. Значение по умолчанию – «no»
KerberosGetAFSToken	Если AFS активна и у пользователя имеется Kerberos 5 TGT, получать талон AFS перед обращением к домашнему каталогу пользователя. Значение по умолчанию – «no».
KerberosOrLocalPasswd	В случае непринятия аутентификации посредством Kerberos, проверять пароль другими механизмами, такими как /etc/passwd. Значение по умолчанию – «yes»
KerberosTicketCleanup	Очищать ли кэш талонов пользователя при завершении сеанса. Значение по умолчанию – «yes»
KeyRegenerationInterval	В протоколе версии 1 эфемерный ключ сервера будет автоматически регенерироваться по истечении этого количества секунд. Цель регенерации состоит в том, чтобы предохранить кодированные установленные сеансы от более поздних вторжений на машину и захвата ключей. Ключ нигде не сохраняется. Если установлено значение 0, то ключ не будет регенерироваться. Значение по умолчанию – 3600 (секунд)
ListenAddress	Локальные адреса, по которым sshd должен ожидать соединения. Может быт использован следующие форматы записей: ListenAddress хост|адрес-IPv4|адрес-IPv6 ListenAddress хост|адрес-IPv4:порт ListenAddress [хост|адрес-IPv6]:порт

Продолжение таблицы 7

Параметр	Описание
	Если порт не указан, sshd будет ожидать соединения на указанном адресе и на всех указанных ранее (но не после) в параметре `Port` портах. По умолчанию ожидается соединение на всех локальных адресах. Допустимо указание нескольких параметров
`LoginGraceTime`	Сервер отключается по истечении этого времени, если пользователю не удалась регистрация в системе. Если стоит значение 0, то время ожидания не ограничено. Значение по умолчанию – 120 секунд
`LogLevel`	Задает степень подробности сообщений для протоколов sshd. Допустимыми являются значения: `QUIET`, `FATAL`, `ERROR`, `INFO`, `VERBOSE`, `DEBUG`, `DEBUG1`, `DEBUG2`, и `DEBUG3`. Значение по умолчанию – `INFO`. Значения `DEBUG` и `DEBUG1` эквивалентны. Использование значения `DEBUG*` нарушает конфиденциальность пользователей и потому не рекомендуется
`MACs`	Допустимые алгоритмы MAC (Message Authentication Code – код установления подлинности сообщения). Они используются в протоколе версии 2 для гарантирования целостности данных. Несколько алгоритмов следует указывать через запятую. Значение по умолчанию: `hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-sha1-96,hmac-md5-96,hmac-sha2-256,hmac-sha256-96,hmac-sha2-512,hmac-sha2-512-96`
`Match`	Начинает условный блок. Если все критерии на строке Match удовлетворены, указанные в блоке директивы будут иметь больший приоритет, чем указанные в глобальном разделе файла конфигурации. Концом блока считается либо следующая директива `Match`, либо конец файла. В качестве аргументов `Match` принимаются пары критерий-шаблон.Допустимые критерии: `User Group Host` и `Address`. В самом блоке `Match` допустимо указание следующих параметров: `AllowAgentForwarding`, `AllowTcpForwarding`, `AuthorizedKeysFile`, `AuthorizedPrincipalsFile`, `Banner`, `ChrootDirectory`, `ForceCommand`, `GatewayPorts`, `GSSAPIAuthentication`, `HostbasedAuthentication`, `HostbasedUsesNameFromPacketOnly`, `KbdInteractiveAuthentication`, `Kerber-osAuthentication`, `Match`, `MaxAuthTries`, `MaxSessions`, `PasswordAuthentication`, `PermitEmptyPasswords`, `PermitOpen`, `PermitRoot-Login`, `PermitTunnel`, `PubkeyAuthentication`, `RhostsRSAAuthentication`, `RSAAuthentication`, `X11DisplayOffset`, `X11Forwarding` и `X11UseLocalHost`
`MaxAuthTries`	Ограничение на число попыток идентифицировать себя в течение одного соединения. При достижении количества неудачных попыток аутентификации записи о последующих неудачах будут вноситься в протокол. Значение по умолчанию:
`MaxSesstions`	Ограничение на число одновременно открытых сессий в каждом сетевом соединении. Значение по умолчанию – 10

Продолжение таблицы 7

Параметр	Описание
`MaxStartups`	Ограничение на число одновременных соединений, в которых не был пройден этап аутентификации. Все последующие соединения не будут приниматься, пока на уже существующем соединении не будет произведена аутентификация или не истечет время, указанное в параметре `LoginGraceTime`. Значение по умолчанию – «10:30:100». Как альтернатива может быть задействован ранний случайный отказ в подключении путем указания трех разделенных через двоеточие значений «старт:норма:предел» (например, «10:30:60»). Соединение будет сбрасываться с вероятностью «норма/100» (30%) если имеется «старт» (10) (10) соединений с не пройденным этапом аутентификации. Вероятность возрастает линейно и постоянно, попытки будут отвергаться при достижении числа «предел» (60)
`PasswordAuthentication`	Допускать аутентификацию по паролю. Значение по умолчанию – «yes»
`PermitEmptyPasswords`	Допускать использование пустых паролей при аутентификации по паролю. Значение по умолчанию – «no»

`PermitOpen`	Ограничить возможные конечные точки для туннелирования TCP. Допустимые формы указания точек:
	`PermitOpen`
	`хост:порт`
	`PermitOpen`
	`адрес-IPv4:порт`
	`PermitOpen`
	`[адрес-IPv6]:порт`
	Возможно указание нескольких конечных точек через пробел. Значение «any» снимает ограничение и является значением по умолчанию

`PermitRootLogin`	Допускать вход в систему через ssh в качестве пользователя с идентификатором root. Допустимые значения: «yes», «without-password», «forced-commands-only», «no». Значение по умолчанию – «without-password». Если этот параметр установлен в значение «without-password» войти в систему в качестве пользователя с идентификатором root, указав для аутентификации пароль, будет невозможно. Если этот параметр установлен в значение «forced-commands-only» будет разрешена регистрация пользователя с идентификатором root в системе по открытому ключу, но только если определен параметр command команда (может быть полезно для удаленного создания резервных копий, даже если регистрация пользователя с идентификатором root в системе не разрешена). Все другие методы аутентификации для пользователя с идентификатором root будут отключены. При значении «no» вход в систему в качестве root будет полностью запрещен
`PermitTunnel`	Допускать использование перенаправления для устройств tun. Допустимые значения: «yes» «point-to-point» (уровень 3), «ethernet» (уровень 2), «no». Значение «yes» эквивалентно «point-to-point» и «ethernet» одновременно. Значение по умолчанию – «no»

Продолжение таблицы 7

Параметр	Описание
PermitUserEnvironment	Учитывать ли файл ~/.ssh/environment и параметры environment= в файле ~/.ssh/authorized_keys. Значение по умолчанию – «no». Посредством изменения переменных среды пользователи могут обойти ограничения своих полномочий. Например, с помощью механизма LD_PRELOAD
PidFile	Файл в который следует записывать идентификатор процесса службы SSH. Значение по умолчанию – /var/run/sshd.pid
Port	Порт, на котором следует ожидать запросы на соединение. Значение по умолчанию – 22. Допустимо указание параметра несколько раз. См. также ListenAddress
PrintLastLog	Выводить ли время и дату предыдущего входа в систему при интерактивной регистрации пользователя в ней. Значение по умолчанию – «yes»
PrintMotd	Выводить ли содержимое файла /etc/motd при интерактивной регистрации пользователя в системе (в некоторых системах это выполняется оболочкой, сценарием /etc/profile или аналогичным). Значение по умолчанию – «yes»
Protocol	Версии протокола, которые следует принимать. Допустимые значения – «1» и «2» Несколько значений указываются через запятую. Значение по умолчанию – «2». Порядок указания протоколов не имеет значения, т. к. протокол выбирается клиентом из списка доступных
PubkeyAuthentication	Допускать аутентификацию по открытому ключу. Значение по умолчанию – «yes». Данный параметр относится только к протоколу версии 2
RhostsRSAAuthentication	Допускать аутентификацию по rhosts или /etc/hosts.equiv совместно с аутентификацией по хосту RSA. Значение по умолчанию – «no» Данный параметр относится только к протоколу версии 1
RSAAuthentication	Допускать аутентификацию только по ключу RSA. Значение по умолчанию – «yes». Данный параметр относится только к протоколу версии 1
ServerKeyBits	Длина ключа сервера для эфемерного протокола 1. Минимальное значение – 512 (по умолчанию – 1024)
StrictModes	Проверять наборы прав доступа и принадлежность конфигурационных файлов и домашнего каталога пользователя перед разрешением регистрации в системе. Это рекомендуется выполнять потому, что новички иногда оставляют свои каталоги или файлы доступными для записи всем. Значение по умолчанию – «yes»
Subsystem	Позволяет настроить внешнюю подсистему (например, службу FTP). В качестве параметров должны выступать имя подсистемы и команда, которая будет выполняться при запросе подсистемы. Команда sftp-server реализует подсистему передачи файлов sftp. По умолчанию подсистемы не определены. Данный параметр относится только к протоколу версии 2

Продолжение таблицы 7

Параметр	Описание
SyslogFacility	Код источника сообщений для протокола syslog. Допустимые значения: DAEMON, USER, AUTHPRIV, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7. Значение по умолчанию – AUTHPRIV
TCPKeepAlive	Указывает, будет ли система посылать другой стороне контрольные сообщения для удержания соединения активным. Если они посылаются, то разрыв соединения или аварийный отказ одной из машин будут должным образом замечены. При этом временная потеря маршрута также повлечет за собой разрыв соединения. С другой стороны, если контрольные сообщения не посылаются, сеанс на сервере может зависнуть, оставив после себя «пользователей-привидений» и отнимая ресурсы сервера. Значение по умолчанию – «yes». Это позволяет избежать бесконечно долгих сеансов. Для отключения отправки сообщений TCP keepalive установите значение «no»
UseDNS	Выполнять ли запросы DNS для получения имени удаленного хоста для того чтобы убеждаться в том, что обратное преобразование выдает тот же самый IP-адрес. Значение по умолчанию – «no»
UseLogin	Использовать login для интерактивных сеансов регистрации в системе. Значение по умолчанию – «no». login никогда не используется для удаленного выполнения команд. Если этот параметр включен, функция X11Forwarding будет отключена, потому что login не может обрабатывать cookie xauth В случае использования разделения полномочий (UsePrivilegeSeparation) данный параметр будет отключен после прохождения аутентификации
UsePAM	Включить интерфейс модулей аутентификации Pluggable Authentication Module. При значении «yes» аутентификация PAM будет доступна через ChallengeResponseAuthentication и PasswordAuthentication в дополнение к учетной записи PAM и обработке модулей сеансов для всех типов аутентификации. Поскольку беспарольная аутентификация PAM «вызов-ответ» служит заменой аутентификации по паролю, нужно отключить либо PasswordAuthentication, либо ChallengeResponseAuthentication. При включенном UsePAM службу sshd можно будет выполнять только с правами root. Значение по умолчанию – «yes»
UsePrivilegeSeparation	Разделять полномочия посредством создания дочернего процесса с меньшими правами для обработки входящего трафика. После прохождения аутентификации для работы с клиентом будет создан специальный процесс, соответствующий его правам. Если значение параметра равно «sandbox», то на непривилегированный процесс до прохождения аутентификации будут наложены дополнительные ограничения. Значение по умолчанию – «sandbox»

Окончание таблицы 7

Параметр	Описание
`X11DisplayOffset`	Номер первого дисплея доступного для туннелирования трафика X11 sshd (по умолчанию – 10). Позволяет избежать вмешательства sshd в работу настоящих серверов X11
`X11Forwarding`	Допускать туннелирование X11. Допустимые значения – «yes» и «no». Значение по умолчанию – «yes». Если дисплей-посредник ожидает соединений от любых адресов (или по шаблону) sshd включение туннелирования X11 подвергает сервер и логические дисплеи клиентов дополнительной опасности. Поэтому такое поведение не является поведением по умолчанию. Проверка и подмена аутентификационных данных при атаке выполняются на стороне клиента При туннелировании X11 графический сервер клиента может подвергаться атаке при запросе клиентом SSH туннелирования. Для большей защиты пользователей администратор может запретить туннелирование, установив значение «no». Туннелирование X11 отключается автоматически при включении `UseLogin`
`X11UseLocalhost`	К какому адресу следует привязывать сервер туннелирования X11: к кольцевому (loopback) или адресу, указанному по шаблону. По умолчанию сервер туннелирования привязывается к кольцевому адресу, а в качестве хоста в переменную среды DISPLAY заносится «localhost». Это не позволяет удаленным хостам подключаться к дисплею-посреднику. Однако, в случае старых клиентов X11, такая конфигурация может не сработать. Установите тогда `X11UseLocalhost` в «no». Допустимые значения – «yes» и «no». Значение по умолчанию – «yes»
`XAuthLocation`	Путь к команде xauth. Значение по умолчанию – `/usr/bin/xauth`

8.12.2.2. Указание времени

Ключи командной строки sshd и параметры файлы конфигурации могут требовать указания времени. Оно должно указываться в виде последовательности:

`время [единицы]`

где время – положительное целое, единицы могут принимать следующие значения:

- ничего – секунды;
- s | S – секунды;
- m | M – минуты;
- h | H – часы;
- d | D – дни;
- w | W – недели.

Итоговое время получается в результате сложения всех выражений.

Примеры:

- 600 – 600 секунд (10 минут);

- 10m – 10 минут;

- 1h30m – 1 час 30 минут (90 минут).

8.13. Прокси-сервер (Squid)

Для обеспечения контролируемого доступа ПЭВМ локальной сети к сети Интернет в составе ОС Альт СП используется кэширующий прокси-сервер Squid.

Примечание. Пакет squid не установлен по умолчанию, для установки выполнить следующую команду:

```
# apt-get install squid
```

Для обеспечения возможности использования ПЭВМ, на которую установлен Squid, в качестве прокси-сервера нужно настроить таблицы управления доступом (Access Control Lists, далее – ACL), которые хранятся в конфигурационном файле `squid.conf` в директории `/etc/squid/`.

Для того чтобы сервер Squid принимал соединения из всей внутренней сети, нужно в раздел `# TAG: acl` включить следующую запись:

```
acl our_networks src <адреса внутренней сети>
http_access allow our_networks
```

При настройке таблиц управления доступом следует учитывать, что при обработке запроса на доступ к серверу Squid все строки `http_access` файла `squid.conf` просматриваются последовательно сверху вниз до первой строки, соответствующей параметрам запроса.

8.13.1. Настройка прозрачного доступа через прокси-сервер

Для настройки прозрачного доступа пользователей локальной сети к сети Интернет через прокси-сервер нужно выполнить настройку фильтра адресов, для этого нужно выполнить команду `iptables`, перенаправляющую HTTP-запросы к внешним серверам на порт Squid:

```
# iptables -t nat -A PREROUTING ! -d <прокси-сервер> \
-i <внутренний_интерфейс> -p tcp -m tcp --dport 80 \
-j REDIRECT --to-ports 3128
```

Также можно выполнить альтернативную команду:

```
# iptables -t nat -A PREROUTING -p tcp -d 0/0 --dport www \
-i <внутренний_сетевой_интерфейс> -j DNAT \
--to <локальный_адрес_на_котором_слушает_прокси>:3128
```

Настройка squid.conf при этом использует обратное проксирование. Далее нужно добавить в конфигурационный файл squid.conf следующую строку:

```
http_port 80 intercept
```

Примечание. Параметр intercept заменяет параметр transparent, который также использовался в предыдущих версиях squid.conf.

8.13.2. Фильтрация доступа

В Squid существует гибкая схема фильтрации внешних ссылок, с помощью которой предоставляется возможность ограничить (запретить) доступ к определенным сетевым ресурсам. Содержимое фильтруется с помощью таблиц управления доступом ACL и настроек http_access deny, примеры которых приведены в конфигурационном файле squid.conf. При задании фильтруемого URL или доменного имени сервера можно использовать регулярные выражения, определяя в одной строке фильтр для целого класса адресов или доменных имен.

Запрет доступа к домену baddomain.com, например, можно оформить следующим образом:

```
acl Bad dstdomain baddomain.com
http_access deny Bad
```

8.13.3. Авторизация доступа

Squid позволяет настраивать таблицы доступа ACL индивидуально для пользователей и (или) категорий пользователей. Если для определения того, какой именно пользователь подключается к серверу, недостаточно IP-адреса его компьютера, следует использовать схемы авторизации, принятые в Squid. Авторизация конфигурируется с помощью тега TAG: auth_param. Схемы (программы) авторизации, поддерживаемые Squid, хранятся в каталоге /usr/lib/squid.

Для настройки аутентификации в LDAP можно использовать следующую конфигурацию:

```
auth_param basic program /usr/lib/squid/squid_ldap_auth -b
ou=People,dc=office,dc=lan -f (uid=%s) -h ldap.office.lan
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
```

8.13.4. Кэширование данных

Squid обеспечивает возможность кэширования данных, полученных по запросам из сети Интернет (при повторных запросах данные извлекаются из сохраненной копии).

Настройка правил кэширования данных осуществляется с помощью таблиц доступа ACL, а также с помощью настройки конфигурационного файла `squid.conf`. Для отключения функции кэширования данных нужно использовать параметр `always_direct`, для включения принудительного кэширования – `never_direct`.

Например, чтобы запретить кэширование данных, получаемых по протоколу FTP, нужно в конфигурационный файл `squid.conf` добавить следующие строки:

```
acl FTP proto FTP
always_direct allow FTP
```

Squid поддерживает возможность обмена данными с кэшем авторизованного сервера (`parent peer` (родительский прокси-сервер) `/sibling peer` (братский прокси-сервер)), например, если запрашиваемый ресурс в локальном кэше Squid не найден.

8.13.5. Настройка режима работы в качестве обратного прокси-сервера

Squid поддерживает режим работы в качестве обратного прокси-сервера. Работа в таком режиме обеспечивает ретрансляцию запросов из внешней сети на один или несколько серверов, логически расположенных во внутренней сети, и позволяет скрыть реальное расположение и структуру серверов, а также уменьшить нагрузку на них.

Для настройки сервера Squid для работы в качестве единственного обратного прокси-сервера, принимающего HTTP-запросы из внешней сети, нужно в конфигурационный файл squid.conf добавить следующие строки:

```
http_port 80 accel defaultsite=internal.www.com
cache_peer <имя сервера> parent 80 <порт ICP> no-query
originserver
```

Примечания:

1. В примере в качестве порта, принимающего запросы из внешней сети по протоколу HTTP, используется порт 80.

2. Так как сервер Squid играет роль единственного обратного прокси-сервера, нужно выключить ICP, указав в качестве порта ICP значение 0.

3. parent (родительский прокси-сервер) – тип прокси-сервера в соответствии с иерархией серверов.

Для обратного проксирования нескольких внутренних серверов нужно, чтобы внешние запросы к ресурсам сети Интернет с разными доменными именами попадали на вход Squid, который бы ставил в соответствие каждому имени действительный адрес сервера во внутренней сети и в соответствии с этим перенаправлял запрос. Делается это с помощью механизма виртуальных хостов.

Для организации прокси для двух серверов (www1.foo.bar и www2.foo.bar), адреса которых в DNS указывают на машину со Squid-сервером нужно в конфигурационный файл squid.conf добавить следующую запись:

```
http_port 80 accel defaultsite=www1.foo.bar vhost
hosts_file /etc/hosts
```

Настройка defaultsite используется сервером для заполнения HTTP-заголовков. Для преобразования доменных имен в адреса серверов во внутренней сети следует использовать файл /etc/hosts:

```
10.0.0.1 www1.foo.bar
10.0.0.2 www2.foo.bar
```

8.13.6. Сбор статистики и ограничение полосы доступа

В состав Squid входит утилита кэш-менеджер, предназначенная для отображения статистики и загрузки сервера. Кэш-менеджер представляет собой cgi-приложение и должен выполняться под управлением сконфигурированного HTTP-сервера. Все настройки кэш-менеджера выполняются с помощью

конфигурирования файла `squid.conf` (строки, которые относятся к кэш-менеджеру, обычно включают cachemgr).

Squid также обеспечивает возможность ограничения полосы пропускания для пользователей (для этого используются параметры `delay_pools` и `delay_class`).

8.13.7. Кеширование DNS-запросов

Squid содержит встроенный минисервер запросов DNS. Он выступает как посредник между Squid и внешними DNS-серверами. При запуске Squid производит начальное тестирование доступности DNS (можно отключить, используя опцию `–D`). Время кеширования удачного DNS-запроса по умолчанию составляет шесть часов.

8.14. FTP-сервер

Модуль «FTP-сервер» (пакет alterator-vsftpd) из раздела «Серверы» (рис. 111) 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 распространенный 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 нужно отметить параметр «Разрешить настройку локальных пользователей».

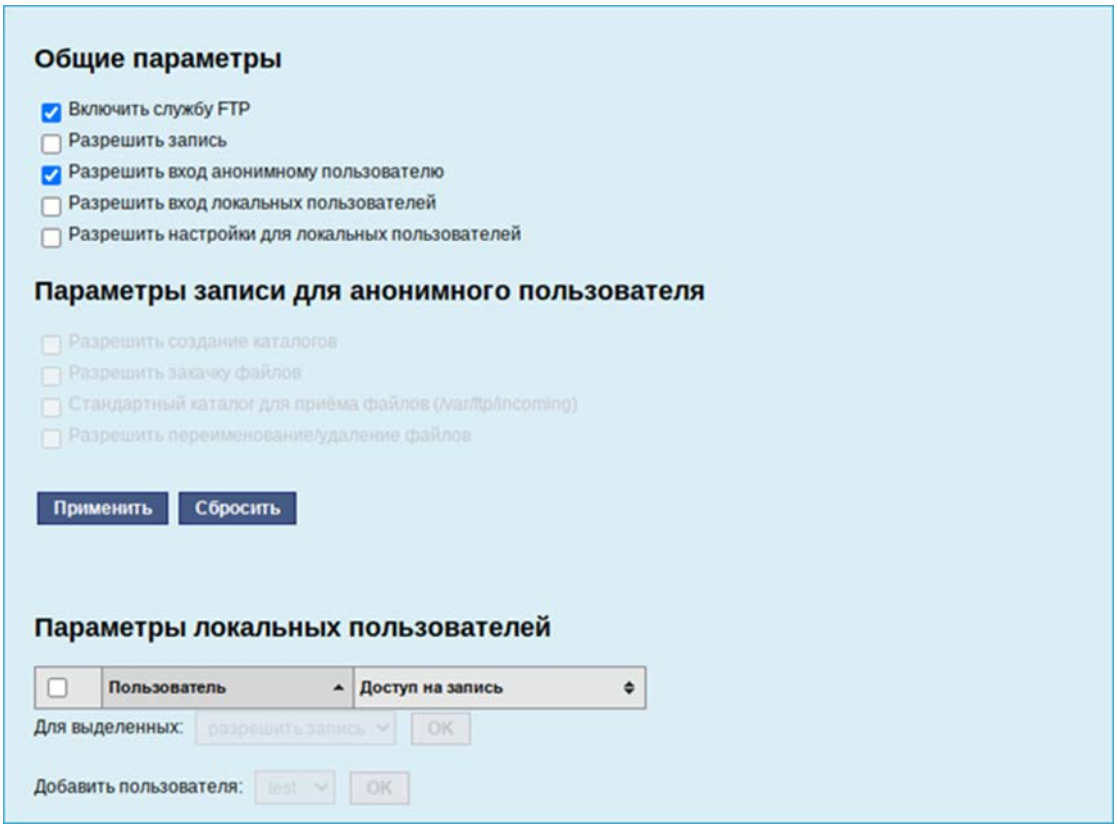


Рис. 111 – Настройка модуля «FTP-сервер»

Если нужно создать анонимный FTP-сервер, можно 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 создается каталог, который будет корневым при анонимном подключении, – `/var/ftp` с 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.

Многие параметры использования FTP-сервера, в том числе относящиеся к безопасности, могут быть заданы при помощи xinetd (демона Интернет-служб).

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 (рис. 112).

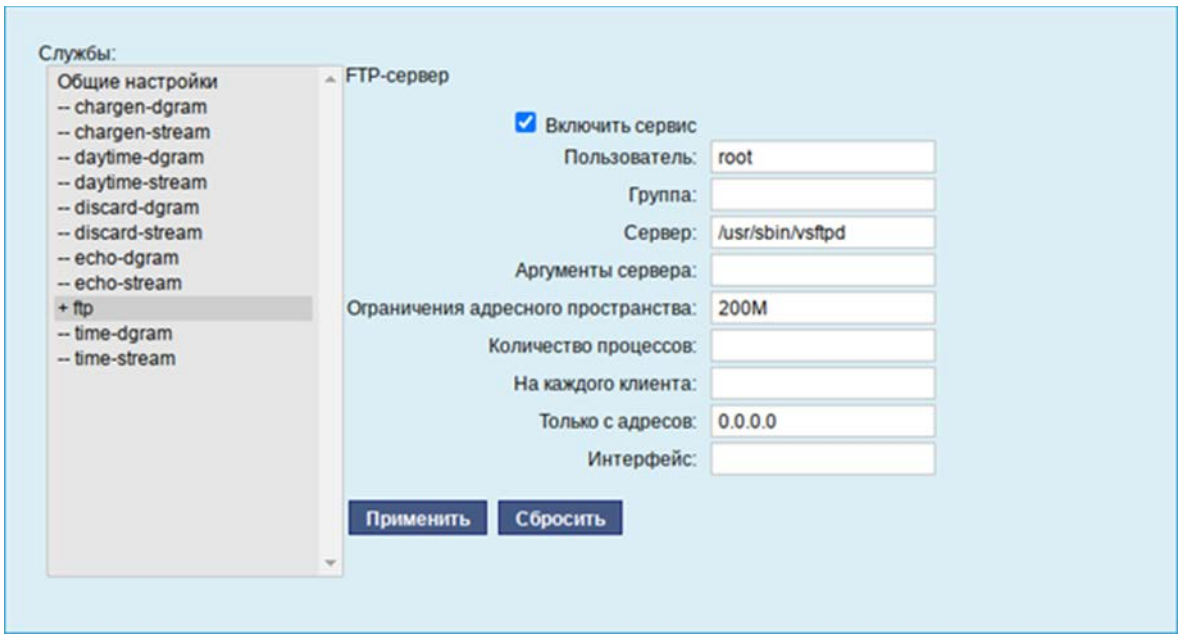


Рис. 112 – Настройка параметров vsftpd в модуле «Службы xinetd»

8.15. Доступ к службам из сети Интернет

8.15.1. 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 нужно 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, можно сделать их доступными для соединений на внешних сетевых интерфейсах (рис. 113). Если нужно предоставить доступ к службе, отсутствующей в списке, то нужно задать используемые этой службой порты в соответствующих полях.

Можно выбрать один из двух режимов работы:

- роутер – 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 на компьютере настроен, по крайней мере, один внешний и один внутренний интерфейс.

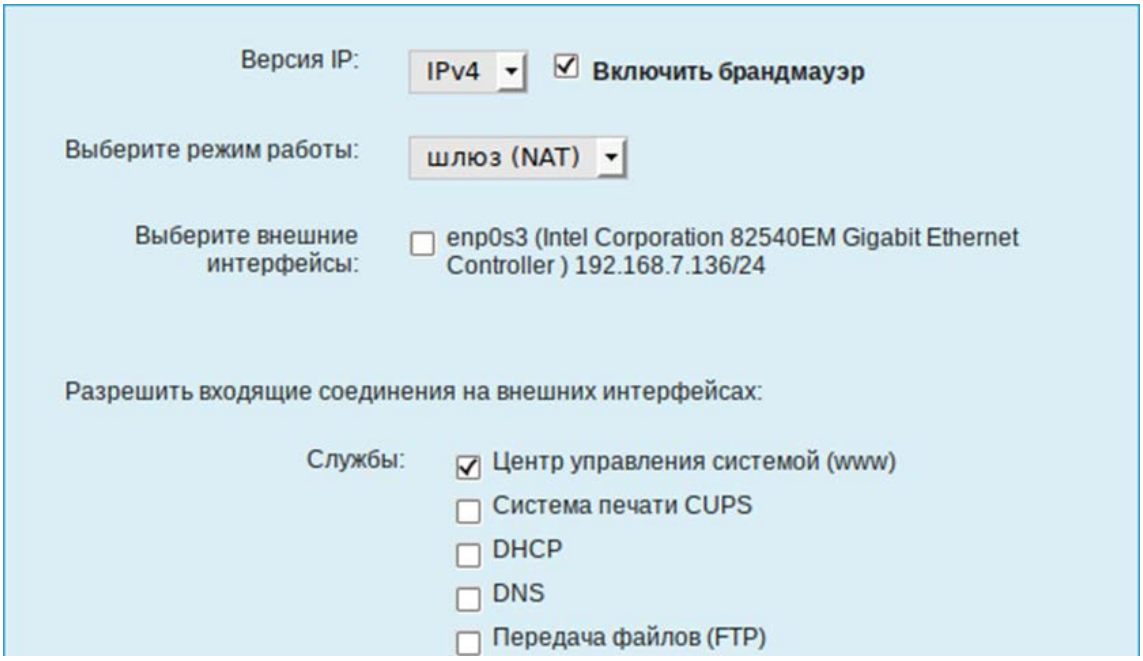


Рис. 113 – Модуль «Внешние сети»

Примечания:

1. В любом режиме включено только перенаправление пакетов с внутренних интерфейсов. Перенаправление пакетов с внешних интерфейсов всегда выключено.
2. Все внутренние интерфейсы открыты для любых входящих соединений.

8.15.2. Список блокируемых хостов

Модуль ЦУС «Список блокируемых хостов» (пакет alterator-net-bl) позволяет настроить блокировку любого сетевого трафика с указанных в списке узлов (входящий, исходящий и пересылаемый).

Блокирование трафика с указанных в списке узлов начинается после установки флага «Использовать черный список» (рис. 114).

Для добавления блокируемого узла нужно ввести IP-адрес в поле «Добавить IP-адрес сети или хоста:» и нажать на кнопку «Добавить».

Для удаления узла нужно выбрать его из списка и нажать на кнопку «Удалить».

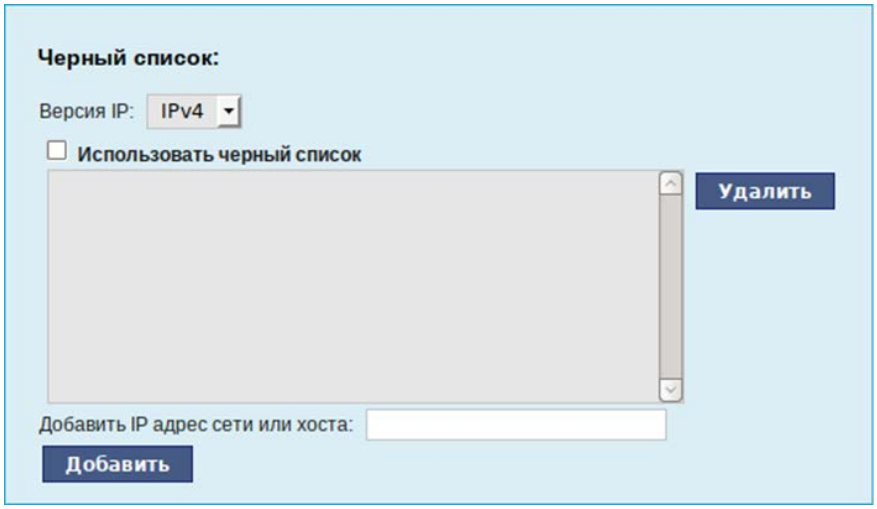


Рис. 114 – Модуль «Список блокируемых хостов»

8.16. Статистика

8.16.1.1. Сетевой трафик

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

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

Для включения сбора данных нужно установить флаг «Включить сбор данных», и нажать на кнопку «Применить» (рис. 115).

Для просмотра статистики указывается 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 нужно выбрать интересующий и нажать на кнопку «Показать» (рис. 115).

Трафик на указанном интерфейсе за заданный период показывается в виде:

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

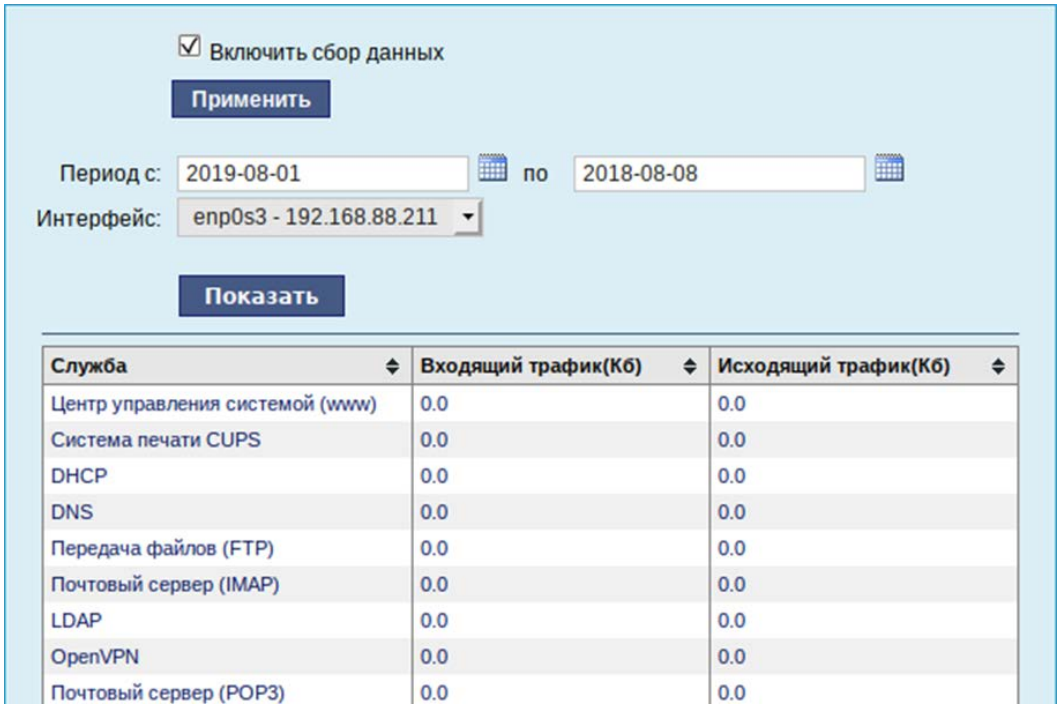


Рис. 115 – Просмотр статистики входящих и исходящих пакетов

8.16.1.2. Прокси-сервер

Пересылка каждого запроса во внешнюю сеть фиксируется прокси-сервером в специальном журнале. На основании этих данных автоматически формируются отчеты о статистике использования ресурсов сети, в том числе потраченного времени и количества переданных данных (трафика).

Статистика не собирается по умолчанию. Включить ее сбор следует в модуле ЦУС «Прокси-сервер» (пакет alterator-squidmill) из раздела «Статистика». Для включения сбора статистики прокси-сервера нужно установить флаг «Включить сбор данных прокси-сервера» (рис. 116).

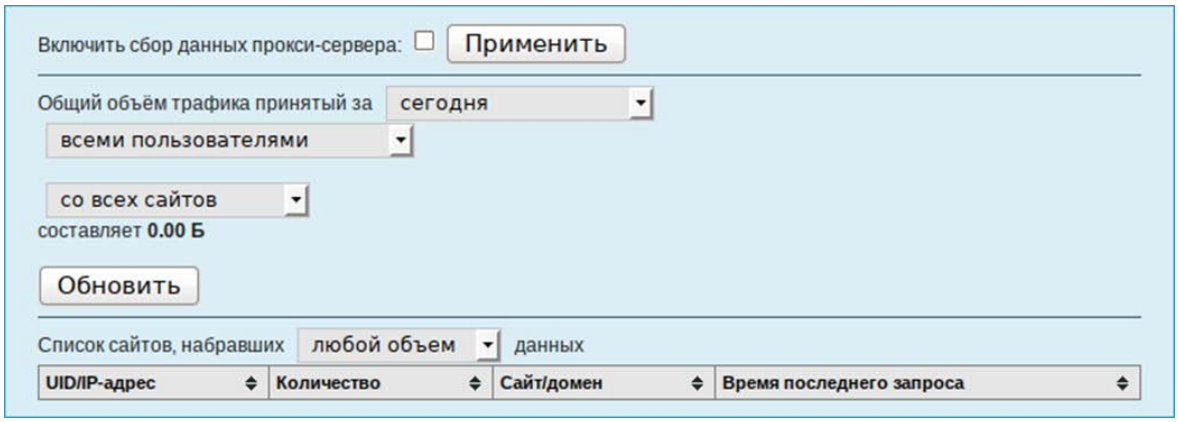


Рис. 116 – Настройка сбора статистики прокси-сервера

В том случае, если на прокси-сервере производилась аутентификация пользователей, отчеты будут содержать данные об обращениях каждого пользователя. Иначе отчеты будут формироваться только на основании адресов локальной сети.

Для показа отчета нужно задать условия фильтра и нажать на кнопку «Показать».

Данные в таблице отсортированы по объему трафика в порядке убывания.

Для учета пользователей в статистике нужно добавить хотя бы одно правило. Самое очевидное правило – запрет неаутентифицированных пользователей. Только после этого в статистике начнут показываться пользователи.

8.17. Обслуживание системы

Для безотказной работы системы очень важно следить за корректной работой. Регулярный мониторинг состояния системы, своевременное резервное копирование, обновление установленного ПО, являются важной частью комплекса работ по обслуживанию.

8.17.1. Мониторинг состояния системы

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

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» (рис. 117).

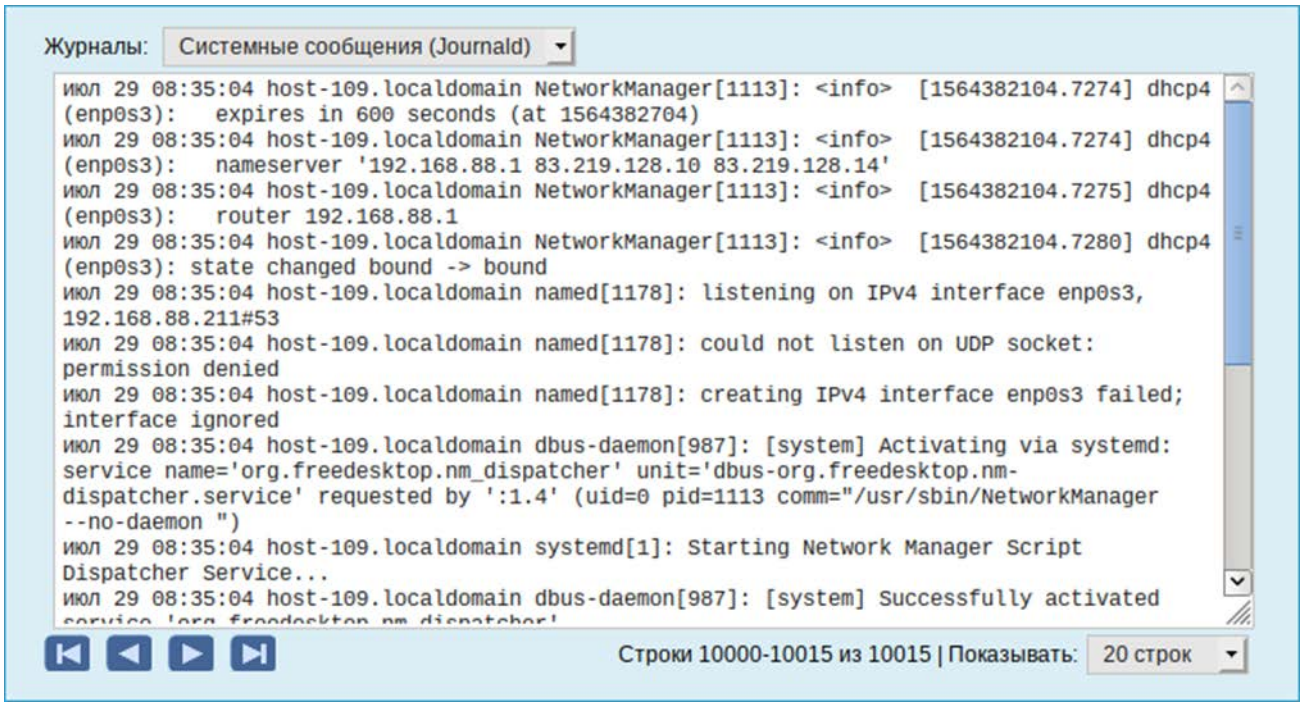


Рис. 117 – Модуль «Системные журналы»

Доступны следующие виды журналов:

- брандмауэр – отображаются события безопасности, связанные с работой межсетевого экрана ОС;
- системные сообщения – сообщения от системных служб (сообщения с типом DAEMON).

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

8.17.2. 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 нужно, применить опцию запуска службы при загрузке системы (рис. 118).

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

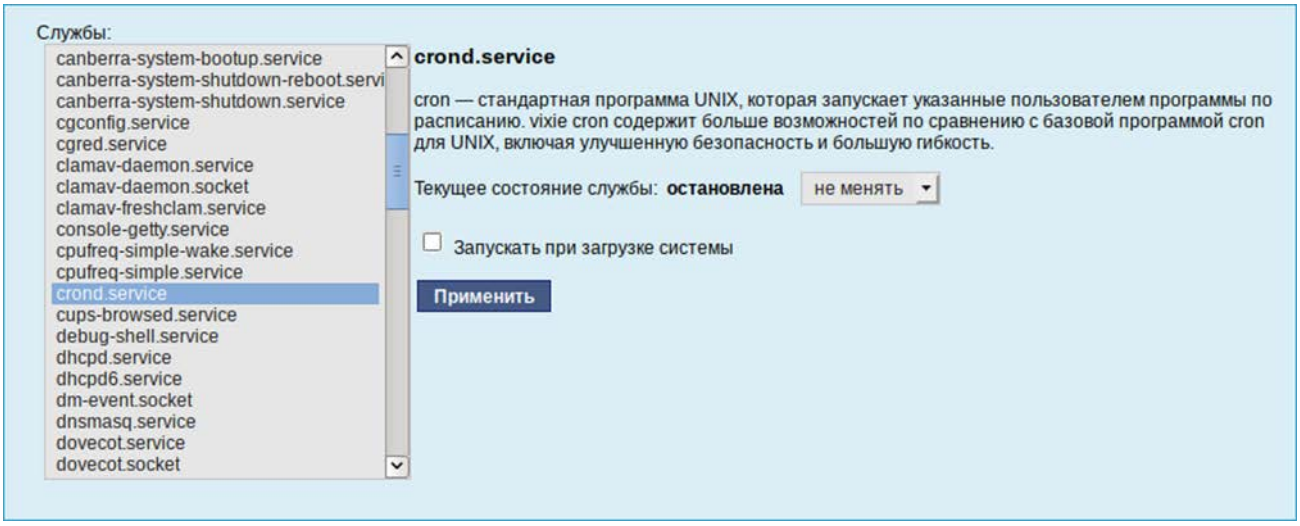


Рис. 118 – Модуль «Системные службы»

8.17.3. Поддержка дополнительных рабочих мест

Модуль ЦУС раздел «Система» → «Настройка нескольких рабочих мест» (пакет alterator-multiseat) – графическое средство настройки мультитерминального режима, позволяющего обеспечить одновременную работу нескольких пользователей на одном компьютере.

Примечание. В системе должен использоваться systemd. Также дисплейный менеджер должен поддерживать концепцию множественных рабочих мест (seat).

Условием для организации нескольких рабочих мест является наличие нескольких видеокарт, одна из которых может быть встроенной. Если вам нужно три места, потребуется три видеокарты.

Для реальной одновременной работы на нескольких рабочих местах кроме видеокарты понадобятся мониторы и комплекты клавиатуры/мыши на каждое рабочее место. Клавиатура и мышь могут быть подключены по USB, возможно через хаб (при задействовании хаба в мониторе стоит убедиться, что он адекватно работает при отключении/подключении устройств).

По умолчанию в системе есть единственное рабочее место с именем `seat0`, к которому подключены все доступные устройства, они перечислены в списке «Устройства seat0». Это рабочее место нельзя удалить или изменить.

В списке «Рабочие места» перечислены дополнительные рабочие места (если они есть), в скобках приводится количество подключенных к данному месту устройств. Чтобы просмотреть устройства, подключенные к дополнительному рабочему месту, нужно выделить его в списке «Рабочие места», устройства будут показаны в списке «Устройства рабочего места» (рис. 119).

Активные рабочие места отмечены знаком [+].

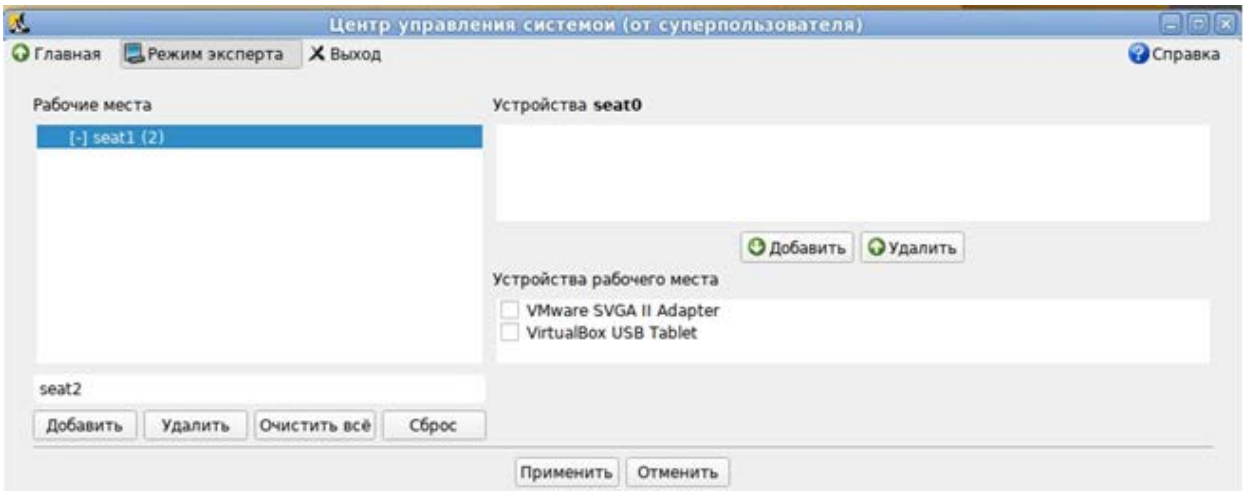


Рис. 119 – Вкладка «Центр управления системой (от суперпользователя)

Назначение кнопок:

- «Применить» – сохраняет текущую конфигурацию, активирует ее (подключает устройства к рабочим местам) и перезагружает компьютер;
- «Отменить» – освобождает все подключенные устройства (возвращает все устройства на seat0);
- «Очистить все» – удаляет все дополнительные места;
- «Сброс» – восстанавливает последнюю сохраненную конфигурацию.

Для создания дополнительного рабочего места ввести желаемое имя в поле ввода, расположенное под списком рабочих мест, и нажать на кнопку «Добавить» (см. рис. 119). Новое рабочее место будет добавлено в список «Рабочие места».

Примечание. Имя рабочего места может содержать только символы a-z, A-Z, 0-9, «-» и «_» и должно начинаться с префикса `seat`. По умолчанию будут сгенерированы имена: `seat1`, `seat2` и т.д.

Выделить нужное рабочее место в списке «Рабочие места», а в списке «Устройства seat0» выбрать устройство, которое нужно назначить выбранному рабочему месту. Нажать на кнопку «Добавить». Устройство появится в списке устройств выбранного рабочего места. К дополнительному рабочему месту нужно добавить видеокарту, клавиатуру и мышь.

ВНИМАНИЕ!

Основную видеокарту нельзя переключать на другие рабочие места.

Примечание. Если в USB-порт вставлен хаб, можно подключить к рабочему месту хаб целиком. Все устройства, которые уже вставлены в него, или будут вставлены потом, автоматически унаследуют подключение к нужному рабочему месту.

Для удаления устройства выделите нужное устройство из списка «Устройства рабочего места» и нажать на кнопку «Удалить».

Аналогичным образом настраиваются все рабочие места.

Для подключения назначенных устройств к дополнительным рабочим местам нажать на кнопку «Применить» и подтвердить активацию (рис. 120). Чтобы настройки вступили в силу нужно перезагрузить компьютер.

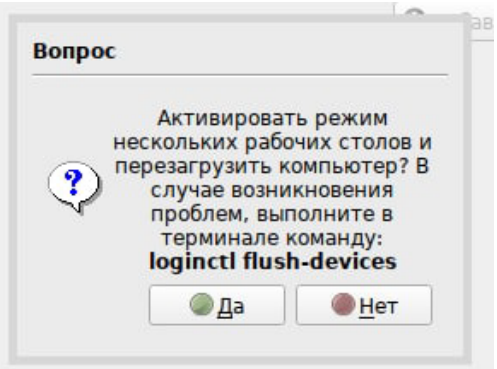


Рис. 120 – Активация режима нескольких рабочих столов

После перезагрузки на мониторах рабочих мест должны появиться приглашения к логину в графическую сессию. Пользователи могут одновременно входить в свои сессии и работать независимо.

ВНИМАНИЕ!

Если после перезагрузки на мониторы не выводится никакая информация, это означает, что «закрепленная» за `seat0` видеокарта была передана на другое рабочее место.

Чтобы исправить данную проблему нужно сбросить настройки. Для этого нужно выполнить вход в учетную запись во второй текстовой консоли («Alt»+»Ctrl»+»F2») и удалить дополнительные рабочие места, выполнив команду (от root):

```
# loginctl flush-devices
```

Перезагрузить компьютер.

8.17.4. Обновление системы

После установки системы крайне важно следить за обновлениями ПО. Обновления для ОС Альт СП 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 надежности работы системы.

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 (рис. 122).

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 (см. в п. 17.14)).

Процесс обновления системы будет запускаться автоматически согласно заданному расписанию.

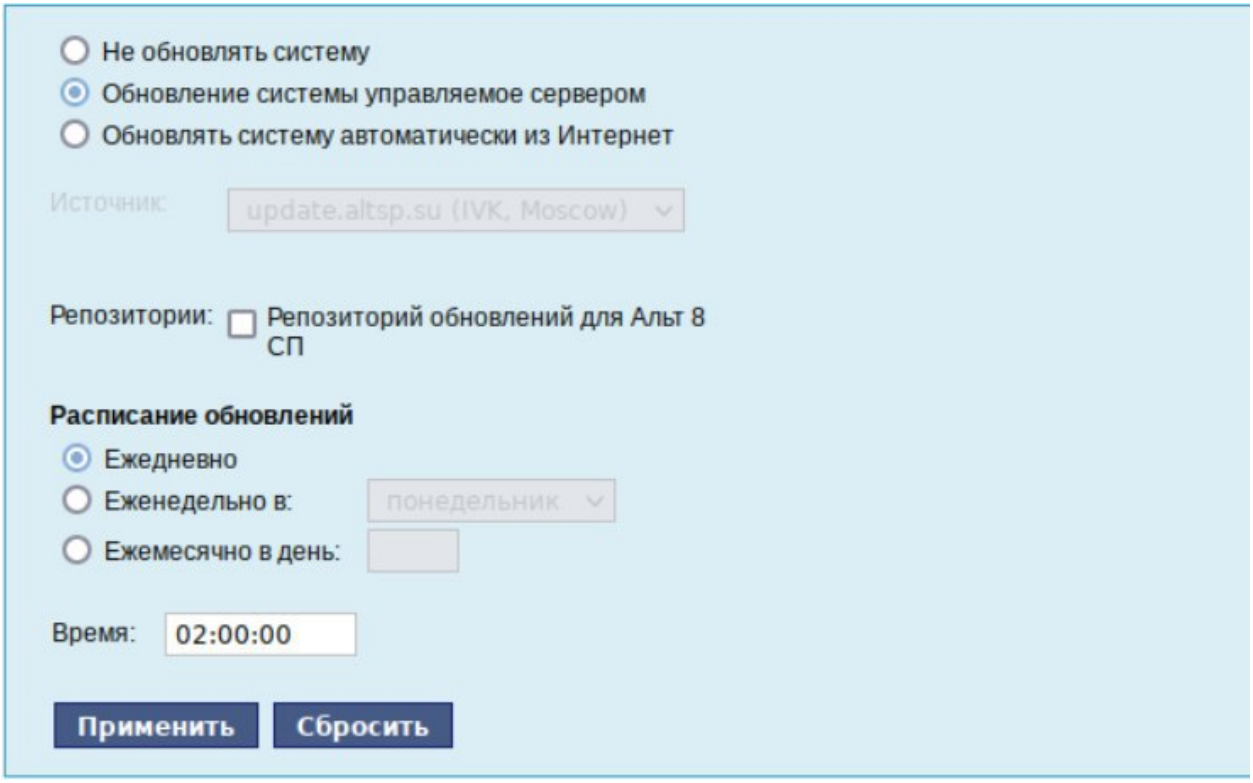


Рис. 122 – Модуль «Обновление системы»

8.17.5. Локальные учетные записи

Модуль «Локальные учетные записи» (пакет alterator-users) из раздела «Пользователи» предназначен для администрирования системных пользователей.

Для создания новой учетной записи нужно ввести имя новой учетной записи и нажать на кнопку «Создать», после чего имя отобразится в списке слева (рис. 123).

Для дополнительных настроек нужно выделить добавленное имя, либо, если нужно изменить существующую учетную запись, выбрать ее из списка.

⚠ При создании пользователя через ЦУС нужно снимать отметку с пунктов «Входит в группу администраторов» и «Автоматический вход в систему» (см. рис. 124).

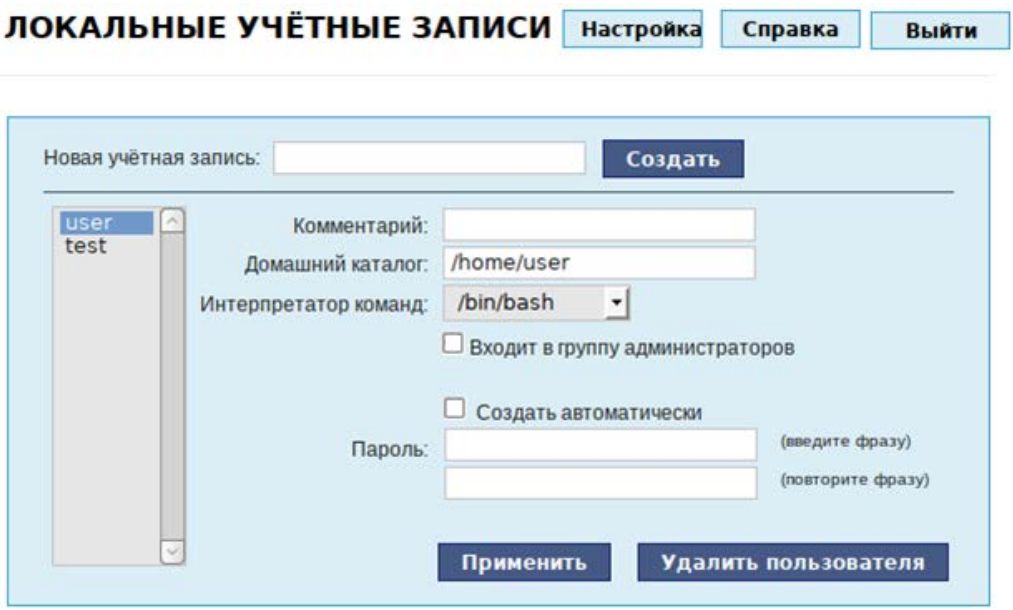


Рис. 123 – Управление локальными пользователями в веб-интерфейсе ЦУС

В модуле ЦУС «Локальные учетные записи» (только GUI) можно задать профиль киоска для пользователя. Режим «киоск» служит для ограничения прав пользователей в системе (рис. 124).

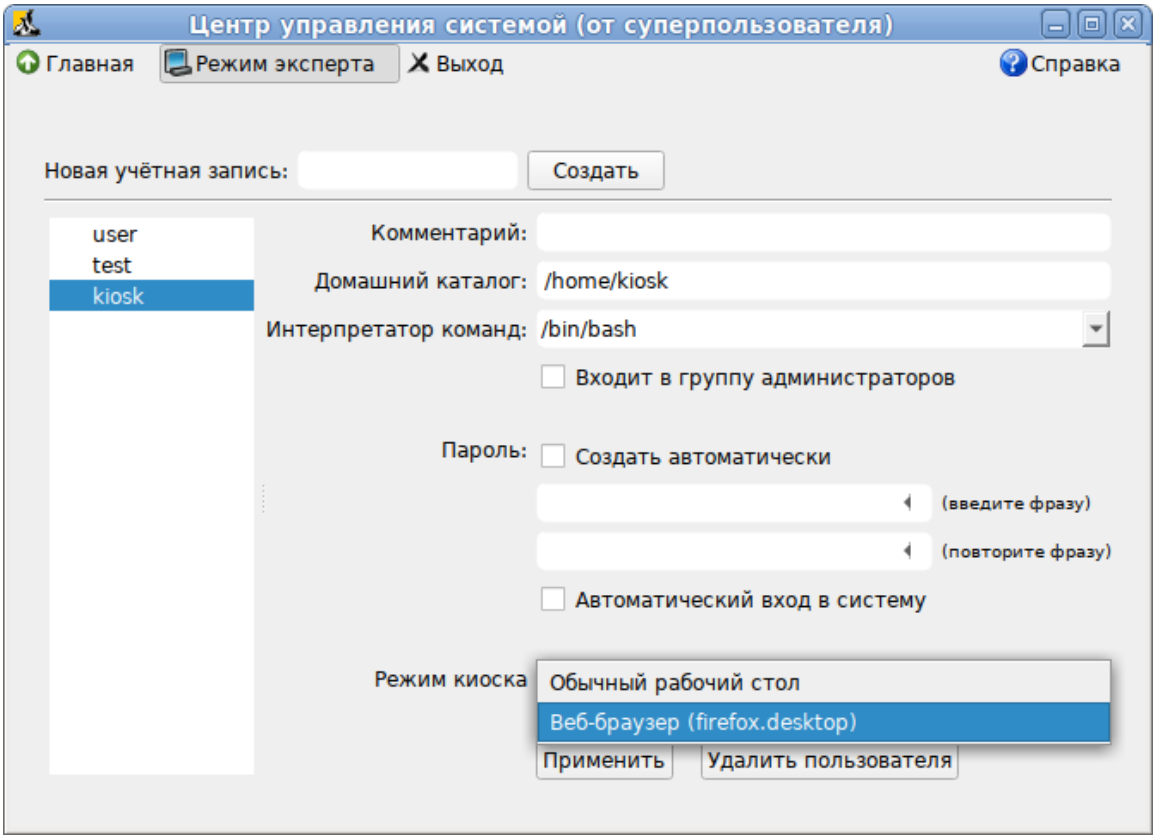


Рис. 124 – Ограничение прав пользователя в системе

Профиль киоска – файл `.desktop` (обычно из `/usr/share/applications`), размещаемый в каталог `/etc/kiosk`.

Для создания профиля можно просто скопировать файл `.desktop` (например, `firefox.desktop`) из `/usr/share/applications`, в каталог `/etc/kiosk`, но лучше создать свой desktop-файл и скрипт, содержащий требуемое ПО.

Пример настройки режима «киоск»:

- создать каталог `/etc/kiosk` (если он еще не создан);
- создать файл `/etc/kiosk/webkiosk.desktop` со следующим содержимым:

```
#!/usr/bin/env xdg-open
[Desktop Entry]
Version=1.0
Type=Application
Terminal=false
Exec=/usr/local/bin/webkiosk
Name=WEB-kiosk
Icon=start
```

- создать файл `/usr/local/bin/webkiosk` со следующим содержимым:

```
#!/bin/bash
marco --replace &
firefox --kiosk --incognito https://ya.ru
```

- сделать файл `/usr/local/bin/webkiosk` исполняемым:

```
# chmod +x /usr/local/bin/webkiosk
```

- в модуле «Локальные учетные записи», выбрать учетную запись пользователя, затем в выпадающем списке «Режим киоска» выбрать пункт «WEB-kiosk» (webkiosk.desktop) и нажать на кнопку «Применить»;
- завершить сеанс текущего пользователя и войти в систему используя учетную запись пользователя, для которого настроен режим «киоск».

Пользователю будет доступен только веб-браузер Mozilla Firefox, по умолчанию будет загружена страница, адрес которой указан в файле `/usr/local/bin/webkiosk`.

8.17.6. Администратор системы

В модуле «Администратор системы» (пакет alterator-root) из раздела «Пользователи» можно изменить пароль суперпользователя (`root`), заданный при начальной настройке системы (рис. 125).

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

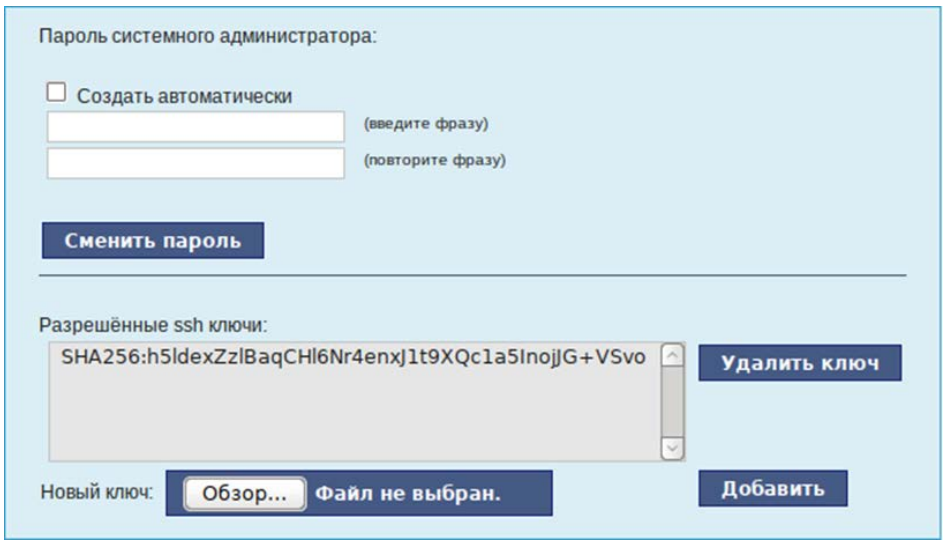


Рис. 125 – Модуль «Администратор системы»

8.17.7. 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 (рис. 126).

Системное время зависит от следующих факторов:

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

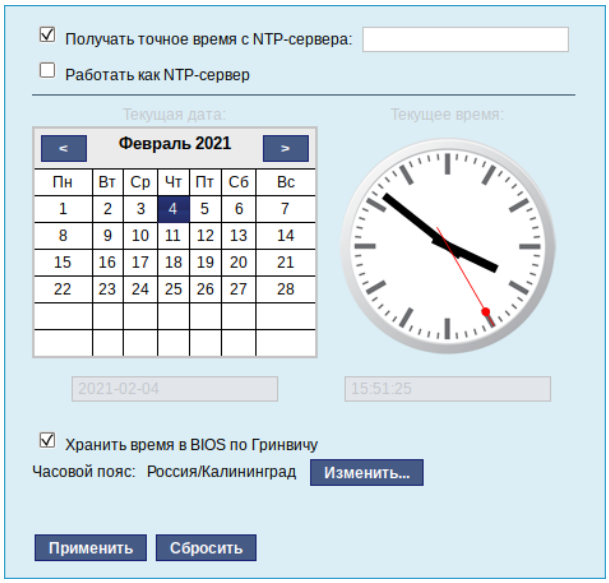


Рис. 126 – Модуль «Дата и время»

При запуске системы происходит активация системных часов и их синхронизация с аппаратными, кроме того, в определенных 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» и нажать на кнопку «Применить» (см. рис. 126).

8.17.8. Ограничение использования диска

Модуль «Использование диска» (пакет alterator-quota) в разделе «Пользователи» позволяет ограничить использование дискового пространства пользователями, заведенными в системе в модуле «Пользователи».

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» (рис. 127).

Модуль позволяет задать ограничения (квоты) для пользователя при использовании определенного раздела диска. Ограничить можно как суммарное количество Кбайт, занятых файлами пользователя, так и количество этих файлов (рис. 127). Выберите пользователя в списке «Пользователь», установите ограничения и нажмите на кнопку «Применить».

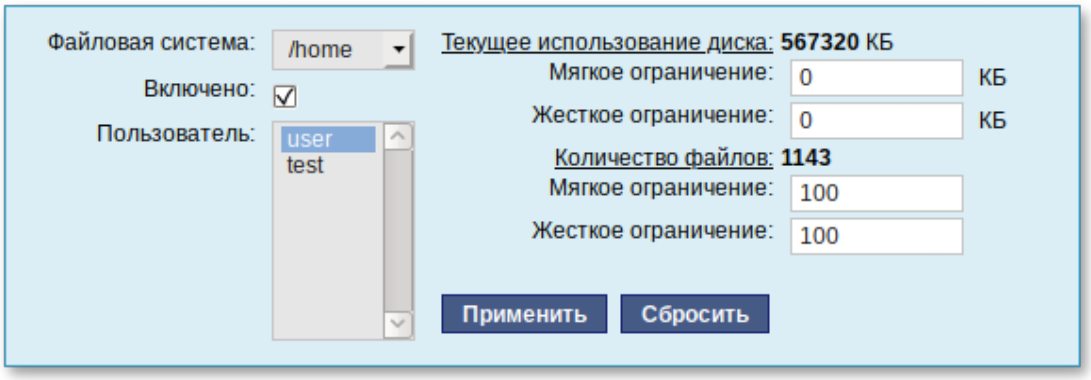


Рис. 127 – Модуль «Использование диска»

При задании ограничений различают жесткие и мягкие ограничения:

- мягкое ограничение: нижняя граница ограничения, которая может быть временно превышена. Временное ограничение – одна неделя;
- жесткое ограничение: использование диска, которое не может быть превышено ни при каких условиях.

Значение 0 при задании ограничений означает отсутствие ограничений.

8.17.9. Резервное копирование

Резервное копирование является важной частью работ по поддержанию работоспособности сервера и всего домена. Так как сервер является критичной частью сети, производите регулярное резервное копирование. При возникновении нештатных ситуаций, например, выхода из строя оборудования, восстановить работоспособное состояние сервера можно из резервной копии.

Bacula – кроссплатформенное клиент-серверное ПО, позволяющее управлять резервным копированием, восстановлением, и проверкой данных по сети для компьютеров и ОС различных типов. Также о Bacula смотрите в документе «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03».

9. ГРУППОВЫЕ ПОЛИТИКИ

Решение представляет собой систему централизованного управления конфигурациями пользователей и компьютеров в домене Active Directory и реализует централизованное хранение на серверах (виртуальной инфраструктуре) данных о пользователях, рабочих станциях, а также предоставляет возможности управления доменом Active Directory и групповыми политиками с помощью графических средств.

9.1. Разворачивание стенда

9.1.1. Схема стенда

Схема стенда показана на рис. 128. Состав технических и программных средств стенда приведен в таблице 8.

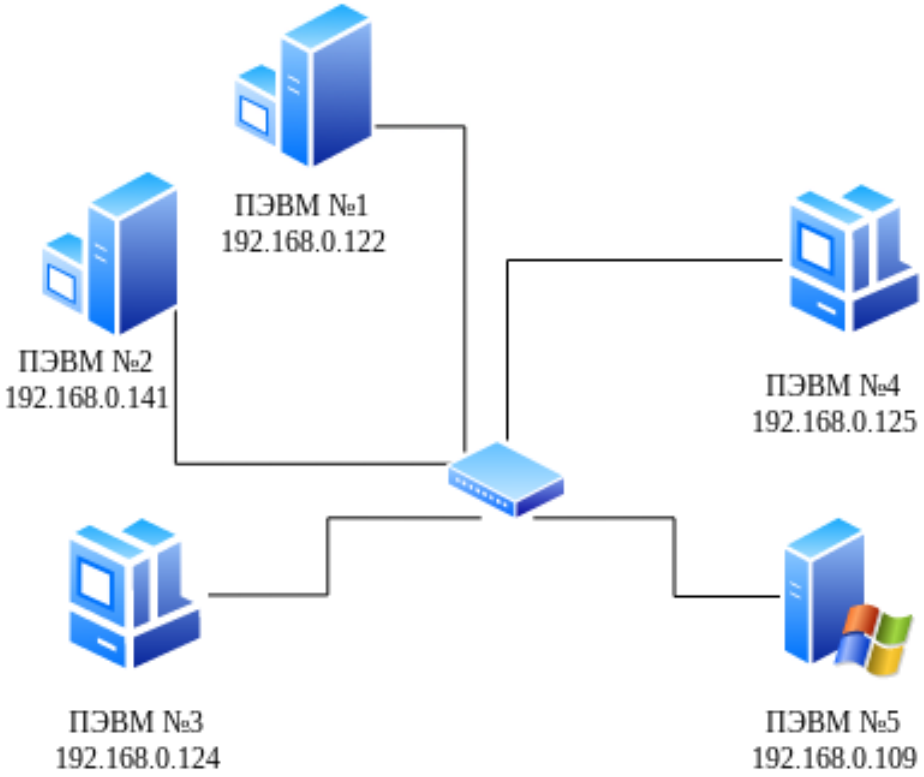


Рис. 128 – Схема стенда

Таблица 8 – Состав технических и программных средств стенда

ПЭВМ №	Программная среда	Описание
1	ОС Альт СП Сервер	Контроллер домена (DC)
2	ОС Альт СП Сервер/ОС Альт СП Рабочая станция	Вторичный DC
3	Должны быть установлены модуль удаленного управления базой данных конфигурации (ADMC) и модуль редактирования настроек клиентской конфигурации (GPUI)	Целевая рабочая станция с инструментами администрирования
4	ОС Альт СП Рабочая станция	Целевая рабочая станция
5	ОС Microsoft Windows Server (управление сервером Samba с помощью RSAT поддерживается из среды до Windows 2012R2 включительно)	Рабочая станция с административными инструментами

Параметры домена:

- домен AD – test.alt;
- сервер AD (ОС ALT) – dc1.test.alt (192.168.0.122);
- вторичный сервер AD (ОС ALT) – dc2.test.alt (192.168.0.141);
- рабочая станция 1 (ОС ALT) – host-01.test.alt (192.168.0.124);
- рабочая станция 2 (ОС ALT) – host-02.test.alt (192.168.0.125);
- рабочая станция 3 (ОС Windows) – PK1.test.alt (192.168.0.109);
- имя пользователя-администратора – Administrator;
- пароль администратора – Pa$$word.

9.1.2. Контроллер домена (Samba AD DC)

9.1.2.1. Разворачивание сервера Samba AD DC

Все действия выполняются на узле dc1.test.alt (192.168.0.122).

Для установки Samba AD DC выполняются следующие шаги:

1) установить пакет task-samba-dc:

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

2) так как Samba в режиме контроллера домена (DC) использует как свой LDAP, так и свой сервер Kerberos, несовместимый с MIT Kerberos, перед установкой нужно 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) если домен уже создавался, нужно очистить базу и конфигурацию Samba:

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

⚠ Перед созданием домена нужно обязательно удалить `/etc/samba/smb.conf`: `rm -f /etc/samba/smb.conf`

---

4) установить имя домена (этот шаг можно пропустить, если имя компьютера было задано при установке системы на этапе «Настройка сети» (см. п. 5.4.9)). Имя домена для разворачиваемого DC должно состоять минимум из двух компонентов, разделенных точкой.

При этом должно быть установлено правильное имя узла и домена для сервера. Для этого в файл `/etc/sysconfig/network` добавить строку:

```
HOSTNAME=dc1.test.alt
```

И выполнить команды:

```
# hostnamectl set-hostname dc1.test.alt
# domainname test.alt
```

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

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

---

5) для корректного функционирования домена в файле `/etc/resolv.conf` должна присутствовать строка:

```
nameserver 127.0.0.1
```

Если этой строки в файле `/etc/resolv.conf` нет, то в конец файла `/etc/resolvconf.conf` следует добавить строку:

```
name_servers='127.0.0.1'
```

и перезапустить сервис resolvconf:

```
# resolvconf -u
```

6) создать домен test.alt с паролем администратора Pa$$word:

```
# 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 --use-rfc2307
```

где:

- `---realm` – область Kerberos (LDAP), и DNS имя домена;
- `---domain` – имя домена (имя рабочей группы);
- `---adminpass` – пароль основного администратора домена;
- `-dns forwarder` – внешний DNS-сервер;
- `---server-role` – тип серверной роли;
- `---use-rfc2307` – позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux.

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трех групп из четырех 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.

7) запустить службу:

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

8) настроить Kerberos. В момент создания домена Samba конфигурирует шаблон файла `krb5.conf` для домена в каталоге `/var/lib/samba/private/`. Заменить этим файлом файл, находящийся в каталоге `/etc/`:

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

9) проверить работоспособность домена:

- просмотр общей информации о домене:

```
# samba-tool domain info 127.0.0.1
Forest              : test.alt
Domain              : test.alt
Netbios             : TEST
domain
DC name             : dc1.test.alt
DC   netbios        : DC1
name
Server site         : Default-First-Site-Name
Client site         : Default-First-Site-Name
```

- убедиться в наличии nameserver 127.0.0.1 в файле `/etc/resolv.conf`:

```
# cat /etc/resolv.conf
search test.alt
nameserver 127.0.0.1

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

- проверить 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
```

- проверка Kerberos (имя домена должно быть в верхнем регистре):

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

Примечание. Если имена не находятся, нужно проверить выключение службы named.

10) создать и разблокировать пользователя ivanov в домене:

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

9.1.2.2. Установка административных шаблонов

Для задания конфигурации нужно установить административные шаблоны (ADMX-файлы). Для этого:

1) установить пакеты политик:

```
# apt-get install admx-basealt admx-samba admx-chromium admx-firefox
```

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

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

9.1.2.3. Заведение вторичного DC и настройка репликации

Все действия выполняются на узле dc2.test.alt (192.168.0.141), если не указано иное.

Для заведения вторичного DC выполняются следующие шаги:

1) установить пакет:

```
# 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:

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

4) задать имя компьютера (этот шаг можно пропустить, если имя компьютера было задано при установке системы на этапе «Настройка сети» (см. п. 5.4.9)):

```
# hostnamectl set-hostname dc2.test.alt
```

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

5) на вторичном DC в файле `/etc/resolv.conf` обязательно должен быть добавлен Primary Domain Controller (PDC) как `nameserver` (этот шаг можно пропустить, если имя компьютера было задано при установке системы на этапе «Настройка сети» (см. п. 5.4.9)):

```
# 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
```

6) на 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
```

7) на PDC завести IP-адрес для dc2:

⚠ Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

```
# samba-tool dns add 192.168.0.122 test.alt DC2 A 192.168.0.141 -Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

8) на вторичном DC установить следующие параметры в файле конфигурации клиента Kerberos (файл `/etc/krb5.conf`):

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

9) для проверки настройки запросить билет Kerberos для администратора домена:

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
Убедиться, что билет получен:
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
14.09.2022      15:50:40             15.09.2022      01:50:40
krbtgt/TEST.ALT@TEST.ALT
    renew until 21.09.2022 15:50:34
```

10) 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 все нормально, в конце будет выведена информация о присоединении к домену:

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

11) запустить и сделать службу samba запускаемой по умолчанию:

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

9.1.2.3.1. Настройка репликации

1) Репликация на вторичном DC (с первичного):

```
# samba-tool drs replicate dc2.test.alt dc1.test.alt dc=test,dc=alt -Uadministrator
Password for [TEST\administrator]:
Replicate from dc1.test.alt to dc2.test.alt was successful.
```

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

2) Репликация на вторичном DC (на первичный):

```
# samba-tool drs replicate dc1.test.alt dc2.test.alt dc=test,dc=alt -Uadministrator
Password for [TEST\administrator]:
Replicate from dc2.test.alt to dc1.test.alt was successful.
```

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

3) Просмотр статуса репликации на PDC:

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

9.1.3. Настройка рабочей станции

9.1.3.1. Ввод рабочей станции в домен Active Directory

Для ввода компьютера в Active Directory потребуется установить пакет task-auth-ad-sssd (и все его зависимости) и пакет alterator-gpupdate для включения групповых политик:

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

П р и м е ч а н и е . Нужно произвести настройку сети, если она не выполнялась при установке системы. Для этого в ЦУС в разделе «Сеть» → «Ethernet интерфейсы» следует задать имя компьютера, указать в поле «DNS-серверы» DNS-сервер домена и в поле «Домены поиска» – домен для поиска (рис. 129).

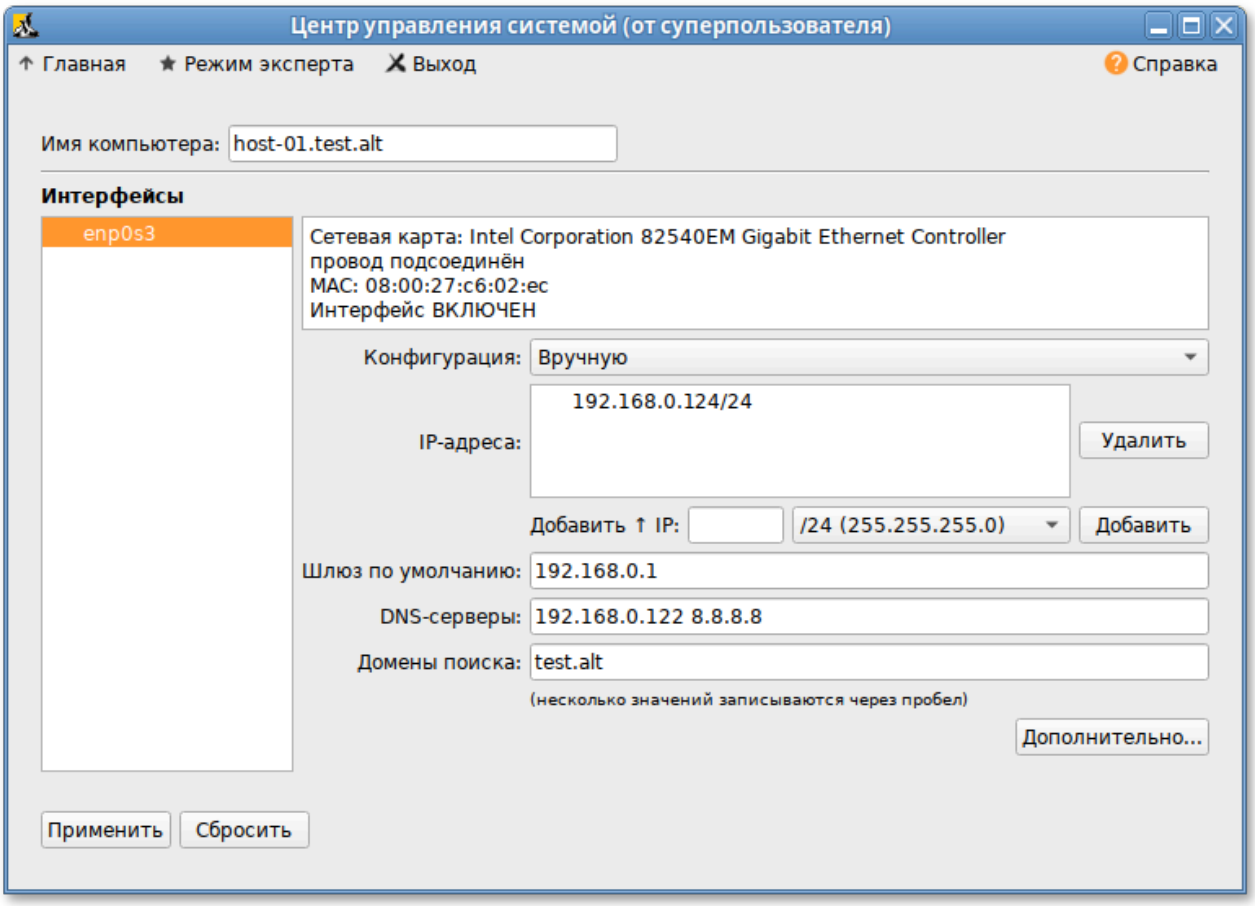


Рис. 129 – Окно «Центр управления системой (от суперпользователя)»

В результате в файле `/etc/resolv.conf` должны появиться строки:

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

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

Для ввода рабочей станции в домен нужно запустить ЦУС («Меню» → «Система» → «Администрирование» → «Центр управления системой»). В ЦУС следует перейти в раздел «Пользователи» → «Аутентификация». В открывшемся окне следует выбрать пункт «Домен Active Directory», заполнить поля и нажать кнопку «Применить» (рис. 130).

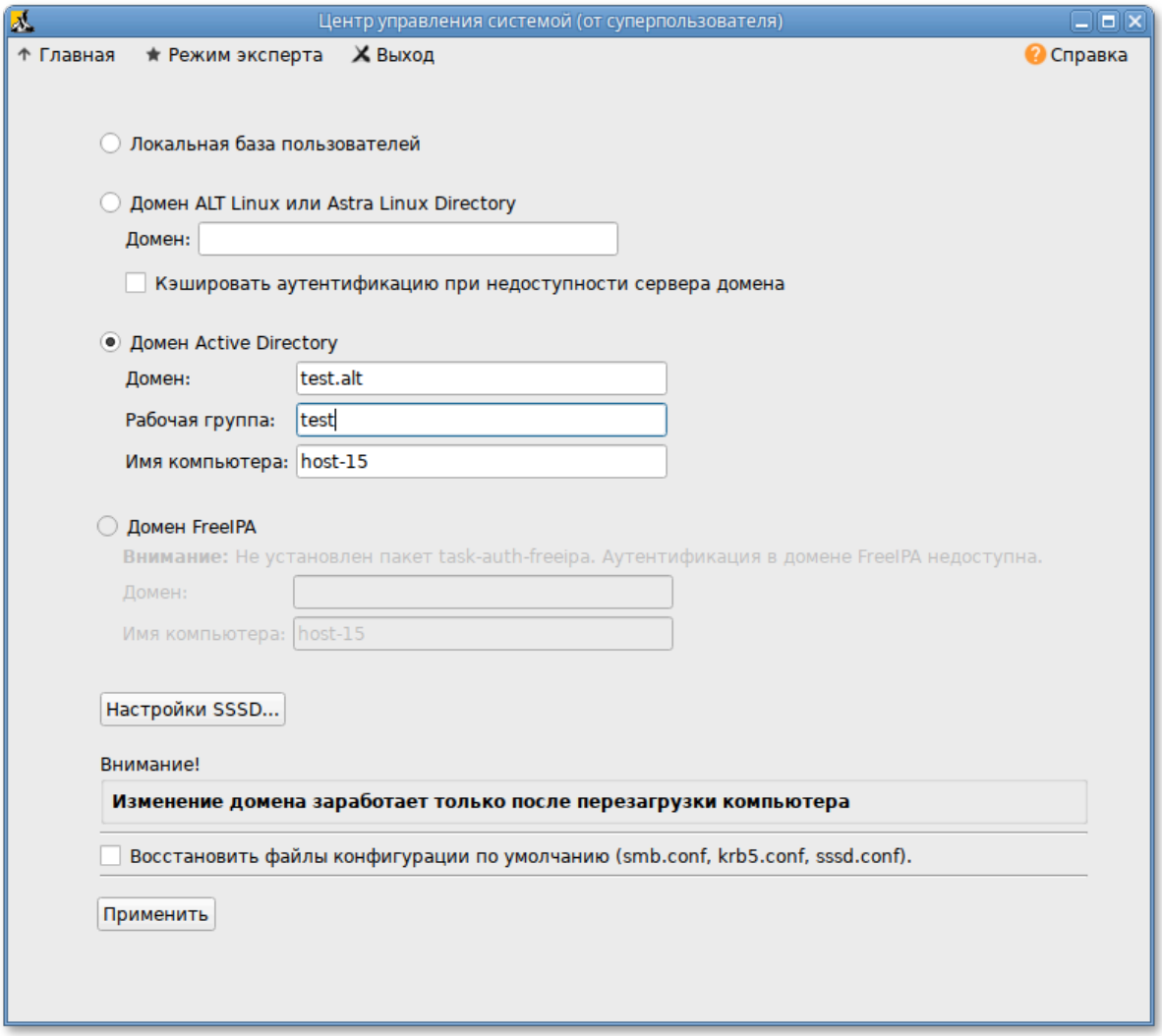


Рис. 130 – Окно ввода рабочей станции в домен

В открывшемся окне нужно ввести имя пользователя, имеющего право вводить машины в домен, и его пароль, установить отметку в поле «Включить групповые политики» и нажать кнопку «ОК» (рис. 131).

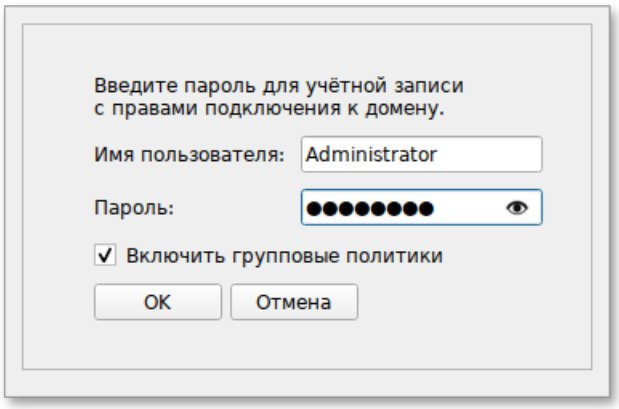


Рис. 131 – Окно ввода имени пользователя и пароля

При успешном подключении к домену, отобразится соответствующая информация (рис. 132).

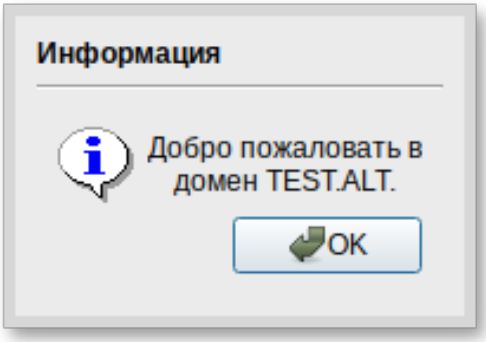


Рис. 132 – Окно информации об успешном подключении к домену

Далее нужно перезагрузить рабочую станцию.

Проверить подключение к домену (ivanov – пользователь в домене):

```
# getent passwd Ivanov
ivanov:*:1327601105:1327600513:Иван
Иванов:/home/TEST.ALT/ivanov:/bin/bash

# net ads info
LDAP server: 192.168.0.122
LDAP server name: dc1.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
LDAP port: 389
Server time: Пн, 18 июл 2022 15:54:05 EET
KDC server: 192.168.0.122
Server time offset: -1270
Last machine account password change: Пн, 18 июл 2022 15:54:05 EET

# net ads testjoin
Join is OK
```

Примечание. Список пользователей можно посмотреть на сервере командой:

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

9.1.4. Установка административных инструментов

Административные инструменты устанавливаются на рабочей станции, введенной в домен.

9.1.4.1. Модуль удаленного управления базой данных конфигурации (ADMC)

Установить пакет admc:

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

Запуск ADMC осуществляется из меню запуска приложений: пункт «Системные» → «ADMC» или из командной строки (команда admc) (рис. 133).

Примечание. Для использования ADMC нужно предварительно получить ключ Kerberos для администратора домена. Получить ключ Kerberos можно, например, выполнив следующую команду:

```
$ kinit administrator
```

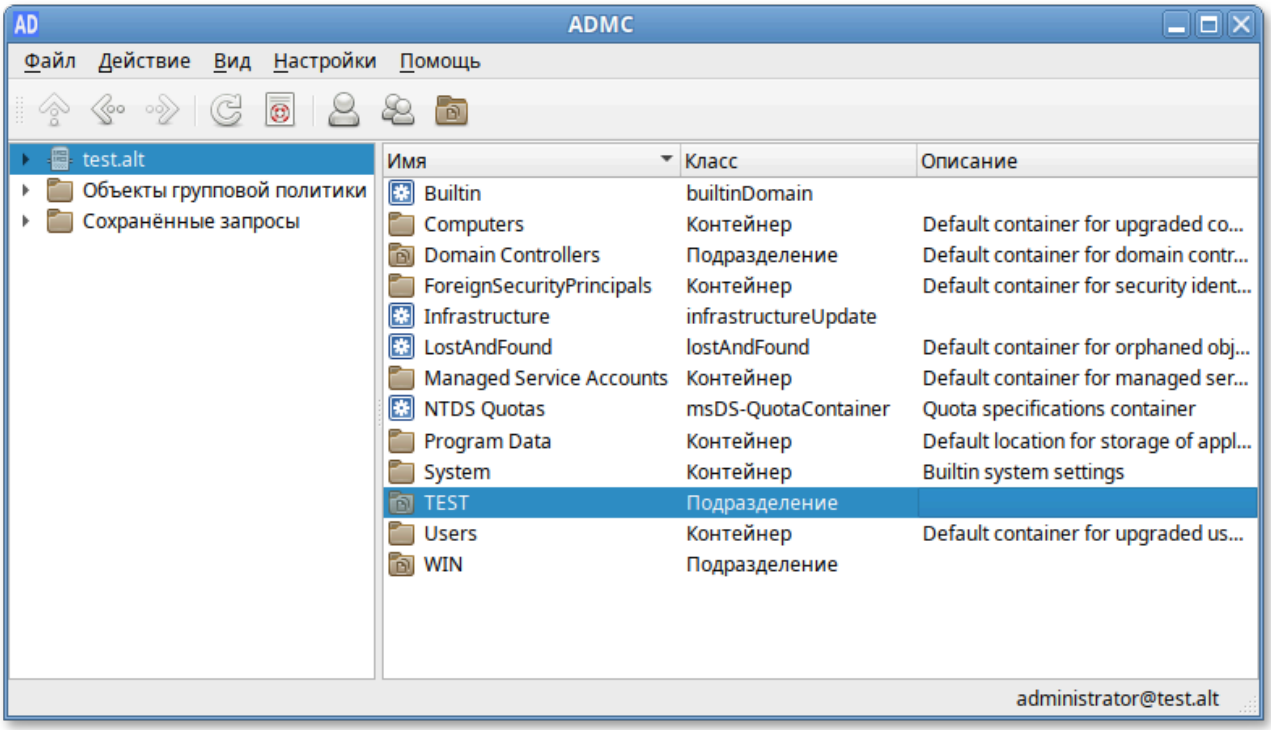


Рис. 133 – Окно модуля удаленного управления базой данных конфигурации (ADMC)

9.1.4.2. Модуль редактирования настроек клиентской конфигурации (GPUI)

Установить пакет gpui:

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

Примечание. В настоящее время GPUI не умеет читать файлы ADMX с контроллера домена. Для корректной работы нужно установить пакеты admx:

```
# apt-get install admx-basealt admx-samba admx-chromium admx-firefox
```

Для использования GPUI нужно предварительно получить ключ Kerberos для администратора домена (рис. 134). Получить ключ Kerberos можно, например, выполнив следующую команду:

```
$ kinit administrator
```

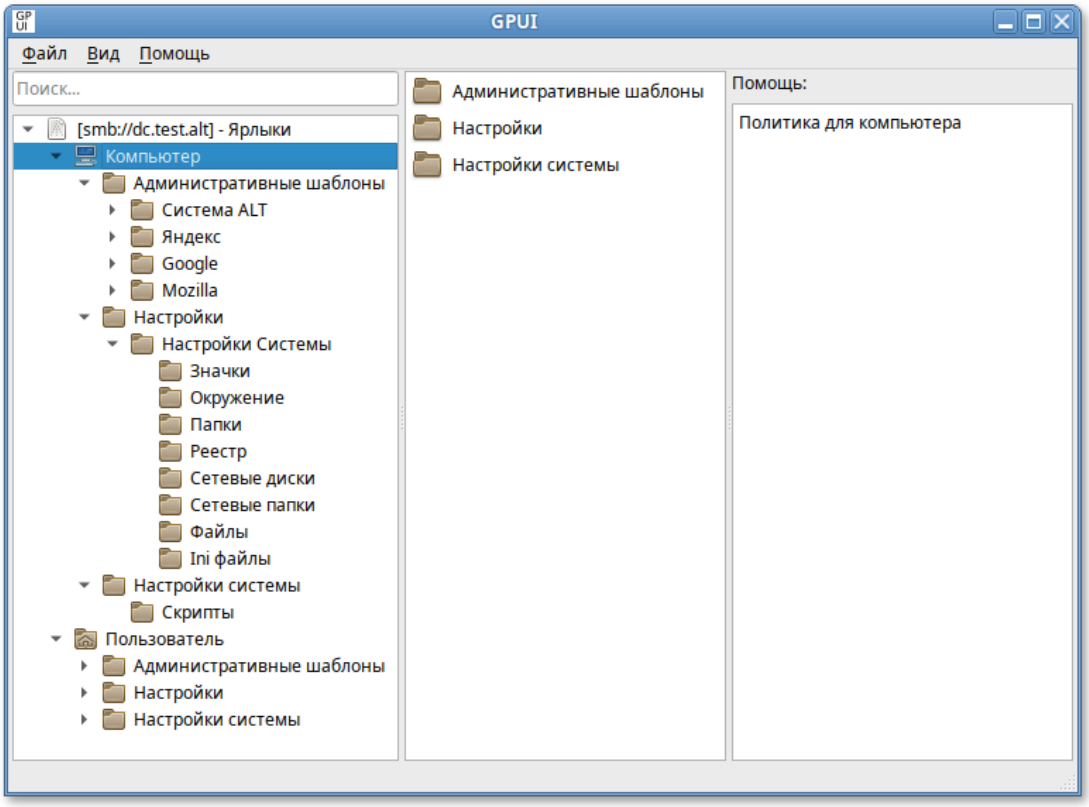


Рис. 134 – Окно модуля редактирования настроек клиентской конфигурации (GPUI)

По умолчанию GPUI не редактирует никаких политик. Для того чтобы редактировать политику, GPUI нужно запустить либо из ADMC, выбрав в контекстном меню объекта групповой политики пункт «Изменить…» (рис. 135).

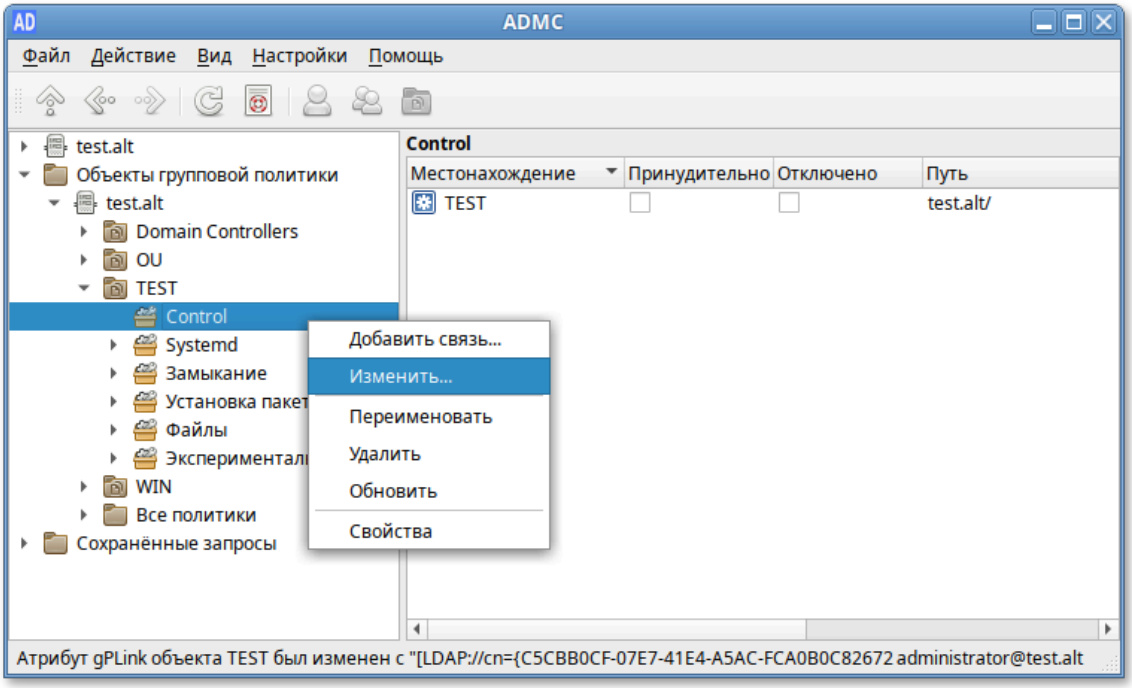


Рис. 135 – Редактирование политики GPUI

либо с указанием каталога групповой политики:

```
$ gpui-main -p "smb://dc1.test.alt/SysVol/test.alt/Policies/{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXXX}"
```

Ключ `-p` позволяет указать путь к шаблону групповой политики, который нужно редактировать, `dc1.test.alt` – имя контроллера домена, а `{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXXX}` – GUID шаблона групповой политики для редактирования. Можно указывать как каталоги smb, так и локальные каталоги.

Пример запуска GPUI для редактирования политики:

```
$ gpui-main -p "smb://dc1.test.alt/SysVol/test.alt/Policies/{2E80AFBE-BBDE-408B-B7E8-AF79E02839D6}"
```

9.2. Описание функций

9.2.1. Описание структуры

Логическая структура Решения содержит следующие компоненты (рис. 136):

- сервер базы данных с информацией о клиентах и их конфигурации;
- клиентское ПО для репликации и применения конфигурации;
- графическая панель управления включением механизма применения конфигурации;
- графический редактор базы данных конфигурации;
- графический редактор настроек клиентской конфигурации.

Решение включает следующие компоненты:

- модуль панели управления операционной системы для включения механизма применения конфигурации на клиентских машинах;
- модуль клиентской машины для применения конфигурации;
- модуль удаленного управления базой данных конфигурации;
- модуль редактирования настроек клиентской конфигурации.

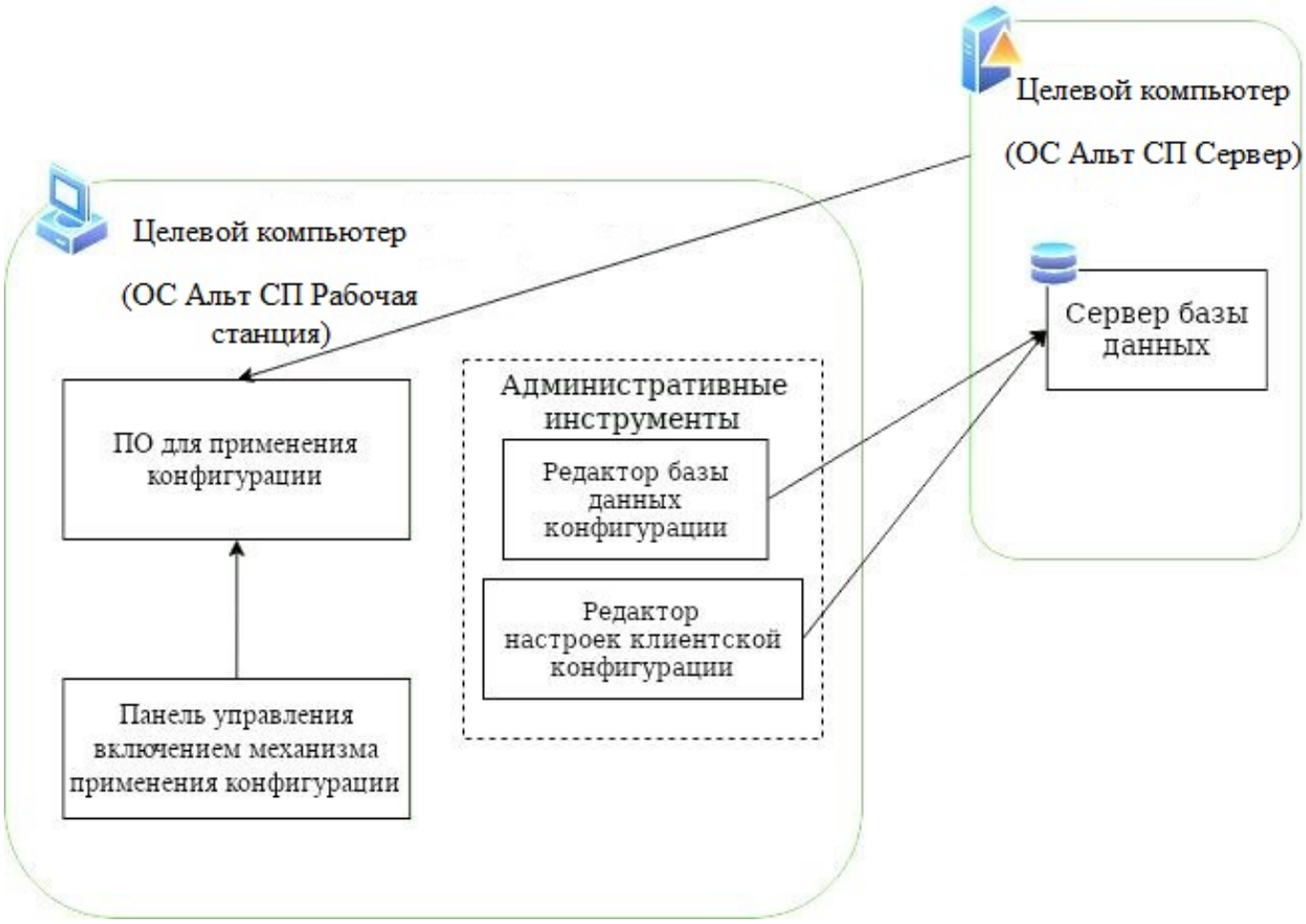


Рис. 136 – Логическая структура

9.2.2. Модуль панели управления операционной системы для включения механизма применения конфигурации на клиентских машинах

Модуль панели управления операционной системы для включения механизма применения конфигурации на клиентских машинах предназначен для управления включением работы групповых политик и выбором политики по умолчанию.

Модуль панели управления операционной системы для включения механизма применения конфигурации на клиентских машинах представляет собой модули ЦУС:

- «Аутентификация» (пакет alterator-auth);
- «Групповые политики» (пакет alterator-gpupdate).

ЦУС представляет собой удобный интерфейс для выполнения наиболее востребованных административных задач по управлению сервером: добавление и удаление локальных пользователей, настройка сетевых подключений, просмотр информации о состоянии системы и т. п. ЦУС состоит из независимых диалогов-модулей. Каждый модуль отвечает за настройку определенной функции или свойства системы. Модули настройки сгруппированы по задачам, как показано на рис. 137.

Возможность включения групповых политик реализована как при вводе машины в домен AD, так и на уже включенной в домен рабочей станции.

Для включения групповых политик при вводе машины в домен следует в модуле ЦУС «Аутентификация» выбрать пункт «Домен Active Directory», заполнить поля «Домен», «Рабочая группа» и «Имя компьютера», и нажать кнопку «Применить» (рис. 138).

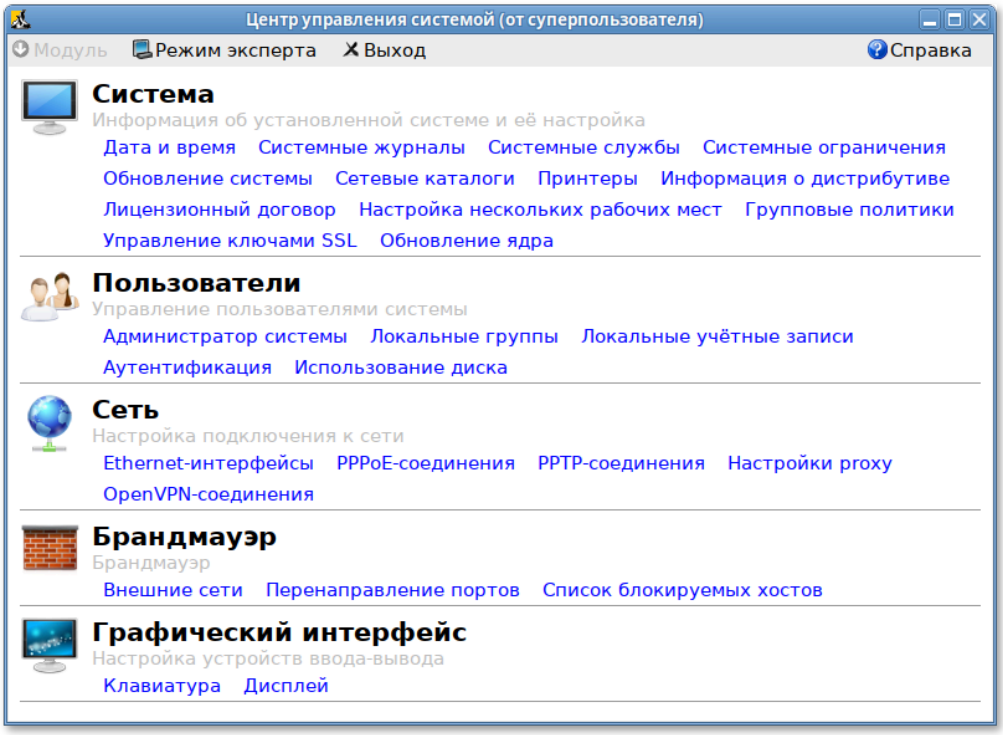


Рис. 137 – Группировка модулей настройки

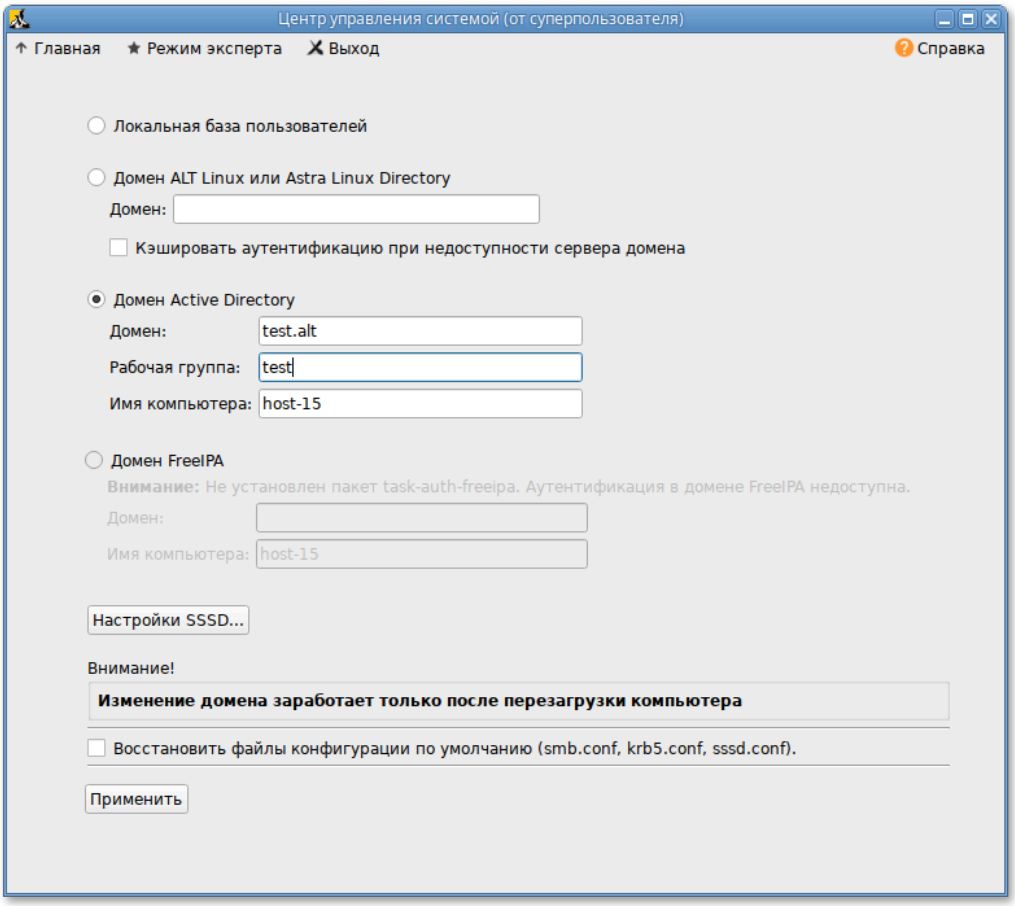


Рис. 138 – Включение групповых политик

В открывшемся окне ввести имя пользователя, имеющего право вводить машины в домен, и его пароль, отметить пункт «Включить групповые политики» и нажать кнопку «ОК» (рис. 139).

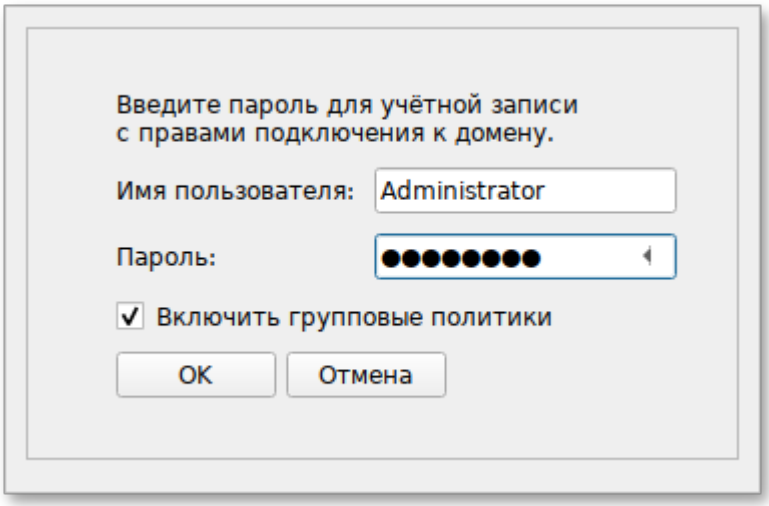


Рис. 139 – Включение групповых политик. Вход в учетную запись

Включить поддержку управления групповыми политиками на машине уже введенной в домен можно в модуле ЦУС «Групповые политики» (рис. 140).

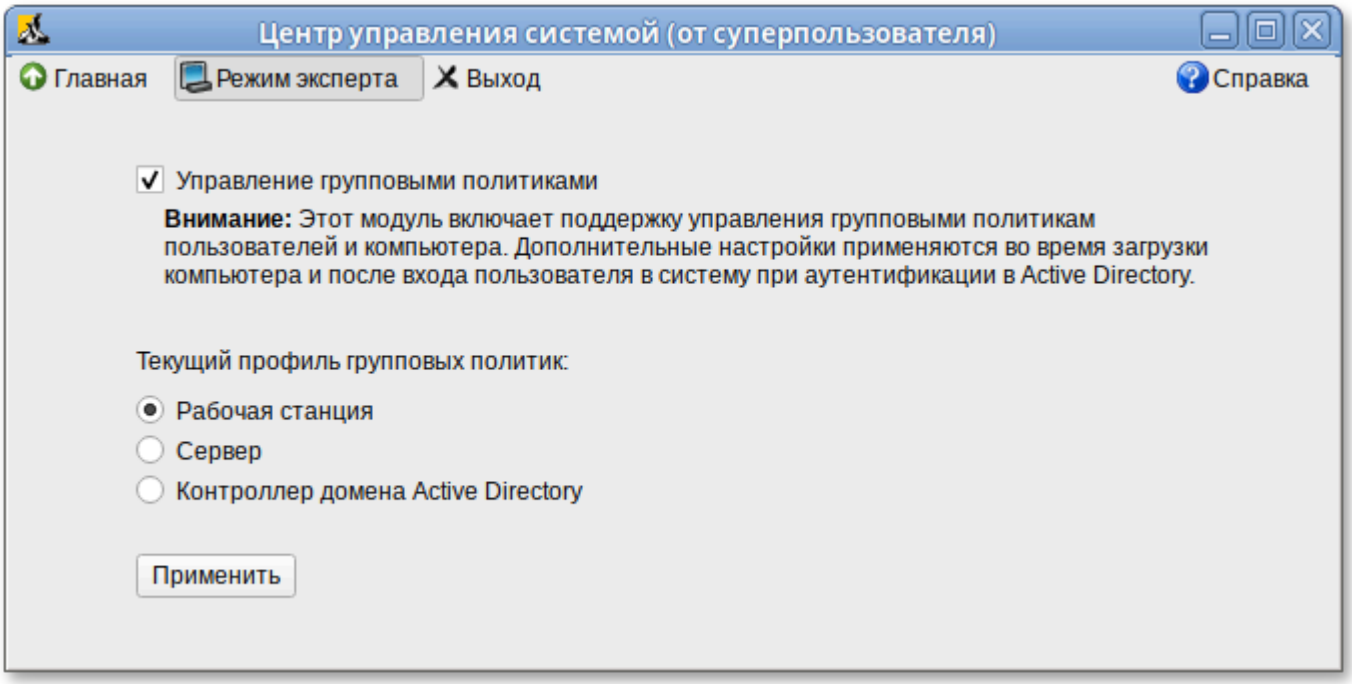


Рис. 140 – Включение поддержки управления групповыми политиками

Модуль «Групповые политики» позволяет управлять включением/выключением поддержки групповых политик на машинах, введенных в домен, а также выбирать профиль политики по умолчанию:

- «Сервер»;
- «Контроллер домена Active Directory»;
- «Рабочая станция».

Для возможности включения групповых политик на машинах под управлением ОС Альт СП, на которых не установлена графическая оболочка, модуль «Групповые политики» доступен также в веб-интерфейсе ЦУС (рис. 141).

Работа с веб-ориентированным интерфейсом ЦУС может происходить из любого веб-браузера с любого компьютера сети.

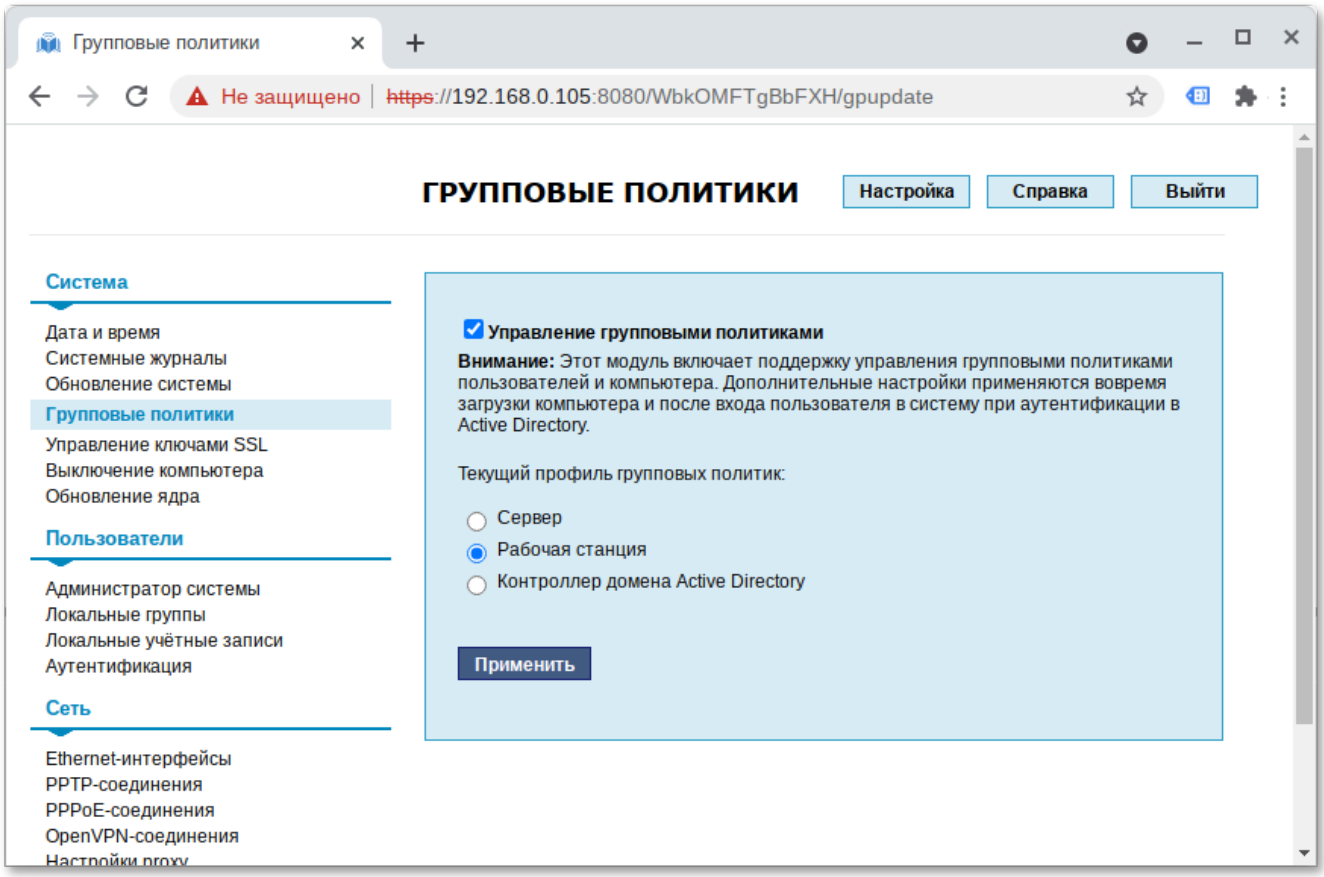


Рис. 141 – Модуль «Групповые политики» в веб-интерфейсе

9.2.3. Модуль клиентской машины для применения конфигурации

Модуль клиентской машины для применения конфигурации (далее – gpupdate) отвечает за применение заданных администратором системы настроек конфигурации к клиентской машине и/или пользователю машины.

ПО состоит из компонента, который авторизуется в домене и выполняет скачивание файлов настроек на клиентскую машину. Далее происходит разбор файлов настроек и складывание полученных данных в хранилище именуемое также «реестр». Это позволяет развязать методы доставки и применения настроек.

При успешной репликации настроек запускается часть системы, называемая «фронтенд». Она отвечает за запуск различных модулей (appliers), каждый из которых отвечает за свою логическую функцию. Например, модуль firefox отвечает за вычитывание настроек для веб-браузера Mozilla Firefox и создание файла политик для него, а модуль ntp отвечает за чтение настроек, касающихся NTP-сервера и создании подходящей конфигурации.

Количество и функционал модулей может меняться по мере развития и актуализации продукта и компонентов системы, с которыми они работают.

Групповые политики обрабатываются в следующем порядке:

- объект локальной групповой политики;
- объекты групповой политики, связанные с доменом (в рамках возможностей и ограничений поддержки леса доменов в Samba, как наборе клиентских компонент);
- объекты групповой политики, связанные с OU, обрабатываются в определенном порядке. Сначала обрабатываются объекты групповой политики, находящейся на самом высоком уровне в иерархии Active Directory, затем объекты групповой политики, связанные с дочерним подразделением и т. д. Последними обрабатываются объекты групповой политики, в которой находится пользователь или компьютер.

Процесс применения настроек:

- настройки для машины реплицируются при запуске компьютера и далее обновляются раз в час;
- настройки для пользователя реплицируются при входе пользователя в систему и далее обновляются раз в час.

Для работы механизмов применения пользовательских настроек задействовано множество компонентов ОС таких, как systemd, D-Bus, PAM (рис. 142).

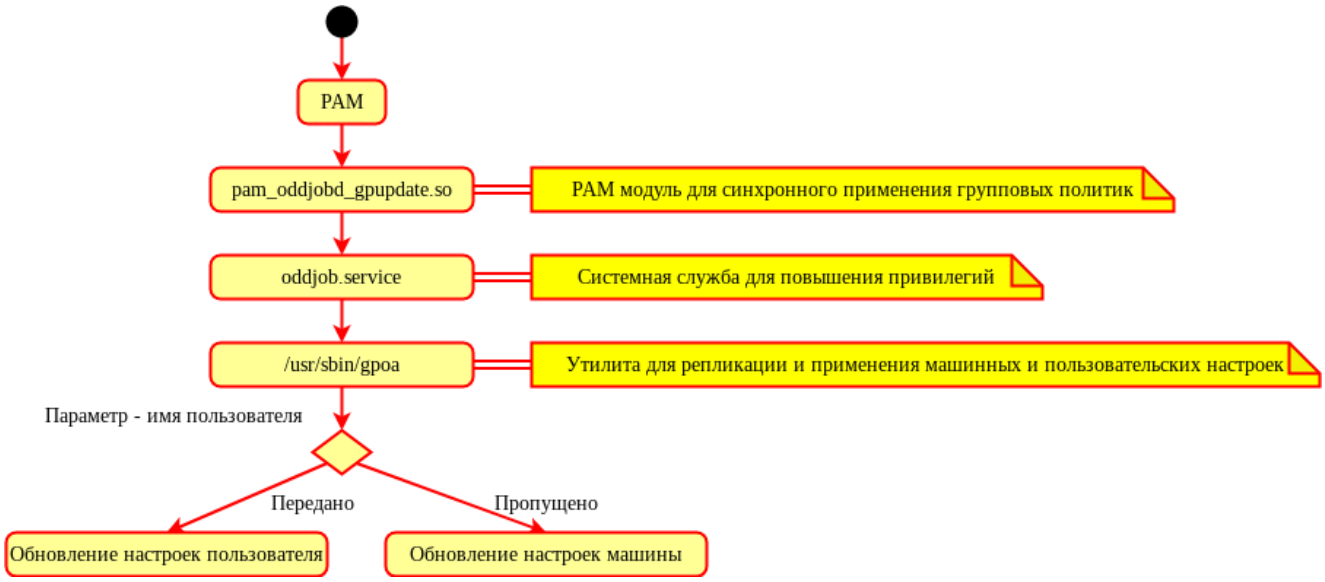


Рис. 142 – Компоненты ОС

Часть проекта, отвечающая за получение и применение групповых политик, внутри использует базу данных («реестр»), для хранения настроек, полученных из различных источников.

9.2.3.1. Утилиты модуля

Модуль состоит из трех утилит:

- gpoa – системная утилита, осуществляющая применение групповых политик для компьютера или пользователя (gpoa без параметра отрабатывает только для машины, для пользователя нужно указывать username);
- gpupdate – утилита, осуществляющая запрос на применение групповых политик. При запуске с привилегиями администратора может непосредственно выполнить применение групповых политик, минуя нужность повышения привилегий;
- gpupdate-setup – инструмент администрирования механизмов применения групповых политик. Позволяет включать и отключать применение групповых политик, а также задавать шаблон политики по умолчанию («Рабочая станция», «Сервер», «Контроллер домена»).

Синтаксис команды gpoa:

`gpoa [-h] [--dc DC] [--nodomain] [--noupdate] [--noplugins] [--list-backends] [--loglevel LOGLEVEL] [пользователь]`

Опции команды gpoa указаны в таблице 9.

Таблица 9 – Опции команды gpoa

Ключ	Описание
-h, --help	Вывести справку о команде
--dc DC	Указать полное имя (FQDN) контроллера домена для реплицирования SYSVOL
--nodomain	Работать без домена (применить политику по умолчанию)
--noupdate	Не пытаться обновить хранилище, только запустить appliers
--noplugins	Не запускать плагины
--list-backends	Показать список доступных бэкэндов
--loglevel LOGLEVEL	Установить уровень журналирования
пользователь	Имя пользователя домена

Примеры работы с командой gpoa:

- получить и применить настройки для текущей машины:

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

- применить закэшированные настройки для текущей машины:

```
# gpoa --noupdate
```

- получить и применить настройки с контроллера домена dc1.test.alt для пользователя ivanov:

```
# gpoa --dc dc1.test.alt --loglevel 3 ivanov
```

- применить политику по умолчанию:

```
# gpoa --–nodomain --loglevel 0
```

Синтаксис команды gpupdate:

```
gpupdate [-h] [-u USER] [-t {ALL,USER,COMPUTER}] [-l LOGLEVEL] [-s]
```

Опции команды gpupdate указаны в таблице 10.

Таблица 10 – Опции команды gpupdate

Ключ	Описание
-h, --help	Вывести справку о команде
-u USER, --user USER	Имя пользователя для обновления GPO
--target TARGET	Указать политики, которые нужно обновить (пользователя или компьютера). Возможные значения: All (по умолчанию), Computer, User
--loglevel LOGLEVEL	Установить уровень журналирования
-s, --system	Запустить gpupdate в системном режиме

Только root может указать любое имя пользователя для обновления. Пользователь может выполнять gpupdate только для машины или самого себя.

Примеры работы с командой gpupdate:

- получить и применить настройки для текущей машины:

```
$ gpupdate --target Computer
Apply group policies for computer.
```

- получить и применить настройки для текущего пользователя:

```
$ gpupdate --target User
Apply group policies for kudrin.
```

- получить и применить настройки для текущего пользователя и машины:

```
$ gpupdate
Apply group policies for kudrin.
```

- попытаться получить настройки для пользователя ivanov (с правами пользователя kudrin):

```
$ gpupdate -u ivanov --target User --loglevel 0
```

```
2022-03-15 08:38:50.676|[D00010]| Групповые политики будут обновлены для указанной цели|{'target': 'User'}
2022-03-15 08:38:50.677|[W00002]| Текущий уровень привилегий не позволяет выполнить gpupdate для указанного пользователя. Будут обновлены настройки текущего пользователя.|{'username': 'kudrin'}
2022-03-15 08:38:50.690|[D00013]| Запускается GPOA обращением к oddjobd через D-Bus|{}
2022-03-15 08:38:50.691|[D00006]| Запускается GPOA для пользователя обращением к oddjobd через D-Bus|{'username': 'kudrin'}
2022-03-15 08:39:12.282|[D00012]| Получен код возврата из утилиты|{'retcode': dbus.Int32(0)}
Apply group policies for kudrin.
```

- попытаться получить настройки для пользователя ivanov (с правами суперпользователя):

```
# gpupdate -u ivanov --target User --loglevel 0
```

```
2022-03-24 13:32:16.243|[D00010]| Групповые политики будут обновлены для указанной цели|{'target': 'User'}
2022-03-24 13:32:16.257|[D00013]| Запускается GPOA обращением к oddjobd через D-Bus|{}
2022-03-24 13:32:16.258|[D00006]| Запускается GPOA для пользователя обращением к oddjobd через D-Bus|{'username': 'ivanov'}
2022-03-24 13:32:24.615|[D00012]| Получен код возврата из утилиты|{'retcode': dbus.Int32(0)}
Apply group policies for ivanov.
```

Синтаксис команды gpupdate-setup:

gpupdate-setup [-h] действие

Опции команды gpupdate-setup указаны в таблице 11.

Таблица 11 – Опции команды gpupdate-setup

Ключ	Описание
list	Показать список доступных типов локальной политики
list-backends	Показать список доступных бэкэндов
status	Показать текущий статус групповой политики (действие по умолчанию)
enable	Включить подсистему групповой политики
disable	Отключить подсистему групповой политики
update	Обновить состояние. Проверяет в каком состоянии находилась служба gpupdate. В случае если служба gpupdate запущена, gpupdate-setup также запустит весь перечень служб (например, gpupdate-run-scripts)
write	Операции с групповыми политиками (включить, отключить, указать тип политики по умолчанию)
set-backend	Установить или изменить активную в данный момент серверную часть (бэкэнд)
default-policy	Показать название политики по умолчанию
active-policy	Показать название текущего профиля политики
active-backend	Показать текущий настроенный бэкэнд

Примеры работы с командой gpupdate-setup:

- просмотр текущего состояния подсистемы групповых политик:

```
# gpupdate-setup
disabled
```

- включение групповых политик (для включения через ЦУС доступен соответствующий графический модуль управления, а также отметка во время введения машины в домен см. п. 9.2.2):

```
# gpupdate-setup enable
workstation
```

```
Created symlink /etc/systemd/user/default.target.wants/gpupdate-user.service → /usr/lib/systemd/user/gpupdate-user.service.
Created symlink /etc/systemd/system/multi-user.target.wants/gpupdate-scripts-run.service → /lib/systemd/system/gpupdate-scripts-run.service.
Created symlink /etc/systemd/user/default.target.wants/gpupdate-scripts-run-user.service → /usr/lib/systemd/user/gpupdate-scripts-run-user.service.
Created symlink /etc/systemd/system/timers.target.wants/gpupdate.timer → /lib/systemd/system/gpupdate.timer.
Created symlink /etc/systemd/user/timers.target.wants/gpupdate-user.timer → /usr/lib/systemd/user/gpupdate-user.timer.
```

```
# control system-policy
gpupdate
```

- выключение групповых политик:

```
# gpupdate-setup disable
```

```
Removed /etc/systemd/system/multi-user.target.wants/gpupdate.service.
```

```
Removed /etc/systemd/user/default.target.wants/gpupdate-user.service.
Removed /etc/systemd/system/timers.target.wants/gpupdate.timer.
Removed /etc/systemd/user/timers.target.wants/gpupdate-user.timer.
Removed /etc/systemd/system/multi-user.target.wants/gpupdate-scripts-run.service.
Removed /etc/systemd/user/default.target.wants/gpupdate-scripts-run-user.service.
```

- вывод списка доступных бэкендов:

```
# gpupdate-setup list-backends
local
samba
```

- включение групповых политик и установка профиля политики по умолчанию server:

```
# gpupdate-setup write enable server
```

По умолчанию, нет необходисти конфигурирования `gpupdate`. Однако в файле `/etc/gpupdate/gpupdate.ini` можно указать в явном виде следующие опции:

1) раздел `[gpoa]`:
   - `backend` – способ получения настроек;
   - `local-policy` – профиль политики по умолчанию, который будет применен сразу после загрузки ОС (`ad-domain-controller`, `workstation`, `server`, `default`);
2) раздел `[samba]`: `dc` – mba]tionузки ОС (по умолчанию, который будет применен сразуолчаниюПример, файла `/etc/gpupdate/gpupdate.ini` на контроллере домена:

```
[gpoa]
backend = samba
local-policy = ad-domain-controller
```

Пример, файла `/etc/gpupdate/gpupdate.ini` на рабочей станции:

```
[gpoa]
backend = samba
local-policy = workstation
```

В следующем примере указан пустой профиль локальной политики. Указать пустой профиль бывает нужно для тестирования групповых политик, чтобы они не наслаивались на локальные политики:

```
[gpoa]
backend = samba
local-policy = /usr/share/local-policy/default
```

```
[samba]
dc = dc1.test.alt
```

9.2.3.2. Локальная политика

Настройки локальной политики находятся в каталоге `/usr/share/local-policy/`. Данные настройки по умолчанию поставляются пакетом local-policy. Администраторы инфраструктур имеют возможность поставлять собственный пакет с локальной политикой и разворачивать ее единообразно на всех клиентах.

Формат шаблонов политик, по умолчанию, представляет собой архивный формат политик Samba с дополнительными модификациями. Локальную политику рекомендуется править только опытным администраторам. Состав локальной политики может меняться или адаптироваться системным администратором (таблица 12).

Т а б л и ц а 12 – Состав локальной политики

Описание	Комментарий
Включение oddjobd.service	Нужно для обеспечения возможности запуска `gpupdate` для пользователя с правами администратора
Включение gpupdate.service	Нужно для регулярного обновления настроек машины
Включение sshd.service	Нужно для обеспечения возможности удаленного администрирования
Включение аутентификации с помощью GSSAPI для sshd	Нужно для аутентификации в домене при доступе через SSH
Ограничение аутентификации для sshd по группам wheel и remote	Нужно для ограничения доступа при доступе через SSH для всех пользователей домена (только при наличии соответствующей привилегии)
Открытие порта 22	Нужно для обеспечения возможности подключения по SSH на машинах при старте Firewall applier

Пример локальной политики (файл `/usr/share/local-policy/workstation/Machine/Registry.pol.xml`):

```
<?xml version="1.0" encoding="utf-8"?>
<PolFile num_entries="9" signature="PReg" version="1">
    <Entry type="1" type_name="REG_SZ">
        <Key>Software\BaseALT\Policies\Control</Key>
        <ValueName>sshd-gssapi-auth</ValueName>
        <Value>enabled</Value>
    </Entry>
    <Entry type="1" type_name="REG_SZ">
        <Key>Software\BaseALT\Policies\Control</Key>
        <ValueName>ssh-gssapi-auth</ValueName>
        <Value>enabled</Value>
    </Entry>
    <Entry type="1" type_name="REG_SZ">
        <Key>Software\BaseALT\Policies\Control</Key>
        <ValueName>sshd-allow-groups</ValueName>
        <Value>enabled</Value>
    </Entry>
    <Entry type="1" type_name="REG_SZ">
        <Key>Software\BaseALT\Policies\Control</Key>
        <ValueName>sshd-allow-groups-list</ValueName>
        <Value>remote</Value>
    </Entry>
    <Entry type="1" type_name="REG_SZ">
        <Key>Software\BaseALT\Policies\Control</Key>
        <ValueName>system-policy</ValueName>
        <Value>gpupdate</Value>
    </Entry>
    <Entry type="4" type_name="REG_DWORD">
        <Key>Software\BaseALT\Policies\SystemdUnits</Key>
        <ValueName>oddjobd.service</ValueName>
        <Value>1</Value>
    </Entry>
    <Entry type="4" type_name="REG_DWORD">
        <Key>Software\BaseALT\Policies\SystemdUnits</Key>
        <ValueName>sshd.service</ValueName>
        <Value>1</Value>
    </Entry>
    <Entry type="4" type_name="REG_DWORD">
        <Key>Software\BaseALT\Policies\SystemdUnits</Key>
        <ValueName>gpupdate.service</ValueName>
        <Value>1</Value>
    </Entry>
    <Entry type="1" type_name="REG_SZ">
        <Key>SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules</Key>
        <ValueName>OpenSSH</ValueName>

<Value>v2.20|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=22|Name=Open  SSH
port|Desc=Open SSH port|</Value>
    </Entry>
</PolFile>
```

9.2.3.3. Модули клиентской стороны (Applier)

На клиентский компьютер должны распространяться параметры политики, указанные в соответствующем объекте GPO.

Каждая группа параметров групповой политики обслуживается определенным модулем (Applier) клиентской стороны (таблица 13).

Т а б л и ц а 13 – Список модулей

Расширение клиентской стороны	Модуль	Описание
Управление control framework	control	Управляет фреймворком control. Может быть вызван только машинной политикой. Принцип работы – вызвать утилиту control с нужным параметром
Политики доступа к съемным носителям	polkit	Управляет генерацией настроек PolicyKit. Данный applier является машинным и способен реагировать на одно единственное свойство – запрет подключения всех внешних носителей информации. Работа с правилами PolicyKit ведется методом генерации файлов `.rules`
Включение или выключение различных служб	systemd	Управление включением или выключением сервисов systemd. Данный applier реализован только для машин. Его функция – включение или выключение systemd units (при их наличии). Applier способен обрабатывать параметры, полученные из PReg файлов (через ADMX) в виде ветвей реестра
Настройка веб-браузера Chromium	chromium	Генерирует файл политики для Chromium (`policies.json`). Данные настройки устанавливаются из ADMX-файлов для Chromium. Может быть вызван только машинной политикой.
Настройка веб-браузера Firefox	firefox	Генерирует файл политики для Firefox (`policies.json`). Данные настройки устанавливаются из ADMX-файлов для Firefox. Может быть вызван только машинной политикой.
Управление ярлыками запуска программ	shortcuts	Управляет `.desktop` файлами (создание/удаление/замена)
Управление ярлыками запуска программ	shortcuts_user	Управляет `.desktop` файлами в контексте пользователя. Способен реагировать на опцию выполнения операций в контексте администратора или пользователя
Управление подключением сетевых дисков	drives	Управляет подключением сетевых дисков
Управление подключением сетевых дисков	drives_user	Управляет подключением сетевых дисков в контексте пользователя

Окончание таблицы 13

Расширение клиентской стороны	Модуль	Описание
Управление каталогами файловой системы	folder	Управляет каталогами файловой системы (создание/удаление/пересоздание)
Управление каталогами файловой системы	folder_user	Управляет каталогами файловой системы в контексте пользователя
Управление файлами	files	Управляет файлами (создание/удаление/пересоздание)
Управление файлами	files_user	Управляет файлами в контексте пользователя
Управление INI-файлами	inifiles	Управляет INI-файлами (создание/удаление/пересоздание)
Управление INI-файлами	inifiles_user	Управляет INI-файлами в контексте пользователя
Управление переменными среды	environmentvariables	Управляет переменными среды
Управление переменными среды	environmentvariables_user	Управляет переменными среды в контексте пользователя
Управление общими каталогами	networkshares	Управляет общими каталогами
Управление общими каталогами	networkshares_user	Управляет общими каталогами в контексте пользователя
Управление gsettings (настройки графической среды MATE)	gsettings	Разворачивает системные настройки gsettings. Редактирование системных настроек осуществляется методом развертывания файлов с расширением `.gschema.override` (в формате INI) в директории с XML схемами. После разворачивания нужно осуществить вызов glib-compile-schemas для того, чтобы настройки вступили в силу
Управление gsettings (настройки графической среды MATE)	gsettings_user	Устанавливает настройки gsettings для пользователя
Управление пакетами	package	Средство работы с пакетным менеджером для установки и удаления пакетов программ

Модель групповых политик вызывает Applier отвечающие за внесение изменений, согласно параметрам политики. Для выполнения настроек, указанных в параметрах групповой политики, расширения клиентской стороны изменяют конкретные параметры операционной системы. Изменения, внесенные в операционную систему при помощи модуля групповых политик, записываются в журналы событий.

9.2.3.4. Периодичность запуска групповых политик

Каждый фронтенд срабатывает на определенные ветки настроек. Запуск фронтенда для машины по умолчанию производится раз в час средством Systemd – gpupdate.timer. Запуск фронтенда для пользователя в административном контексте производится с помощью модуля pam_oddjob при входе в систему и далее раз в час (по умолчанию) также средством Systemd – gpupdate-user.timer.

Для мониторинга и контроля времени выполнения службы `gpupdate.service` используются системный таймер `gpupdate.timer` и пользовательский таймер `gpupdate-user.timer`. Для управления периодом запуска групповых политик достаточно изменить параметр соответствующего таймера systemd (по умолчанию период запуска составляет 1 час).

Изменить периодичность запуска системного таймера можно, изменив значение параметра `OnUnitActiveSec` в файле `/lib/systemd/system/gpupdate.timer`:

```
[Unit]
Description=Run gpupdate every hour
[Timer]
OnStartupSec=1
OnUnitActiveSec=60min

[Install]
WantedBy=timers.target
```

По умолчанию таймер `gpupdate.timer` запустится после загрузки ОС, а затем будет запускаться каждый час во время работы системы. Просмотреть статус системного таймера можно, выполнив команду:

```
# systemctl status gpupdate.timer
● gpupdate.timer - Run gpupdate every hour
```

```
Loaded: loaded (/lib/systemd/system/gpupdate.timer; enabled; vendor preset: disabled)
Active: active (waiting) since Fri 2022-12-09 09:31:41 EET; 3h 31min ago
Trigger: Fri 2022-12-09 13:15:05 EET; 12min left
Triggers: ● gpupdate.service

дек 09 09:31:41 edu.test.alt systemd[1]: Started Run gpupdate every hour.
```

Изменить периодичность запуска пользовательского таймера можно, изменив в файле `/usr/lib/systemd/user/gpupdate-user.timer` значение параметра `OnUnitActiveSec`:

```
[Unit]
Description=Run gpupdate-user every hour

[Timer]
OnStartupSec=1
OnUnitActiveSec=60min

[Install]
WantedBy=timers.target
```

По умолчанию таймер gpupdate-user.timer запустится после входа пользователя в систему, а затем будет запускаться каждый час, пока активен сеанс соответствующего пользователя. Просмотреть статус пользовательского таймера можно, выполнив команду от имени пользователя:

```
$ systemctl --user status gpupdate-user.timer
```

```
● gpupdate-user.timer - Run gpupdate-user every hour
Loaded: loaded (/usr/lib/systemd/user/gpupdate-user.timer; enabled; vendor preset: enabled)
Active: active (waiting) since Fri 2022-12-09 12:49:21 EET; 2min 54s ago
Trigger: Fri 2022-12-09 13:49:28 EET; 57min left
Triggers: ● gpupdate-user.service

дек 09 12:49:21 edu.test.alt systemd[47372]: Started Run gpupdate-user every hour.
```

Чтобы изменения, внесенные в файл `/usr/lib/systemd/user/gpupdate-user.timer`, вступили в силу следует выполнить команду:

```
$ systemctl --user daemon-reload
```

Примечание. Управлять периодичностью запуска gpupdate можно также через групповые политики (см. п. 9.2.5.5.10).

Просмотреть список запущенных системных таймеров можно, выполнив команду:

```
$ systemctl list-timers
```

Просмотреть список запущенных пользовательских таймеров можно, выполнив команду:

```
$ systemctl --user list-timers
```

9.2.4. Модуль удаленного управления базой данных конфигурации (ADMC)

Компонент удаленного управления базой данных конфигурации (далее – ADMC) предназначен для управления:

- объектами в домене (пользователями, группами, компьютерами, подразделениями);
- групповыми политиками.

ADMC позволяет:

- создавать и администрировать учетные записи пользователей, компьютеров и групп;
- менять пароли пользователя;
- создавать организационные подразделения, для структурирования и выстраивания иерархической системы распределения учетных записей в AD;
- просматривать и редактировать атрибуты объектов;
- создавать и просматривать объекты групповых политик;
- выполнять поиск объектов по разным критериям;
- сохранять поисковые запросы;
- переносить поисковые запросы между компьютерами (выполнять экспорт и импорт поисковых запросов).

В «ADMC» реализована функция поиска объектов групповых политик.

9.2.4.1. Запуск ADMC

Запуск ADMC осуществляется из меню запуска приложений: пункт «Системные» → «ADMC» или из командной строки (команда `admc`).

П р и м е ч а н и е . Для использования ADMC нужно предварительно получить ключ Kerberos для администратора домена. Получить ключ Kerberos можно, например, выполнив следующую команду:

```
$ kinit administrator
```

9.2.4.2. Интерфейс ADMC

Интерфейс ADMC приведен на рис. 143.

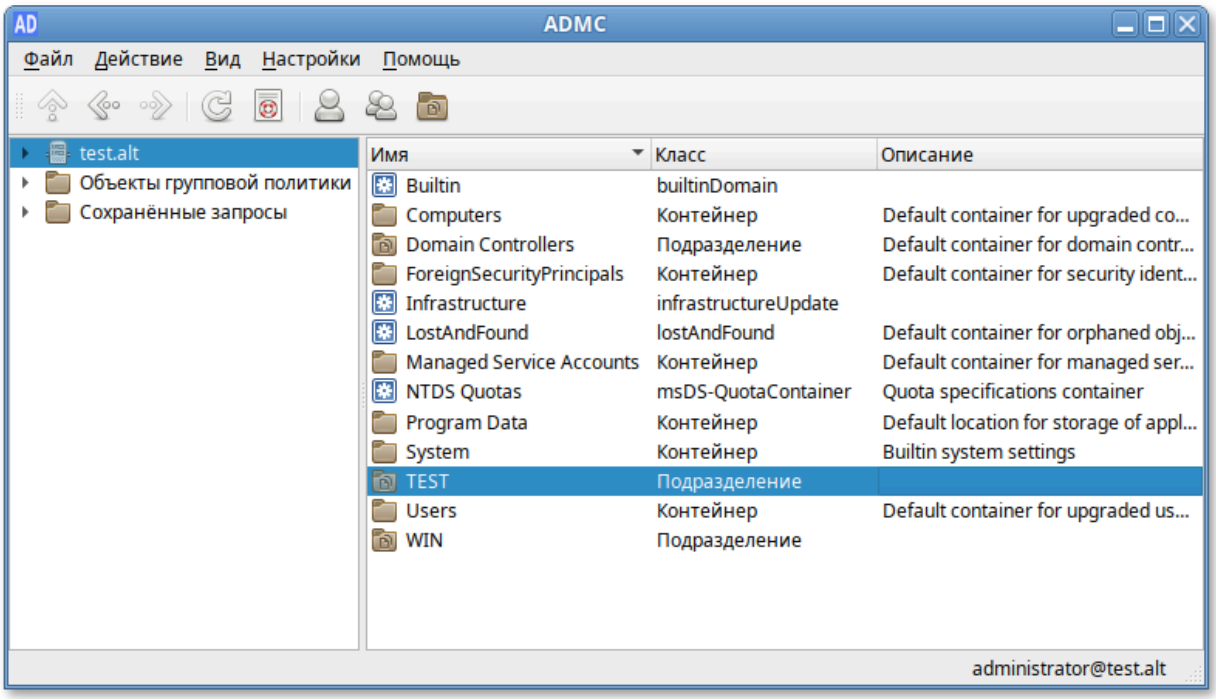


Рис. 143 – Интерфейс ADMC

Включить/выключить отображение панелей можно, отметив соответствующий пункт в меню «Вид» (рис. 144).

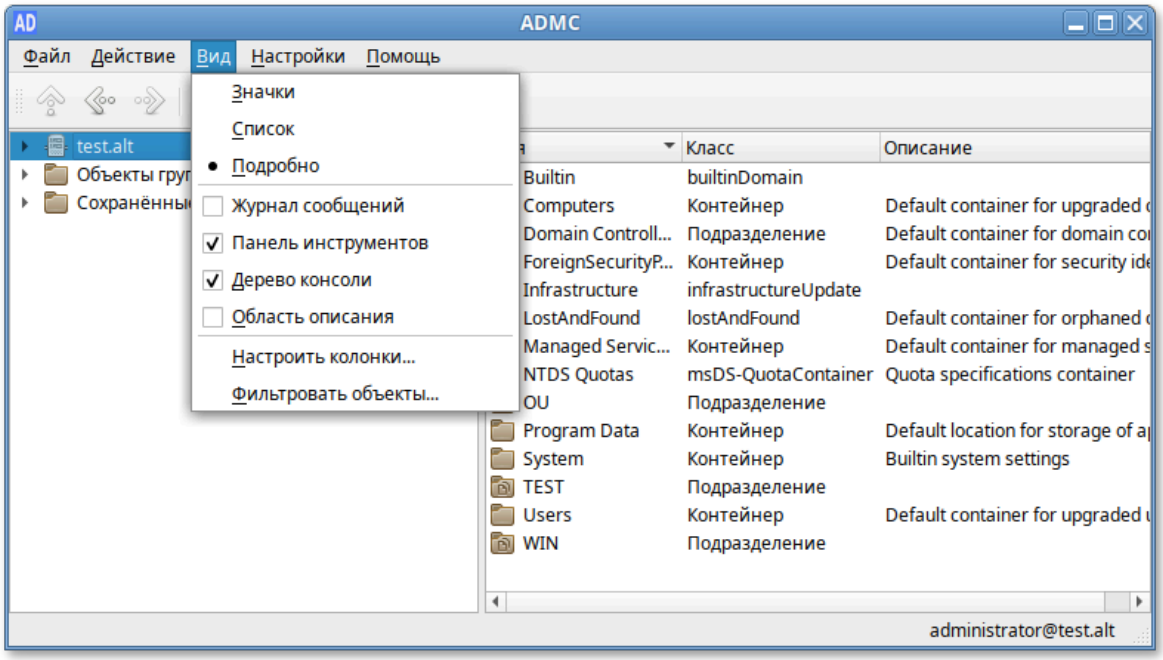


Рис. 144 – Включение/выключение отображения панелей

«Журнал сообщений» – показать/скрыть панель журнала. В панели журнала отображается сообщения о статусе приложения. Эти сообщения содержат отчеты обо всех выполненных действиях над объектами (рис. 145).

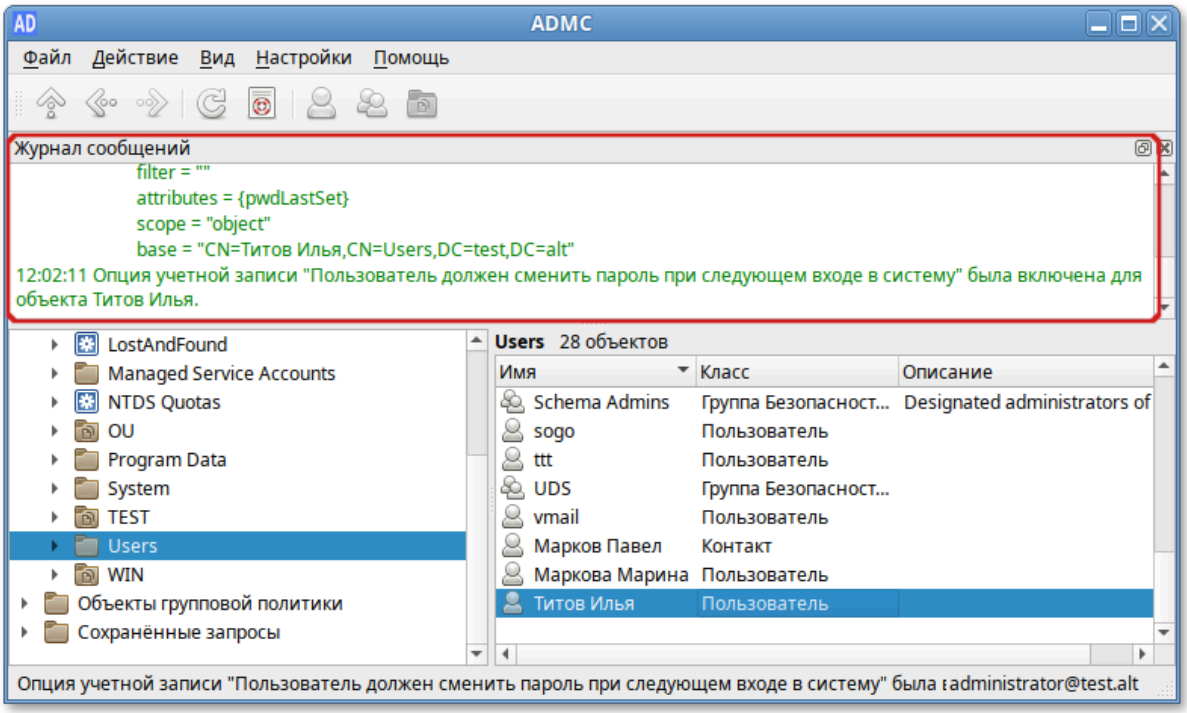


Рис. 145 – Панель «Журнал сообщений»

«Панель инструментов» – показать/скрыть панель инструментов (рис. 146).

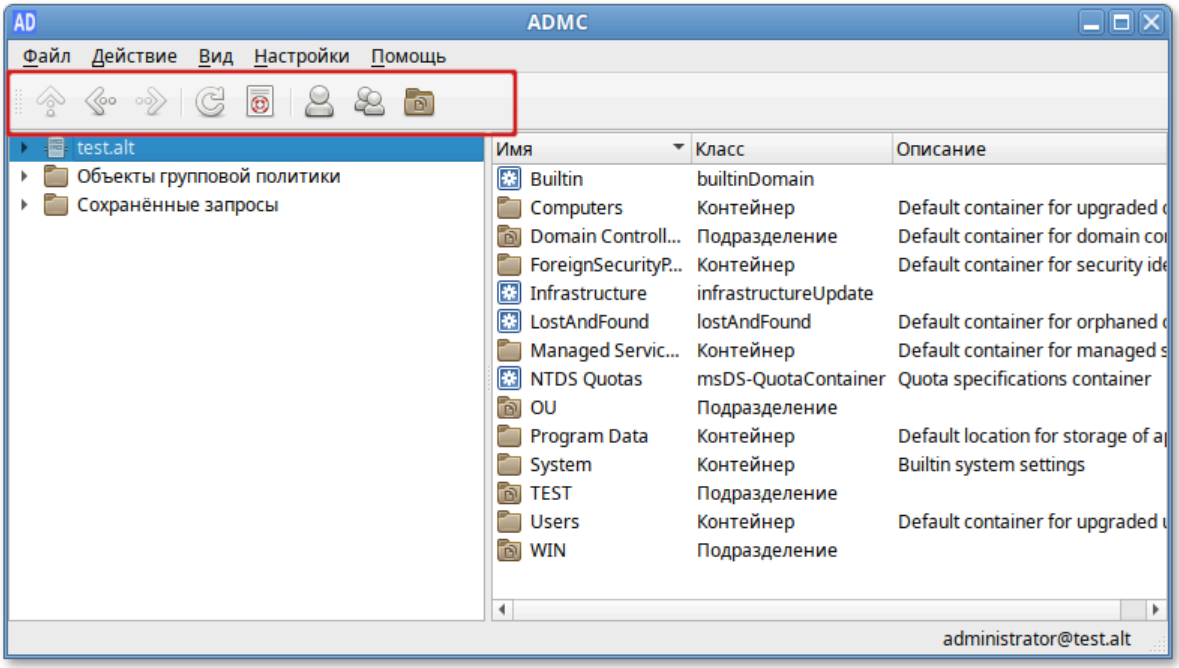


Рис. 146 – «Панель инструментов»

«Дерево консоли» – показать/скрыть панель дерева объектов Active Directory. Панель дерева объектов Active Directory отображается слева, в правой панели будут отображаться сведения о выбранном объекте. По умолчанию дерево показывает объекты типа «контейнер» (рис. 147).

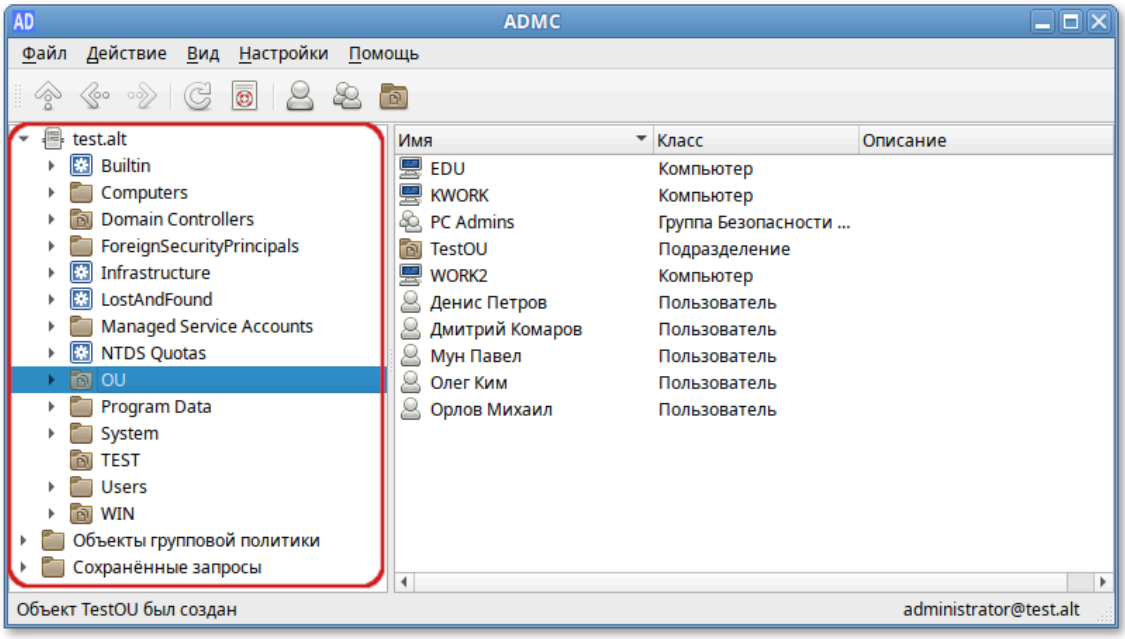


Рис. 147 – Панель «Дерево консоли»

«Область описания» – выводить описание контейнера. В области описания отображается название контейнера и количество объектов в контейнере (рис. 148).

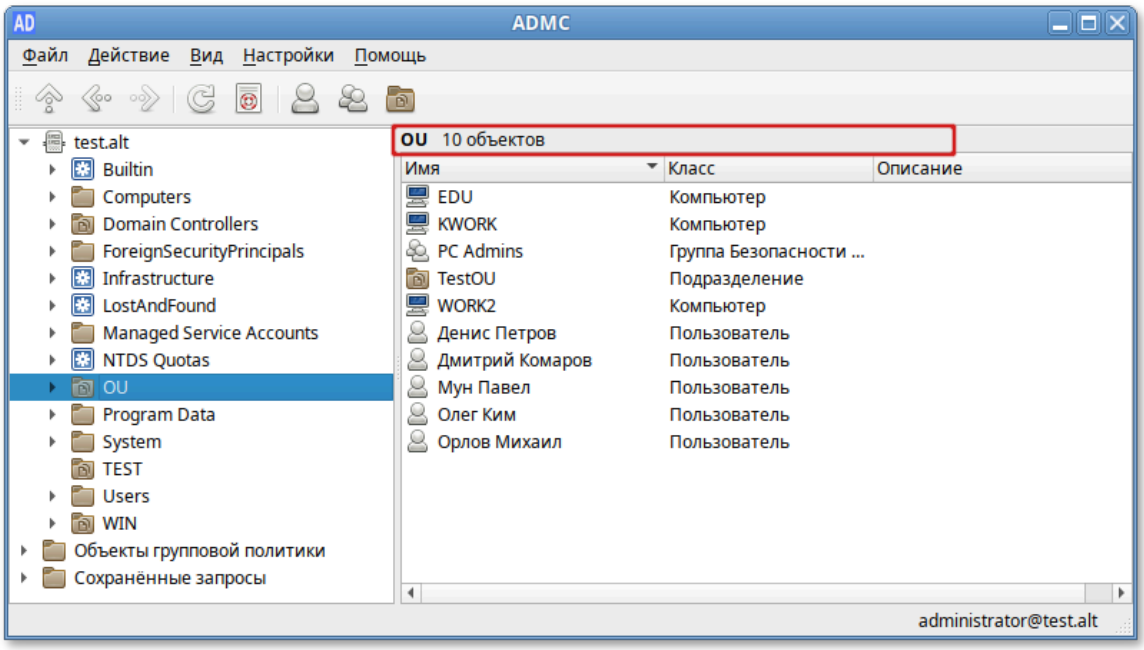


Рис. 148 – Панель «Область описания»

В меню «Настройки» можно изменить параметры ADMC (рис. 149).

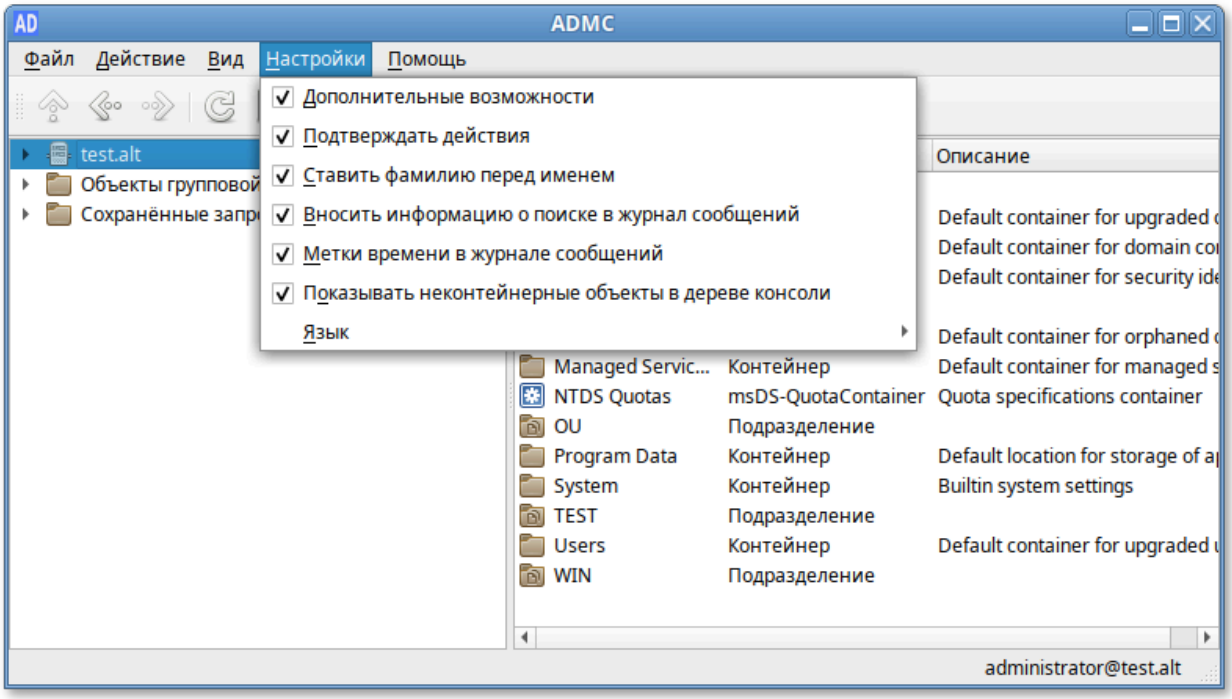


Рис. 149 – Меню «Настройки»

«Дополнительные возможности» – показывать расширенные объекты и элементы приложения.

«Подтверждать действия» – выводить окно «Подтвердить действие» при выполнении потенциально опасных действий, например, удалении объекта (рис. 150).

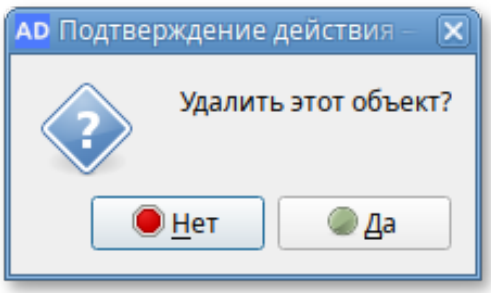


Рис. 150 – Окно «Подтвердить действие»

Параметры программы:

- «Ставить фамилию перед именем» – изменить формат полного имени (поле «cn») по умолчанию на «Фамилия Имя»;

- «Вносить информацию о поиске в журнал сообщений» – вносить в журнал поисковые запросы;
- «Метки времени в журнале сообщений» – показывать в журнале время события;
- «Показывать неконтейнерные объекты в дереве консоли» – показывать неконтейнерные объекты (например, учетные записи пользователей и компьютерные учетные записи) в панели дерева объектов Active Directory;
- «Язык» – выбрать язык интерфейса (русский или английский).

Выбранные параметры сохраняются и восстанавливаются при каждом запуске программы.

Меню операций с объектом открывается из строки меню, пункт «Действие» после выбора объекта (рис. 151) или в контекстном меню объекта (рис. 152).

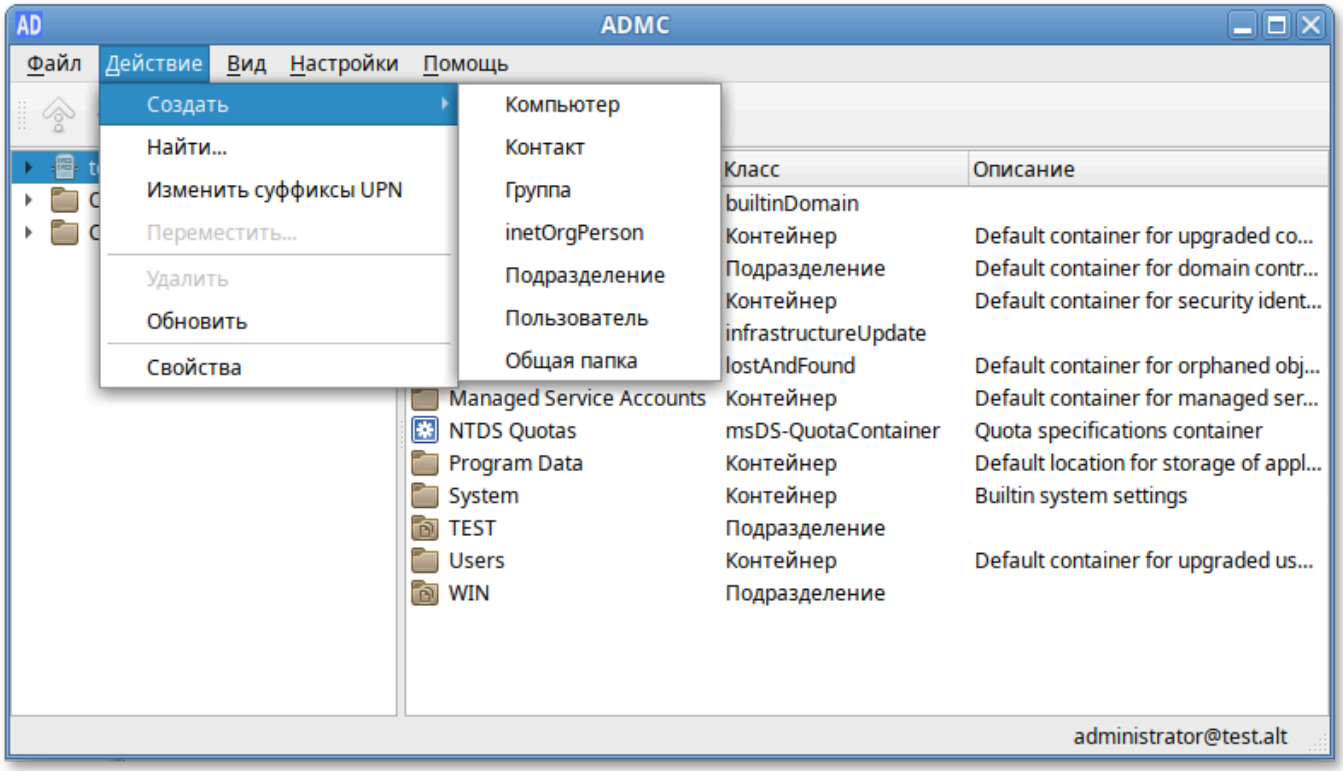


Рис. 151 – Пункт «Действие»

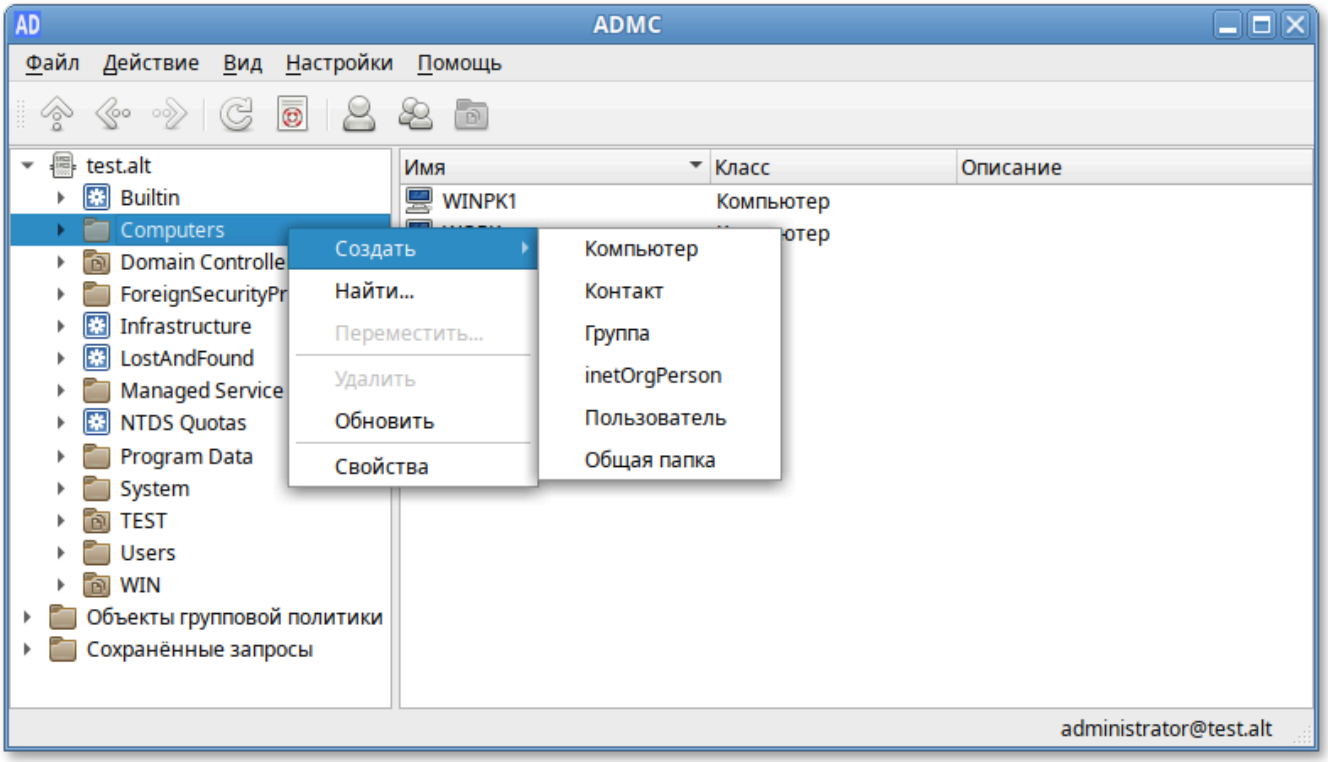


Рис. 152 – Контекстное меню объекта

Меню операций содержит действия применимые к выделенному объекту.

9.2.4.3. Свойства объектов

Существует два режима работы ADMC: обычный и расширенный режим.

При включении расширенного режима («Настройки» → «Дополнительные возможности») в свойствах всех объектов появляются дополнительно две вкладки: «Атрибуты» и «Объект». Для объекта пользователь также появляется вкладка «Безопасность».

Окно «Учетная запись пользователя» – «Свойства» в расширенном режиме (рис. 153).

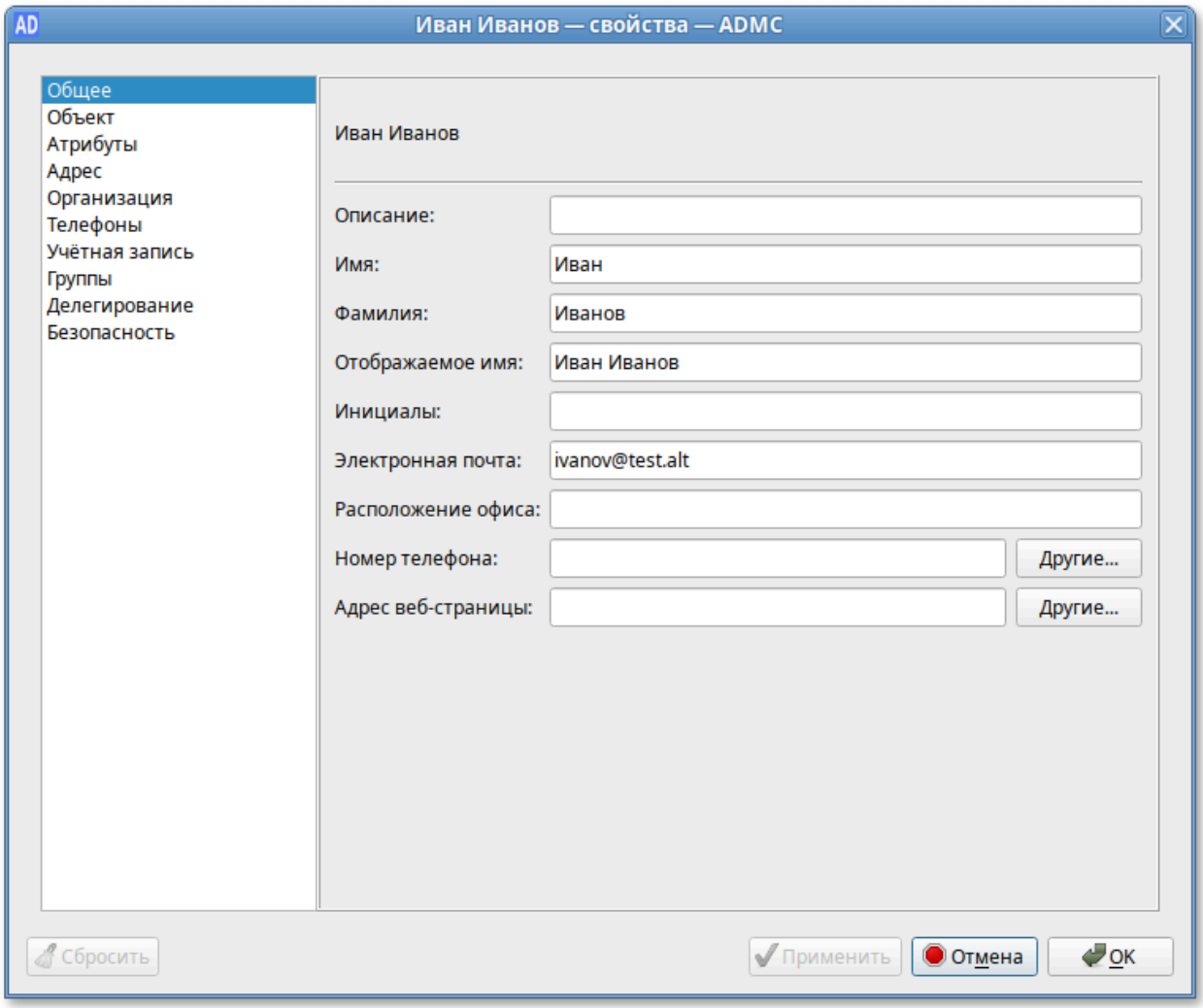


Рис. 153 – Окно «Учетная запись пользователя» – «Свойства»

По умолчанию отображается вкладка «Общее» (таблица 14).

Т а б л и ц а 14 – Назначение вкладок окна «Свойства учетной записи пользователя»

Вкладка	Описание	Расширенный режим
Общее	Основная вкладка, содержащая информацию, идентифицирующую личность пользователя, которой соответствует данная учетная запись	-
Учетная запись	Характеристики учетной записи пользователя, настройка правил регистрации в сети	-
Адрес	Почтовый адрес пользователя	-
Организация	Данные о сотруднике согласно штатному расписанию	-
Телефоны	Настройка телефонии	-
Группы	Управление членством в группах безопасности	-
Атрибуты	Список атрибутов объекта	+
Объект	Информация об объекте	+
Делегирование		-
Безопасность	Права доступа к объекту	+

Во вкладке «Общее» задаются личные данные сотрудника и его контактная информация: телефоны, размещение, адрес электронной почты и др. Вкладка «Общее» отображается по умолчанию при вызове свойств учетной записи любого объекта AD. В качестве значений параметров указаны названия соответствующих им полей в AD (таблица 15).

Т а б л и ц а 15 – Соответствие параметров на вкладке «Общее» полям в AD

Поле на вкладке «Общее»	Примечание	Поле в Active Directory	Тип
Полное имя	Во вкладке «Общее» значение этого поля изменить нельзя	`cn, name`	Юникод
Описание		`description`	Юникод
Имя		`givenName`	Юникод
Фамилия		`sn`	Юникод
Отображаемое имя	Значение этого параметра складывается из суммы значений трех параметров: First Name, Initials и Last Name	`diplayName`	Юникод
Инициалы	Длина не более 6 символов	`initials`	Юникод
Электронная почта	Автоматически заполняемое поле в соответствии с форматом UPN (RFC 822) при создании почтового ящика для учетной записи пользователя. По умолчанию поле пустое	`mail`	Юникод
Расположение офиса	Указывается физическое месторасположение пользователя: комната, офис и т.д.	`physicalDeliveryOfficeName`	Юникод
Номер телефона		`telephoneNumber`	Юникод
Другие телефоны	Можно задать, нажав кнопку «Другие…»	`otherTelephone`	Юникод
Адрес веб-страницы		`wWWHomePage`	Юникод
Другие адреса веб-страниц	Можно задать, нажав кнопку «Другие…»	`url`	Юникод

Во вкладке «Учетная запись» сосредоточены настройки, характеризующие правила доступа пользователя к сети, включая имя входа в сеть (рис. 154).

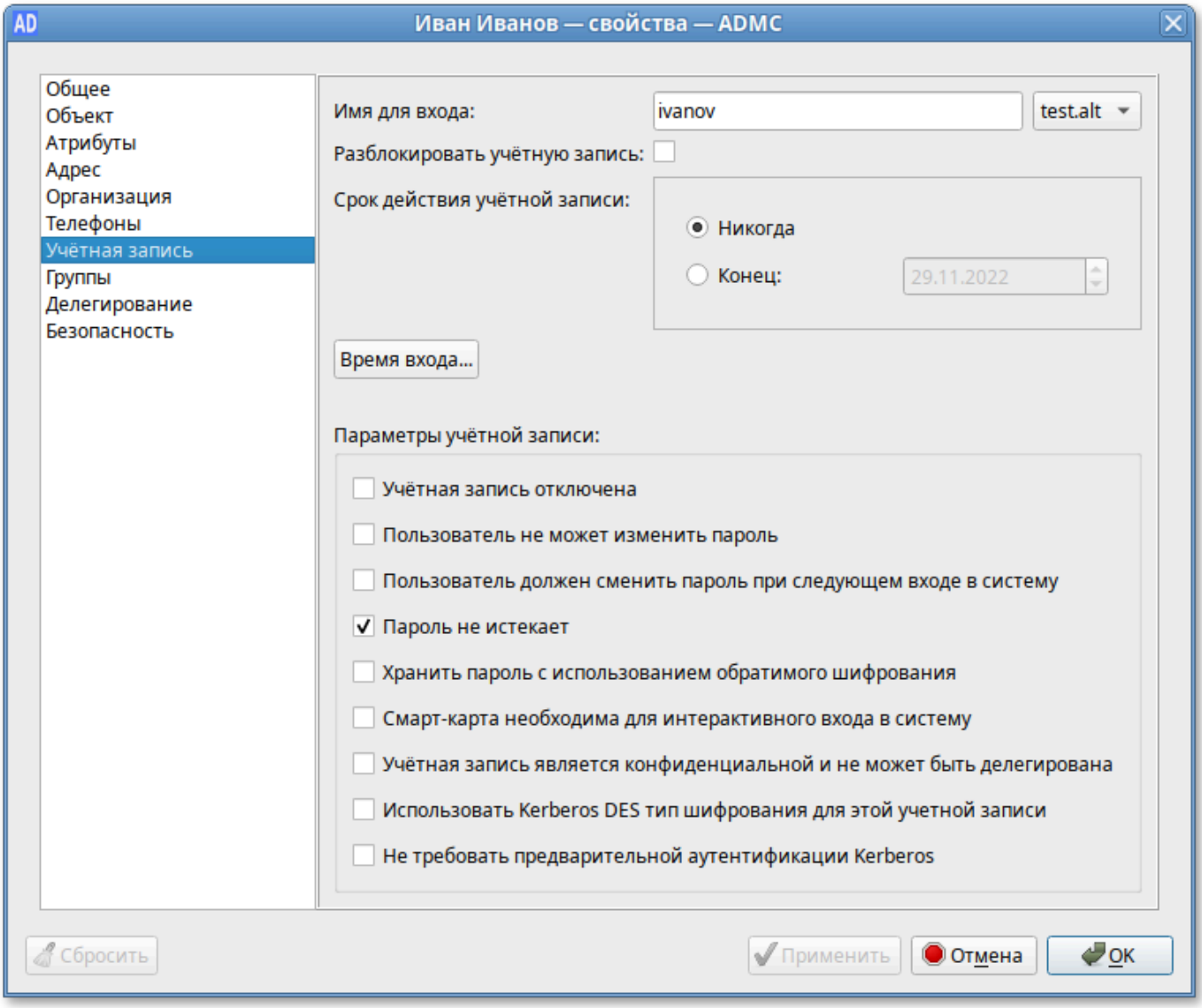


Рис. 154 – Вкладка «Учетная запись»

Соответствие параметров на вкладке «Учетная запись» полям в AD приведено в таблице 16.

Т а б л и ц а 16 – Соответствие параметров на вкладке «Учетная запись» полям в AD

Поле на вкладке «Учетная запись»	Примечание	Поле в Active Directory	Тип
Имя для входа	Имя пользователя для входа (логин пользователя)	`userPrincipalName`	Юникод
Разблокировать учетную запись	Позволяет разблокировать учетную запись пользователя, если она была заблокирована, например, из-за слишком большого количества неудачных попыток входа	`userAccountControl = 16`	Целое число
Срок действия учетной записи	Дата отключения учетной записи (по умолчанию «Никогда» – неограниченный срок действия). Если нужно задать дату окончания срока действия учетной записи пользователя, следует выбрать «Конец» и затем выбрать дату	`accountExpires`	Большое целое число
Время входа…	Часы, в которые пользователю разрешено выполнять вход в домен	`logonHours`	Октет
Учетная запись отключена (ACCOUNTDISABLE)	Если эта опция включена, пользователь не сможет войти в систему	`userAccountControl = 0x0002 (2)`	Целое число
Пользователь не может изменить пароль (PASSWD_CANT_CHANGE)		`userAccountControl = 0x0040 (64)`	Целое число
Пользователь должен сменить пароль при следующем входе в систему		`pwdLastSet`	Большое целое число
Пароль не истекает (DONT_EXPIRE_PASSWORD)	Срок действия пароля для этой учетной записи никогда не истечет	`userAccountControl = 0x10000 (65536)`	Целое число
Хранить пароль с использованием обратимого шифрования (ENCRYPTED_TEXT_PWD_ALLOWED)	Для шифрования ключей использовать DES-шифрование. Эта политика обеспечивает поддержку приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности	`userAccountControl = 0x0080 (128)`	Целое число

Окончание таблицы 16

Поле на вкладке «Учетная запись»	Примечание	Поле в Active Directory	Тип
Смарт-карта нужна для интерактивного входа в систему (SMARTCARD_REQUIRED)	Пользователь должен войти в систему с помощью смарт-карты	`userAccountControl = 0x40000 (262144)`	Целое число
Учетная запись является конфиденциальной и не может быть делегирована (NOT_DELEGATED)	Пользователю нельзя доверять делегирование полномочий	`userAccountControl = 0x100000 (1048576)`	Целое число
Использовать Kerberos DES тип шифрования для этой учетной записи (USE_DES_KEY_ONLY)	Ограничить этот субъект использованием только типов шифрования DES (стандарт шифрования данных) для ключей	`userAccountControl = 0x200000 (2097152)`	Целое число
Не требовать предварительной аутентификации Kerberos (DONT_REQ_PREAUTH)	Для доступа к ресурсам сети не нужно предварительно проверять подлинность с помощью протокола Kerberos	`userAccountControl = 0x400000 (4194304)`	Целое число

Примечание. userAccountControl – атрибут управления учетной записью пользователя. Значение атрибута userAccountControl, образуется путем суммирования всех установленных значений. В таблице приведены только те значения, которые можно изменить явным образом на вкладках «Учетная запись» и «Делегирование».

Значения UserAccountControl по умолчанию для определенных объектов:

- обычный пользователь (NORMAL_ACCOUNT): 0x200 (512);
- контроллер домена (SERVER_TRUST_ACCOUNT): 0x2000 (8192);
- рабочая станция или сервер (WORKSTATION_TRUST_ACCOUNT): 0x1000 (4096).

На вкладке «Группы» формируется список групп, членом которых является текущий пользователь. Здесь также можно назначить основную группу (Primary Group). Для управления членством пользователя в группах безопасности AD используются две кнопки, находящиеся под списком групп, членами которой является пользователь: «Добавить» и «Удалить». По умолчанию пользователь входит в группу Domain Users (рис. 155).

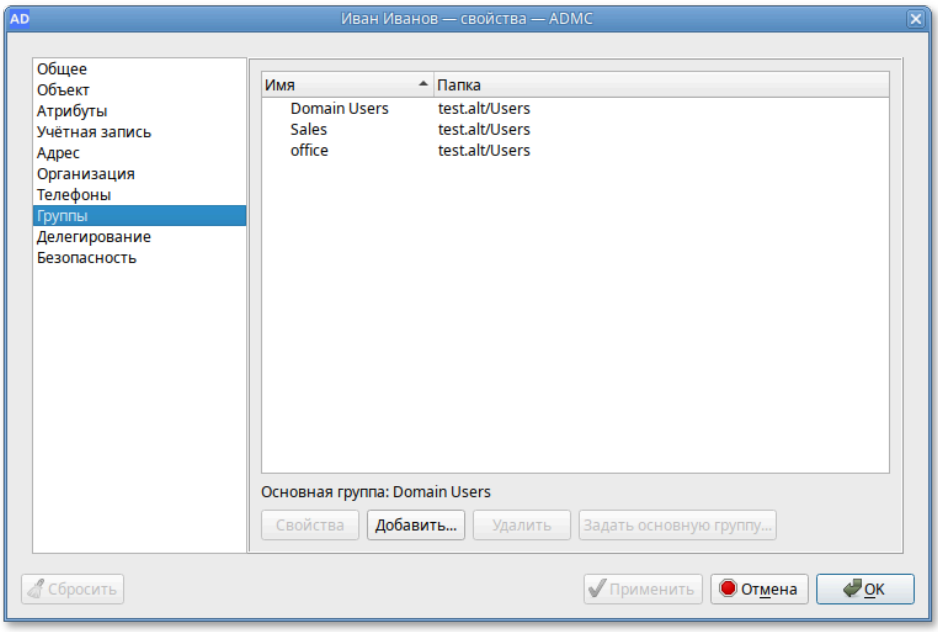


Рис. 155 – Вкладка «Группы»

На вкладке «Делегирование» доступно два параметра (рис. 156):

- «Не доверять делегирование» – запрещение делегирования услуг;
- «Доверять делегирование любых служб с использованием Kerberos» – задает возможность делегирования услуг только с помощью протокола Kerberos.

Примечание. Протокол проверки подлинности Kerberos – это основной протокол безопасности для проверки подлинности в домене. Он проверяет подлинность пользователя и системы.

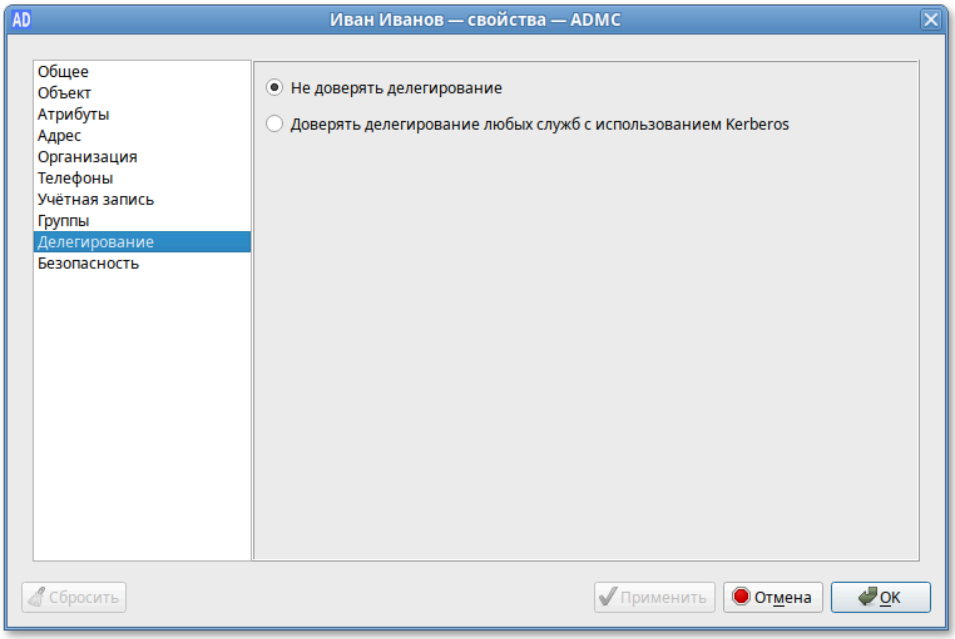


Рис. 156 – Вкладка «Делегирование»

Каждому объекту в сети назначается набор данных об управлении доступом. Этот набор данных определяет, какой тип доступа разрешается пользователям и группам. Управление разрешениями для выбранного объекта доступно на вкладке «Безопасность» (рис. 157).

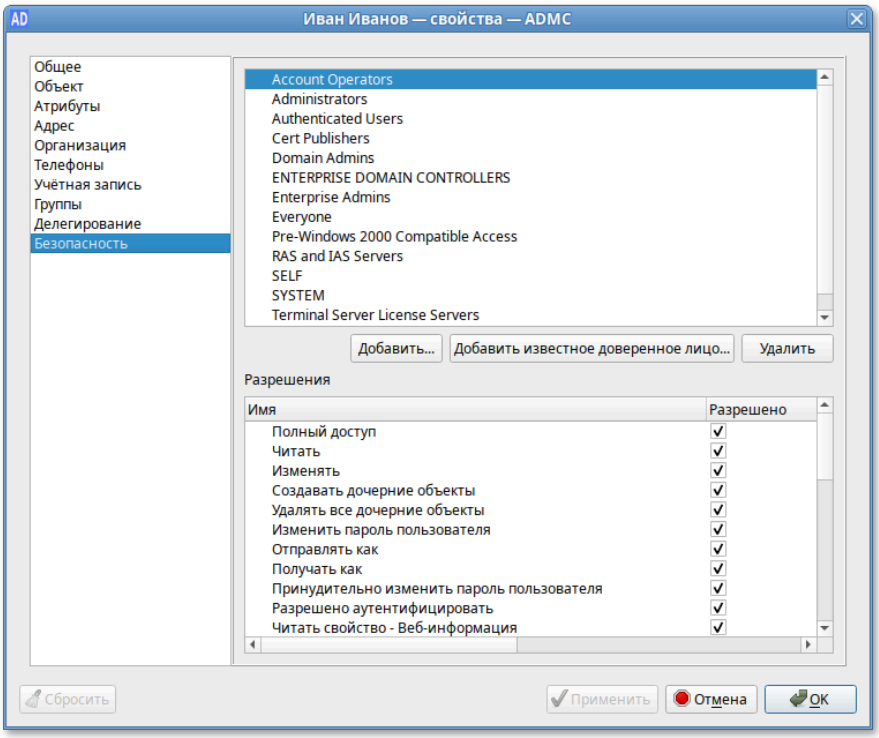


Рис. 157 – Вкладка «Безопасность»

В поле «Разрешения» отображается список действующих разрешений и запретов для каждой выбранной группы. Чтобы установить разрешения для группы, которая отсутствует в списке можно воспользоваться кнопкой «Добавить…» или «Добавить известное доверенное лицо…».

Для тонкого редактирования свойств объектов AD (пользователей, компьютеров, групп) можно воспользоваться вкладкой «Атрибуты» (рис. 158).

Эту вкладку можно использовать для просмотра и редактирования атрибутов, недоступных через другие вкладки окна «Свойства объекта» (например, для просмотра значений неизменяемых атрибутов).

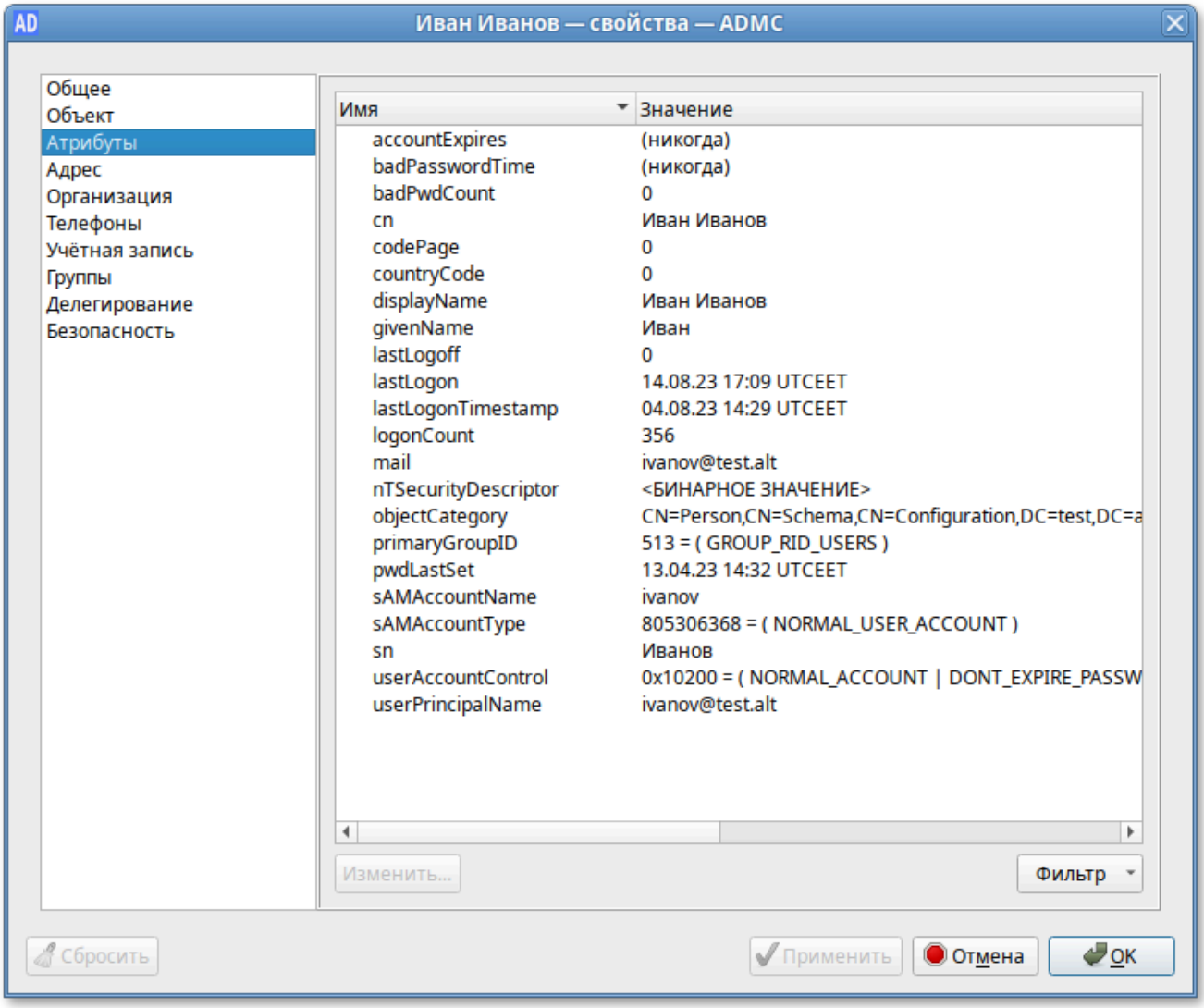


Рис. 158 – Вкладка «Атрибуты»

Содержимое окна редактирования атрибута зависит от типа атрибута. Окно редактирования атрибута целого типа (рис. 159).

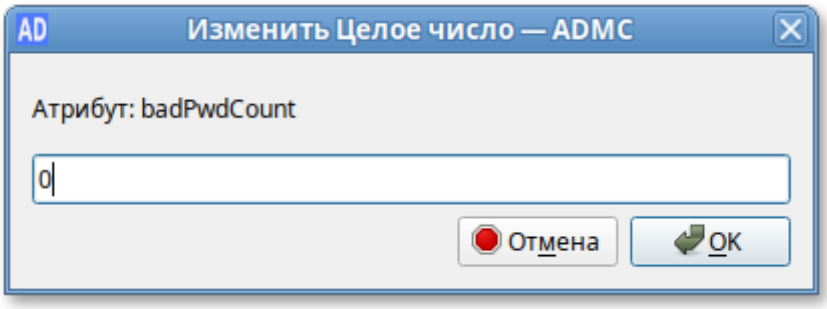


Рис. 159 – Окно редактирования атрибута целого типа

Окно редактирования атрибута логического типа (рис. 160).

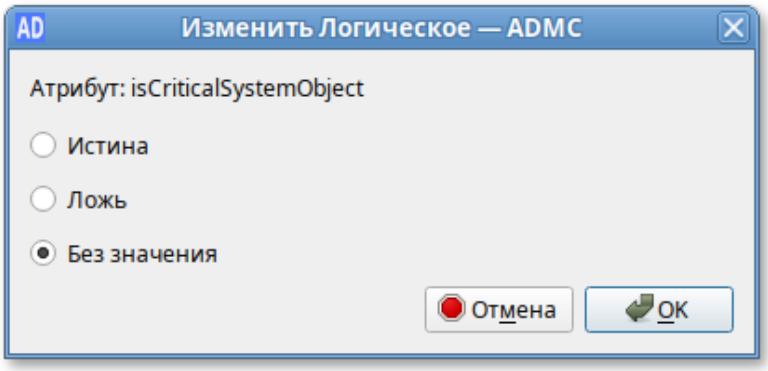


Рис. 160 – Окно редактирования атрибута логического типа

Для большинства атрибутов AD имеется встроенная функция декодирования значений. Например, значение атрибута `lastLogon` или `lastLogonTimestamp` (информация о времени последнего входа пользователя в домен) во вкладке «Атрибуты» и в окне редактирования атрибута отображается в формате «Дата Время», хотя время хранится в виде большого целого числа, представляющего число 100-наносекундных интервалов с 1 января 1601 (UTC) (рис. 161).

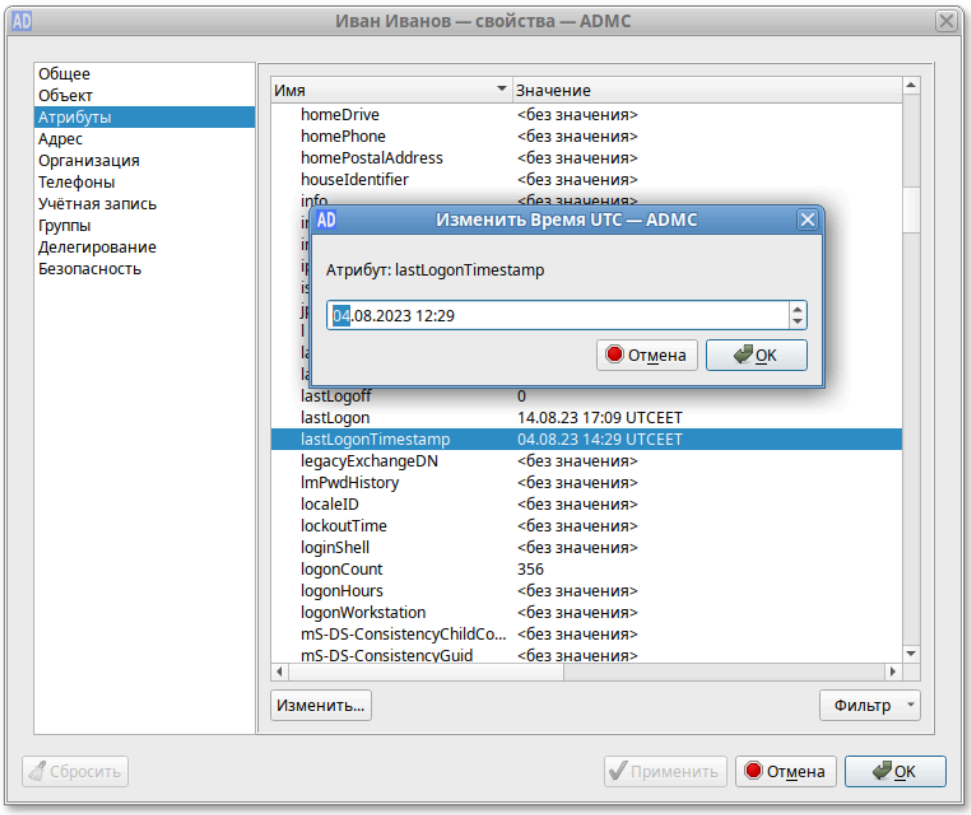


Рис. 161 – Вкладка «Атрибуты»

Кнопка «Фильтр» позволяет управлять отображением списка атрибутов (рис. 162):

- «Без значения» – показывать пустые атрибуты;
- «Только для чтения» – показывать все атрибуты, в том числе на правку которых нет полномочий. Если снять отметку с этого пункта, будут показаны только те атрибуты, на правку которых делегированы полномочия (например, если у пользователя нет полномочий на изменение атрибутов данного объекта, список атрибутов будет пуст);
- «Обязательные» – показывать обязательные атрибуты;
- «Необязательные» – показывать необязательные (дополнительные) атрибуты;
- «Системные» – показывать системные атрибуты, которые может изменять только сервер AD (например, objectClass);
- «Сконструированные» – показывать атрибуты, которые не хранятся в каталоге, но вычисляются контроллером домена (например, canonicalName);
- «Обратные ссылки» – показывать связанные атрибуты (например, memberOf).

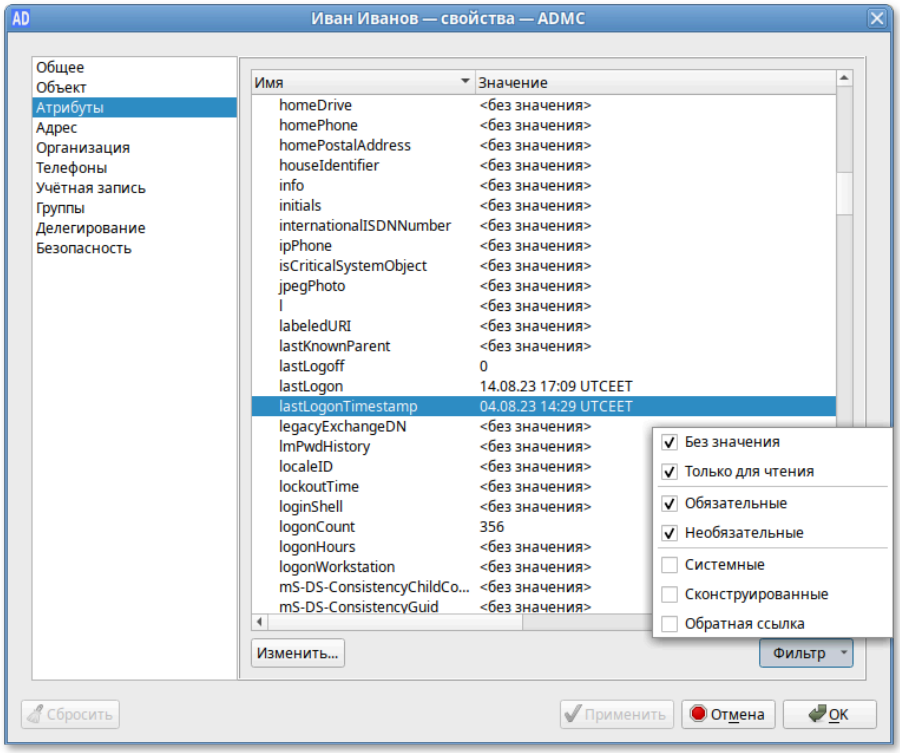


Рис. 162 – Кнопка «Фильтр»

9.2.4.4. Выбор контейнера

При перемещении объекта в новый контейнер (пункт «Переместить…» в контекстном меню объекта) открывается окно, в котором можно выбрать контейнер, в который следует переместить объект (рис. 163).

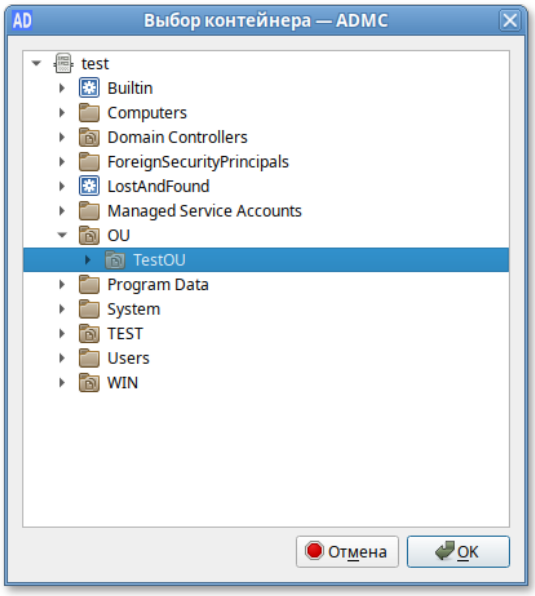


Рис. 163 – Выбор контейнера, в который следует переместить объект

9.2.4.5. Управление пользователями

Учетная запись пользователя AD:

- удостоверяет личность пользователя;

- разрешает или запрещает доступ к ресурсам домена.

В ADMC предусмотрена возможность создания новых учетных записей пользователей в доменных службах AD и управления существующими учетными записями пользователей.

Примечание. Для доступа к некоторым операциям нужно быть членом одной из этих групп: Account Operators, Domain Admins, Enterprise Admins.

Примечание. Объект InetOrgPerson является производным от класса пользователь (user). Он может работать в качестве субъекта безопасности так же, как и объект класса пользователь. Для создания учетной записи InetOrgPerson в контекстном меню контейнера следует выбрать пункт «Создать» → «inetOrgPerson».

9.2.4.5.1. Создание учетной записи пользователя

Для создания учетной записи пользователя в контекстном меню контейнера следует выбрать пункт «Создать» → «Пользователь». Окно мастера создания учетной записи пользователя (рис. 164).

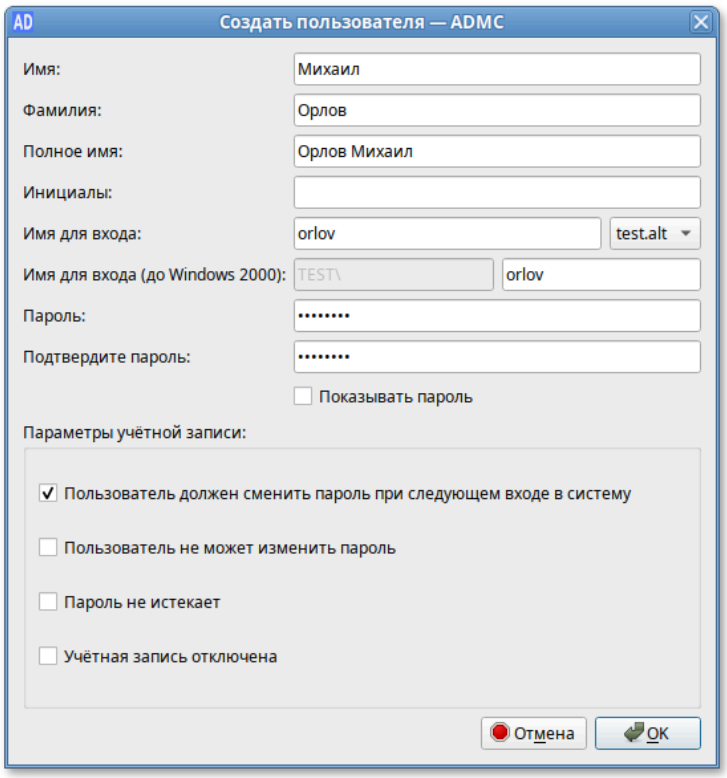


Рис. 164 – Окно мастера создания учетной записи пользователя

При создании учетной записи пользователя можно указать следующие параметры (атрибуты):

- «Имя» – имя пользователя;
- «Фамилия» – фамилия пользователя;
- «Полное имя» – полное имя пользователя (в это поле можно добавить отчество или поменять имя и фамилию местами);
- «Инициалы» – инициалы пользователя;
- «Имя для входа» – имя пользователя для входа (логин пользователя). В раскрывающемся списке перечисляются доступные суффиксы основного имени пользователя (UPN), которые можно использовать для создания имени пользователя для входа (рис. 165).

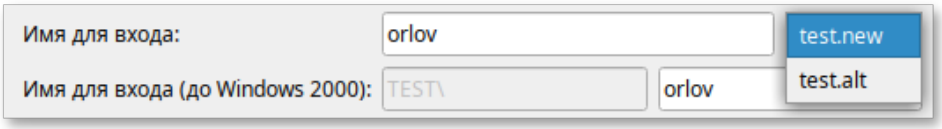


Рис. 165 – Ввод имени для входа

Список содержит полное имя системы доменных имен (DNS) текущего домена и все альтернативные суффиксы UPN:

- «Имя для входа (до Windows 2000)» – имя пользователя для входа в старые системы (пред-Windows 2000);
- «Пароль/Подтвердите пароль» – пароль пользователя;
- «Пользователь должен сменить пароль при следующем входе в систему» – пользователь должен изменить пароль при следующем входе в систему. Если эта опция включена, только пользователь будет знать свой пароль;
- «Пользователь не может изменить пароль» – предотвращает изменение пароля пользователем;
- «Пароль не истекает» – установить бессрочный пароль. Если эта опция включена, срок действия учетной записи пользователя не ограничен (по умолчанию срок действия пароля задан атрибутом `minPwdAge`);
- «Учетная запись отключена» – отключить учетную запись пользователя. Если эта опция включена, пользователь не сможет войти в систему.

Примечание. Для совместимости с доменами пред-Windows 2000 (Windows NT) в AD задается два имени пользователя, значения которых имеют разный формат. Первое имя, используемое в доменах Window 2k, – UPN-имя, которому в AD соответствует поле `userPrincipalName`, имеющее формат `user@domain`, где:

- domain – DNS-имя домена, например, TEST.ALT;
- user – имя пользователя в сети.

Для удобства назначения имен UPN-имя разделено на две части (префикс UPN и суффикс UPN). Второе задаваемое имя пользователя – SAM-имя, которое используется для совместимости в доменах Windows NT. Структура SAM-имени следующая: `domain\user`, где:

- domain – сокращенное имя домена, например, TEST;
- user – имя пользователя.

В AD хранится только имя пользователя в поле `samAccountName`. Первая часть SAM-имени однозначно вычисляется из DNS-имени домена.

По умолчанию суффиксом основного имени (UPN) для учетной записи пользователя является DNS имя домена AD, которое содержит учетную запись пользователя. Для упрощения процессов администрирования и входа пользователя в систему можно добавить альтернативные суффиксы UPN.

9.2.4.5.2. Изменение учетной записи пользователя

Для изменения учетной записи пользователя следует в контекстном меню пользователя выбрать соответствующее действие (рис. 166).

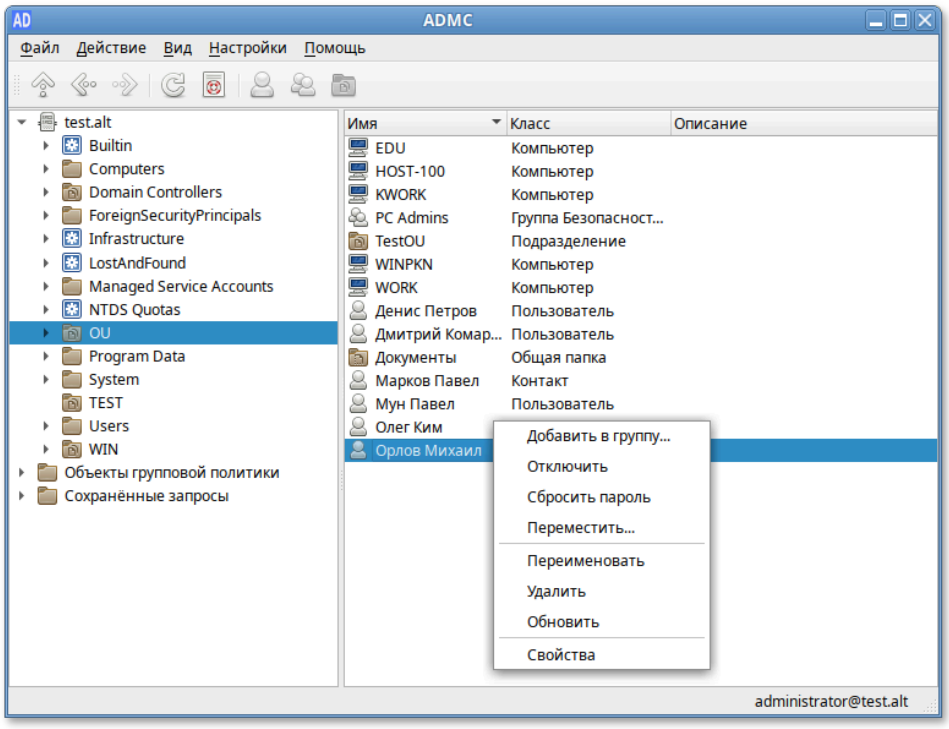


Рис. 166 – Изменение учетной записи пользователя

Для добавления пользователя в группу:

1) в контекстном меню пользователя выбрать пункт «Добавить в группу…»;
2) в открывшемся окне выбрать группы, в которые следует добавить учетную запись пользователя в качестве участника (рис. 167);
3) нажать кнопку «ОК».

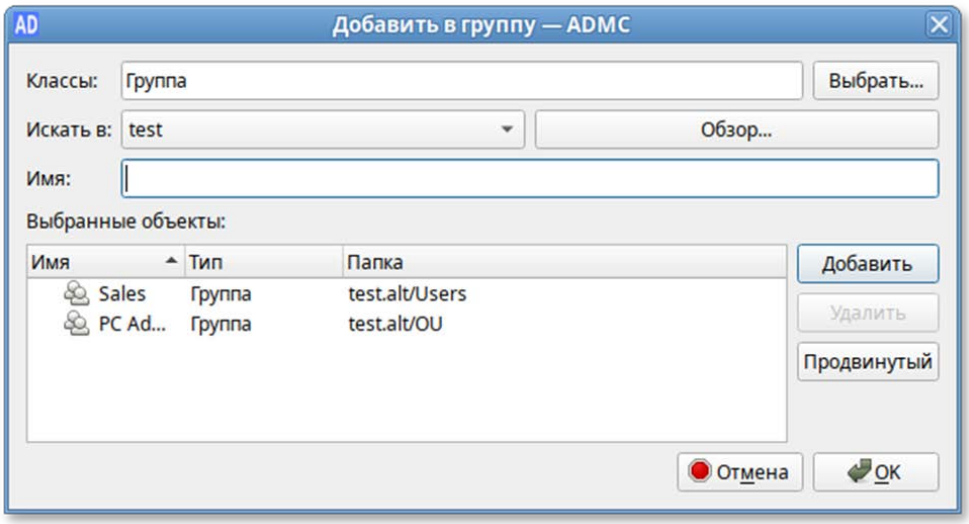


Рис. 167 – Добавление учетной записи пользователя

Для переименования пользователя:

1) в контекстном меню пользователя выбрать пункт «Переименовать»;
2) в открывшемся окне, если нужно, изменить соответствующие поля (рис. 168);
3) нажать кнопку «ОК» для сохранения изменений.

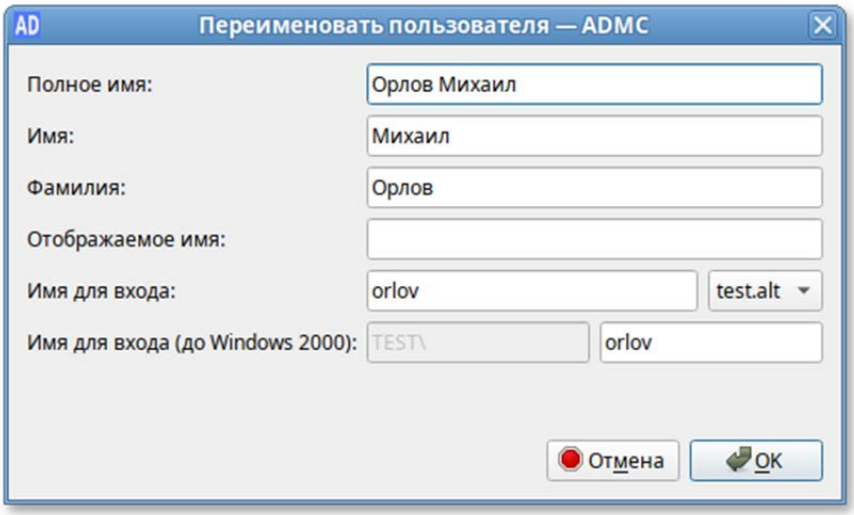


Рис. 168 – Перемеинование пользователя

Для изменения пароля пользователя:

1) в контекстном меню пользователя выбрать пункт «Сбросить пароль»;
2) в открывшемся окне ввести новый пароль и подтвердить его (рис. 169);

3) если нужно, чтобы пользователь изменил этот пароль при следующем входе в систему, установить отметку «Пользователь должен изменить пароль при следующем входе в систему»;
4) установить отметку «Разблокировать учетную запись», если нужно разблокировать учетную запись пользователя;
5) нажать кнопку «ОК» для сохранения изменений.

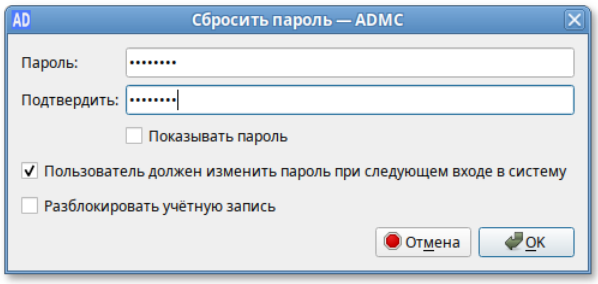


Рис. 169 – Подтверждение пароля

Для перемещения пользователя в другой контейнер (рис. 170):

1) в контекстном меню пользователя выбрать пункт «Переместить…»;
2) в открывшемся окне выбрать контейнер, в который следует переместить учетную запись пользователя;
3) нажать кнопку «ОК».

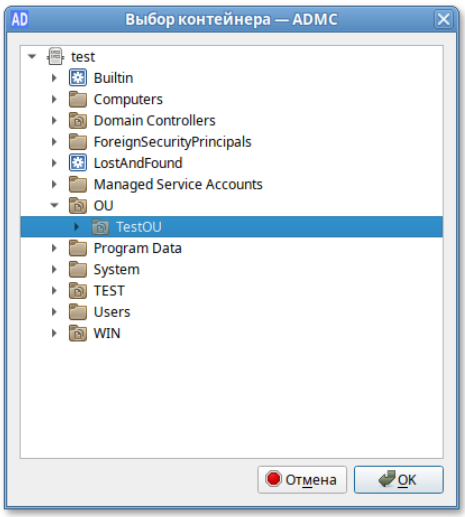


Рис. 170 – Перемещение пользователя в другой контейнер

Для включения/отключения учетной записи пользователя нужно в контекстном меню пользователя выбрать пункт «Отключить» или «Включить» (в зависимости от состояния учетной записи будет доступно одно из этих действий).

Чтобы разблокировать учетную запись пользователя:

1) в контекстном меню пользователя выбрать пункт «Свойства»;
2) в открывшемся окне на вкладке «Учетная запись» отметить пункт «Разблокировать учетную запись» (рис. 171);
3) нажать кнопку «ОК» или «Применить»;
4) для удаления учетной записи пользователя следует в контекстном меню пользователя выбрать пункт «Удалить».

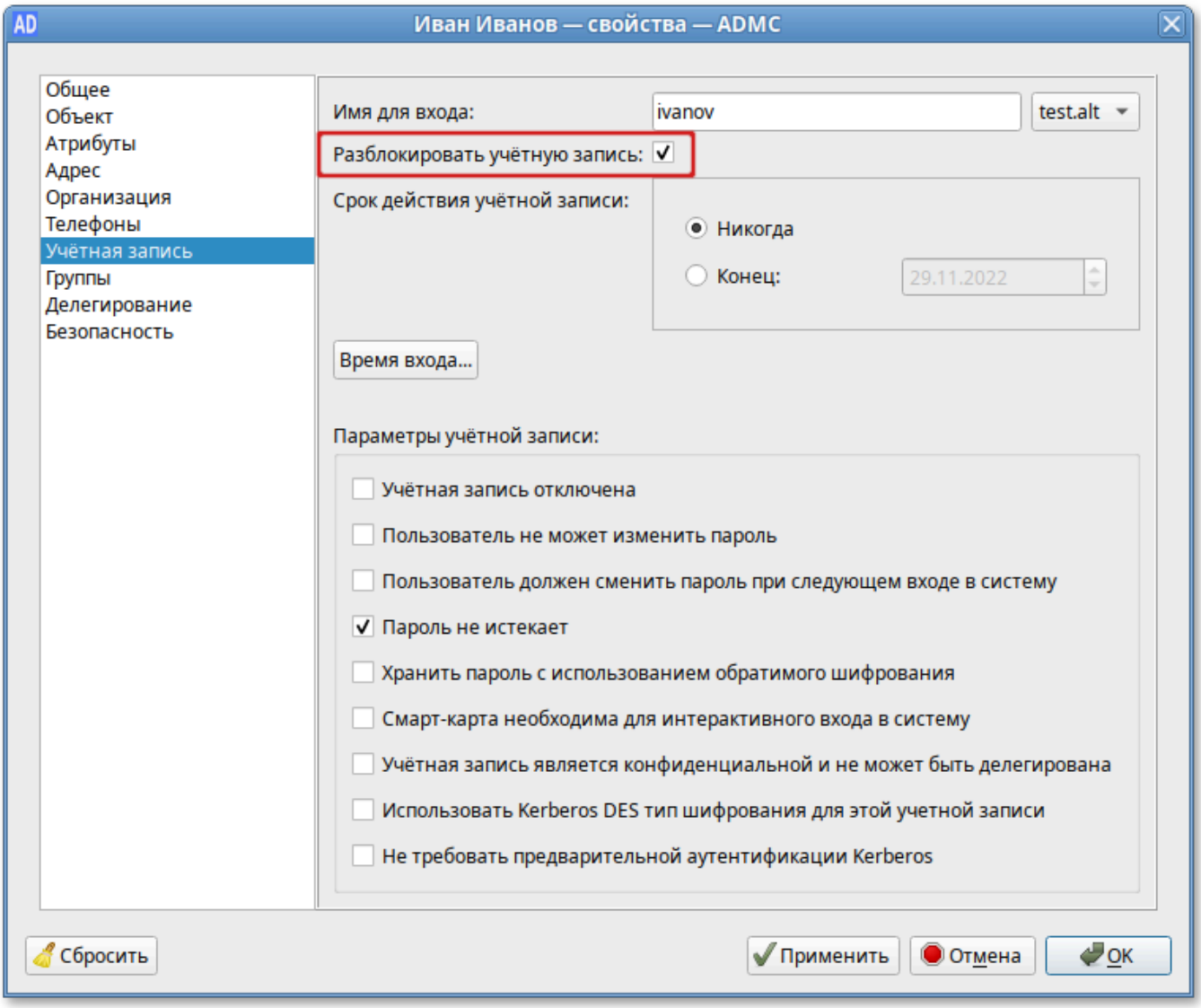


Рис. 171 – Пункт «Разблокировать учетную запись»

⚠ Если в настройках ADMC не отмечен пункт «Подтверждать действия», пользователь будет удален сразу после выбора пункта меню «Удалить».

Для того чтобы найти группы, участником которых является пользователь:

1) в контекстном меню пользователя выбрать пункт «Свойства» (рис. 172);

2) в открывшемся окне на вкладке «Группы» будут отображаться группы, в которые входит данный пользователь.

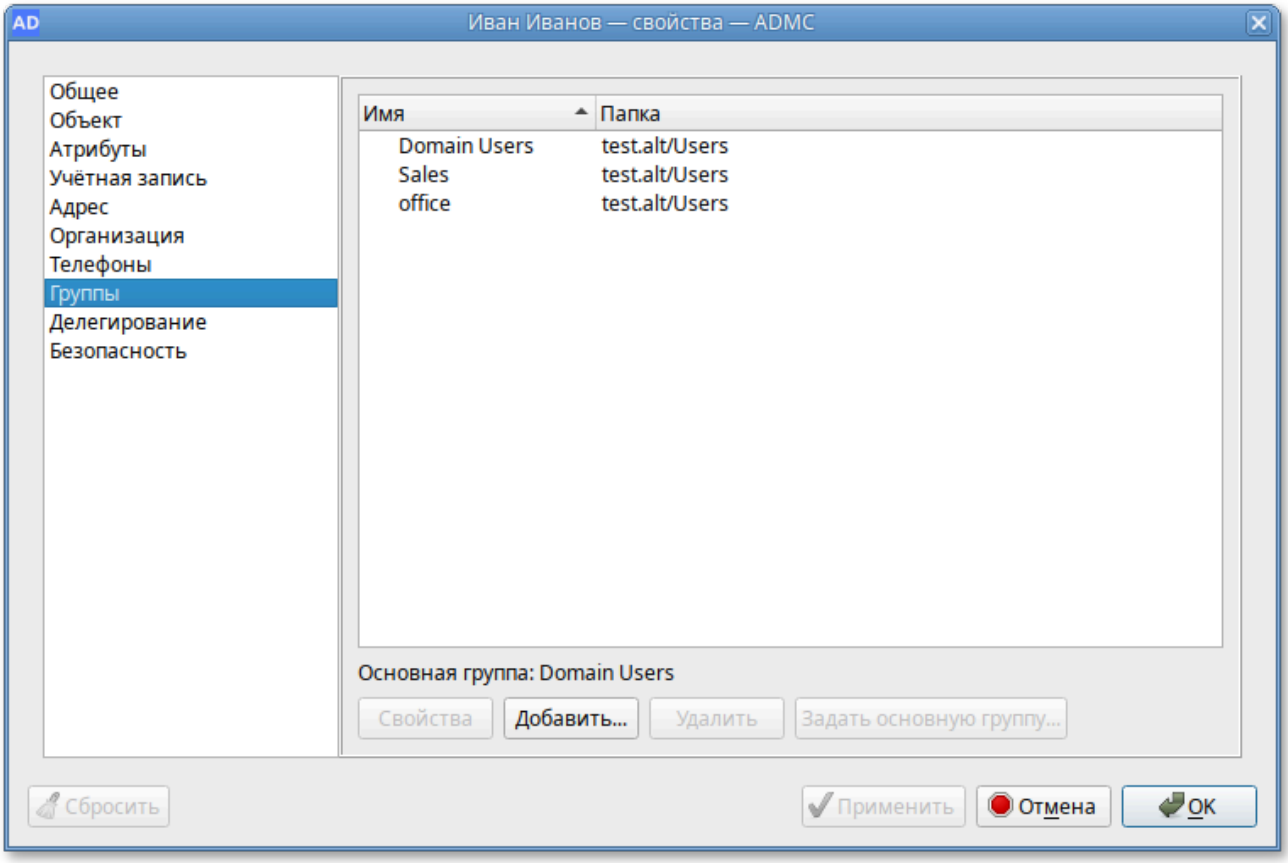


Рис. 172 – Вкладка «Группы»

9.2.4.6. Управление контактами

Контакт предназначен для хранения информации о пользователях, которым не требуется регистрация в домене.

9.2.4.6.1. Создание контакта

Для создания контакта в контекстном меню контейнера следует выбрать пункт «Создать» → «Контакт». Окно мастера создания контакта (рис. 173).

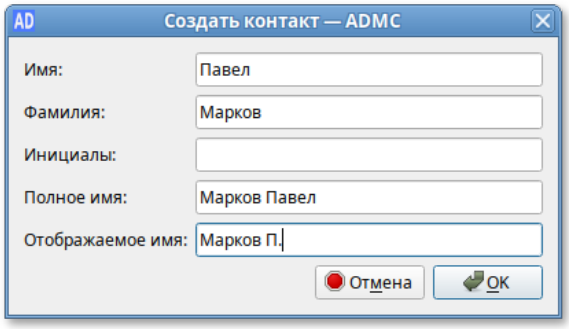


Рис. 173 – Окно мастера создания контакта

При создании контакта можно указать следующие параметры (атрибуты):

- «Имя» – имя пользователя;
- «Фамилия» – фамилия пользователя;
- «Инициалы» – инициалы пользователя;
- «Полное имя» – полное имя пользователя (в это поле можно добавить отчество или поменять имя и фамилию местами);
- «Отображаемое имя» – имя, отображаемое в адресной книге для определенной учетной записи.

9.2.4.6.2. Изменение свойств контакта

Для изменения учетной записи пользователя следует в контекстном меню контакта выбрать соответствующее действие (рис. 174).

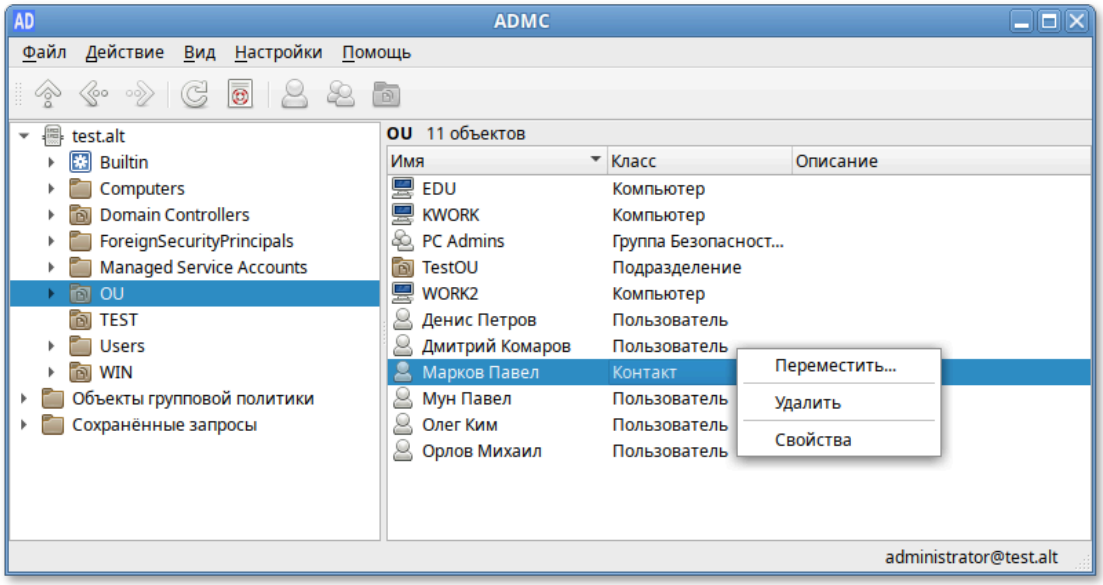


Рис. 174 – Изменение учетной записи пользователя

Вкладки «Общие», «Адрес», «Телефоны» и «Организация» в окне «Свойства» контакта идентичны соответствующим вкладкам окна «Свойства» учетной записи пользователя.

На вкладке «Группы» можно, по аналогии с учетными записями пользователей, указать, членом каких групп является контакт. Возможность членства в группах не дает контакту никаких прав в рамках домена и предназначена для организации групп рассылки.

Для контакта нельзя указать основную группу, так как это не требуется для функционирования групп рассылки.

9.2.4.7. Управление группами

Группа состоит из учетных записей пользователей и компьютеров, контактов и других групп и может управляться как единое целое. Пользователи и компьютеры, входящие в определенную группу, являются членами группы.

Группы характеризуются областью действия и типом. Область действия группы определяет пределы применения группы внутри домена или леса. Тип группы определяет возможность использования группы для назначения разрешений с ресурса общего доступа (для групп безопасности) или только для списков рассылки электронной почты (для групп рассылки).

Создание группы

Для создания группы следует в контекстном меню контейнера выбрать пункт «Создать» → «Группа». Окно мастера создания группы (рис. 175).

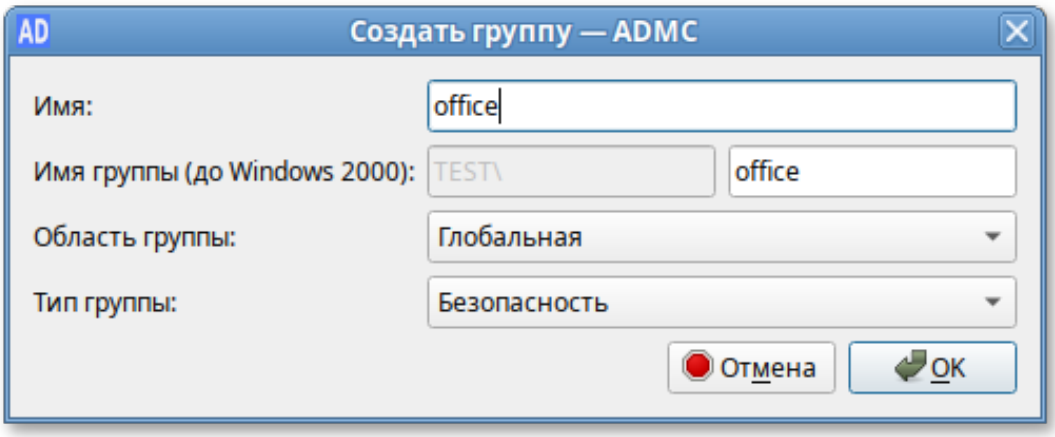


Рис. 175 – Окно мастера создания группы

При создании группы можно указать следующие параметры (атрибуты):

- «Имя» – название группы;
- «Имя группы (до Windows 2000)» – название группы для старых систем (пред-Windows 2000);
- «Область группы» – область действия группы;
- «Глобальная» – членами глобальной группы могут быть другие группы и учетные записи только из того домена, в котором определена группа. Членам этой группы разрешения могут назначаться в любом домене леса;
- «Домен локальная» – членам такой группы разрешения могут назначаться только внутри домена (доступ к ресурсам одного домена);
- «Универсальная» – членами универсальных групп могут быть другие группы и учетные записи из любого домена дерева доменов или леса. Членам такой группы разрешения могут назначаться в любом домене дерева доменов или леса;
- «Тип группы» – тип группы;
- «Безопасность» – используется для назначения разрешений доступа к общим ресурсам;
- «Рассылка» – используется для создания списков рассылки электронной почты.

9.2.4.7.1. Изменение группы

Для изменения группы следует в контекстном меню группы выбрать соответствующее действие (рис. 176).

Для добавления группы в другую группу (рис. 177):

1) в контекстном меню группы выбрать пункт «Добавить в группу…»;
2) в открывшемся окне выбрать группы, в которые следует добавить данную группу в качестве участника;
3) нажать кнопку «ОК».

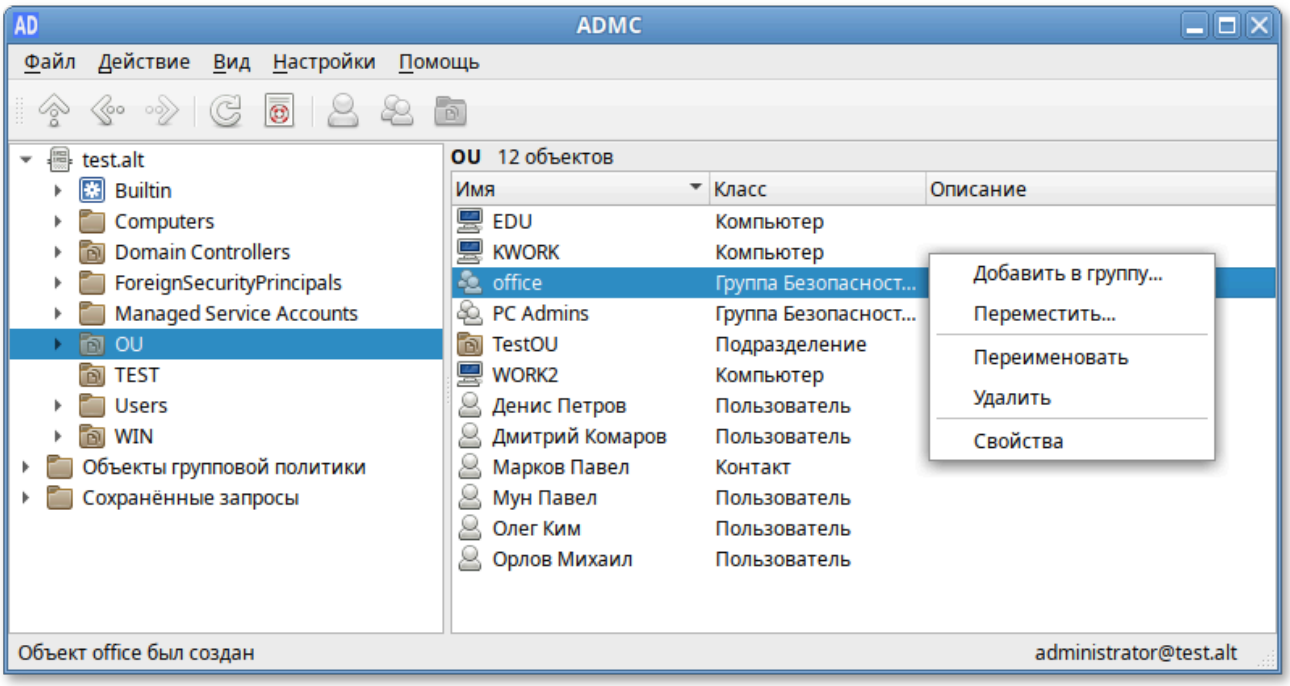


Рис. 176 – Изменение группы

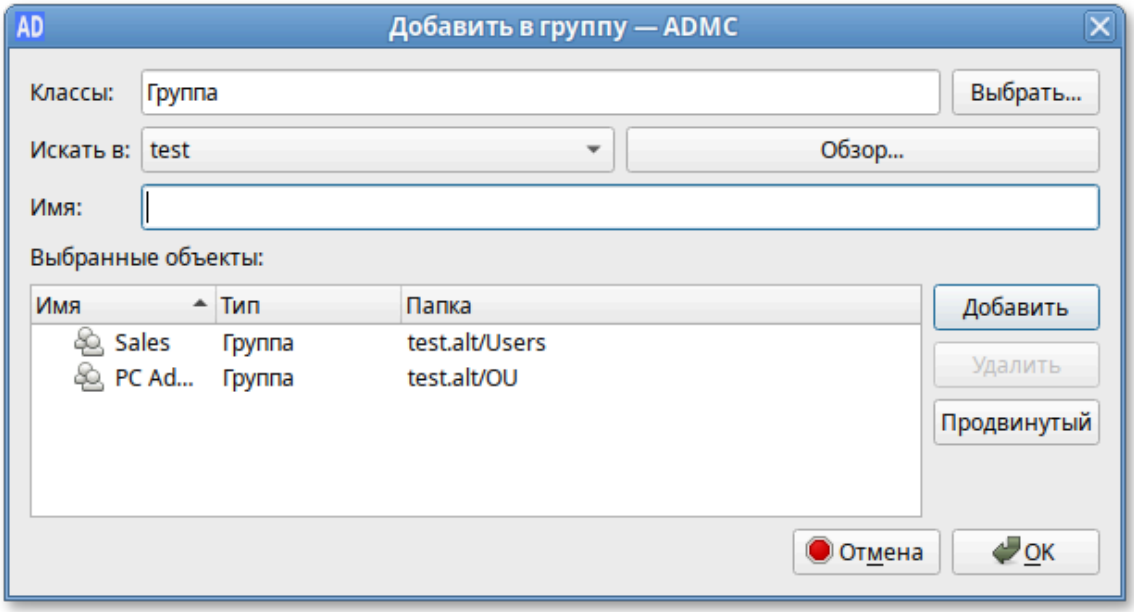


Рис. 177 – Добавление группы в другую группу

Для перемещения группы в другой контейнер (рис. 178):

1) в контекстном меню группы выбрать пункт «Переместить…»;
2) в открывшемся окне выбрать контейнер, в который следует переместить группу;
3) нажать кнопку «ОК».

Для переименования группы:

1) в контекстном меню группы выбрать пункт «Переименовать» (рис. 179);

2) в открывшемся окне, если нужно, изменить соответствующие поля;

3) нажать кнопку «ОК» для сохранения изменений.

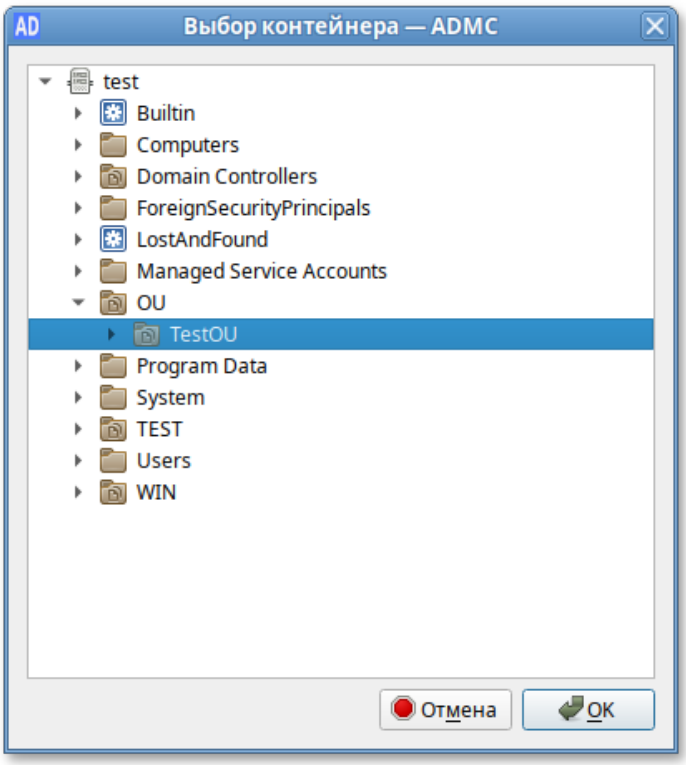


Рис. 178 – Перемещение группы в другой контейнер

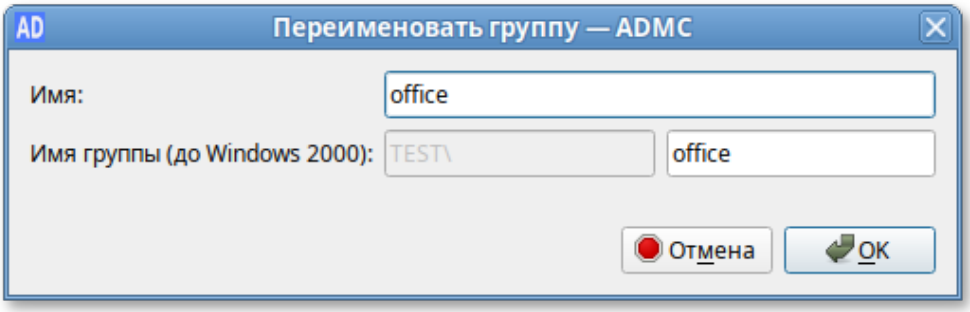


Рис. 179 – Перемеинование группы

Для удаления группы следует в контекстном меню группы выбрать пункт «Удалить».

⚠ Если в настройках ADMC не отмечен пункт «Подтверждать действия», группа будет удалена сразу после выбора пункта меню «Удалить».

Для того чтобы добавить участников в группу:

1) в контекстном меню группы выбрать пункт «Свойства»;
2) в открывшемся диалоговом окне на вкладке «Участники» нажать кнопку «Добавить…» (рис. 180);

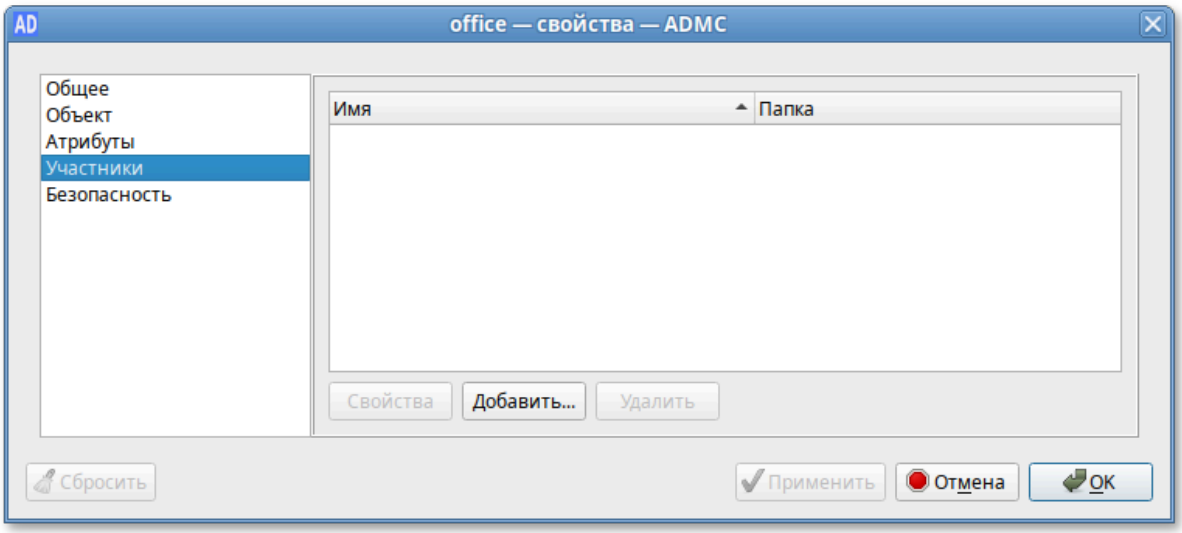


Рис. 180 – Добавление участников в группу

3) выбрать объекты, которые нужно добавить в группу (рис. 181):
   - нажать кнопку «ОК»;
   - нажать кнопку «ОК» или «Применить» для сохранения изменений;

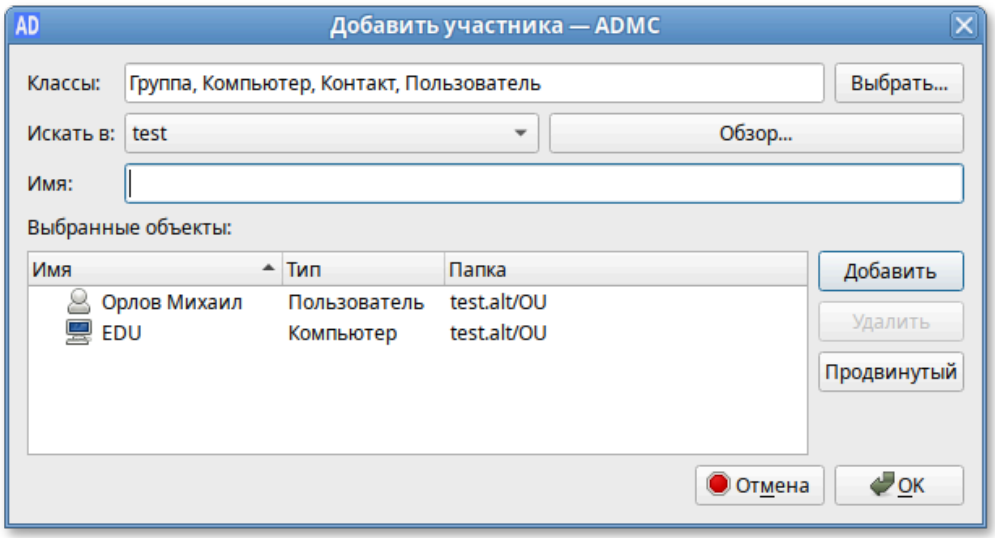


Рис. 181 – Выбор объектов, которые нужно добавить в группу

4) для изменения области действия/типа группы:

- в контекстном меню группы выбрать пункт «Свойства»;
- в открывшемся диалоговом окне на вкладке «Общее» в выпадающем списке «Тип группы» выбрать тип группы, в выпадающем списке «Область группы» выбрать область действия группы (рис. 182);
- нажать кнопку «ОК» или «Применить» для сохранения изменений.

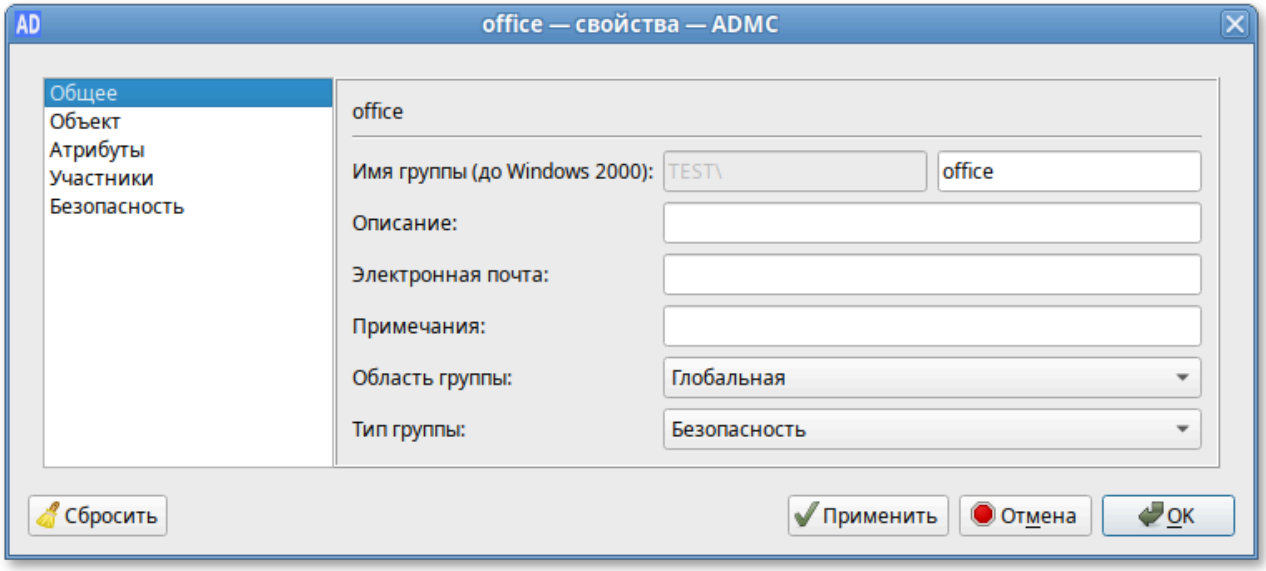


Рис. 182 – Изменение области действия/типа группы

9.2.4.8. Управление компьютерами

Учетные записи компьютеров представляют собой устройства, подключенные к AD. Они хранятся в базе данных AD после того, как их подключат к домену.

9.2.4.8.1. Создание учетной записи компьютера

Учетная запись компьютера создается во время стандартной процедуры присоединения к домену.

Для создания вручную учетной записи компьютера следует в контекстном меню контейнера выбрать пункт «Создать» → «Компьютер». Окно мастера создания учетной записи компьютера (рис. 183).

При создании учетной записи компьютера нужно указать название компьютера (поле «Имя») и название компьютера для старых систем (поле «Имя для входа (до Windows 2000)»).

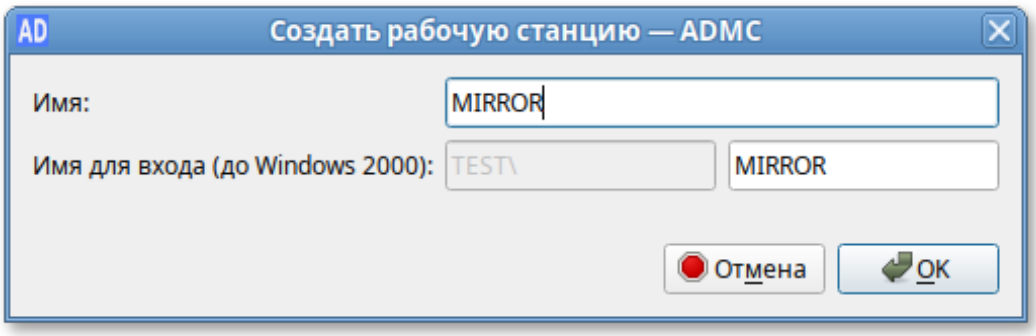


Рис. 183 – Создание учетной записи компьютера

9.2.4.8.2. Изменение учетной записи компьютера

Для изменения учетной записи компьютера следует в контекстном меню компьютера выбрать соответствующее действие (рис. 184).

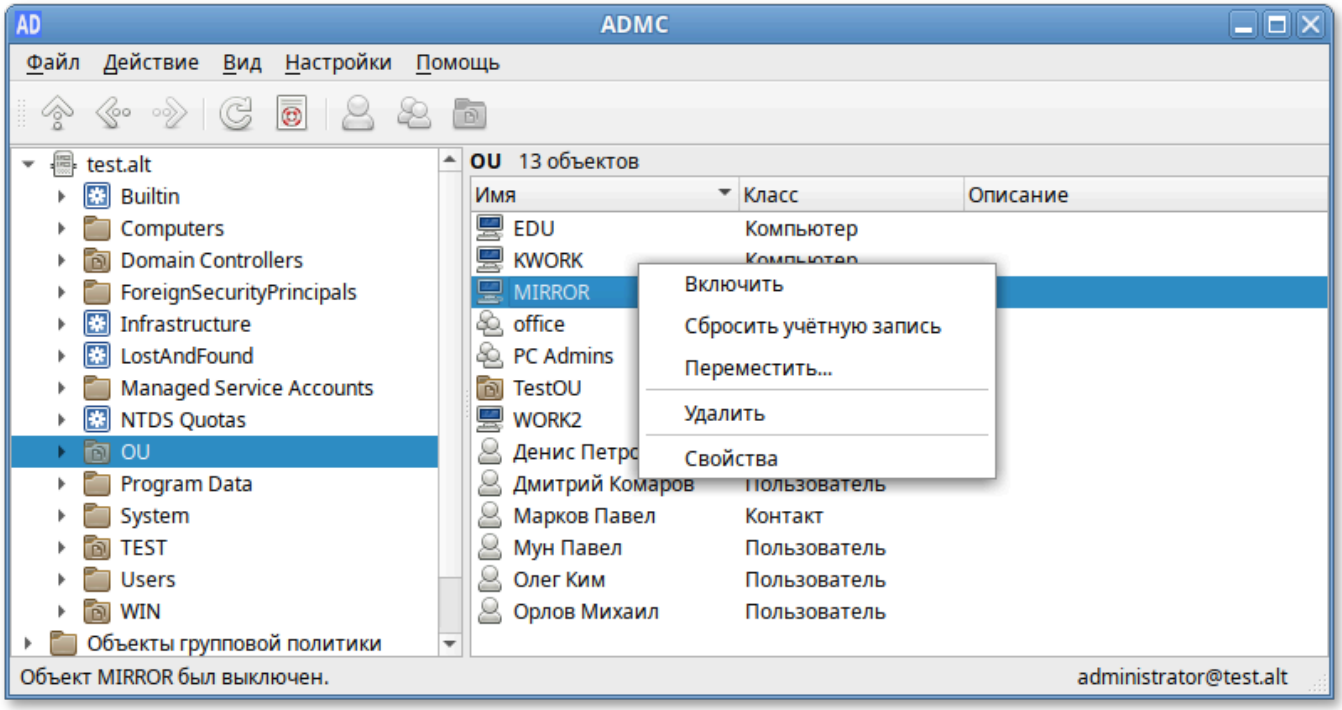


Рис. 184 – Изменение учетной записи компьютера

Для включения/отключения учетной записи компьютера нужно в контекстном меню компьютера выбрать пункт «Отключить» или «Включить» (в зависимости от состояния учетной записи будет доступно одно из этих действий).

Для сброса учетной записи компьютера следует в контекстном меню компьютера выбрать пункт «Сбросить учетную запись». При этом учетная запись выбранного компьютера будет переустановлена. Переустановка учетной записи компьютера прекращает его подключение к домену и требует заново ввести данный компьютер в домен.

Для перемещения компьютера в другой контейнер:

1) в контекстном меню компьютера выбрать пункт «Переместить…» (рис. 185);
2) в открывшемся окне выбрать контейнер, в который следует переместить учетную запись компьютера;
3) нажать кнопку «ОК».

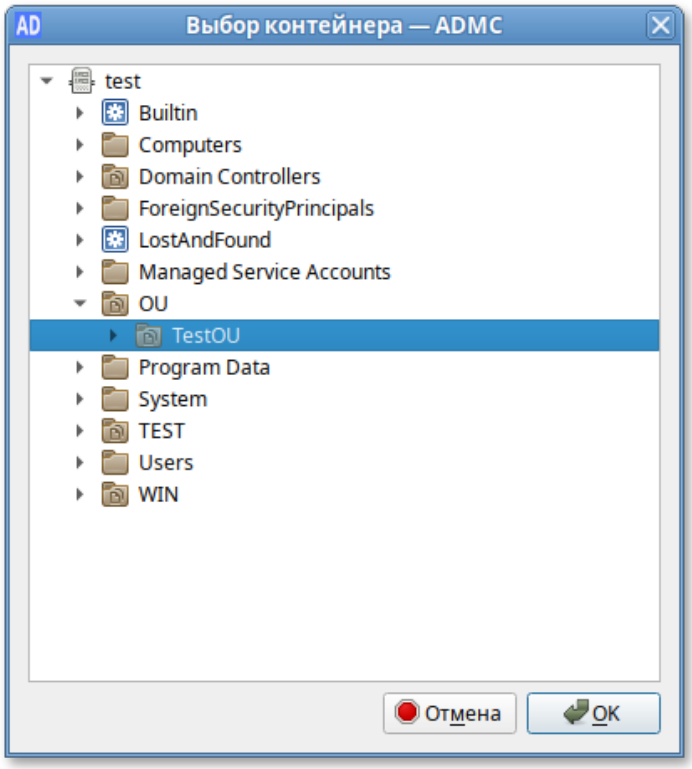


Рис. 185 – Перемещение компьютера в другой контейнер

Для удаления учетной записи компьютера следует в контекстном меню компьютера выбрать пункт «Удалить».

⚠ Если в настройках ADMC не отмечен пункт «Подтверждать действия», компьютер будет удален сразу после выбора пункта меню «Удалить».

9.2.4.9. Управление подразделениями

Организационная единица или, подразделение (Organizational Unit, OU) – это субконтейнер в AD, в который можно помещать пользователей, группы, компьютеры и другие объекты AD. Подразделение – самая маленькая область или единица, для которой можно назначить параметры групповой политики. Подразделения могут быть вложенными.

9.2.4.9.1. Создание подразделения

Для создания подразделения следует в контекстном меню контейнера выбрать пункт «Создать» → «Подразделение». Окно мастера создания подразделения (рис. 186).

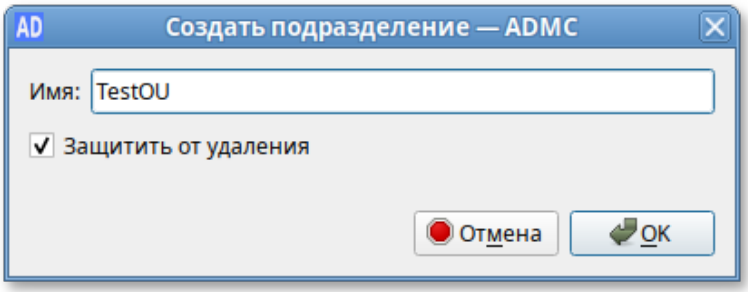


Рис. 186 – Окно мастера создания подразделения

При создании подразделения нужно указать название подразделения (поле «Имя»).

Примечание. Если при создании подразделения отметить пункт «Защитить от удаления», то для удаления данного подразделения, нужно сначала снять данную отметку в окне свойств подразделения.

9.2.4.9.2. Изменение подразделения

Для изменения подразделения следует в контекстном меню подразделения выбрать соответствующее действие (рис. 187).

Для переименования подразделения:

1) в контекстном меню подразделения выбрать пункт «Переименовать»;

2) в открывшемся окне изменить имя подразделения (рис. 188);

3) нажать кнопку «ОК» для сохранения изменений.

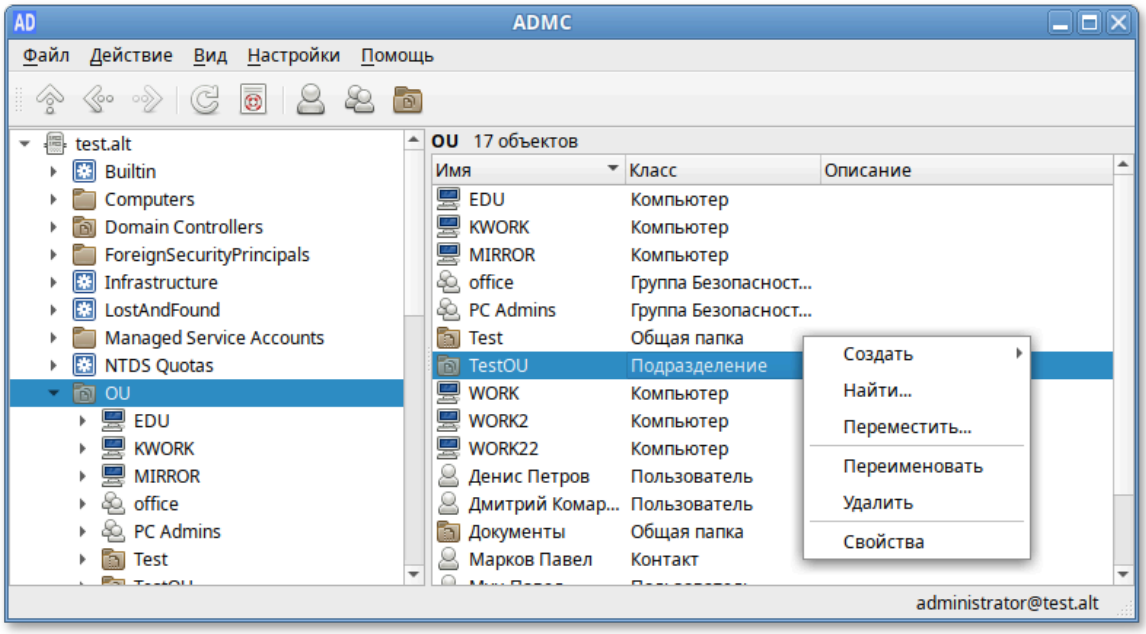


Рис. 187 – Изменение подразделения

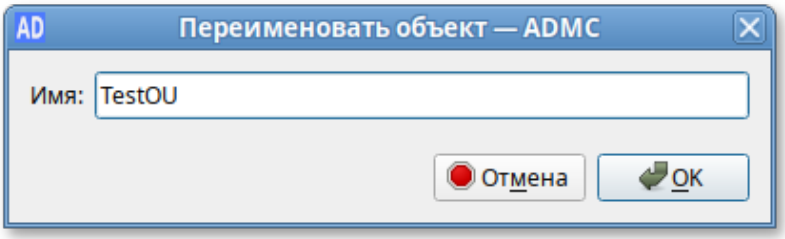


Рис. 188 – Перемеинование подразделения

Для удаления подразделения следует в контекстном меню подразделения выбрать пункт «Удалить».

⚠ Если при создании подразделения был отмечен пункт «Защитить от удаления», то сразу удалить подразделение не получится, нужно сначала снять данную отметку в окне свойств подразделения (рис. 189).

Для перемещения подразделения в другой контейнер:

1) в контекстном меню подразделения выбрать пункт «Переместить…»;
2) в открывшемся окне выбрать контейнер, в который следует переместить подразделение (рис. 190);
3) нажать кнопку «ОК».

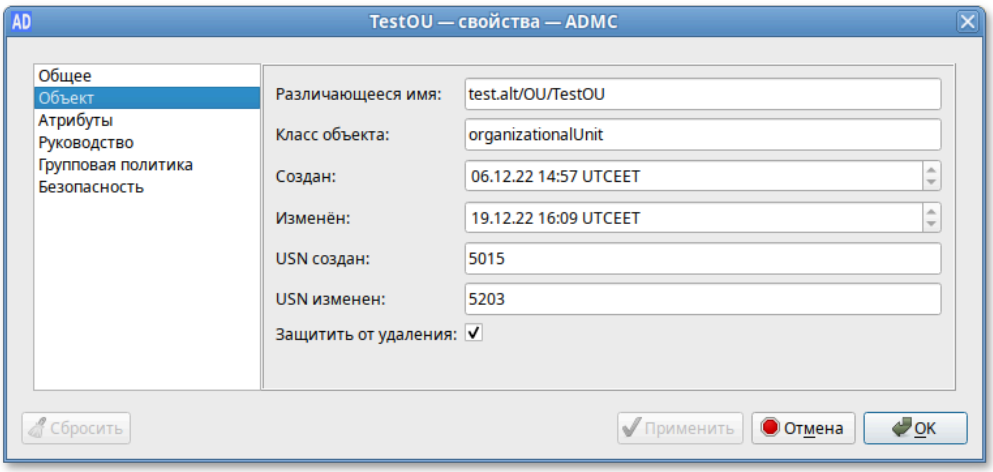


Рис. 189 – Удаление подразделения

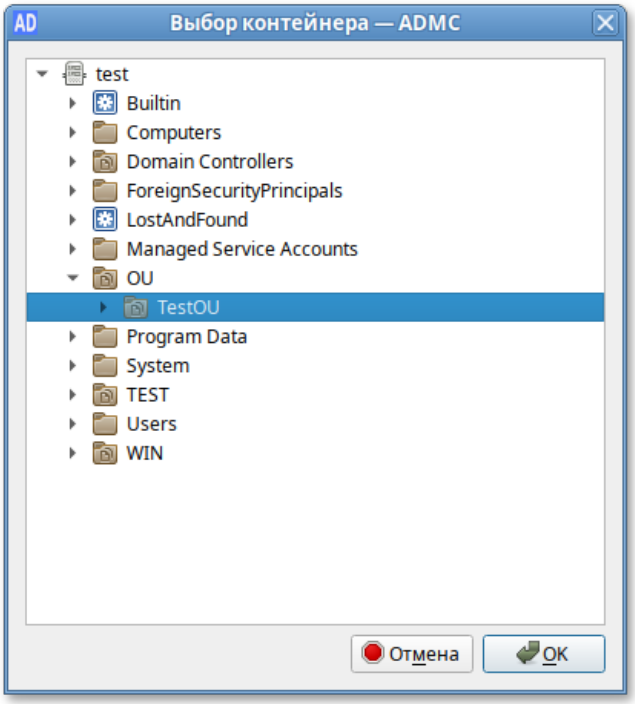


Рис. 190 – Перемещение подразделения в другой контейнер

9.2.4.10. Управление общими папками

Общая папка является ссылкой на общий сетевой ресурс и не содержит никаких данных.

Для создания общей папки следует в контекстном меню контейнера выбрать пункт «Создать» → «Общая папка». Окно мастера создания общей папки (рис. 191).

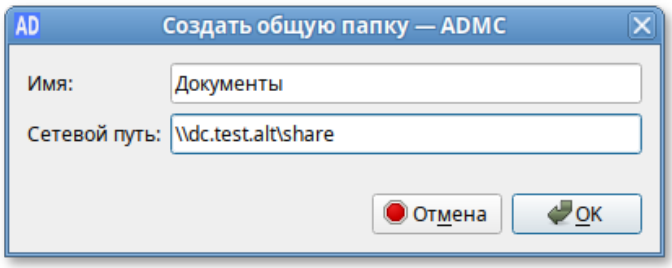


Рис. 191 – Создание общей папки

В поле «Имя» следует ввести название папки, под которым она будет отображаться в каталоге AD, а в поле «Сетевой путь» – полный сетевой путь к общей папке.

Примечание. Чтобы просмотреть содержимое общей папки, на машине Windows в дереве консоли управления «Active Directory – пользователи и компьютеры» в контекстном меню общей папки следует выбрать пункт Проводник. Откроется новое окно Проводника, в котором будет показано содержимое общей папки.

Для изменения общей папки следует в контекстном меню общей папки выбрать соответствующее действие (рис. 192).

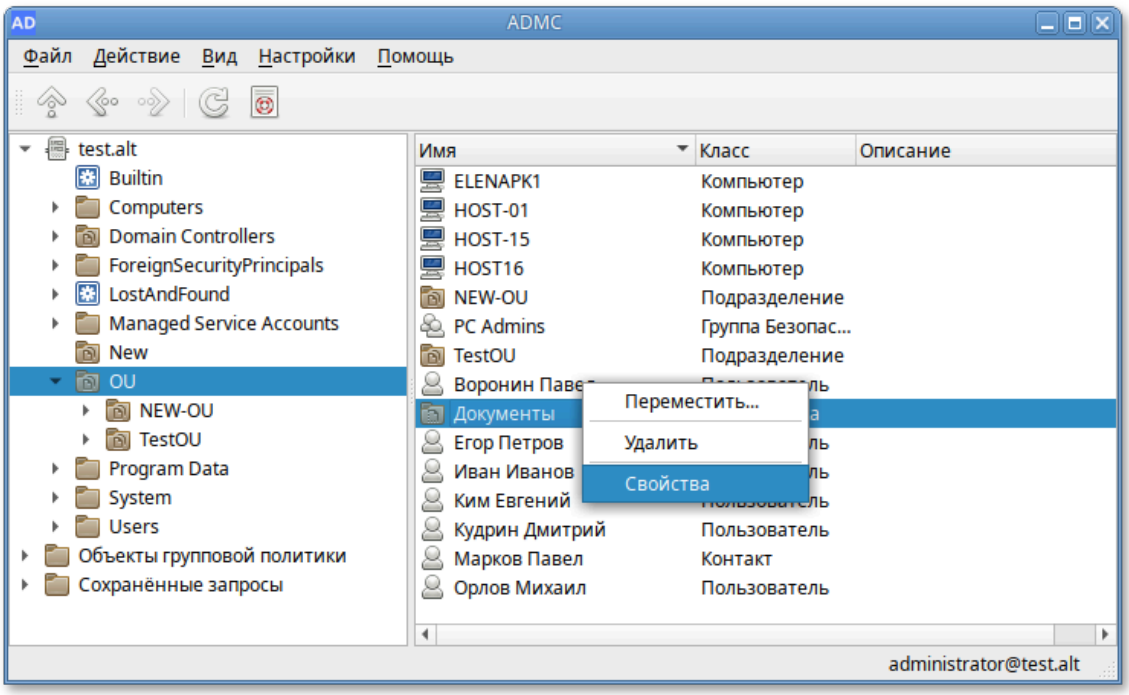


Рис. 192 – Изменение общей папки

9.2.4.11. Управление объектами групповых политик

Групповая политика состоит из набора политик, называемых объектами групповой политики. Для вступления настроек в силу, объект групповой политики нужно связать с одним или несколькими контейнерами AD. Любой объект групповой политики может быть связан с несколькими контейнерами, и, наоборот, с конкретным контейнером может быть связано несколько объектов групповой политики. Контейнеры наследуют объекты групповой политики, например, объект групповой политики, связанный с подразделением, применяется ко всем пользователям и компьютерам в его дочерних подразделениях. Аналогичным образом, объект групповой политики, применяемый к OU, применяется не только ко всем пользователям и компьютерам в этом OU, но и наследуется всем пользователям и компьютерам в дочерних OU.

ADMC позволяет управлять объектами групповых политик: создавать, удалять, создавать ссылки на групповые политики.

В разделе «Объекты групповой политики» отображаются групповые политики, которые назначены на различные OU (отображается вся структура OU). Полный список политик (GPO) в текущем домене доступен в разделе «Все политики» (рис. 193).

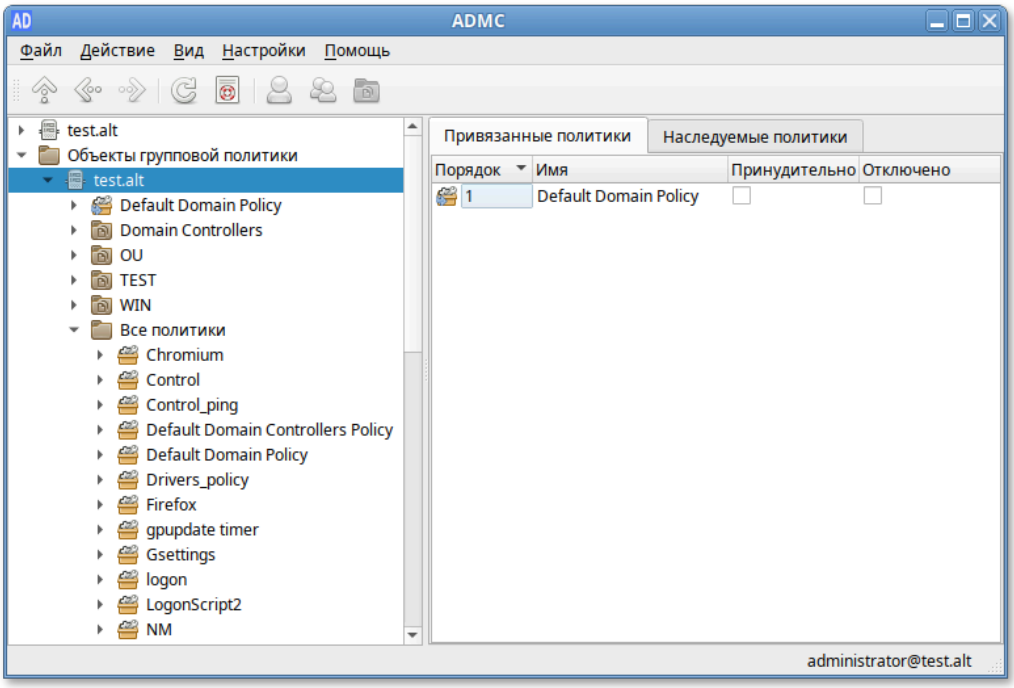


Рис. 193 – Раздел «Все политики»

П р и м е ч а н и е . В каждом домене Active Directory по умолчанию создаются два объекта групповой политики, которые действуют на все компьютеры и контроллеры домена соответственно (рис. 194):

- Default Domain Policy;

- Default Domain Controller Policy.

П р и м е ч а н и е . Эти объекты групповой политики очень важны, поэтому не рекомендуется вносить в них изменения без крайней нужности.

Групповые политики Active Directory можно назначить на OU или весь домен. Чаще всего политики привязываются к OU с компьютерами или пользователями.

П р и м е ч а н и е . Редактирование групповых политик реализуется в модуле редактирования настроек клиентской конфигурации (GPUI).

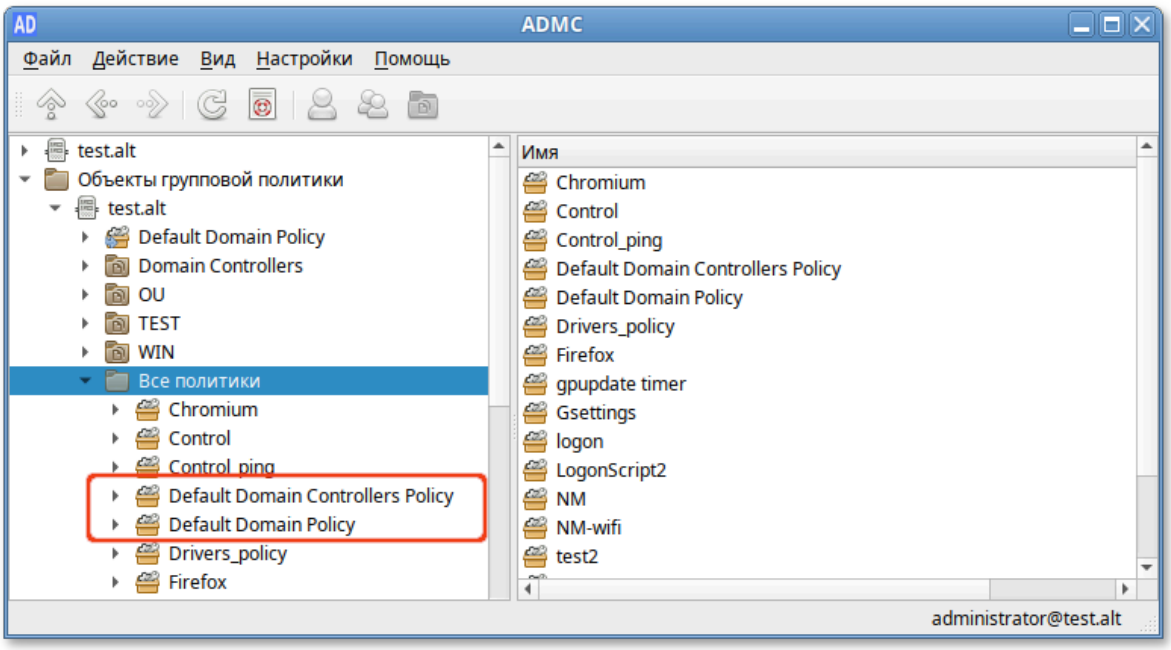


Рис. 194 – Объекты групповой политикой

9.2.4.11.1. Создание объекта групповой политики

Для того чтобы создать новый объект групповой политики и сразу назначить его на OU нужно выполнить следующие действия:

1) в контекстном меню нужного контейнера выбрать пункт «Создать политику и связать с этим подразделением» (рис. 195);

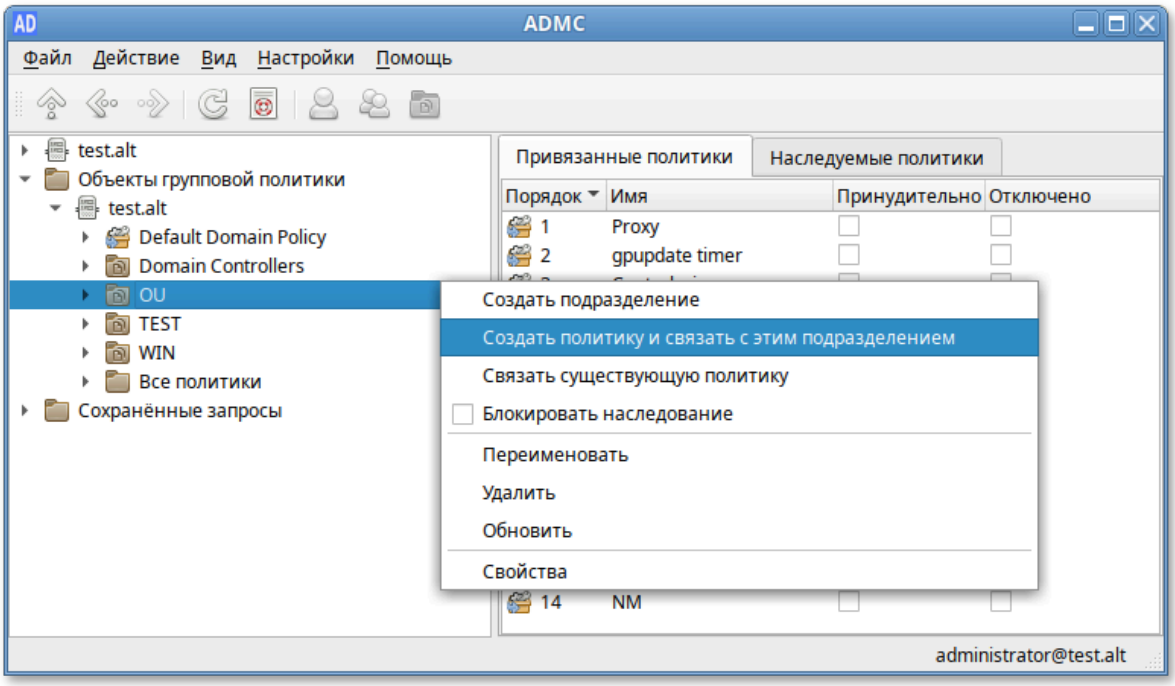


Рис. 195 – Создание объекта групповой политики

2) в открывшемся окне задать имя политики (рис. 196);

3) нажать кнопку «ОК».

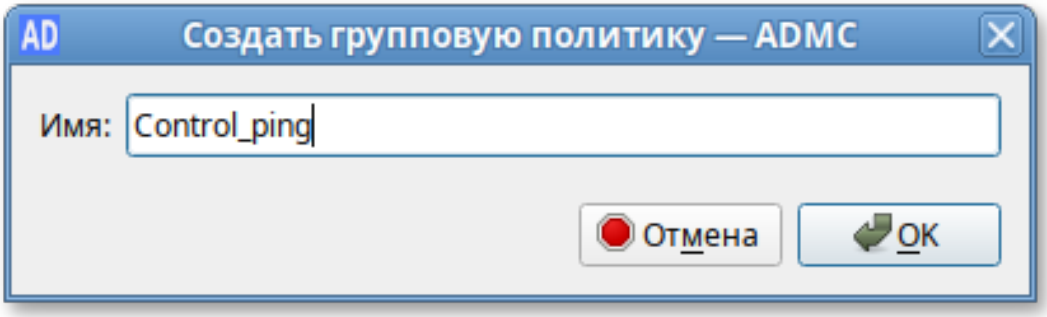


Рис. 196 – Имя политики

Для того чтобы создать новый объект групповой политики, не назначая его на OU, нужно выполнить следующие действия:

1) в контекстном меню папки «Все политики» выбрать пункт «Создать политику» (рис. 197);

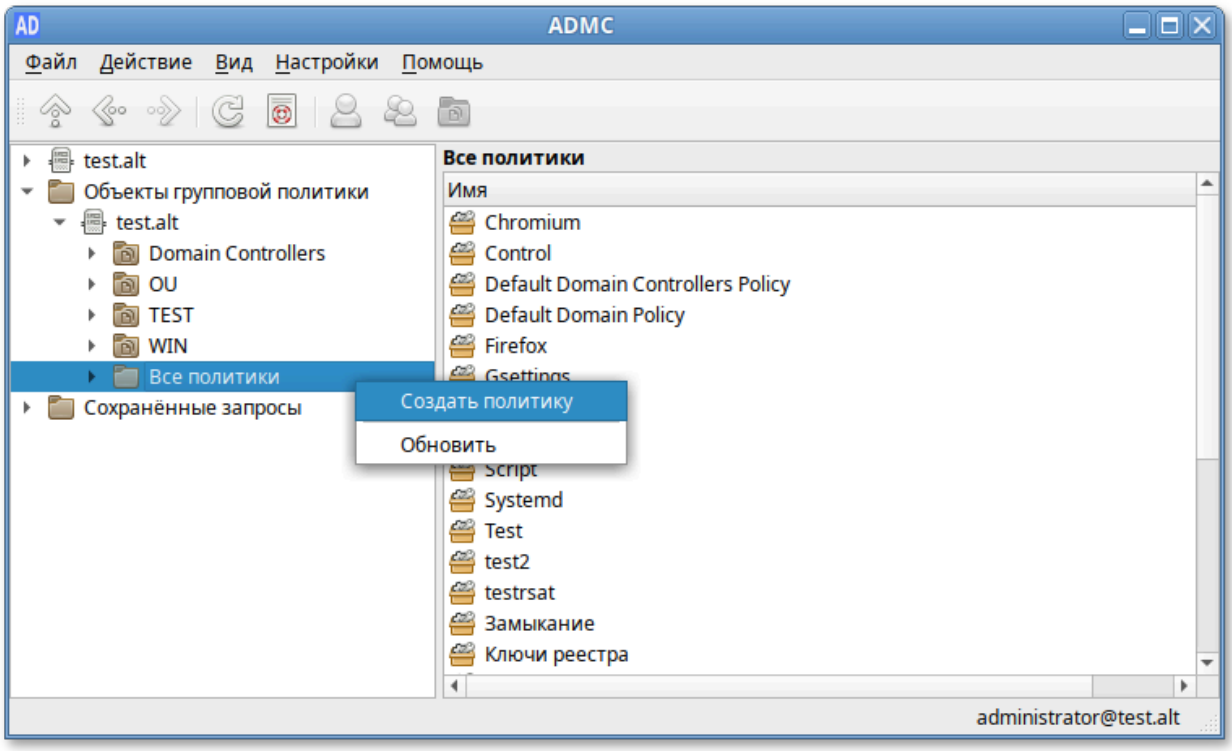


Рис. 197 – Папка «Все политики»

2) в открывшемся окне задать имя политики (рис. 198);

3) нажать кнопку «ОК».

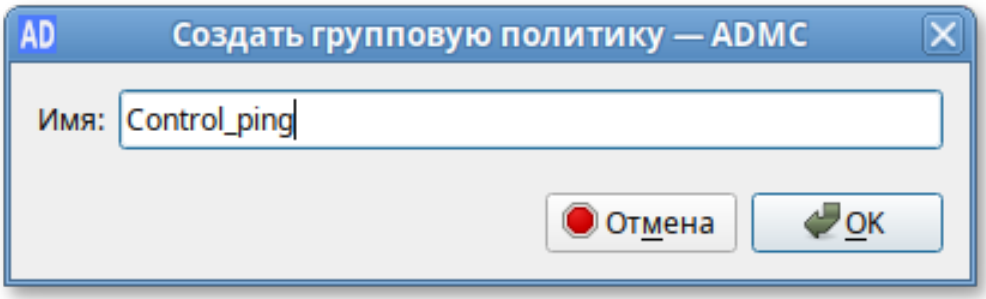


Рис. 198 – Задание имя политики

Созданный объект групповой политики не будет задействован, пока не будет привязан к подразделению.

9.2.4.11.2. Изменение объекта групповой политики

Для изменения объекта групповой политики следует в контекстном меню политики выбрать соответствующее действие (рис. 199, рис. 200).

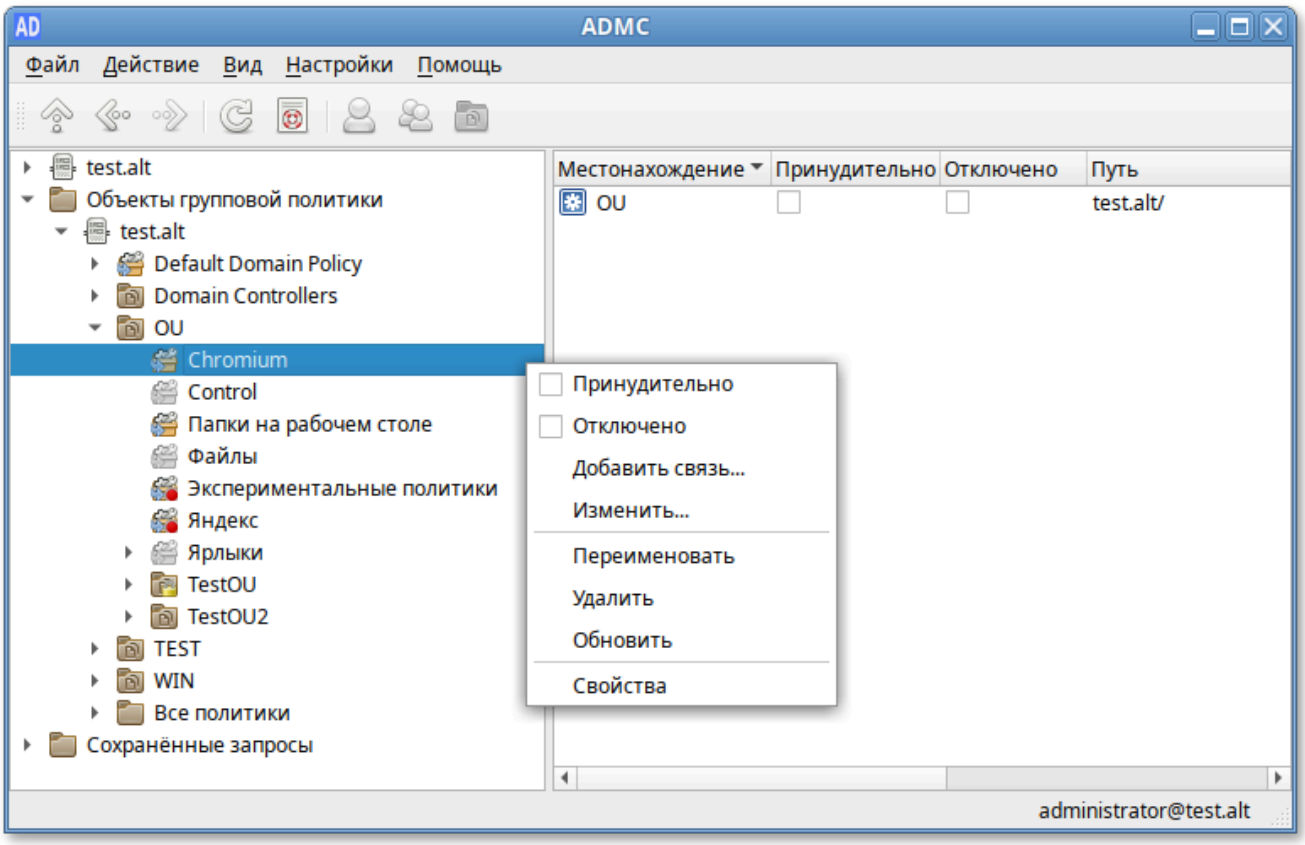


Рис. 199 –Изменение объекта групповой политики

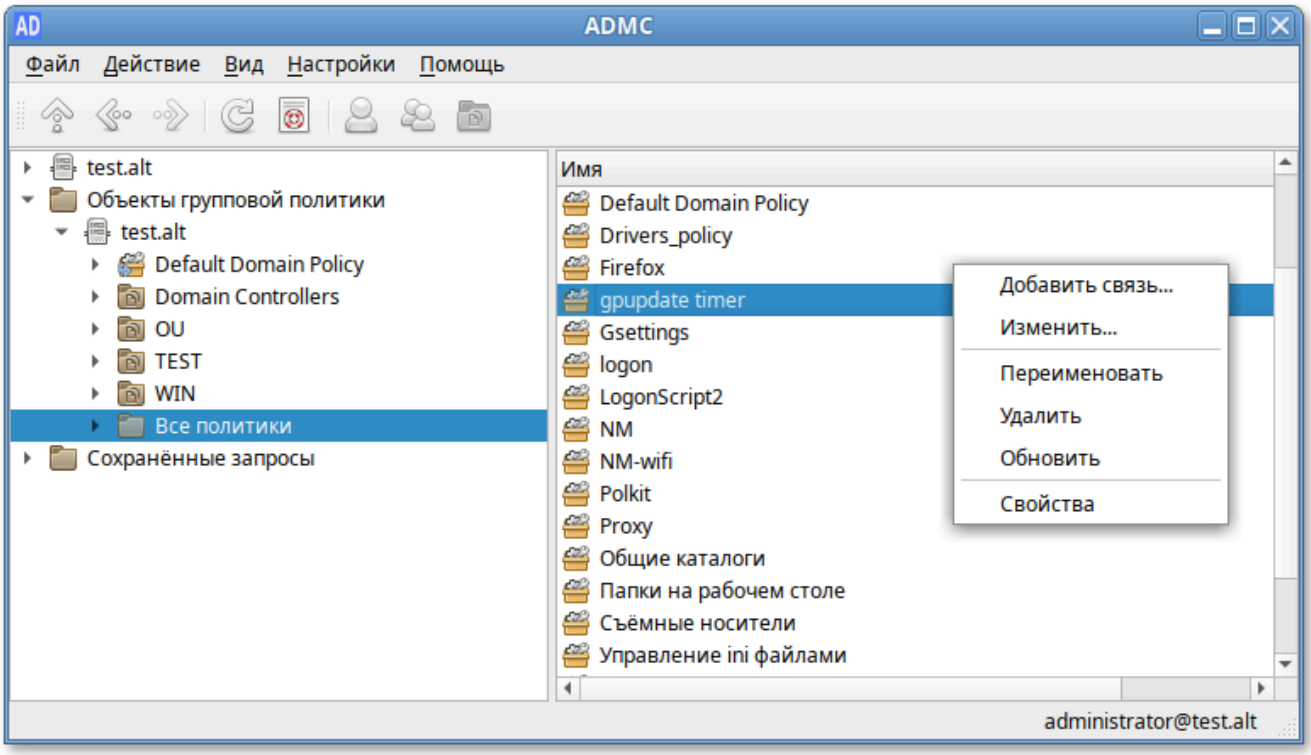


Рис. 200 – Всплывающее окно изменения объекта групповой политики

9.2.4.11.2.1 Переименование объекта групповой политики

Для переименования политики:

1) в контекстном меню политики выбрать пункт «Переименовать»;

2) в открывшемся окне ввести новое название (рис. 201);

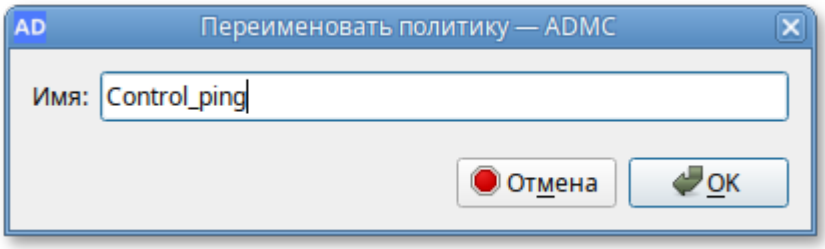


Рис. 201 – Переименование объекта групповой политики

3) нажать кнопку «ОК» для сохранения изменений.

9.2.4.11.2.2 Удаление объекта групповой политики

Для удаления политики:

1) в контекстном меню политики в разделе «Все политики» выбрать пункт «Удалить» (рис. 202);

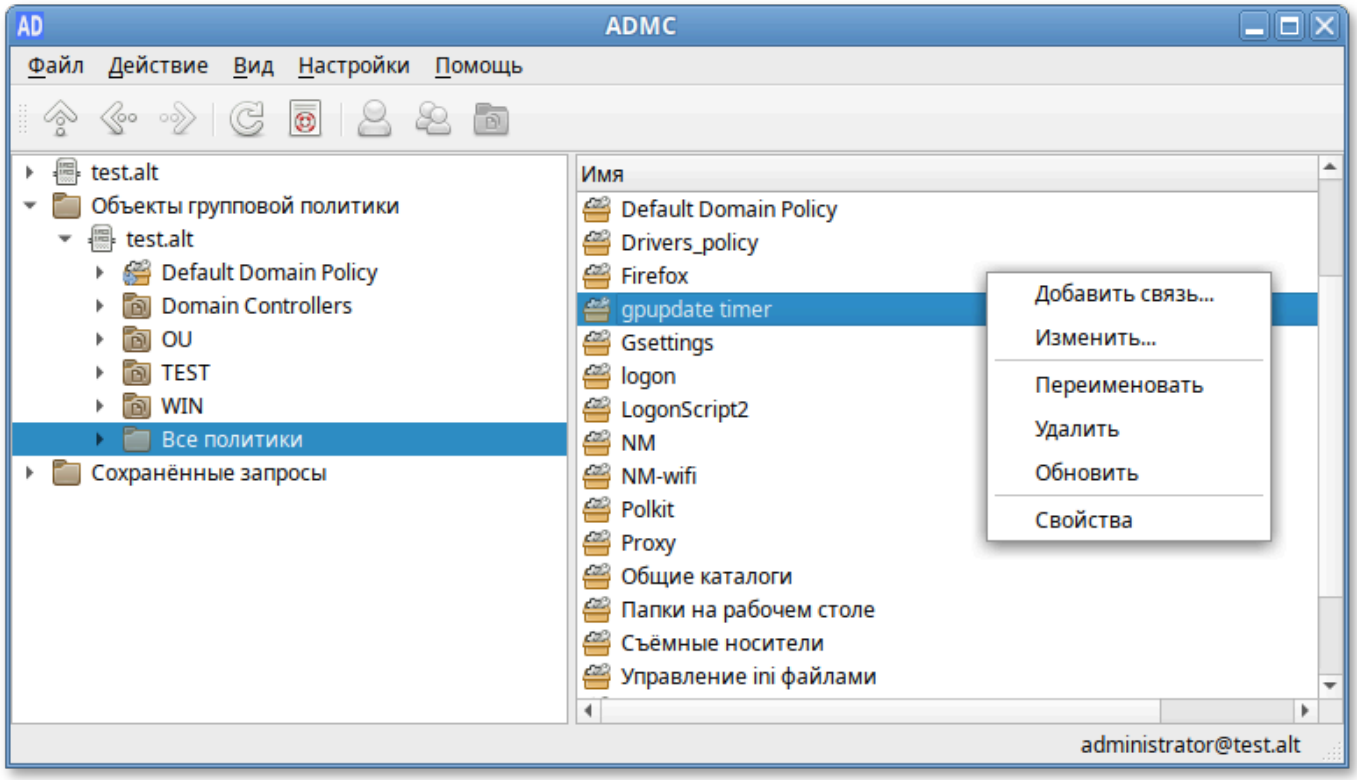


Рис. 202 – Удаление объекта групповой политики

2) подтвердить удаление, нажав кнопку «Да» (рис. 203).

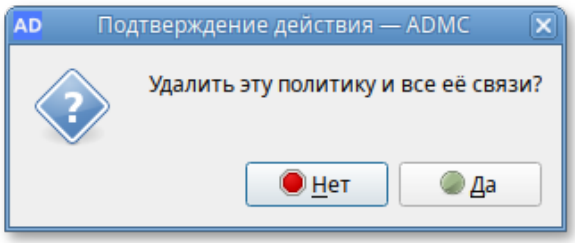


Рис. 203 – Подтверждение удаления

Примечание. Если выбрать пункт «Удалить» в контекстном меню политики в подразделении, на которое она назначена, будет удалена только связь между политикой и подразделением (рис. 204, рис. 205).

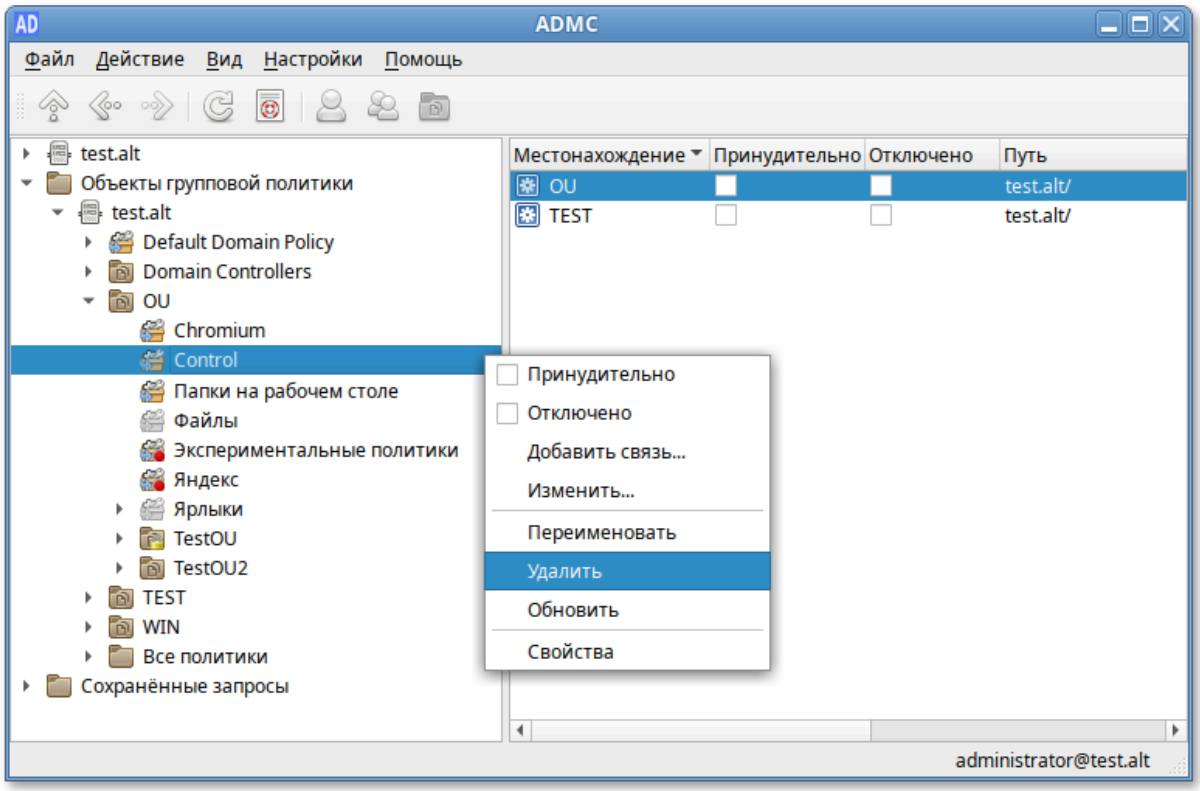


Рис. 204 – Пункт «Удалить»

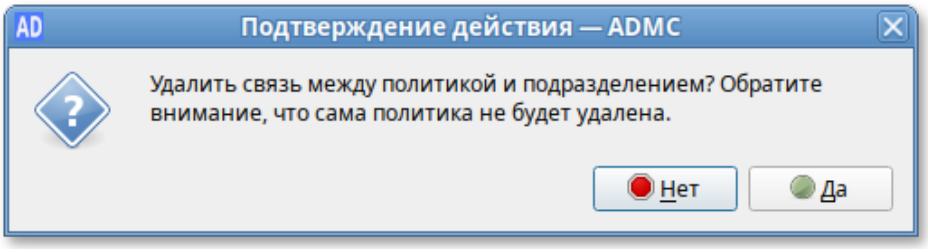


Рис. 205 – Подтверждение действия

9.2.4.11.2.3 Создание и удаление связи между политикой и подразделением

Для связи между политикой и подразделением (создания ссылки на политику):

1) в контекстном меню политики выбрать пункт «Добавить связь…»;
2) выбрать объекты, которые нужно связать с политикой;
3) нажать кнопку «ОК» (рис. 206).

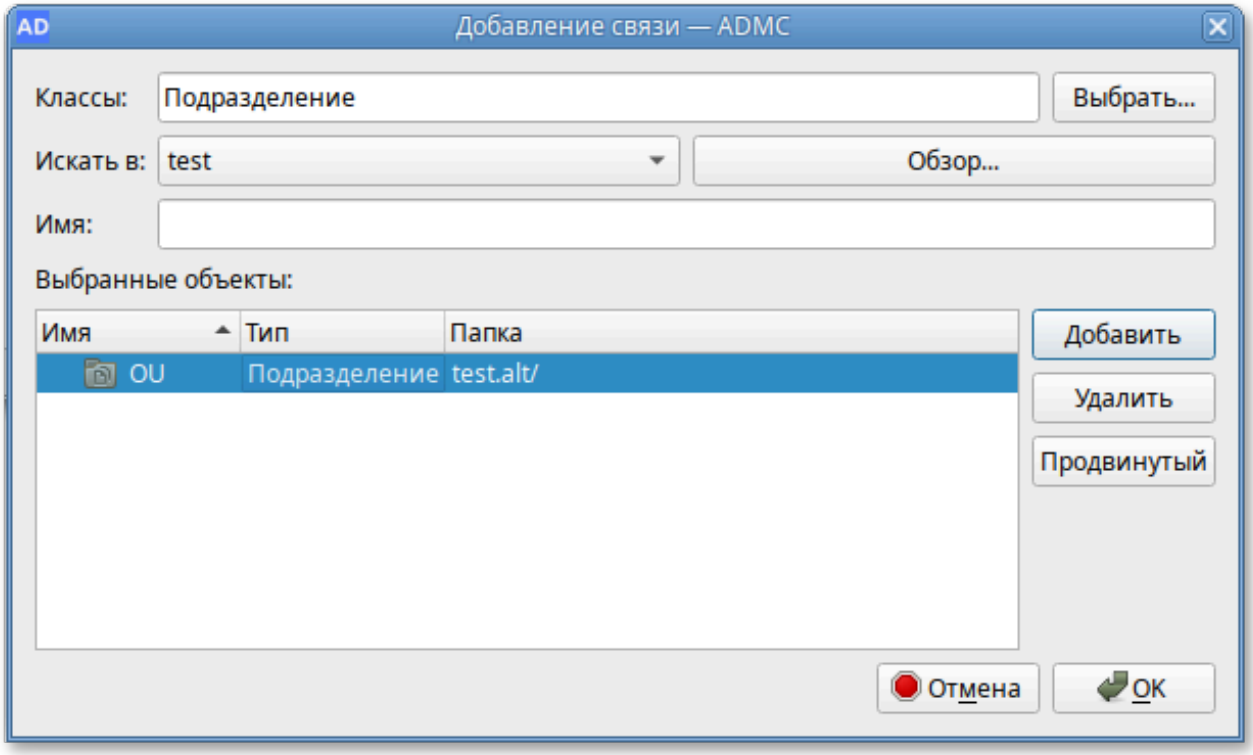


Рис. 206 – Добавление связи

Для удаления ссылки на объект групповой политики:

1) выбрать политику, которую следует изменить (в папке «Все политики» или в папке соответствующего OU);
2) в контекстном меню подразделения, связь с которым нужно отключить от политики, выбрать пункт «Удалить связь» (рис. 207).

Удалить связь между политикой и подразделением также можно, выбрав пункт «Удалить» в контекстном меню политики в подразделении, на которое она назначена (рис. 208).

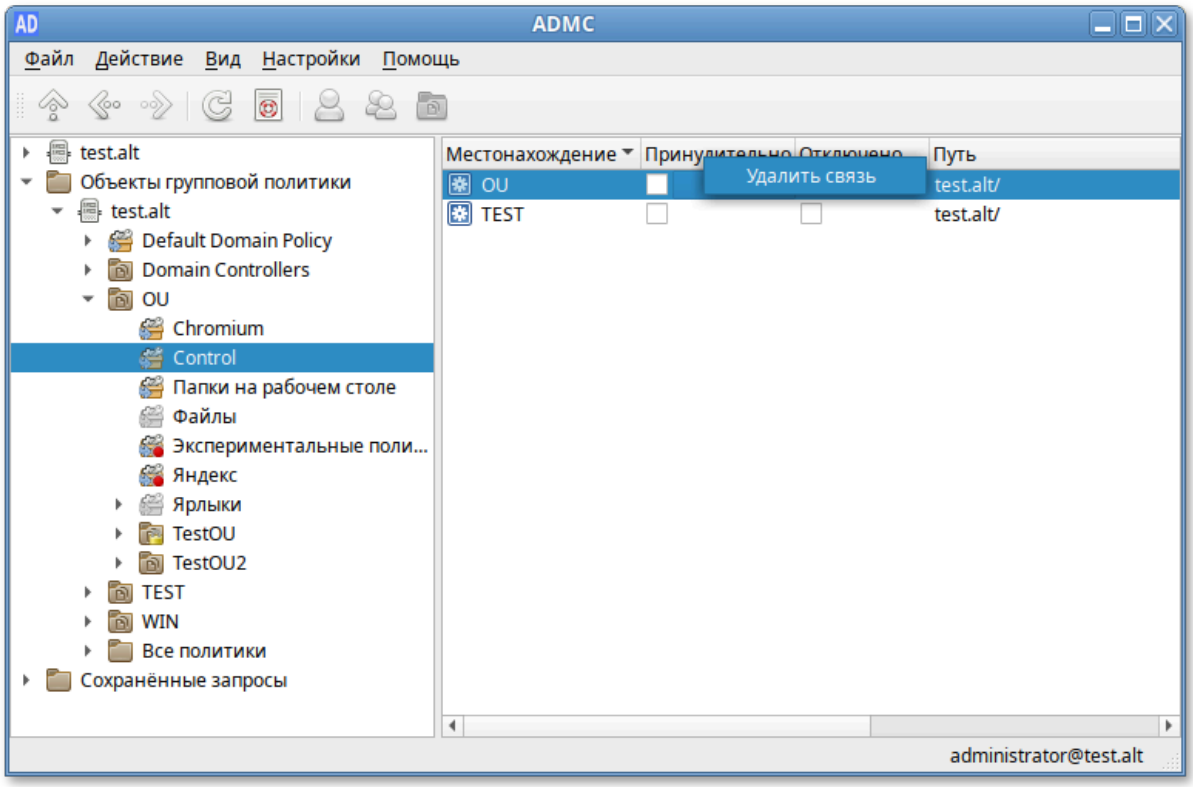


Рис. 207 – Пункт «Удалить связь»

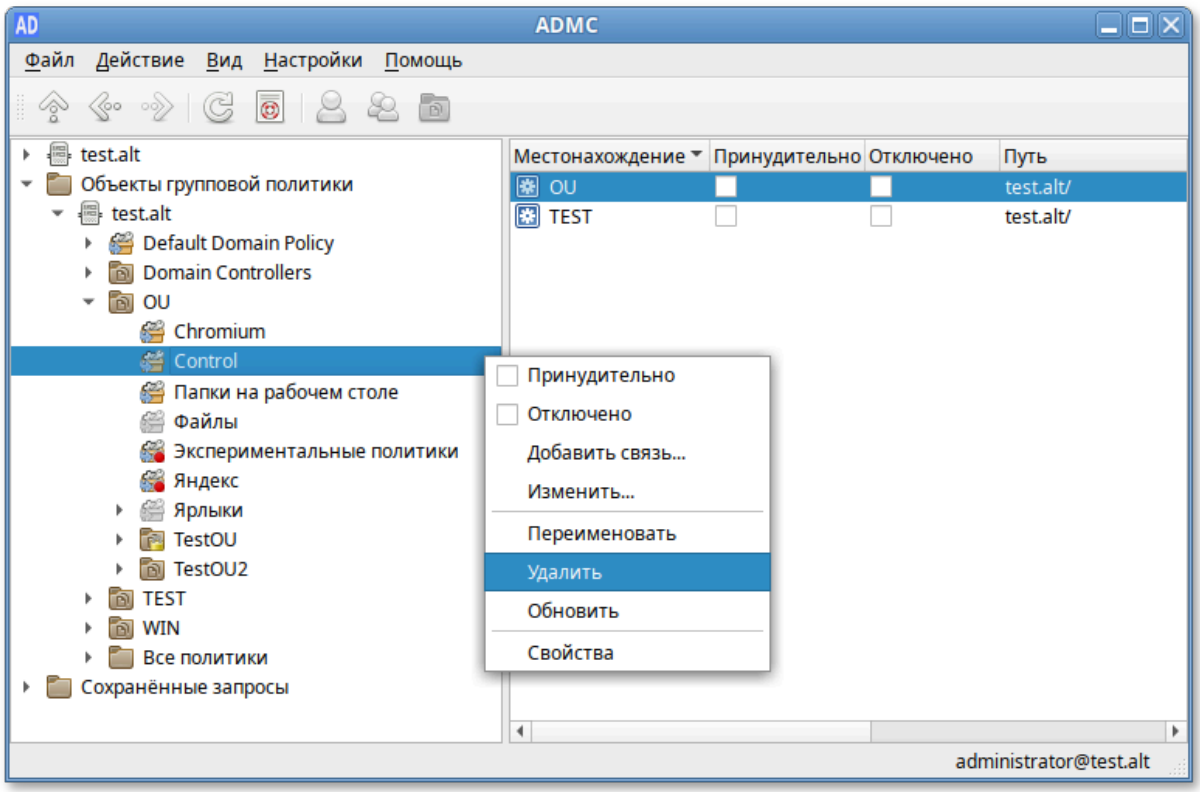


Рис. 208 – Удаление связи между политикой и подразделением

9.2.4.11.2.4 Параметры ссылки на объект групповой политики

В ADMC можно изменить параметры ссылки на объект групповой политики:

- опция «Принудительно» – принудительное применение политик более высокого уровня к объекту;
- опция «Отключено» – временно отключить связь политики с подразделением.

Чтобы отредактировать параметры ссылки, нужно (рис. 209):

1) выбрать политику, которую следует отредактировать;
2) на панели результатов найти подразделение, для которого нужно изменить параметры ссылки;
3) включить опцию «Принудительно», чтобы запретить переопределение параметров политик (см. п. 9.2.4.11.3). Политика, с включенной опцией «Принудительно», отображается в списке политик с красным кружком;
4) включить опцию «Отключено», чтобы временно отключить действие политики. Отключенная политика, в списке политик отображается серым цветом.

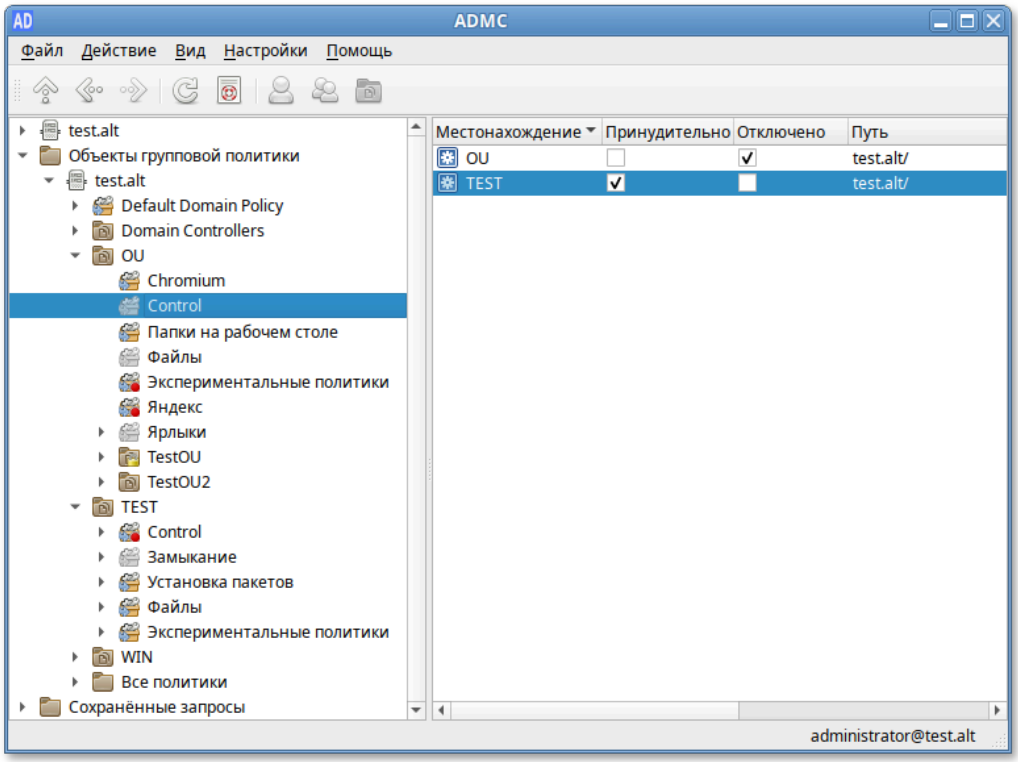


Рис. 209 – Редактирование параметров ссылки

Примечание. Если нужно, чтобы политика перестала действовать на клиентов в данном подразделении, можно либо удалить ссылку (при этом сама объект GPO не будет удален), либо временно отключить действие политики.

Включить/отключить опции «Принудительно» и «Отключено» также можно:

- в контекстном меню политики в подразделении (рис. 210);

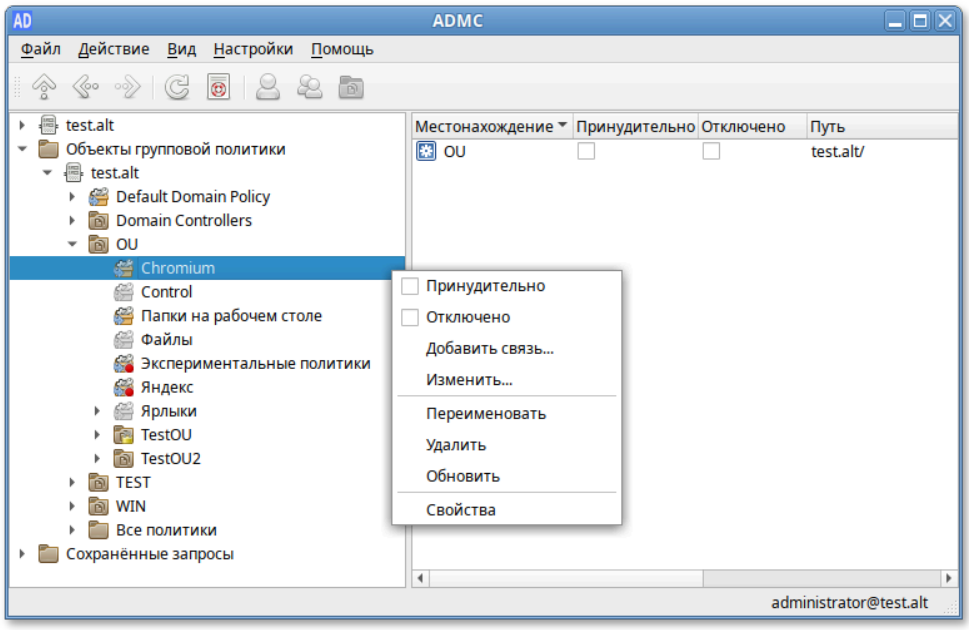


Рис. 210 – Включить/отключить опции «Принудительно» и «Отключено» в контекстном меню

- на вкладке Привязанные политики подразделения (рис. 211).

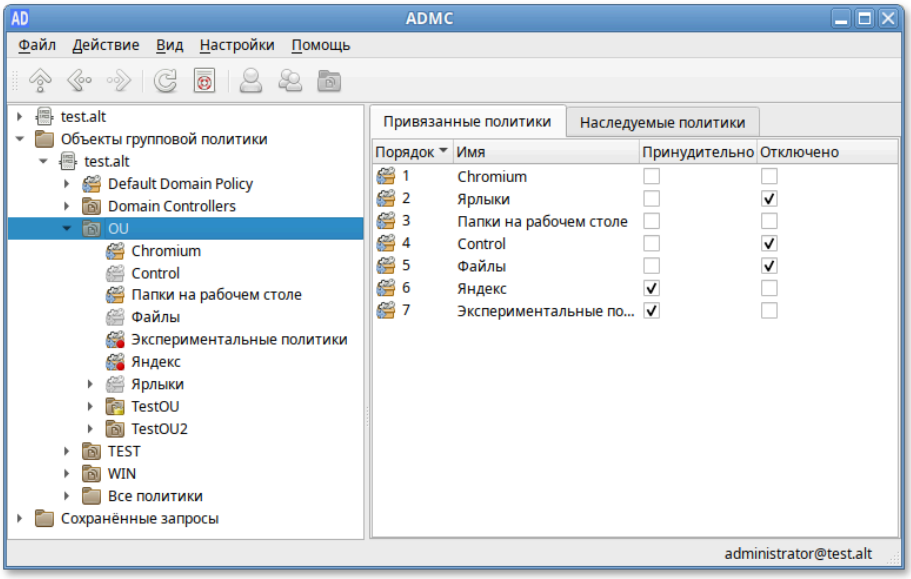


Рис. 211 – Включить/отключить опции «Принудительно» и «Отключено» на вкладке подразделения

9.2.4.11.2.5 Редактирование настроек групповой политики

Примечание. Для возможности редактирования настроек политики, на машине должен быть установлен модуль редактирования настроек клиентской конфигурации (GPUI).

Для изменения настроек политики нужно в контекстном меню политики выбрать пункт «Изменить…», будет запущен модуль редактирования настроек клиентской конфигурации, где можно изменить параметры групповой политики.

При создании каждого нового объекта групповой политики, в базе данных AD создается контейнер групповой политики (Group Policy Container, GPC). Для возможности просмотра контейнера групповой политики (это дочерний контейнер Policies контейнера System) в настройках ADMC должен быть отмечен пункт «Дополнительные возможности».

В AD контейнер групповой политики создается как тип groupPolicyContainer, причем его GUID можно увидеть в ADMC в столбце «Имя» (рис. 212).

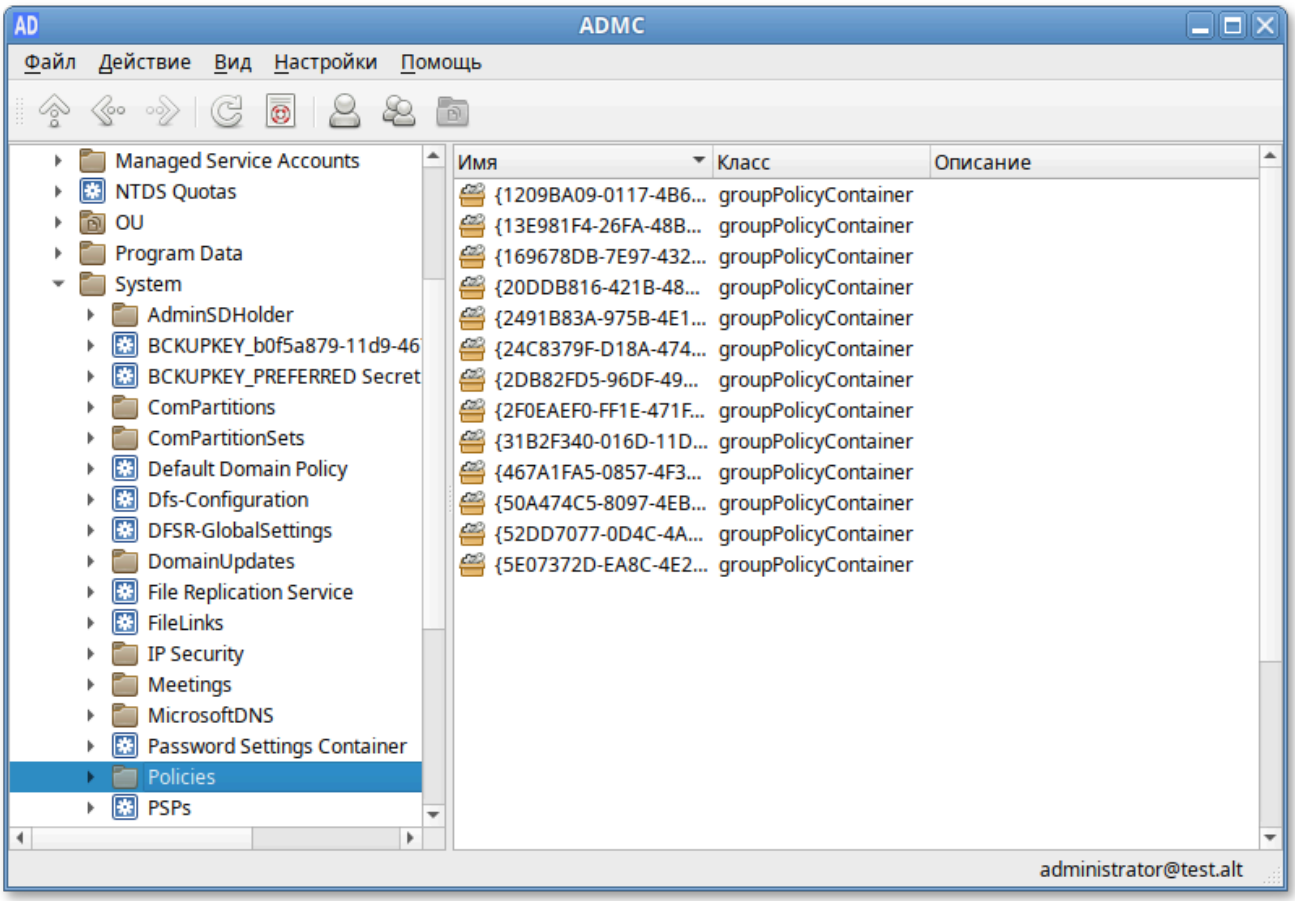


Рис. 212 – Столбец «Имя» в ADMC

Ниже перечислены некоторые атрибуты, позволяющие описать различные типы данных объекта групповой политики:

- `displayName` – атрибут, определяющий имя объекта групповой политики;
- `gPCFileSysPath` – атрибут, указывающий путь к расположению текущего шаблона групповой политики с соответствующим именем GUID;
- `gPCMachineExtensionNames` – атрибут, определяющий список расширений клиентской стороны конфигурации компьютера, используемых для обработки объекта групповой политики. Значение атрибута выглядит следующим образом: [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{D02B1F72-3407-48AE-BA88-E8213C6761F1}], что представляет собой [{GUID CSE-расширения}{GUID расширения MMC}{GUID второго расширения MMC}][GUID-идентификаторы последующих CSE- и MMC-расширений];
- `gPCUserExtensionNames` – атрибут, определяющий список расширений клиентской стороны конфигурации пользователя, используемых для обработки объекта групповой политики;
- `versionNumber` – в этом атрибуте определен номер версии контейнера GPC объекта групповой политики, который, для осуществления синхронизации двух объектов, должен быть идентичным с номером версии шаблона групповой политики;
- `flags` – состояние объекта групповой политики: объект GPO включен (значение 0), отключен раздел «Конфигурация пользователя» (значение 1), отключен раздел «Конфигурация компьютера» (значение 2), объект GPO полностью отключен (значение 3).

Примечание. Вручную изменять атрибуты объекта групповой политики не рекомендуется.

9.2.4.11.3. Блокирование наследования

Для того чтобы параметры групповой политики, определенные на уровне вышестоящих контейнеров, не распространялись на содержимое конфигурируемого контейнера нужно выполнить одно из следующих действий:

1) в контекстном меню контейнера, к которому привязан объект групповой политики, установить отметку «Блокировать наследование» (рис. 213);

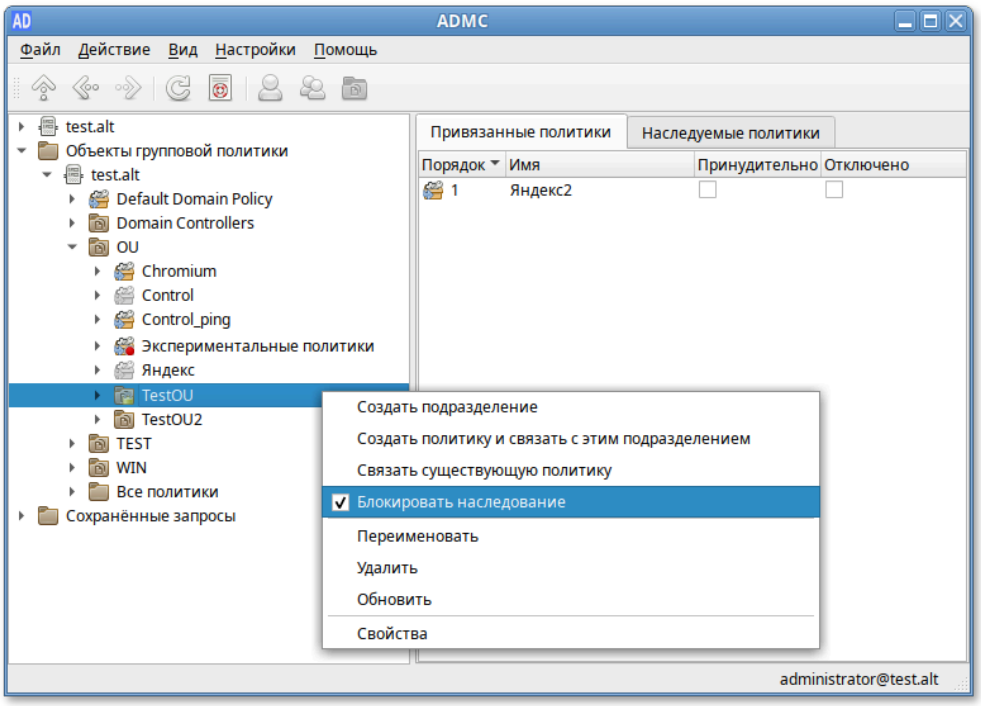


Рис. 213 – Отметка «Блокировать наследование»

2) в окне свойств контейнера, к которому привязан объект групповой политики, на вкладке «Групповая политика» установить отметку «Заблокировать наследование политик» (рис. 214);

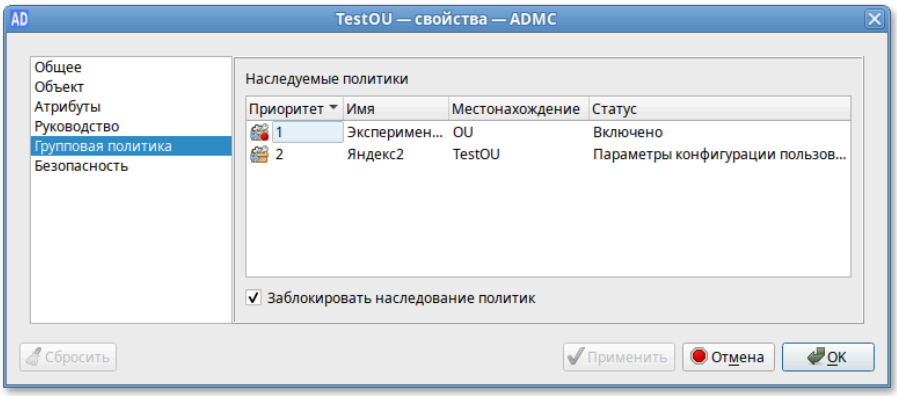


Рис. 214

3) так как администратор домена может не согласиться с тем, что администратор подразделения блокирует параметры политики домена, существует возможность запретить переопределение параметров с помощью отметки «Принудительно» (рис. 215).

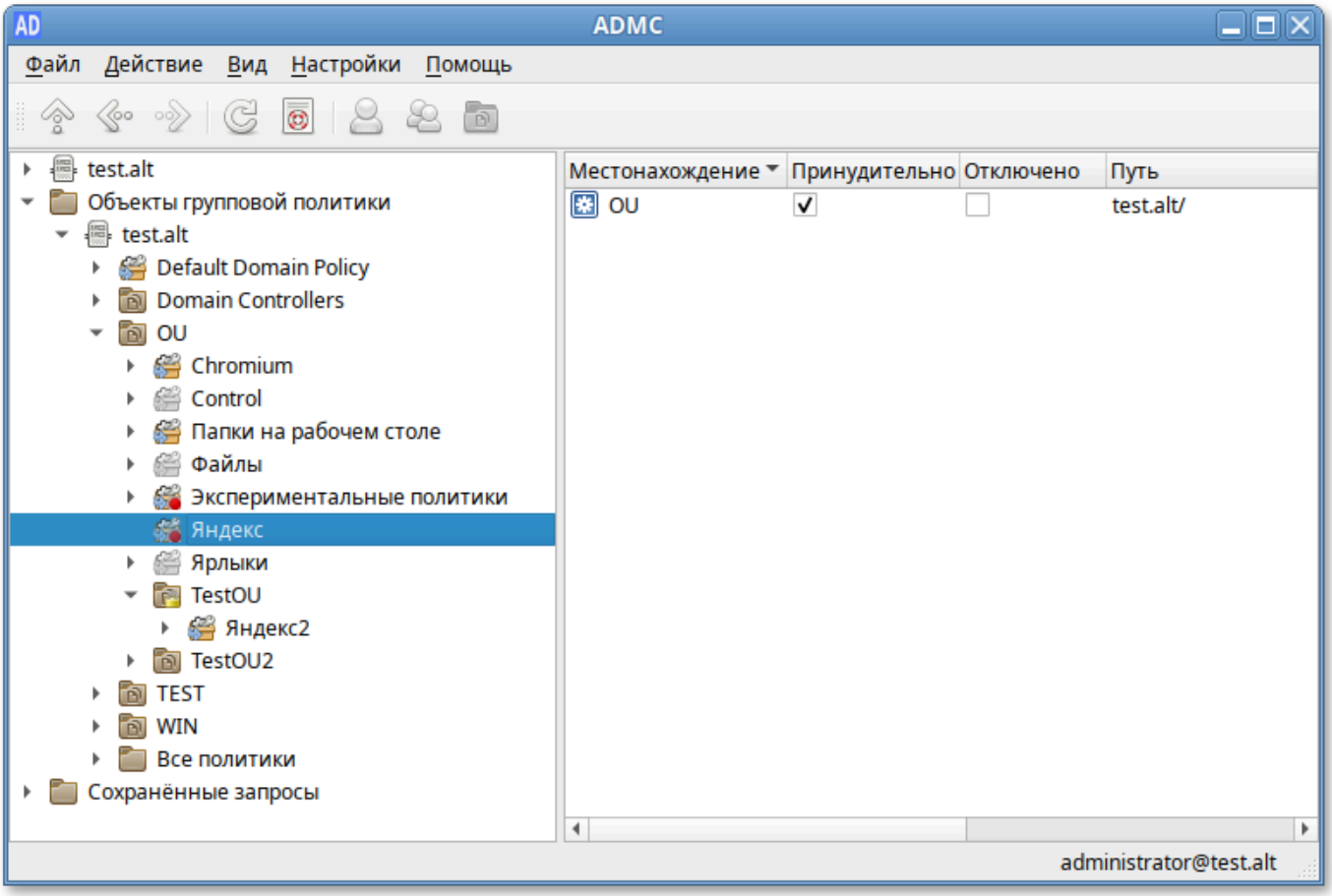


Рис. 215 – Переопределение параметров с помощью отметки «Принудительно»

Отметка в поле «Принудительно» означает, что связь установлена принудительно. Это приведет к принудительному применению политик более высокого уровня к объектам более низкого уровня, например, применение политики домена ко всем дочерним подразделениям, или применения политики сайта ко всем доменам и подразделениям в пределах сайта.

При использовании параметра «Принудительно» выигрывает та политика, которая находится выше в иерархии домена (например, при включении «Принудительно» у политики Default Domain Policy, она выигрывает у всех других групповых политик).

Примечание. Подразделение с блокированным наследованием отображается в дереве консоли со значком замка.

После установки параметра «Принудительно», на значке групповой политики появится красный кружок, означающий, что для данной политики запрещено переопределение параметров (рис. 216).

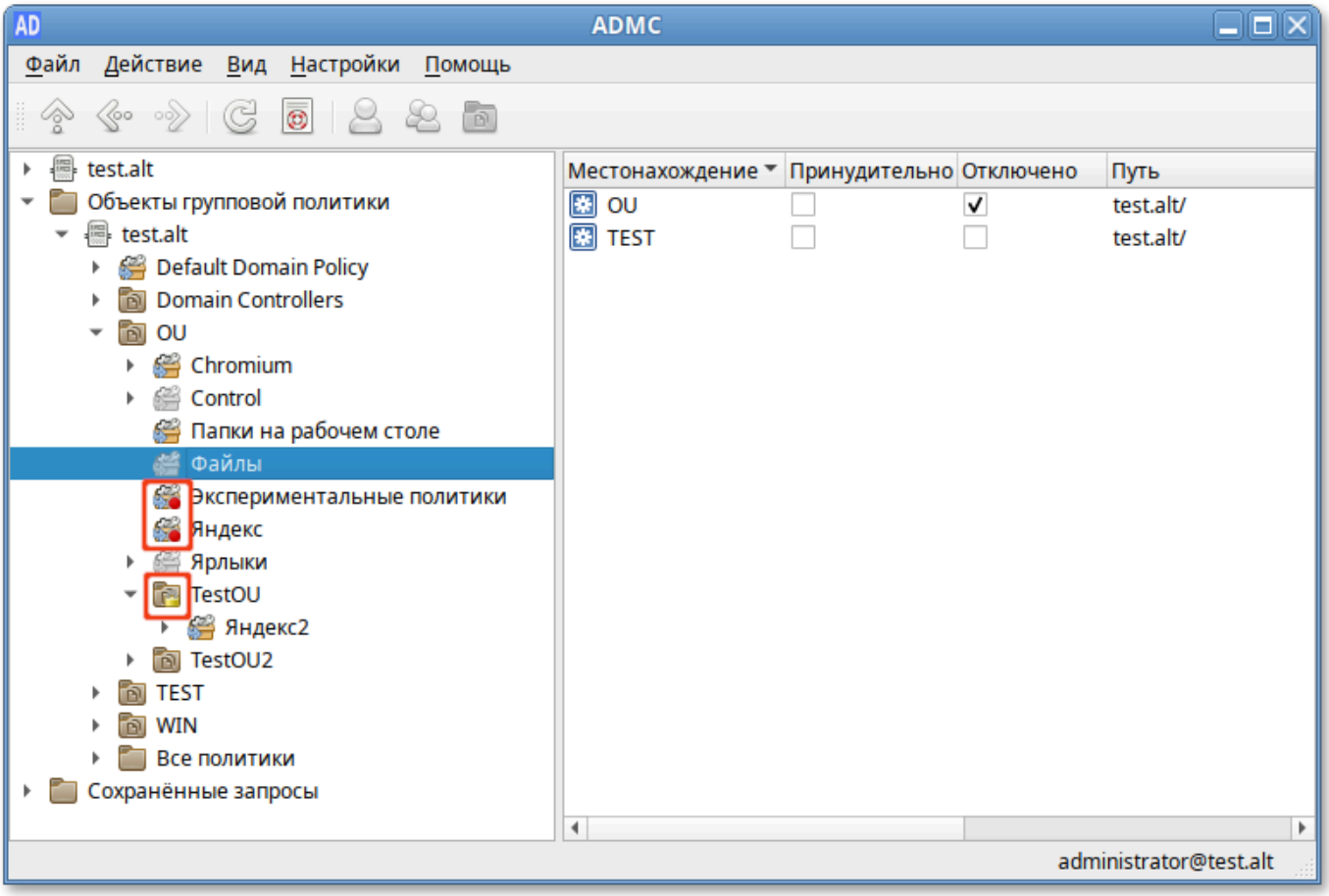


Рис. 216 – Запрет переопределения параметров

На вкладке «Наследуемые политики» подразделения можно увидеть, какие политики применяются к подразделению, а также местонахождение политики (рис. 217).

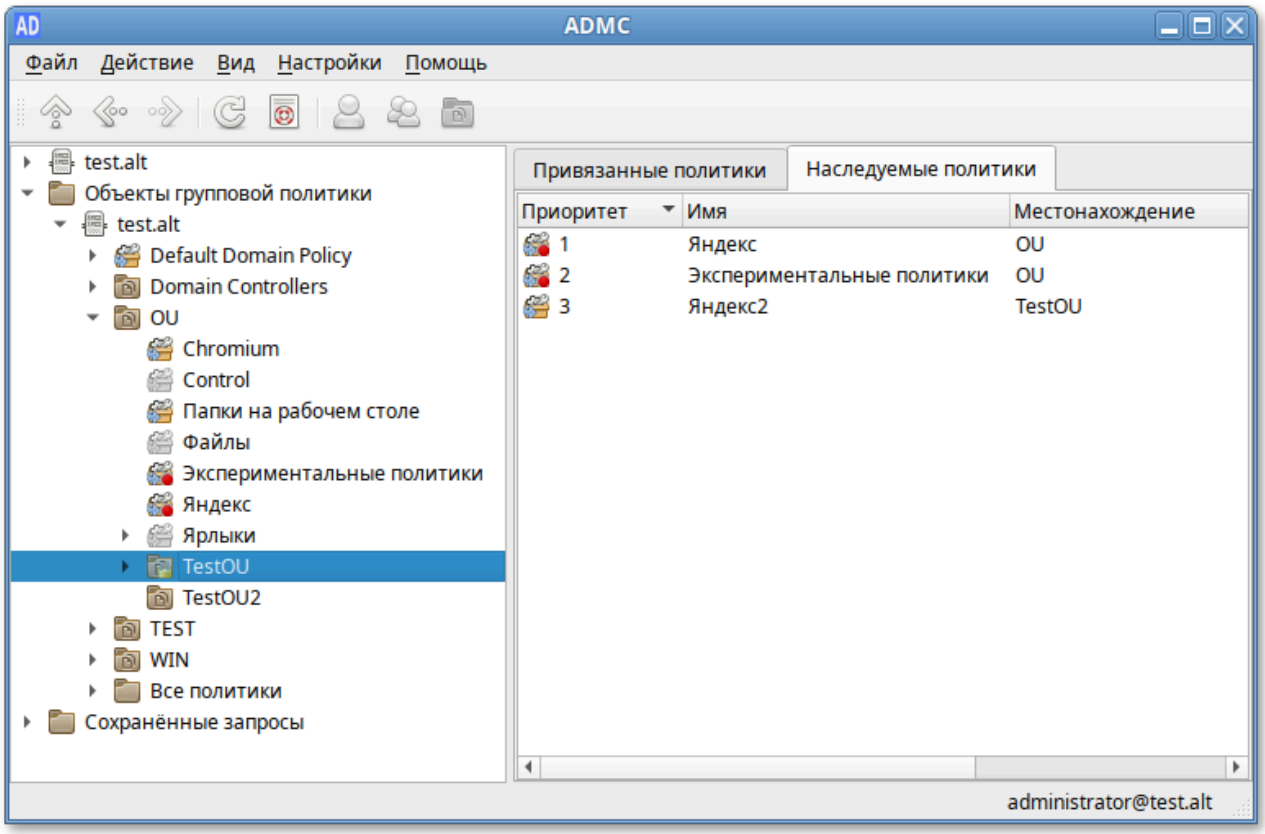


Рис. 217 – Вкладка «Наследуемые политики»

9.2.4.12. Добавление/Удаление UPN суффиксов

UserPrincipalName (UPN) – имя для входа пользователя в формате e-mail-адреса, например, ivanov@test.alt. Здесь ivanov это UPN-префикс (имя пользователя в домене AD), test.alt – UPN-суффикс. По умолчанию в AD в качестве UPN-суффикса используется DNS имя домена AD. Добавление дополнительных имен доменов позволяет упростить процесс входа и повысить безопасность.

Для того чтобы добавить/удалить дополнительный UPN-суффикс, нужно выполнить следующие шаги:

1) в контекстном меню домена выбрать пункт «Изменить суффиксы UPN» (рис. 218);
2) в открывшемся диалоговом окне нажать кнопку «Добавить…» (рис. 219);

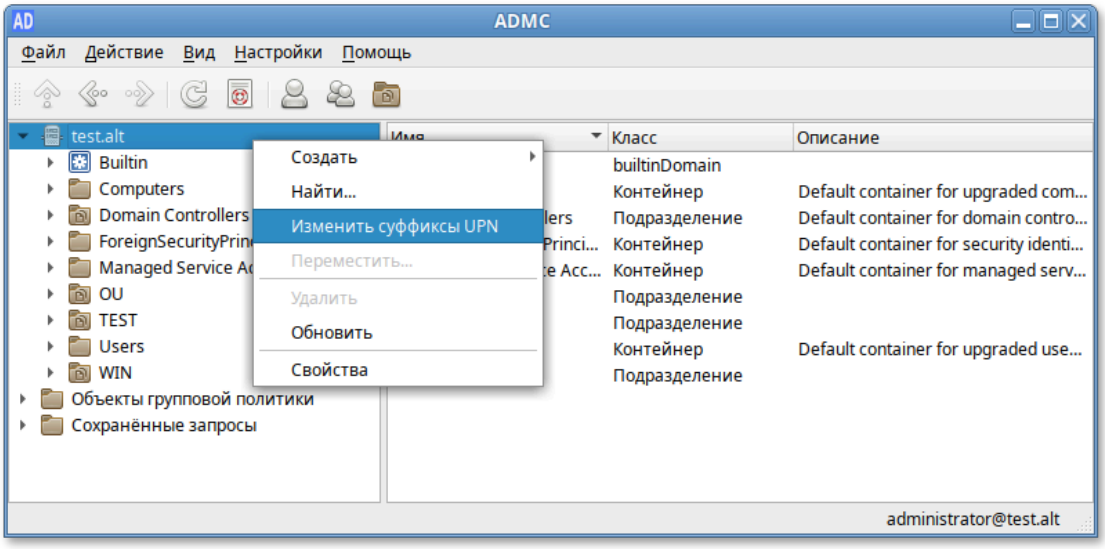


Рис. 218 – Пункт «Изменить суффиксы UPN»

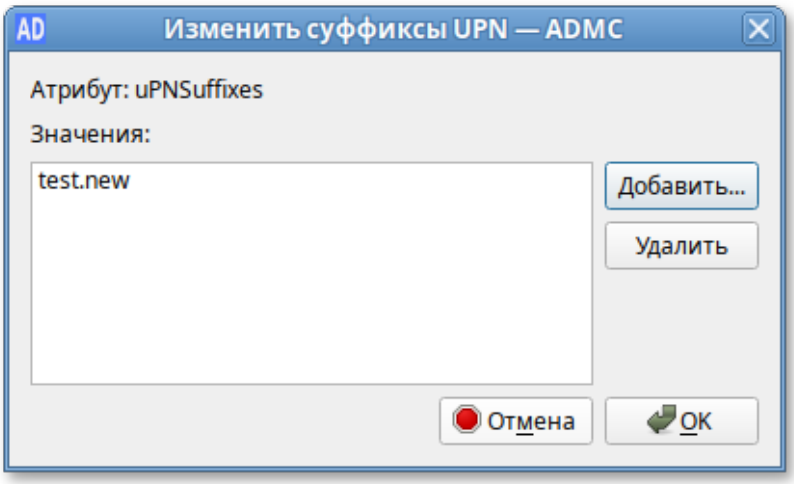


Рис. 219 – Кнопка «Добавить…»

3) ввести альтернативный суффикс (рис. 220).

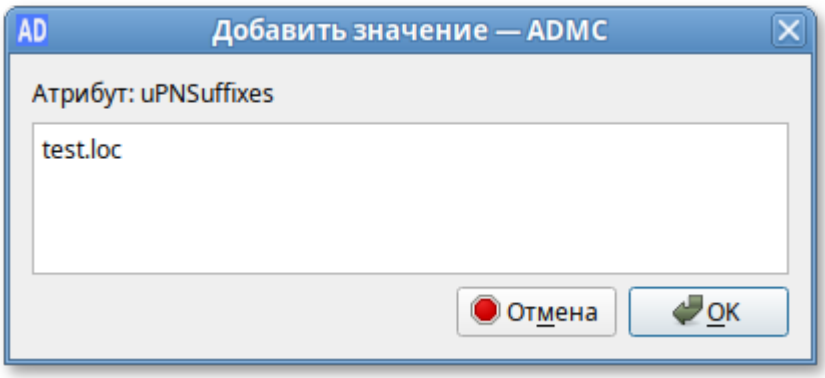


Рис. 220 – Введение альтернативного суффикса

Не требуется, чтобы суффикс UPN был действительным DNS-именем домена. Суффиксы UPN должны соответствовать условиям DNS-имен в отношении допустимых символов и синтаксиса.

1) нажать кнопку «ОК», чтобы добавить новый суффикс в список;
2) чтобы удалить существующий суффикс, нужно выбрать его в списке и нажать кнопку «Удалить» (рис. 221).

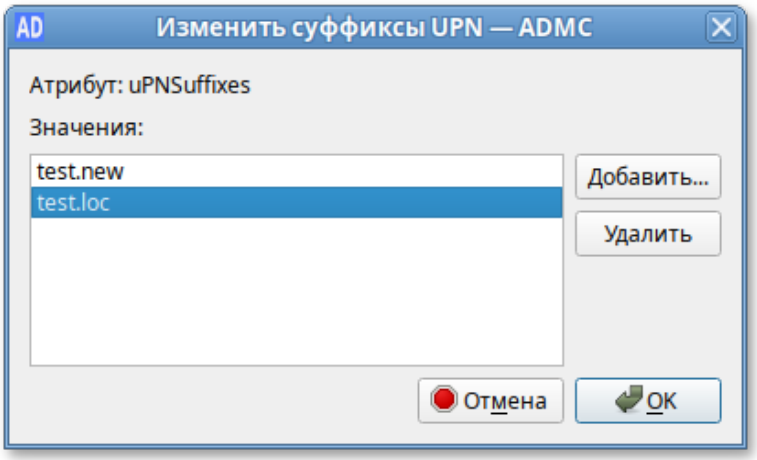


Рис. 221 – Удаление существующего суффикса

9.2.4.13. Роли FSMO

FSMO, или Flexible single-master operations (операции с одним исполнителем) – это операции, выполняемые контроллерами домена AD, которые требуют обязательной уникальности сервера для каждой операции. В зависимости от типа операции уникальность FSMO подразумевается в пределах одного домена

или леса доменов. Различные типы FSMO могут выполняться как на одном, так и на нескольких контроллерах домена. Выполнение FSMO сервером называют ролью сервера, а сами сервера – хозяевами операций.

Для просмотра текущего владельца роли нужно выбрать пункт меню «Файл» → «Мастера Операций». В открывшемся окне в списке слева выбрать роль и в поле «Текущий мастер» будет показан владелец роли (рис. 222).

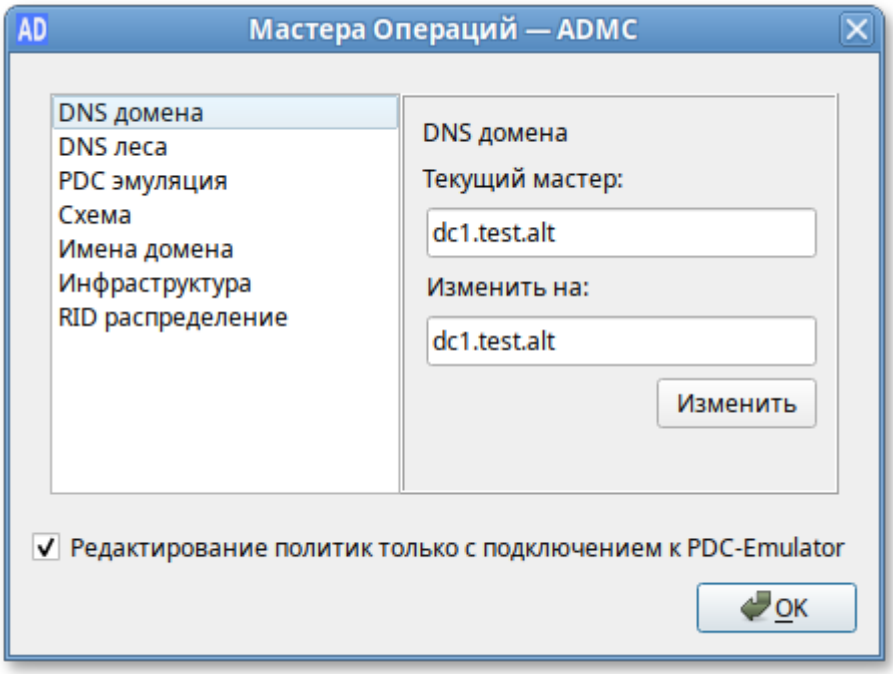


Рис. 222 – Поле «Текущий мастер»

Список возможных ролей:

1) «DNS домена» – Domain DNS Zone Master role;

2) «DNS леса» – Forest DNS Zone Master role;

3) «PDC эмуляция» – эмулятор PDC;

4) «Схема» – хозяин схемы;

5) «Имена домена» – хозяин именования доменов;

6) «Инфраструктура» – хозяин инфраструктуры;

7) «RID распределение» – хозяин RID.

Если отмечен пункт «Редактирование политик только с подключением к PDC-Emulator», при отсутствии подключения к контроллеру домена с ролью PDC-эмуляции, действия, затрагивающие шаблоны групповых политик

(редактирование/изменение/удаление политик) будут запрещены, появится сообщение, показанное на рис. 223.

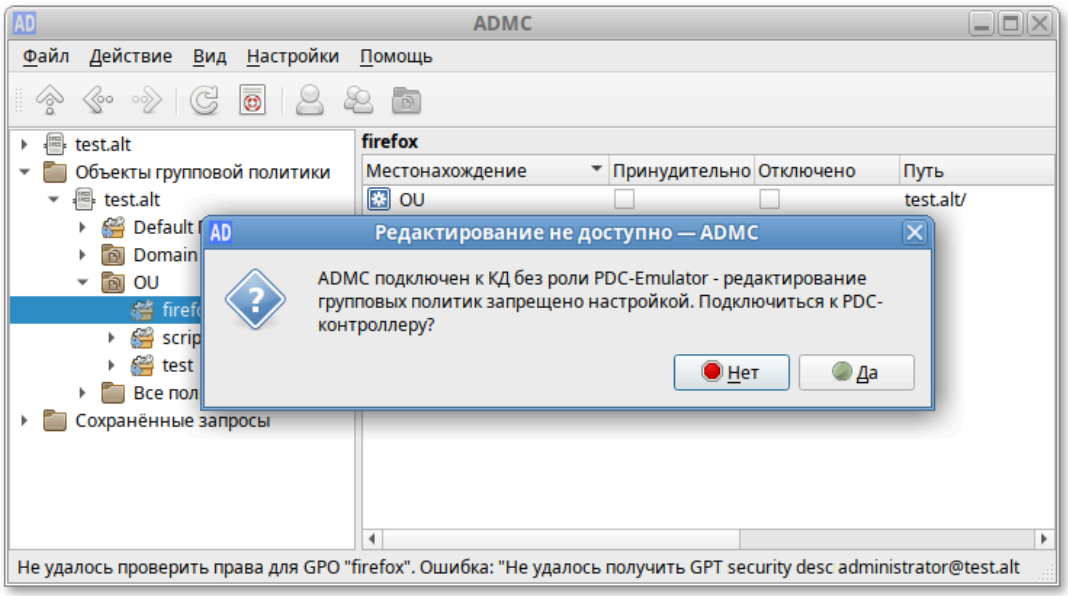


Рис. 223 – Окно «Редактирование не доступно»

Для штатной передачи роли нужно выполнить следующие действия:

1) в окне «Параметры подключения – ADMC» («Файл» → «Параметры подключения») выбрать контроллер домена, который должен стать новым владельцем роли и нажать кнопку «ОК» (рис. 224);

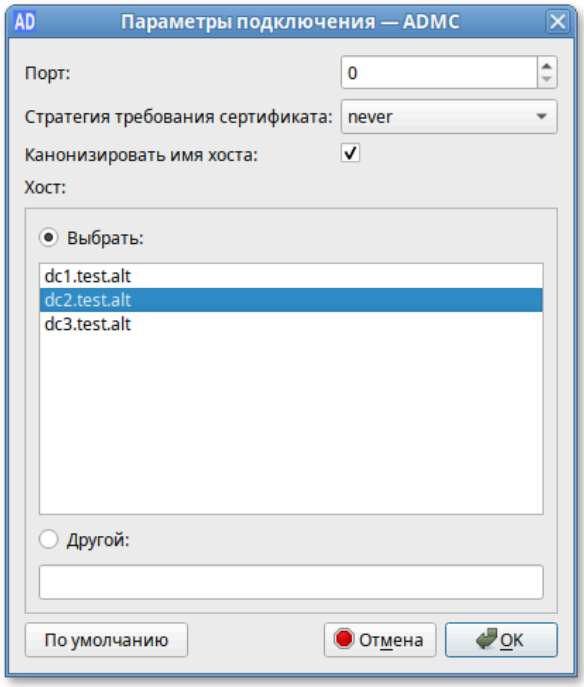


Рис. 224 – Окно «Параметры подключения – ADMC»

2) в окне «Мастера Операций – ADMC» («Файл» → «Мастера Операций») выбрать роль (при этом в поле «Текущий мастер» будет показан текущий владелец роли, а в поле «Изменить на» – контроллер домена, который должен стать новым владельцем роли) и нажать кнопку «Изменить» (рис. 225).

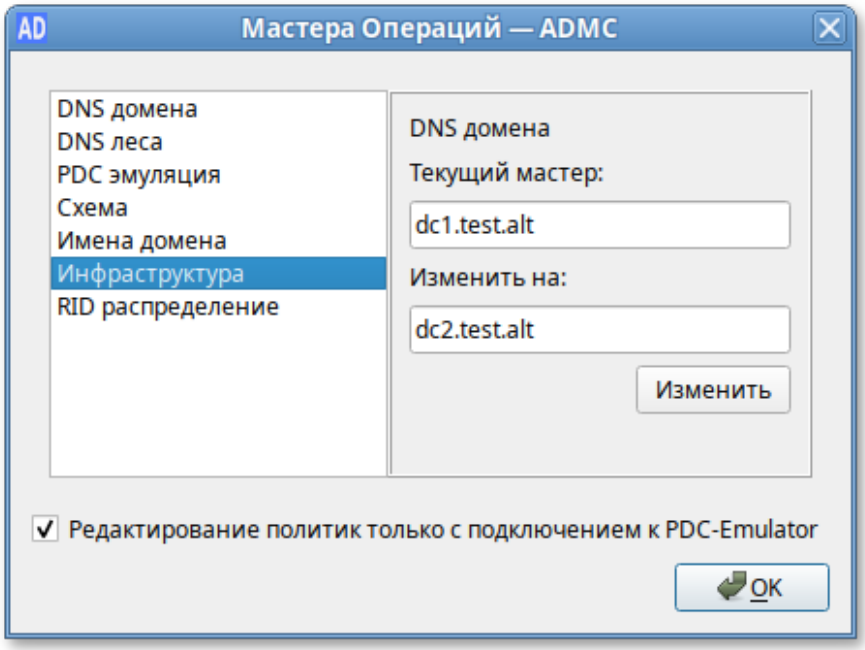


Рис. 225 – Окно «Мастера Операций – ADMC»

Владелец роли будет изменен (рис. 226).

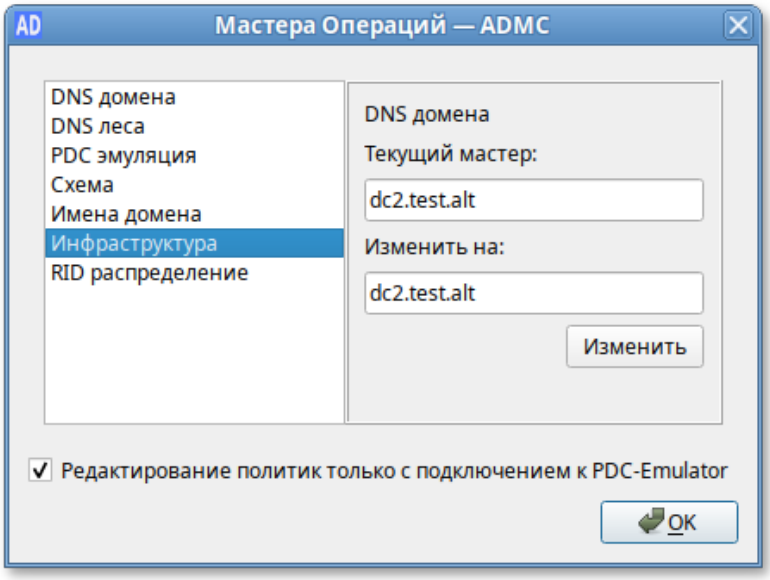


Рис. 226 – Вкладка «Инфраструктура»

9.2.4.14. Выбор объектов

Выбор объектов осуществляется в диалоговом окне «Выбрать объекты – ADMC». Доступ к этому диалоговому окну можно получить из разных мест, например, при выборе действия «Добавить в группу…» в контекстном меню учетной записи пользователя (рис. 227).

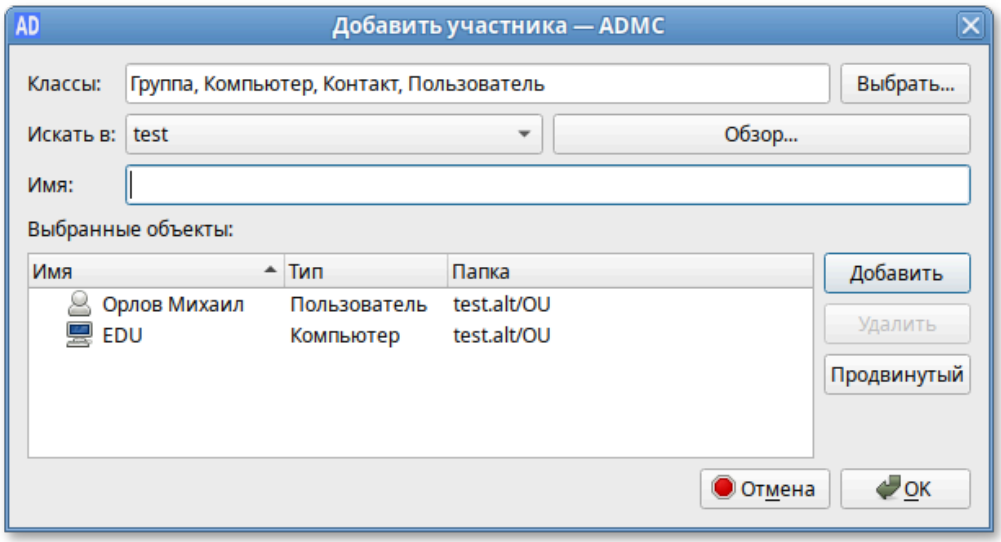


Рис. 227 – Добавление участника

Для выбора объекта достаточно указать класс объекта, выбрать расположение, с которого требуется начать поиск и в поле «Имя» ввести имена объектов:

1) в поле «Классы», нажав кнопку «Выбрать…», выбрать типы объектов, которые будут использоваться для поиска (в большинстве случаев это поле будет заполнено автоматически, в зависимости от контекста задачи);
2) в поле «Искать в» выбрать объект, который будет использоваться в качестве основы для поиска;
3) в поле «Имя» ввести имя объекта (можно ввести часть имени или выполнить поиск по имени для входа);
4) нажать кнопку «Добавить» для поиска объекта по названию;
5) если объект найден, он будет добавлен в список найденных объектов;
6) если объект не найден, исправить имя и повторить попытку;
7) если есть несколько совпадений, откроется диалоговое окно, в котором можно выбрать одно или несколько совпадений (рис. 228);

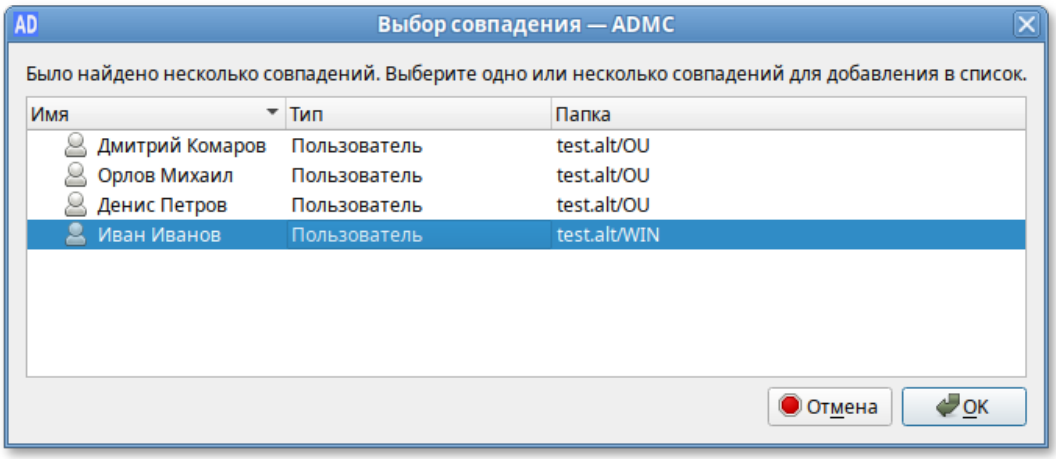


Рис. 228 – Выбор совпадения

8) если объект не найден, исправить имя и повторить попытку;
9) повторить пункты 1) – 7), пока не будут добавлены все объекты;
10) чтобы удалить объект из списка, нужно выбрать объект и нажать кнопку «Удалить»;
11) для выбора объектов можно также использовать продвинутый поиск, который можно открыть, нажав кнопку «Продвинутый».

9.2.4.15. Поиск объектов

Поиск объектов осуществляется в диалоговом окне «Поиск объектов – ADMC». Доступ к этому диалоговому окну можно получить, выбрав пункт «Найти…» в меню «Действие» или в контекстном меню контейнера (рис. 229).

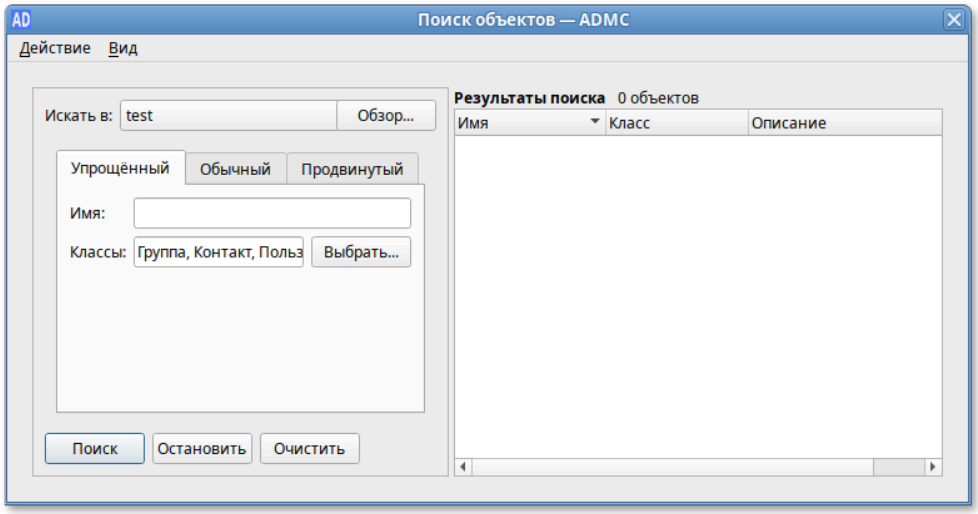


Рис. 229 – Поиск объектов

Поиск объектов в домене возможен по разным критериям:

- по типу и имени (простой поиск) – вкладка «Упрощенный»;

- по атрибутам – вкладка «Обычный»;

- в синтаксисе запросов LDAP – вкладка «Продвинутый».

Примечание. В диалоговом окне, вызываемом меню «Вид» → «Настроить колонки» можно выбрать поля, которые будут отображаться в списке результатов поиска (рис. 230).

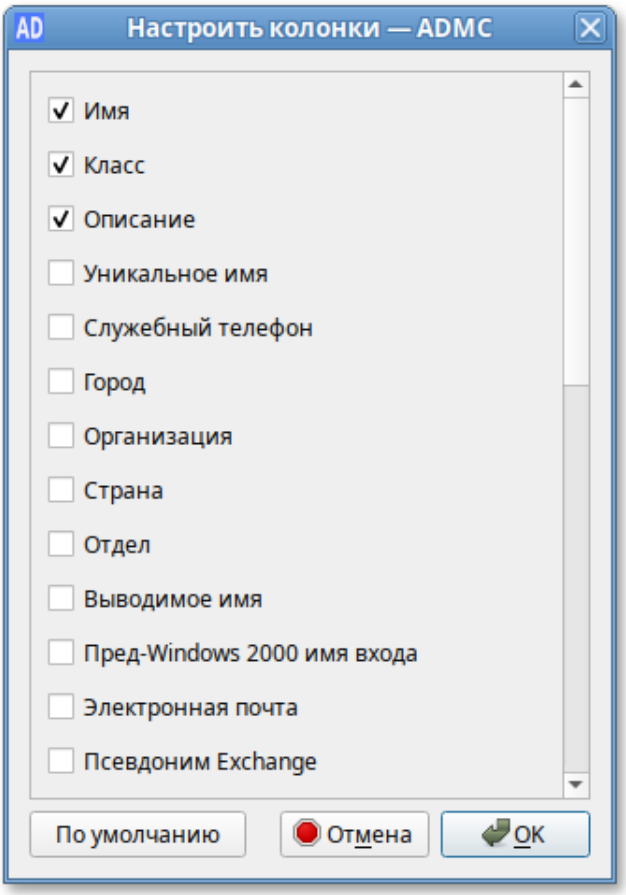


Рис. 230 – Меню «Вид» → «Настроить колонки»

9.2.4.15.1. Простой поиск

Процедура простого поиска:

1) в диалоговом окне «Поиск объектов – ADMC» выбрать вкладку «Упрощенный» (рис. 231);

2) в поле «Классы», нажав кнопку «Выбрать…», выбрать классы объектов для поиска (рис. 232);

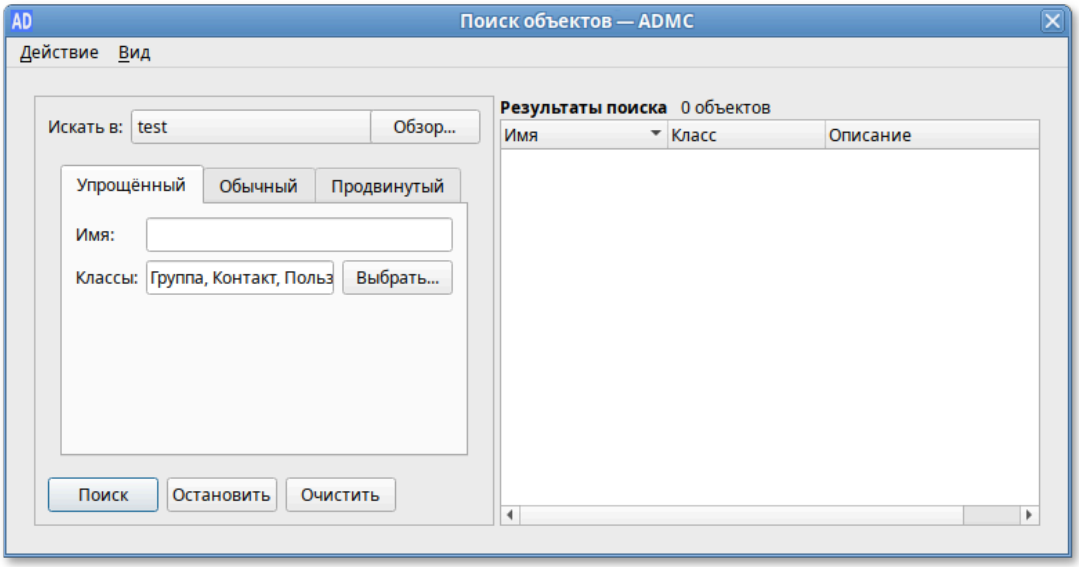


Рис. 231 – Вкладка «Упрощенный»

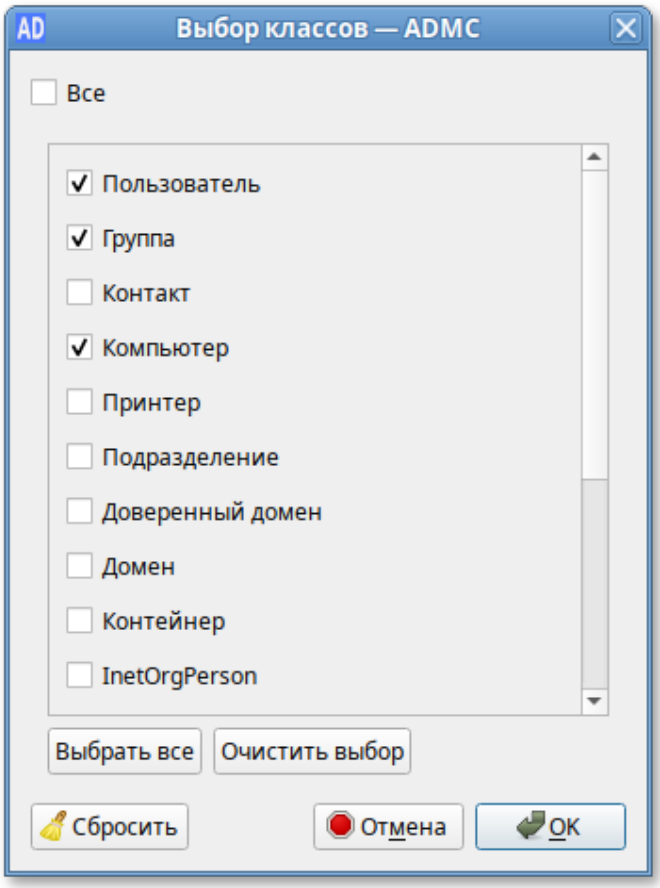


Рис. 232 – Выбо классов объектов для поиска

3) в поле «Имя» ввести имя объекта и нажать кнопку «Поиск» (рис. 233).

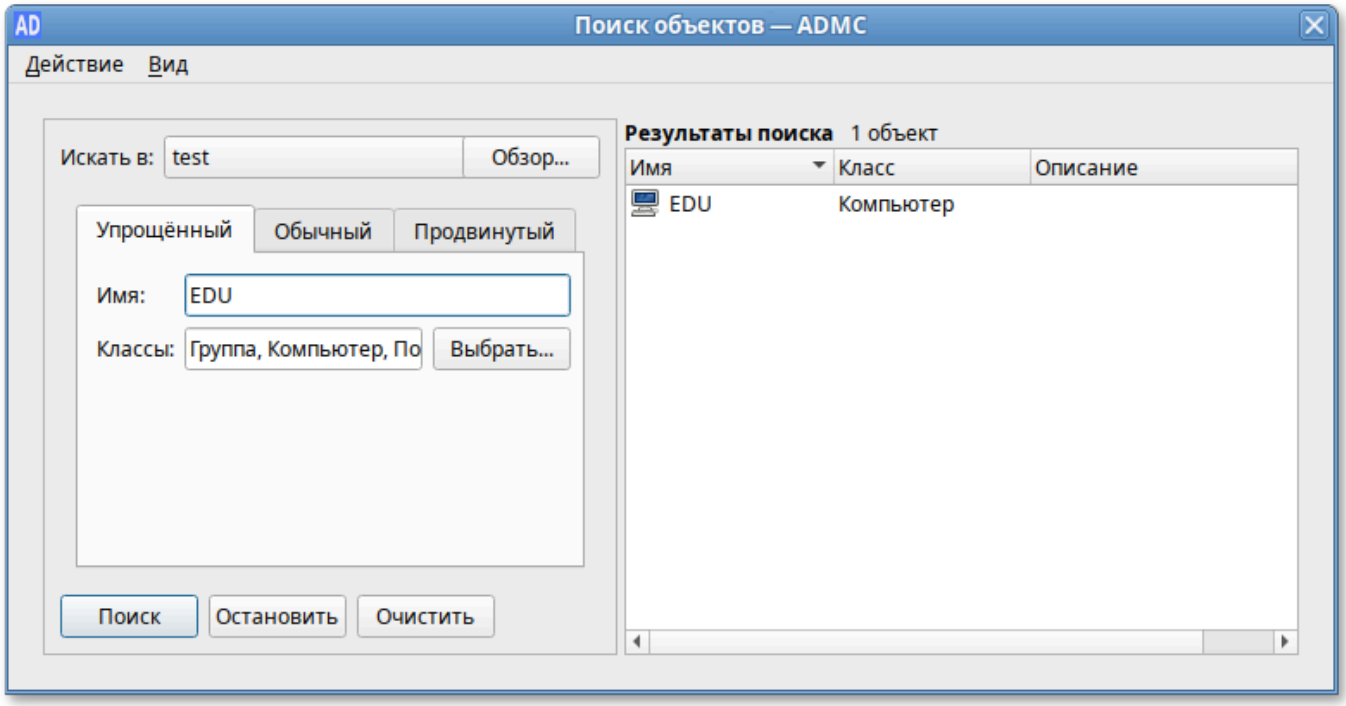


Рис. 233 – Поле «Имя»

9.2.4.15.2. Обычный поиск

При использовании обычного поиска создаются фильтры, определяющие критерии поиска:

1) в диалоговом окне «Поиск объектов – ADMC» выбрать вкладку «Обычный» (рис. 234);

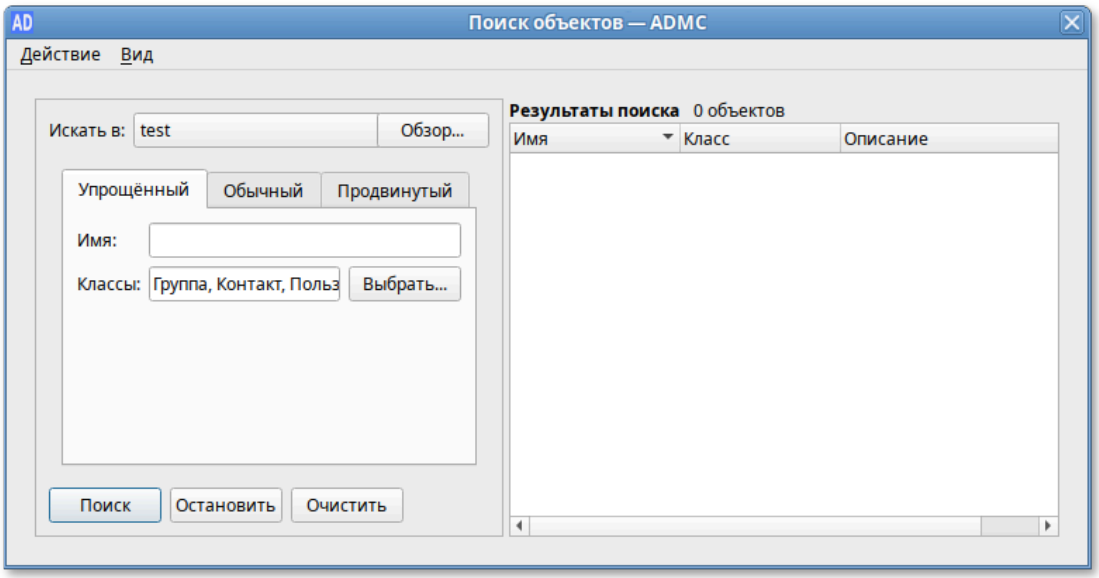


Рис. 234 – Вкладка «Обычный»

2) в поле «Классы», нажав кнопку «Выбрать…», выбрать классы объектов для поиска (рис. 235);

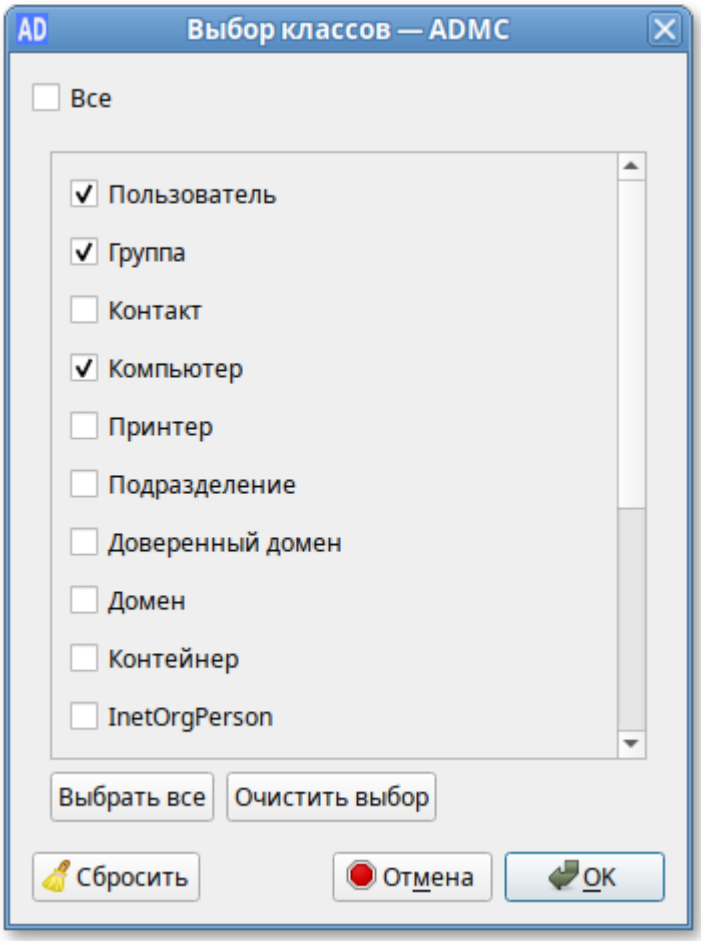


Рис. 235 – Выбор классов объектов для поиска

3) создать фильтр:
   - в списке «Класс атрибута» выбрать класс атрибута;
   - в списке «Атрибут» выбрать атрибут (список атрибутов зависит от выбранного класса атрибутов);
   - в списке «Состояние» выбрать условие, которое будет использоваться для фильтра;
   - в поле «Значение» ввести значение условия (не для всех условий нужно вводить значения);
4) нажать кнопку «Добавить»;
5) повторить пункты 2) – 3), чтобы добавить больше фильтров (фильтры для создания критериев поиска объединяются логическим И);

6) нажать кнопку «Удалить», если нужно удалить фильтр из списка;

7) нажать кнопку «Очистить», если нужно очистить список фильтров;

8) нажать кнопку «Поиск» (рис. 236).

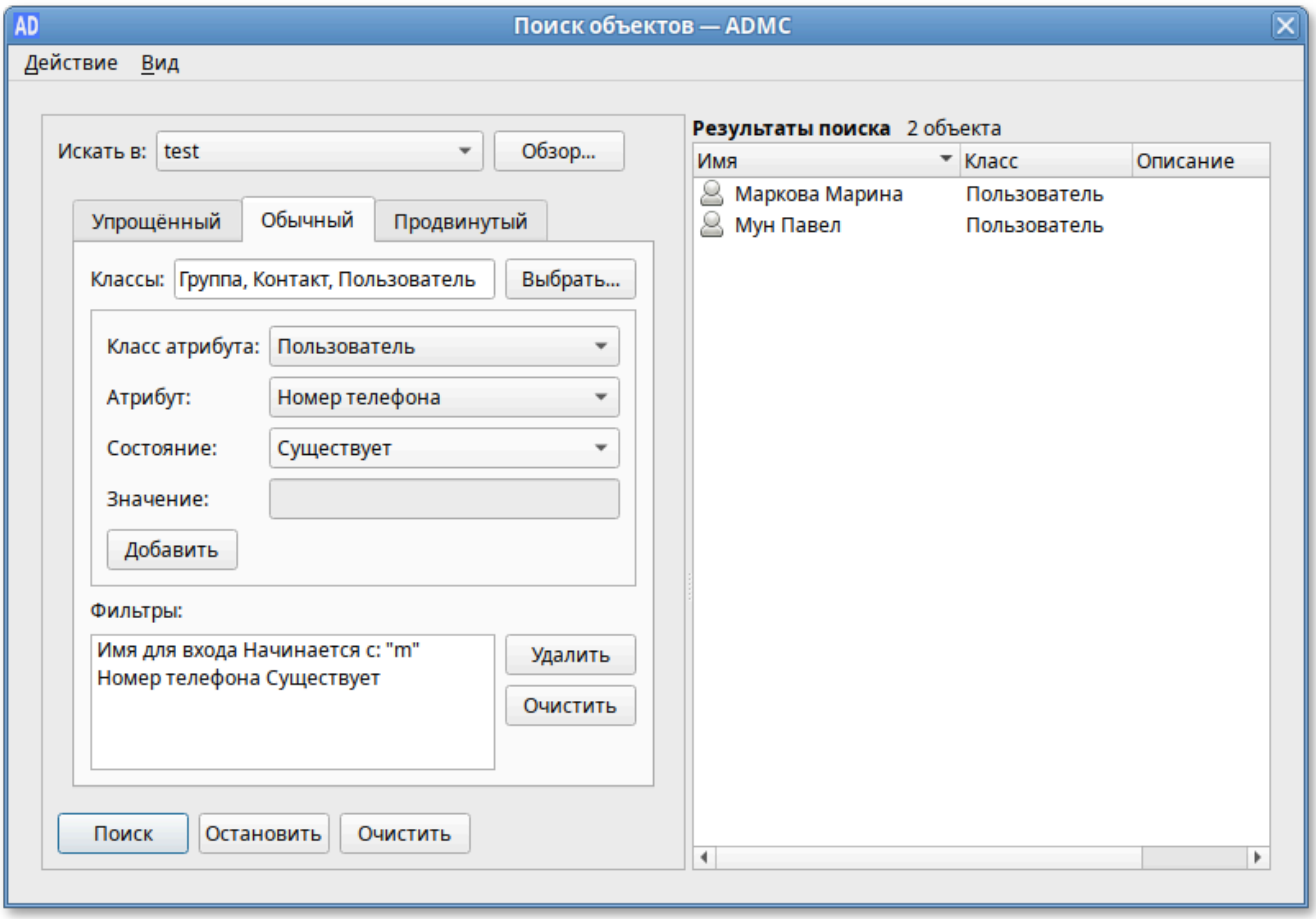


Рис. 236 – Поиск

9.2.4.15.3. Продвинутый поиск

Продвинутый поиск предполагает использование LDAP-фильтров.

Использование LDAP-фильтров является наиболее эффективным способом поиска объектов в AD.

Синтаксис LDAP-фильтра имеет вид:

```
<Фильтр>=(<Атрибут><оператор сравнения><значение>)
```

При наличии нескольких условий поиска фильтры можно комбинировать с помощью логических операторов.

Процедура продвинутого поиска:

1) в диалоговом окне «Поиск объектов – ADMC» выбрать вкладку «Продвинутый» (рис. 237);

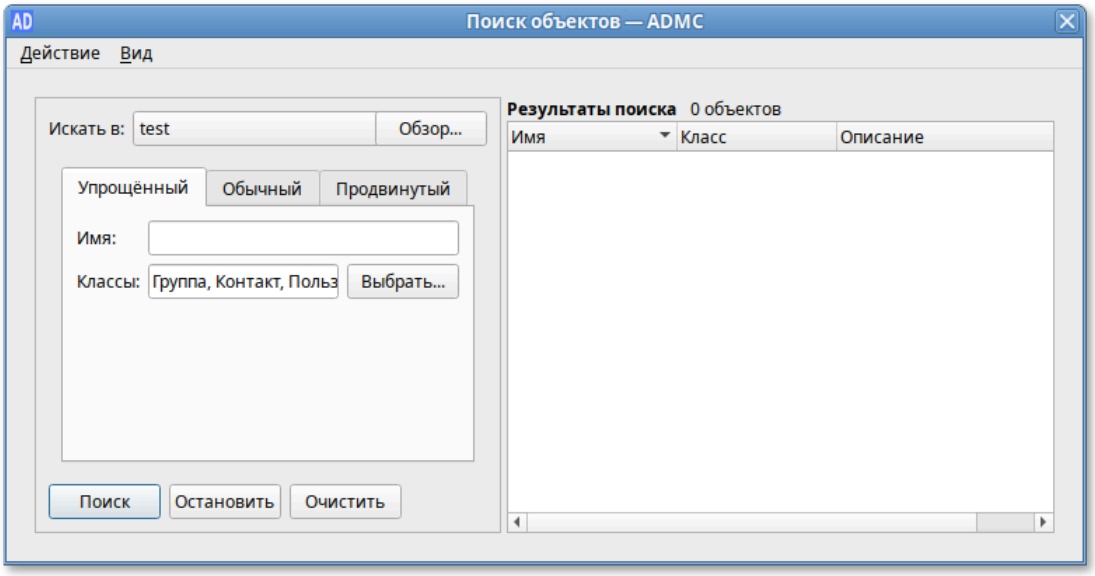


Рис. 237 – Вкладка «Продвинутый»

2) в поле «Искать в» выбрать область поиска (можно воспользоваться кнопкой «Обзор»);

3) ввести LDAP-фильтр в поле «Введите фильтр LDAP»;

4) нажать кнопку «Поиск» (рис. 238).

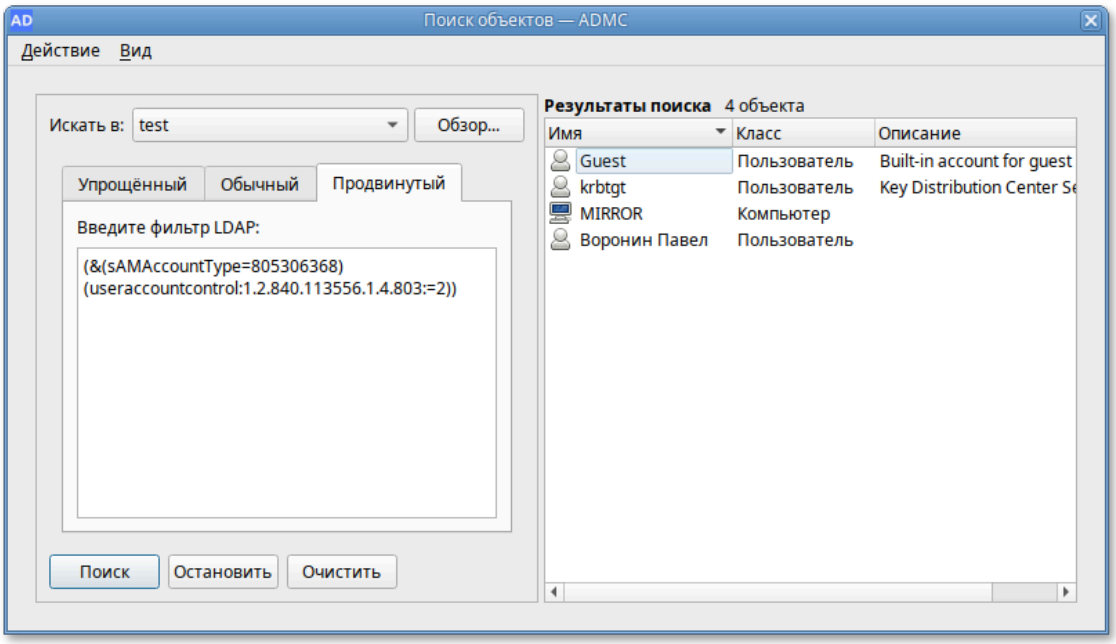


Рис. 238 – Поле «Введите фильтр LDAP»

9.2.4.16. Использование сохраненных результатов поиска

Сохранение запросов (результатов поиска) – это удобный способ сохранять и воспроизводить поиск. Сохраненные запросы позволяют создавать различные LDAP-фильтры для выборки объектов AD. С помощью сохраненных запросов можно быстро и эффективно решать задачи поиска и выборки объектов в AD по различным критериям.

При использовании сохраненных запросов администратор может выполнять групповые операции с объектами из разных OU AD. Например, можно выполнить массовую блокировку/разблокировку, удаление учетных записей, переименование.

Сохраненные запросы можно организовать в древовидную структуру (рис. 239).

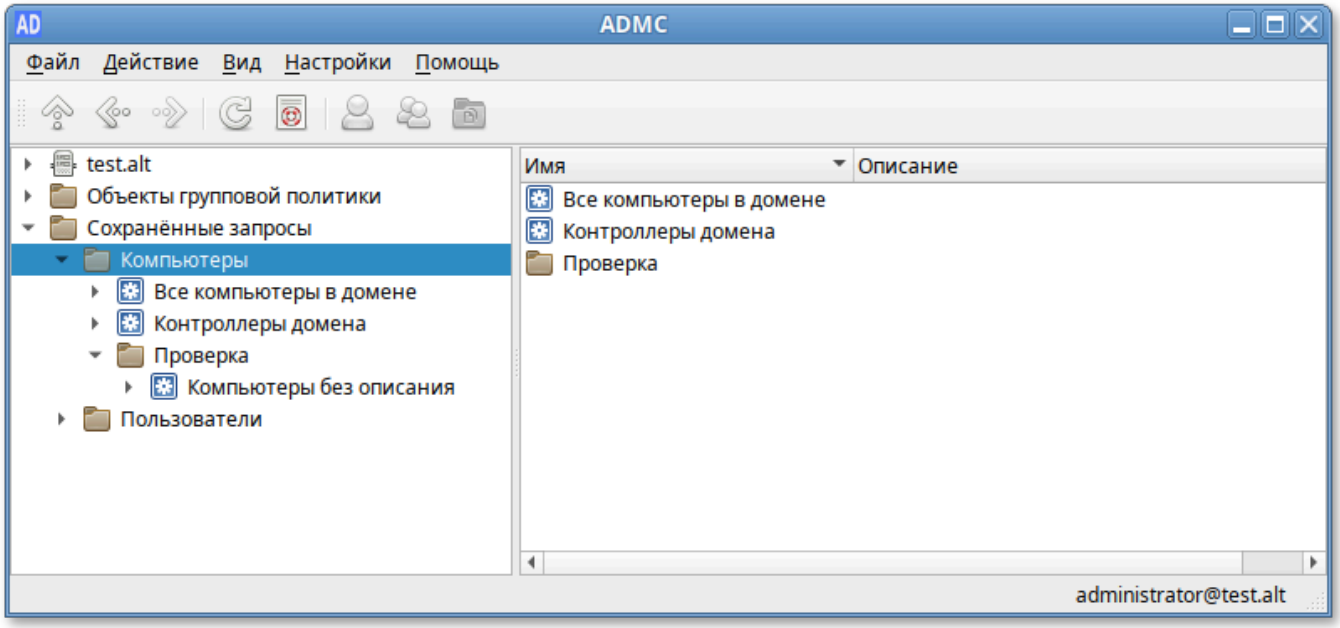


Рис. 239 – Сохраненные запросы в древовидной структуре

Создание папки запросов:

1) в контекстном меню папки «Сохраненные запросы» или ее подпапки выбрать пункт «Создать» → «Папка запросов» (рис. 240);

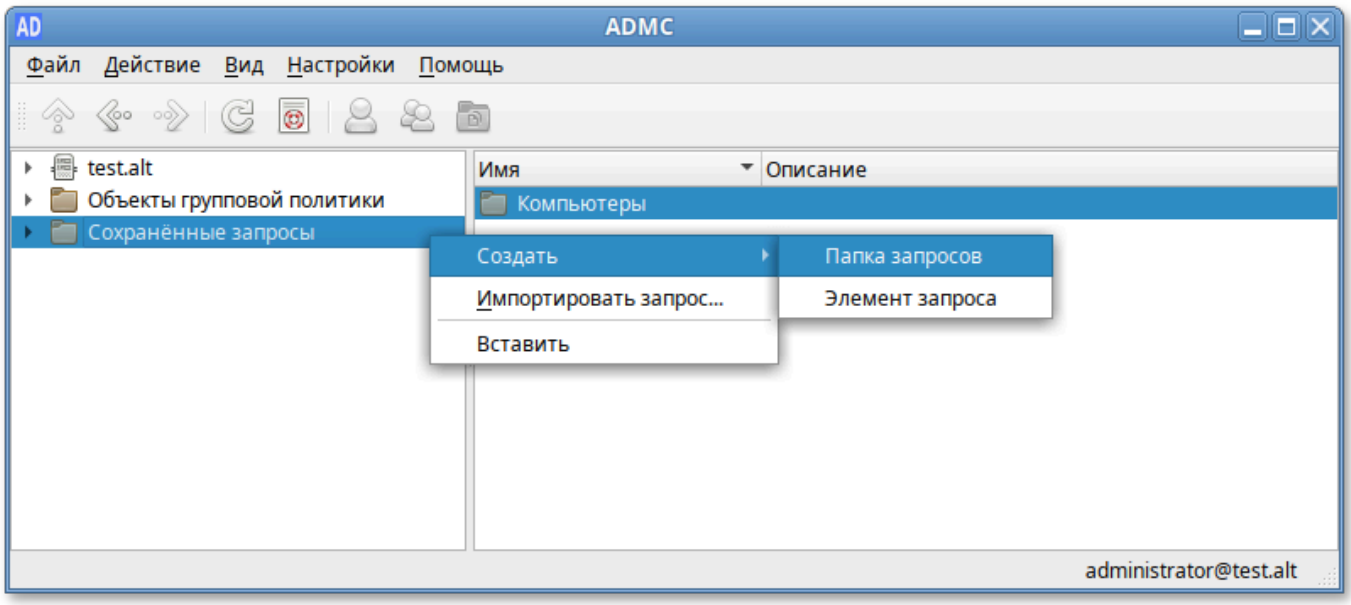


Рис. 240 – Пункт «Папка запросов»

2) в диалоговом окне «Создать папку запросов – ADMC» в поле «Имя» вести название папки, в поле «Описание» можно добавить описание папки (рис. 241);
3) нажать кнопку «ОК».

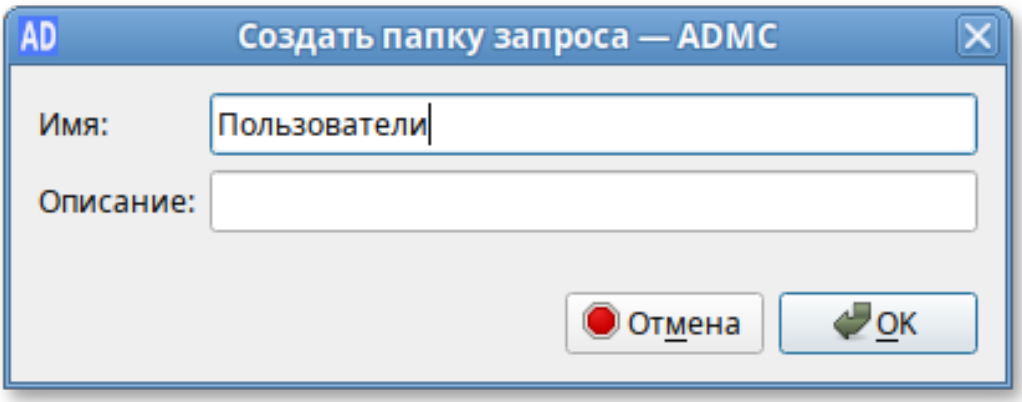


Рис. 241 – Поле «Описание»

Создание запроса:

1) в контекстном меню папки запроса выбрать пункт «Создать» → «Элемент запроса» (рис. 242);

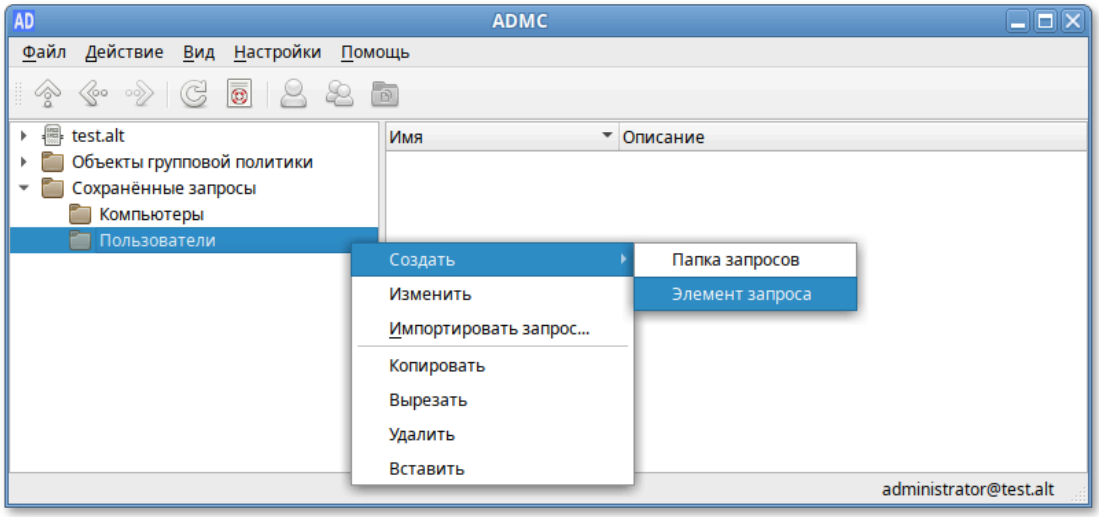


Рис. 242 – Пункт «Элемент запроса»

2) в диалоговом окне создания запроса указать:

- «Имя» – название запроса;
- «Описание» – описание запроса;
- «Искать в» – объект, который будет использоваться в качестве основы для поиска. По умолчанию поиск выполняется по всему домену AD. Сузить область поиска можно, нажав кнопку «Обзор» и выбрав контейнер;
- «Рекурсивный поиск» – поиск должен включать объекты более чем одного уровня (рис. 243);

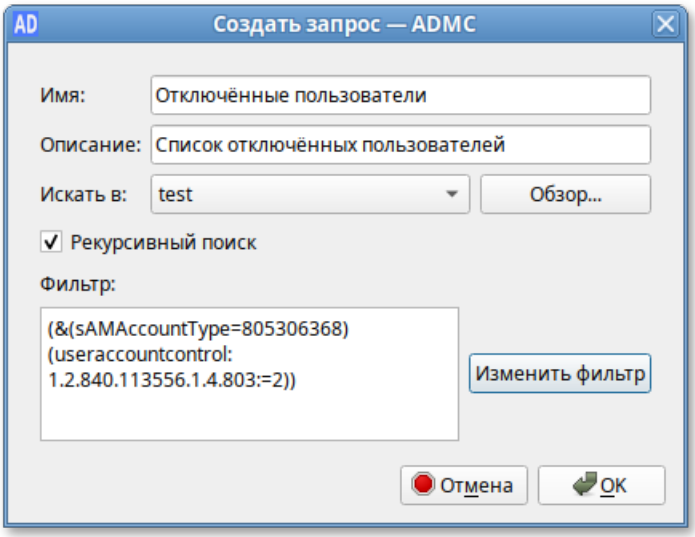


Рис. 243 – Диалоговое окно создания запроса

3) нажать кнопку «Изменить фильтр», чтобы создать фильтр поиска (для получения информации о том, как создавать фильтры см. п. 9.2.4.15);
4) после создания фильтра, он будет отображаться в поле «Фильтр» (в формате LDAP);
5) нажать кнопку «ОК».

При выборе сохраненного запроса, в правом окне появится список объектов, который соответствует данному запросу (рис. 244).

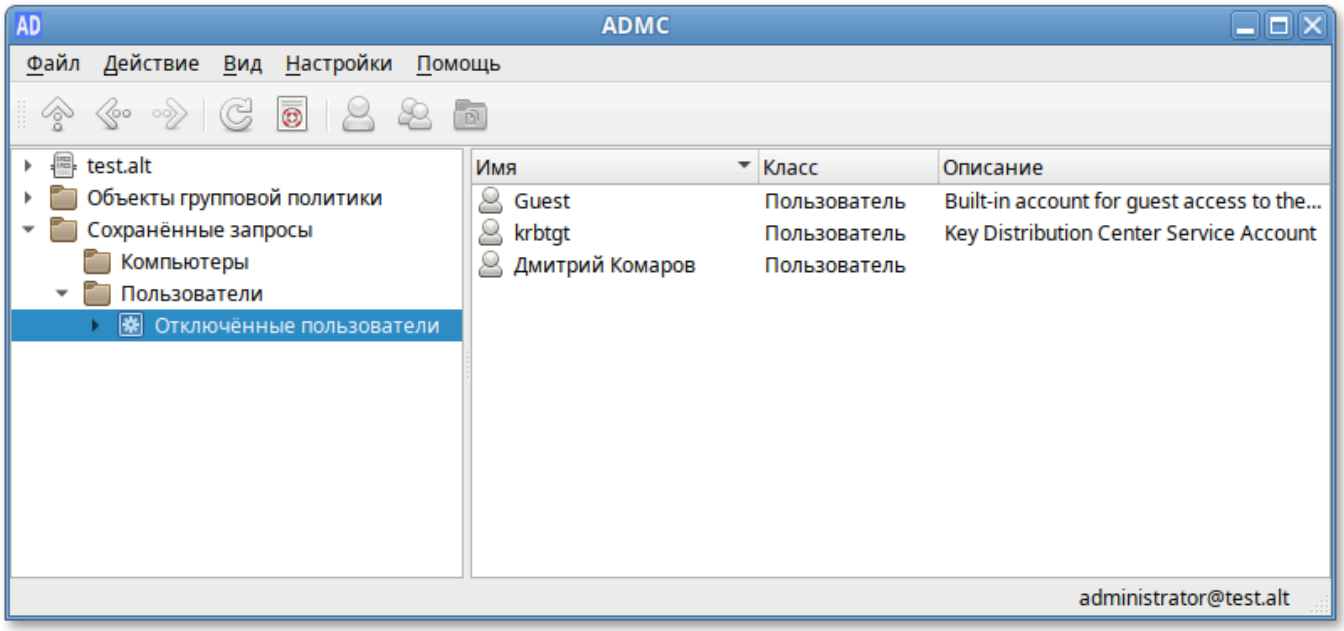


Рис. 244 – Окно выбора сохраненного запроса

В ADMC существует возможность переноса поисковых запросов между компьютерами (экспорт и импорт поисковых запросов).

Экспорт запроса:

1) в контекстном меню запроса выбрать пункт «Экспортировать запрос…» (рис. 245);
2) в открывшемся диалоговом окне указать название файла (`<имя_файла>.json`) и место назначения;
3) нажать кнопку «Открыть».

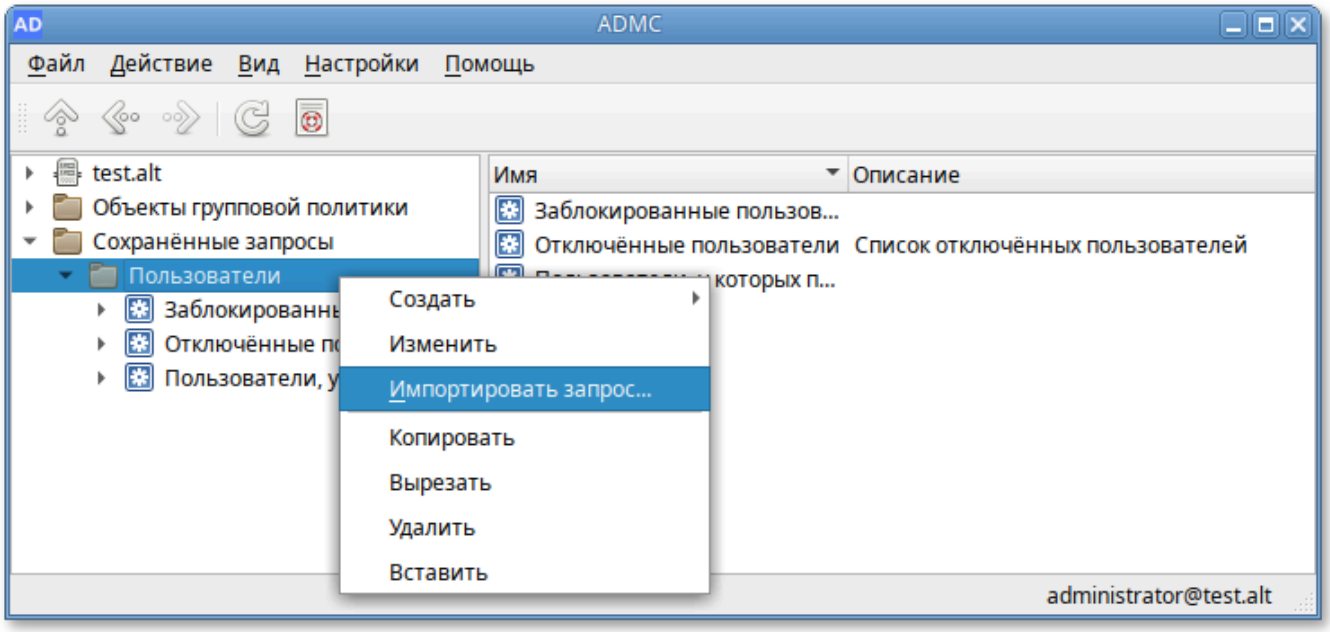


Рис. 245 – Пункт «Экспортировать запрос…»

Импорт запроса:

1) в контекстном меню папки, в которую будет импортирован запрос, выбрать пункт «Импортировать запрос…»;
2) в открывшемся диалоговом окне выбрать экспортированный файл поиска;
3) нажать кнопку «Сохранить».

Для удаления запроса или папки запросов в контекстном меню объекта выбрать пункт «Удалить».

9.2.5. Модуль редактирования настроек клиентской конфигурации (GPUI)

Модуль редактирования настроек клиентской конфигурации (далее – GPUI) предназначен для настройки и изменения параметров групповой политики в объектах групповой политики, которые могут ссылаться на организационные подразделения в AD.

GPUI предоставляет администраторам иерархическую древовидную структуру для настройки параметров групповой политики в объектах групповой политики. Эти объекты групповой политики могут быть связаны с организационными единицами (OU), содержащими компьютерные или пользовательские объекты. Связать объекты групповой политики с OU можно в модуле ADMC.

GPUI состоит из двух основных разделов: конфигурация компьютера и конфигурация пользователя. Раздел конфигурация компьютера содержит параметры всех политик, определяющих работу компьютера. Групповая политика применяется к компьютеру на этапе загрузки системы и в дальнейшем при выполнении циклов обновления. Раздел конфигурация пользователя содержит параметры всех политик, определяющих работу пользователя на компьютере. Групповая политика применяется к пользователю при его регистрации на компьютере и в дальнейшем при выполнении циклов обновления.

Каждая политика в объекте GPO может находиться в одном из трех состояний: «Включено», «Отключено», «Не сконфигурировано». В состоянии «Отключено» в настройках можно указать параметры политики. В состоянии «Не сконфигурировано» – политика на объект не воздействует.

GPUI является расширяемым инструментом. Самый простой способ для разработчиков расширить редактор объектов групповой политики для своих приложений – это написать файлы настраиваемых административных шаблонов, которые «подключаются» к редактору объектов групповой политики.

9.2.5.1. Запуск GPUI для редактирования доменных политик

По умолчанию GPUI не редактирует никаких политик. Для того чтобы редактировать политику, GPUI нужно запустить либо из ADMC, выбрав в контекстном меню объекта групповой политики пункт «Изменить…» (рис. 246).

Те же действия можно произвести при помощи указания каталога групповой политики:

```
$ gpui-main -p "smb://dc1.test.alt/SysVol/test.alt/Policies/{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXXX}"
```

Ключ `-p` позволяет указать путь к шаблону групповой политики, который нужно редактировать, `dc1.test.alt` – имя контроллера домена, а `{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXXX}` – GUID шаблона групповой политики для редактирования. Можно указывать как каталоги smb, так и локальные каталоги.

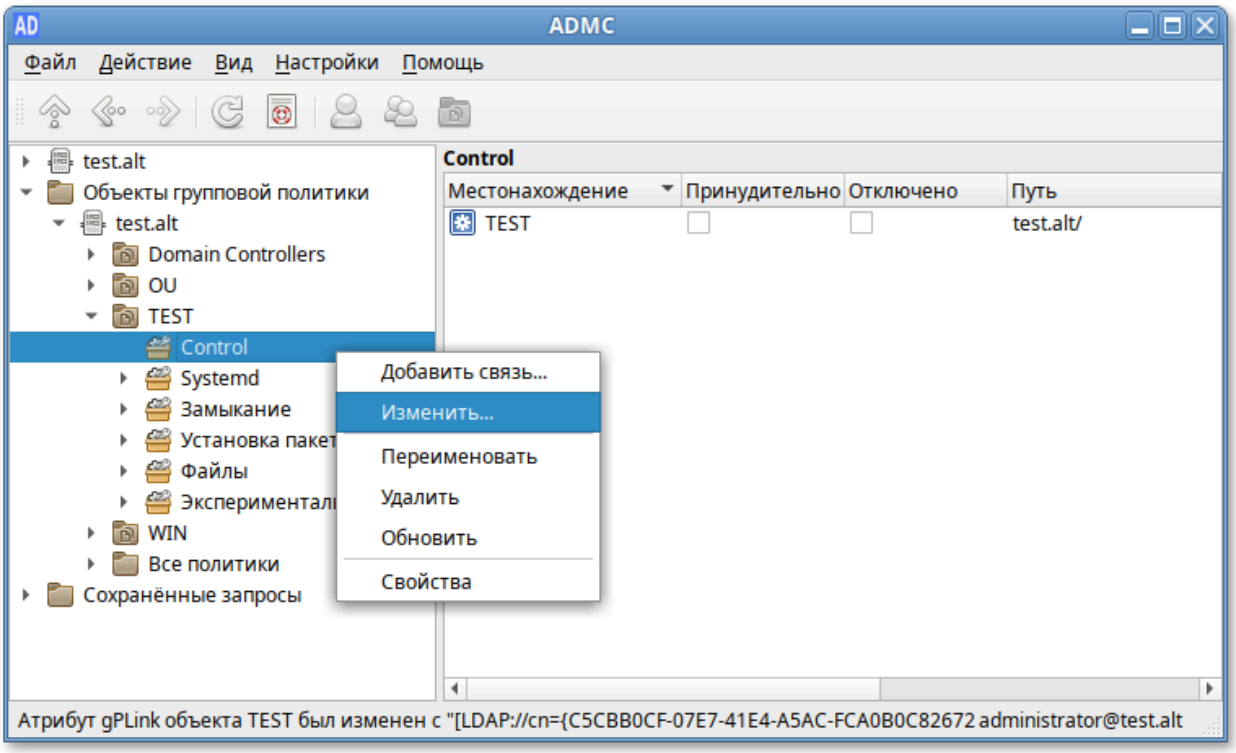


Рис. 246 – Пункт «Изменить…»

П р и м е ч а н и е . GUID шаблона групповой политики можно узнать в ADMC (это дочерний контейнер Policies контейнера System), в настройках должен быть отмечен пункт «Дополнительные возможности» (рис. 247).

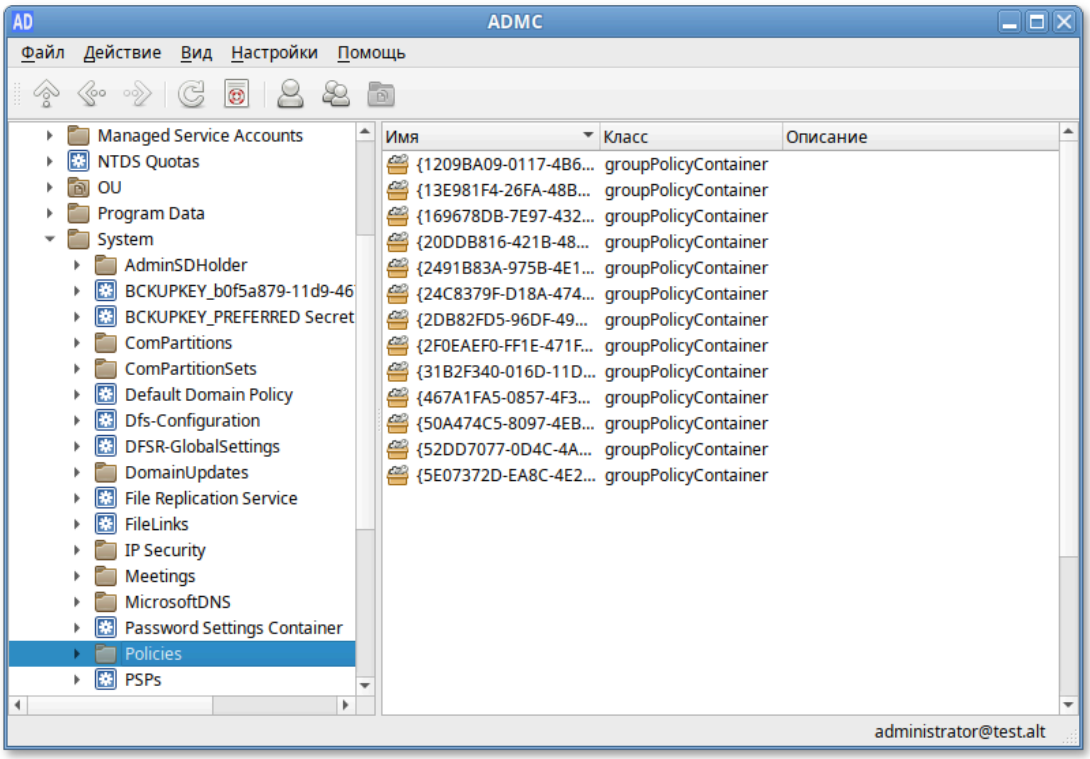


Рис. 247 – Пункт «Дополнительные возможности»

Пример запуска GPUI для редактирования политики:

```
$ gpui-main -p "smb://dc1.test.alt/SysVol/test.alt/Policies/{2E80AFBE-BBDE-408B-B7E8-AF79E02839D6}"
```

9.2.5.2. Выбор набора шаблонов групповых политик

По умолчанию GPUI загружает ADMX-файлы, содержащие описание шаблонов групповых политик, из каталога `/usr/share/PolicyDefenitions`.

Для того что бы указать другой набор шаблонов групповых политик, GPUI можно запустить с ключом `-b`:

```
$ gpui-main -b "/usr/share/PolicyDefinitions"
```

Каталог шаблонов групповых политик можно также выбрать в графическом интерфейсе:

1) выбрать пункт меню «Файл» → «Открыть папку с ADMX файлами» (рис. 248);
2) открыть папку с шаблонами.

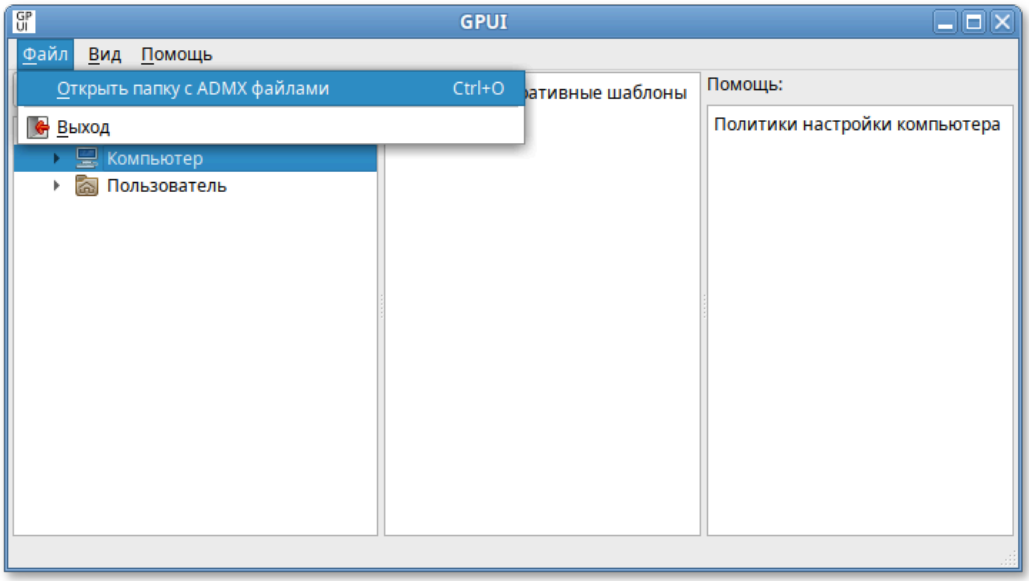


Рис. 248 – Подпункт «Открыть папку с ADMX файлами»

9.2.5.3. Интерфейс

Все настройки в GPUI разделены на два раздела:

- «Компьютер» («Machine») – раздел с настройками параметров компьютера;
- «Пользователь» («User») – раздел с настройками параметров пользователей AD (рис. 249).

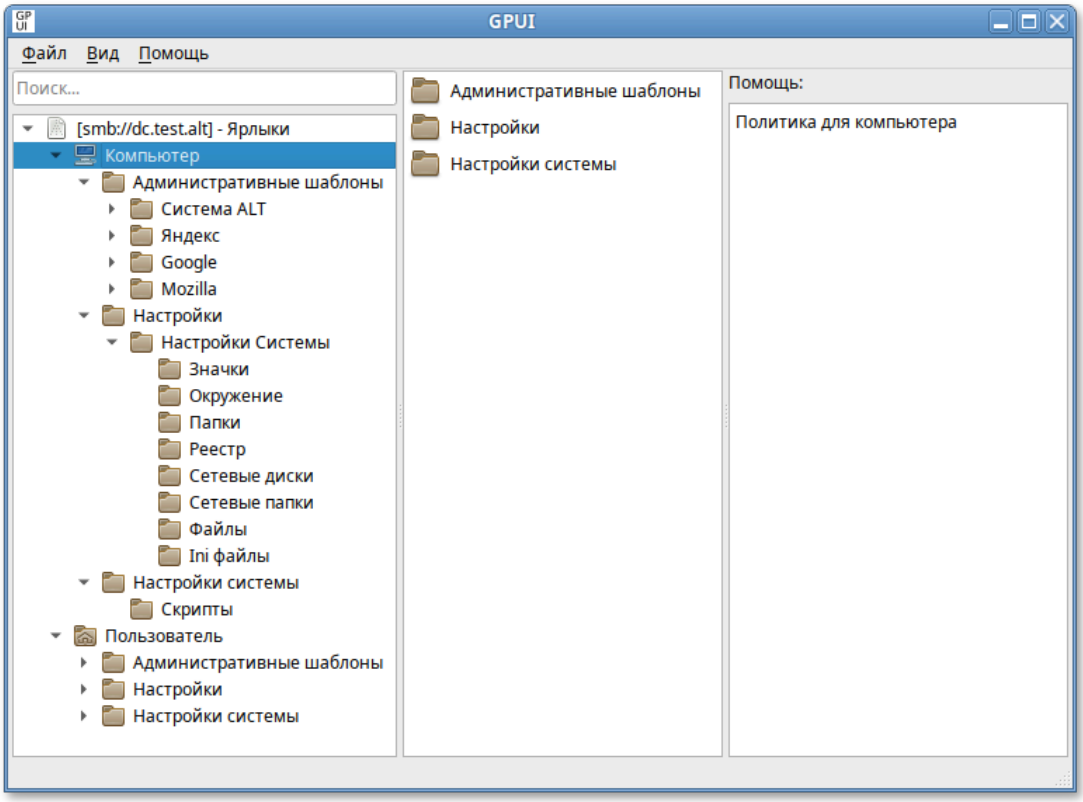


Рис. 249 – Интерфейс

В каждом разделе есть три подраздела:

- «Административные шаблоны» («Administrative Templates») – содержит параметры различных компонентов. Здесь доступны как административные шаблоны ОС Альт СП и Windows, так и дополнительные admx-шаблоны (например, admx-шаблоны для Mozilla Firefox или для Google Chrome);
- «Настройки» («Preferences») – содержит дополнительный набор настроек (предпочтений). С помощью предпочтений можно настроить, в том числе такие параметры: создание ярлыков, подключение сетевых дисков, копирование файлов и папок на компьютеры;
- «Настройки системы» («System settings») – позволяет указать сценарии запуска и завершения работы компьютера, входа и выхода из системы пользователя.

Для быстрого доступа к политике можно воспользоваться поиском, для этого следует ввести в поле «Поиск…» ключевое слово.

9.2.5.3.1. Редактирование параметров в разделе «Административные шаблоны»

Чтобы изменить любой параметр групповой политики, нужно найти раздел, в котором он находится, и открыть его настройки в правой панели.

Параметры политики административных шаблонов могут иметь одно из трех состояний: «Не сконфигурировано»/ «Включено»/ «Отключено». Параметры политики в состоянии «Не сконфигурировано» не влияют на пользователей или компьютеры. Если параметр политики находится в состоянии «Включено», к пользователю или компьютеру применяется действие, описанное в заголовке параметра политики. Если параметр политики находится в состоянии «Отключено», к пользователю или компьютеру применяется действие, противоположное описанному в заголовке параметра политики. Как правило, состояния параметров политики «Не сконфигурировано» и «Отключено» приводят к одинаковым результатам (рис. 250).

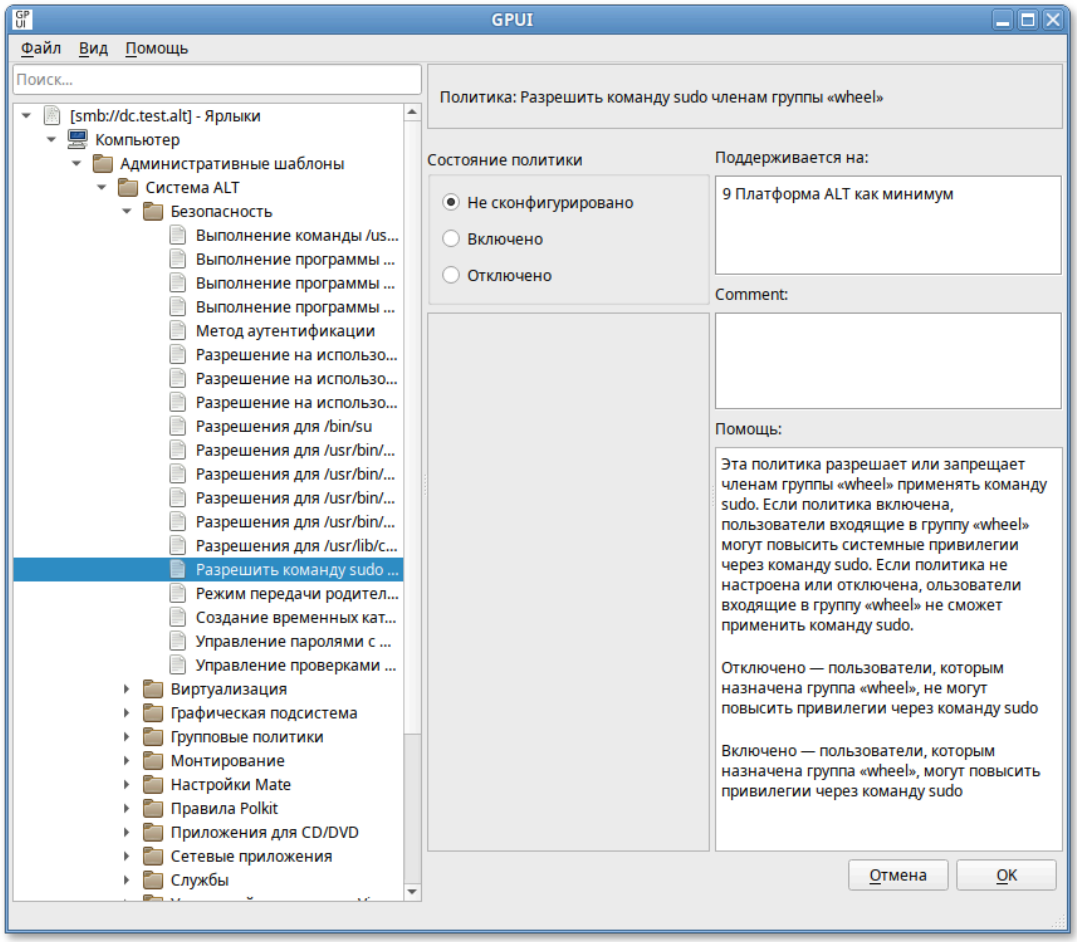


Рис. 250 – Состояние параметров политики

В каждом параметре политики административных шаблонов предоставлены подробные сведения о состояниях «Включено», «Отключено» и «Не сконфигурировано». Можно просмотреть эти сведения в поле «Помощь» для каждого параметра политики административных шаблонов.

В поле «Поддерживается на» указаны версии ОС, для которых данная политика применима.

По умолчанию все параметры в разделе административных шаблонов не настроены (не сконфигурированы). Чтобы изменить настройку параметра групповой политики, достаточно выбрать новое состояние и нажать кнопку «ОК».

У некоторых настроек групповых политик можно задать дополнительные параметры, которые можно настроить в секции «Опции». Например, чтобы установить изображение в качестве фона рабочего стола через групповые политики, нужно включить политику и указать путь к файлу с изображением в поле «Файл» (рис. 251).

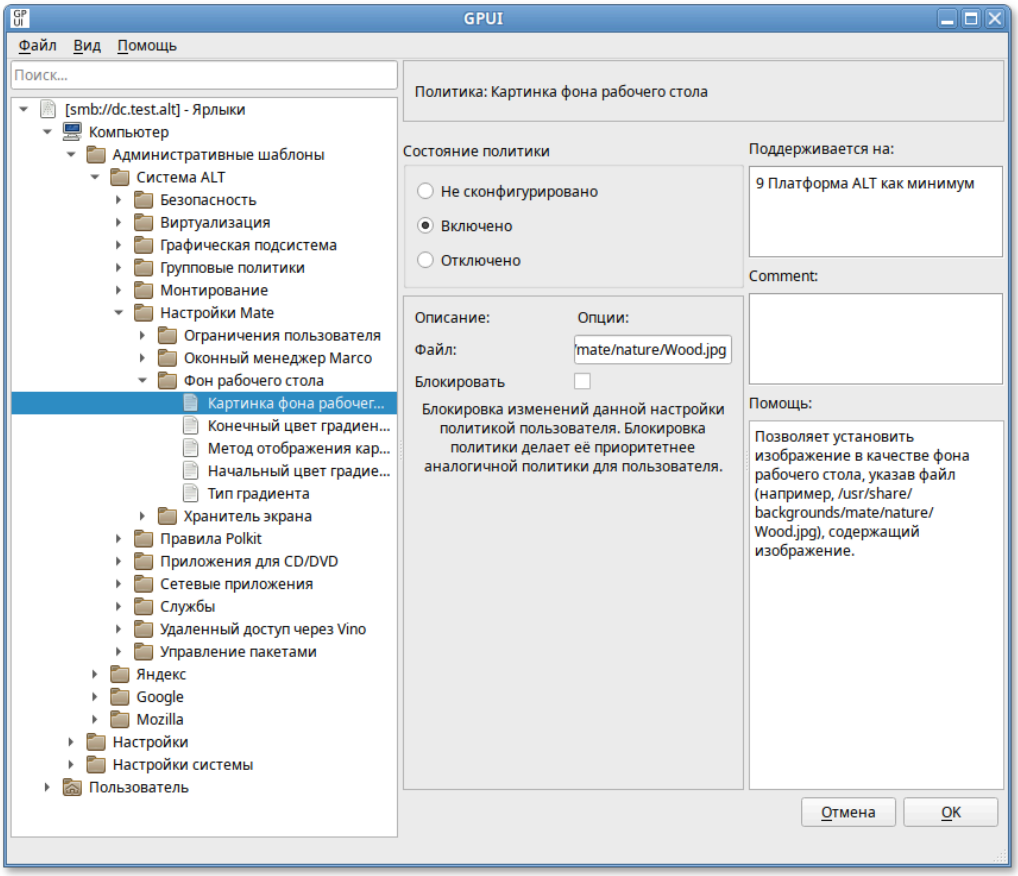


Рис. 251 – Установка изображения в качестве фона рабочего стола через групповые политики

В поле «Комментарий» («Comment») можно указать примечание для групповой политики.

9.2.5.3.2. Фильтрация административных шаблонов

По умолчанию в GPUI отображаются все установленные административные шаблоны. Чтобы изменить отображение параметров политик административных шаблонов можно настроить фильтр административных шаблонов.

Фильтр административных шаблонов можно применять, если найти определенный параметр политики или ограничить количество параметров политики, отображаемых в GPUI.

Административные шаблоны можно отфильтровать на основе следующих факторов:

- настраиваемых параметров политики;
- ключевых слов в заголовке политики или тексте помощи к параметрам политики;
- требований параметров политики к платформам или приложениям (рис. 252).

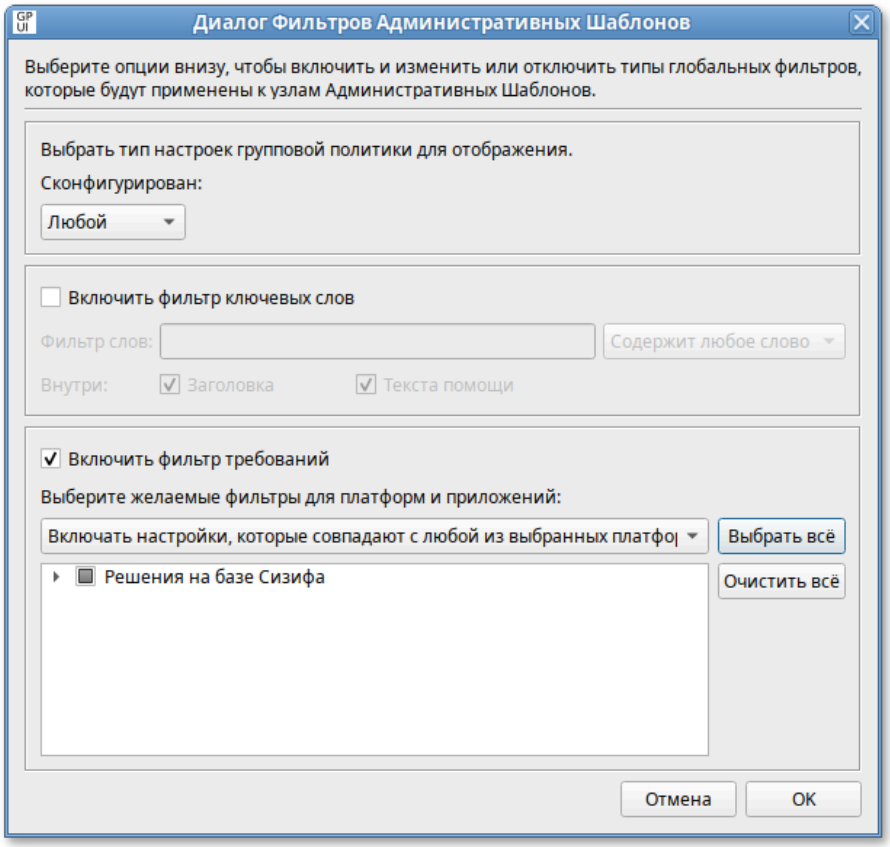


Рис. 252 –Фильтрация административных шаблонов

Примечание. Фильтры являются включающими, поэтому выбирайте элементы, которые следует отображать, а не элементы, которые следует исключать.

9.2.5.3.2.1 Фильтр по настроенным параметрам

Фильтр по настроенным параметрам имеет три состояния:

- «Любой» – отображать все параметры политики административных шаблонов (по умолчанию);
- «Да» – отображать только сконфигурированные параметры политики административных шаблонов;
- «Нет» – отображать только не сконфигурированные параметры политики административных шаблонов.

Для установки фильтра по настроенным параметрам:

1) в меню выбрать «Вид» → «Фильтр» → «Редактировать фильтр» (рис. 253);

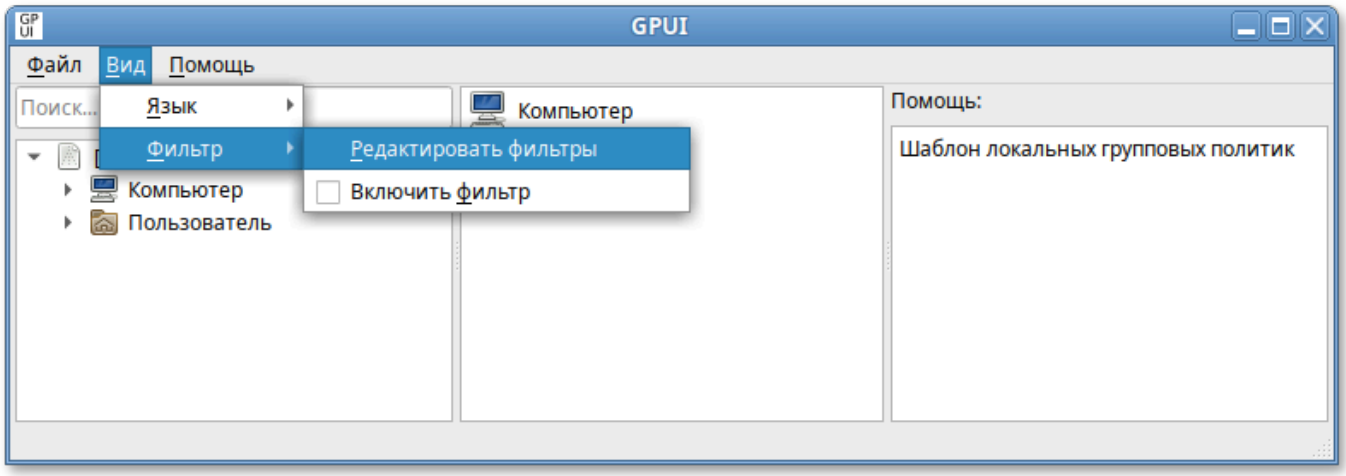


Рис. 253 – Фильтр по настроенным параметрам

2) в открывшемся окне в списке «Сконфигурирован» выбрать фильтр (рис. 254);
3) нажать кнопку «ОК», чтобы сохранить параметры фильтра;
4) чтобы применить фильтр в меню выбрать «Вид» → «Фильтр» → «Включить фильтр» (рис. 255).

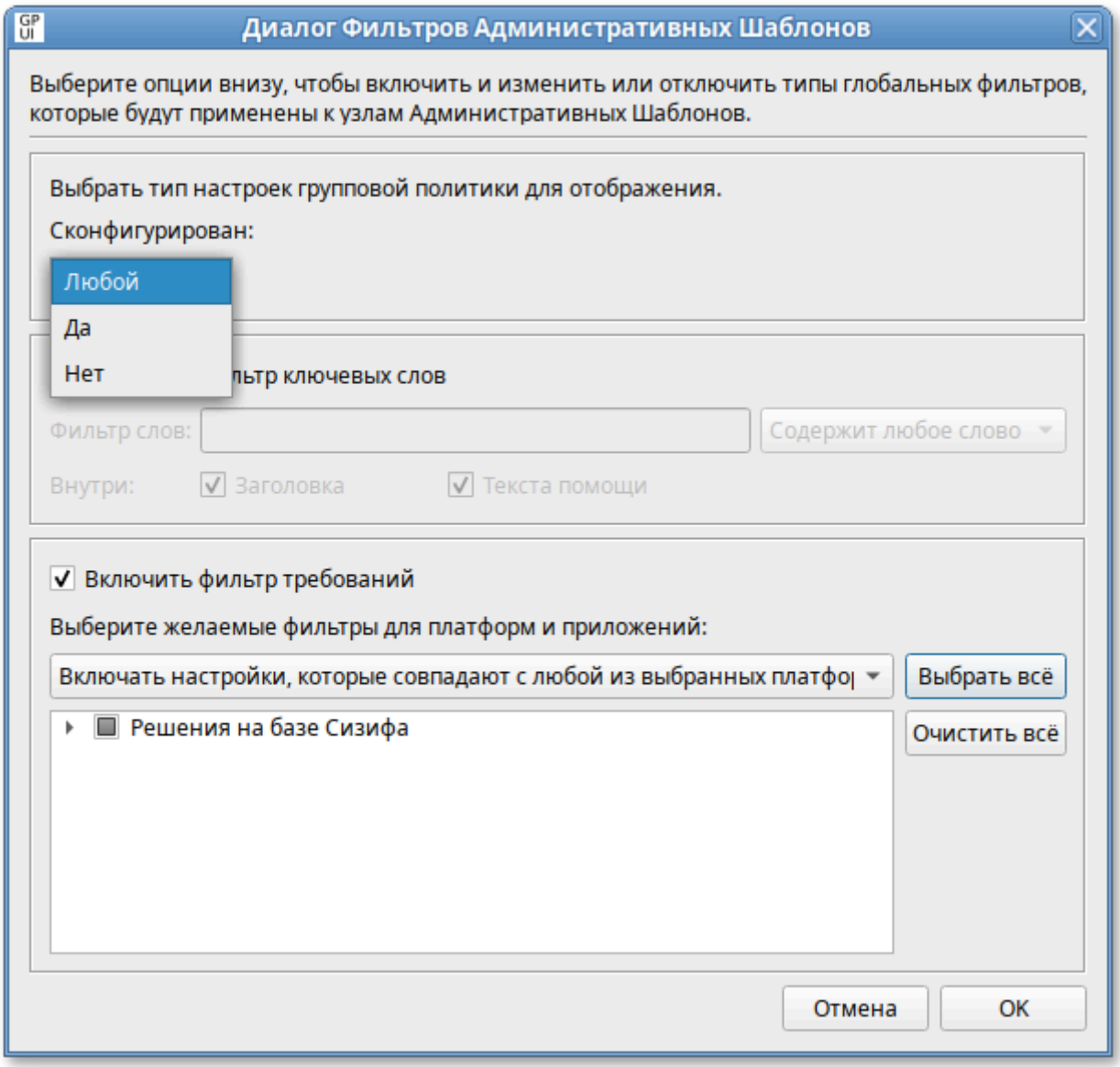


Рис. 254 – «Диалог Фильтров Административных Шаблонов»

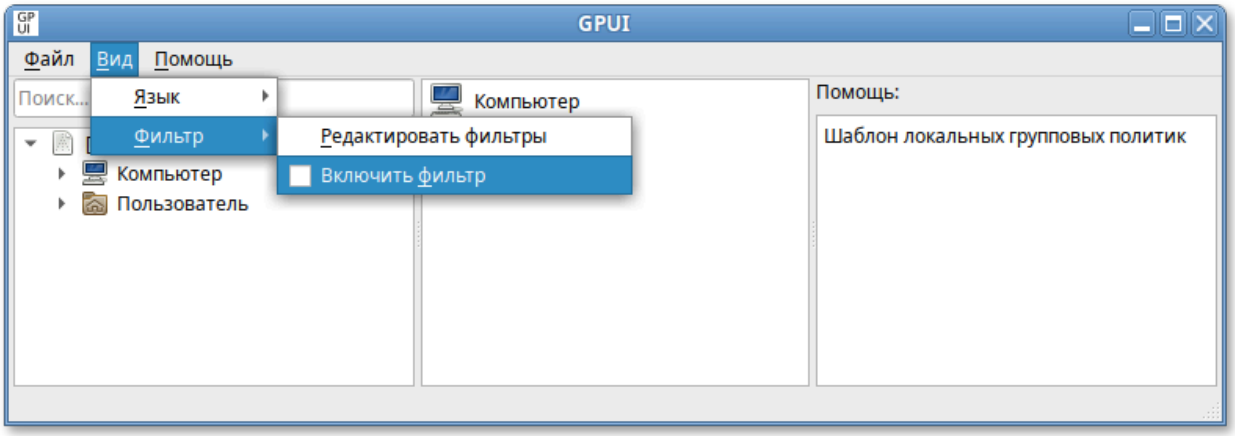


Рис. 255 – Вкладка «Вид». «Включить фильтр»

9.2.5.3.2.2 Фильтр по ключевым словам

Для установки фильтра по ключевым словам:

1) в меню выбрать «Вид» → «Фильтр» → «Редактировать фильтр» (рис. 256);

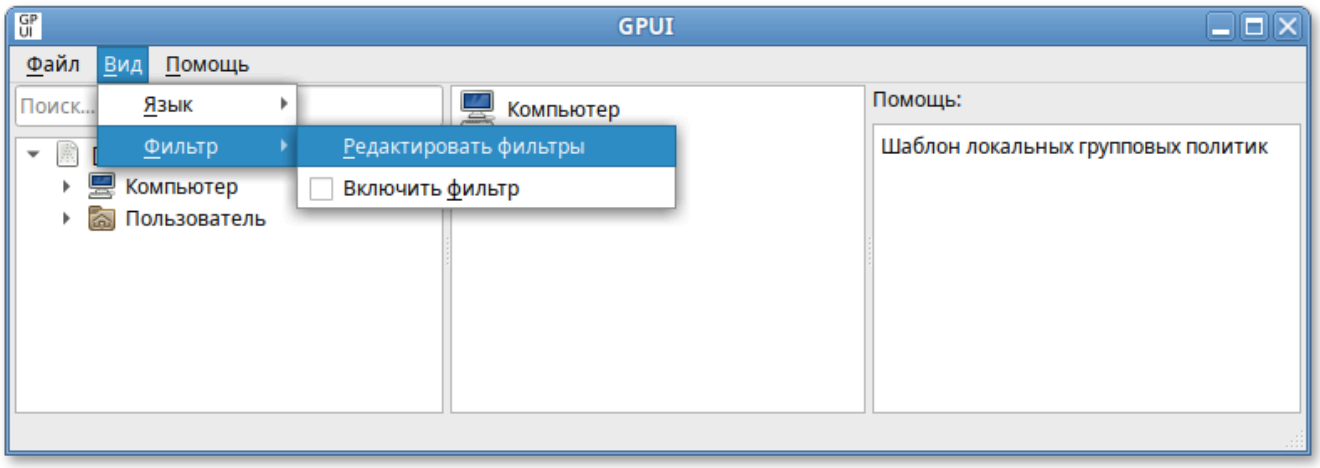


Рис. 256 – Вкладка «Вид». «Редактировать фильтр»

2) в открывшемся окне установить отметку «Включить фильтр ключевых слов» (рис. 257);

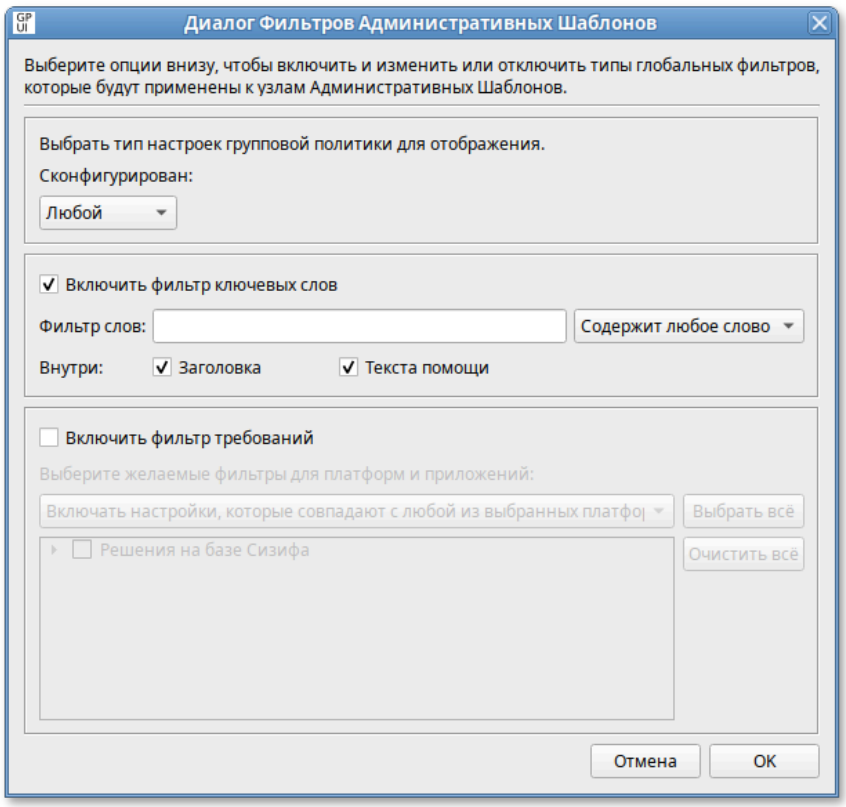


Рис. 257 – Отметка «Включить фильтр ключевых слов»

3) ввести одно или несколько ключевых слов в поле «Фильтр слов» и выбрать фильтр:
   - «Содержит любое слово» – фильтр содержит любое слово из поля Фильтр слов;
   - «Содержит все слова» – фильтр содержит все слова из поля Фильтр слов;
   - «Полностью совпадает» – фильтр содержит точное соответствие словам Фильтр слов;
4) установить соответствующие отметки в поле «Внутри»:
   - «Заголовка» – фильтр включает поиск в заголовке параметра политики;
   - «Текста помощи» – фильтр включает поиск в тексте помощи параметра политики;
5) нажать кнопку «ОК», чтобы сохранить параметры фильтра (рис. 258);

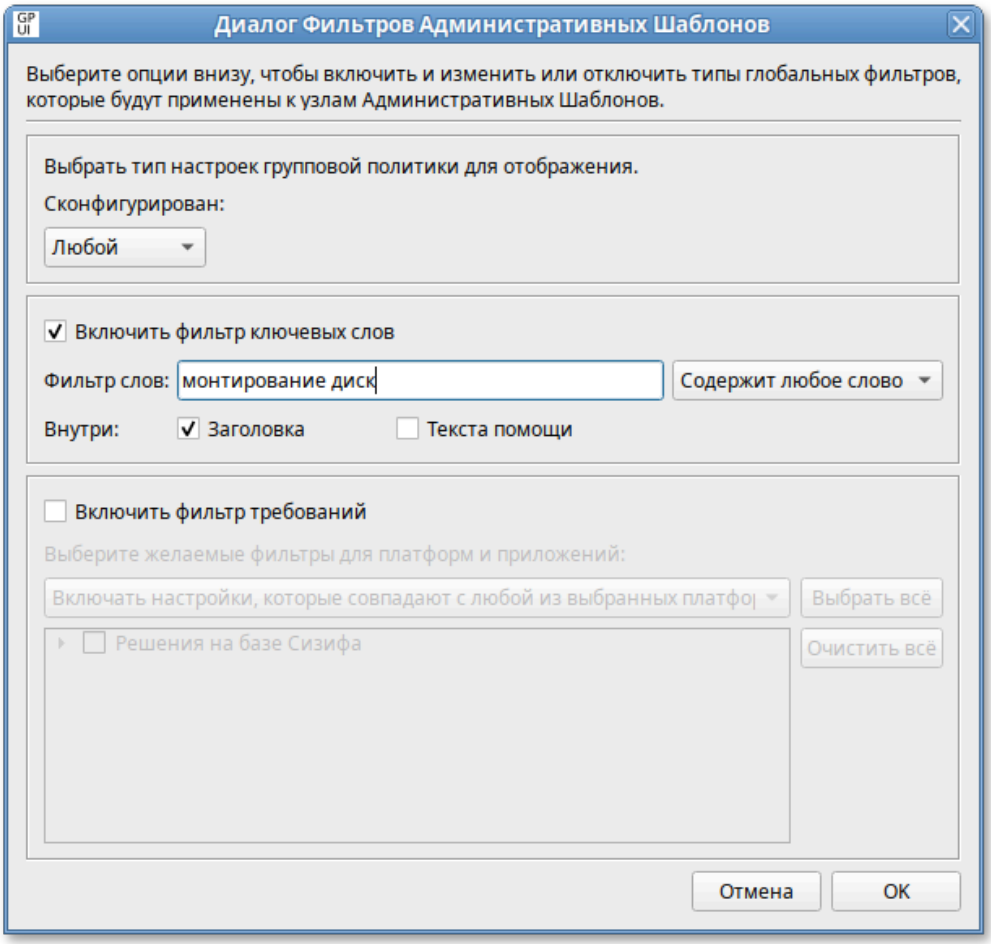


Рис. 258 – Параметры фильтра

6) чтобы применить фильтр в меню выбрать «Вид» → «Фильтр» → «Включить фильтр» (рис. 259);

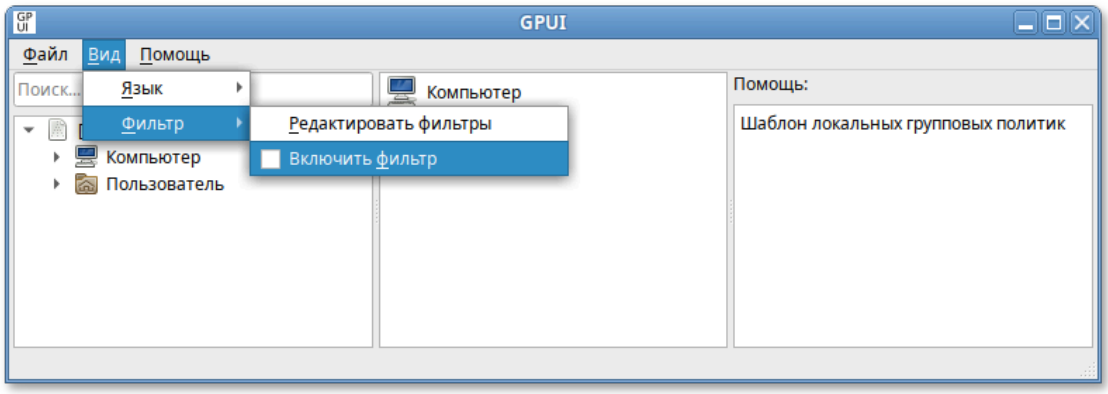


Рис. 259 – Применение фильтра

Результат применения фильтра по ключевым словам (рис. 260).

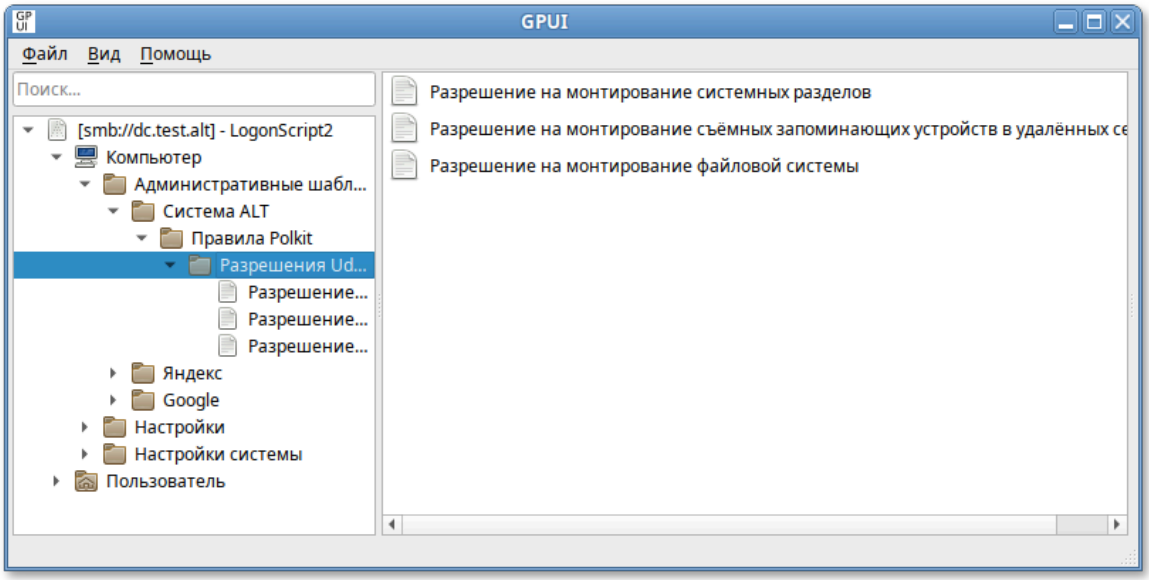


Рис. 260 – Результат применения фильтра по ключевым словам

9.2.5.3.2.3 Фильтр по требованиям

При помощи этого способа фильтрации, можно отобразить параметры, соответствующие всем выбранным платформам или отобразить параметры, соответствующие любым из выбранных платформ.

Для установки фильтра по требованиям:

1) в меню выбрать «Вид» → «Фильтр» → «Редактировать фильтр» (рис. 261);

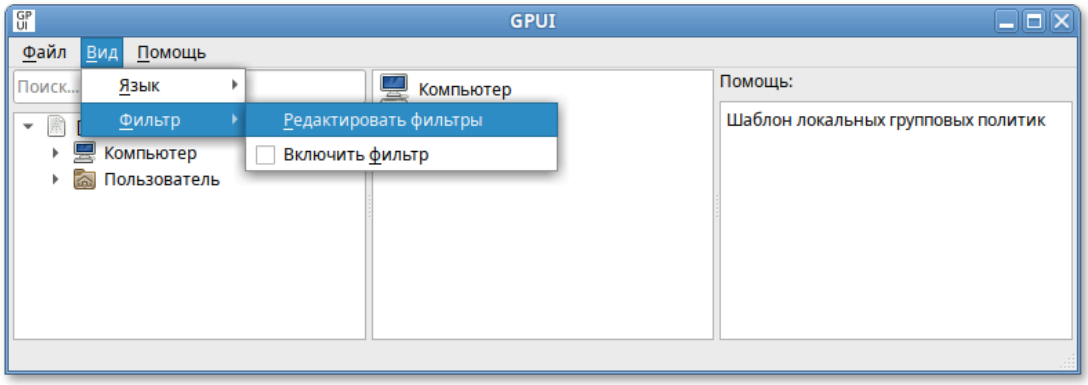


Рис. 261 – Установка фильтра по требованиям

2) в открывшемся окне установить отметку «Включить фильтр ключевых требований» (рис. 262);

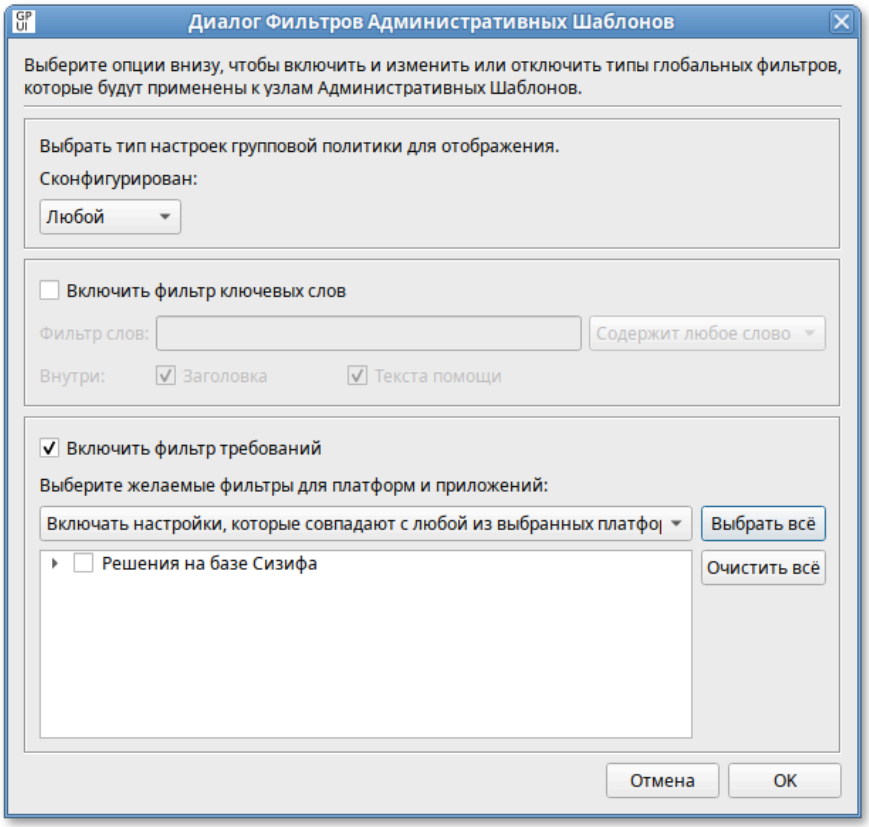


Рис. 262 – Отметка «Включить фильтр ключевых требований»

3) в списке «Выберите желаемые фильтры для платформы и приложений» выбрать фильтр:

- включать настройки, которые совпадают с любой из выбранных платформ;

- включить настройки, которые совпадают со всеми выбранными платформами;

4) выбрать платформы. Можно выбрать пункт «Решения на базе Сизифа» нажать кнопку «Выбрать все», чтобы выбрать все элементы в списке, или нажать кнопку «Очистить все», чтобы снять выделение всех элементов списка;
5) нажать кнопку «ОК», чтобы сохранить параметры фильтра;
6) чтобы применить фильтр в меню выбрать «Вид» → «Фильтр» → «Включить фильтр» (рис. 263).

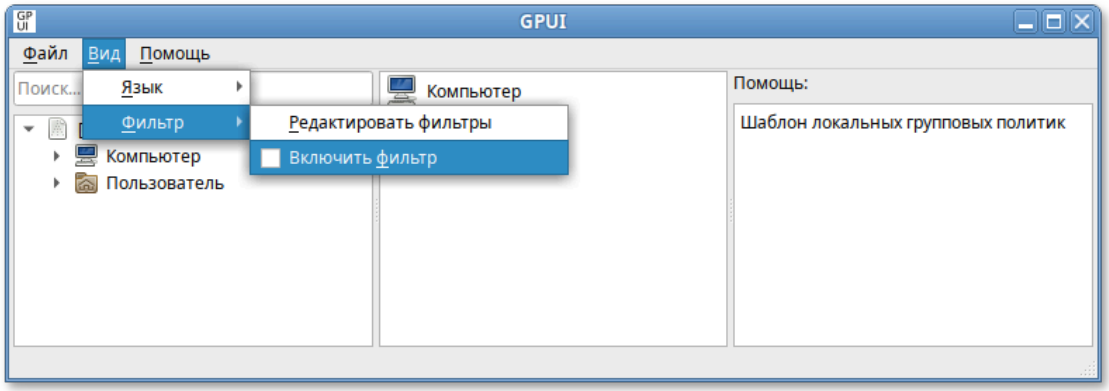


Рис. 263 – Фильтр по требованиям

9.2.5.3.3. Работа с предпочтениями групповых политик

GPUI позволяет настраивать следующие предпочтения:

- «Значки» – создание, редактирование или удаление ярлыков;
- «Окружение» – создание, редактирование или удаление переменных среды;
- «Папки» – создание, редактирование или удаление папок;
- «Реестр» – копирование параметров реестра и их применение к другим компьютерам, создание, замена или удаление параметров реестра (для машин Windows);
- «Сетевые папки» – создание, удаление (скрытие из общего доступа) или редактирование общих ресурсов;
- «Сетевые диски» – создание, редактирование или удаление сопоставленных дисков и настройка видимости всех дисков;

- «Файлы» – копирование, замена, удаление или изменение атрибутов файлов;
- «INI-файлы» – добавление, замена или удаление разделов/свойств файлов параметров настройки (INI) или информации об установке (INF).

Предпочтения можно настроить для пользователей и компьютеров (пункт «Настройки» соответственно в элементах «Компьютер» и «Пользователь») (рис. 264).

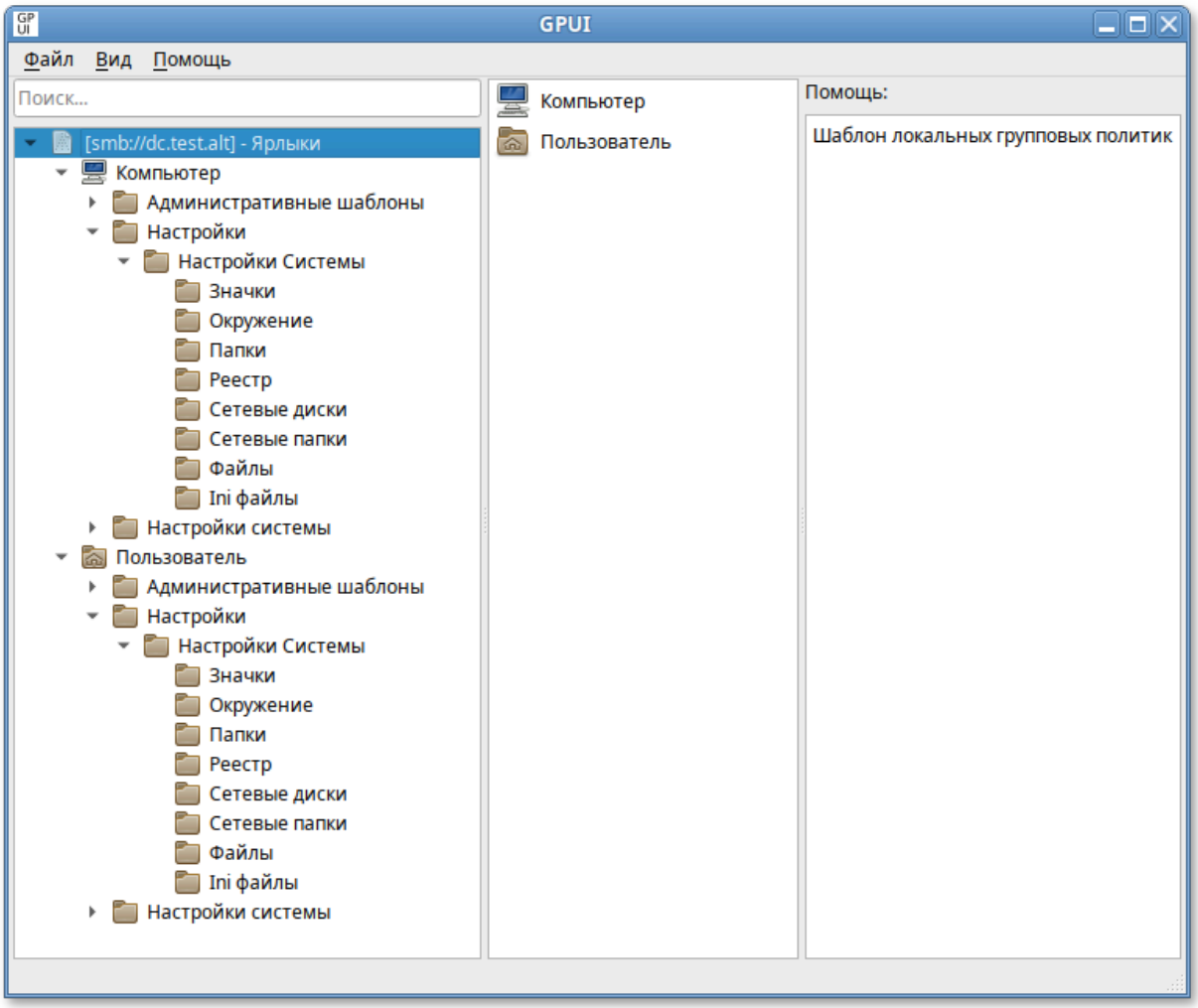


Рис. 264 – Настройка предпочтений

В каждом объекте групповой политики с каждым из расширений предпочтения можно создать несколько элементов предпочтения.

Для создания предпочтения нужно перейти в «Компьютер/Пользователь» → «Настройки» → «Настройки системы», выбрать соответствующее предпочтение, затем в контекстном меню свободной области выбрать пункт «Новый» → «Название_предпочтения».

Например, для создания нового предпочтения «Папки» нужно перейти в «Компьютер/Пользователь» → «Настройки» → «Настройки системы» → «Папки». В контекстном меню свободной области выбрать пункт «Новый» → «Папки» (рис. 265).

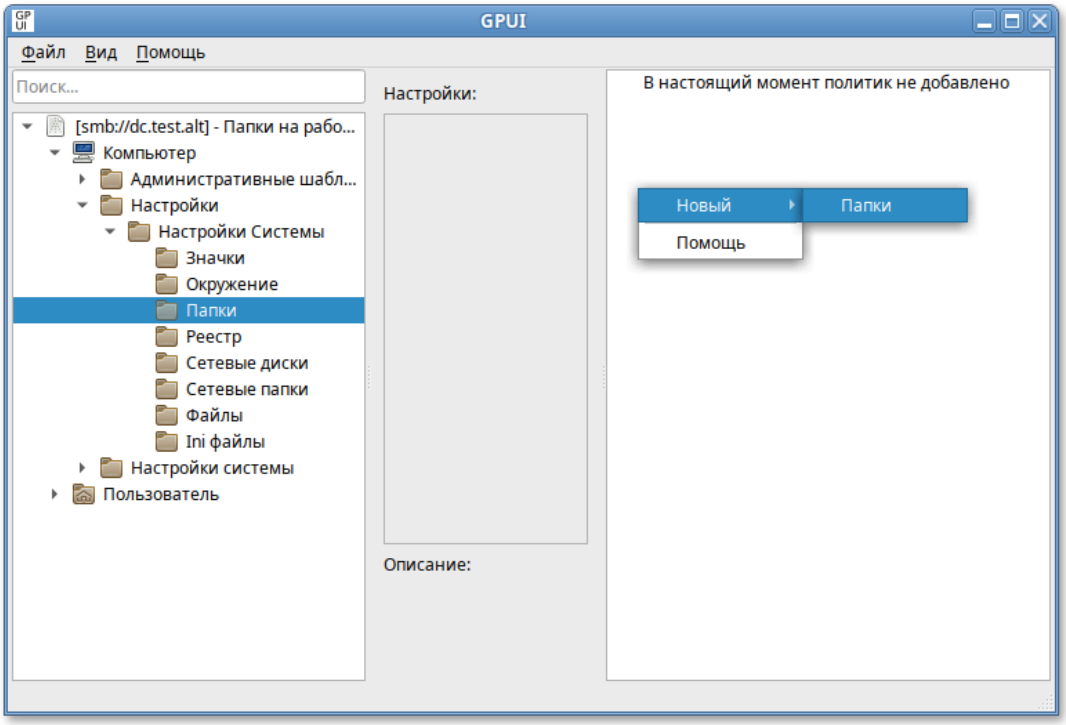


Рис. 265 – Контекстное меня свободной области

Откроется диалоговое окно «Диалог настроек», где на вкладке «Основные настройки» можно задать параметры, характерные для соответствующего предпочтения (подробнее параметры настройки предпочтений рассмотрены в следующих разделах данного документа) (рис. 266).

Вкладка «Общие» содержит настройки одинаковые для всех предпочтений:

- «Остановить обработку элементов в этом расширении при возникновении ошибки» – при сбое элемента предпочтений обработка других элементов предпочтений в этом расширении останавливается;
- «Выполнять в контексте безопасности текущего пользователя (опция пользовательских политик)»;
- «Удалить элемент, если больше не применим»;
- «Описание» (рис. 267).

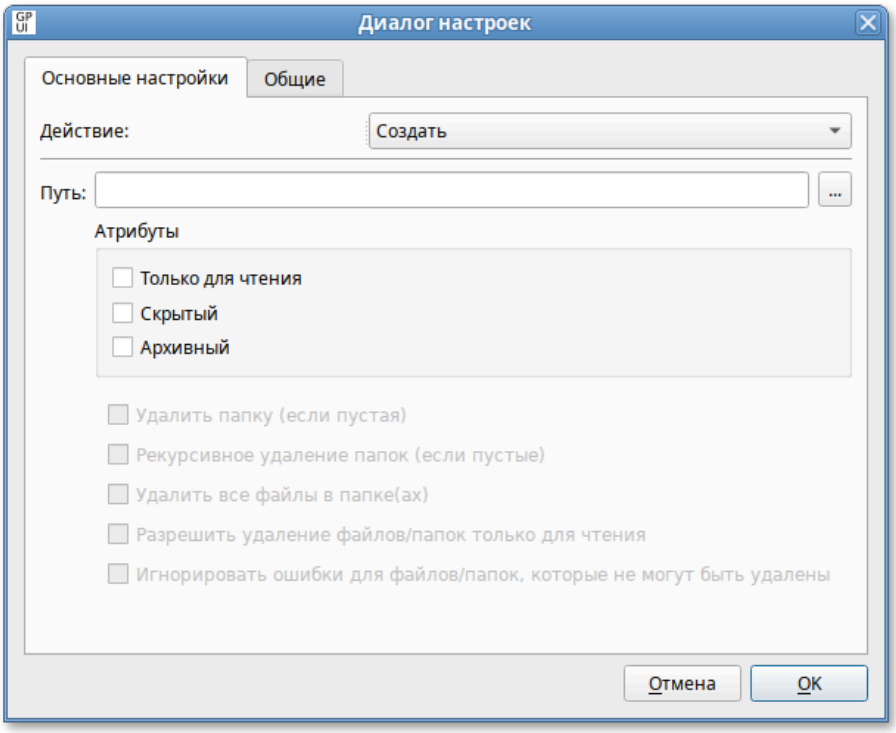


Рис. 266 – Вкладка «Основные настройки»

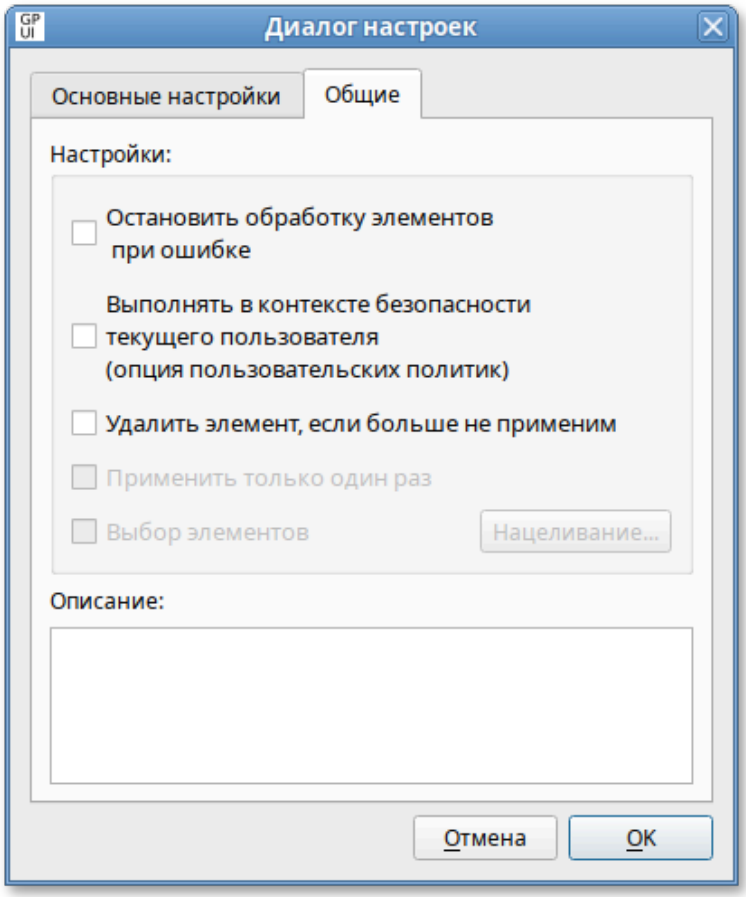


Рис. 267 – Вкладка «Общие»

Для редактирования элемента предпочтения следует дважды щелкнуть мышью по элементу (рис. 268).

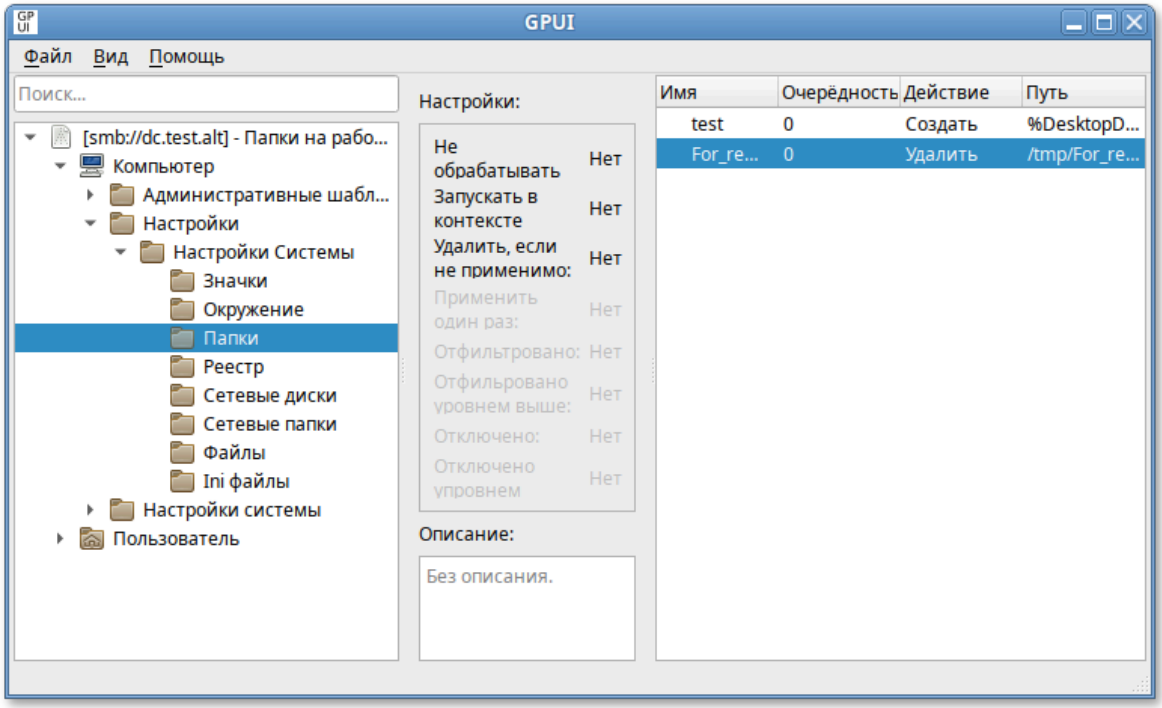


Рис. 268 – Редактирование элемента

Далее откроется окно редактирования предпочтения (рис. 269).

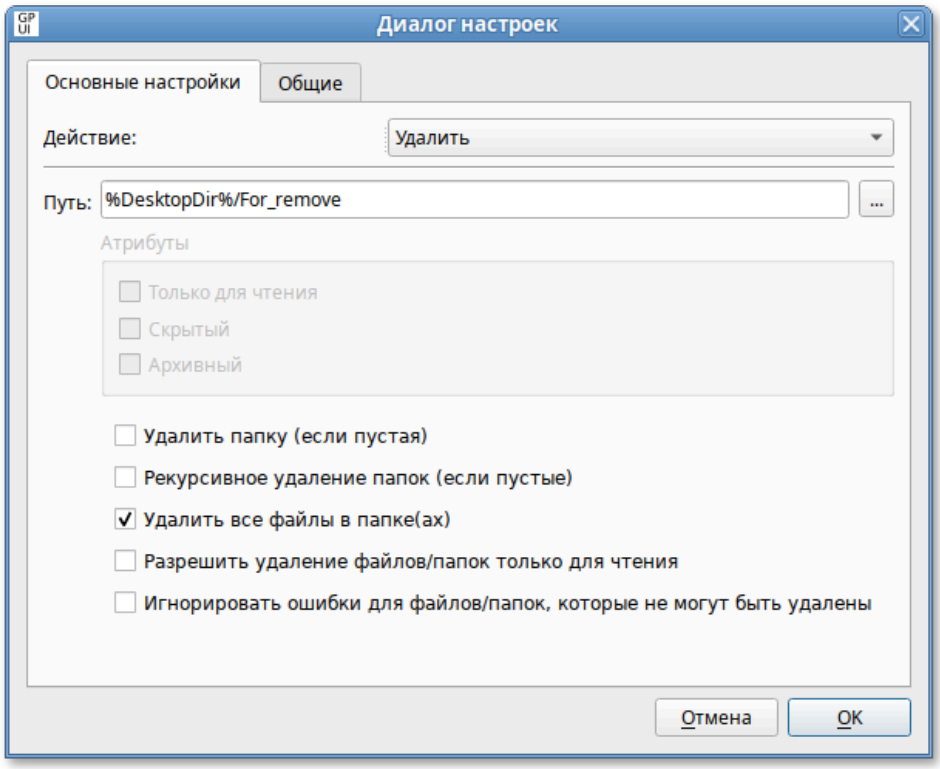


Рис. 269 – Редактирование предпочтения

Для удаления элемента следует в контекстном меню предпочтения выбрать пункт «Удалить элемент» (рис. 270).

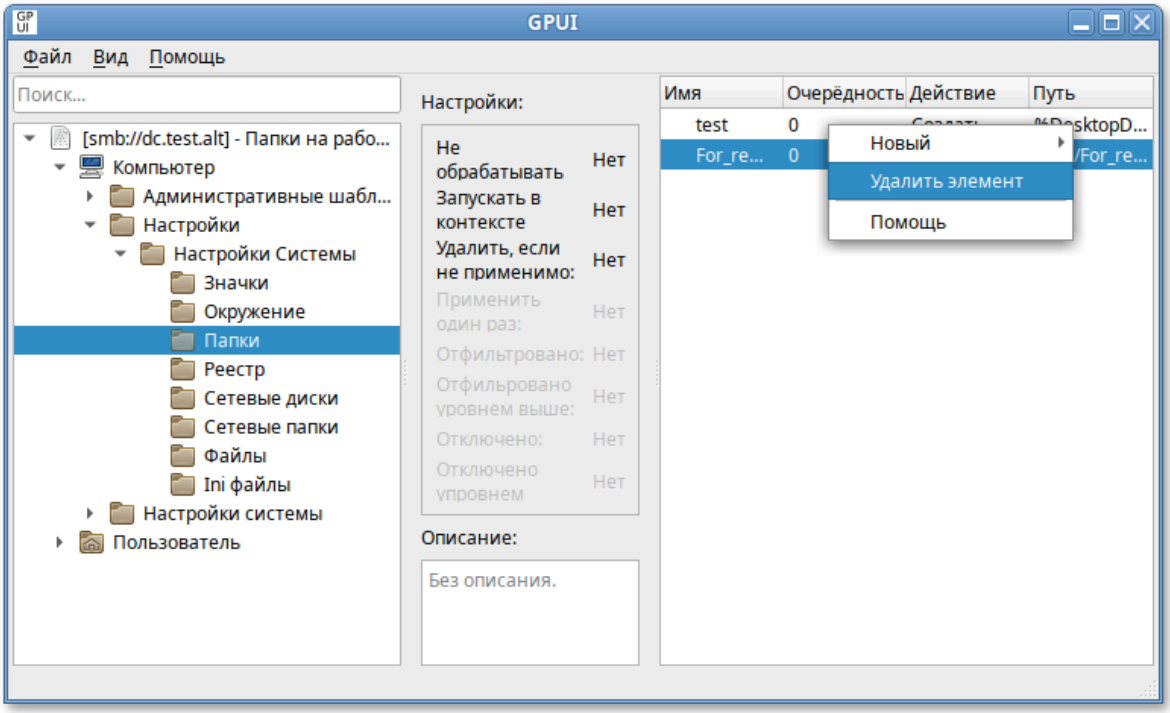


Рис. 270 – Пункт «Удалить элемент»

9.2.5.3.4. Работа со скриптами

Работа со скриптами подробно описана в п. 9.2.5.6.

9.2.5.3.5. Смена языка

Для того чтобы изменить язык интерфейса, нужно в меню выбрать «Вид» → «Язык» (рис. 271).

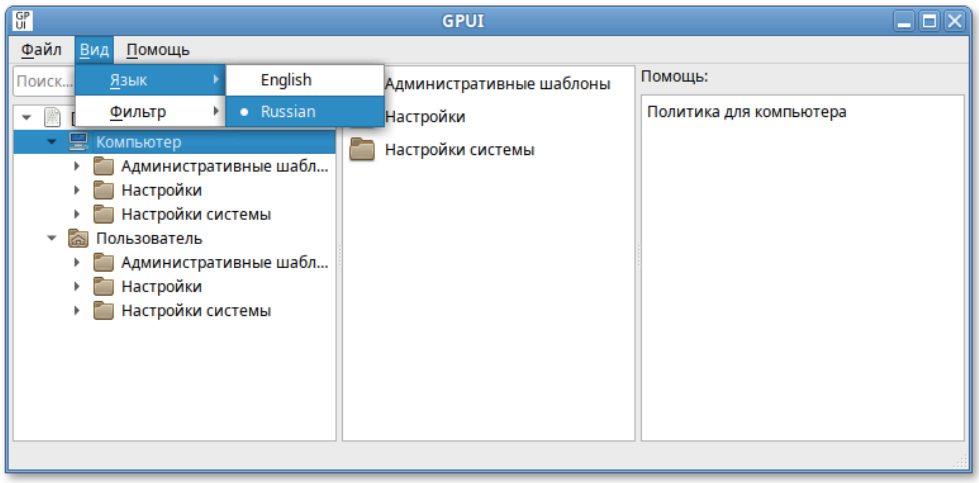


Рис. 271 – Выбор языка

9.2.5.4. Редактирование групповых политик

9.2.5.4.1. Включение или выключение различных служб (сервисов systemd)

Данные групповые политики позволяют управлять состоянием (включением или выключением) различных служб (сервисов systemd).

Для настройки политики следует перейти в «Компьютер» → «Административные шаблоны» → «Система ALT» → «Службы» → «Systemd» (рис. 272).

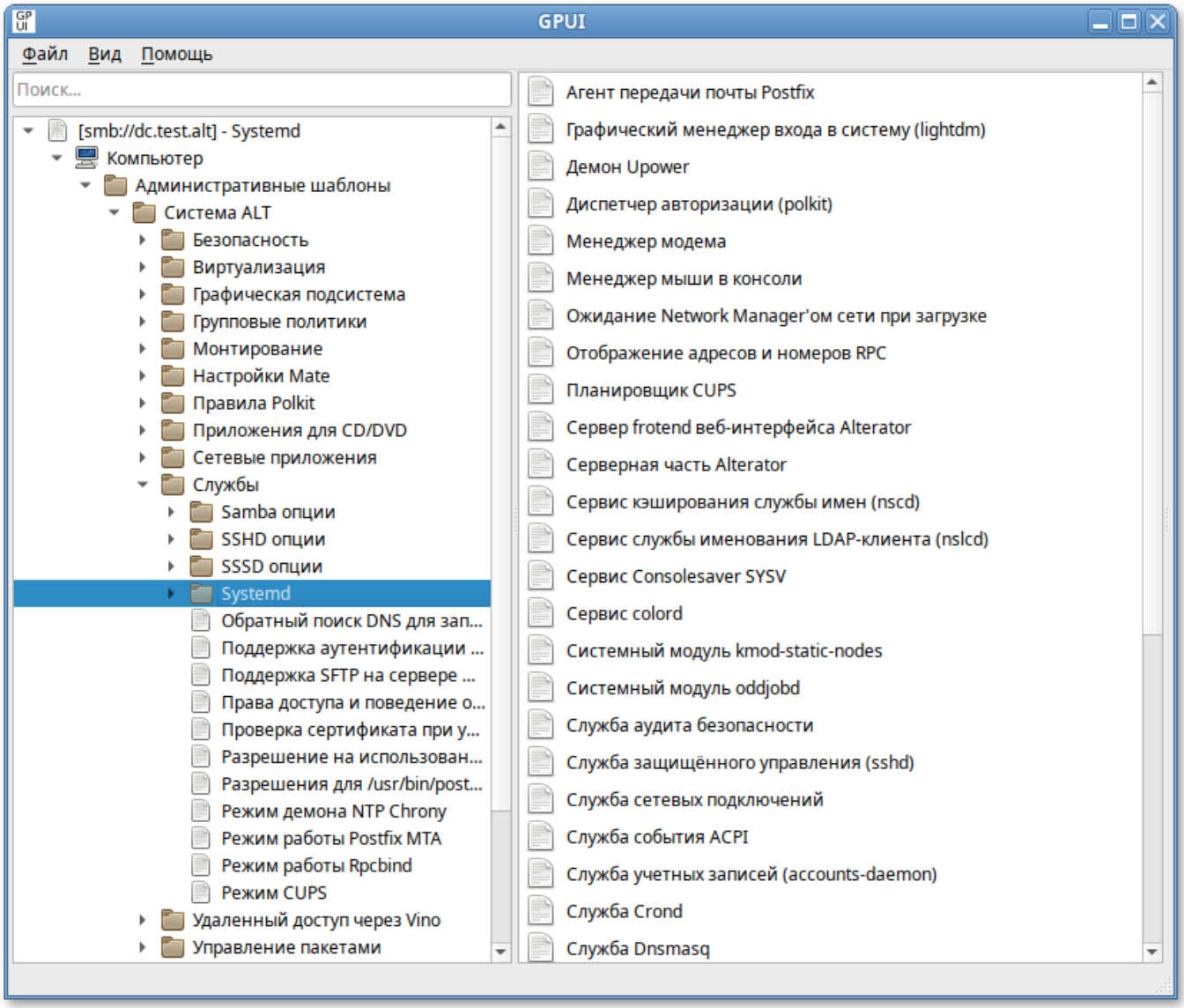


Рис. 272 – Путь для настройки политики

При выборе политики, откроется диалоговое окно настройки политики (рис. 273).

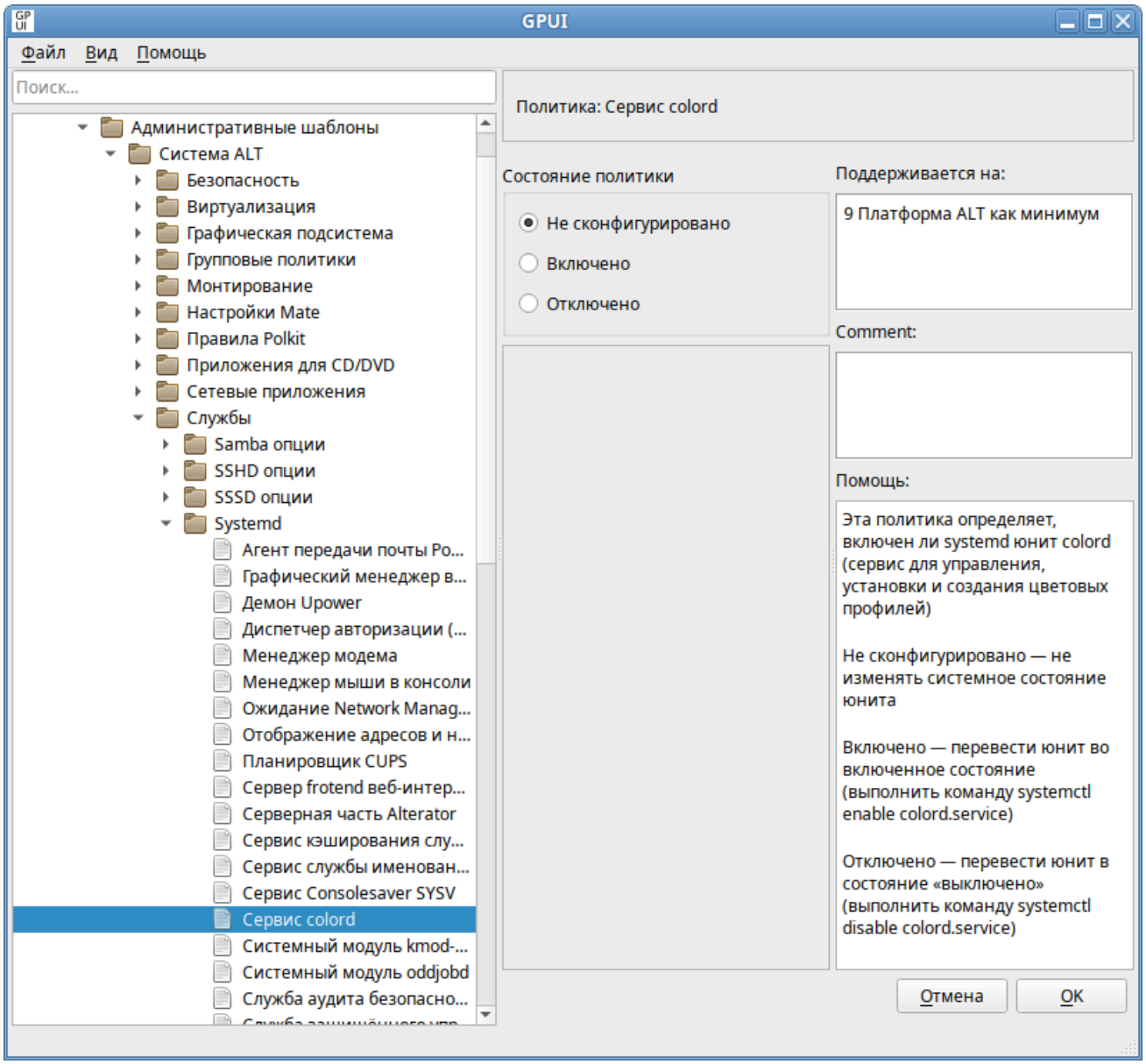


Рис. 273 – Диалоговое окно настройки политики

Можно не задавать настройку политики, включить или отключить:

- «Не сконфигурировано» – не изменять системное состояние службы;
- «Включено» – перевести службу во включенное состояние (выполнить команду `systemctl enable <служба>`);
- «Отключено» – перевести службу в состояние выключено (выполнить команду `systemctl disable <служба>`).

Список служб, состояние которых можно изменить, настроив соответствующую политику в GPUI, указан в таблице 17.

Таблица 17 – Список служб, состояние которых можно изменить, настроив соответствующую политику в GPUI

Служба	Описание	Сервис systemd
Менеджер модема	Политика определяет, включен ли systemd юнит диспетчера модемов	ModemManager.service
Ожидание Network Manager'ом сети при загрузке	Политика определяет, включен ли systemd юнит «Network Manager Wait Online»	NetworkManager-wait-online.service
Управление службой Network Manager	Политика определяет, включен ли systemd юнит «Network Manager»	NetworkManager.service
Служба учетных записей (accounts-daemon)	Политика определяет, включен ли systemd юнит службы учетных записей (accounts-daemon)	accounts-daemon.service
Служба события ACPI	Политика определяет, включен ли systemd юнит системной службы событий ACPI	acpid.service
Сервер frontend веб-интерфейса Alterator	Политика определяет, включен ли systemd юнит веб-сервера frotend WWW интерфейса Alterator	ahttpd.service
Серверная часть Alterator	Политика определяет, включен ли systemd юнит внутреннего сервера Alterator	alteratord.service
Служба аудита безопасности	Политика определяет, включен ли системный модуль службы аудита безопасности	auditd.service
Avahi mDNS/DNS-SD	Политика определяет, включен ли systemd юнит стека mDNS/DNS-SD Avahi	avahi-daemon.service
DNS-сервер BIND	Политика определяет, включен ли systemd юнит DNS-сервера (сервиса) BIND (Berkeley Internet Name Domain)	bind.service
	Политика определяет, включен ли systemd юнит NTP клиента/сервера Chronyd	chronyd.service
Сервис colord	Политика определяет, включен ли systemd юнит colord (сервис для управления, установки и создания цветовых профилей)	colord.service
Сервис Consolesaver SYSV	Политика определяет, включен ли systemd юнит Consolesaver (SYSV: этот пакет загружает конфигурацию энергосбережения консоли)	consolesaver.service
Cpufreq-simple сервис	Политика определяет, включен ли systemd юнит службы Cpufreq-simple (загружает модули ядра, которые требуются для масштабирования cpufreq)	cpufreq-simple.service
Служба Crond	Политика определяет, включен ли systemd юнит службы Cron	crond.service
Шина системных сообщений D-Bus	Политика определяет, включен ли systemd юнит шины системных сообщений D-Bus	dbus.service
Служба Dnsmasq	Политика определяет, включен ли systemd юнит службы Dnsmasq (облегченный DHCP и кэширующий DNS-сервер, а также TFTP-сервер для поддержки загрузки по сети)	dnsmasq.service

Окончание таблицы 17

Служба	Описание	Сервис systemd
Менеджер мыши в консоли	Политика определяет, включен ли sytemd юнит диспетчера мыши консоли	gpm.service
Системный модуль kmod-static-nodes	Политика определяет, включен ли systemd юнит kmod-static-nodes (создает список статических узлов устройства для текущего ядра)	kmod-static-nodes.service
Kerberos 5 KDC	Политика определяет, включен ли systemd юнит Kerberos 5 KDC	krb5kdc.service
Графический менеджер входа в систему (lightdm)	Политика определяет, включен ли systemd юнит службы графического менеджера входа в систему	lightdm.service
Служба сетевых подключений	Политика определяет, включен ли systemd юнит службы сетевых подключений	network.service
Samba NMB сервис	Политика определяет, включен ли systemd юнит сервиса Samba NMB	nmb.service
Сервис кэширования службы имен (nscd)	Политика определяет, включен ли systemd юнит сервиса кэширования службы имен	nscd.service
Сервис службы именования LDAP-клиента (nslcd)	Политика определяет, включен ли systemd юнит сервиса служб именования клиента LDAP	nslcd.service
Системный модуль oddjobd	Политика определяет, включен ли systemd юнит oddjobd (используется для запуска привилегированных операций для непривилегированных процессов)	oddjobd.service
SYSV: интерфейс терминала смарт-карт	Политика определяет, включен ли systemd юнит Openct (SYSV: терминал смарт-карт)	openct.service
Планировщик CUPS	Политика определяет, включен ли systemd юнит Service CUPS (планировщик)	org.cups.cupsd.service
Служба PC/SC Smart Card	Политика определяет, включен ли systemd юнит службы поддержки PC/SC Smart Card	pcscd.service
Диспетчер авторизации (polkit)	Политика определяет, включен ли systemd юнит диспетчера авторизации (polkit)	polkit.service
Агент передачи почты Postfix	Политика определяет, включен ли systemd юнит агента передачи почты Postfix	postfix.service
Сервис отображения универсальных адресов и номеров программ RPC	Политика определяет, включен ли systemd юнит RPC bind	rpcbind.service
Samba SMB сервис	Политика определяет, включен ли systemd юнит сервис Samba SMB	smb.service
Служба защищенного управления (sshd)	Политика определяет, включен ли systemd юнит демона сервера OpenSSH	sshd.service
Демон Upower	Политика определяет, включен ли systemd юнит Daemon Upower (управление питанием)	upower.service
Samba Winbind сервис	Политика определяет, включен ли systemd юнит Samba Winbind	winbind.service

9.2.5.4.2. Управление control framework

Через групповые политики реализовано управление настройками control.

control, использующийся в ОС Альт СП, механизм переключения между неким набором фиксированных состояний для задач, допускающих такой набор. Подсистема control используется для управления доступом к службам и позволяет переключать многие системные службы между заранее определенными состояниями.

Для настройки политики следует перейти в «Компьютер» → «Административные шаблоны» → «Система ALT». В этом разделе есть несколько подразделов, соответствующих категориям control (рис. 274).

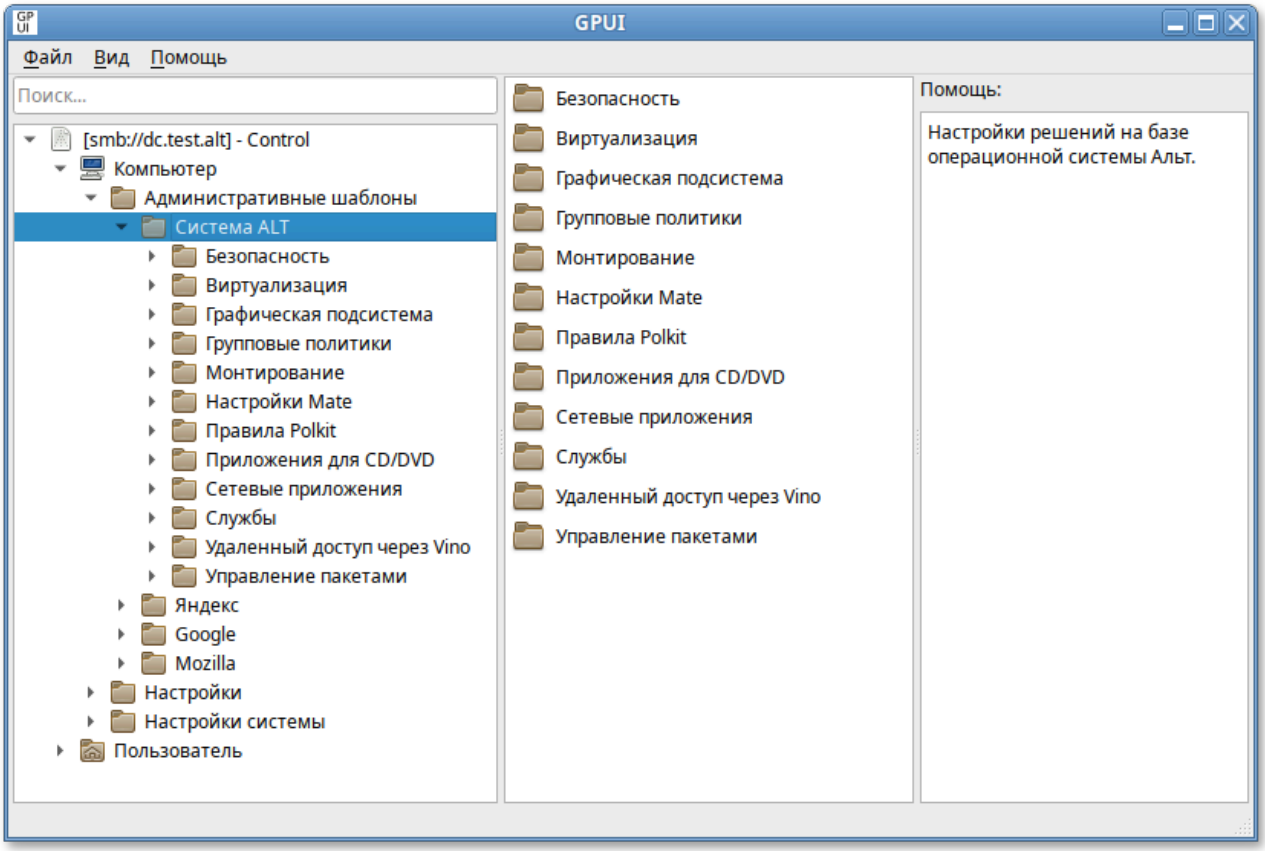


Рис. 274 – Подразделы, соответсвующие категориям control

После выбора категории, в правом окне редактора отобразится список политик (рис. 275).

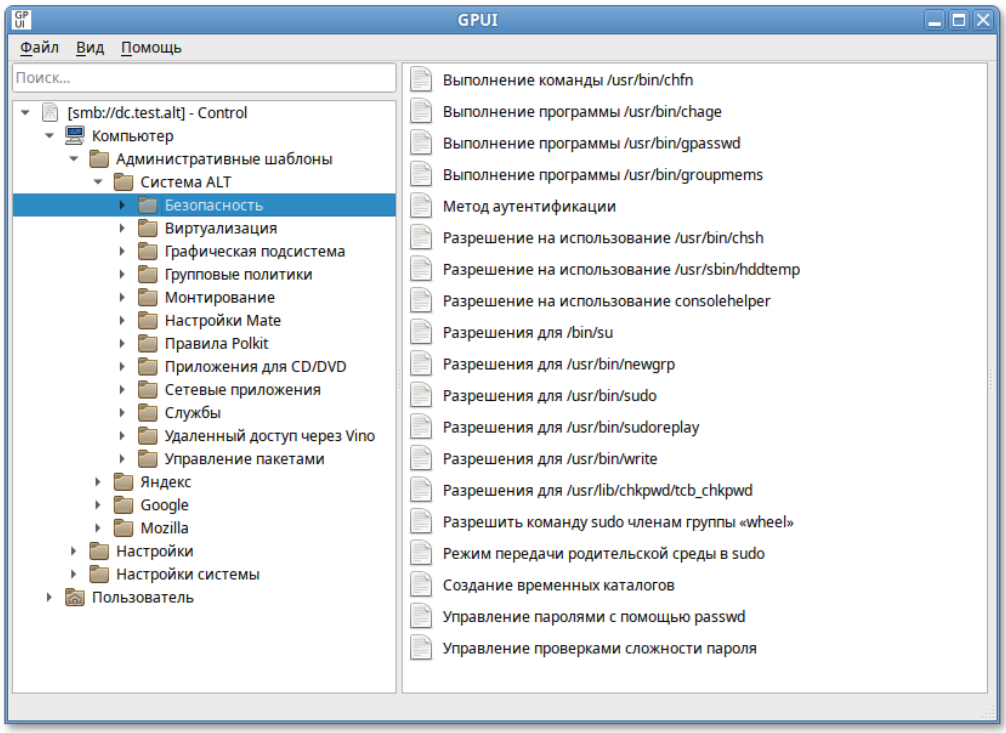


Рис. 275 – Список политик

При выборе политики, откроется диалоговое окно настройки политики (рис. 276).

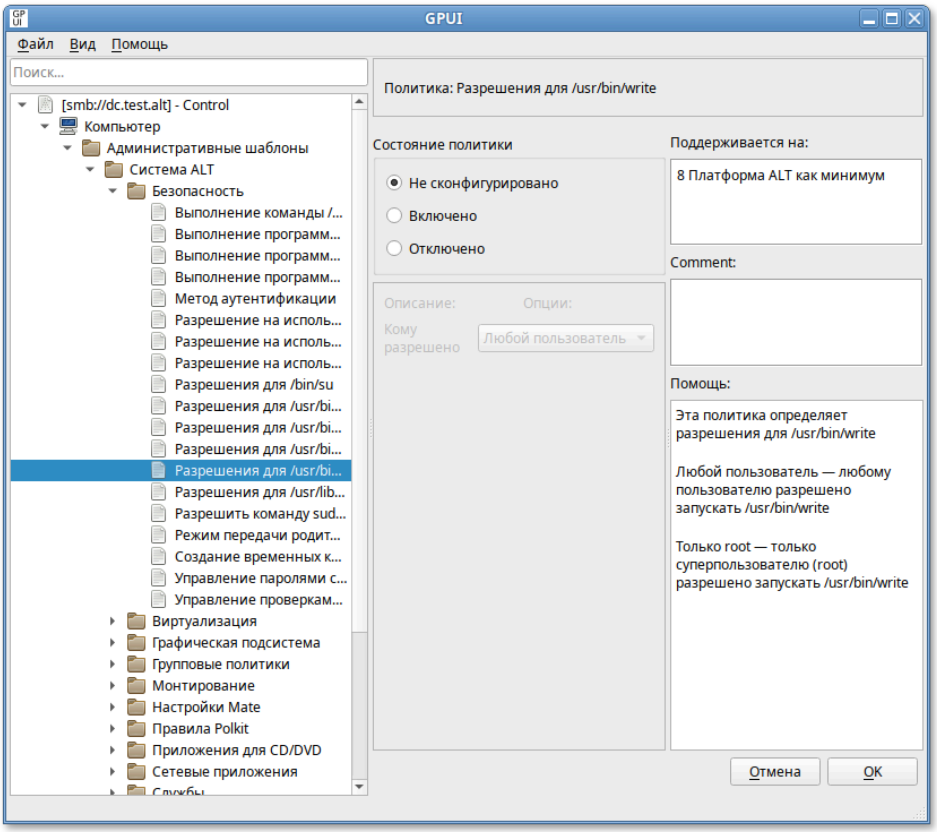


Рис. 276 – Диалоговое окно настройки политики

Можно не задавать настройку политики, включить или отключить. Если выбрать параметр «Включено», в разделе «Параметры» в выпадающем списке можно выбрать режим доступа для данного control (рис. 277).

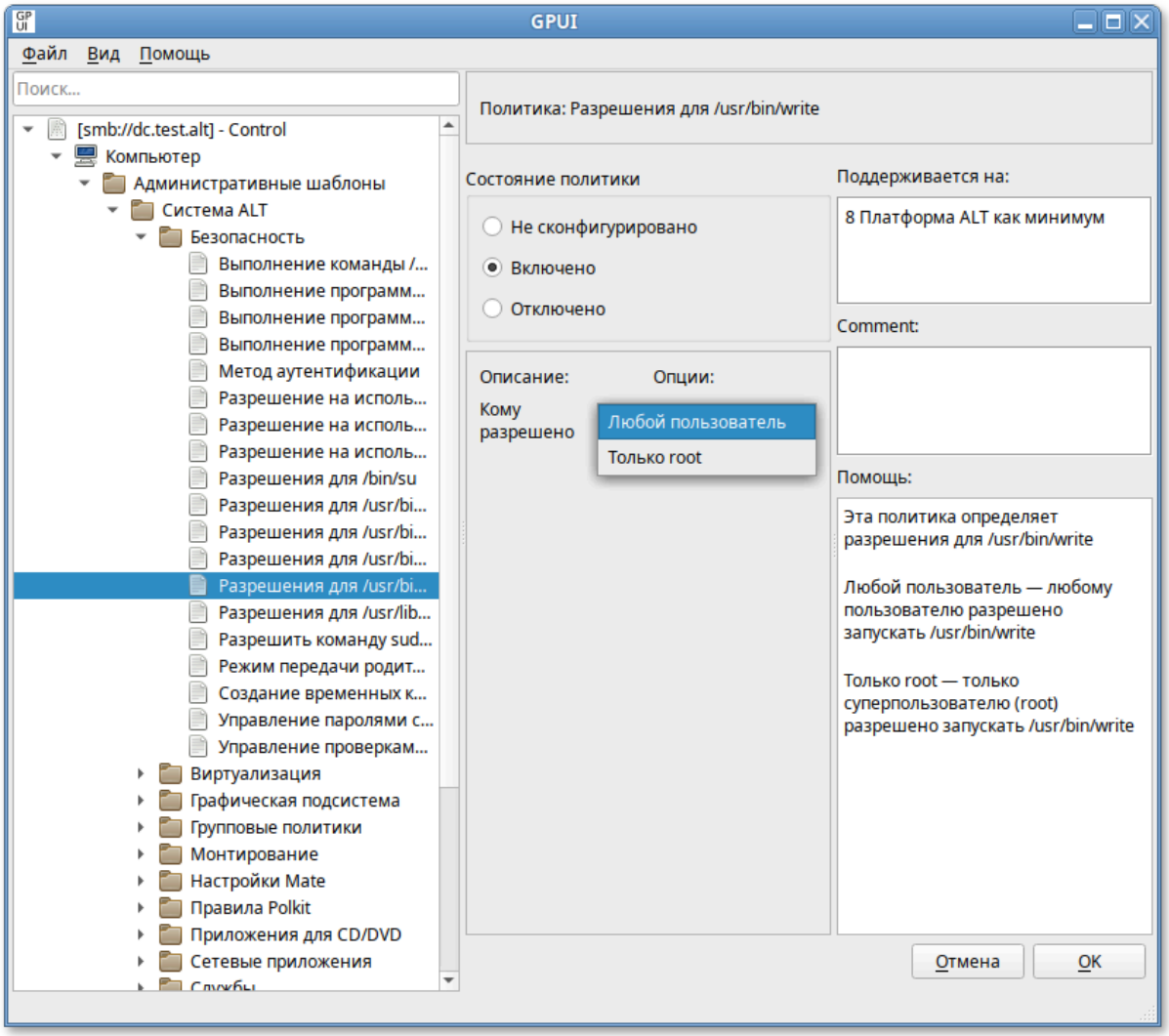


Рис. 277 – Режим доступа

Все control в GPUI разделены на категории:

- «Безопасность» (см. таблицу 18);
- «Службы» (см. таблицу 19);
- «Сетевые приложения» (см. таблицу 20);
- «Приложения для CD/DVD» (см. таблицу 21);
- «Монтирование» (см. таблицу 22);
- «Виртуализация» (см. таблицу 23);
- «Графическая подсистема» (см. таблицу 24).

Категория «Безопасность» приведена в таблице 18.

Т а б л и ц а 18 – Категория «Безопасность»

Политика	Control	Описание	Режимы
Выполнение программы `/usr/bin/chage`	chage	Политика позволяет контролировать доступ для выполнения программы `/usr/bin/chage`	«Только root» – только суперпользователь (root) может выполнить `/usr/bin/chage`. «Любой пользователь» – любой пользователь может просмотреть, когда ему следует сменить свой пароль, используя команду `chage -l имя_пользователя`
Выполнение программы `/usr/bin/chfn`	chfn	Политика позволяет контролировать поведение и права доступа к команде `chfn` (`/usr/bin/chfn`). Команда `chfn` может изменить полное имя пользователя, номер кабинета, номера офисного и домашнего телефона для учетной записи пользователя. Обычный пользователь может изменять поля только для своей учетной записи, с учетом ограничений в `/etc/login.defs` (конфигурация по умолчанию не позволяет пользователям менять свое полное имя)	«Только root» – только суперпользователь (root) может выполнить `/usr/bin/chfn`. «Любой пользователь» – любой пользователь может использовать команду `/usr/bin/chfn`
Разрешение на использование Consolehelper	consolehelper	Определяет права доступа к инструменту `consolehelper` (`/usr/lib/consolehelper/priv/auth`), который позволяет пользователям консоли запускать системные программы, выполняя аутентификацию через PAM. Когда это возможно, аутентификация выполняется графически; в противном случае выполняется в текстовой консоли, с которой был запущен `consolehelper`	«Любой пользователь» – любой пользователь может использовать `consolehelper`. «Только wheel» – только члены группы «wheel» могут использовать команду `consolehelper`. «Только root» – только суперпользователь (root) может использовать `consolehelper`

Продолжение таблицы 18

Политика	Control	Описание	Режимы
Выполнение программы `/usr/bin/chsh`	chsh	Политика позволяет управлять правами доступа к команде `chsh` (`/usr/bin/chsh`). Команда `chsh` позволяет изменить командную оболочку (или интерпретатор командной строки), запускаемую по умолчанию при регистрации пользователя в текстовой консоли (по умолчанию используется `/bin/bash`). Обычный пользователь может изменить командную оболочку только для своей учетной записи (командная оболочка должна быть перечислена в файле `/etc/shells`). Суперпользователь может изменить настройки для любой учетной записи (могут быть указаны любые значения)	«Только root» – только суперпользователь (root) может выполнить `/usr/bin/chsh`. «Все пользователи» – любой пользователь может использовать команду `/usr/bin/chsh`
Выполнение программы `usr/bin/gpasswd`	gpasswd	Определяет права на запуск инструмента `/usr/bin/gpasswd`	«Любой пользователь» – любой пользователь может выполнить `/usr/bin/gpasswd`. «Только wheel» – только члены группы «wheel» могут выполнять `/usr/bin/gpasswd`. «Только root» – только суперпользователь (root) может выполнить `/usr/bin/gpasswd`
Создание временных каталогов	pam_mktemp	Определяет, следует ли создавать отдельные временные каталоги для пользователей	«Отключено» – отключить создание отдельных временных каталогов для пользователей. «Включено» – включить создание отдельных временных каталогов для пользователей

Продолжение таблицы 18

Политика	Control	Описание	Режимы
Выполнение программы usr/bin/groupmems	groupmems	Определяет права на выполнение программы /usr/bin/groupmems	«Любой пользователь» – любой пользователь может выполнить /usr/bin/groupmems. «Только wheel» – только члены группы «wheel» могут выполнять команду /usr/bin/groupmems. «Только root» – только суперпользователь (root) может выполнить /usr/bin/groupmems
Выполнение программы usr/sbin/hddtemp	groupmems	Разрешение на использование инструмента usr/sbin/hddtemp – отслеживание температуры жесткого диска	«Любой пользователь» – любой пользователь может выполнить usr/sbin/hddtemp. «Только wheel» – только члены группы «wheel» могут выполнять usr/sbin/hddtemp. «Только root» – только суперпользователь (root) может выполнить usr/sbin/hddtemp
Разрешения для usr/bin/newgrp	newgrp	Разрешение на использование инструмента /usr/bin/newgrp	«Любой пользователь» – любой пользователь может выполнить /usr/bin/newgrp. «Только wheel» – только члены группы «wheel» могут выполнять /usr/bin/newgrp. «Только root» – только суперпользователь (root) может выполнить /usr/bin/newgrp

Продолжение таблицы 18

Политика	Control	Описание	Режимы
Управление паролями с помощью passwd	Passwd	Определяет политику управления паролями с помощью команды /usr/bin/passwd	«TCB» – любой пользователь может изменить свой пароль, используя /usr/bin/passwd, когда включена схема tcb. «Традиционный (схема tcb отключена)» – любой пользователь может изменить свой пароль, используя /usr/bin/passwd, когда схема tcb отключена. «Только root» – только суперпользователь (root) имеет право изменять пароли пользователей
Управление проверками сложности пароля	passwdqc-enforce	Политика управляет паролями для достаточной надежности пароля	«Все» – включить проверку сложности пароля для всех пользователей. «Только для пользователей» – включить проверку сложности пароля для всех пользователей, кроме суперпользователей
Разрешения для /bin/su	su	Определяет разрешения для /bin/su	«Любой пользователь» – любой пользователь может запускать /bin/su. «Все пользователи, кроме root» – любой пользователь может запускать /bin/su, но только пользователи группы «wheel» могут повышать привилегии суперпользователя. «Только wheel» – только пользователи из группы «wheel» могут запускать /bin/su. «Только root» – только суперпользователь (root) может запускать /bin/su

Продолжение таблицы 18

Политика	Control	Описание	Режимы
Разрешения для /usr/bin/sudo	sudo	Определяет разрешения для /usr/bin/sudo	«Любой пользователь» – любой пользователь может запускать /usr/bin/sudo. «Только wheel» – только пользователи из группы «wheel» могут запускать /usr/bin/sudo. «Только root» – только суперпользователь (root) может запускать /usr/bin/sudo
Режим передачи родительской среды в sudo	sudoers	Определяет, передаются ли переменные среды в sudo	«Строгий» – не передавать переменные окружения дочернему процессу. «Слабый» – передать переменные окружения дочернему процессу
Разрешения для /usr/bin/sudoreplay	sudoreplay	Определяет разрешения для /usr/bin/sudoreplay	«Любой пользователь» – любой пользователь может запускать /usr/bin/sudoreplay. «Только wheel» – только пользователи из группы «wheel» могут запускать /usr/bin/sudoreplay. «Только root» – только суперпользователь (root) может запускать /usr/bin/sudoreplay
Разрешить команду sudo членам группы «wheel»	sudowheel	Эта политика разрешает или запрещает членам группы «wheel» применять команду sudo. Если политика включена, пользователи, входящие в группу «wheel» могут повысить системные привилегии через команду sudo. Если политика не настроена или отключена, пользователи, входящие в группу «wheel» не смогут применить команду sudo	«Отключено» – пользователи группы «wheel» не могут повысить привилегии через команду sudo. «Включено» – пользователи группы «wheel» могут повысить привилегии через команду sudo

Окончание таблицы 18

Политика	Control	Описание	Режимы
Метод аутентификации	system-auth	Определяет метод аутентификации пользователя	«Winbind» – использовать Winbind для аутентификации. «SSSD» – использовать метод проверки подлинности демона System Security Services
Разрешения для `/usr/lib/chkpwd/tcb_chkpwd`	tcb_chkpwd	Определяет разрешения для привилегированного помощника `/usr/lib/chkpwd/tcb_chkpwd`	«Любой пользователь с отключенным tcb» – любой пользователь может быть аутентифицирован с использованием привилегированного помощника `/usr/lib/chkpwd/tcb_chkpwd` когда отключена схема `tcb`. «Любой пользователь с включенным tcb» – любой пользователь может аутентифицироваться с помощью привилегированного помощника `/usr/lib/chkpwd/tcb_chkpwd` если включена схема `tcb`. «Только root» – только суперпользователь (root) может быть аутентифицирован с помощью `/usr/lib/chkpwd/tcb_chkpwd`
Разрешения для `/usr/bin/write`	write	Определяет разрешения для `/usr/bin/write`	«Любой пользователь» – любой пользователь может запускать `/usr/bin/write`. «Только root» – только суперпользователь (root) может запускать `/usr/bin/write`

Т а б л и ц а 19 – Категория «Службы»

Политика	Control	Описание	Режимы
Права доступа и поведение очереди заданий `/usr/bin/at`	at	Политика позволяет контролировать поведение и права доступа для запуска очереди заданий (права доступа для запуска `/usr/bin/at`)	«Все пользователи» – всем пользователям разрешено запускать `/usr/bin/at`. «Только root» – только суперпользователь (root) может запускать `/usr/bin/at`. «Режим совместимости» – режим «atdaemon» (не должен использоваться)
Режим демона NTP Chrony	chrony	Политика определяет режим работы (конфигурацию) демона Chrony, который реализует функции сетевого протокола времени	«Сервер» – в файл конфигурации будет добавлена директива «allow all». «Клиент» – директива «allow» в файле конфигурации демона будет закомментирована
Разрешение на использование cron tab	crontab	Политика определяет права доступа к инструменту crontab (`/usr/bin/crontab`)	«Любой пользователь» – любой пользователь может использовать `/usr/bin/crontab`. «Только root» – только суперпользователь (root) может использовать `/usr/bin/crontab`
Режим CUPS	cups	Политика определяет поведение CUPS	«Внешний интерфейс IPP» – внешний интерфейс IPP доступен для пользователя. «Только локальные утилиты» – только локальные утилиты могут работать с CUPS
Обратный поиск DNS для запросов OpenLDAP	ldap-reverse-dns-lookup	Политика определяет, разрешен ли обратный поиск DNS для запросов OpenLDAP	«Разрешить» – выполнять обратный поиск DNS для запросов OpenLDAP. «Не разрешать» – не выполнять обратный поиск DNS для запросов OpenLDAP. «По умолчанию» – выполнять обратный поиск DNS для запросов OpenLDAP

Продолжение таблицы 19

Политика	Control	Описание	Режимы
Проверка сертификата при установлении соединений TLS OpenLDAP	ldap-tls-cert-chec	Политика определяет режим проверки сертификата при установке TLS соединений OpenLDAP	«По умолчанию» – установить соединение только с правильным сертификатом. «Разрешить» – установить соединение, даже если сертификат отсутствует или неверный. «Пробовать» – установить соединение, если нет или с действующим сертификатом. «Требовать» – установить соединение только с правильным сертификатом. «Никогда» – не выполнять никаких проверок
Режим работы Postfix MTA	postfix	Политика определяет режим работы MTA Postfix (почтовый транспортный агент)	«Локальный (отключен)» – Postfix MTA отключен. «Сервер (фильтры отключены)» – Postfix MTA включен без почтовых фильтров. «Фильтр» – Postfix MTA включен с почтовыми фильтрами
Разрешения для `/usr/bin/postqueue`	postqueue	Определяет разрешения для `/usr/bin/postqueue`	«Любой пользователь» – любому пользователю разрешено запускать `/usr/bin/postqueue`. «Группа mailadm» – пользователям из группы «mailadm» разрешено запускать `/usr/bin/postqueue`. «Только root» – только суперпользователю (root) разрешено запускать `/usr/bin/postqueue`
Режим работы Rpcbind	rpcbind	Политика определяет режим работы rpcbind (`/sbin/rpcbind`)	«Сервер» – rpcbind будет прослушивать входящие соединения из сети. «Локальный» – rpcbind будет принимать только локальные запросы
Поддержка SFTP на сервере OpenSSH	sftp	Политика определяет поддержку SFTP на сервере OpenSSH	«Включено» – включить поддержку SFTP на сервере OpenSSH. «Отключено» – отключить поддержку SFTP на сервере OpenSSH

Продолжение таблицы 19

Политика	Control	Описание	Режимы
Поддержка аутентификации OpenSSH-клиентов через GSSAPI	ssh-gssapi-auth	Эта политика определяет функциональные возможности поддержки аутентификации OpenSSH-клиентов через GSSAPI	«Включено» – поддержка аутентификации через GSSAPI для OpenSSH-клиентов включена. «Отключено» – поддержка аутентификации через GSSAPI для OpenSSH-клиентов отключена
Samba опции			
Гостевой доступ к общим каталогам	smb-conf-usershare-allow-guests	Политика управляет возможностью предоставления гостевого доступа общему ресурсу. Данная политика управляет параметром usershare allow guests в файле `/etc/samba/usershares.conf`.	«Включено» – разрешить предоставление гостевого доступа к общему ресурсу; разрешить создание общих каталогов с параметром доступа без авторизации (`usershare allow guests = yes`). «Отключено» – запретить предоставление гостевого доступа к общему ресурсу; запретить создание общих каталогов с параметром доступа без авторизации (`usershare allow guests = no`)
Доступ к общим каталогам других пользователей	smb-conf-usershare-owner-only	Политика управляет правом пользователя на предоставление общего доступа или доступ к каталогу, если пользователь не является владельцем этого каталога. Данная политика управляет параметром usershare owner only в файле `/etc/samba/usershares.conf`.	«Включено» – запретить предоставление общего доступа не владельцу каталога; запретить доступ к общим каталогам пользователей, без проверки владельца каталога (`usershare owner only = yes`). «Отключено» – разрешить предоставление общего доступа не владельцу каталога; разрешить доступ к общим каталогам пользователей, без проверки владельца каталога (`usershare owner only = no`)

Продолжение таблицы 19

Политика	Control	Описание	Режимы
Запрет на создание общих каталогов в системных каталогах	smb-conf-usershare-deny-list	Данная политика управляет параметром usershare prefix deny list в файле `/etc/samba/usershares.conf` – открывая или закрывая комментарием этот параметр. Параметр usershare prefix deny list определяет каталоги в корневом каталоге (/), в которых пользователю запрещено создавать общие каталоги. Если абсолютный путь к общему каталогу пользователя начинается с одного из перечисленных каталогов, то доступ к нему будет запрещен. Таким образом ограничивается список каталогов, в которых возможно создавать общие пользовательские каталоги. По умолчанию в параметре usershare prefix deny list заданы каталоги: `/etc`, `/dev`, `/sys`, `/proc`. Если настроен список запрещенных каталогов `usershare prefix deny list`, и список разрешенных каталогов `usershare prefix allow list`, сначала обрабатывается список запрета, а затем уже список разрешений.	«Включено» – включить список запрещенных каталогов (параметр usershare prefix deny list будет раскомментирован). «Отключено» – отключить список запрещенных каталогов (параметр usershare prefix deny list будет закомментирован)

Продолжение таблицы 19

Политика	Control	Описание	Режимы
Разрешение на создание общих каталогов в системных каталогах	smb-conf-usershare-allow-list	Данная политика управляет параметром usershare prefix allow list в файле `/etc/samba/usershares.conf` – открывая или закрывая комментарием этот параметр. Параметр usershare prefix allow list определяет каталоги в корневом каталоге (/), в которых пользователю разрешено создавать общие каталоги. Если абсолютный путь к общему каталогу пользователя не начинается с одного из перечисленных каталогов, то доступ к нему будет запрещен. Таким образом ограничивается список каталогов, в которых возможно создавать общие пользовательские каталоги. По умолчанию в параметре usershare prefix allow list заданы каталоги: `/home`, `/srv`, `/mnt`, `/media`, `/var`. Если настроен список запрещенных каталогов `usershare prefix deny list`, и список разрешенных каталогов `usershare prefix allow list`, сначала обрабатывается список запрета, а затем уже список разрешений.	«Включено» – включить список разрешенных каталогов (параметр usershare prefix allow list будет раскомментирован). «Отключено» –отключить список разрешенных каталогов (параметр usershare prefix allow list будет закомментирован)

Продолжение таблицы 19

Политика	Control	Описание	Режимы
Доступ членам группы «sambashare» к управлению общими каталогами	role-sambashare	Политика управляет разрешением членам группы «sambashare» управлять общими каталогами. Конфигурации пользовательских общих ресурсов расположены в каталоге `/var/lib/samba/usershares`, права на запись в котором имеют члены группы «usershares». Данная политика позволяет расширить привилегии членов группы «sambashare», добавляя их в группу «usershares».	«Включено» – разрешить членам группы «sambashare» управлять общими каталогами. «Отключено» – запретить членам группы «sambashare» управлять общими каталогами
Доступ членам группы «users» к управлению общими каталогами	role-usershares	Политика управляет разрешением членам группы «users» управлять общими каталогами. Конфигурации пользовательских общих ресурсов расположены в каталоге `/var/lib/samba/usershares`, права на запись в котором имеют члены группы «usershares». Данная политика позволяет расширить привилегии членов группы «users», добавляя их в группу «usershares».	«Включено» – разрешить членам группы «users» управлять общими каталогами. «Отключено» – запретить членам группы «users» управлять общими каталогами. Данный параметр также влияет на разрешение управления общими каталогами через настройку предпочтений
Разрешение на создание пользовательских общих каталогов	smb-conf-usershare	Политика управляет возможностью создания пользовательских общих каталогов на компьютере.	«Включено» – включить возможность создания и использования общих каталогов пользователей (`usershare max shares = 100`).

Продолжение таблицы 19

Политика	Control	Описание	Режимы
		Данная политика управляет параметром usershare max shares в файле `/etc/samba/usershares.conf`, который устанавливает предельное число общих каталогов.	«Отключено» –отключить возможность создания и использования общих каталогов пользователей (`usershare max shares = 0`)
SSHD опции			
Контроль доступа по группам к серверу OpenSSH	ssh-gssapi-auth	Эта политика включает в службе удаленного доступа OpenSSH контроль доступа по списку разрешенных групп	«Включено» –контроль доступа по группам для службы удаленного доступа OpenSSH включен. «Отключено» – контроль доступа по группам для службы удаленного доступа OpenSSH отключен
Группы для контроля доступа к серверу OpenSSH	sshd-allow-groups-list	Эта политика определяет, какие группы входят в список разрешенных для службы удаленного доступа к серверу OpenSSH	«Все пользователи» – разрешить доступ к серверу OpenSSH для групп «wheel» и «users». «Группы wheel и remote» – разрешить доступ к серверу OpenSSH для групп администраторов и пользователей удаленного доступа («wheel» и «remote»). «Только wheel» – разрешить доступ к серверу OpenSSH только для группы администраторов («wheel»). «Только remote» – разрешить доступ к серверу OpenSSH только для группы «remote»
Поддержка GSSAPI-аутентификации на сервере OpenSSH	sshd-gssapi-auth	Эта политика включает поддержку аутентификации с использованием GSSAPI на сервере OpenSSH	«Включено» –поддержка GSSAPI на сервере OpenSSH включена. «Отключено» –поддержка GSSAPI на сервере OpenSSH отключена

Продолжение таблицы 19

Политика	Control	Описание	Режимы
Аутентификация по паролю на сервере OpenSSH	sshd-password-auth	Эта политика включает поддержку аутентификации по паролю на сервере OpenSSH	«Включено» –поддержка аутентификации по паролю на сервере OpenSSH включена. «Отключено» –поддержка аутентификации по паролю на сервере OpenSSH отключена
Аутентификация суперпользователя на сервере OpenSSH	sshd-permit-root-login	Эта политика определяет режимы аутентификации для суперпользователя (root) на сервере OpenSSH	«Только без пароля» – суперпользователю разрешена только беспарольная аутентификация на сервере OpenSSH. «Разрешено» – суперпользователю разрешена аутентификация на сервере OpenSSH. «Запрещено» – суперпользователю запрещена аутентификация на сервере OpenSSH. «По умолчанию» –сбросить режим аутентификации для суперпользователя на значение по умолчанию в пакете
SSSD опции			
Игнорирование политик при недоступности GPT	sssd-ad-gpo-ignore-unreadable	Эта настройка определяет будут ли проигнорированы правила управления доступом в SSSD основанные на групповых политиках, если недоступен какой-либо шаблон (GPT) объекта групповой политики (GPO)	«Включить» –игнорировать правила управления доступом через групповые политики, если шаблоны групповых политик не доступны для SSSD. «Отключить» – запретить доступ пользователям SSSD AD, которым назначены групповые политики, если шаблоны групповых политик не доступны. «По умолчанию» – настройка игнорирования политик, при недоступности шаблонов групповых политик сброшена на значение по умолчанию в пакете

Продолжение таблицы 19

Политика	Control	Описание	Режимы
Контроль доступа в SSSD через групповые политики	sssd-ad-gpo-access-control	Эта политика определяет в каком режиме будет осуществляться контроль доступа в SSSD основанный на групповых политиках Active Directory (GPO)	«Принудительный режим» – правила управления доступом в SSSD основанные на GPO выполняются, ведется логирование. «Разрешающий режим» – правила управления доступом в SSSD основанные на GPO не выполняются, ведется только логирование. Такой режим требуется администратору, чтобы оценить как срабатывают новые правила. «Отключить» – правила управления доступом в SSSD основанные на GPO не логируются и не выполняются. «По умолчанию» – настройка контроля доступом в SSSD основанное на GPO сброшена на значение по умолчанию в пакете
Кэширование учетных данных пользователей	sssd-cache-credentials	Эта политика определяет, будут ли учетные данные удаленных пользователей сохраняться в локальном кэше SSSD	«Включить» –сохранение в локальном кэше SSSD учетных данных пользователей включено. «Отключить» –сохранение в локальном кэше SSSD учетных данных пользователей отключено. «По умолчанию» – настройка сохранения в локальном кэше SSSD учетных данных пользователей сброшена на значение по умолчанию в пакете

Окончание таблицы 19

Политика	Control	Описание	Режимы
Режим привилегий службы SSSD	sssd-drop-privileges	Эта политика позволяет сбросить права службы SSSD, чтобы избежать работы от имени суперпользователя (root)	«Привилегированный» – служба SSSD запущена от имени привилегированного суперпользователя (root). «Непривилегированный» – служба SSSD запущена от имени непривилегированного пользователя (_sssd). «По умолчанию» –режим привилегий службы SSSD задан по умолчанию в пакете
Обновление DNS-записей прямой зоны	sssd-dyndns-update	Эта политика позволяет включить или отключить автоматическое обновление DNS-записей (защищенных с помощью GSS-TSIG) с IP-адресом клиента через SSSD	«Включить» – автоматическое обновление DNS-записи клиента через SSSD включено. «Отключить» – автоматическое обновление DNS-записи клиента через SSSD отключено. «По умолчанию» – настройка автоматического обновления DNS-записи клиента через SSSD задана по умолчанию в пакете
Обновление DNS-записей обратной зоны	sssd-dyndns-update-ptr	Данная политика определяет будет ли обновляться клиентская PTR-запись (защищенная с помощью GSS-TSIG). Эта политика работает только если включено «Обновление DNS-записей прямой зоны»	«Включить» – автоматическое обновление DNS-записи обратной зоны через SSSD включено. «Отключить» – автоматическое обновление DNS-записи обратной зоны через SSSD отключено. «По умолчанию» – настройка автоматического обновления DNS-записи обратной зоны задана по умолчанию в пакете

Т а б л и ц а 20 – Категория «Сетевые приложения»

Политика	Control	Описание	Режимы
Разрешение на использование /usr/bin/mtr	mtr	Разрешение на использование сетевого инструмента /usr/bin/mtr	«Любой пользователь» – любой пользователь может выполнить /usr/bin/mtr. «Группа netadmin» – только члены группы «netadmin» могут выполнять /usr/bin/mtr. «Только root» – только суперпользователь (root) может выполнить /usr/bin/mtr
Разрешения для /usr/bin/ping	ping	Эта политика определяет разрешения для /usr/bin/ping	«Любой пользователь» – любой пользователь может запускать /usr/bin/ping. «Группа netadmin» – пользователям из группы «netadmin» разрешено запускать /usr/bin/ping. «Только root» – только суперпользователь (root) может запускать /usr/bin/ping. «Любой пользователь (в контейнерах)» – любой пользователь может запускать /usr/bin/ping (в контейнерах). «Группа netadmin (в контейнерах)» – пользователям из группы «netadmin» разрешено запускать /usr/bin/ping (в контейнерах)
Разрешения для /usr/sbin/pppd	ppp	Эта политика определяет разрешения для /usr/sbin/pppd	«Только root» – только суперпользователю (root) разрешено запускать /usr/sbin/pppd. «Традиционный» – любой пользователь имеет право запустить /usr/sbin/pppd без повышения привилегий. «Группа uucp» – пользователям из группы «uucp» имеют право запускать /usr/sbin/pppd с правами суперпользователя. «Любой пользователь» – любой пользователь имеет право запускать /usr/sbin/pppd с правами суперпользователя
Разрешения для wireshark-capture (dumpcap)	wireshark-capture	Эта политика определяет функциональные возможности (режимы) разрешения для захвата wireshark (/usr/bin/dumpcap)	«Любой пользователь» – любой пользователь имеет право запустить /usr/bin/dumpcap, захват трафика включен. «Любой пользователь, без захвата трафика» – любой пользователь имеет право запустить /usr/bin/dumpcap, захват трафика отключен. «Группа netadmin» – пользователям из группы «netadmin» имеют право запускать /usr/bin/dumpcap. «Только root» – только суперпользователь (root) может запускать /usr/bin/dumpcap

Т а б л и ц а 21 – Категория «Приложения для CD/DVD»

Политика	Control	Описание	Режимы
Разрешение на использование `/usr/bin/dvd-ram-control`	dvd-ram-control	Эта политика определяет права доступа к `/usr/bin/dvd-ram-control`	«Только cdwriter» – только члены группы «cdwriter» могут выполнять `/usr/bin/dvd-ram-control`. «Только root» – только суперпользователь (root) может выполнять `/usr/bin/dvd-ram-control`. «Режим совместимости» – режим совместимости, не должен использоваться
Разрешения на использование `/usr/bin/dvd+rw-booktype`	dvd+rw-booktype	Эта политика определяет права доступа к `/usr/bin/dvd+rw-booktype`	«Только cdwriter» – только члены группы «cdwriter» могут выполнять `/usr/bin/dvd+rw-booktype`. «Только root» – только суперпользователь (root) может выполнять `/usr/bin/dvd+rw-booktype`. «Режим совместимости» – режим совместимости, не должен использоваться
Разрешения на использование `/usr/bin/dvd+rw-format`	dvd+rw-format	Эта политика определяет права доступа к `/usr/bin/dvd+rw-format`	«Только cdwriter» – только члены группы «cdwriter» могут выполнять `/usr/bin/dvd+rw-format`. «Только root» – только суперпользователь (root) может выполнять `/usr/bin/dvd+rw-format`. «Режим совместимости» – режим совместимости, не должен использоваться
Разрешения на использование `/usr/bin/dvd+rw-mediainfo`	dvd+rw-mediainfo	Эта политика определяет права доступа к `/usr/bin/dvd+rw-mediainfo`	«Только cdwriter» – только члены группы «cdwriter» могут выполнять `/usr/bin/dvd+rw-mediainfo`. «Только root» – только суперпользователь (root) может выполнять `/usr/bin/dvd+rw-mediainfo`. «Режим совместимости» – режим совместимости, не должен использоваться
Разрешения на использование `/usr/bin/growisofs`	growisofs	Эта политика определяет права на использование инструмента `/usr/bin/growisofs`	«Только cdwriter» – только члены группы «cdwriter» могут выполнять `/usr/bin/growisofs`. «Только root» – только суперпользователь (root) может выполнять `/usr/bin/growisofs`. «Режим совместимости» – режим совместимости, не должен использоваться

Т а б л и ц а 22 – Категория «Монтирование»

Политика	Control	Описание	Режимы
Доступ к инструментам FUSE	fusermount	Эта политика определяет права доступа для монтирования файловой системы FUSE (выполнение программ `/usr/bin/fusermount` и `/usr/bin/fusermount3`)	«Любой пользователь» – любой пользователь может выполнить `/usr/bin/fusermount` и `/usr/bin/fusermount3`. «Только fuse» – только члены группы «fuse» могут выполнять `/usr/bin/fusermount` и `/usr/bin/fusermount3`. «Только wheel» – только члены группы «wheel» могут выполнять `/usr/bin/fusermount` и `/usr/bin /fusermount3`. «Только root» – только суперпользователь (root) может выполнить `/usr/bin/fusermount` и `/usr/bin /fusermount3`
Разрешения для `/bin/mount` и `/bin/umount`	mount	Эта политика определяет разрешения для `/bin/mount` и `/bin/umount`	«Любой пользователь» – любому пользователю разрешено запускать `/bin/mount` и `/bin/umount`. «Группа wheel» – пользователям из группы «wheel» разрешено запускать `/bin/mount` и `/bin/umount`. «Непривилегированный пользователь» – любой пользователь может запускать `/bin/mount` и `/bin/umount` для непривилегированных действий (не от имени root). «Только root» – только суперпользователь (root) может запускать `/bin/mount` и `/bin/umount`
Разрешения для `/sbin/mount.nfs`	nfsmount	Эта политика определяет разрешения для `/sbin/mount.nfs`	«Любой пользователь» – любому пользователю разрешено запускать `/sbin/mount.nfs` «Только wheel» – пользователям из группы «wheel» разрешено запускать `/sbin/mount.nfs` «Только root» – только суперпользователю (root) может запускать `/sbin/mount.nfs`
Правила подключения USB-накопителей	udisks2	Эта политика определяет правила подключения USB-накопителей	«По умолчанию» – подключить накопитель индивидуально (/run/media/$user/) для каждого пользователя. «Общий» – подключить накопитель к общедоступной точке (`/media/`)

Т а б л и ц а 23 – Категория «Виртуализация»

Политика	Control	Описание	Режимы
Права на устройства QEMU KVM	kvm	Политика определяет права на устройства QEMU KVM	«Любой пользователь» – любой пользователь имеет право использовать KVM. «Группа vmusers» – пользователи группы «vmusers» имеют право использовать KVM. «Только root» – только суперпользователь (root) имеет право использовать KVM
Разрешения для VirtualBox	virtualbox	Эта политика определяет разрешения для VirtualBox	«Любой пользователь» – любому пользователю разрешено использовать VirtualBox. «Группа vboxusers» – пользователям из группы «vboxusers» разрешено использовать VirtualBox. «Только root» – только суперпользователю (root) разрешено использовать VirtualBox

Т а б л и ц а 24 – Категория «Графическая подсистема»

Политика	Control	Описание	Режимы
Список пользователей в greeter (LightDM)	lightdm-greeter-hide-users	Эта политика определяет, будет ли показан список всех пользователей при входе в систему с помощью LightDM (в greeter – на экране приветствия/входа в систему LightDM) или нет	«Показать» – показать список доступных пользователей в greeter. «Скрыть» – не перечислять всех пользователей в greeter
Стандартные каталоги в home	xdg-user-dirs	Эта политика определяет, работает ли функция стандартных каталогов (Документы, Загрузки, Изображения и т.д.) xdg-user-dirs в домашнем каталоге (home) пользователя	«Отключено» – функция сохранения списка пользовательских каталогов отключена. «Группа vboxusers» – функция сохранения списка пользовательских каталогов включена
Разрешения для Xorg	xorg-server	Эта политика определяет разрешения для Xorg (`/usr/bin/Xorg`)	«Любой пользователь» – любому пользователю разрешено запускать `/usr/bin/Xorg`. «Группа xgrp» – пользователям группы «xgrp» разрешено запускать `/usr/bin/Xorg`. «Только root» – только суперпользователь (root) может запускать `/usr/bin/Xorg`

9.2.5.4.3. Управление настройками службы Polkit

Через групповые политики реализовано управление настройками службы Polkit (PolicyKit).

В настоящий момент реализованы следующие настройки:

- разрешения Udisks2 – формирование правил PolKit для монтирования файловых систем (демон udisk2);
- разрешения PackageKit – формирование правил PolKit для установки, удаления, обновления пакетов;
- разрешения NetworkManager – формирование правил PolKit для операций с сетевыми подключениями и настройкой сетевых интерфейсов;
- разрешения для работы с токенами и смарт-картами – формирование правил PolKit для работы с токенами и смарт-картами.

Для настройки политики следует перейти в «Компьютер»/«Пользователь» → «Административные шаблоны» → «Система ALT» → «Правила Polkit». Выбрать раздел, в правом окне редактора отобразится список политик (рис. 278).

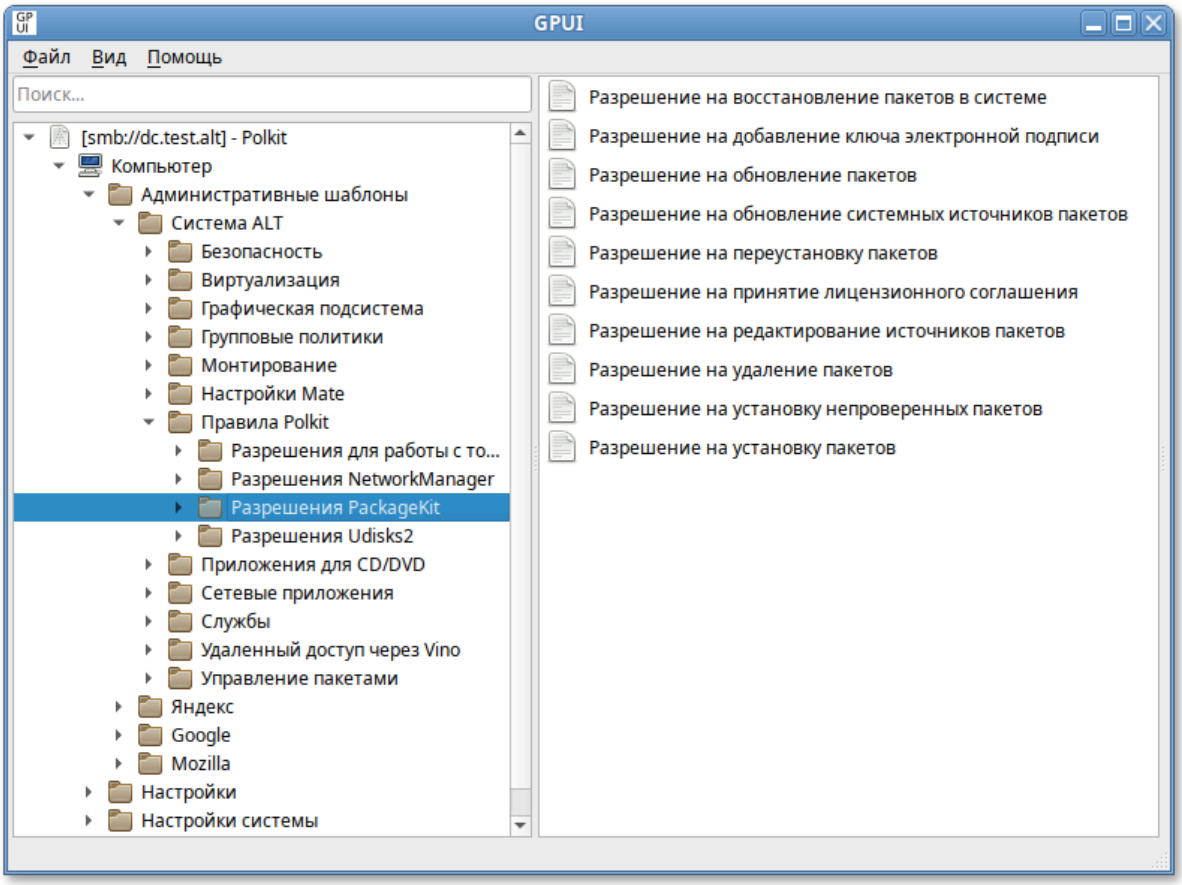


Рис. 278 – Список политик в разделе

При выборе политики, откроется диалоговое окно настройки политики (рис. 279).

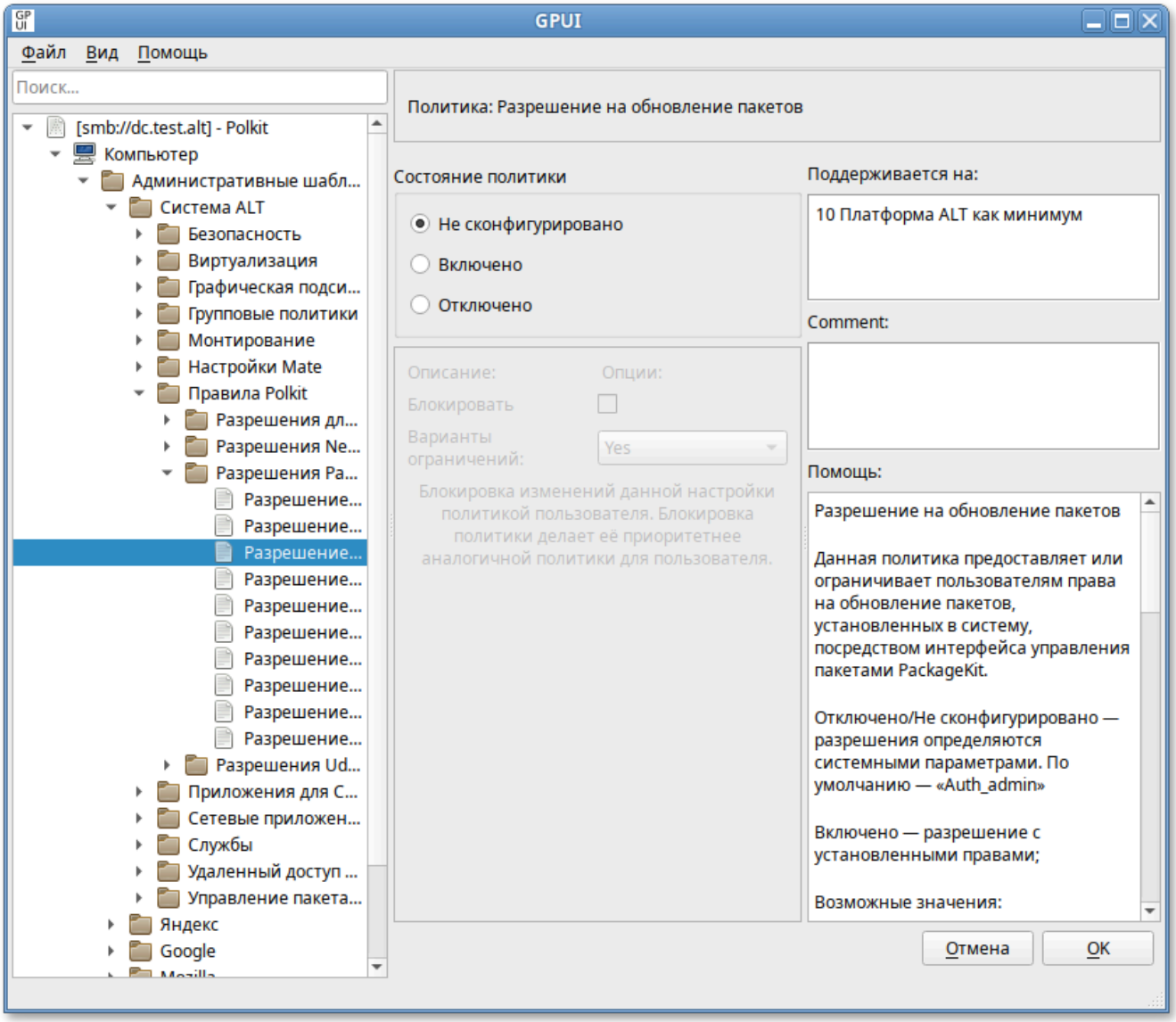


Рис. 279 – Диалоговое окно настройки политики

Можно не задавать настройку политики, включить или отключить. Если политика находится в состоянии «Отключено»/«Не сконфигурировано» разрешения определяются системными параметрами (по умолчанию – «Auth_admin»). Если выбрать параметр «Включено», в разделе «Опции» в выпадающем списке можно выбрать вариант ограничения для данного разрешения (рис. 280).

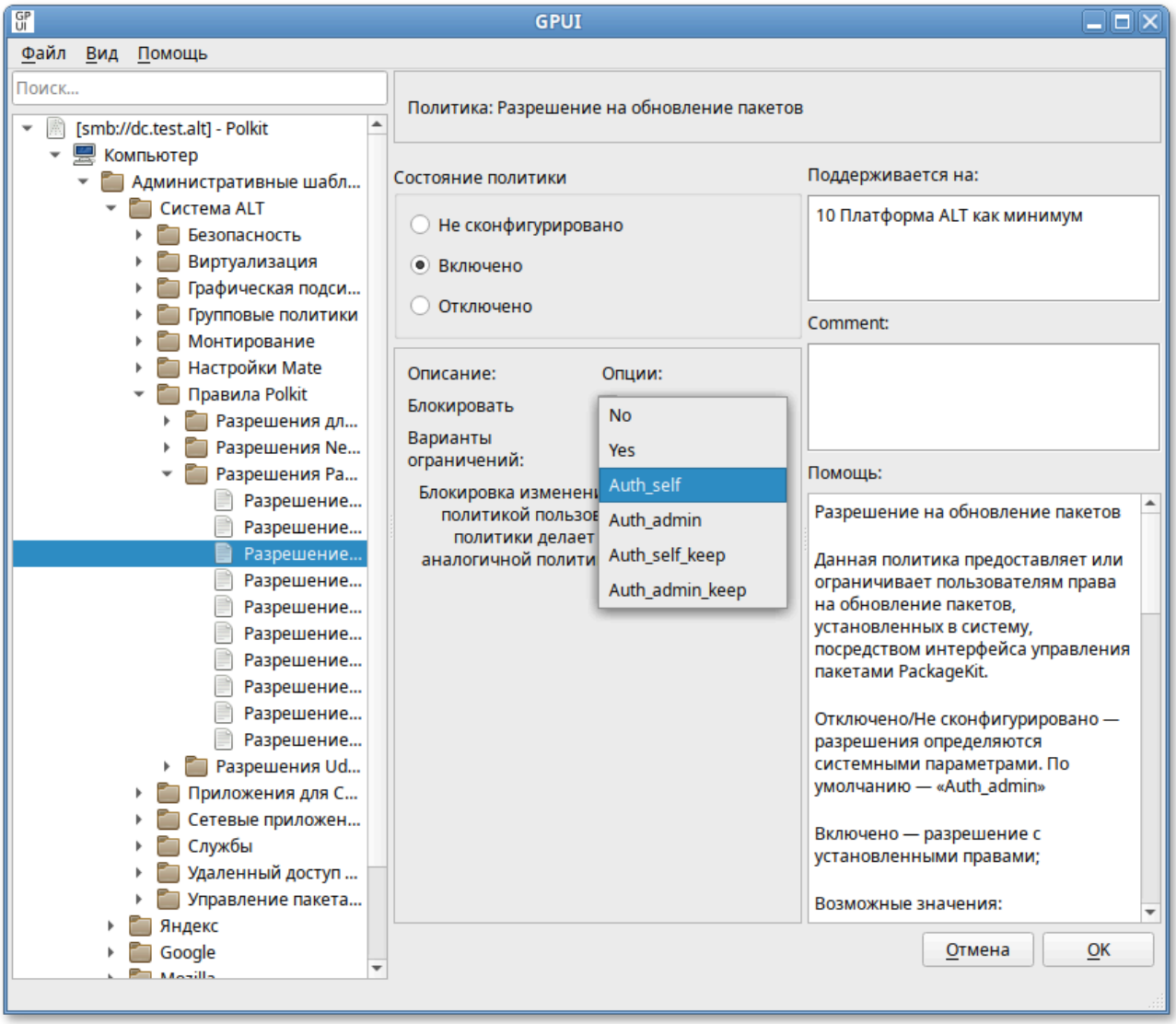


Рис. 280 – Вариант ограничения для данного разрешения

Если выбран параметр «Включено», для каждой из этих политик доступны следующие разрешения:

- «No» – заблокировать разрешения (пользователю не разрешено выполнять действие);
- «Yes» – предоставить разрешения (пользователь может выполнять действие без какой-либо аутентификации);
- «Auth_self» – пользователь должен ввести свой пароль для аутентификации. Следует обратить внимание, что этого разрешения недостаточно для большинства применений в многопользовательских системах, обычно рекомендуется разрешение «Auth_admin»;

- «Auth_admin» – пользователь должен ввести пароль администратора при каждом запросе. Требуется аутентификация пользователя с правами администратора;
- «Auth_self_keep» – подобно «Auth_self», но авторизация сохраняется в течение короткого периода времени (например, пять минут). Следует обратить внимание, что этого разрешения недостаточно для большинства применений в многопользовательских системах, обычно рекомендуется разрешение «Auth_admin_keep»;
- «Auth_admin_keep» – аналогично «Auth_admin», но авторизация сохраняется в течение короткого периода времени (например, пять минут).

Примечание. Администратор – в ОС Альт СП определен в правиле `/etc/polkit-1/rules.d/50-default.rules`:

```
polkit.addAdminRule(function(action, subject) {
        return ["unix-group:wheel"];
});
```

По умолчанию запрашивается пароль пользователя, находящегося в группе wheel.

Для машинной политики создается файл правил `49-alt_group_policy_permissions.rules`, для пользовательской политики – `48-alt_group_policy_permissions_user.<USERNAME>.rules`. Правила для пользовательской политики обрабатываются до правил для машинной политики. У машинных политик имеются блокировки (параметр «Блокировать»), при установке которых машинные политики становятся приоритетнее пользовательских (создается файл правил `47-alt_group_policy_permissions.rules`).

Разрешения для работы с токенами и смарт-картами приведены в таблице 25.

Разрешения NetworkManager приведены в таблице 26.

Разрешения PackageKit приведены в таблице 27.

Разрешения Udisks2 приведены в таблице 28.

Т а б л и ц а 25 – Разрешения для работы с токенами и смарт-картами

Политика	Описание	Правило Polkitd
Разрешение на доступ к демону PC/SC	Данная политика управляет разрешением доступа к демону PC/SC и регулирует работу с токенами	org.debian.pcsc-lite.access_pcsc
Разрешение на доступ к смарт-картам	Данная политика управляет разрешением доступа к смарт-картам	org.debian.pcsc-lite.access_card

Т а б л и ц а 26 – Разрешения NetworkManager

Политика	Описание	Правило Polkitd
Разрешение включения или отключения сети	Политика управляет разрешением для включения или отключения сетевого взаимодействия системы. Если сетевое взаимодействие отключено, все управляемые интерфейсы отсоединяются и деактивируются. Если сетевое взаимодействие включено, все управляемые интерфейсы доступны для активации	org.freedesktop.NetworkManager.enable-disable-network
Разрешение включения или отключения статистики	Политика управляет разрешением на включение или отключение счетчика статистики устройства	org.freedesktop.NetworkManager.enable-disable-statistics
Разрешение включения или отключения устройств Wi-Fi	Данная политика предоставляет или ограничивает пользователям права для включения или отключения устройств Wi-Fi	org.freedesktop.NetworkManager.enable-disable-wifi
Разрешение включения или отключения устройств WiMAX	Данная политика предоставляет или ограничивает пользователям права для включения или отключения мобильных широкополосных устройств WiMAX	org.freedesktop.NetworkManager.enable-disable-wimax
Разрешение включения или отключения WWAN-устройств	Политика предоставляет или ограничивает пользователям права для включения или отключения мобильных широкополосных устройств	org.freedesktop.NetworkManager.enable-disable-wwan
Разрешение изменения общих настроек DNS	Политика управляет разрешением изменений общей конфигурации DNS	org.freedesktop.NetworkManager.settings.modify.global-dns
Разрешение изменения персональных сетевых настроек	Данная политика управляет разрешением изменений личных сетевых соединений	org.freedesktop.NetworkManager.settings.modify.own
Разрешение изменения постоянного имени хоста	Данная политика управляет разрешением изменения постоянного имени (hostname) системы	org.freedesktop.NetworkManager.settings.modify.hostname

Окончание таблицы 26

Политика	Описание	Правило Polkitd
Разрешение изменения сетевых подключений для всех пользователей	Политика управляет разрешением изменения системных сетевых настроек для всех пользователей	org.freedesktop.NetworkManager.settings.modify.system
Разрешение изменения системных настроек для сети	Политика управляет разрешением изменения системных сетевых настроек	org.freedesktop.NetworkManager.network-control
Разрешение изменения состояния сна NetworkManager	Данная политика управляет разрешением на перевод NetworkManager в спящий режим или пробуждение из спящего режима (должна использоваться только для управления питанием системы)	org.freedesktop.NetworkManager.sleep-wake
Разрешение отката конфигурации сетевых интерфейсов к контрольной точке	Политика управляет разрешением для создания контрольной точки сетевых интерфейсов или откату к ней	org.freedesktop.NetworkManager.checkpoint-rollback
Разрешение перезагрузки NetworkManager	Политика управляет разрешением перезагрузки конфигурации NetworkManager	org.freedesktop.NetworkManager.reload
Разрешение проверки подключения сети	Политика управляет разрешением на включение или отключение проверки подключения к сети	org.freedesktop.NetworkManager.enable-disable-connectivity-check
Разрешение сканирования Wi-Fi сетей	Данная политика разрешением сканирования Wi-Fi сетей	org.freedesktop.NetworkManager.wifi.scan
Разрешение совместных подключений через защищенную сеть Wi-Fi	Политика управляет разрешением совместного подключения через защищенную сеть Wi-Fi	org.freedesktop.NetworkManager.wifi.share.protected
Разрешение совместных подключений через открытую сеть Wi-Fi	Политика управляет разрешением совместного подключения через открытую сеть Wi-Fi	org.freedesktop.NetworkManager.wifi.share.open

Разрешения NetworkManager для текущего пользователя можно просмотреть, выполнив команду:

```
$ nmcli general permissions
PERMISSION                                                    VALUE
org.freedesktop.NetworkManager.checkpoint-rollback            auth
org.freedesktop.NetworkManager.enable-disable-connectivity-check  нет
org.freedesktop.NetworkManager.enable-disable-network         auth
org.freedesktop.NetworkManager.enable-disable-statistics      auth
org.freedesktop.NetworkManager.enable-disable-wifi            да
org.freedesktop.NetworkManager.enable-disable-wimax           да
```

org.freedesktop.NetworkManager.enable-disable-wwan да
org.freedesktop.NetworkManager.network-control да
org.freedesktop.NetworkManager.reload auth
org.freedesktop.NetworkManager.settings.modify.global-dns нет
org.freedesktop.NetworkManager.settings.modify.hostname auth
org.freedesktop.NetworkManager.settings.modify.own auth
org.freedesktop.NetworkManager.settings.modify.system да
org.freedesktop.NetworkManager.sleep-wake да
org.freedesktop.NetworkManager.wifi.scan да
org.freedesktop.NetworkManager.wifi.share.open да
org.freedesktop.NetworkManager.wifi.share.protected да

Таблица 27 – Разрешения PackageKit

Политика	Описание	Правило Polkitd
Разрешение на восстановление пакетов в системе	Данная политика предоставляет или ограничивает пользователям права на восстановление системы пакетов, если в ней возникли проблемы, например, пропали зависимости, посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.repair-system
Разрешение на добавление ключа электронной подписи	Данная политика предоставляет или ограничивает пользователям право на добавление ключа подписи в список доверенных ключей системы посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.system-trust-signing-key
Разрешение на обновление пакетов	Данная политика предоставляет или ограничивает пользователям права на обновление пакетов, установленных в систему, посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.system-update
Разрешение на обновление системных источников пакетов	Данная политика предоставляет или ограничивает пользователям права на обновление системных источников пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.system-sources-refresh
Разрешение на переустановку пакетов	Данная политика предоставляет или ограничивает пользователям право на переустановку пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-reinstall
Разрешение на принятие лицензионного соглашения	Данная политика предоставляет или ограничивает право на принятие пользовательского соглашения программ посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-eula-accept

Окончание таблицы 27

Политика	Описание	Правило Polkitd
Разрешение на редактирование источников пакетов	Данная политика предоставляет или ограничивает пользователям права на редактирование источников пакетов в системе посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.system-sources-configure
Разрешение на удаление пакетов	Данная политика предоставляет или ограничивает пользователям права на удаление пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-remove
Разрешение на установку пакетов	Данная политика предоставляет или ограничивает пользователям права на установку пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-install
Разрешение на установку непроверенных пакетов	Данная политика предоставляет или ограничивает пользователям права на установку ненадежных или непроверенных пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-install-untrusted

Таблица 28 – Разрешения Udisks2

Политика	Описание	Правило Polkitd
Общая политика монтирования	Данная политика предоставляет или ограничивает разрешения на монтирование файловой системы, монтирование файловых систем системных устройств, монтирование файловых систем в удаленных сеансах	org.freedesktop.udisks2.filesystem-mount org.freedesktop.udisks2.filesystem-mount-other-seat org.freedesktop.udisks2.filesystem-mount-system
Разрешение на монтирование файловой системы	Данная политика управляет разрешением на монтирование файловой системы устройства	org.freedesktop.udisks2.filesystem-mount
Разрешение на монтирование файловых систем в удаленных сеансах	Данная политика предоставляет или ограничивает разрешения на монтирование файловых систем с устройства, подключенного к удаленному рабочему месту (например, на другом компьютере или удаленной сессии)	org.freedesktop.udisks2.filesystem-mount-other-seat
Разрешение на монтирование файловых систем системных устройств	Политика предоставляет или ограничивает разрешения на монтирование файловых систем системных устройств. Системное устройство хранения информации – это неизвлекаемое устройство. Для таких устройств переменная «HintSystem» установлена в значение True. Жесткий диск с установленной ОС относится к системным устройствам.	org.freedesktop.udisks2.filesystem-mount-system

Все настройки политики управления пакетами хранятся в файлах `{GUID GPT}/Machine/Registry.pol` и `{GUID GPT}/User/Registry.pol`.

Пример файла `Registry.pol`:

```
PReg
[Software\BaseALT\Policies\PolkitLocks;org.freedesktop.udisks2.filesystem-mount;;;]
[Software\BaseALT\Policies\Polkit;org.freedesktop.udisks2.filesystem-mount;;;No]
[Software\BaseALT\Policies\Polkit;org.freedesktop.packagekit.system-
update;;;Auth_self]
[Software\BaseALT\Policies\PolkitLocks;org.freedesktop.NetworkManager.network-
control;;;]
[Software\BaseALT\Policies\Polkit;org.freedesktop.NetworkManager.network-
control;;Yes]
```

9.2.5.4.4. Политика доступа к съемным носителям

Эта групповая политика позволяет централизованно для компьютеров или пользователей настраивать доступ к съемным запоминающим устройствам (CD, DVD, USB и др.).

П р и м е ч а н и е . Политика полного запрета на доступ к съемным носителям реализована через правила в Polkit (`/etc/polkit-1/rules.d/`).

Правила для пользовательской политики обрабатываются до правил для машинной политики. Для машинной политики создается файл правил `49-gpoa_disk_permissions.rules`, для пользовательской политики – `48-gpoa_disk_permissions_user.<USERNAME>.rules`.

Для настройки этой политики следует перейти в «Компьютер»/ «Пользователь» → «Административные шаблоны» → «Система» → «Доступ к съемным запоминающим устройствам» (рис. 281).

П р и м е ч а н и е . На данный момент реализована только политика «Съемные запоминающие устройства всех классов: Запретить любой доступ» (машинная и пользовательская).

Щелкнуть левой кнопкой мыши на политике «Съемные запоминающие устройства всех классов: Запретить любой доступ», откроется диалоговое окно настройки политики. Можно не задавать настройку политики, включить или отключить (рис. 282).

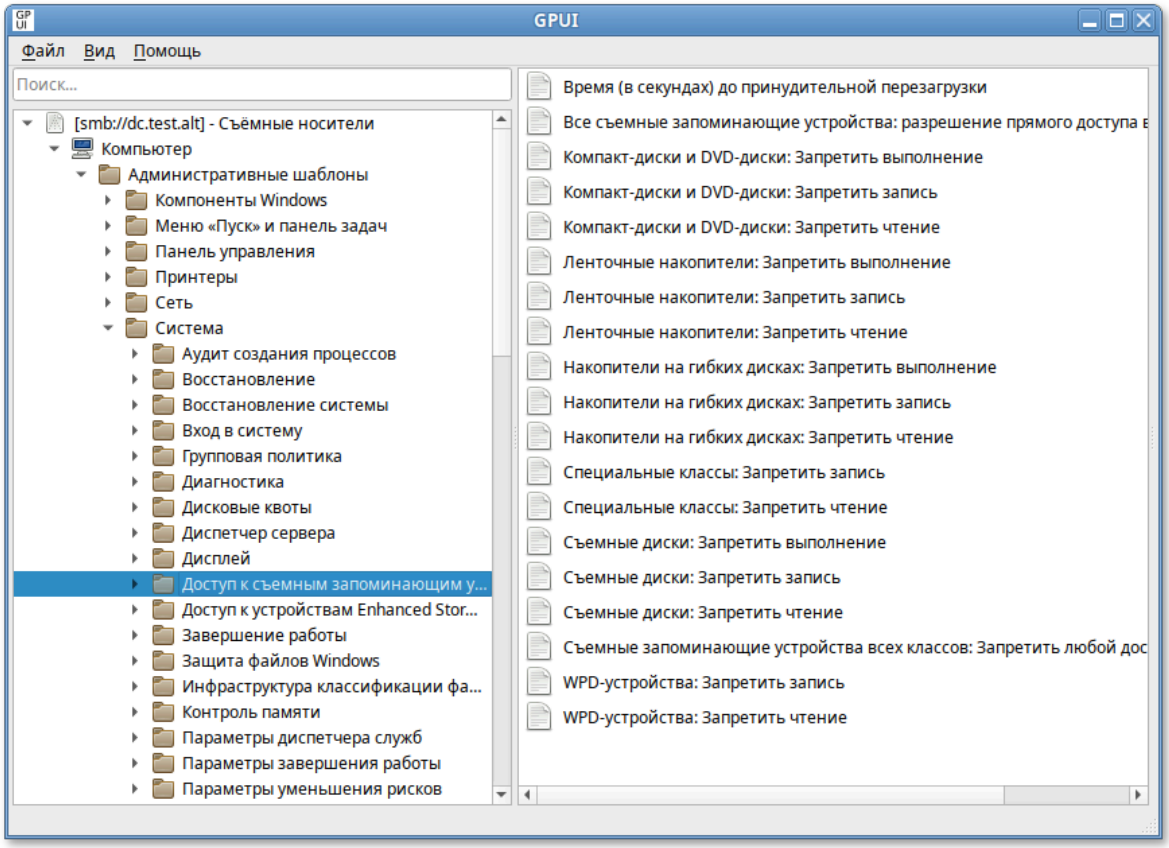


Рис. 281 – «Доступ к съемным запоминающим устройствам»

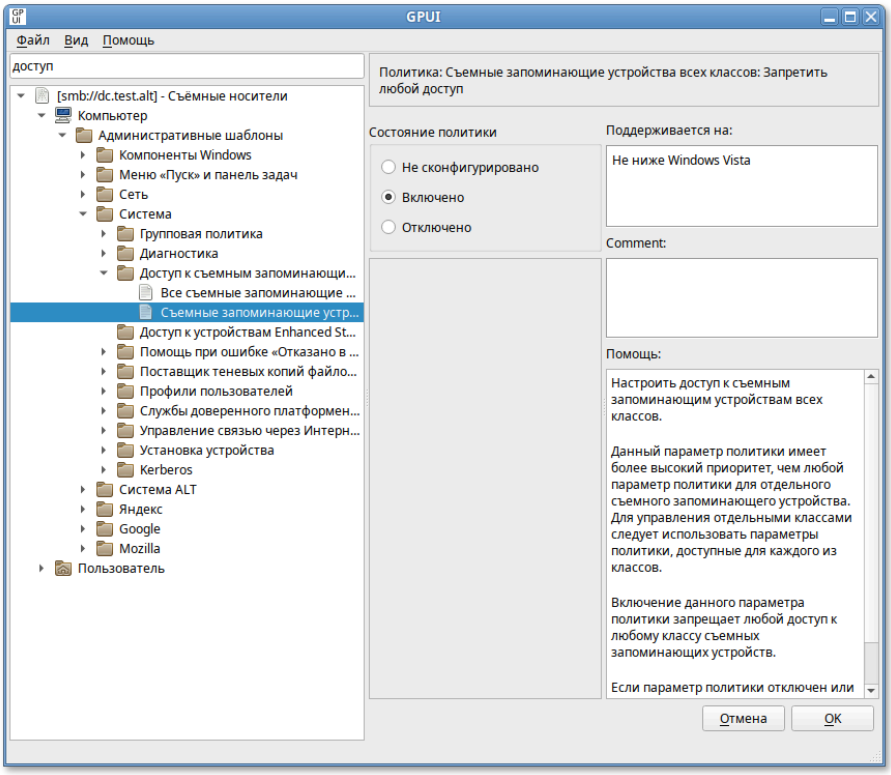


Рис. 282 – Диалоговое окно настройки политики «Съемные запоминающие устройства всех классов: Запретить любой доступ»

Для включения запрета на доступ следует выбрать параметр «Включено», для отключения – «Отключено» или «Не сконфигурировано».

Настройки политики управления пакетами хранятся в файлах `{GUID GPT}/Machine/Registry.pol` и `{GUID GPT}/User/Registry.pol`.

Пример файла `Registry.pol`:

```
PReg
[Software\Policies\Microsoft\Windows\RemovableStorageDevices;Deny_All;;;]
```

9.2.5.4.5. Управление `gsettings`

Данные групповые политики позволяют управлять ключами `gsettings`. В свою очередь `gsettings` управляет ключами `dconf`.

В настоящий момент реализованы настройки удаленного доступа к рабочему столу (VNC) через Vino и настройки графической среды MATE, а именно:

- настройки фона рабочего стола;
- настройки хранителя экрана;
- настройки ограничений пользователя.

Машинные политики являются действующими по умолчанию, а пользовательские, при установке, замещают машинные. У машинных политик имеются блокировки, при установке которых пользовательские настройки игнорируются, а для применения используются значения, установленные машинными политиками.

Порядок применения политик:

1) машинные политики применяются при загрузке компьютера;
2) машинные политики без блокирования могут применяться, но только в том случае, если пользователь ни разу не изменял эти политики;
3) машинные политики с блокировкой применяются независимо от пользовательских настроек;
4) пользовательские политики применяются при логине пользователя и только в случае, если нет таких же машинных политик с блокировкой.

Для настройки политики следует перейти в «Компьютер»/ «Пользователь» → «Административные шаблоны» → «Система ALT» → «Настройки Mate»/ «Удаленный доступ через Vino». Выбрать раздел, в правом окне редактора отобразится список политик (рис. 283).

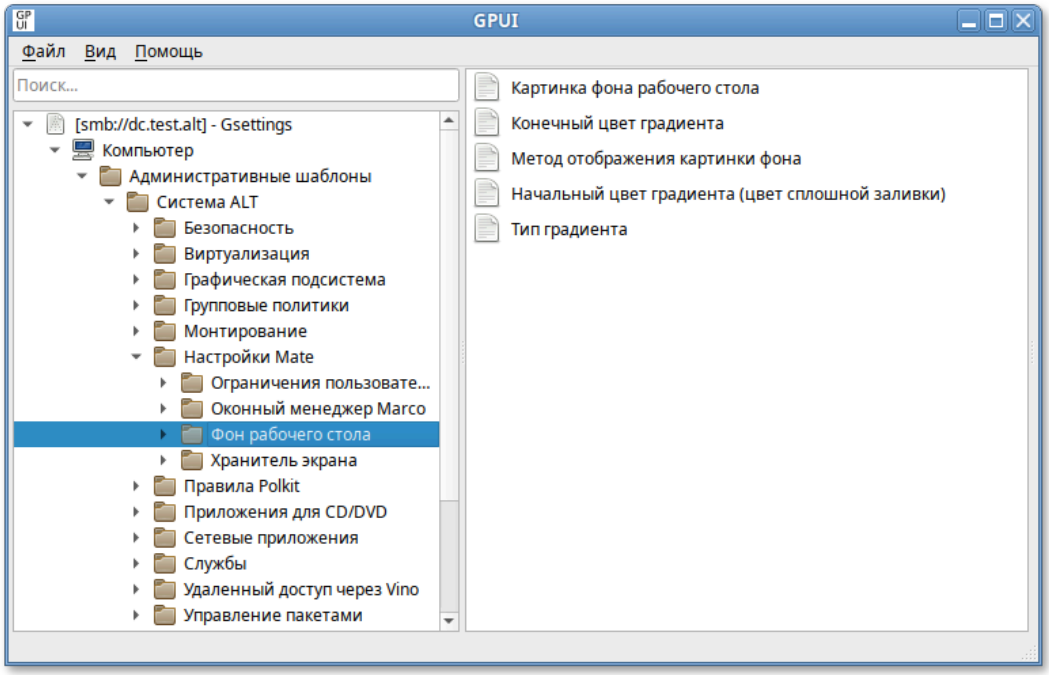


Рис. 283 – Раздел «Фон рабочего стола»

При выборе политики, откроется диалоговое окно настройки политики (рис. 284).

Можно не задавать настройку политики, включить или отключить. Если выбрать параметр «Включено», в разделе «Параметры» в выпадающем списке можно указать настройки политики (рис. 285).

Политика, управляющая настройкой фона рабочего стола, изменяет ключ `KEY` в схеме `org.mate.background`. В реестре Windows изменяет в `Software\BaseALT\Policies\gsettings` ключ `org.mate.background.KEY`. Блокировка устанавливается в ветке реестра `Software\BaseALT\Policies\GSettingsLocks`, ключ `org.mate.background.KEY`.

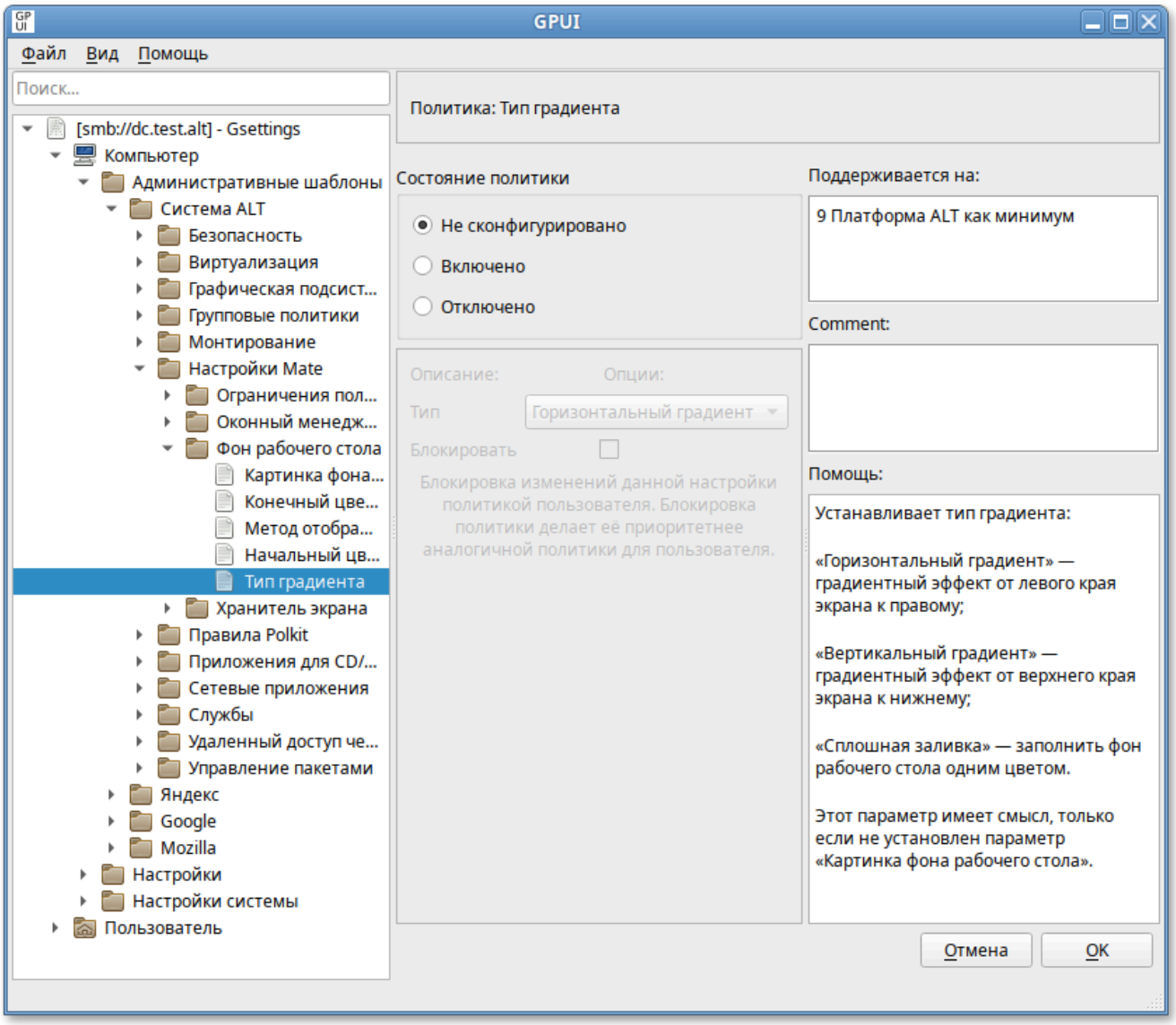


Рис. 284 – Диалоговое окно настройки политики

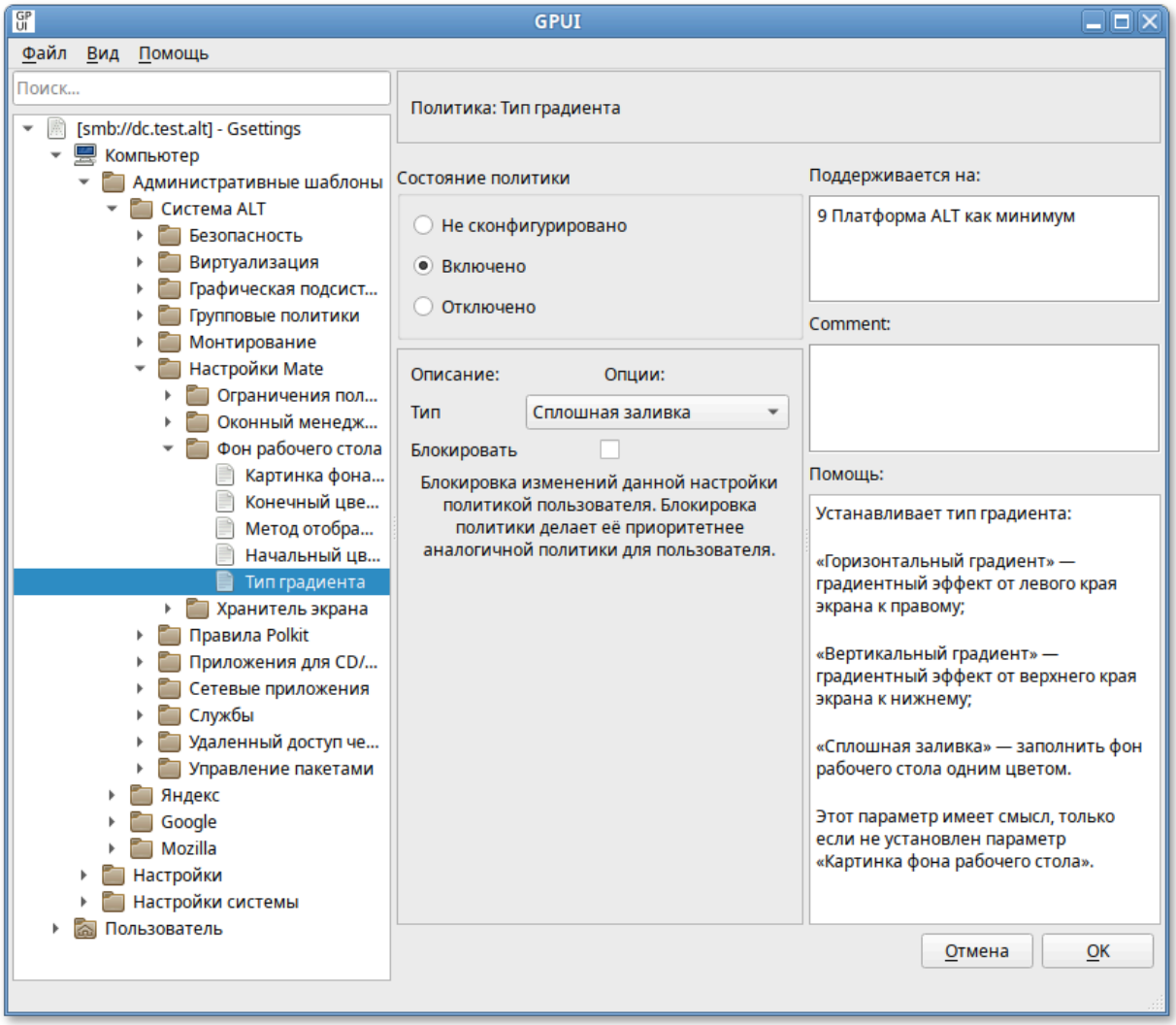


Рис. 285 – Включить или отключить настройки политики

Настройки фона рабочего стола приведены в таблице 29.

Т а б л и ц а 29 – Настройки фона рабочего стола

Политика	Ключ	Описание	Значение
Картинка фона рабочего стола	picture-filename	Позволяет устанавливать изображение в качестве фона рабочего стола, задав имя файла, содержащего изображение	Строка, содержащая путь (с точки зрения клиента) к файлу изображения (например, `/usr/share/backgrounds/mate/nature/Wood.jpg`)
Тип градиента	color-shading-type	Устанавливает тип градиента фона рабочего стола. Этот параметр имеет смысл, только если не установлен параметр «Картинка фона рабочего стола»	«Вертикальный градиент» – градиентный эффект от верхнего края экрана к нижнему краю. «Горизонтальный градиент» – градиентный эффект от левого края экрана к правому. «Сплошная заливка» – заполнить фон рабочего стола одним цветом

Продолжение таблицы 29

Политика	Ключ	Описание	Значение
Метод отображения картинки фона	picture-options	Устанавливает метод отображения изображения, заданного параметром «Картинка фона рабочего стола»	«None» («нет») – нет изображения. «Wallpaper» («мозаика») – дублирует изображение в оригинальном размере таким образом, что изображение полностью покрывает рабочий стол. «Centered» («по центру») – отображает изображение в центре рабочего стола в соответствии с оригинальным размером изображения. «Scaled» («масштаб») – увеличивает изображение, сохраняя пропорции, до тех пор, пока величина одной из границ изображения не совпадет с величиной одной из границ экрана. «Stretched» («растянуть») – увеличивает изображение для соответствия размеру рабочего стола, изменяя пропорции при нужности. «Zoom» («масштаб») – увеличивает наименьшую из сторон изображения до тех пор, пока ее величина не совпадет с величиной соответствующей границы экрана; изображение может быть обрезано по другой стороне. «Stretched» («растянуть») – увеличивает изображение, сохраняя пропорции, до тех пор, пока величина одной из границ изображения не совпадет с величиной одной из границ экрана
Конечный цвет градиента	secondary-color	Устанавливает «конечный» цвет градиента фона рабочего стола. Данным цветом заканчивается градиент и, в зависимости от типа градиента, параметр определяет цвет правого или нижнего края рабочего стола. Данный параметр не используется, если в параметре «Тип градиента» выбрана «Сплошная заливка»	Ключевое слово цвета (red, aqua, navy и т.д.). Строка типа `#RRGGBB`. Строка типа `rgb(0,0,0)`

Окончание таблицы 29

Политика	Ключ	Описание	Значение
Начальный цвет градиента	primary-color	Устанавливает начальный цвет градиента фона рабочего стола. Данным цветом начинается градиент и, в зависимости от типа градиента, параметр определяет цвет левого или верхнего края рабочего стола, или цвет сплошной заливки	Ключевое слово цвета (red, aqua, navy и т.д.). Строка типа `#RRGGBB`. Строка типа `rgb(0,0,0)`

Политика, управляющая настройкой хранителя экрана, изменяет ключ `KEY` в схеме `org.mate.screensaver`. В реестре Windows изменяет в `Software\BaseALT\Policies\gsettings` ключ `org.mate.screensaver.KEY`. Блокировка устанавливается в ветке реестра `Software\BaseALT\Policies\GSettingsLocks`, ключ `org.mate.screensaver.KEY`.

Настройки хранителя экрана приведены в таблице 30.

Таблица 30 – Настройки хранителя экрана

Политика	Ключ	Описание	Значение
Время смены тем	cycle-delay	Устанавливает интервал (в минутах) между сменами тем хранителя экрана. Этот параметр имеет смысл только при активированном параметре «Включение хранителя экрана» и если для параметра «Режим работы» установлено значение «Случайные темы».	Время в минутах
Время до блокировки паролем	lock-delay	Устанавливает количество минут, по истечении которых после активации хранителя экрана, компьютер будет заблокирован. Этот параметр имеет смысл только при активированном параметре «Включение хранителя экрана» и «Блокировка компьютера»	Время в минутах
Блокировка компьютера	lock-enabled	Включает блокировку компьютера при активации хранителя экрана. Блокировка будет включена через интервал времени, установленный настройкой «Время до блокировки паролем». Этот параметр имеет смысл только при активированном параметре «Включение хранителя экрана»	-

Окончание таблицы 30

Политика	Ключ	Описание	Значение
Время до выхода из сеанса	logout-delay	Устанавливает количество минут, по истечении которых после активации хранителя экрана, при разблокировании пользователю будет предоставлена возможность выхода из сеанса. Этот параметр имеет смысл только при активированном параметре «Включение хранителя экрана» и «Выход из системы после блокировки»	Время в минутах
Выход из системы после блокировки	logout-enabled	После некоторой задержки добавляет кнопку выхода из системы (>«Завершить сеанс») к диалогу разблокирования экрана. Время задержки указывается в настройке «Время выхода из сеанса». Этот параметр имеет смысл только при активированном параметре «Включение хранителя экрана» и «Блокировка компьютера» (так как без блокировки не появляется диалог с кнопкой)	-
Режим работы	mode	Устанавливает режим работы хранителя экрана. Этот параметр имеет смысл только при активированном параметре «Включение хранителя экрана»	Доступны следующие режимы: «Отключен» – режим отключен «Пустой экран» – не показывать никаких изображений, только черный экран; «Выбранная тема» – показывать одну (указанную) тему хранителя экрана; «Случайные темы» – выбрать тему хранителя экрана случайным образом
Переключить пользователя после блокировки	user-switch-enabled	Добавляет кнопку «Переключить пользователя» к диалогу разблокирования экрана. Этот параметр имеет смысл только при активированном параметре «Включение хранителя экрана» и «Блокировка компьютера» (так как без блокировки не появляется диалог с кнопкой)	-
Включение хранителя экрана	idle-activation-enabled	Обеспечивает включение хранителя экрана при бездействии системы	-

Политика, управляющая настройкой ограничений пользователя, изменяет ключ `KEY` в схеме `org.mate.lockdown`. В реестре Windows изменяет в `Software\BaseALT\Policies\gsettings` ключ `org.mate.lockdown.KEY`. Блокировка устанавливается в ветке реестра `Software\BaseALT\Policies\GSettingsLocks`, ключ `org.mate.lockdown.KEY`.

Настройки ограничений пользователя приведены в таблице 31.

Таблица 31 – Настройки ограничений пользователя

Политика	Ключ	Описание	Значение
Запрет блокировки экрана	picture-filename	Запрещает пользователю блокировать экран паролем. При установке данной настройки, значение параметра «Блокировка компьютера» игнорируется	-
Запрет пользователю завершать сеанс	disable-log-out	Запрещает пользователю завершать свой сеанс	-
Запрет выбора тем рабочего стола	picture-filename	Запрещает пользователю изменять тему оформления графической среды MATE	-
Запрет переключения пользователей	disable-user-switching	Запрещает пользователю переключение на другую учетную запись, пока активен его сеанс. Отключает кнопку «Переключить пользователя» в диалоговом окне, вызываемом при выборе в главном меню пункта «Завершить сеанс»	-

Политика, управляющая настройкой удаленного доступа VNC, изменяет ключ `KEY` в схеме `org.gnome.Vino`. В реестре Windows изменяет в `Software\BaseALT\Policies\gsettings` ключ `org.gnome.Vino.KEY`. Блокировка устанавливается в ветке реестра `Software\BaseALT\Policies\GSettingsLocks`, ключ `org.gnome.Vino.KEY`.

Настройки ограничений пользователя приведены в таблице 32.

Т а б л и ц а 32 – Настройки удаленного доступа VNC

Политика	Ключ	Описание	Значение
Альтернативный порт	alternative-port	Устанавливает альтернативный порт для удаленного подключения к рабочему столу. Используется только при установленном параметре «Включить альтернативный порт»	Значение номера порта в пределах от 5 000 до 50 000. По умолчанию используется порт 5900
Методы аутентификации	authentication-methods	Устанавливает методы аутентификации пользователей, подключающихся к рабочему столу. Используется только при установленном параметре «Пароль для подключения»	«None» – пароль для подключения не требуется. «Vnc» – для подключения нужен пароль
Удаленный доступ	enabled	Разрешает удаленный доступ к рабочему столу с использованием протокола RFB и VNC	«Включено» – удаленный доступ разрешен. «Отключено» – удаленный доступ запрещен
Иконка подключения	icon-visibility	Управляет отображением значка подключения в области уведомления	«Никогда» – значок не отображается. «Всегда» – значок отображается всегда. «Только при подключении клиента» – значок отображается при подключении удаленного пользователя
Подтверждение при подключении	prompt-enabled	Включает запрос подтверждения при любой попытке доступа к рабочему столу. Рекомендуется при отсутствии защиты подключения паролем	«Включено» – запрашивается подтверждение доступа. «Отключено» – подтверждение доступа не запрашивается
Включить альтернативный порт	prompt-enabled	Включить прослушивание альтернативного порта для удаленных подключений (вместо порта по умолчанию 5 900). Порт указывается в параметре «Альтернативный порт»	«Включено» – включить прослушивание альтернативного порта. «Отключено» – не включать прослушивание альтернативного порта
Удаленное управление	view-only	Запрещает удаленное управление рабочим столом. Удаленным пользователям, разрешается только просматривать рабочий стол, но не управлять мышью и клавиатурой	«Включено» – удаленное управление разрешено. «Отключено» – удаленное управление запрещено

Окончание таблицы 32

Политика	Ключ	Описание	Значение
Пароль для подключения	vnc-password	Установка пароля для подключения к рабочему столу. Пароль должен быть закодирован в base64. Пароль будет запрашивается только при использовании метода аутентификации vnc, установленном в параметре «Методы аутентификации». Примечание. Протокол VNC ограничивает длину пароля 8 символами. Пароли длиной более 8 символов будут автоматически обрезаны	Пароль в кодировке base64 (для генерации пароля в base64 можно воспользоваться командой: `echo -n "password" | base64`)

Политика, управляющая настройкой оконного менеджера Marco, изменяет ключ `KEY` в схеме `org.mate.Marco.general`. В реестре Windows изменяет в `Software\BaseALT\Policies\gsettings` ключ `org.mate.pMarco.general.KEY`. Блокировка устанавливается в ветке реестра `Software\BaseALT\Policies\GSettingsLocks`, ключ `org.mate.Marco.general.KEY`.

Настройки оконного менеджера Marco приведены в таблице 33.

Таблица 33 – Настройки оконного менеджера Marco

Политика	Ключ	Описание	Значение
Иконки заголовка окна	button-layout	Настройки расположения кнопок в заголовке окна	Строка вида: `menu:minimize,maximize,spacer,close.` Разделителем правой и левой половин является двоеточие. Имена кнопок разделяются запятыми. Например, строка `'menu:minimize,maximize,spacer,close'` – расположить кнопку меню окна слева, а справа кнопки свернуть, распахнуть, закрыть окно. Дублирование кнопок не допускается. Неизвестные имена кнопок игнорируются без уведомления. Специальный элемент spacer может использоваться для вставки пробела между двумя кнопками

Продолжение таблицы 33

Политика	Ключ	Описание	Значение
Действие по нажатию средней кнопки	action-middle-click-titlebar	Установка действия, выполняемого по нажатию средней кнопки мыши по заголовку окна	«toggle_shade» («Свернуть в заголовок») – свернуть окно в заголовок. По двойному щелчку окно разворачивается обратно. «toggle_maximize» («На весь экран») – распахнуть окно на весь экран или восстановить исходный размер. «toggle_maximize_vertically» («Растянуть по вертикали») – развернуть окно вертикально без изменения его ширины. «toggle_maximize_horizontally» («Растянуть по горизонтали») – развернуть окно горизонтально без изменения его высоты. «minimize» («Свернуть») – свернуть окно. «menu» («Показать меню») – показать меню окна. «lower» («Задвинуть») – поместить окно под другими. «none» («Ничего не делать») – никакого действия не производить. «last» («Последнее действие») – повторить предыдущее действие
Действие по нажатию правой кнопки	action-right-click-titlebar	Установка действия, выполняемого по нажатию правой кнопки мыши по заголовку окна	«toggle_shade» («Свернуть в заголовок») – свернуть окно в заголовок. По двойному щелчку окно разворачивается обратно. «toggle_maximize» («На весь экран») – распахнуть окно на весь экран или восстановить исходный размер. «toggle_maximize_vertically» («Растянуть по вертикали») – развернуть окно вертикально без изменения его ширины. «toggle_maximize_horizontally» («Растянуть по горизонтали») – развернуть окно горизонтально без изменения его высоты. «minimize» («Свернуть») – свернуть окно. «menu» («Показать меню») – показать меню окна. «lower» («Задвинуть») – поместить окно под другими. «none» («Ничего не делать») – никакого действия не производить. «last» («Последнее действие») – повторить предыдущее действие
Размер окна переключения Alt+Tab	alt-tab-max-columns	Устанавливает количество колонок в окне переключения приложений Alt+Tab	Количество колонок

Продолжение таблицы 33

Политика	Ключ	Описание	Значение
Действие по двойному щелчку	action-double-click-titlebar	Установка действия, выполняемого по двойному щелчку левой кнопкой мыши по заголовку окна	«toggle_shade» («Свернуть в заголовок») – свернуть окно в заголовок. По двойному щелчку окно разворачивается обратно. «toggle_maximize» («На весь экран») – распахнуть окно на весь экран или восстановить исходный размер. «toggle_maximize_vertically» («Растянуть по вертикали») – развернуть окно вертикально без изменения его ширины. «toggle_maximize_horizontally» («Растянуть по горизонтали») – развернуть окно горизонтально без изменения его высоты. «minimize» («Свернуть») – свернуть окно. «menu» («Показать меню») – показать меню окна. «lower» («Задвинуть») – поместить окно под другими. «none» («Ничего не делать») – никакого действия не производить. «last» («Последнее действие») – повторить предыдущее действие
Изменение размеров при перетаскивании	primary-color	Включает изменение размеров окна при перетаскивании его в различные области экрана. Если включено, перетаскивание окна на границу экрана распахивает окно вертикально и изменяет горизонтальный размер до половины доступного пространства. Если активирован параметр «Распахнуть окно при перетаскивании к верхнему краю экрана», перетаскивание окна наверх разворачивает окно	-

Продолжение таблицы 33

Политика	Ключ	Описание	Значение
Разворачивание при перетаскивании (Распахнуть окно при перетаскивании к верхнему краю экрана)	allow-top-tiling	Включает разворачивание окна во весь экран при перетаскивании его к верхнему краю экрана. Этот параметр имеет смысл только при активированном параметре «Изменение размеров при перетаскивании»	-
Задержка при восстановлении (Задержка перед автоматическим поднятием окна)	alt-tab-max-columns	Временной интервал в миллисекундах, по истечении которого окно в фокусе будет поднято поверх остальных. Этот параметр имеет смысл только при активированном параметре «Автоматически поднимать окно, получившее фокус»	Время в миллисекундах
Подъем окна в фокусе (Автоматически поднимать окно, получившее фокус)	auto-raise	При включении, окно, получившее фокус, автоматически отображается поверх остальных. Параметр «Переключение фокуса окон» должен быть установлен в «sloppy» или «mouse ». Интервал, по истечении которого, окно поднимается, устанавливается в параметре «Задержка при восстановлении»	-
Новые окна по центру	center-new-windows	Если включено, то новые окна будут открываться по центру экрана. В противном случае они будут открыты в левом верхнем углу экрана	-

Продолжение таблицы 33

Политика	Ключ	Описание	Значение
Миниатюры при переключении окон	compositing-fast-alt-tab	Если включено, то вместо миниатюр предварительного просмотра в окне переключения Alt+Tab будут отображаться значки приложения	-
Переключение фокуса окон	focus-mode	Режим переключения фокуса в окно определяет, как активируются окна	«Click» – для активации окна на нем надо щелкнуть. «Sloppy» – окно активируется, когда на него перемещается указатель мыши. «Mouse» – окно активируется, когда в него перемещается указатель мыши, и перестает быть активным, когда указатель мыши уходит из него
Переключение фокуса на новое окно	focus-new-windows	Определяет, как новое окно получает фокус	«Smart» – новое окно получает фокус при создании. «Strict» – окна, запущенные из терминала, не получают фокус
Размер иконок (Размер значков в окне Alt+Tab)	icon-size	Устанавливает размер значков, отображаемых в окне переключения приложений Alt+Tab	Интервал допустимых значений: 8 – 256
Количество рабочих областей (мест)	num-workspaces	Установка количества рабочих мест	Интервал допустимых значений 1 – 36
Расположение новых окон	placement-mode	Указывает, как будут позиционироваться новые окна	«Automatic» («Автоматически») – система выбирает местоположение на основе доступного пространства на рабочем столе, или располагает каскадом, если нет места. «Pointer» («Указатель») – новые окна размещаются в соответствии с положением указателя мыши. «Manual» («Ручной») – пользователь должен вручную расположить новое окно с помощью мыши или клавиатуры

Окончание таблицы 33

Политика	Ключ	Описание	Значение
Граница окна при переключении	show-tab-border	Выделять границу выбранного окна при переключении с помощью Alt+Tab	-
Тема оформления	theme	Устанавливает тему, отвечающую за отображение границ окон, заголовка и т.д.	Строка, содержащая название темы (например, Dopple)
Шрифт заголовка	titlebar-font	Устанавливает шрифт заголовков окон. Этот параметр игнорируется, если активирован параметр «Системн ый шрифт в заголовке окон»	Строка, содержащая название шрифта и через пробел, размер шрифта (например, Noto Sans Bold 10)
Системный шрифт в заголовке окон	titlebar-uses-system-font	Если включено, в заголовках окон используется стандартный системный шрифт. Параметр «Шрифт заголовка окна» при этом игнорируется	-
Переключение рабочих областей (столов)	wrap-style	Определяет, каким образом пролистывать от одного рабочего стола к другому на границе переключателя рабочих мест	«No wrap» – при попытке пролистать рабочее место за границу переключателя ничего не произойдет. «Classic» – конец одной строки ведет на начало следующей и конец одной колонки ведет к началу следующей. «Toroidal» – конец каждой строки ведет к ее же началу и конец каждой колонки ведет к ее же началу

Политика, управляющая настройкой клавиатуры, изменяет ключ `KEY` в схеме `org.mate.peripherals-keyboard`. В реестре Windows изменяет в `Software\BaseALT\Policies\gsettings` ключ `org.mate.peripherals-keyboard.KEY`. Блокировка устанавливается в ветке реестра `Software\BaseALT\Policies\GSettingsLocks`, ключ `org.mate.peripherals-keyboard.KEY`.

Настройки клавиатуры приведены в таблице 34.

Т а б л и ц а 34 – Настройки клавиатуры

Политика	Ключ	Описание	Значение
Задержка перед повтором	delay	Задержка перед повтором нажатой и удерживаемой клавиши	Время в миллисекундах
Скорость повтора	rate	Устанавливает скорость повтора нажатой и удерживаемой клавиши	Количество повторов в секунду
Повторять удерживаемую нажатой клавишу	repeat	Включить повтор нажатой и удерживаемой клавиши. Если нажать и удерживать клавишу при включенном повторе ввода, действие, соответствующее клавише, будет повторяться. Например, если нажать и удерживать клавишу с буквой, то эта буква будет многократно повторена.	-

9.2.5.4.6. Управление пакетами

Эта групповая политика позволяет централизованно для компьютеров устанавливать и удалять пакеты.

Для настройки политики следует перейти в «Компьютер»/«Пользователь»→ «Административные шаблоны» → «Система ALT» → «Управление пакетами». Выбрать раздел, в правом окне редактора отобразится список политик (рис. 286).

Для задания списка пакетов, которые нужно установить, щелкнуть левой кнопкой мыши на политике «Установка пакетов», откроется диалоговое окно настройки политики (рис. 287).

Для включения политики следует установить отметку в поле «Включено». Для задания списка пакетов, которые должны быть установлены/удалены нажать кнопку «Редактировать» и в открывшемся окне ввести список пакетов, по одному на каждой строке (рис. 288).

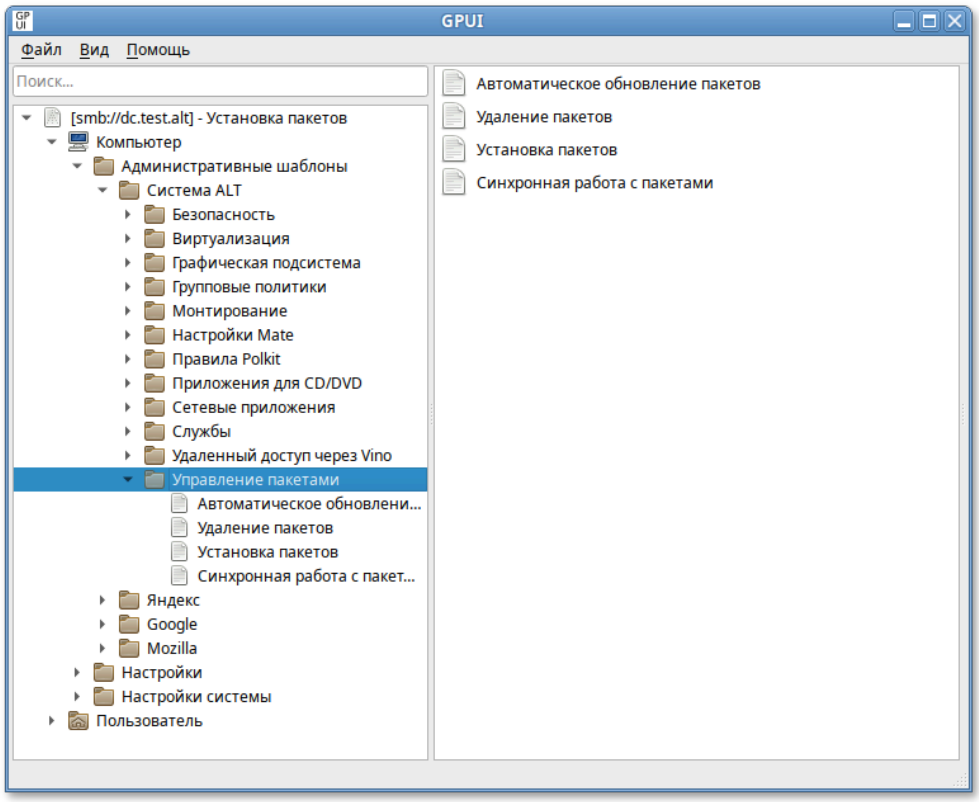


Рис. 286 – Список политик

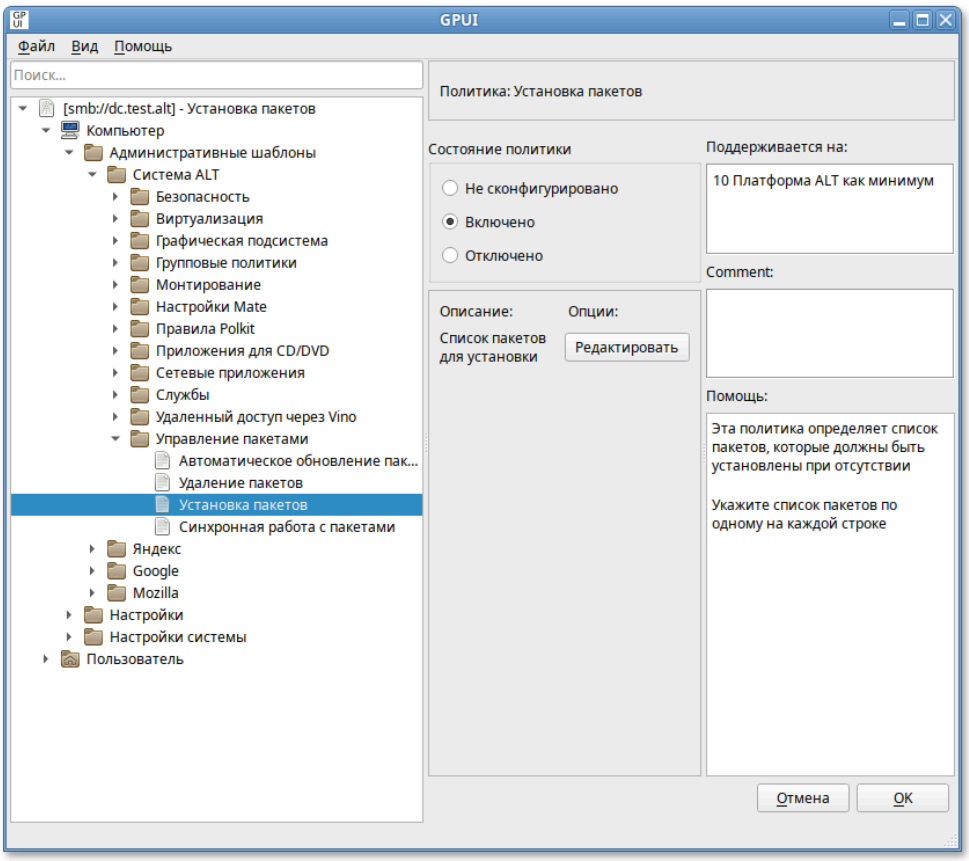


Рис. 287 – Диалоговое окно настройки политики

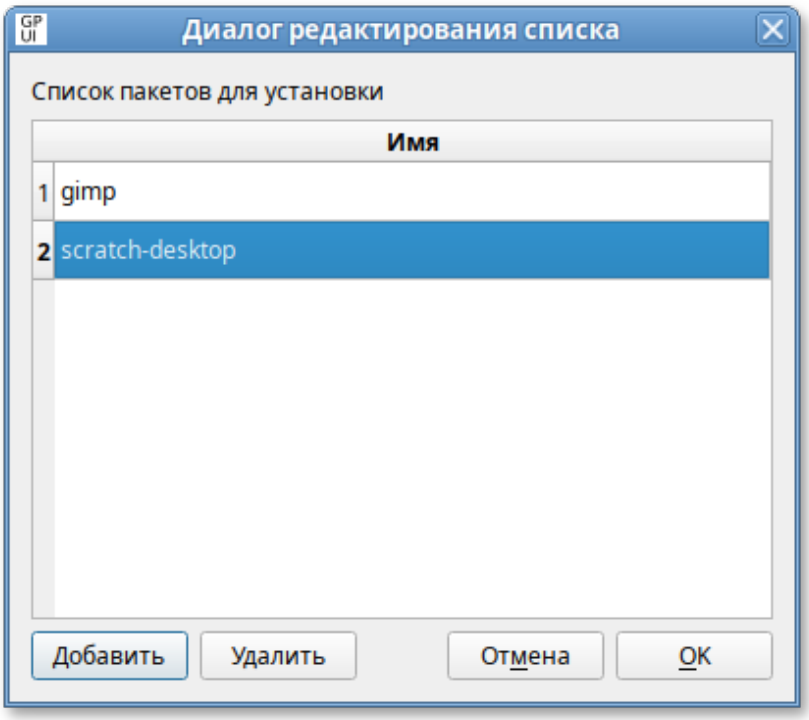


Рис. 288 – Список пакетов для установки

Для добавления/удаления строк можно воспользоваться соответствующими кнопками.

П р и м е ч а н и е . Для задания списка пакетов, которые нужно удалить, нужно выбрать политику «Удаление пакетов».

Также можно включить политику «Синхронная работа с политиками». Включение данной настройки запретит работу (установка, удаление) с пакетами в фоновом режиме, что может замедлить работу компьютера при применении политики (при загрузке машины, если политика машинная, или входе пользователя в систему, если политика пользовательская).

Для включения политики «Синхронная работа с политиками» следует в разделе «Компьютер»/«Пользователь» → «Административные шаблоны» → «Система ALT» → «Управление пакетами» выбрать пункт «Синхронная работа с пакетами», в открывшемся окне установить отметку в поле «Включено» и нажать кнопку «ОК», для сохранения изменений (рис. 289).

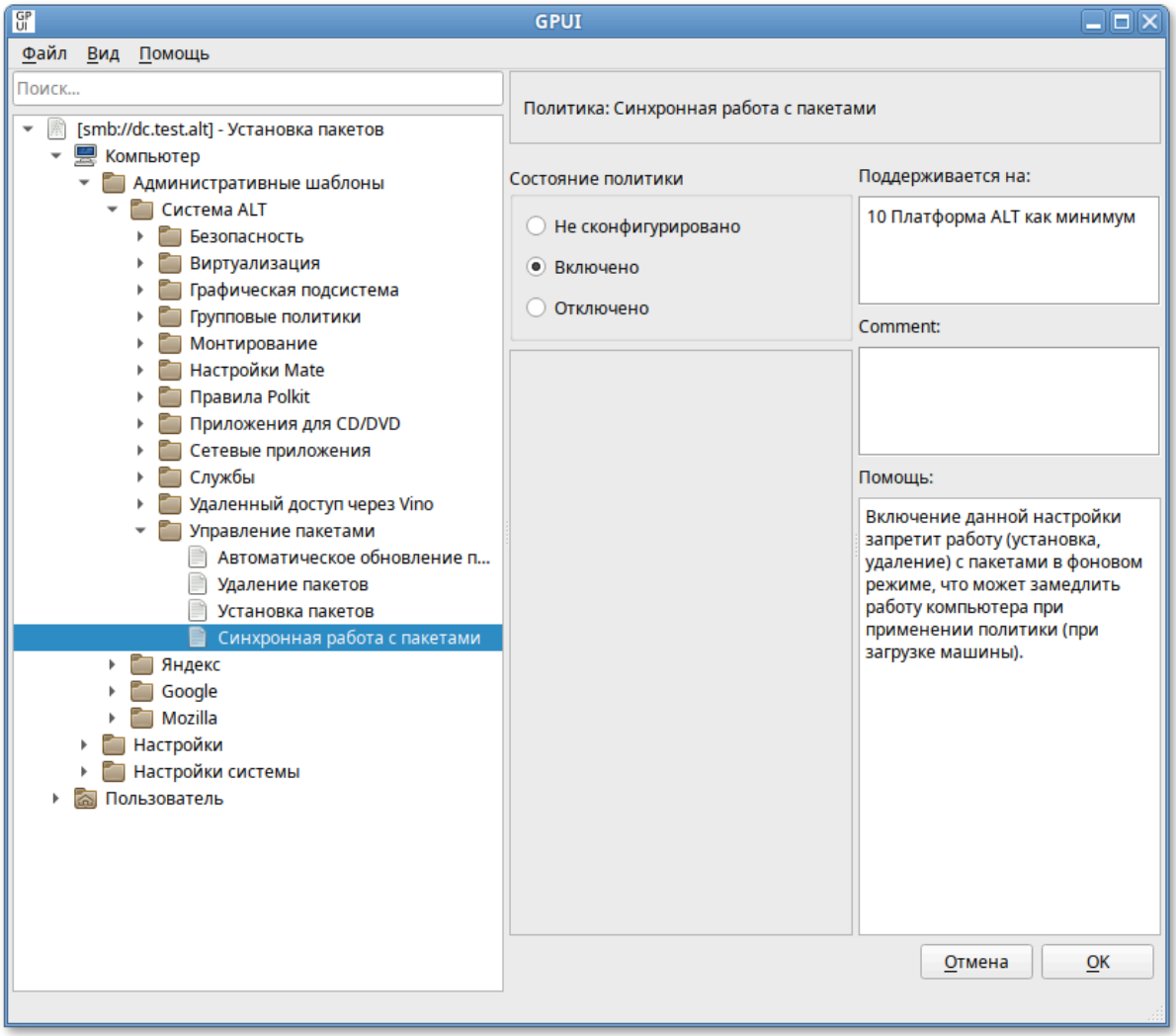


Рис. 289 – Политика «Синхронная работа с политиками»

Политики управления пакетами относятся к экспериментальным, поэтому на машинах с ОС Альт СП где они применяются должны быть включены экспериментальные групповые политики как указано в п. 9.2.5.4.7.

Все настройки политики управления пакетами хранятся в файлах `{GUID GPT}/Machine/Registry.pol` и `{GUID GPT}/User/Registry.pol`.

Пример файла `Registry.pol`:

```
PReg
[Software\BaseALT\Policies\GPUpdate;GlobalExperimental;;;]
[Software\BaseALT\Policies\Packages;Sync;;;]
[Software\BaseALT\Policies\Packages\Install;gimp;;;gimp]
[Software\BaseALT\Policies\Packages\Install;simple-scan;;;simple-
scan]
[Software\BaseALT\Policies\Packages\Remove;python3-
tools;;;python3-tools]
```

9.2.5.4.7. Экспериментальные групповые политики

На тех машинах Альт, где применяются экспериментальных политики, должны быть включены «Экспериментальные групповые политики».

Для включения экспериментальных групповых политик следует в разделе «Компьютер»/ «Пользователь» → «Административные шаблоны» → «Система ALT» → «Групповые политики» выбрать пункт «Экспериментальные групповые политики» и установить в открывшемся окне отметку в поле «Включено» (рис. 290).

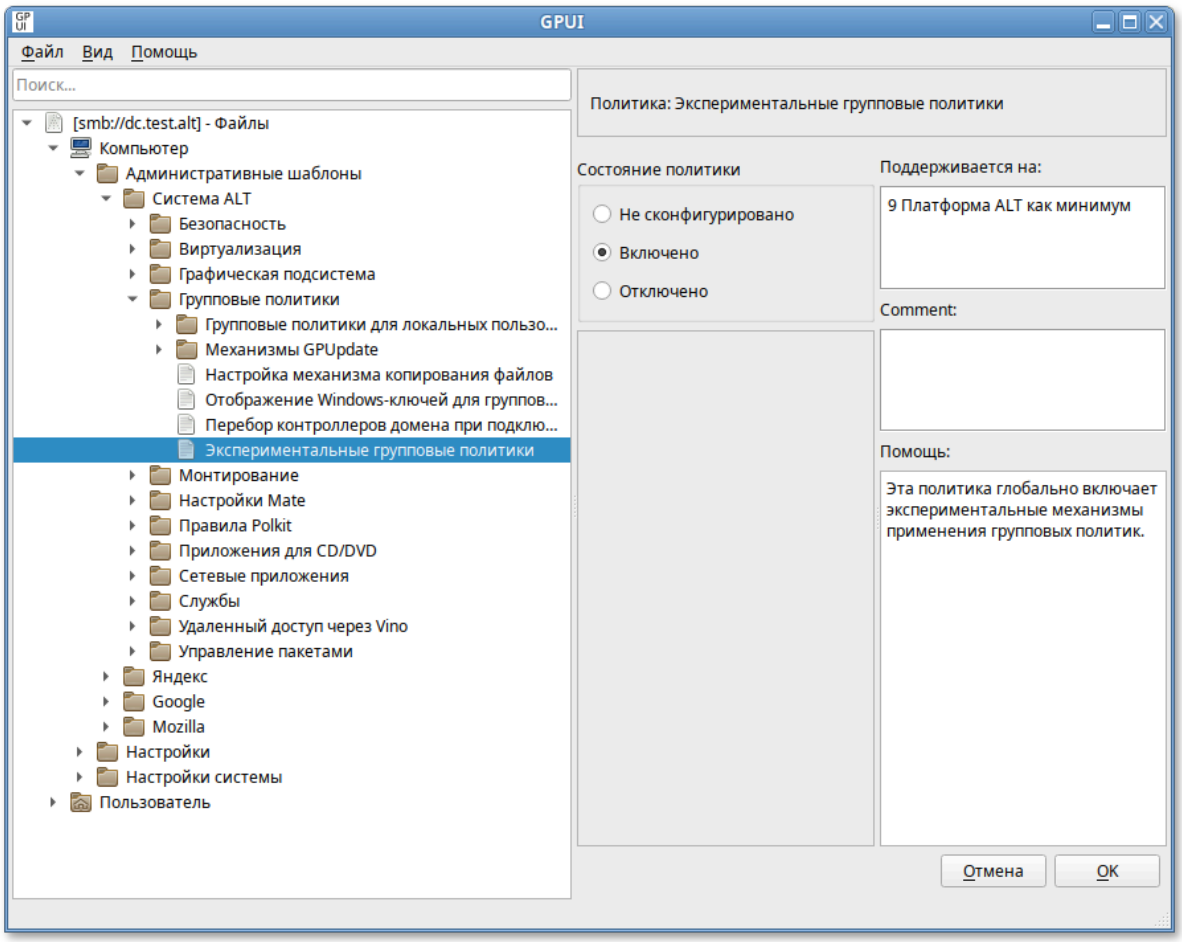


Рис. 290 – «Экспериментальные групповые политики»

9.2.5.4.8. Механизмы GPUpdate

Каждый механизм применения групповых политик можно отдельно включить или отключить. Для этого следует включить/отключить соответствующую политику в разделе «Компьютер»/«Пользователь» → «Административные шаблоны» → «Система ALT» → «Групповые политики»→ «Механизмы GPUpdate».

Например, включить/отключить механизм групповых политик управления пакетами (Packages) можно, включив/отключив политики «Установка и удаление программ» или «Установка и удаление программ для пользователей» (рис. 291).

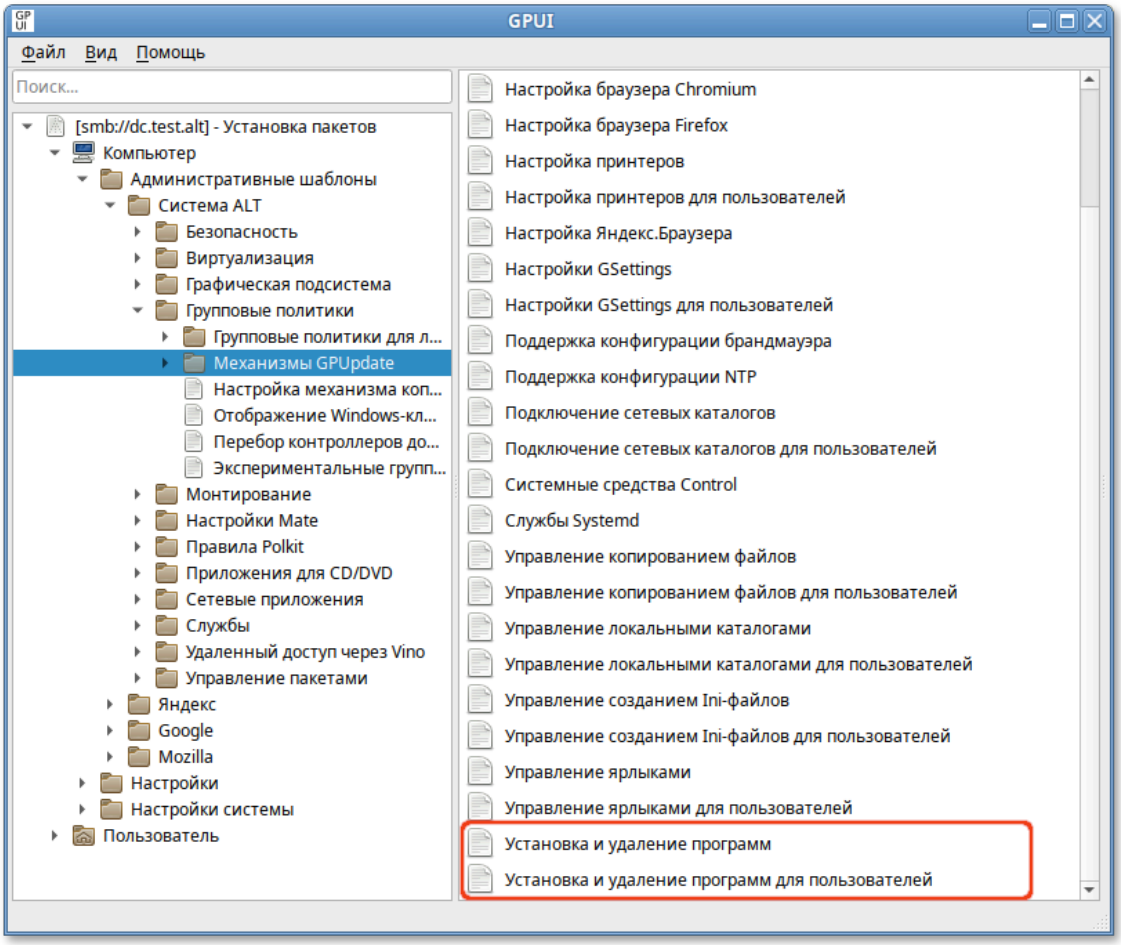


Рис. 291 – Механизм применения групповых политик

9.2.5.4.9. Управление политиками браузера Chromium

Эти групповые политики позволяют централизованно для компьютеров управлять настройками интернет-браузера Google Chromium.

Механизм Chromium в составе пакета gpupdate формирует JSON-файл для веб-браузера из шаблонов групповых политик. Во время запуска веб-браузер Google Chromium считывает файл `/etc/chromium/policies/managed/policies.json` и применяет параметры групповых политик. Групповые политики на основе `policies.json` предоставляют кроссплатформенную совместимость, что позволяет управлять веб-браузерами в любом дистрибутиве Альт с установленным окружением рабочего стола (рис. 292).

Примечание. Данный механизм реализован только для машинных политик.

Примечание. Настройка политик для веб-браузера Chromium требует дополнительной установки ADMX-файлов Google Chrome (пакет admx-chromium).

Результат применения параметров групповой политики для Chromium можно проверить, указав в адресной строке URL: `chrome://policy`.

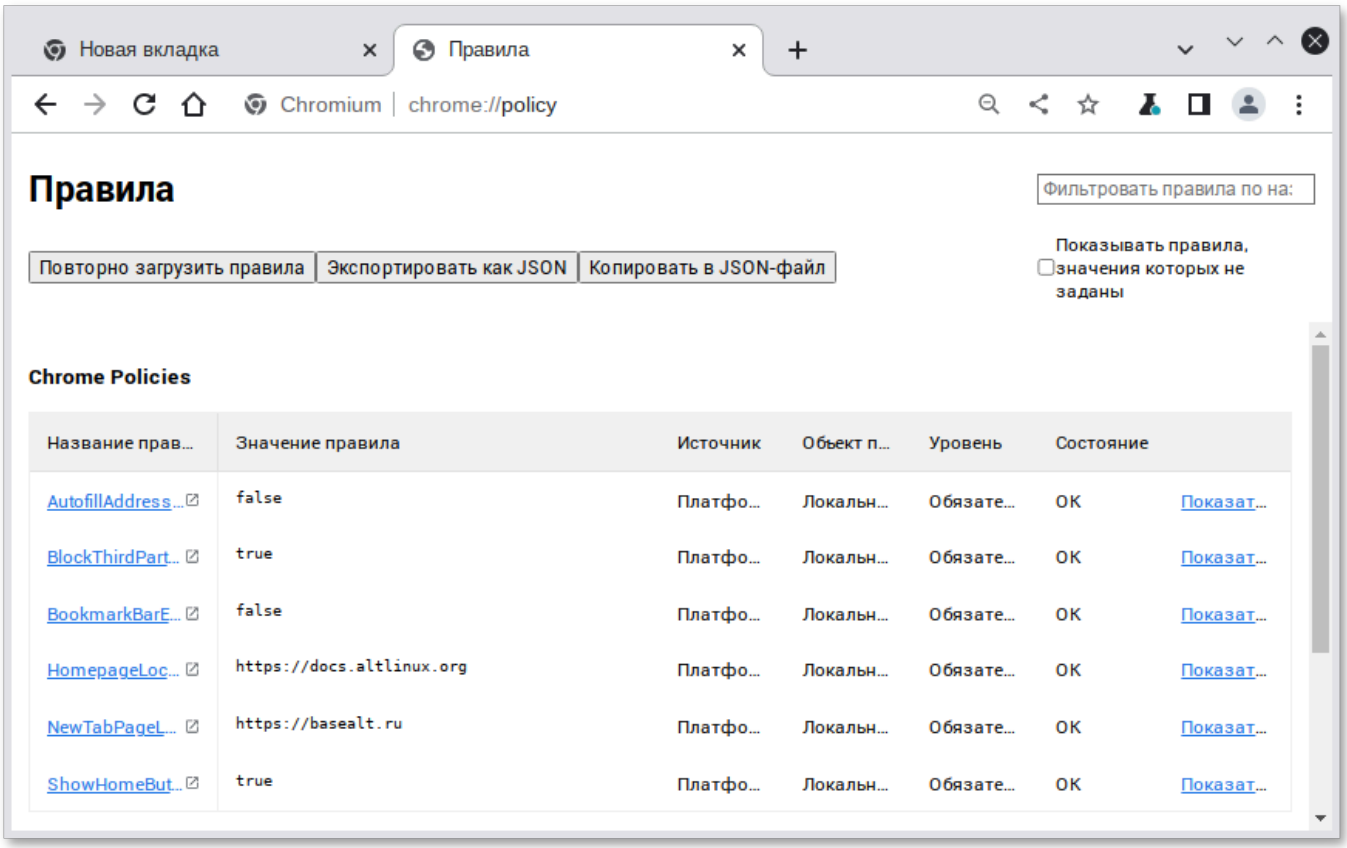


Рис. 292 – Управление политиками веб-браузера Chromium

В качестве примера рассмотрим политику установки URL домашней страницы. Для редактирования политик веб-браузера Chromium следует перейти в «Компьютер» → «Административные шаблоны» → «Google» → «Google Chrome». Отобразится список политик (рис. 293).

Для установки URL домашней страницы следует выбрать пункт «Главная страница и страница быстрого доступа при запуске», щелкнуть левой кнопкой мыши на политике «Настройка URL домашней страницы», откроется диалоговое окно настройки политики. Выбрать параметр «Включено», в разделе «Параметры» ввести URL и нажать кнопку «ОК» (рис. 294).

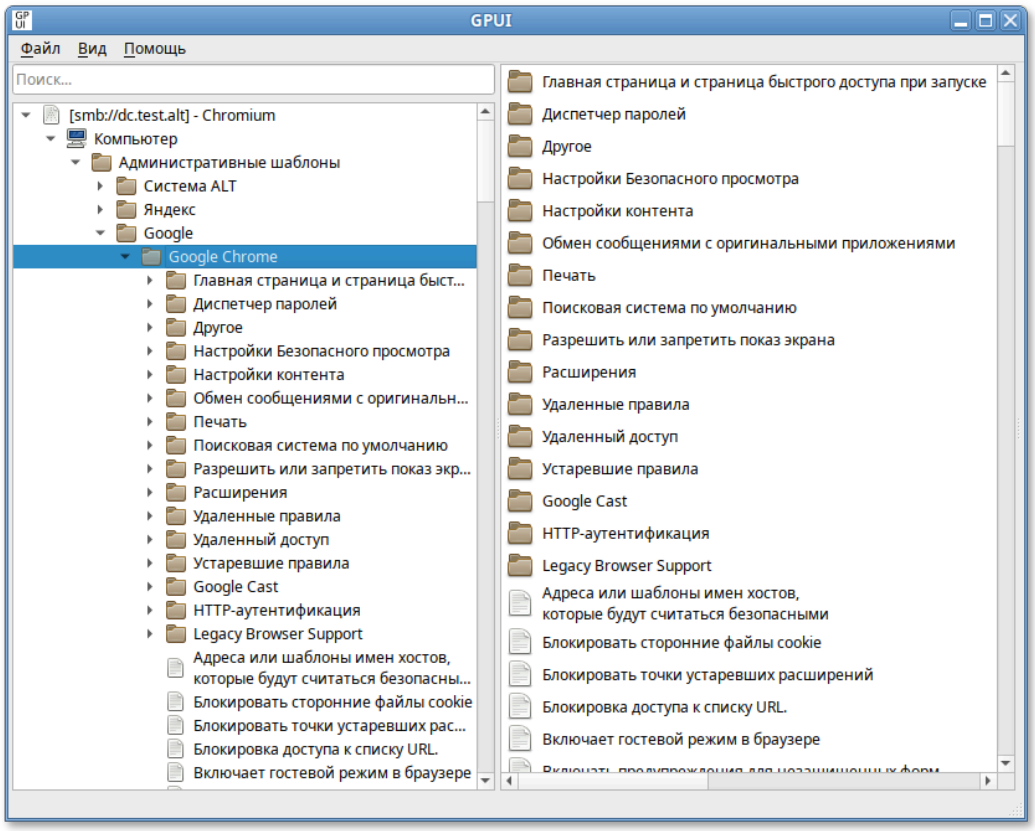


Рис. 293 – Редактирование политик веб-браузера Chromium

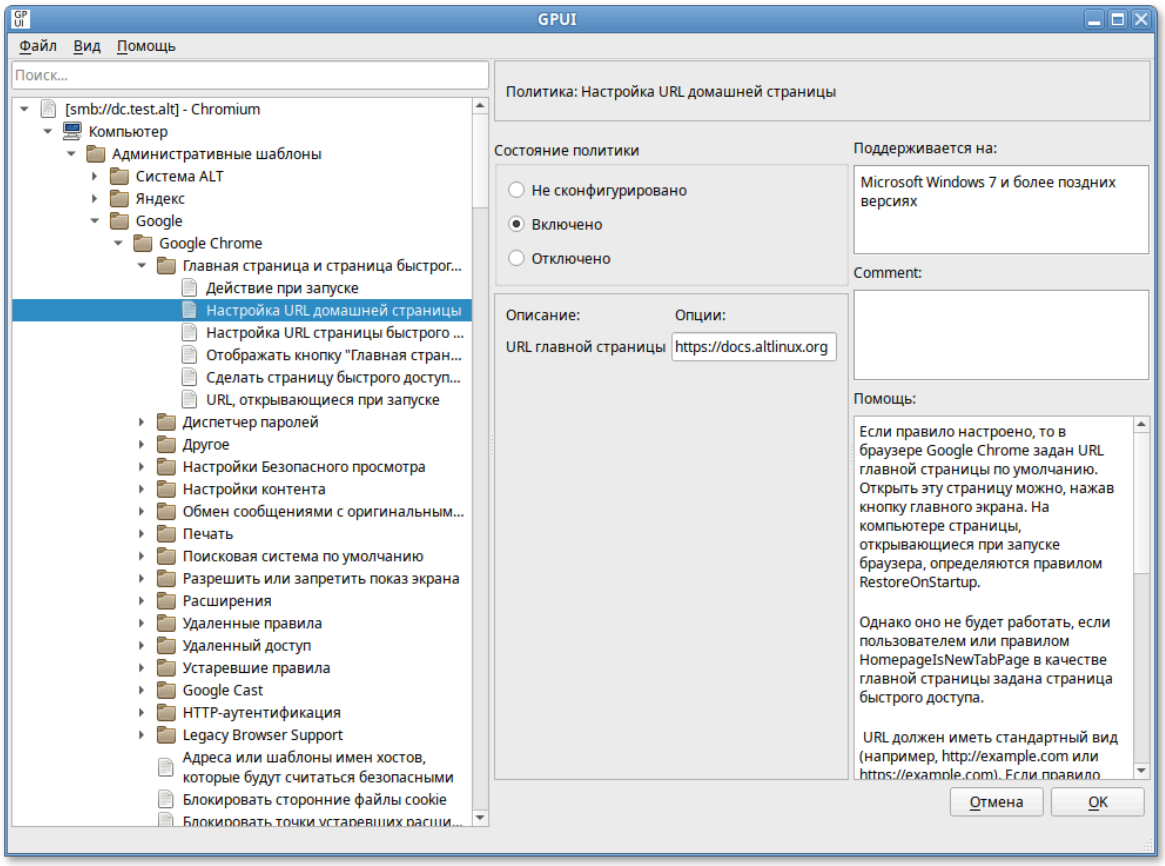


Рис. 294 – Установка URL домашней страницы

Результат применения политики (рис. 295).

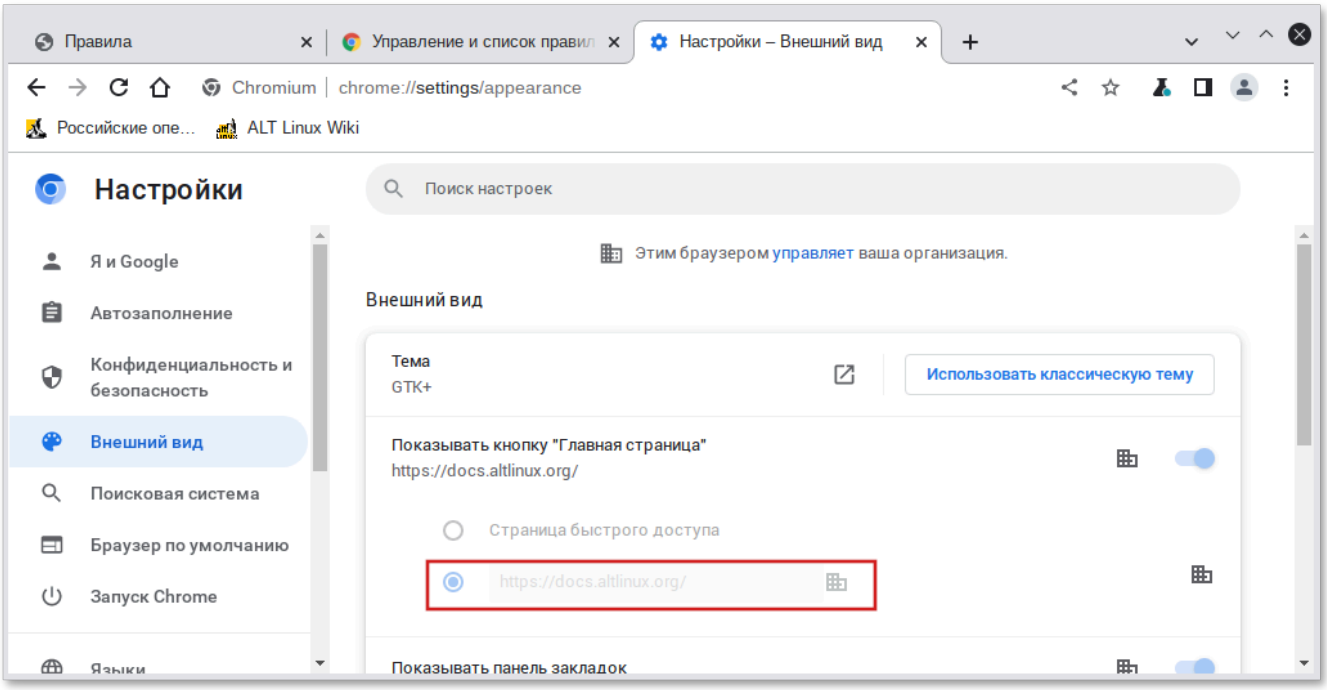


Рис. 295 – Результат применения политики

Все настройки политики веб-браузера Chromium хранятся в файле `{GUID GPT}/Machine/Registry.pol`.

Пример файла `Registry.pol`:

`PReg[Software\Policies\Google\Chrome;HomepageLocation;;;https://docs.altlinux.org]`

В таблице 35 описаны только некоторые политики. Полный список политик и их описание можно найти в веб-браузере Chromium, указав в адресной строке URL: `chrome://policy` и установив отметку на пункте «Показывать правила, значения которых не заданы».

Т а б л и ц а 35 – Примеры политик управляющих настройками браузера Chromium

Политика	Ключ	Описание
Действие при запуске	RestoreOnStartup	Настройка процесса запуска Chromium. При выборе значения «Восстановить последний сеанс» или «Открыть список URL и восстановить последний сеанс» будут отключены некоторые функции, такие как удаление данных о работе в веб-браузере или сессионных файлов cookie при завершении работы. Если для политики указано значение «Открыть список URL и восстановить последний сеанс», веб-браузер будет восстанавливать предыдущий сеанс и открывать URL, заданные в политике «URL, открывающиеся при запуске», в отдельном окне. Если пользователь не закроет страницы с этими URL, они также будут восстановлены в новом сеансе. Если политика находится в состоянии «Включено», пользователи не смогут изменить эту настройку в Chromium
Настройка URL домашней страницы	HomepageLocation	Позволяет установить URL домашней страницы и запрещает пользователям его изменять. Если политика находится в состоянии «Включено», можно установить домашнюю страницу по умолчанию (открыть эту страницу в Chromium можно, нажав кнопку «Главная страница» на панели инструментов). Пользователи при этом не смогут изменить домашнюю страницу. Если политика находится в состоянии «Отключено», пользователи не смогут установить домашнюю страницу. Если политика находится в состоянии «Не сконфигурировано», пользователь может сам установить и изменить домашнюю страницу. Данная политика не будет работать, если пользователем или политикой «Сделать страницу быстрого доступа главной» в качестве главной страницы была задана страница быстрого доступа
Настройка URL страницы быстрого доступа	NewTabPageLocation	Позволяет установить URL страницы быстрого доступа по умолчанию и запрещает пользователям его изменять. Страница быстрого доступа появляется, когда пользователь открывает новую вкладку или окно. Политика не определяет, какие страницы открываются при запуске. Для этого применяется политика «Действие при запуске». Но если страница быстрого доступа используется в качестве главной или стартовой страницы, эта политика также распространяется и на них. Если политика находится в состоянии «Не сконфигурировано» или URL не указан, используется страница быстрого доступа, установленная по умолчанию

Продолжение таблицы 35

Политика	Ключ	Описание
Отображать кнопку «Главная страница» на панели инструментов	ShowHomeButton	Позволяет управлять отображением кнопки «Главная страница» на панели инструментов. Если политика находится в состоянии «Включено», кнопка «Главная страница» отображается на панели инструментов. Если политика находится в состоянии «Отключено», кнопка «Главная страница» не будет отображаться. Если эта политика настроена, пользователи не смогут изменить эту настройку в Chromium. В противном случае пользователи смогут добавить или скрыть кнопку главного экрана
Сделать страницу быстрого доступа главной	HomepageIsNewTabPage	Если политика находится в состоянии «Включено», в качестве главной страницы используется страница быстрого доступа. Заданный URL главной страницы игнорируется. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», страница быстрого доступа открывается, только когда в качестве URL главной страницы указан путь `chrome://newtab`. Если эта политика настроена, пользователи не смогут изменить главную страницу в Chromium. Если политика не настроена, они смогут выбрать, устанавливать ли страницу быстрого доступа в качестве главной
URL, открывающиеся при запуске	RestoreOnStartupURLs	Если для политики «Действие при запуске» задано значение «Открыть одну или несколько страниц», в данной политике можно настроить список URL-адресов. В противном случае при запуске будет открываться страница быстрого доступа
Включить сохранение паролей	PasswordManagerEnabled	Если политика находится в состоянии «Включено» или «Не сконфигурировано», Chromium будет предлагать запоминать введенные пароли (а также предлагать их при следующем входе). Если политика находится в состоянии «Отключено», пользователям будут доступны только ранее сохраненные пароли, а сохранить новые будет нельзя. Если политика настроена, пользователи не могут изменить ее в Chromium. В противном случае пользователи при желании смогут отключить функцию сохранения паролей
Включить поисковую систему по умолчанию	DefaultSearchProviderEnabled	Если политика находится в состоянии «Включено», то при вводе в адресную строку текста (не URL) будет выполняться поиск в используемой по умолчанию поисковой системе.

Продолжение таблицы 35

Политика	Ключ	Описание
		Задать поисковую систему по умолчанию можно с помощью других политик. Если значения для этих политик не установлены, пользователь может сам выбрать поисковую систему по умолчанию. Если политика находится в состоянии «Отключено», то поиск текста, введенного в адресную строку, не выполняется
Название поисковой системы по умолчанию	DefaultSearchProvider Name	Если политика «Включить поисковую систему по умолчанию» включена, то данная политика задает название поисковой системы по умолчанию. Если параметр «Включить поисковую систему по умолчанию» не задан, то используется имя хоста, указанное в URL поискового запроса
Показ URL страницы быстрого доступа в поисковой системе по умолчанию	DefaultSearchProvider NewTabURL	Если политика «Включить поисковую систему по умолчанию» включена, то данная политика указывает URL поисковой системы, используемой для страницы быстрого доступа. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», страница быстрого доступа не будет использоваться
URL поиска для поисковой системы по умолчанию	DefaultSearchProvider SearchURL	Если политика «Включить поисковую систему по умолчанию» включена, то данная политика содержит URL поисковой системы, используемой по умолчанию. В URL должна быть строка '{searchTerms}', которая во время отправки запроса заменяется на текст пользователя. URL поисковой системы Google можно указать так: `'{google:baseURL}search?q={searchTerms}&{google:RLZ}{google:originalQueryForSuggestion}{google:assistedQueryStats}{google:searchFieldtrialParameter}{google:searchClient}{google:sourceId}ie={inputEncoding}'`
Включить панель закладок	BookmarkBarEnabled	Если политика находится в состоянии «Включено», в Chromium будет видна панель закладок. Если политика находится в состоянии «Отключено», панель закладок будет всегда скрыта. Если эта политика настроена, пользователи не смогут ее изменить. Если политика находится в состоянии «Не сконфигурировано», пользователи смогут самостоятельно решать, использовать эту функцию или нет.
Разрешить пользователям менять фон на странице быстрого доступа	NTPCustomBackgroundEnabled	Если политика находится в состоянии «Отключено», пользователи не смогут изменять фон страницы быстрого доступа. Уже используемые изображения удаляются без возможности восстановления. Если политика находится в состоянии «Включено» или «Не сконфигурировано», пользователи могут изменять фон страницы быстрого доступа

Продолжение таблицы 35

Политика	Ключ	Описание
Блокировать изображения на этих сайтах	ImagesBlockedForUrls	Позволяет задать список шаблонов URL для указания сайтов (значение * не поддерживается для этой политики), на которых запрещен показ изображений. Если политика находится в состоянии «Включено», Chromium будет блокировать изображения на указанных сайтах. Если политика находится в состоянии «Не сконфигурировано», то действует политика «Настройка изображений по умолчанию») при условии, что оно задано. В противном случае применяются персональные настройки пользователя
Блокировка доступа к списку URL	URLBlocklist	Если политика находится в состоянии «Включено», страницы с запрещенными URL не загружаются (задаются шаблоны запрещенных URL). Если политика находится в состоянии «Не сконфигурировано», веб-браузер не блокирует URL. Формат шаблона URL должен соответствовать требованиям, указанным на странице `https://www.chromium.org/administrators/url-blocklist-filter-format`. В политике URLAllowlist можно задавать не более 1000 исключений
Всегда открывать PDF-файлы во внешнем приложении	AlwaysOpenPdfExternally	Если политика находится в состоянии «Включено», встроенное средство просмотра PDF-файлов в Chromium отключается, они начинают обрабатываться как скачанный контент, а пользователю разрешается открывать их в приложении, установленном по умолчанию. Если политика находится в состоянии «Отключено», для просмотра PDF-файлов будет использоваться плагин PDF (если он не отключен пользователем). Если политика находится в состоянии «Не сконфигурировано», пользователи смогут настраивать этот параметр самостоятельно
Всегда указывать место для скачивания	PromptForDownloadLocation	Если политика находится в состоянии «Включено», то при скачивании каждого файла пользователь должен указать, в какой каталог его сохранить. Если политика находится в состоянии «Отключено», скачивание выполняется без запроса каталога для сохранения. Если политика находится в состоянии «Не сконфигурировано», пользователи могут выбрать каталог, в который всегда будут сохраняться файлы
Выбор каталога для скачиваний	DownloadDirectory	В этой политике указывается каталог, в котором веб-браузер Chromium сохраняет скачиваемые файлы. Данный каталог используется, даже если пользователь выбрал каталог для сохранения или установил флажок, позволяющий выбирать каталог при каждом скачивании файла.

Продолжение таблицы 35

Политика	Ключ	Описание
		Эта политика отменяет действие политики DefaultDownloadDirectory. Если политика находится в состоянии «Не сконфигурировано», веб-браузер Chromium скачивает файлы в каталог по умолчанию, а пользователь может его изменить. Список переменных можно посмотреть на странице `https://www.chromium.org/administrators/policy-list-3/user-data-directory-variables`
Доступ к поисковой системе по умолчанию в контекстном меню	DefaultSearchProviderContextMenuAccessAllowed	Позволяет использовать поисковую систему по умолчанию в контекстном меню. Если политика находится в состоянии «Включено» или «Не сконфигурировано», поиск в системе по умолчанию будет доступен в контекстном меню. Если политика находится в состоянии «Отключено», поиск будет недоступен в контекстном меню. Значение этой политики применяется только в том случае, если включена политика «Включить поисковую систему по умолчанию»
Доступность режима инкогнито	IncognitoModeAvailability	Определяет, может ли пользователь просматривать страницы в Chromium в режиме инкогнито. Если политика находится в состоянии «Включено» или значение не задано, страницы можно открывать в режиме инкогнито. Если политика находится в состоянии «Отключено», пользователи не смогут открывать страницы в режиме инкогнито. Если для политики выбрано значение «Включить принудительно», страницы можно просматривать ТОЛЬКО в режиме инкогнито
Удаление истории просмотров и загрузок веб-браузера	AllowDeletingBrowserHistory	Определяет, может ли пользователь удалять историю просмотров и скачиваний. Если политика находится в состоянии «Включено» или «Не сконфигурировано», то историю просмотров и скачиваний можно удалить. Если политика находится в состоянии «Отключено», то историю просмотров и скачиваний удалить нельзя
Разрешить вызов окна выбора файлов	AllowFileSelectionDialogs	Если политика находится в состоянии «Включено» или «Не сконфигурировано», то пользователи смогут открывать в Chromium окна выбора файлов. Если политика находится в состоянии «Отключено», и пользователь выполняет действия, для которых нужно открыть окно выбора файлов (например, импортирует закладки, загружает файлы, сохраняет ссылки и т. д.), вместо окна отображается сообщение и предполагается, что пользователь нажал кнопку «Отмена» в окне выбора файлов

Продолжение таблицы 35

Политика	Ключ	Описание
Включить поисковые подсказки	SearchSuggestEnabled	Если политика находится в состоянии «Включено», в адресной строке Chromium при поиске будут появляться подсказки. Если политика находится в состоянии «Отключено», поисковые подсказки не отображаются. Эта политика не влияет на показ в строке поиска закладок и страниц из истории просмотров. Если политика настроена, пользователи не могут изменить ее. Если политика не настроена, подсказки при поиске будут включены, но пользователи смогут отключить их в любое время
Настройка изображений по умолчанию	DefaultImagesSetting	Если политика находится в состоянии «Включено» и выбрано значение 1 – «Разрешить показ изображений на всех сайтах», на всех сайтах могут показываться изображения. При значении 2 – «Запретить показ изображений на всех сайтах», показ изображений на сайтах запрещен. Если политика находится в состоянии «Не сконфигурировано», показ изображений разрешен, но пользователи могут изменять этот параметр
Разрешить полноэкран-ный режим	FullscreenAllowed	Если политика находится в состоянии «Включено» или «Не сконфигурировано», то при наличии разрешений пользователи, приложения и расширения смогут включать полноэкранный режим, в котором виден только контент веб-страниц. Если политика находится в состоянии «Отключено», то полноэкранный режим будет заблокирован для всех пользователей, приложений и расширений
Включить анонимный сбор данных	UrlKeyedAnonymizedDataCollectionEnabled	Если политика находится в состоянии «Включено», то всегда выполняется анонимный сбор данных о URL (эти сведения отправляются в Google с целью улучшить поиск и просмотр веб-страниц). Если политика находится в состоянии «Отключено», сбор данных о URL не выполняется. Если политика находится в состоянии «Не сконфигурировано», пользователь может разрешить или запретить анонимный сбор данных о URL
Управляемые закладки	ManagedBookmarks	Политика позволяет установить список закладок в Chromium. Если политика настроена, будет создан список закладок Каждая закладка представляет собой словарь, где ключам name и url соответствуют значения – название закладки и URL-адрес сайта `([{"name": "Документация","url": "docs.altlinux.org"},{"name": "Wiki","url": "altlinux.org"}]).` По умолчанию папка называется «Управляемые закладки».

Продолжение таблицы 35

Политика	Ключ	Описание
		Чтобы изменить это название, нужно добавить в правило дополнительный словарь с единственным ключом toplevel_name и названием папки в качестве значения. Также можно задать подпапку для закладок. Для этого вместо ключа url следует использовать ключ children, а в качестве его значения указать список вложенных закладок или папок `([{"toplevel_name":"ALT"},{"name":"BaseALT","url":"basealt.ru"}, {"name":"ALT docs","children":[{"name": "Документация","url": "docs.altlinux.org"}, {"name": "Wiki","url": "altlinux.org"}]}]).` Chromium дополняет неполные URL так же, как при их вводе в адресной строке. Например, адрес altlinux.org будет преобразован в `https://altlinux.org/`. Пользователи не смогут изменять папки с закладками, а только скрывать их на панели. Управляемые закладки не синхронизируются с аккаунтом пользователя, а расширения не могут их изменять
Отключить синхронизацию данных с Google	SyncDisabled	Если политика находится в состоянии «Включено», синхронизация данных в Chromium с помощью сервисов, размещенных в Google, отключается. Полностью отключить сервис «Chrome Sync» можно через Google Admin console. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователи могут самостоятельно решать, использовать ли им сервис «Chrome Sync»
Включает гостевой режим в браузере	BrowserGuestModeEnabled	Если политика находится в состоянии «Включено» или «Не сконфигурировано», разрешается использовать гостевой доступ. При гостевом доступе все окна для профилей Chromium открываются в режиме инкогнито. При гостевом доступе все окна для профилей Chromium открываются в режиме инкогнито. Если политика находится в состоянии «Отключено», в веб-браузере не разрешается использовать гостевые профили
Удаление данных о работе в веб-браузере при выходе	ClearBrowsingDataOnExitList	Политика позволяет настроить список данных о работе в веб-браузере, которые должны удаляться, когда пользователь закрывает все окна веб-браузера. Можно указать следующие типы данных: - browsing_history (история веб-браузера); - download_history (история скачиваний); - cookies_and_other_site_data (файлы cookie и другие данные сайтов); - cached_images_and_files (изображения и другие файлы, сохраненные в кэше); - password_signin (пароли); - autofill (автозаполнение);

Продолжение таблицы 35

Политика	Ключ	Описание
		- site_settings (настройки сайтов); - hosted_app_data (данные размещенных приложений). У этой политики нет приоритета над политикой «Удаление истории просмотров и загрузок веб-браузера». Эта политика работает, если политика «Отключить синхронизацию данных с Google» находится в состоянии «Включено». В противном случае политика игнорируется. Если Chromium закрывается непредвиденно (например, из-за сбоя в работе веб-браузера или ОС), данные о работе в веб-браузере удаляются при следующей загрузке профиля. Если политика находится в состоянии «Отключено», то данные о работе, при закрытии веб-браузера, не удаляются
Задать объем кеша в байтах	DiskCacheSize	Если для политики задано значение «None», Chromium использует объем кэша по умолчанию для хранения кэшированных файлов на диске. В этом случае пользователи не могут изменить правило. Если политика находится в состоянии «Включено», Chromium будет использовать указанный размер кэша независимо от того, указали ли пользователи значение экспериментального параметра `--disk-cache-size`. Объем кэша задается в байтах, например, чтобы задать размер кэша 300МБ, нужно указать 314572800. Значения меньше нескольких мегабайтов округляются. Если политика находится в состоянии «Не сконфигурировано», Chromium использует объем по умолчанию. В этом случае пользователи могут менять размер кэша с помощью экспериментального параметра `--disk-cache-size`. Указанное в правиле значение используется различными подсистемами в веб-браузере как справочное. Поэтому фактический объем используемого дискового пространства может превышать указанное значение, но будет иметь такой же порядок
Список разрешенных серверов для аутентификации	AuthServerAllowlist	Это правило указывает, какие серверы можно использовать для встроенной проверки подлинности Windows (IWA). Встроенная проверка подлинности включается, только когда Chromium получает запрос на аутентификацию от прокси-сервера или от сервера из списка разрешенных. Если политика находится в состоянии «Не сконфигурировано», Chromium отвечает на запросы IWA только после того, как определяет, находится ли сервер в интранете. Если сервер находится в Интернете, Chromium игнорирует поступающие от него IWA запросы (веб-сайту не разрешается использовать аутентификацию SPNEGO с помощью веб-браузера). Названия серверов нужно разделять запятыми. Допустимы подстановочные знаки (*)

Продолжение таблицы 35

Политика	Ключ	Описание

Управление расширениями (Позволяет управлять расширениями)	ExtensionSettings	Это правило контролирует настройки управления расширениями в Chromium, включая те, которые заданы другими правилами. Оно заменяет любые ранее действовавшие правила.
		Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователи могут самостоятельно настраивать расширения.
		Если политика находится в состоянии «Включено», настройки расширений задает администратор с помощью кода, указанного в параметрах политики:
		- идентификатор расширения или URL обновления привязывается только к одной конкретной настройке;
		- идентификатор * действует на все расширения, для которых в политике не задана отдельная конфигурация. Если указан URL обновления, заданная конфигурация применяется ко всем расширениям, в манифесте которых приведен этот URL.
		Пример значения:
		`{`
		`  "hdokiejnpimakedhajhdlcegeplioahd": {`
		`  "installation_mode": "force_installed",`
		`  "update_url": "https://clients2.google.com/service/update2/crx"`
		`  },`
		`  "pioclpoplcdbaefihamjohnefbikjilc": {`
		`  "installation_mode": "force_installed",`
		`  "update_url": "https://clients2.google.com/service/update2/crx"`
		`  }`
		`}`

Управление расшире-ниями (Позволяет управлять расшире-ниями)	ExtensionSettings	Параметры политики: 1) allowed_types – типы приложений и расширений, которые пользователям разрешено устанавливать в веб-браузере (допустимые строки: «extension», «hosted_app», «legacy_packaged_app», «tplatform_appeme», «theme», «user_script»). Используется только для настройки конфигурации по умолчанию со значением *; 2) blocked_install_message – уведомление (не более 1000 символов), которое будет появляться на устройствах пользователей при попытке установить запрещенные расширения; 3) blocked_permissions – запрещает пользователям устанавливать и запускать расширения, требующие разрешений API (список доступных разрешений указан в манифесте расширения); 4) installation_mode – указывает, разрешено ли добавлять заданные расширения. Допустимые режимы: - allowed – пользователи могут установить это расширение (поведение по умолчанию);

Продолжение таблицы 35

Политика	Ключ	Описание
		- blocked – пользователи не могут установить это расширение; - removed – пользователи не могут установить это расширение. Если расширение было установлено, оно будет удалено; - force_installed – расширение устанавливается автоматически. Пользователи не могут его удалить. В этом режиме нужно указать ссылку для скачивания расширения (параметр update_url); - normal_Installed – расширение устанавливается автоматически. Пользователи могут его удалить. В этом режиме нужно указать ссылку для скачивания расширения (параметр update_url); 5) install_sources – список URL страниц, с которых разрешено загружать и устанавливать расширения. Нужно разрешить URL расположения CRX-файла и страницы, с которой начинается скачивание (то есть URL перехода); 6) minimum_version_required – отключает расширения (в том числе установленные принудительно) более ранних версий, чем определено этим параметром. Формат строки версии аналогичен формату, который используется в манифесте расширения; 7) install_sources – список URL страниц, с которых разрешено загружать и устанавливать расширения. Нужно разрешить URL расположения CRX-файла и страницы, с которой начинается скачивание (то есть URL перехода); 8) install_sources – список URL страниц, с которых разрешено загружать и устанавливать расширения. Нужно разрешить URL расположения CRX-файла и страницы, с которой начинается скачивание (то есть URL перехода); 9) minimum_version_required – отключает расширения (в том числе установленные принудительно) более ранних версий, чем определено этим параметром. Формат строки версии аналогичен формату, который используется в манифесте расширения; 10) update_url – определяет, откуда загружается расширение
Управление расширениями (Позволяет управлять расширениями)	ExtensionSettings	Можно указать URL интернет-магазина Chrome, Opera или использовать XML-файл: - если расширение размещено в интернет-магазине Chrome, следует указать `https://clients2.google.com/service/update2/crx`

Окончание таблицы 35

Политика	Ключ	Описание
		- если расширение размещено в интернет-магазине Opera, следует указать `https://extension-updates.opera.com/api/omaha/update/` - override_update_url – указывает, что для всех последующих обновлений расширения будет использоваться URL из поля update_url или update в политике ExtensionInstallForcelist. Если это политика не настроена или отключена, будет использоваться URL из манифеста расширения; - verified_contents_url – указывает путь до файла «extension.verified_contents». С его помощью расширение проверяется на доверие (используется, если нет доступа в интернет); - runtime_allowed_hosts – разрешает взаимодействие расширений с указанными сайтами, даже если они указаны в поле runtime_blocked_hosts. Можно указать до 100 сайтов; - runtime_blocked_hosts – запрещает расширениям взаимодействовать с указанными сайтами или изменять их, в том числе вставлять скрипты, получать доступ к файлам cookie и изменять веб-запросы. Можно указать до 100 сайтов; - toolbar_pin – определяет, закреплен ли значок расширения на панели инструментов. Возможные значения: а) force_pinned – значок расширения закреплен на панели инструментов и постоянно виден. Пользователь не может скрыть его в меню расширения; б) default_unpinned – расширение скрыто в меню расширений (по умолчанию), пользователь может закрепить его на панели инструментов

9.2.5.4.10. Управление политиками веб-браузера Firefox

Эти групповые политики позволяют централизованно для компьютеров управлять настройками интернет-браузера Mozilla Firefox.

Механизм Firefox в составе пакета gpupdate формирует JSON-файл для веб-браузера из шаблонов групповых политик. Во время запуска веб-браузер Mozilla Firefox считывает собственный файл policies.json и применяет параметры групповых политик. Групповые политики на основе policies.json предоставляют

кроссплатформенную совместимость, что позволяет управлять веб-браузерами в любом дистрибутиве Альт с установленным окружением рабочего стола.

Путь к файлу «policies.json», в зависимости от версии веб-браузера Mozilla Firefox:

- `/etc/firefox/policies` – новые версии;

- `/usr/lib64/firefox/distribution` – старые версии.

Примечание. Данный механизм реализован только для машинных политик.

Примечание. Настройка политик для веб-браузера Mozilla Firefox требует дополнительной установки ADMX-файлов Firefox (пакет admx-firefox) (рис. 296).

Результат применения параметров групповой политики для Mozilla Firefox можно проверить, указав в адресной строке URL:

`about:policies#active`

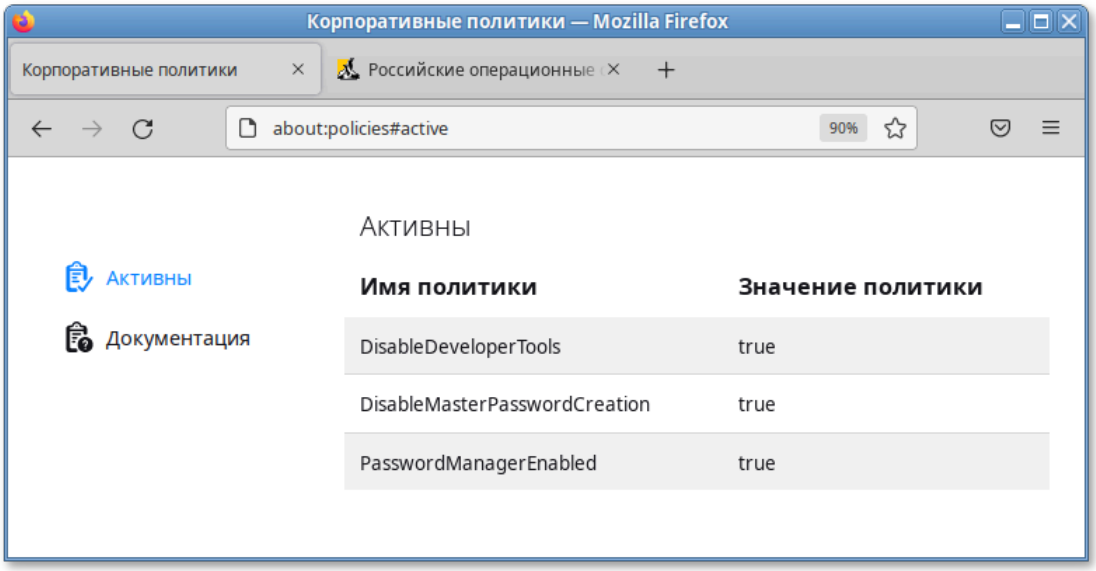


Рис. 296 – Настройка политик для веб-браузера Mozilla Firefox

В качестве примера рассмотрим политику установки URL домашней страницы.

Для редактирования политик веб-браузера Mozilla Firefox следует перейти в «Компьютер» → «Административные шаблоны» → «Mozilla» → «Firefox» (рис. 297).

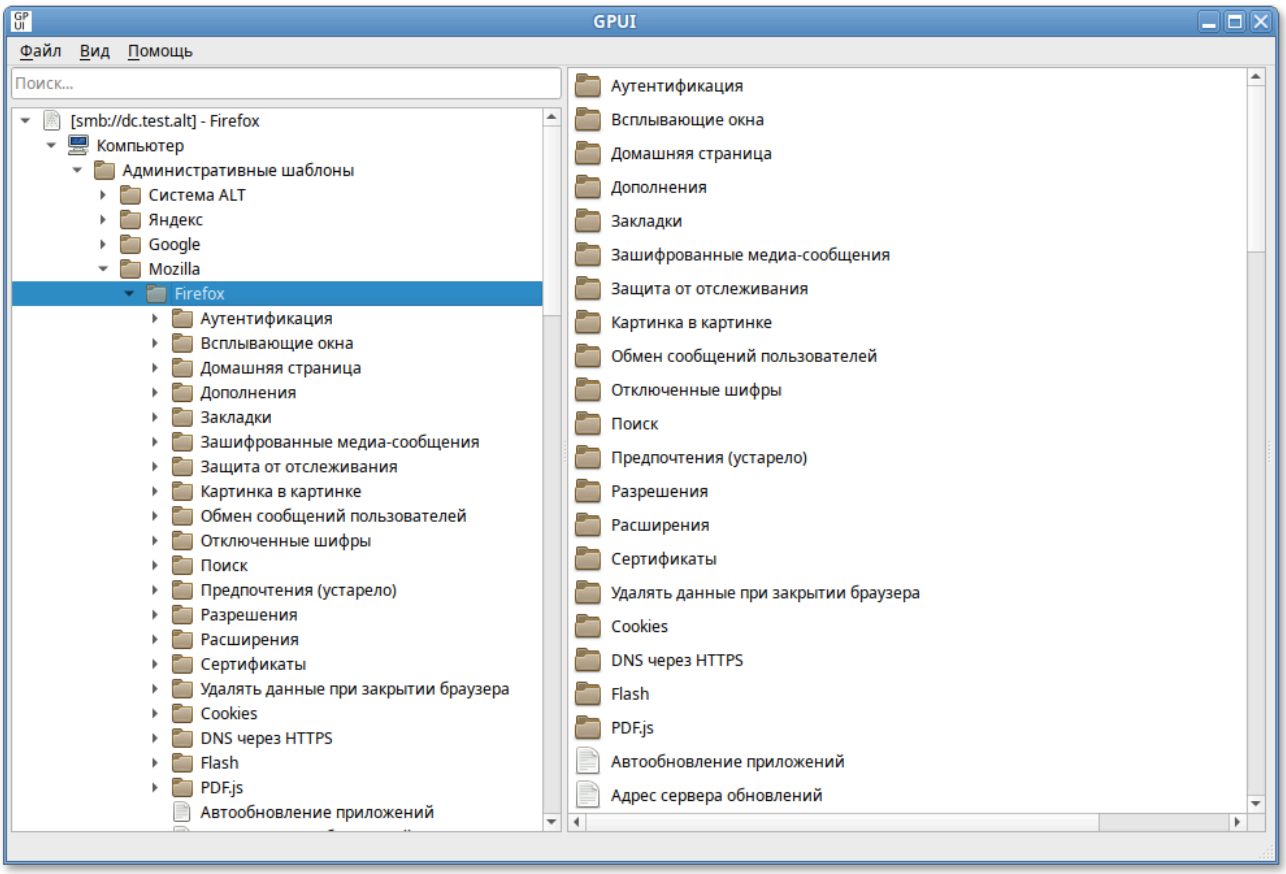


Рис. 297 – Редактирование политик веб-браузера Mozilla Firefox

Раскрыть группу «Домашняя страница», щелкнуть левой кнопкой мыши на политике «URL для домашней страницы», откроется диалоговое окно настройки политики. Выбрать параметр «Включено», в разделе «Параметры» ввести URL и нажать кнопку «ОК» (рис. 298).

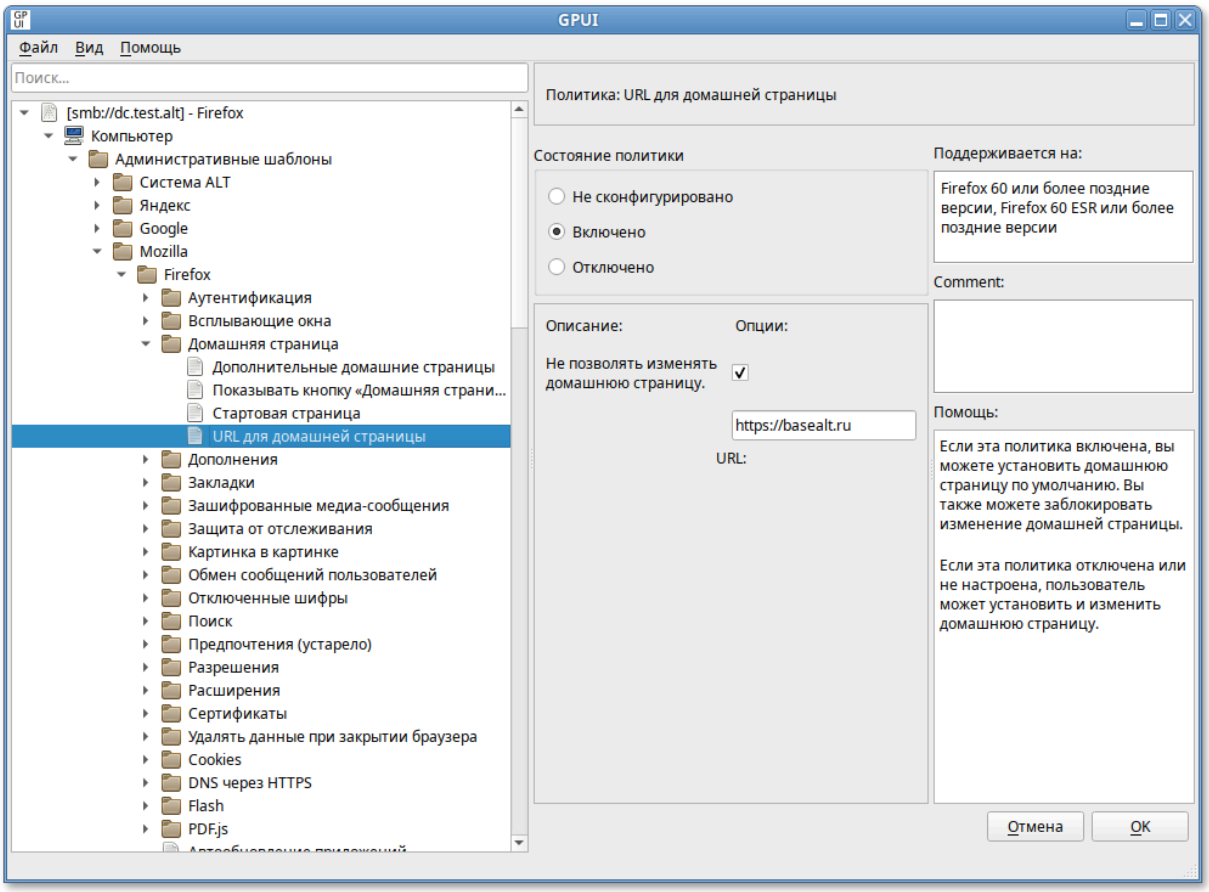


Рис. 298 – Группа «Домашняя страница»

В результате применения данной политики будет установлена домашняя страница по умолчанию, а также будет заблокирована возможность изменения домашней страницы пользователем (рис. 299).

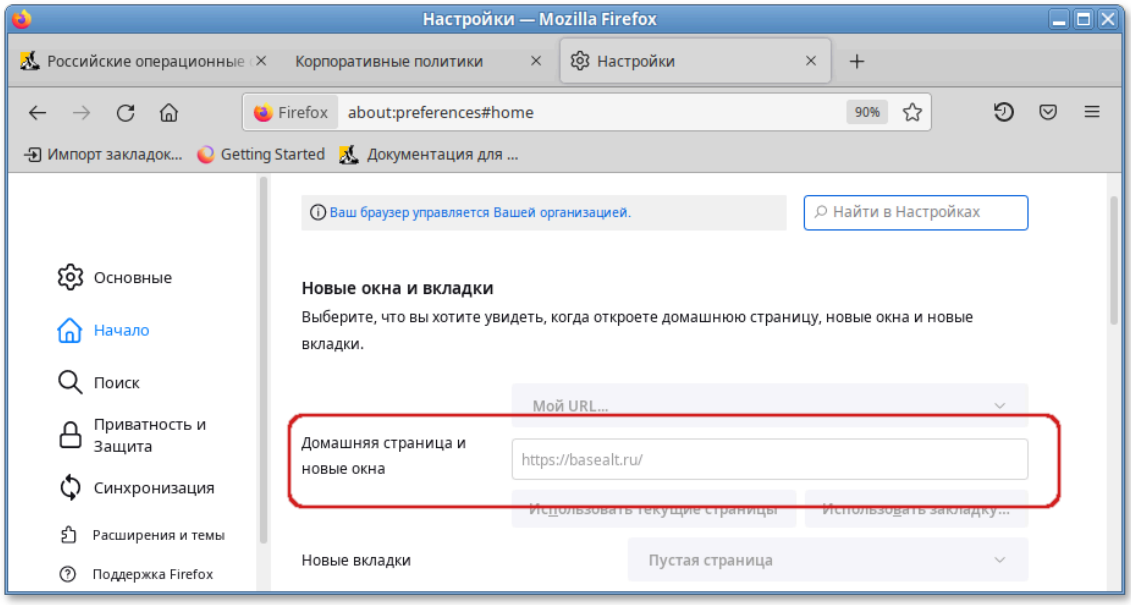


Рис. 299 – Результат применения данной политики

Все настройки политики веб-браузера Chromium хранятся в файле `{GUID GPT}/Machine/Registry.pol`.

Пример файла `Registry.pol`:

```
PReg[Software\Policies\Mozilla\Firefox\Homepage;URL;;;https://basealt.ru]
[Software\Policies\Mozilla\Firefox\Homepage;Locked;;;]
```

В таблице 36 описаны только некоторые политики. Полный список политик и их описание можно найти в веб-браузере Mozilla Firefox, указав в адресной строке URL:

`about:policies#documentation`

Таблица 36 – Примеры политик управляющих настройками веб-браузера Mozilla Firefox

Политика	Ключ	Описание
Менеджер паролей	PasswordManagerEnabled	Позволяет запретить доступ к менеджеру паролей через настройки и блокирует about:logins. Если эта политика находится в состоянии «Включено» или «Не сконфигурировано», менеджер паролей доступен в настройках и на странице about:logins. Если эта политика находится в состоянии «Отключено», Firefox запрещает доступ к менеджеру паролей через настройки и блокирует about:logins
Отключить создание мастер-пароля	DisableMasterPasswordCreation	Позволяет отключить возможность установить мастер-пароль (основной пароль). Если эта политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователи могут создать мастер-пароль. Если эта политика находится в состоянии «Включено», то она работает так же, как установка политики «Основной (главный) пароль» состояние «Отключено», и пользователи не могут создать мастер-пароль. Если используются и политика «Отключить создание мастер-пароля», и «Основной (главный) пароль», то политика «Отключить создание мастер-пароля» имеет приоритет
Предлагать сохранить логины	OfferToSaveLogins	Позволяет настроить будет ли Firefox предлагать запоминать сохраненные логины и пароли. Если политика находится в состоянии «Отключено», Firefox не будет предлагать сохранять логины и пароли веб-сайтов. Если политика находится в состоянии «Включено» или «Не сконфигурировано», Firefox будет предлагать сохранять логины и пароли веб-сайтов
Отключить инструменты разработчика	DisableDeveloperTools	Позволяет управлять доступом к инструментам разработчика. Если политика находится в состоянии «Включено»,

Продолжение таблицы 36

Политика	Ключ	Описание
		инструменты веб-разработчика недоступны в Firefox. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», инструменты веб-разработчика доступны в Firefox
Отключить инструменты разработчика	DisableDeveloperTo ols	Позволяет управлять доступом к инструментам разработчика. Если политика находится в состоянии «Включено», инструменты веб-разработчика недоступны в Firefox. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», инструменты веб-разработчика доступны в Firefox
Отключить приватный просмотр	DisablePrivateBrows ing	Запрещает доступ к приватному просмотру. Если политика находится в состоянии «Включено», приватный просмотр запрещен. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», приватный просмотр разрешен
Нет закладок по умолчанию	NoDefaultBookmark s	Отключает создание закладок по умолчанию (идущих вместе с Firefox), и смарт-закладки (часто посещаемые, недавние). Если политика находится в состоянии «Включено», закладки по умолчанию и смарт-закладки (наиболее посещаемые, недавние теги) не создаются. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», создаются закладки по умолчанию и смарт-закладки (наиболее посещаемые, последние теги). П р и м е ч а н и е : эта политика эффективна только в том случае, если она используется до первого запуска профиля
Запрос места загрузки	PromptForDownload Location	Спрашивает, куда сохранять файлы при загрузке. Если политика находится в состоянии «Отключено», файлы будут сохраняться в каталог указанный в настройках (пользователю не предлагается указать место для загрузки файла). Если политика находится в состоянии «Включено», пользователю будет всегда выдаваться запрос на сохранение файла. Если политика находится в состоянии «Не сконфигурировано», пользователю будет выдаваться запрос на сохранение файла, но он может изменить значение по умолчанию
Отключить историю форм	DisableFormHistory	Отключает запоминание истории поиска и данных форм. Если политика находится в состоянии «Включено», Firefox не запоминает историю форм или поиска. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», Firefox будет помнить историю форм и поиска

Продолжение таблицы 36

Политика	Ключ	Описание
Блокировка редактора настроек (about:config)	BlockAboutConfig	Блокирует доступ к странице about:config. Если эта политика находится в состоянии «Включено», пользователь не может получить доступ к about:config. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь может получить доступ к about:config
Блокировка страницы управления профилями (about:profiles)	BlockAboutProfiles	Блокирует доступ к странице about:profiles. Если политика находится в состоянии «Включено», пользователь не может получить доступ к профилям about:profiles. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь может получить доступ к профилям about:profiles
Блокировка информации об устранении неполадок	BlockAboutSupport	Блокирует доступ к странице about:support. Если политика находится в состоянии «Включено», пользователь не может получить доступ к информации для устранения неполадок или about:support. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь может получить доступ к информации для устранения неполадок или about:support
Captive Portal (портал захвата)	CaptivePortal	Включает или отключает тест соединения (поддержку перехватывающего портала). Если политика находится в состоянии «Отключено», то поддержка captive portal отключена. Если политика находится в состоянии «Включено» или «Не сконфигурировано», то поддержка captive portal включена. П р и м е ч а н и е : Веб-браузер Mozilla Firefox при запуске проверяет, требует ли используемое сетевое соединение вход в систему. Во время теста Firefox пытается подключиться к `http://detectportal.firefox.com/success.txt`, чтобы проверить возможность соединения с этим адресом. Этот адрес также используется для проверки поддержки активного сетевого соединения IPv6. Отключение этой функциональности уменьшает количество автоматических подключений и может немного ускорить запуск веб-браузера
Отключить встроенную программу просмотра PDF (PDF.js)	DisableBuiltinPDFViewer	Отключает PDF.js, встроенный просмотрщик PDF в Firefox. Если политика находится в состоянии «Включено», файлы PDF не просматриваются в Firefox. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», файлы PDF просматриваются в Firefox

Продолжение таблицы 36

Политика	Ключ	Описание
Отключить команды обратной связи	DisableFeedbackCommands	Отключает команды отправки отзывов в меню «Справка» («Отправить отзыв…» и «Сообщить о поддельном сайте…»). Если политика находится в состоянии «Включено», пункты меню «Отправить отзыв…» и «Сообщить о поддельном сайте…» недоступны из меню «Справка». Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пункты меню «Отправить отзыв…» и «Сообщить о поддельном сайте…» доступны из меню «Справка»
Отключить снимки экрана Firefox	DisableFirefoxScreenshots	Отключает функцию Firefox Screenshots. Если политика находится в состоянии «Включено», снимки экрана Firefox недоступны. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», доступны скриншоты Firefox
Отключить учетные записи Firefox	DisableFirefoxAccounts	Отключает службы, основанные на Аккаунте Firefox, включая синхронизацию. Если политика находится в состоянии «Включено», учетные записи Firefox отключены, в том числе отключена синхронизация. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», доступны Аккаунты Firefox и синхронизация
Отключить исследования Firefox	DisableFirefoxStudies	Запрещает Firefox выполнять исследования. Если политика находится в состоянии «Включено», Firefox никогда не будет проводить исследования SHIELD или опросы Heartbeat. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь может включить исследования SHIELD или опросы Heartbeat. Для получения дополнительной информации см. `https://support.mozilla.org/en-US/kb/shield` и `https://wiki.mozilla.org/Firefox/Shield/Heartbeat`
Отключить кнопку «Забыть»	DisableForgetButton	Закрывает доступ к кнопке «Забыть». Если политика находится в состоянии «Включено», кнопка «Забыть о части истории веб-серфинга» недоступна. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», кнопка «Забыть о части истории веб-серфинга» доступна
Запретить показывать пароли в сохраненных логинах	DisablePasswordReveal	Не позволяет просматривать пароли у сохраненных логинов. Если политика находится в состоянии «Включено», пользователи не могут отображать пароли в сохраненных логинах.

Продолжение таблицы 36

Политика	Ключ	Описание
		Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователи могут отображать пароли в сохраненных логинах
Отключить Pocket	DisablePocket	Отключает сохранение страниц в Pocket. Если политика находится в состоянии «Включено», Pocket недоступен. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», Pocket доступен. П р и м е ч а н и е . Pocket – это специальный сервис для хранения различной информации, найденной в ходе веб-серфинга
Отключить импорт профиля	DisableProfileImport	Отключает команду меню для импорта данных из другого веб-браузера. Если политика находится в состоянии «Включено», опция «Импортировать данные из другого браузера…» в окне закладок недоступна. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», опция «Импортировать данные из другого браузера…» доступна
Отключить обновление профиля	DisableProfileRefresh	Отключает кнопку «Обновить Firefox» на странице about:support. Если политика находится в состоянии «Включено», кнопка «Обновить Firefox» будет недоступна на странице about:support. Если эта политика отключена или не настроена, кнопка «Обновить Firefox» доступна
Отключить безопасный режим	DisableSafeMode	Отключает функцию для перезапуска в безопасном режиме. Если политика находится в состоянии «Включено», пользователь не может перезапустить веб-браузер в безопасном режиме. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», безопасный режим разрешен
Не проверять веб-браузер по умолчанию	DontCheckDefaultBrowser	Отключает проверку веб-браузера по умолчанию при запуске. Если политика находится в состоянии «Включено», Firefox не проверяет, является ли он веб-браузером по умолчанию при запуске. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», Firefox при запуске проверяет, является ли он веб-браузером по умолчанию
Аппаратное ускорение	HardwareAcceleration	Отключает аппаратное ускорение. Если политика находится в состоянии «Отключено», аппаратное ускорение не может быть включено.

Продолжение таблицы 36

Политика	Ключ	Описание
		Если политика находится в состоянии «Включено» или «Не сконфигурировано», включено аппаратное ускорение
Основной (главный) пароль	PrimaryPassword	Требовать или не давать использовать мастер-пароль. Если политика находится в состоянии «Отключено», пользователи не могут создать основной пароль. Если политика находится в состоянии «Включено» или «Не сконфигурировано», пользователи могут создать основной пароль
Прогнозирование сети	NetworkPrediction	Включает или отключает прогнозирование сети (предварительная выборка DNS). Предварительная выборка DNS – это технология, используемая Firefox для ускорения загрузки новых веб-сайтов. Если политика находится в состоянии «Отключено», прогнозирование сети (предварительная выборка DNS) будет отключено. Если политика находится в состоянии «Включено» или «Не сконфигурировано», будет включено прогнозирование сети (предварительная выборка DNS)
Новая вкладка	NewTabPage	Включает или отключает страницу новой вкладки. Если эта политика находится в состоянии «Отключено», в новой вкладке будет загружена пустая страница. Если эта политика в состоянии «Включено» или «Не сконфигурировано», в новой вкладке будет загружена страница по умолчанию
Подсказки по поиску	SearchSuggestEnabled	Включает или отключает поисковые предложения. Если эта политика находится в состоянии «Отключено», поисковые подсказки будут отключены. Если эта политика в состоянии «Включено», поисковые подсказки будут включены. Если эта политика в состоянии «Не сконфигурировано», поисковые подсказки будут включены, но пользователь может отключить их
Показывать кнопку «Домашняя страница Firefox» на панели инструментов	ShowHomeButton	Включает кнопку «Домашняя страница Firefox» на панели инструментов. Если политика находится в состоянии «Отключено», кнопка «Домашняя страница Firefox» не будет отображаться на панели инструментов. Если политика находится в состоянии «Включено», кнопка «Домашняя страница Firefox» отображается на панели инструментов
Блокировка менеджера дополнений (about:addons)	BlockAboutAddons	Блокирует доступ к менеджеру дополнений (about:addons). Если политика находится в состоянии «Отключено» или «Не сконфигурировано» пользователь может получить доступ к менеджеру дополнений (about:addons).

Продолжение таблицы 36

Политика	Ключ	Описание
		Если политика находится в состоянии «Включено», пользователь не может получить доступ к менеджеру дополнений (about:addons)
URL для домашней страницы	Homepage	Устанавливает URL домашней страницы при старте веб-браузера и, если нужно, блокирует ее смену. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь может установить и изменить домашнюю страницу. Если политика находится в состоянии «Включено», можно установить домашнюю страницу по умолчанию, а также заблокировать возможность изменения домашней страницы
SPNEGO	SPNEGO	Включает аутентификацию через SPNEGO/Kerberos. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», никаким веб-сайтам не разрешается использовать аутентификацию SPNEGO с помощью веб-браузера. Если политика находится в состоянии «Включено», указанным веб-сайтам разрешается использовать аутентификацию SPNEGO в веб-браузере. Записи в списке имеют формат `altlinux.org` или `https://altlinux.org`
Не разрешать изменять настройки аутентификации	Locked	Блокирует настройки аутентификации от изменений пользователем. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь не может изменить параметры проверки подлинности. Если политика находится в состоянии «Включено», пользователь может изменить параметры проверки подлинности
Разрешить неполное доменное имя (Non FQDN)	Authentication AllowNonFQDN	Разрешить SPNEGO или NTLM для неполных доменных имен (Non FQDN). Если политика находится в состоянии «Отключено» или «Не сконфигурировано», NTLM и SPNEGO не будут включены для неполных доменных имен. Если политика находится в состоянии «Включено» (и флажки отмечены), SPNEGO или NTLM будут включены для неполных доменных имен (Non FQDN)
Не разрешать изменять настройки аутентификации	Authentication Locked	Блокирует настройки аутентификации от изменений пользователем. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь не может изменить параметры проверки подлинности. Если политика находится в состоянии «Включено» (и флажки отмечены), пользователь может изменить параметры проверки подлинности

Продолжение таблицы 36

Политика	Ключ	Описание
Расширения для установки	Extensions\Install	Задает список URL-адресов или собственных путей для устанавливаемых расширений. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», расширения не устанавливаются. Если политика находится в состоянии «Включено», можно указать список URL-адресов или путей расширений, которые будут устанавливаться при запуске Firefox. При каждом изменении этого списка политики будут переустанавливаться. URL политики нужно задавать в формате `*.xpi` (например, `https://addons.mozilla.org/firefox/downloads/file/3450175/adapter_rutoken_plugin-1.0.5.0.xpi`). Также можно указать путь на локальный каталог, в который, политикой копирования файлов (см.п. 9.2.5.5.5), скопировать расширение в формате `*.xpi`
Управление расширениями	ExtensionSettings	Это правило позволяет управлять всеми аспектами расширений. Политика сопоставляет идентификатор расширения с его конфигурацией. Если указан идентификатор расширения, конфигурация будет применяться только к указанному расширению. Конфигурация по умолчанию может быть установлена для специального идентификатора *****, который будет применяться ко всем расширениям, для которых не задана пользовательская конфигурация в этой политике. Чтобы получить идентификатор расширения, можно установить расширение и посмотреть идентификатор на странице about:support в разделе «Расширения».Если политика находится в состоянии «Отключено» или «Не сконфигурировано», расширения не будут управляться. Если политика находится в состоянии «Включено», можно использовать JSON для описания политики управления расширениями

Управление расширениями	ExtensionSettings	Пример JSON:
		`{`
		`  "*": {`
		`  "blocked_install_message": "Custom error message"`
		`  },`
		`  "adblockultimate@adblockultimate.net": {`
		`  "installation_mode": "force_installed",`
		`  "install_url": "file:///home/user/file.xpi"`
		`  },`
		`  "rutokenplugin@rutoken.ru": {`
		`  "installation_mode": "force_installed",`
		`  "install_url": "https://addons.mozilla.org/…/plugin.xpi"`
		`  }`
		`}`

Продолжение таблицы 36

Политика	Ключ	Описание
		Конфигурация для каждого расширения – это еще один словарь, который может содержать следующие поля: - installation_mode – режим установки расширения. Допустимые значения: а) allowed – разрешает установку расширения пользователем (поведение по умолчанию). Поле install_url не используется и будет автоматически определено на основе идентификатора; б) blocked – блокирует установку расширения и удаляет его, если оно уже установлено; в) force_installed – расширение устанавливается автоматически и не может быть удалено пользователем. Этот параметр недействителен для конфигурации по умолчанию и требует install_url; г) normal_installed – расширение устанавливается автоматически, но может быть отключено пользователем. Этот параметр недействителен для конфигурации по умолчанию и требует install_url; - install_url – сопоставляется с URL-адресом, указывающим, откуда Firefox может загрузить расширение (при force_installed или normal_installed). При установке из локальной файловой системы следует использовать URL-адрес file:///. При установке с сайта addons.mozilla.org можно использовать URL-адрес в виде `https://addons.mozilla.org/firefox/downloads/file/3450175/adapter_rutoken_plugin-1.0.5.0.xpi`; - install_sources – список источников, из которых разрешена установка расширений с использованием шаблонов соответствия URL. Этот параметр не нужен, если разрешена установка только определенных расширений по идентификатору. Данный параметр можно использовать только для конфигурации по умолчанию; - minimum_version_required – отключает расширения (в том числе установленные принудительно) более ранних версий, чем определено этим параметром. Формат строки версии аналогичен формату, который используется в манифесте расширения; - allowed_types – белый список разрешенных типов расширений/приложений, которые можно установить в Firefox. Значение представляет собой список строк (допустимые строки: «extension», «theme», «dictionary», «locale»). Этот параметр можно использовать только для конфигурации по умолчанию; - override_update_url – указывает, что для всех последующих обновлений расширения будет использоваться URL из поля update_url или update в политике ExtensionInstallForcelist.

Окончание таблицы 36

Политика	Ключ	Описание
		Если это политика не настроена или отключена, будет использоваться URL из манифеста расширения; - override_update_url – указывает, что для всех последующих обновлений расширения будет использоваться URL из поля update_url или update в политике ExtensionInstallForcelist. Если это политика не настроена или отключена, будет использоваться URL из манифеста расширения; - blocked_install_message – сообщение об ошибке, которое будет отображаться для пользователей, если им заблокирована установка расширения. Этот параметр можно использовать только для конфигурации по умолчанию; - restricted_domains – массив доменов, на которых нельзя запускать сценарии контента. Этот параметр можно использовать только для конфигурации по умолчанию; - updates_disabled – логическое значение, указывающее, следует ли отключать автоматические обновления для отдельного расширения; - default_area – указывает, где должен быть размещен значок расширения. Возможные значения: navbar и menupanel

9.2.5.4.11. Политика замыкания

Описание политики замыкания см. в п. 9.3.4.

Для настройки этой политики следует перейти в «Компьютер/Пользователь» → «Административные шаблоны» → «Система» → «Групповая политика» (рис. 300).

Щелкнуть левой кнопкой мыши на политике «Настройка режима обработки замыкания пользовательской групповой политики», откроется диалоговое окно настройки политики. Можно не задавать настройку политики, включить или отключить (рис. 301).

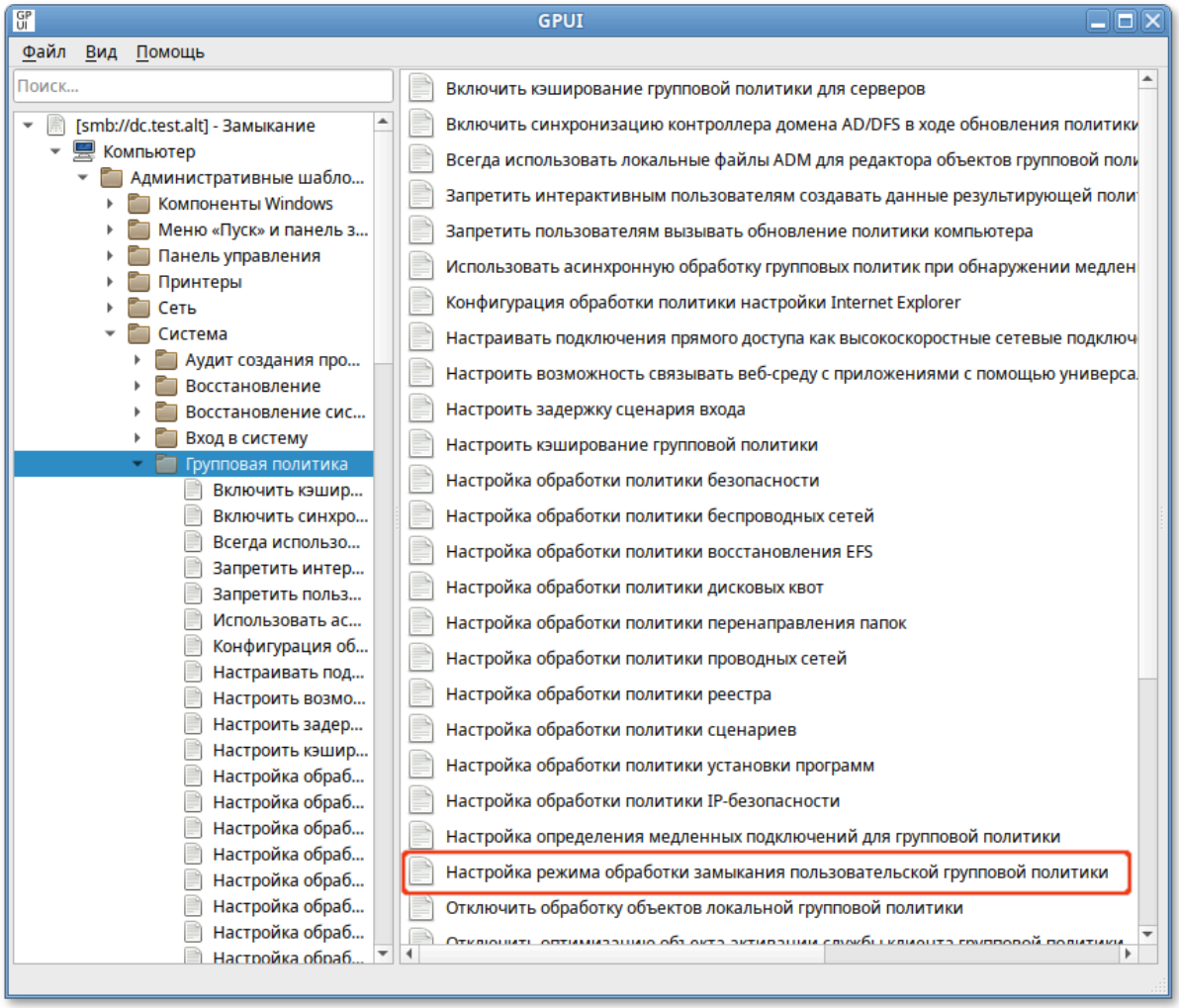


Рис. 300 – Политика замыкания

Если выбрать параметр «Включено», в разделе «Опции» в выпадающем списке можно выбрать режим:

- «Слияние» – указывает, что параметры политики пользователя, определенные в объектах групповой политики компьютера, и обычно применяемые параметры пользователя для этого пользователя должны быть объединены. Если возникает конфликт этих параметров политики, то параметры пользователя в объектах групповой политики компьютера имеют приоритет над обычными параметрами пользователя;
- «Замена» – указывает, что параметры политики пользователя, определенные в объектах групповой политики компьютера, заменяют параметры политики пользователя, обычно применяемые для этого пользователя.

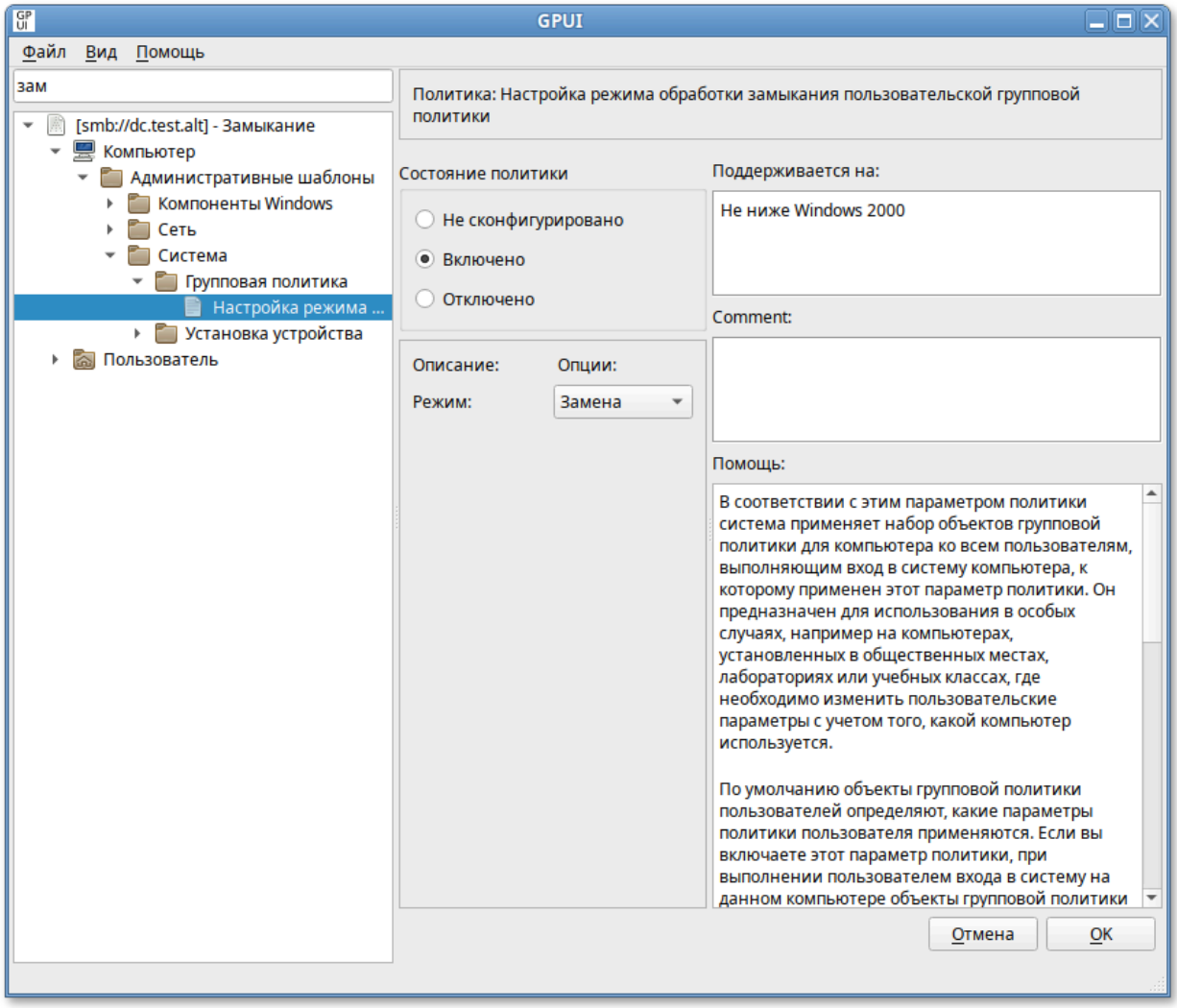


Рис. 301 – Политика «Настройка режима обработки замыкания пользовательской групповой политики»

Если выбрать параметр «Отключено» или не настраивать этот параметр политики, порядок применения параметров определяется объектами групповой политики для пользователей.

9.2.5.5. Редактирование предпочтений

9.2.5.5.1. Управление ярлыками

Групповая политика «Управление ярлыками» позволяет централизованно для компьютеров или пользователей:

- создавать ярлыки;
- удалять ярлыки;
- изменять свойства ярлыков.

Для настройки этой политики следует перейти в «Компьютер/Пользователь» → «Настройки» → «Настройки системы» → «Значки». В контекстном меню свободной области выбрать пункт «Новый» → «Значок» (рис. 302).

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 303).

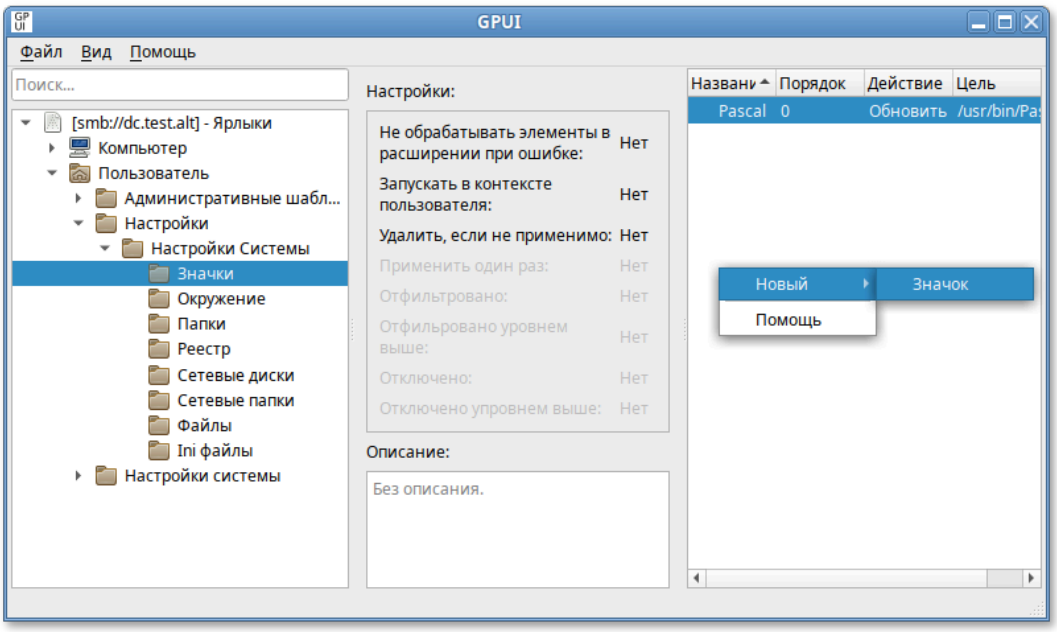


Рис. 302 – Редактирование предпочтений

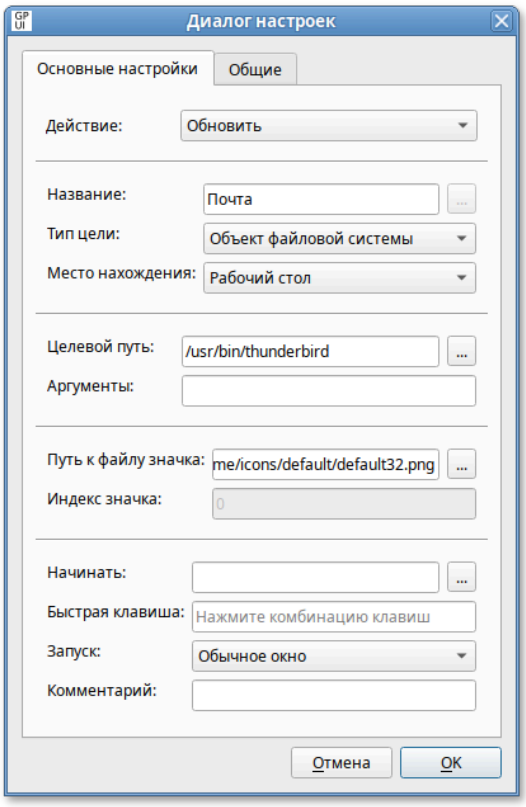


Рис. 303 – Диалоговое окно «Диалог настроек»

Опции доступные на вкладке «Основные настройки»:

1) «Действие» – действие, которое будет выполняться для ярлыка:
   - «Создать» – создание нового ярлыка;
   - «Удалить» – удаление ярлыка;
   - «Заменить» – удаление и повторное создание ярлыка. Если ярлык не существует, то это действие создает новый ярлык;
   - «Обновить» – изменение параметров существующего ярлыка. Если ярлык не существует, то это действие создает ярлык. Это действие отличается от «Заменить» тем, что не удаляет ярлык, а только обновляет параметры ярлыка, определенные в элементе настройки;
2) «Название» – отображаемое имя для ярлыка. При изменении или удалении ярлыка имя должно совпадать с именем существующего ярлыка;
3) «Тип цели» – тип конечного объекта, на который указывает ярлык (при изменении или удалении ярлыка выбранный тип объекта должен соответствовать существующему ярлыку):
   - «Объект файловой системы» – путь в ФС, например, файл, папка, диск, общий ресурс или компьютер;
   - «URL-адрес» – URL-адрес, например, веб-сайт;
   - «Объект оболочки» – объект, например, принтер, элемент рабочего стола или панели управления, файл, папка, общий ресурс, компьютер или сетевой ресурс;
4) «Место нахождения» – место, где ярлык должен отображаться на компьютерах, для которых применяется политика. Размещения, отличные от «Общее…», относятся к текущему пользователю. При изменении существующего ярлыка выбранное размещение должно совпадать с размещением существующего ярлыка. Если выбран пункт «Укажите полный путь», то место задается полным путем в поле «Название» (при этом можно использовать переменные, например, чтобы разместить ярлык с именем «Почта» в подпапке «Ярлыки» в «Program File», нужно ввести `%ProgramFilesDir%\Ярлыки\Почта`). Чтобы разместить ярлык в

подпапке для выбранного размещения из списка, следует указать `<название подпапки>\<имя ярлыка>` в поле «Название», например, чтобы разместить ярлык с именем «Почта» в подпапке «Ярлыки» в размещении «Рабочий стол», нужно ввести Ярлыки/Почта в поле «Название» и выбрать «Рабочий стол» в поле «Место нахождения» (рис. 304);

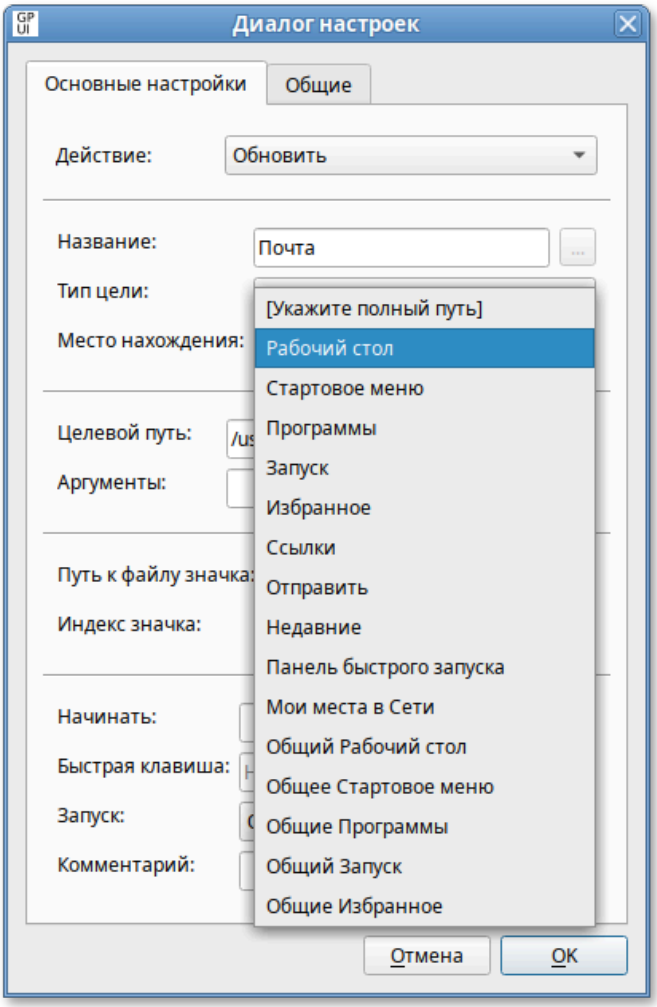


Рис. 304 – Диалог настроек

5) «Целевой путь» – локальный путь (с точки зрения клиента) для типа «Объект файловой системы», URL для типа «URL-адрес» или объект для типа «Объект оболочки». Если выбран тип цели «Объект файловой системы» или «URL-адрес», то это поле может принимать переменные. Это поле недоступно, если выбрано действие «Удалить»;
6) «Аргументы» – аргументы, которые будут использоваться при открытии целевого файла или папки. Это поле доступно только в том случае, если

выбран тип цели «Объект файловой системы», и выбрано действие «Создать», «Заменить» или «Обновить»;

7) «Путь к файлу значка» и «Индекс значка» – значок для ярлыка. Для указания значка, отличного от значка по умолчанию нужно выбрать значок или ввести полный путь к значку (с точки зрения клиента) и указать индекс значка. Поле «Путь к файлу значка» принимает переменные. Эти поля недоступны, если выбрано действие «Удалить»;
8) «Начинать» – рабочий каталог, содержащий файлы, которые требуются для конечного объекта. Это поле принимает переменные. Поле доступно в случае, если выбрано действие «Создать», «Заменить» или «Обновить»;
9) «Быстрая клавиша» – сочетание клавиш для запуска ярлыка. Чтобы назначить сочетание клавиш следует установить курсор в поле «Быстрая клавиша» и нажать комбинацию клавиш. Это поле недоступно, если выбрано действие «Удалить»;
10) «Запуск» – размер окна, в котором нужно открыть цель ярлыка. Поле доступно только в том случае, если выбран тип объекта «Объект файловой системы» или «Объект оболочки», и выбрано действие «Создать», «Заменить» или «Обновить»;
11) «Комментарий» – всплывающая подсказка, когда указатель мыши приостановлен на ярлыке. Поле принимает переменные. Поле доступно только в том случае, если выбран тип объекта «Объект файловой системы» или «Объект оболочки», и выбрано действие «Создать», «Заменить» или «Обновить».

⚠ Чтобы ярлыку назначались корректные права (для пользовательской политики), нужно установить отметку в пункте «Выполнять в контексте безопасности текущего пользователя» на вкладке «Общие».

Все настройки политики для ярлыков хранятся в файлах:

```
{GUID GPT}/Machine/Preferences/Shortcuts/Shortcuts.xml
{GUID GPT}/User/Preferences/Shortcuts/Shortcuts.xml
```

Пример файла `Shortcuts.xml`:

```
<?xml version="1.0" encoding="utf-8"?>
<Shortcuts clsid="{872ECB34-B2EC-401b-A585-D32574AA90EE}">
<Shortcut bypassErrors="0"
    changed="2022-11-17 11:07:40"
    clsid="{4F2F7C55-2790-433e-8127-0739D1CFA327}"
    desc=""
    image="0"
    name="Почта"
    removePolicy="0"
    status=""
    uid="{dfd45a36-4634-47d9-8a22-5f702fba21bc}"
    userContext="0">
<Properties
    action="U"
    arguments=""
    comment=""
    iconPath="/usr/lib64/thunderbird/chrome/icons/default/default32.png"
    pidl=""
    shortcutPath="%DesktopDir%\Почта"
    startIn=""
    targetPath="/usr/bin/thunderbird"
    targetType="FILESYSTEM"
    window=""/>
</Shortcut>
</Shortcuts>
```

9.2.5.5.2. Управление каталогами

Групповая политика «Управление каталогами» позволяет для всех пользователей заданной группы создавать унифицированную структуру каталогов.

Для настройки этой политики следует перейти в «Компьютер»/«Пользователь» → «Настройки» → «Настройки системы» → «Папки». В контекстном меню свободной области выбрать пункт «Новый» → «Папки» (рис. 305).

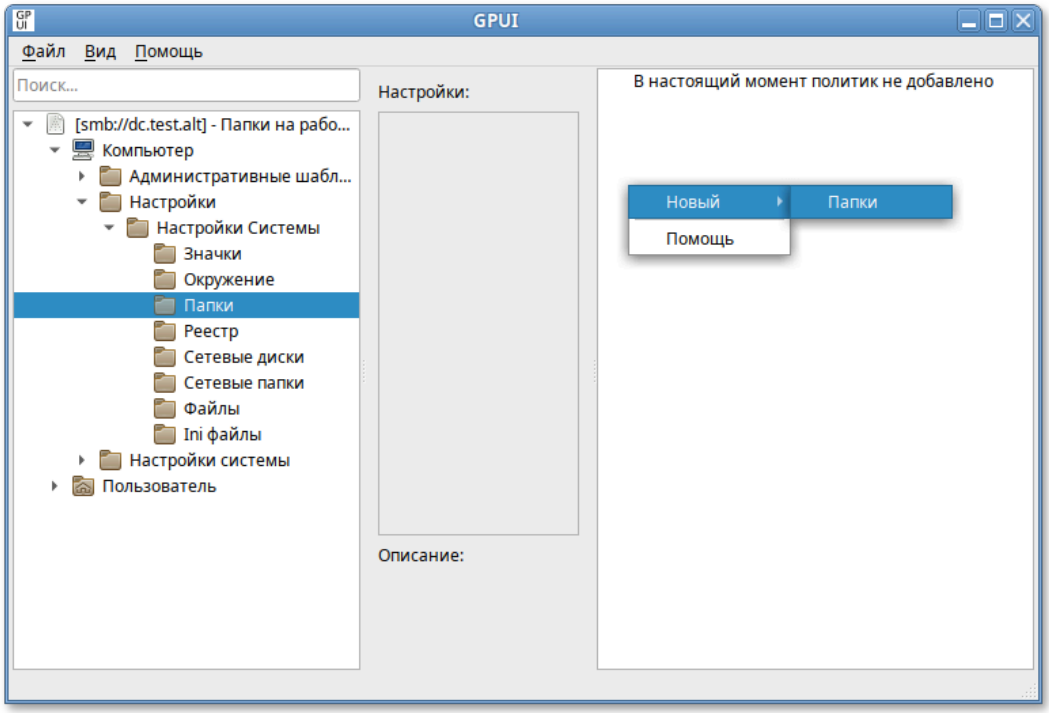


Рис. 305 – Управление каталогами

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 306).

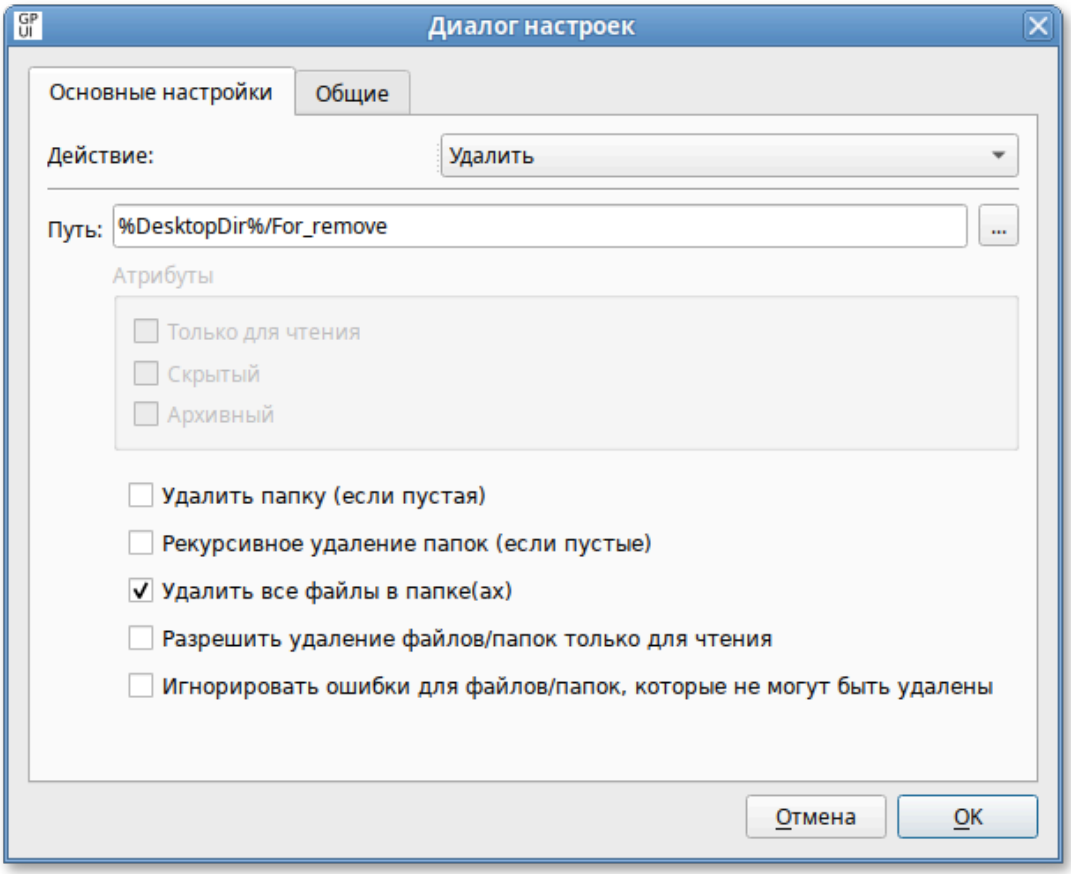


Рис. 306 – Диалог настроек

Опции доступные на вкладке «Основные настройки»:

1) «Действие» – действие, которое будет выполняться для папки:
   - «Создать» – создание новой папки;
   - «Удалить» – удаление папки;
   - «Заменить» – удаление и повторное создание папки. В результате выполнения действия «Заменить» содержимое существующей папки удаляется, и все существующие параметры папки перезаписываются. Если папка не существует, действие «Заменить» создает новую папку;
   - «Обновить» – изменение параметров существующей папки. Если папки не существует, то это действие создает новую папку. Это действие отличается от «Заменить» тем, что не удаляет папку, а только обновляет параметры;
2) «Путь» – путь к папке (с точки зрения клиента). Это поле может содержать переменные (не следует вводить кавычки и завершающую косую черту);
3) «Атрибуты» – атрибуты файловой системы для папки (недоступны для действия «Удалить»):
   - «Только для чтения»;
   - «Скрытый»;
   - «Архивный»;
4) следующие опции доступны только для действий «Заменить» и «Удалить»:
   - «Удалить папку (если пустая)» – если включена эта опция папка, указанная в поле «Путь», удаляется, если она пуста. Будет ли эта папка пустой, оценивается после того, как были обработаны опции «Удалить все файлы в папке(ах)» и «Рекурсивное удаление папок (если пустые)». При выборе действия «Удалить» эта опция включена по умолчанию и ее невозможно отключить;
   - «Рекурсивное удаление папок (если пустые)» – если включена эта опция, самый низкий уровень вложенных папок удаляется, если они пусты, повторяется для каждой родительской папки до достижения

папки, указанной в поле «Путь». Пустые подпапки оцениваются после того, как опция «Удалить все файлы в папке(ах)» была обработана;

- «Удалить все файлы в папке(ах)» – если включена эта опция, удаляются все файлы в папке, которые разрешено удалять. Если также включена опция «Рекурсивное удаление папок (если пустые)», то удаляются также все файлы, которые разрешено удалять во всех подпапках;
- «Разрешить удаление файлов/папок только для чтения» – если включена эта опция, атрибут «Только для чтения» отключается для удаляемых файлов и папок;
- «Игнорировать ошибки для файлов/папок, которые не могут быть удалены» – если включена эта опция, подавляются любые сообщения об ошибках, возникающие из-за невозможности удаления файлов или папок. Если эта опция не включена, возвращается ошибка, если совершается попытка удалить непустую папку, открытый файл, файл или папку, для которых пользователь не имеет разрешений или любой другой файл или папку, которые не могут быть удалены.

Примечание. Атрибуты «Архивный», «Скрытый» и «Только для чтения» применимы только для Windows систем.

Все настройки политики для управления каталогами хранятся в файлах:

```
{GUID GPT}/Machine/Preferences/Folders/Folders.xml
{GUID GPT}/User/Preferences/Folders/Folders.xml
```

Пример файла `Folders.xml`:

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<Folders clsid="{77CC39E7-3D16-4f8f-AF86-EC0BBEE2C861}">
  <Folder clsid="{07DA02F5-F9CD-4397-A550-4AE21B6B4BD3}"
        name="MyDir"
        status="MyDir"
        image="2"
        bypassErrors="1"
        changed="2020-10-27 11:49:19"
        uid="{57F41C87-4A65-4561-BFFF-4219149DCBF7}">
    <Properties
        action="U"
        path="%DesktopDir%\MyDir"
```

```
        readOnly="0"
        archive="1"
        hidden="0"/>
    </Folder>
  </Folders>
```

9.2.5.5.3. Управление INI-файлами

Групповая политика «Управление ini-файлами» позволяет:

- добавить свойство в файл параметров конфигурации (.ini);

- заменить свойство в INI-файле;

- удалить свойство из INI-файла;

- удалить раздел из INI-файла;

- удалить INI-файл.

В разделах INI-файлов используется следующий формат:

```
[sectionA]
var01=value01

[sectionB]
var01=value01
var02=value02
```

Для настройки этой политики следует перейти в «Компьютер»/«Пользователь» → «Настройки» → «Настройки системы» → «Ini файлы». В контекстном меню свободной области выбрать пункт «Новый» → «Ini файл» (рис. 307).

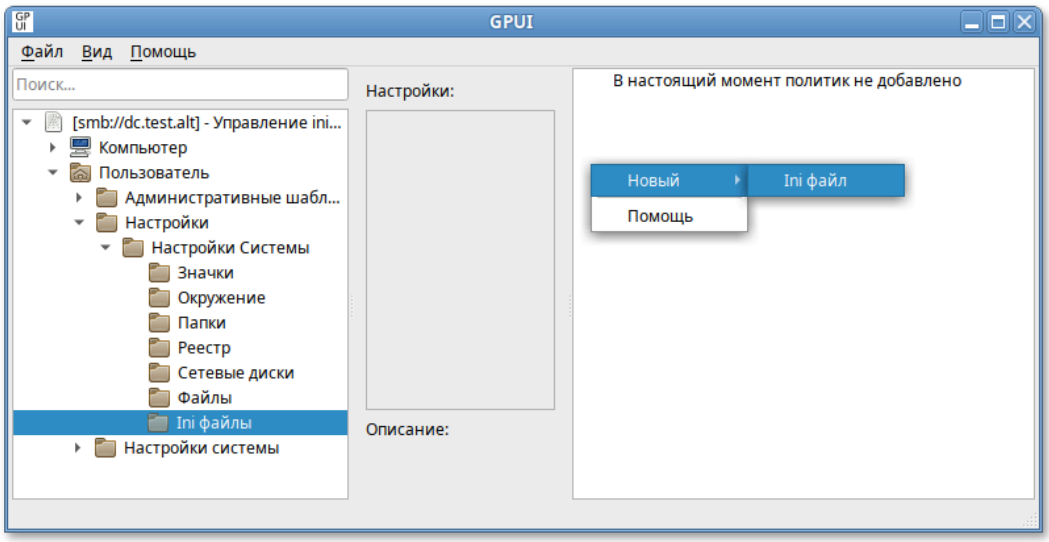


Рис. 307 – Управление INI-файлами

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 308).

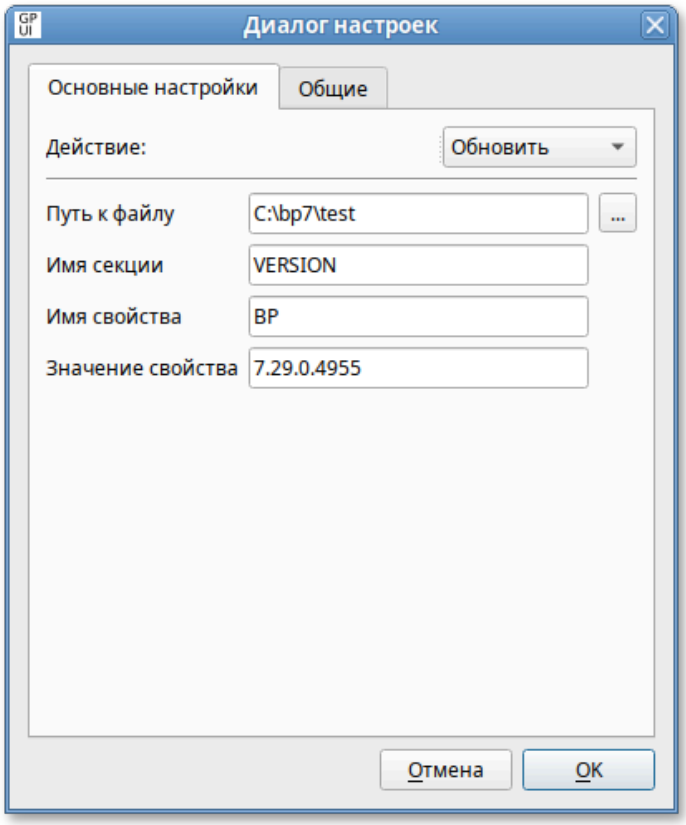


Рис. 308 – Диалог настроек

Опции доступные на вкладке «Основные настройки»:

1) «Действие» – действие, которое будет выполняться для INI-файла:
   - «Создать» – добавление свойства в INI-файл. Если файл не существует, он будет создан;
   - «Удалить» – удаление свойства или раздела из INI-файла (либо удаление INI-файла);
   - «Заменить» – удаление и повторное создание свойства в INI-файле (суммарный итог действия «Заменить» – переопределение свойства. Если свойство не существует, действие «Заменить» создаст его);
   - «Обновить» – удаление и повторное создание свойства в INI-файле (аналогично действию «Заменить»);
2) «Путь к файлу» – путь к INI-файлу с точки зрения клиента (путь не должен включать кавычки). Если файл и родительские папки не существуют, они будут созданы;

3) «Имя секции» – имя раздела в файле, свойство которого нужно настроить или удалить. Чтобы удалить INI-файл целиком, следует оставить это поле пустым;
4) «Имя свойства» – имя свойства, которое нужно настроить или удалить. Чтобы удалить целиком раздел файла или весь файл, следует оставить это поле пустым;
5) «Значение свойства» – значение свойства. Значения могут содержать символы кавычек, которые, однако, при чтении значений приложением или операционной системой обычно удаляются. Все значения воспринимаются как текст. Если данное поле оставлено пустым, свойству присваивается пустое значение, что воспринимается как отсутствие свойства. Этот параметр доступен, если выбрано действие «Создать», «Заменить» или «Обновить».

Политики управления INI-файлами относятся к экспериментальным, поэтому на машинах с ОС Альт СП где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 9.2.5.4.7).

Все настройки политики управления INI-файлами хранятся в файлах:

```
{GUID GPT}/Machine/Preferences/Inifiles/Inifiles.xml
{GUID GPT}/User/Preferences/Inifiles/Inifiles.xml
```

Пример файла `Inifiles.xml`:

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<IniFiles clsid="{694C651A-08F2-47fa-A427-34C4F62BA207}">
  <Ini changed="2022-11-21 09:13:44"
        clsid="{EEFACE84-D3D8-4680-8D4B-BF103E759448}"
        image="3"
        name="version.ini"
        status="version.ini"
        uid="{ADAA9BCF-C2EA-4004-980F-CEDA823E3B91}"
        bypassErrors="1">
    <Properties
        path="C:\tmp\version.ini"
        section=""
        value=""
        property="BP"
        action="D"/>
  </Ini>
</IniFiles>
```

9.2.5.5.4. Управление переменными среды

Групповая политика «Управление переменными среды» позволяет централизованно для компьютеров или пользователей:

1) создать постоянные пользовательские или системные переменные среды;

2) удалить переменные среды;

3) изменить переменные среды, например:

- изменить приглашение командной строки (системная переменная PROMPT для Windows или PS1 для Linux (BASH));
- изменить расположение папки временных файлов (системная переменная TEMP для Windows или TMPDIR для Linux);
- заменить значение всей переменной PATH;
- добавить сегменты в переменную PATH (разделенные точкой с запятой для Windows или двоеточием для Linux);
- удалить сегменты из переменной PATH.

Для настройки этой политики следует перейти в «Компьютер»/«Пользователь» → «Настройки» → «Настройки системы» → «Окружение». В контекстном меню свободной области выбрать пункт «Новый» → «Переменные окружения» (рис. 309).

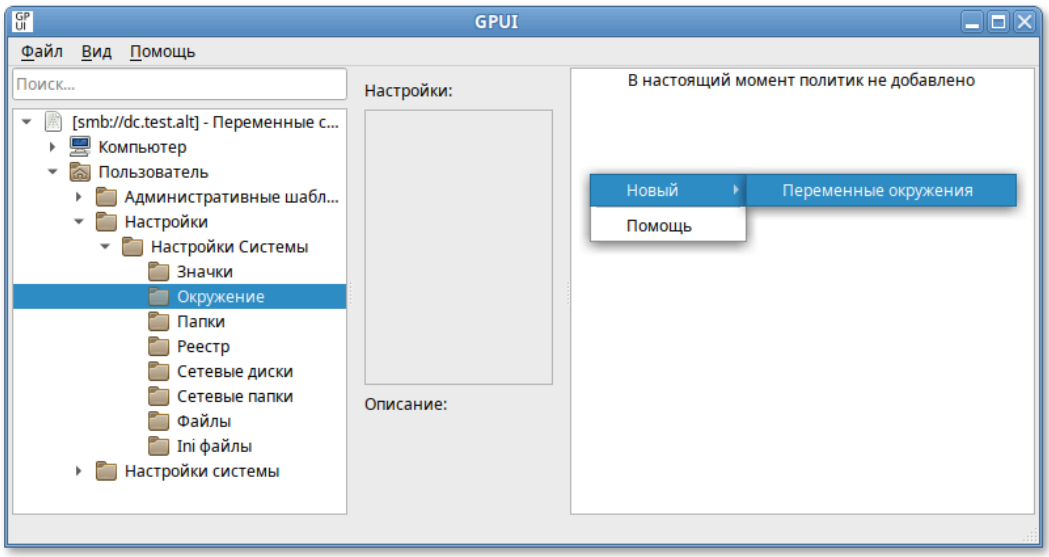


Рис. 309 –Управление переменными среды

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 310).

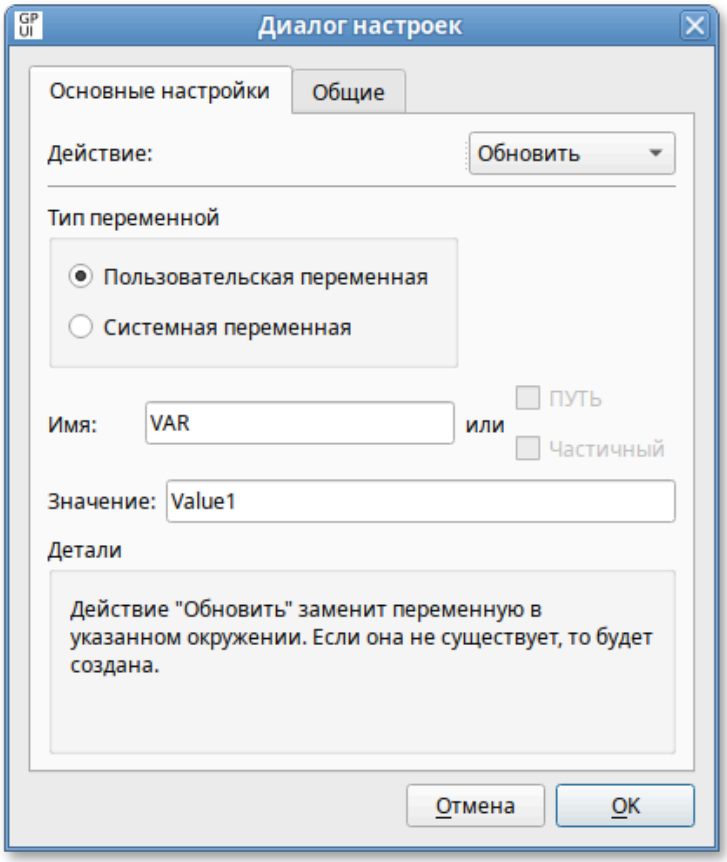


Рис. 310 – Диалог настроек

Опции доступные на вкладке «Основные настройки»:

1) «Действие» – действие, которое будет выполняться для переменной среды:

- «Создать» – создание новой переменной среды (если переменная среды с таким именем уже есть, например, создана локально, то ее значение изменено не будет);
- «Удалить» – удаление переменной среды;
- «Заменить» – удаление и повторное создание переменной среды (если переменная среды с таким именем не существует, то это действие создает новую переменную среды);
- «Обновить» – изменение параметров существующей переменной среды. Если переменная среды с таким именем не существует, то это действие создает новую переменную среды (фактически это действие полностью аналогично действию «Заменить»). Применение этого

действия к сегменту переменной PATH не имеет практического эффекта; в этом сегменте возможно только изменение регистра текста;

2) «Пользовательская переменная»:
   - параметр для переменной среды в разделе «Конфигурация пользователя» – влияние переменной среды будет для каждого пользователя независимым. Переменная среды хранится в разделе реестра HKEY_CURRENT_USER;
   - параметр для переменной среды в разделе «Конфигурация компьютера» – переменная среды будет влиять только на пользователя компьютера по умолчанию;
3) «Системная переменная» – переменная среды будет влиять на всех пользователей компьютера. Переменная среды будет храниться в реестре в разделе HKEY_LOCAL_MACHINE;
4) «Имя» – имя переменной среды, к которой применяется действие. Чтобы выбрать переменную PATH, следует оставить это поле пустым;
5) «Значение» – значение переменной среды. В это поле можно вводить переменные;
6) «PATH» – действие будет применяться к переменной PATH: можно создать/заменить значение переменной PATH или добавить/удалить сегмент значения переменной PATH. В поле «Имя» будет отмечено значение «PATH» и оно не будет доступно для редактирования. Эта опция доступна только в том случае, если выбран параметр «Системная переменная»;
7) «Значение» – значение переменной среды. В это поле можно вводить переменные.

Все настройки политики управления INI-файлами хранятся в файлах:

```
{GUID GPT}/Machine/Preferences/EnvironmentVariables/EnvironmentVariables.xml
{GUID GPT}/User/Preferences/EnvironmentVariables/EnvironmentVariables.xml
```

Пример файла `EnvironmentVariables.xml`:

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<EnvironmentVariables clsid="{BF141A63-327B-438a-B9BF-2C188F13B7AD}">
  <EnvironmentVariable clsid="{78570023-8373-4a19-BA80-2F150738EA19}"
        name="VAR"
        status="VAR = value_1"
        image="0"
        changed="2020-06-05 12:16:20"
        uid="{6738058D-5455-4D9A-9B84-78E87DDD18D7}"
        desc="environment variable example"
        bypassErrors="1">
    <Properties
        action="C"
        name="VAR"
        value="value_1"
        user="1"
        partial="0"/>
  </EnvironmentVariable>
  <EnvironmentVariable clsid="{78570023-8373-4a19-BA80-2F150738EA19}"
        name="PATH"
        status="PATH = value_2"
        image="2"
        changed="2020-06-05 12:16:48"
        uid="{15E854D6-C338-4AD2-BF8D-72292B364BA3}">
    <Properties
        action="U"
        name="PATH"
        value="value_2"
        user="0"
        partial="1"/>
  </EnvironmentVariable>
</EnvironmentVariables>
```

Примечание. Для того чтобы политики применились (под доменным пользователем) нужно перелогиниться. Проверить наличие переменных окружения можно, выполнив команду:

```
$ env |grep имя_переменной
```

Просмотреть все переменные, назначенные с помощью групповой политики, можно в файле `/etc/gpupdate/environment`:

```
TEMP DEFAULT="C:\tmp"
Var DEFAULT="Value1"
HTTPS_PROXY DEFAULT=https://10.0.66.52:3128
```

9.2.5.5.5. Управление файлами

Групповая политика «Файлы» позволяет проводить операции с файлами: копировать файлы в нужное расположение, удалять, заменять, обновлять атрибуты файлов.

Для компьютеров или пользователей эта политика предоставляет возможность:

- копировать файл (или несколько файлов из одного каталога) в новое место, а затем настроить атрибуты этих файлов;
- удалить файл (или несколько файлов в одном каталоге;
- удалить файл (или несколько файлов в одном каталоге) и заменить его копией файла из исходного каталога;
- изменить атрибуты файла (или нескольких файлов в одном каталоге);
- изменить атрибуты, заменить или удалить все файлы с определенным расширением в одном каталоге;
- изменить атрибуты, заменить или удалить все файлы в определенном каталоге.

Примечание. В групповой политике «Файлы» нет встроенной возможности скопировать целиком каталог со всем содержимым. Вместо этого можно использовать политику «Папки», которая позволяет создавать каталоги на компьютере, а для копирования файлов использовать групповую политику «Файлы».

Для настройки этой политики следует перейти в «Компьютер»/«Пользователь» → «Настройки» → «Настройки системы» → «Файлы». В контекстном меню свободной области выбрать пункт «Новый» → «Файл» (рис. 311).

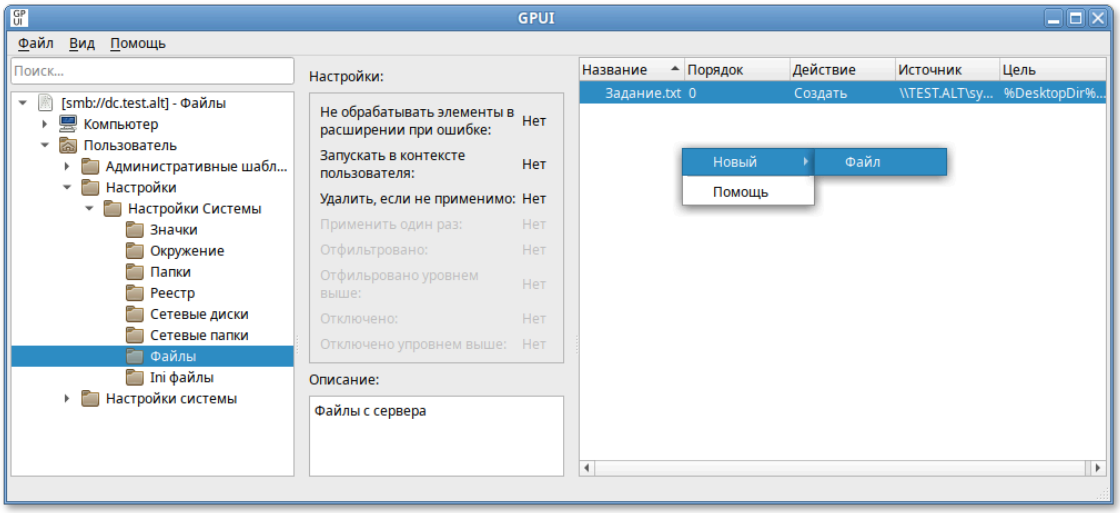


Рис. 311 – Управление файлами

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 312).

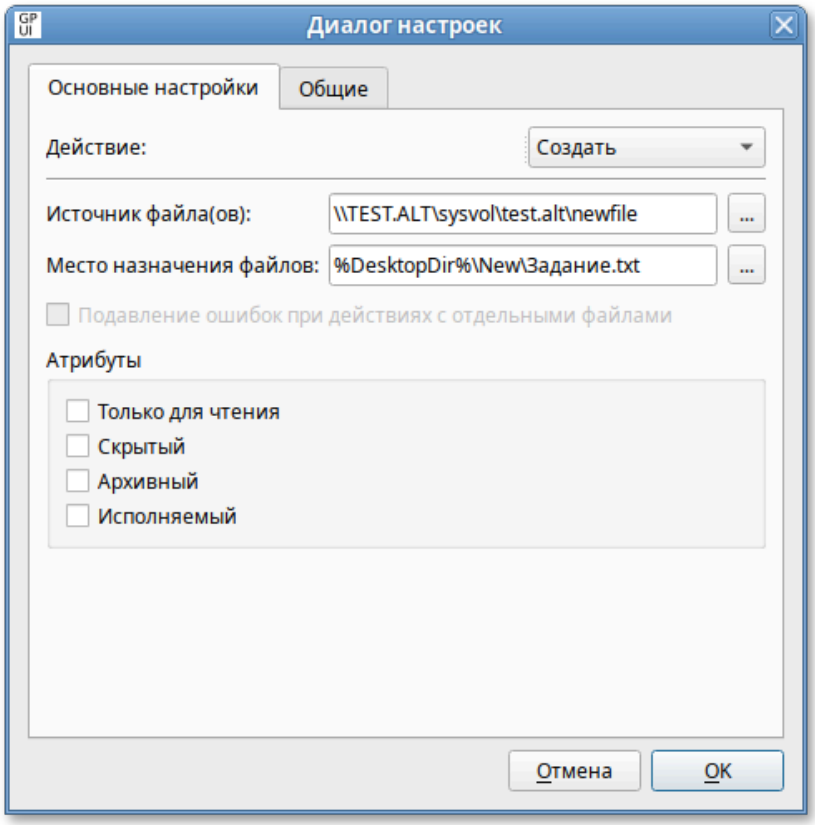


Рис. 312 – Диалог настроек

Опции доступные на вкладке «Основные настройки»:

1) «Действие» – действие, которое будет выполняться для файла(ов):

- «Создать» – копирование файла (или нескольких файлов из одного каталога) из исходного местоположения в конечное, если файл еще не существует в местоположении назначения, и настройка атрибутов этих файлов;
- «Удалить» – удаление файла (или нескольких файлов в одной папке);
- «Заменить» – удаление файла (или нескольких файлов в одной папке), замена его другим файлом и настройка атрибутов этих файлов. Конечным результатом действия «Заменить» будет перезапись файлов в местоположении назначения. Если файл не существует в месте назначения, действие «Заменить» копирует его из исходного местоположения в место назначения;

- «Обновить» – изменение параметров существующего файла (или нескольких файлов в одной папке). Это действие отличается от действия «Заменить» тем, что только обновляет атрибуты файла, определенные в элементе предпочтений. Все остальные атрибуты файла не изменяются. Если файл не существует, действие «Обновить» копирует его из исходного местоположения в место назначения;

2) «Источник файла(ов)» – местоположение (с точки зрения клиента), из которого требуется скопировать исходные файлы. Это местоположение может представлять полный путь UNC, или локальный путь, или сопоставленный диск со стороны клиента. Это поле может содержать переменные. Поле может содержать подстановочные знаки одного (?) или нескольких (*) символов, позволяя копировать или изменять несколько файлов (только для работы с файлами в ОС Windows). Поле недоступно для действия «Удалить».

Примечание. В настоящее время в ОС Альт можно использовать подстановочный знак (*) только для копирования всех файлов из папки (рис. 313).

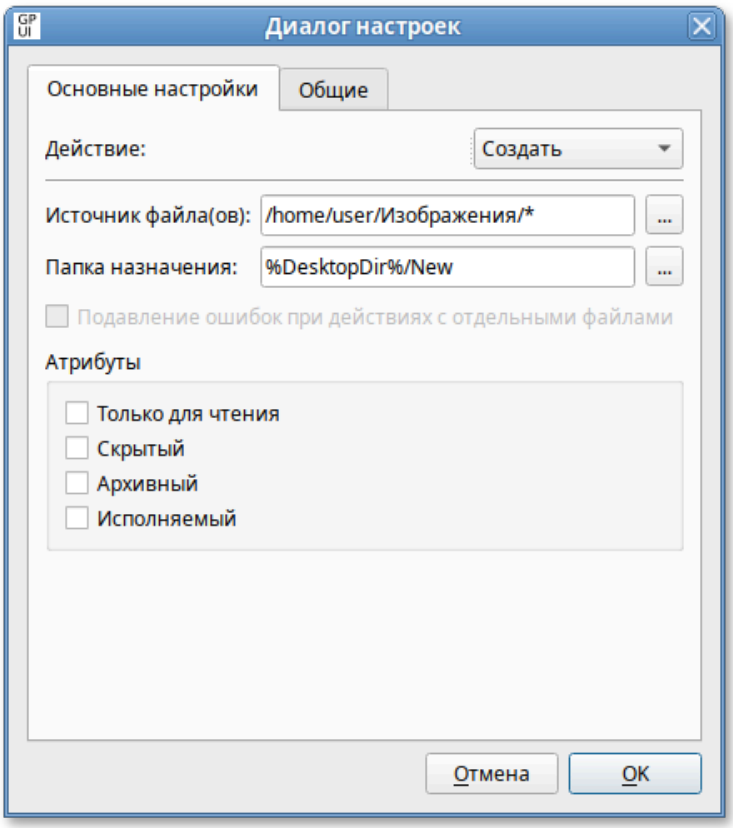


Рис. 313 – Копирование всех файлов из папки

3) «Место назначения файлов» – местоположение папки (с точки зрения клиента), в которую требуется скопировать файлы, или местоположение файлов, которые требуется изменить. Это местоположение может представлять полный путь UNC, или локальный путь, или сопоставленный диск со стороны клиента. Родительские папки создаются по мере нужности. Нужно включить имя файла, которое затем можно будет изменить, указав другое имя в поле Исходные файлы. Это поле может содержать переменные. Этот параметр доступен, если выбрано действие «Создать», «Заменить» или «Обновить», а поле «Источник файла(ов)» не содержит подстановочные знаки;
4) «Папка назначения» – место назначения копирования файла или местоположение файла (с точки зрения клиента), который требуется изменить. Это местоположение может представлять полный путь UNC, или локальный путь, или сопоставленный диск со стороны клиента. Родительские папки создаются по мере нужности. Это поле может содержать переменные. Этот параметр доступен, если выбрано действие «Создать», «Заменить» или «Обновить», а поле «Источник файла(ов)» включает подстановочные знаки;
5) «Удалить файл(ы)» – путь к файлу (с точки зрения клиента), который требуется удалить. Чтобы удалить несколько файлов из одной папки нужно включить в имя файла подстановочные знаки одного (?) или нескольких (*) символов (только для удаления файлов в ОС Windows). Этот параметр доступен, только если выбрано действие «Удалить» (рис. 314).

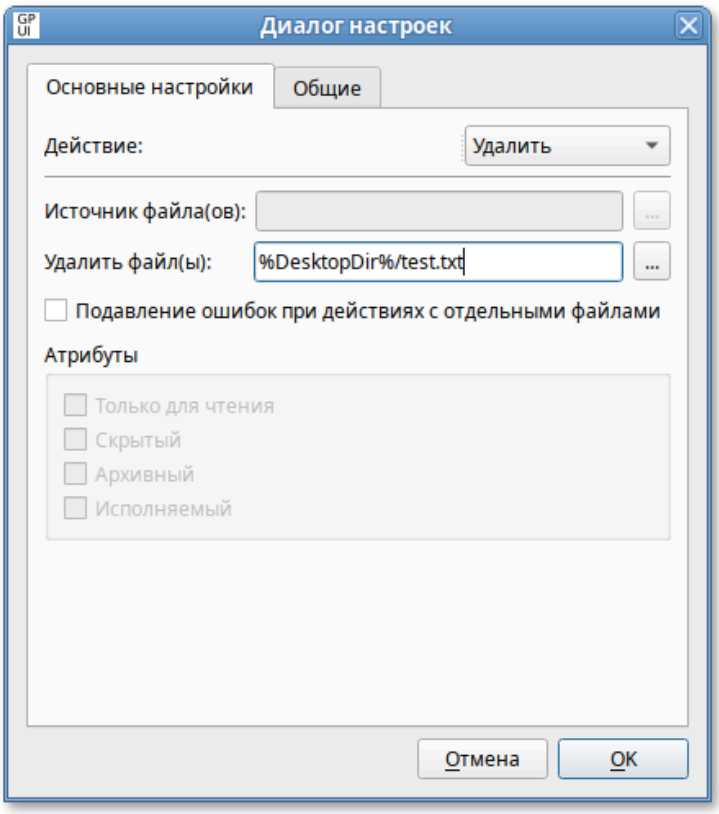


Рис. 314 – Путь к файлу, который необходимо удалить

6) «Подавление ошибок при действиях с отдельными файлами» – разрешить передачу одного или нескольких файлов даже в случае сбоя передачи отдельных файлов. Не отображаются только ошибки, связанные с попыткой замены, удаления или настройки атрибутов файла. Такие ошибки могут быть вызваны тем, что файл используется, был отказ в доступе или исходный файл не найден. Если этот параметр включен, такие ошибки могут быть обнаружены только в файле трассировки. Этот параметр отличается от параметра пропуска ошибок предпочтений по умолчанию, который можно изменить на вкладке «Общее»;
7) «Атрибуты» – атрибуты файловой системы для папки (недоступны для действия «Удалить»):
   - «Только для чтения»;
   - «Скрытый»;
   - «Архивный»;
   - «Исполняемый».

П р и м е ч а н и е . Атрибуты «Архивный», «Скрытый» и «Только для чтения» применимы только для Windows систем.

Политики управления файлами относятся к экспериментальным, поэтому на машинах с ОС Альт СП где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 9.2.5.4.7).

Опционально можно включить политику «Настройка механизма копирования файлов». Данная политика конфигурирует механизм «копирования файлов», формируя список суффиксов (расширений), идентифицирующих файл как исполняемый, (например, .sh) и список целевых путей копирования.

Для включения политики «Настройка механизма копирования файлов» следует в разделе «Компьютер» → «Административные шаблоны» → «Система ALT» → «Групповые политики» выбрать пункт «Настройка механизма копирования файлов». В открывшемся окне установить отметку в поле «Включено» (рис. 315).

Для задания списка суффиксов (расширений), идентифицирующих файл как исполняемый, в поле «Список суффиксов файлов» нажать кнопку «Редактировать» и в открывшемся окне ввести список суффиксов, по одному на каждой строке (рис. 316).

Для задания списка целевых путей копирования в поле «Список путей копирования» нажать кнопку «Редактировать» и в открывшемся окне ввести список путей, по одному на каждой строке (рис. 317).

В результате применения данной политики при копировании файлов с указанными суффиксами в назначенные пути, этим файлам будет задано право на выполнение (`chmod +x`).

Все настройки политики управления файлами хранятся в файлах:

```
{GUID GPT}/Machine/Preferences/Files/Files.xml
{GUID GPT}/User/Preferences/Files/Files.xml
```

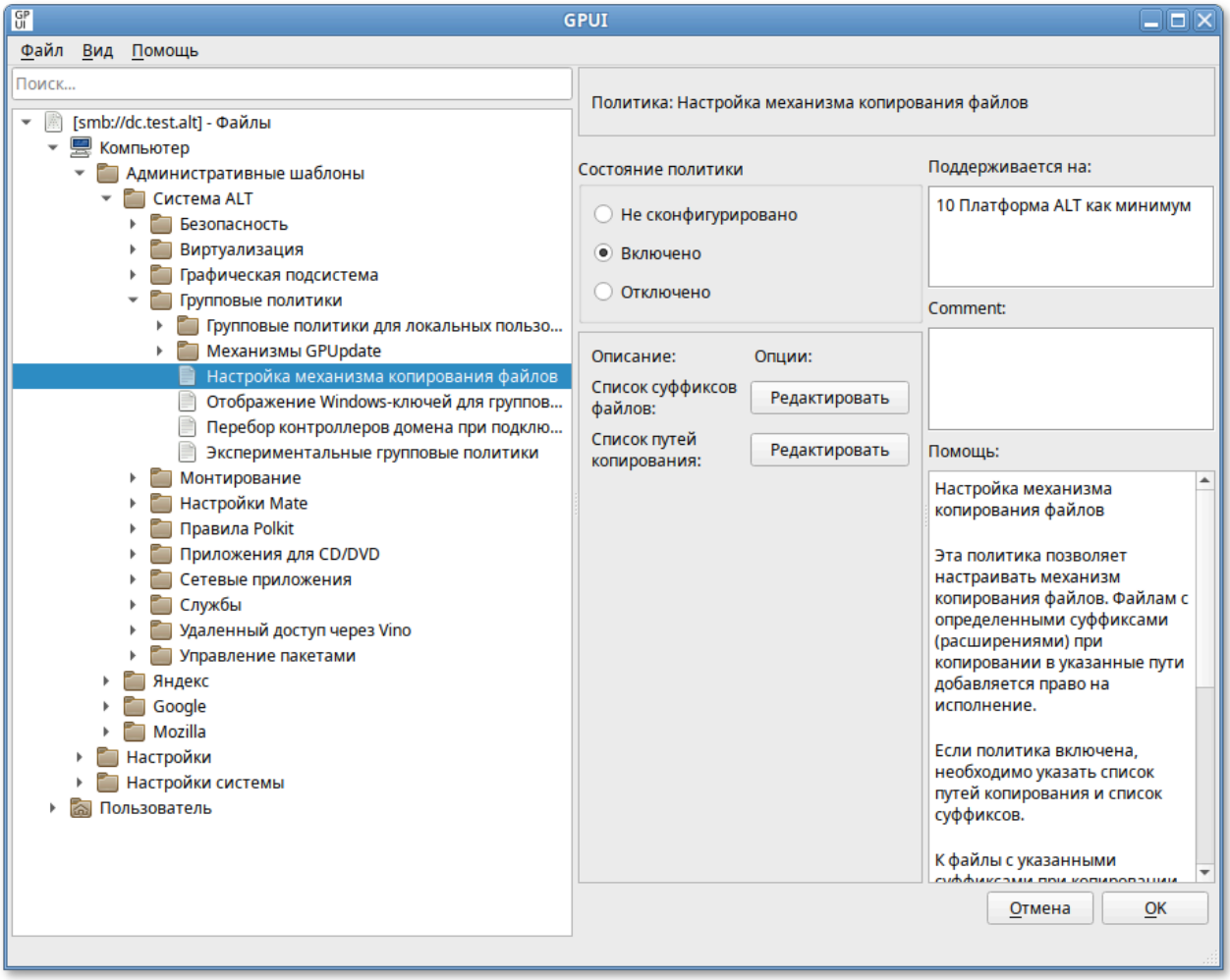


Рис. 315 – Политика «Настройка механизма копирования файлов»

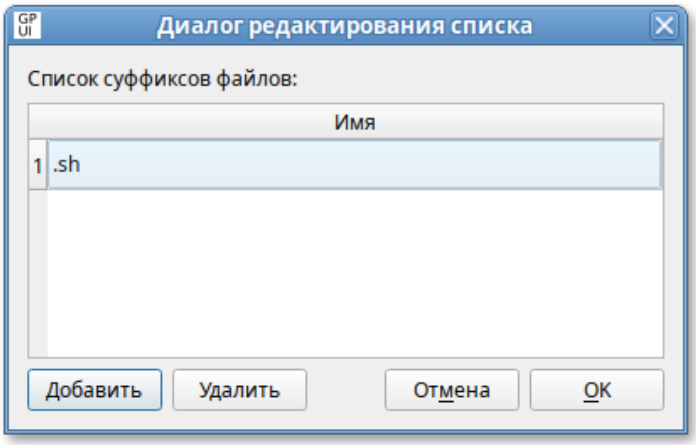


Рис. 316 – Поле «Список суффиксов файлов»

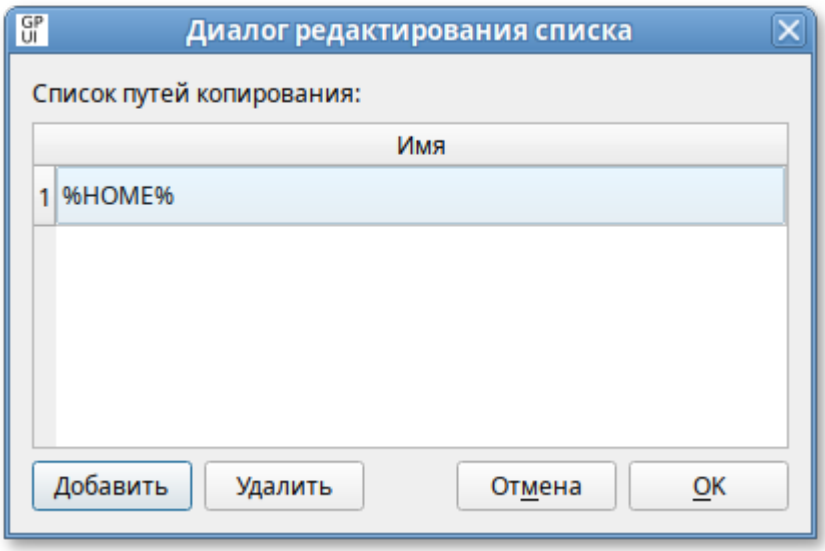


Рис. 317 – Поле «Список путей копирования»

Пример файла `Files.xml`:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<Files clsid="{215B2E53-57CE-475c-80FE-9EEC14635851}">
  <File bypassErrors="0"
        changed="2023-08-20 13:18:25"
        clsid="{50BE44C8-567A-4ed1-B1D0-9234FE1F38AF}"
        desc="Файл с сервера"
        image="0"
        name="Задание.txt"
        removePolicy="0"
        status=""
        uid="{cd0d3cba-8698-4612-9c76-5e21da62cc48}"
        userContext="0">
    <Properties
        action="C"
        archive="0"
        executable="0"
        fromPath="\\TEST.ALT\sysvol\test.alt\newfile"
        hidden="0"
        readOnly="0"
        suppress="0"
        targetPath="%DesktopDir%\New\Задание.txt"/>
  </File>
</Files>
```

9.2.5.5.6. Управление общими каталогами

Групповая политика «Управление общими каталогами» позволяет:

1) создать общие ресурсы и настроить их свойства;
2) изменить путь к папке общего ресурса путем замены ресурса;
3) удалить (вывести из общего доступа) или изменить лимит пользователей, функцию перечисления на основе доступа и комментарий для следующих объектов:
   - общий ресурс;
   - все общие ресурсы, кроме скрытых;
   - все скрытые ресурсы, кроме административных общих ресурсов с присвоением буквы диска;
   - все административные общие ресурсы с присвоением буквы диска;
   - все общие ресурсы.

Примечание. Для создания общего сетевого ресурса, папка, используемая при их создании, должна существовать на всех компьютерах, к которым применяется объект групповой политики. Вместе с удалением сетевого ресурса удаляется ссылка на папку, но не сама папка и ее содержимое.

Примечание. Для поддержки общих сетевых ресурсов с помощью политик на клиенте должны быть выполнены следующие условия:

- установлен пакет samba-usershares;
- control smb-conf-usershares установлен в enabled;
- в файле `/etc/samba/smb.conf` в секции `[global]` подключен файл `/etc/samba/usershares.conf` (`include = /etc/samba/usershares.conf`).

Примечание. Для создания или удаления папок с помощью групповой политики можно использовать предпочтение «Папки».

Для настройки этой политики следует перейти в «Компьютер»/«Пользователь» → «Настройки» → «Настройки системы» → «Сетевые папки». В контекстном меню свободной области выбрать пункт «Новый» → «Сетевая папка» (рис. 318).

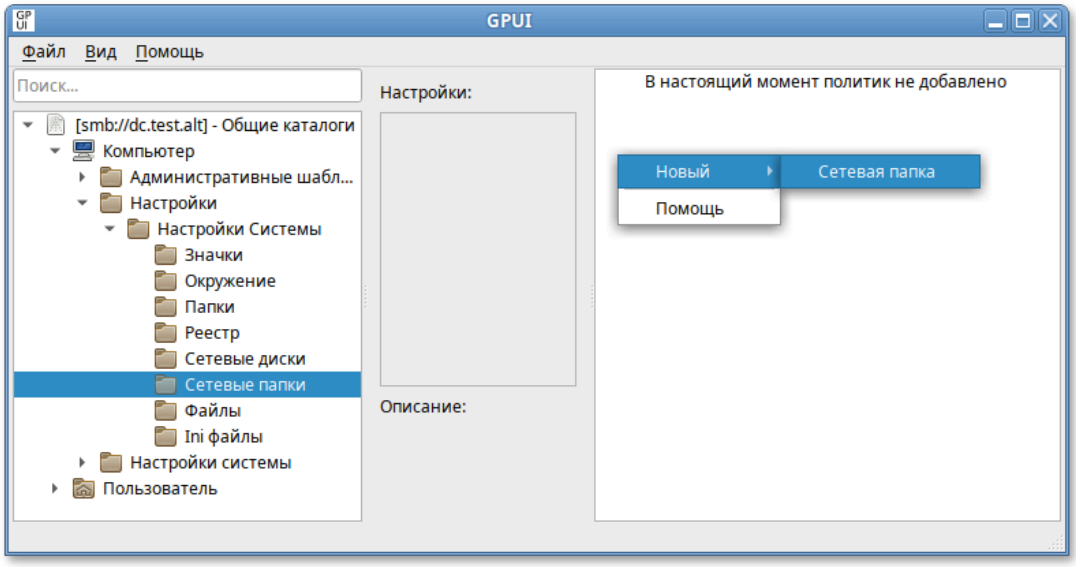


Рис. 318 – Управление общими каталогами

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 319).

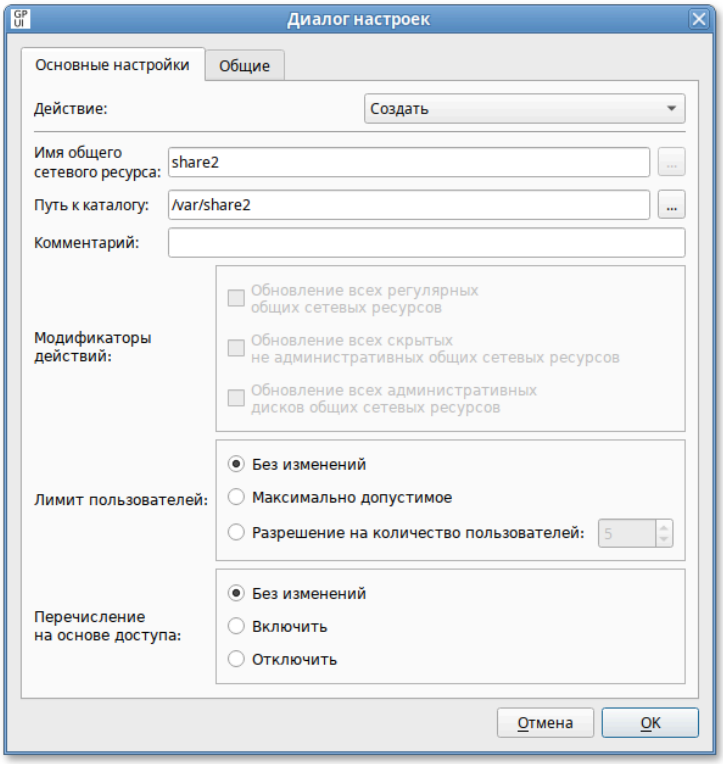


Рис. 319 – Диалог настроек

Опции доступные на вкладке «Основные настройки»:

1) «Действие» – действие, которое будет выполняться для общего сетевого ресурса:
   - «Создать» – создание нового сетевого ресурса;
   - «Удалить» – удаление общего ресурса;
   - «Заменить» – удаление и повторное создание сетевого ресурса. Суммарный итог действия «Заменить» – переопределение всех существующих параметров, связанных с общим ресурсом. Если сетевого ресурса не существует, то это действие создает новый сетевой ресурс;
   - «Обновить» – изменение параметров существующего сетевого ресурса. Если сетевого ресурса не существует, то это действие создает сетевой ресурс. Это действие отличается от «Заменить» тем, что не удаляет сетевой ресурс, а только обновляет параметры сетевого ресурса, определенные в элементе настройки;
2) «Имя общего сетевого ресурса» – имя общего ресурса. В этом поле можно указывать переменные;
3) «Путь к каталогу» – путь к существующей папке, на которую будет указывать общий ресурс. В этом поле можно указывать переменные;
4) «Комментарий» – текст для отображения в поле «Примечание» общего ресурса. Если выбрано действие «Обновить», общий ресурс уже существует и данное поле оставлено пустым, существующий комментарий будет оставлен без изменений. В этом поле можно указывать переменные. Этот параметр доступен, если выбрано действие «Создать», «Заменить» или «Обновить»;
5) «Модификаторы действий» – изменять и удалять общие ресурсы конкретного типа можно не только индивидуально, но и все вместе. Эти параметры доступны, если выбранное действие – «Обновить» или «Удалить»:

- «Обновление всех регулярных общих сетевых ресурсов» – изменение или удаление всех общих ресурсов, которые не являются скрытыми (с именами, оканчивающимися на $) или специальными (SYSVOL или NETLOGON);
- «Обновление всех скрытых не административных общих сетевых ресурсов» – изменение или удаление всех скрытых общих ресурсов, за исключением административных общих ресурсов с буквенным обозначением дисков, ADMIN$, FAX$, IPC$ и PRINT$;
- «Обновление всех административных дисков общих сетевых ресурсов» – изменение или удаление всех административных общих ресурсов с буквенным обозначением дисков (в их именах после буквы диска следует $);

6) «Лимит пользователей» – настройка числа пользователей, которым можно одновременно подключаться к общему ресурсу:
   - «Без изменений» – не изменять допустимое число пользователей при обновлении общего ресурса (если этот параметр выбран при создании или замене общего ресурса, число пользователей будет настроено на максимально допустимое);
   - «Максимально допустимое» – неограниченное число пользователей;
   - «Разрешение на количество пользователей» – ограничить число пользователей (следует ввести допустимый максимум пользователей);
7) «Перечисление на основе доступа» – настройка видимости папок общего ресурса:
   - «Без изменений» – не изменять видимость папок общего ресурса при обновлении общего ресурса;
   - «Включить» – сделать папки общего ресурса видимыми только при наличии доступа на чтение;
   - «Отключить» – сделать папки общего ресурса видимыми для всех пользователей.

Политики управления общими каталогами относятся к экспериментальным, поэтому на машинах с ОС «Альт» где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 9.2.5.4.7).

Все настройки политики управления файлами хранятся в файлах:

```
{GUID GPT}/Machine/Preferences/NetworkShares/NetworkShares.xml
{GUID GPT}/User/Preferences/NetworkShares/NetworkShares.xml
```

Пример файла `NetworkShares.xml`:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<NetworkShareSettings clsid="{520870D8-A6E7-47e8-A8D8-E6A4E76EAEC2}">
  <NetShare changed="2022-11-21 13:03:10"
        clsid="{2888C5E7-94FC-4739-90AA-2C1536D68BC0}"
        image="0"
        name="share2"
        status=""
        uid="{cd0d3cba-8698-4612-9c76-5e21da62cc48}"
        userContext="0"
        removePolicy="0">
    <Properties
        action="C"
        name="share2"
        path="/var/share2"
        comment=""
        limitUsers="NO_CHANGE"
        abe="NO_CHANGE"/>
  </NetShare>
</NetworkShareSettings>
```

9.2.5.5.7. Подключение сетевых дисков

Групповая политика «Подключение сетевых дисков» позволяет осуществлять доступ к сетевым общим каталогам как к каталогам в локальной файловой системе. Политика служит для создания, замены, обновления и удаления сопоставленных дисков и их свойств.

Точки монтирования для отображения общих ресурсов на машинах ОС Альт СП:

- `/media/gpupdate/drives.system` – для системных ресурсов;
- `/media/gpupdate/.drives.system` – для скрытых системных ресурсов;
- `/run/media/USERNAME/drives` – для общих ресурсов пользователя;

- `/run/media/USERNAME/.drives` – для скрытых общих ресурсов пользователя.

Для настройки этой политики следует перейти в «Компьютер»/«Пользователь» → «Настройки» → «Настройки системы» → «Сетевые диски». В контекстном меню свободной области выбрать пункт «Новый» → «Сетевой диск» (рис. 320).

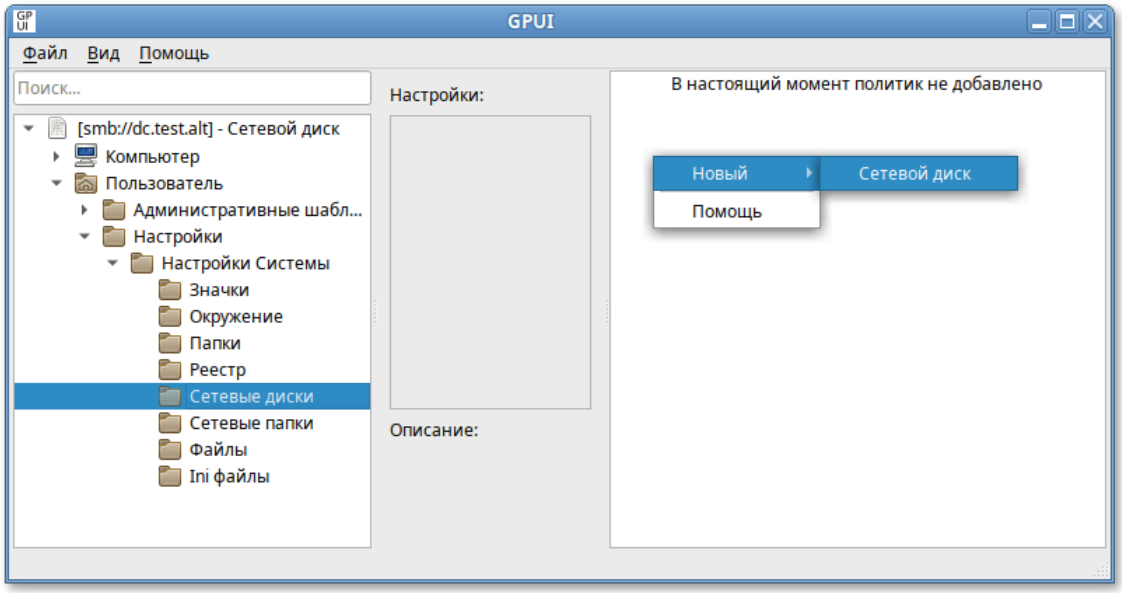


Рис. 320 – Подключение сетевых дисков

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 321).

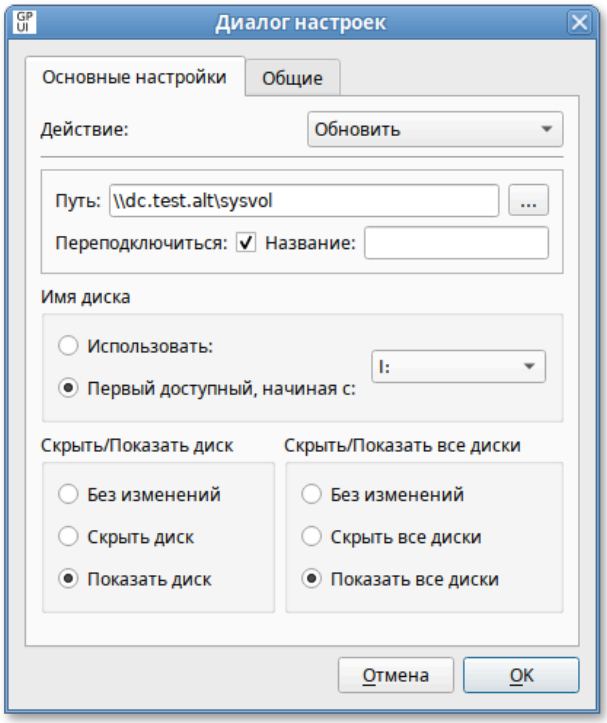


Рис. 321 – Диалог настроек

Опции доступные на вкладке «Основные настройки»:

1) «Действие» – поведение элемента настройки зависит от выбранного действия и от того, существует ли уже выбранная буква диска:
   - «Создать» – создание нового сетевого диска;
   - «Удалить» – удаление сетевого диска. Нельзя удалить локальный диск рабочей станции (жесткий диск, CD-Drive);
   - «Заменить» – удаление и повторное создание сетевого диска. Если диск до этого не был до создан, то будет создан новый диск. Нельзя заменить локальный диск рабочей станции (жесткий диск, CD-Drive);
   - «Обновить» – изменение параметров существующего сетевого диска или создание нового, если диска с заданной буквой не существует. Это действие отличается от «Заменить» тем, что оно не удаляет диск, а только обновляет настройки (кроме пути к общей папке и буквы);
2) «Путь» – путь к общей папке или диску, который нужно отобразить (полный UNC-путь к сетевому общему ресурсу например, `\\server\sharename`, `\\server\hiddenshare$` или

`\\server\sharename\foldername`). Это поле может содержать переменные. Чтобы изменить существующий сетевой диск (определяемый по букве диска), следует оставить это поле пустым;

3) «Переподключиться» – сохранять подключенный диск в настройках пользователя и повторно подключать его при каждом входе в систему;
4) «Название» – пользовательское имя для диска (можно оставить это поле пустым);

Примечание. Название должно представлять собой одно слово, состоящее только из латинских букв, цифр и символа подчеркивания, иначе монтирование не произойдет.

5) «Имя диска» – буква, на которую будет назначен диск:
   - чтобы назначить сетевому диску первую доступную букву диска, следует выбрать «Первый доступный, начиная с», а затем выбрать букву диска, с которой начинать проверку доступности букв;
   - чтобы назначить сетевому диску определенную букву, следует выбрать «Использовать», а затем выбрать букву диска (если рабочая станция уже использует выбранную здесь букву, сопоставление дисков групповой политики завершится неудачно);
   - чтобы изменить существующее сопоставление диска (определяемое буквой диска), следует выбрать «Использовать», а затем выбрать букву диска;
   - чтобы удалить все сопоставления дисков, начиная с определенной буквы, следует выбрать «Удалить, начиная с», а затем выбрать букву диска, с которой следует начать удаление сопоставлений дисков. Физические диски пропускаются без ошибок. Данный параметр доступен только при выбранном действии «Удалить»;
   - чтобы удалить определенный сопоставленный диск, следует выбрать «Удалить», а затем выбрать букву диска. Данный параметр доступен только при выбранном действии «Удалить»;

6) параметры «Скрыть»/«Показать» – настройка отображения сопоставленного диска (параметры «Скрыть»/ «Показать диск» имеют приоритет над параметрами «Скрыть»/«Показать все диски»):
   - «Без изменений» – оставить отображение сопоставленного диска неизменным;
   - «Скрыть диск» – скрыть диск в окне файлового менеджера;
   - «Показать диск» – отобразить диск в окне файлового менеджера.

Политики подключения сетевых дисков относятся к экспериментальным, поэтому на машинах с ОС Альт СП где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 9.2.5.4.7).

Если необходимо, можно включить отображение ссылок (symlink) на соответствующий сетевой ресурс в домашнем каталоге пользователя (чтобы можно было очевидно наблюдать смонтированные ресурсы). Для этого следует включить политики монтирования «Отображение сетевых дисков пользователя в домашнем каталоге» и/или «Отображение сетевых дисков машины в домашнем каталоге». Политики монтирования находятся в разделе «Пользователь» → «Административные шаблоны» → «Система ALT» → «Монтирование» (рис. 322).

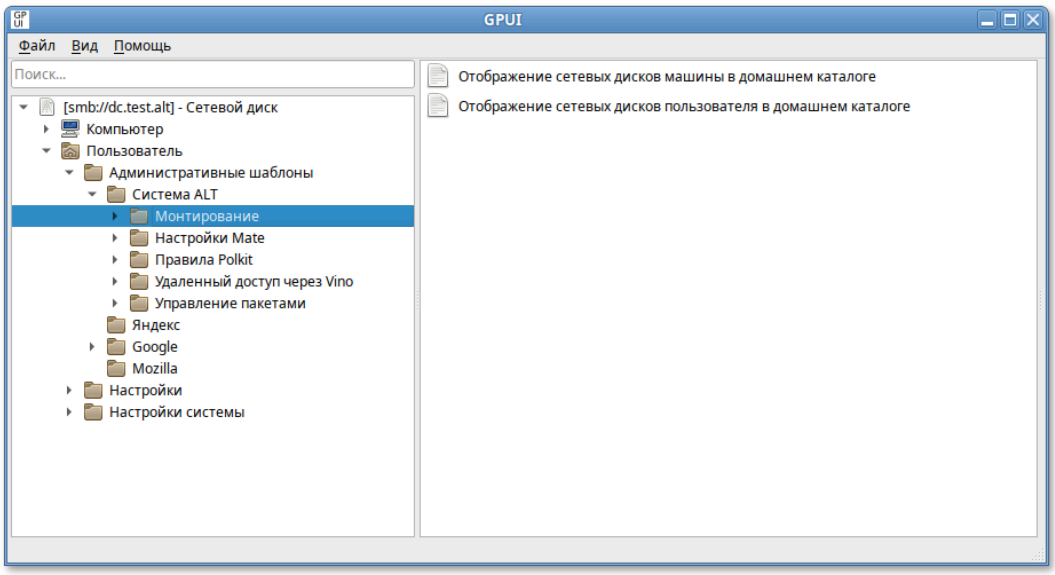


Рис. 322 – Раздел «Монтирование»

Для включения политики монтирования нужно щелкнуть на нужной политике, в открывшемся окне установить отметку в поле «Включено» и нажать кнопку «ОК» (рис. 323).

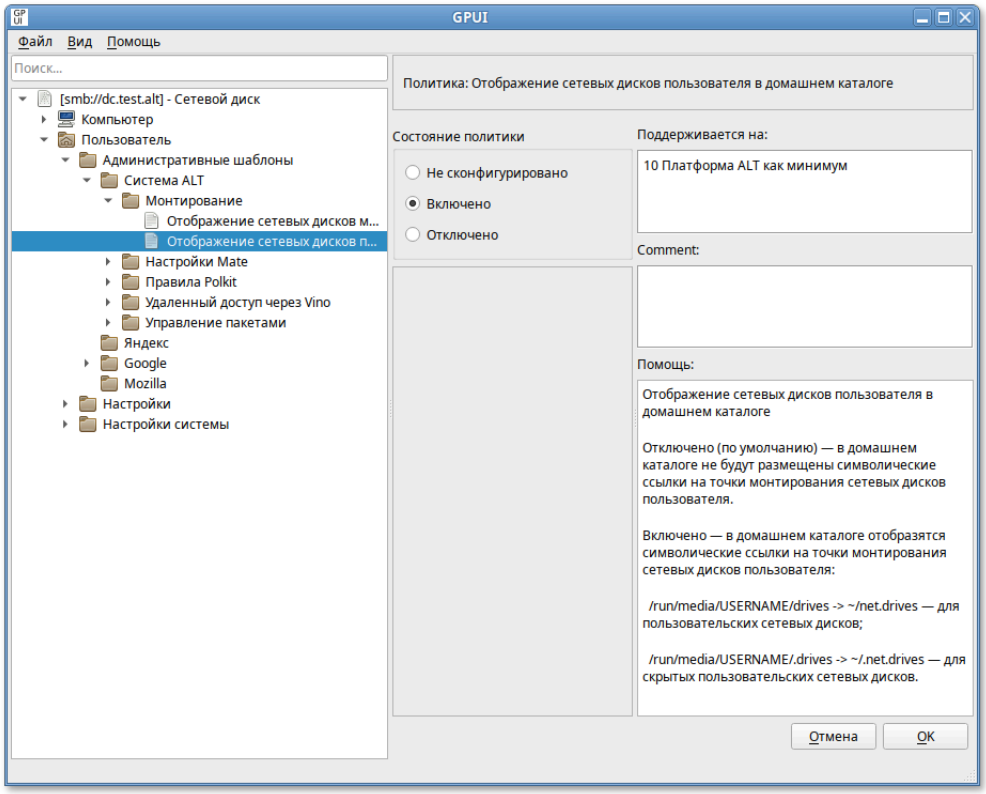


Рис. 323 – Включение политики монтирования

После обновления политик в сессии пользователя будет подключен сетевой диск, доступный из файлового менеджера и других программ (рис. 324, рис. 325).

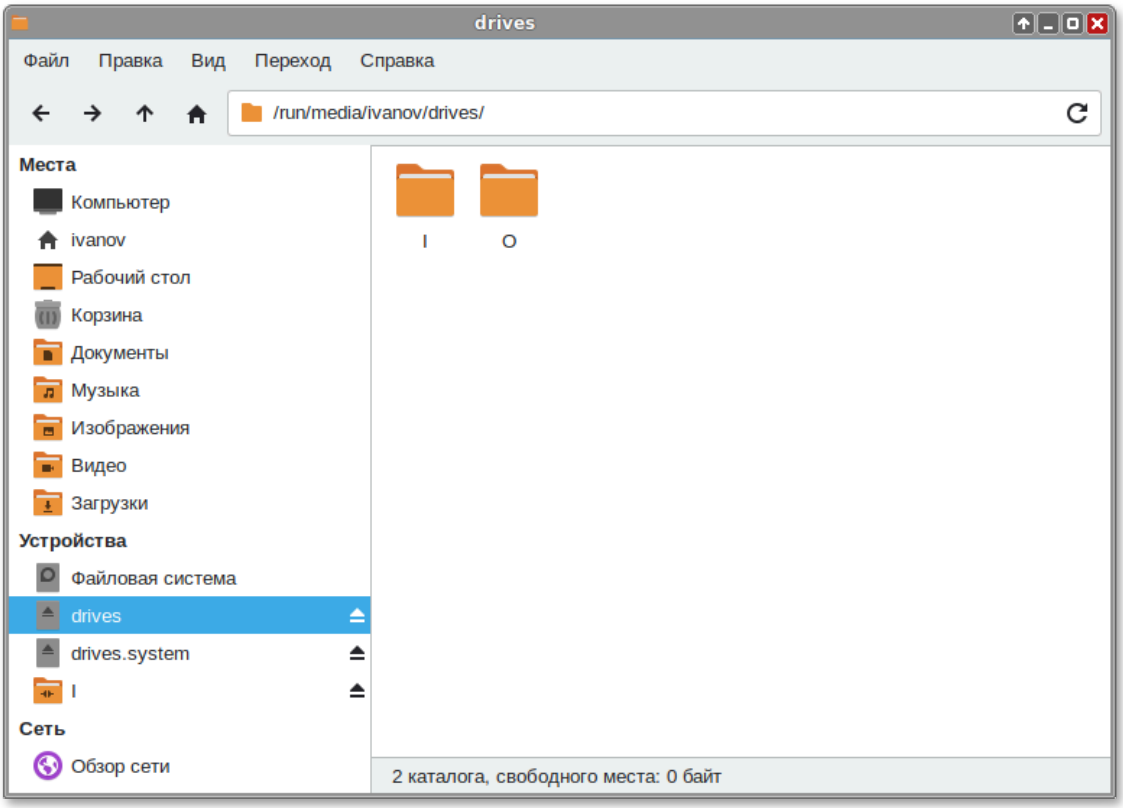


Рис. 324 – Обновление политик в сессии

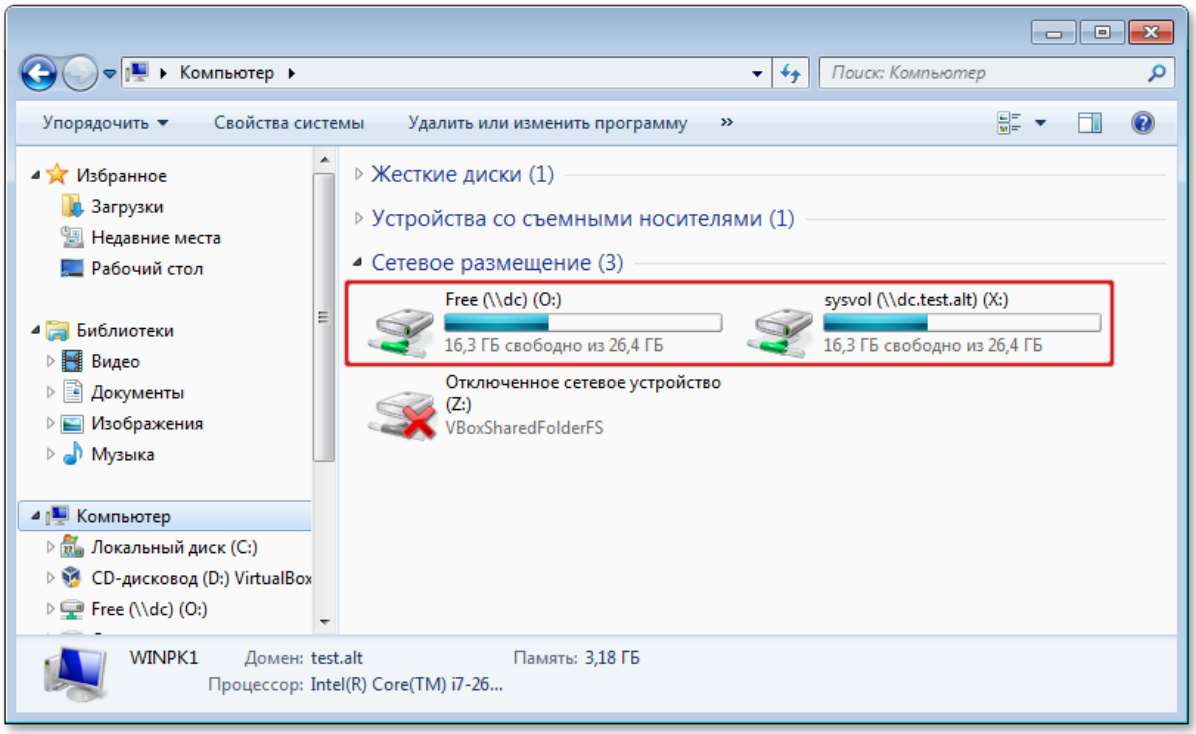


Рис. 325 – Сетевое размещение

Если включены политики монтирования, в домашнем каталоге пользователя появятся ссылки (рис. 326):

- `~/net.drives.system` – ссылка на `/media/gpupdate/drives.system`;
- `~/.net.drives.system` – ссылка на `/media/gpupdate/.drives.system`;
- `~/net.drives` – ссылка на `/run/media/USERNAME/drives`;
- `~/.net.drives` – ссылка на `/run/media/USERNAME/.drives`.

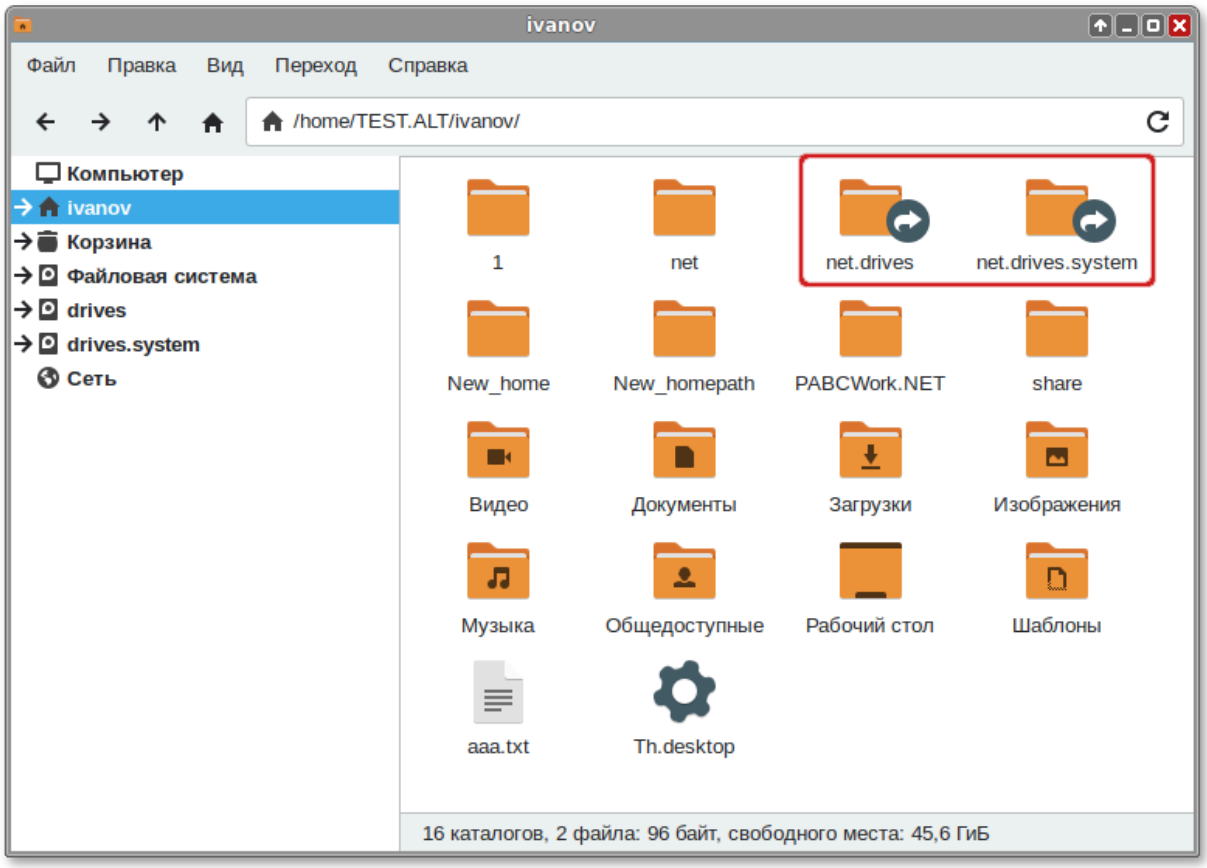


Рис. 326 – Ссылки в домашнем каталоге пользователя

Все настройки политики управления файлами хранятся в файлах:

`{GUID GPT}/Machine/Preferences/Drives/Drives.xml`

`{GUID GPT}/User/Preferences/Drives/Drives.xml`

В одном GPO возможно задать подключение более одного сетевого диска. Пример файла `Drives.xml` с двумя сетевыми дисками:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<Drives clsid="{8FDDCC1A-0C3C-43cd-A6B4-71A6DF20DA8C}">
  <Drive bypassErrors="0"
        changed="2022-11-29 16:28:32"
        clsid="{935D1B74-9CB8-4e3c-9914-7DD559B7A417}"
        desc=""
        image="2"
        name="\\dc\Free"
        removePolicy="0"
        status="O:"
        uid="{D070D4D6-DEB5-4DDE-9A53-6AB33C90352A}"
        userContext="0">
    <Properties
        action="U"
        allDrives="SHOW"
        cpassword=""
        label=""
        letter="O"
        path="\\dc\Free"
        persistent="1"
        thisDrive="SHOW"
        useLetter="1"
        userName=""/>
  </Drive>
  <Drive bypassErrors="0"
        changed="2022-11-29 14:34:53"
        clsid="{935D1B74-9CB8-4e3c-9914-7DD559B7A417}"
        desc=""
        image="2"
        name="I:"
        status="I:"
        uid="{4BDA1724-4BBF-4B4D-B299-E81080D9A4B5}"
        userContext="0">
    <Properties
        action="U"
        allDrives="SHOW"
        cpassword=""
        label=""
        letter="I"
        path="\\dc.test.alt\sysvol"
        persistent="1"
        thisDrive="SHOW"
        useLetter="0"
        userName=""/>
  </Drive>
</Drives>
```

9.2.5.5.8. Настройка реестра

Групповая политика «Настройка реестра» позволяет управлять настройками реестра Windows.

Для настройки этой политики следует перейти в «Компьютер/Пользователь» → «Настройки» → «Настройки системы» → «Реестр». В контекстном меню свободной области выбрать пункт «Новый» → «Значение реестра» (рис. 327).

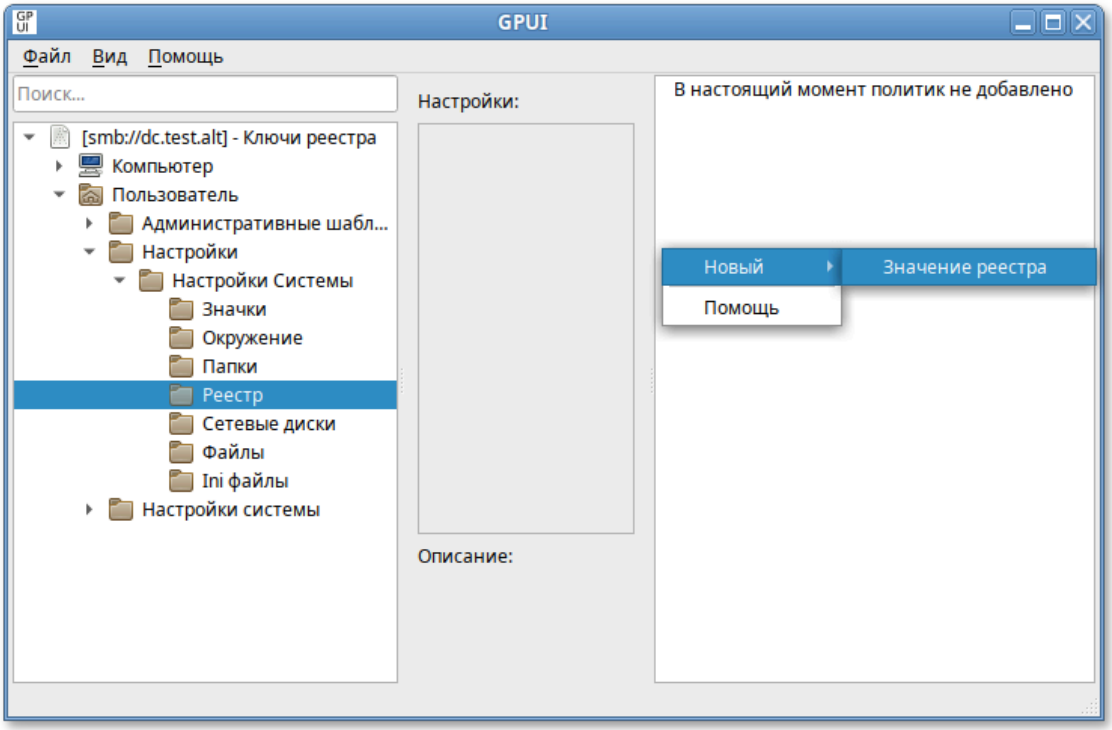


Рис. 327 – Пункт «Значение реестра»

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 328).

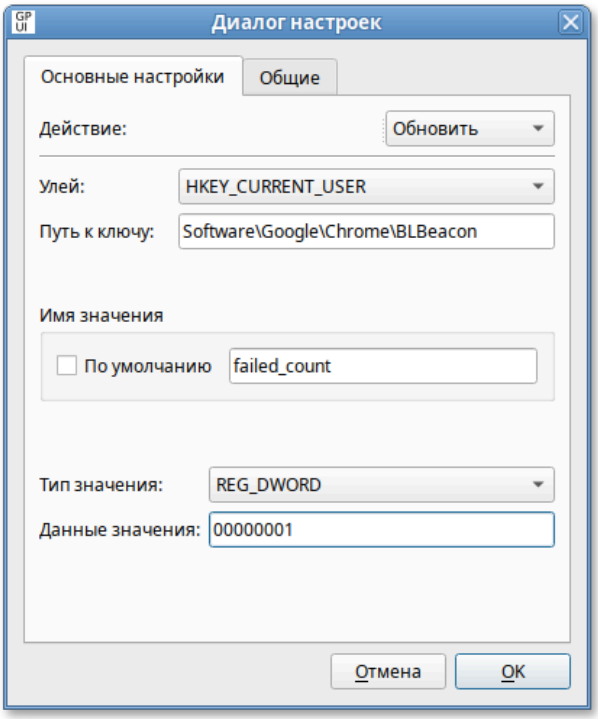


Рис. 328 – Диалоговое окно «Диалог настроек»

Опции доступные на вкладке «Основные настройки»:

1) «Действие» – действие, которое будет выполняться для элемента реестра:

- «Создать» – создание нового значения или раздела, которое будет выполняться для элемента реестра;
- «Удалить» – удаление, которое будет выполняться для элемента реестра, всех его значений и подразделов;
- «Заменить» – удаление и повторное создание значения или раздела реестра. Если целевым объектом является значение реестра, то конечным результатом действия будет перезапись всех существующих параметров, сопоставленных данному значению реестра. Если целевым объектом является раздел реестра, то конечным результатом будет удаление всех значений и подразделов реестра, и останется только имя значения по умолчанию без данных. Если значение или раздел реестра не существует, то действие «Заменить» приведет к созданию нового значения или раздела;

- «Обновить» – изменение параметров существующего значения или раздела реестра. Это действие отличается от «Заменить» тем, что оно обновляет только параметры, определенные в элементе настройки. Все остальные параметры значения или раздела реестра остаются прежними. Если значение или раздел реестра не существует, то действие «Обновить» приведет к созданию нового значения или раздела;

2) «Улей» – улей (куст) для раздела реестра:
   - «HKEY_CLASSES_ROOT» – информация о зарегистрированных в Windows типах файлов (это псевдоним для HKEY_LOCAL_MACHINE\Software\Classes);
   - «HKEY_CURRENT_USER» – настройки пользователя, вошедшего в Windows (это псевдоним для HKEY_USERS\куст текущего пользователя). HKEY_USERS\.Default используется в том случае, когда HKEY_CURRENT_USER настроен в разделе конфигурации компьютера;
   - «HKEY_LOCAL_MACHINE» – настройки, относящиеся к компьютеру (параметр по умолчанию для политики компьютера). Эти параметры применяются ко всем пользователям компьютера;
   - «HKEY_USERS» – настройки для всех пользователей (параметр по умолчанию для политики пользователя). Эти параметры применяются к отдельным пользователям;
   - «HKEY_CURRENT_CONFIG» – сведения о настройках оборудования (это псевдоним для HKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware Profiles\Current).

3) «Путь к ключу» – путь к ключу. Не нужно указывать улей и вводить косую черту до или после пути. Это поле воспринимает переменные процесса настройки;

4) «Имя значения» – для настройки значения следует установить, либо отметку в пункте «По умолчанию», чтобы принять значение раздела по умолчанию, либо ввести имя настраиваемого значения. Чтобы настроить только раздел, следует оставить это поле пустым. В этом поле можно указать переменные;
5) «Тип значения» – тип значения. Данный параметр доступен только при выбранном действии «Создать», «Заменить» или «Обновить», и введенном значении «Имя значения»;
6) «Данные значения» – значения реестра. Чтобы настроить только раздел, следует оставить это поле пустым. В этом поле можно указать переменные. Данный параметр доступен только при выбранном действии «Создать», «Заменить» или «Обновить» и введенном значении «Имя значения».

Все настройки политики управления файлами хранятся в файлах:

```
{GUID GPT}/Machine/Registry/Registry.xml
{GUID GPT}/User/Registry/Registry.xml
```

Пример файла `Registry.xml`:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<RegistrySettings clsid="{A3CCFC41-DFDB-43a5-8D26-0FE8B954DA51}">
  <Registry changed="2022-11-21 18:36:20"
        clsid="{9CD4B2F4-923D-47f5-A062-E897DD1DAD50}"
        image="12"
        name="failed_count"
        status="failed_count"
        uid="{D5855321-D2BA-4595-BD28-4DF452BFF65F}"
        bypassErrors="1">
    <Properties
        action="U"
        displayDecimal="0"
        hive="HKEY_CURRENT_USER"
        key="Software\Google\Chrome\BLBeacon"
        name="failed_count"
        type="REG_DWORD"
        value="00000001">
        <SubProp id="" mask="0" value="0"/">
    </Properties>
  </Registry>
</RegistrySettings>
```

9.2.5.5.9. Указание прокси-сервера

С помощью групповых политик можно указать прокси-сервер.

Примечание. Если прокси-сервер был настроен в модуле «Прокси-сервер» ЦУС, предварительно нужно удалить эти настройки и в файле `/etc/sysconfig/network` удалить строки:

```
HTTP_PROXY=
HTTPS_PROXY=
FTP_PROXY=
NO_PROXY=
```

Для настройки этой политики используется политика управления переменными среды (см. п. 9.2.5.5.4).

Настройка политики для указания прокси-сервера:

1) Настроить групповую политику управления переменными окружения (рис. 329):

- в поле «Действие» выбрать пункт «Заменить»;
- в поле «Имя» указать имя переменной: HTTPS_PROXY;
- в поле «Значение» указать адрес и порт прокси-сервера, также при нужности аутентификационные данные, в формате `http://username:password@address:port`

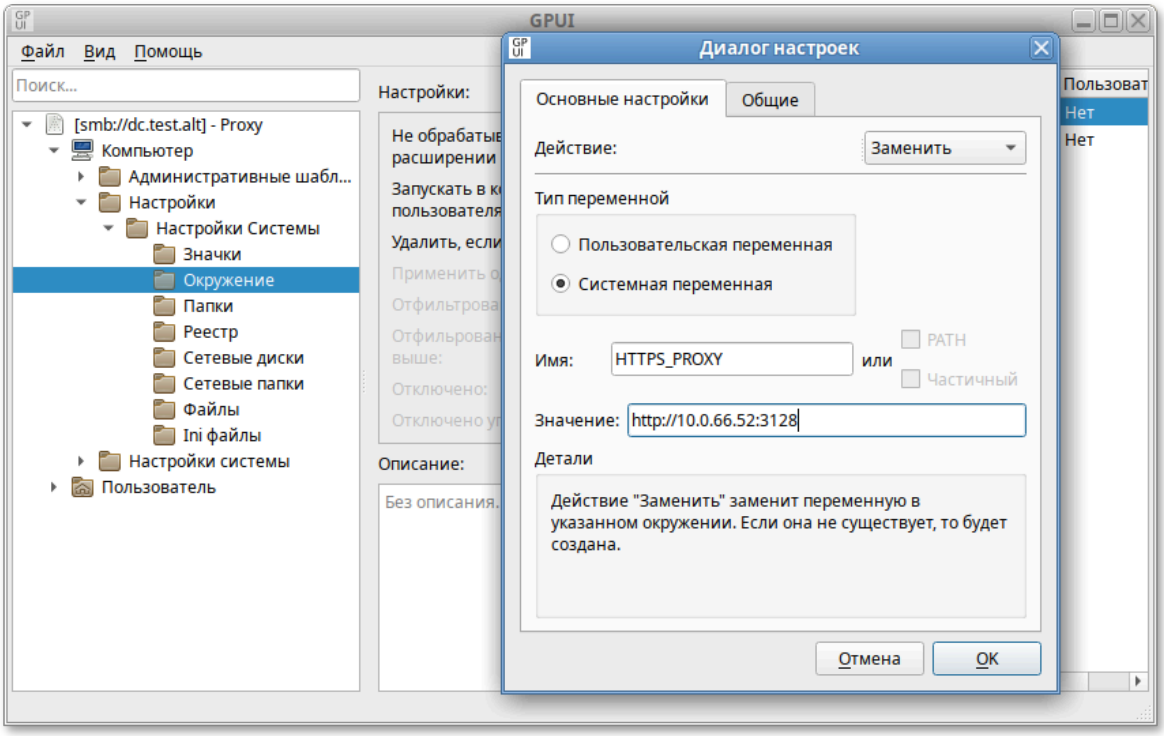


Рис. 329 – Настройка политики

Аналогичным способом создать настройки окружения для переменных HTTP_PROXY и FTP_PROXY (в поле «Имя» указывать соответственно HTTP_PROXY, FTP_PROXY).

Проверка применения политики:

- применить групповые политики на целевом компьютере, выполнив команду:

  ```
  $ gpupdate
  ```

- повторно авторизоваться на целевом компьютере;
- проверить наличие переменных окружения, выполнив команду:

  ```
  $ env |grep PROXY
  HTTP_PROXY=http://10.0.66.52:3128
  HTTPS_PROXY=http://10.0.66.52:3128
  FTP_PROXY=http://10.0.66.52:3128
  ```

- запустить веб-браузер, убедиться, что сайты открываются через прокси-сервер.

9.2.5.5.10. Настройка периодичности запроса конфигураций

Периодичность запроса конфигураций (запроса `gpupdate`) можно установить с помощью групповых политик.

Для настройки этой политики используются политика управления каталогами (см. п. 9.2.5.5.2) и политика управления INI-файлами (см. п. 9.2.5.5.3).

Настройка политики задания периодичности запроса конфигураций:

1) настроить групповую политику создания каталога (рис. 330):
   - в поле «Действие» выбрать пункт «Создать»;
   - в поле «Путь» указать `/etc/systemd/system/gpupdate.timer.d`;
2) настроить групповую политику создания INI-файла (рис. 331):
   - в поле «Действие» выбрать пункт «Обновить»;
   - в поле «Путь» к файлу указать `/etc/systemd/system/gpupdate.timer.d/override.conf`
   - в поле «Имя секции» указать «Timer»;
   - в поле «Имя свойства» указать OnUnitActiveSec;

- в поле «Значение свойства» указать периодичность запроса, в данном примере 10 минут: 10min.

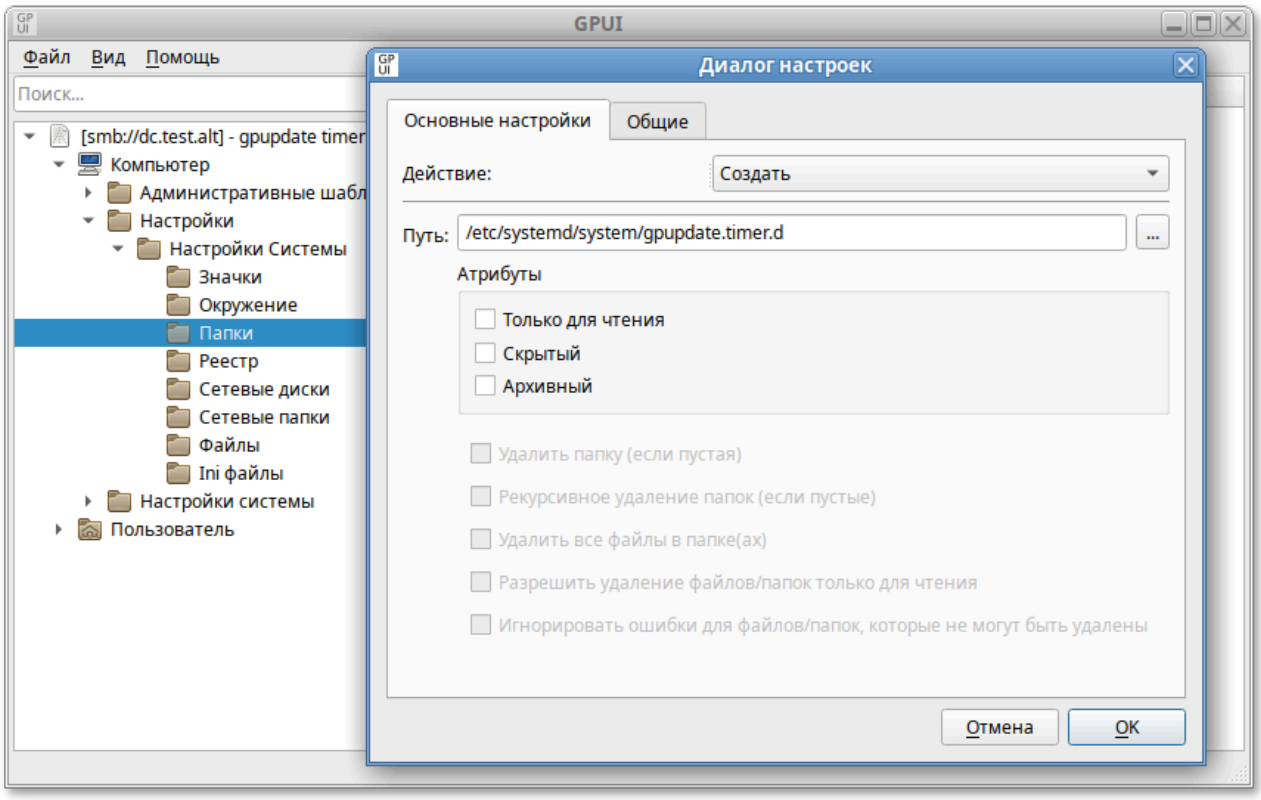


Рис. 330 – Настройка политики задания периодичности запроса конфигураций

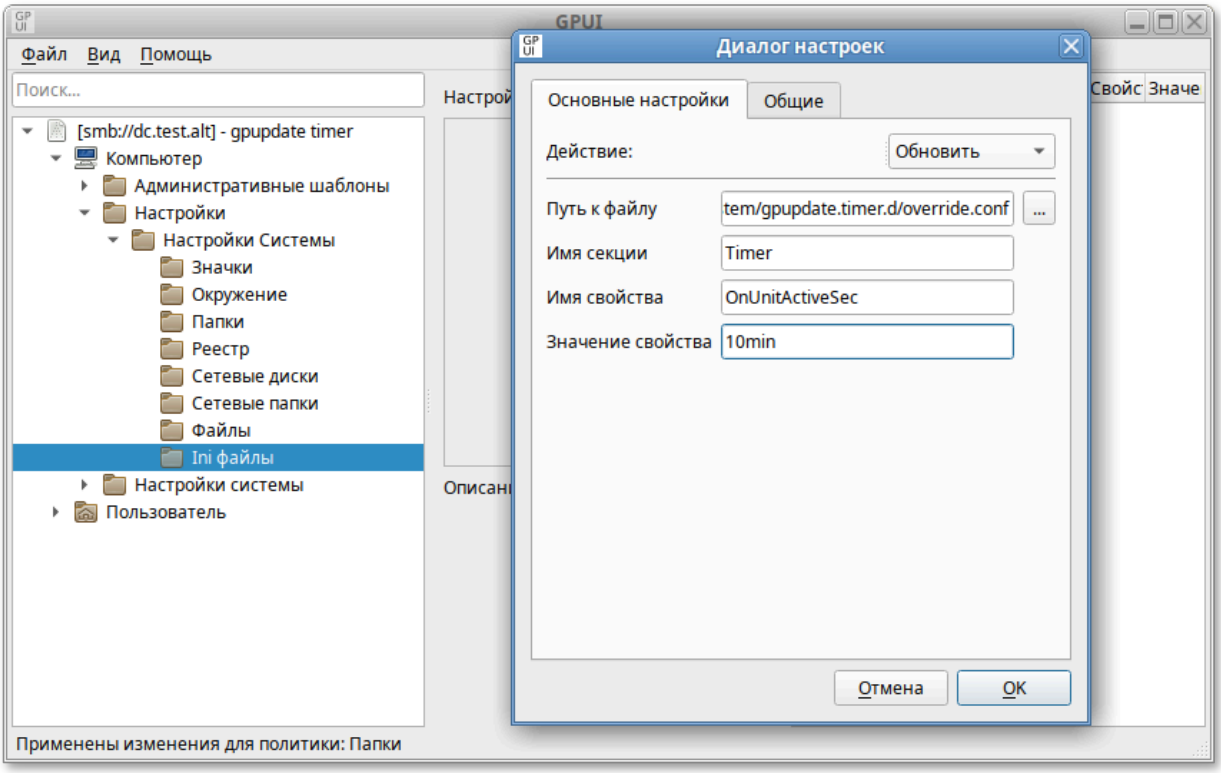


Рис. 331 – Настройка групповой политики создания INI-файла

Проверка применения политики:

1) применить групповые политики на целевом компьютере, выполнив команду:

```
$ gpupdate
```

2) выполнить команду (или перезагрузить компьютер):

```
# systemctl daemon-reload
```

3) убедиться, что политика применилась, выполнив команды:

```
$ cat /etc/systemd/system/gpupdate.timer.d/override.conf
[Timer]
OnUnitActiveSec = 10min

$ systemctl status gpupdate.timer
…
Trigger: Thu 2023-06-29 20:01:06 +04; 3min left
```

Примечание. Файл `override.conf` подменяет настройки системной библиотеки в файле `/lib/systemd/system/gpupdate.timer` только если значение секции Timer в файле `override.conf` меньше, чем значение аналогичной секции в gpupdate.timer.

9.2.5.6. Управление logon-скриптами

Групповые политики позволяют запускать сценарии запуска и завершения работы компьютера, входа и выхода из системы пользователя. Возможно связать один или несколько файлов сценариев (scripts) с четырьмя инициируемыми событиями:

1) для машины:

- запуск компьютера (Startup);
- выключение компьютера/Завершение работы (Shutdown);

2) для пользователя:

- вход пользователя (Logon);
- выход пользователя (Logoff).

Система выполняет сценарии на языках, которые поддерживает клиентский компьютер. В среде Windows эту задачу выполняет Windows Script Host (WSH), который поддерживает языки сценариев, включая bat, cmd, VBScript и Jscript. В случае если указано более одного сценария, они будут выполняться согласно перечню в списке.

Примечание. В сценариях, запускаемых на машинах на базе ОС ALT, нужно в первой строке указывать шебанг, например, `#!/usr/bin/env bash`

Примечание. Если сценарии (scripts) хранятся в SYSVOL, они реплицируются между контроллерами домена. SYSVOL доступен всем членам домена, что гарантирует запуск сценария.

9.2.5.6.1. Сценарии для входа/выхода пользователя

Для удобства можно скопировать нужные сценарии в каталог `User\Scripts\Logon` (например, `\\test.alt\sysvol\test.alt\Policies\{20DDB816-421B-4861-8AC5-007E56CB67D0}\User\Scripts\Logon`) или `User\Scripts\Logoff` соответствующей политики.

Для настройки политики следует перейти в «Пользователь» → «Настройки системы» → «Скрипты». Щелкнуть левой кнопкой мыши на политике «Вход в систему» или «Выход из системы» (рис. 332).

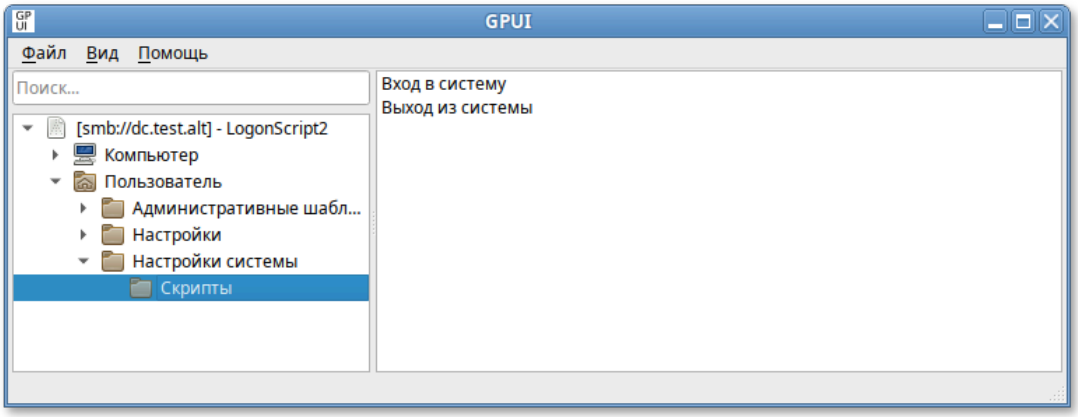


Рис. 332 – Политика «Вход в систему» или «Выход из системы»

В диалоговом окне свойств политики нажать кнопку «Добавить» (рис. 333).

В диалоговом окне «Добавить скрипт» в поле «Имя сценария» ввести путь к сценарию, в поле «Параметры сценария» ввести параметры аналогично вводу этих параметров в командной строке. Нажать кнопку «ОК».

Пример добавления сценария для ОС Альт СП (рис. 334).

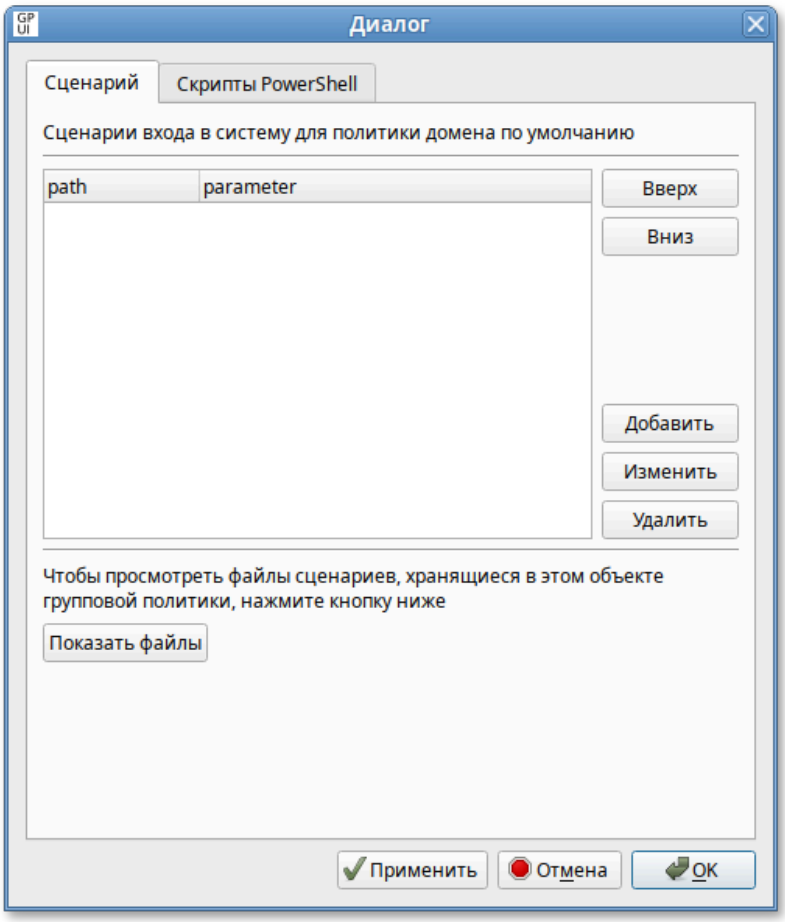


Рис. 333 – Диалоговое окно свойств политики

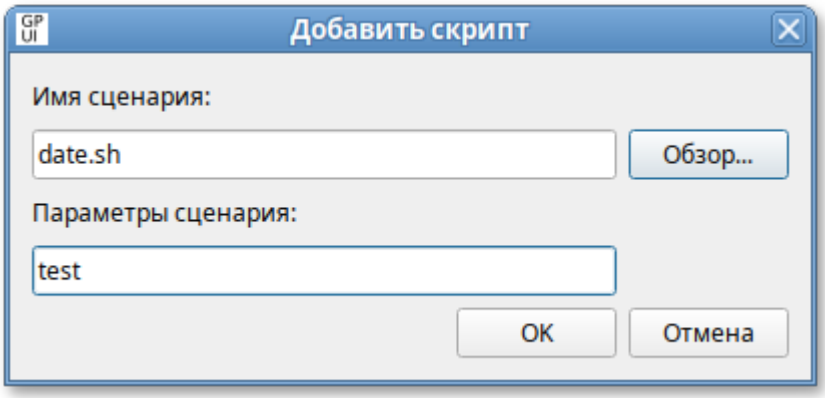


Рис. 334 – Пример добавления сценария

П р и м е ч а н и е . Применение локальных скриптов реализовано в механизме gpupdate версии 0.9.11. В версиях ниже скрипты для ОС Альт СП должны находиться в GPT настраиваемого объекта групповой политики.

Пример добавления сценария для ОС Windows (можно указать локальный скрипт на компьютере клиента) (рис. 335).

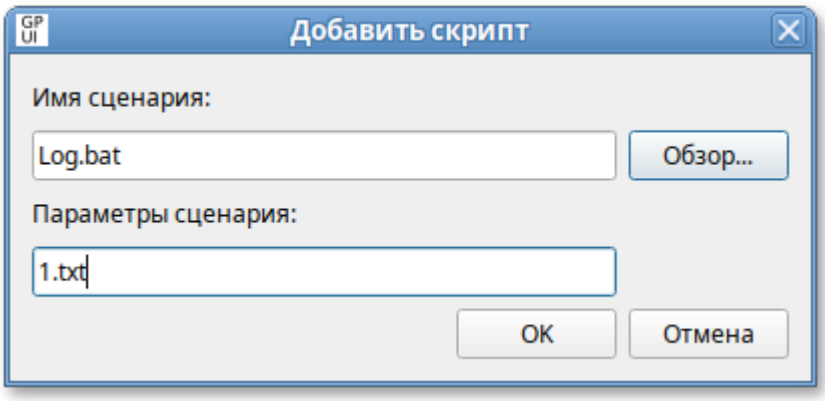


Рис. 335 – Пример добавления сценария для ОС Windows

При назначении нескольких сценариев они будут применяться в заданном порядке. Чтобы переместить сценарий в списке вверх/вниз, следует выбрать его в списке и нажать кнопку «Вверх»/«Вниз».

Для того чтобы изменить параметры сценария, нужно выбрать его в списке и нажать кнопку «Изменить». Кнопка «Удалить» предназначена для удаления сценария из списка (рис. 336).

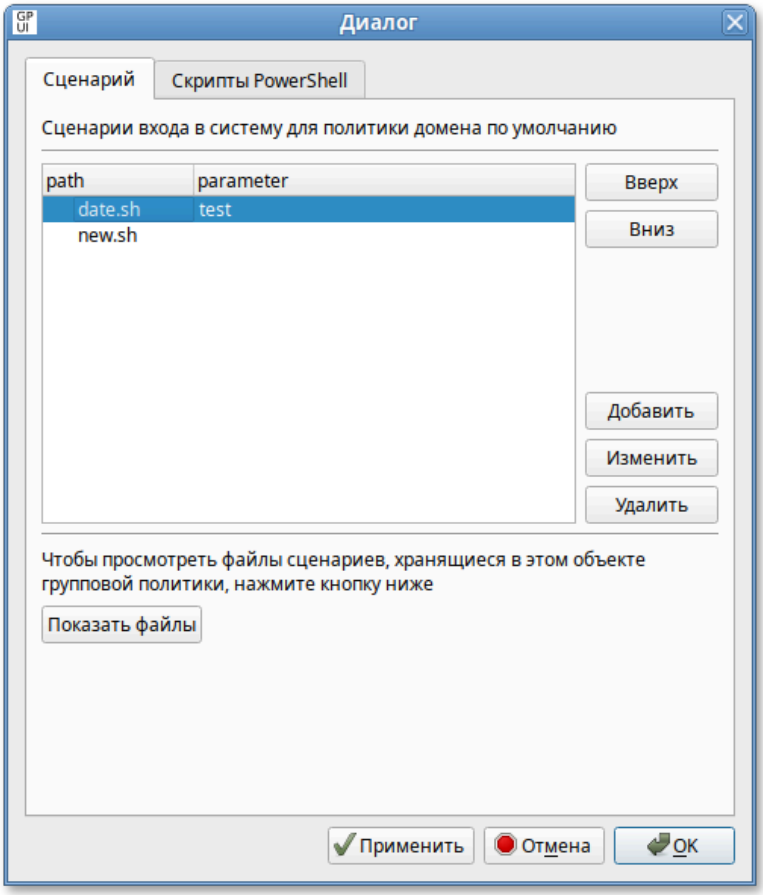


Рис. 336 – Удаление сценария из списка

На вкладке «Скрипты PowerShell» можно добавить сценарии с расширением `*.ps1`.

9.2.5.6.2. Сценарии для автозагрузки или завершения работы компьютера

Для удобства можно скопировать нужные сценарии в каталог `Machine\Scripts\Startup` (например, `\\test.alt\sysvol\test.alt\Policies\{20DDB816-421B-4861-8AC5-007E56CB67D0}\Machine\Scripts\Startup`) или `Machine\Scripts\Shutdown` соответствующей политики.

Для настройки политики следует перейти в «Компьютер» → «Настройки системы» → «Скрипты». Щелкнуть левой кнопкой мыши на политике «Запуск» или «Завершение работы» (рис. 337).

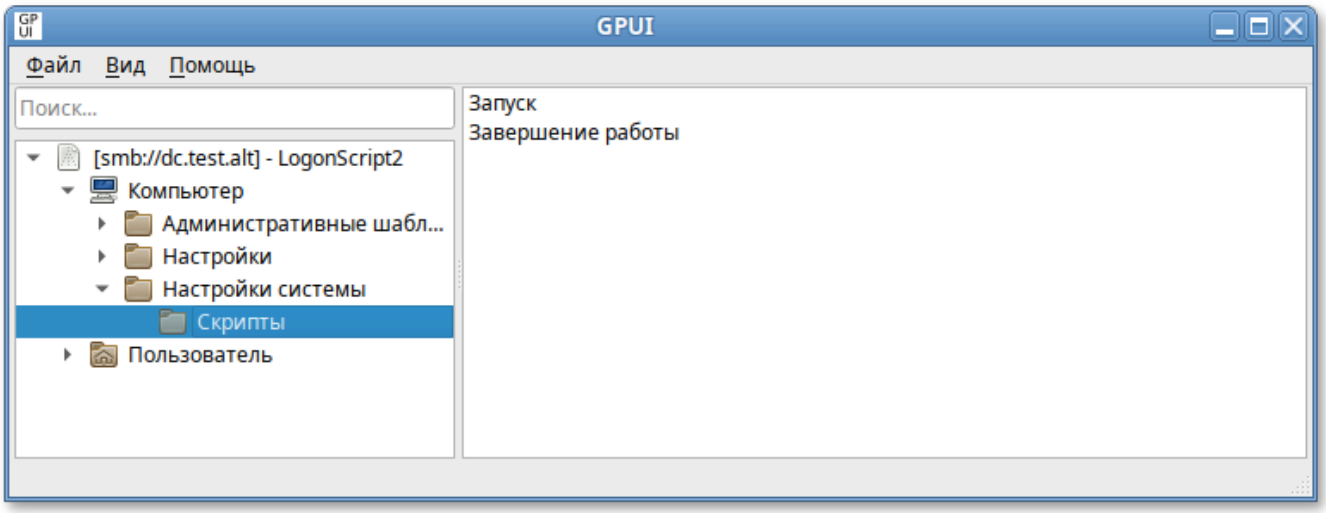


Рис. 337 – Сценарии для автозагрузки или завершения работы компьютера

В диалоговом окне свойств политики нажать кнопку «Добавить» (рис. 338).

В диалоговом окне «Добавить скрипт» в поле «Имя сценария» ввести путь к сценарию, в поле «Параметры сценария» ввести параметры аналогично вводу этих параметров в командной строке. Нажать кнопку «ОК».

Пример добавления сценария для ОС Альт СП (см. рис. 334).

П р и м е ч а н и е . Применение локальных скриптов реализовано в механизме gpupdate версии 0.9.11. В версиях ниже скрипты для ОС Альт СП должны находиться в GPT настраиваемого объекта групповой политики.

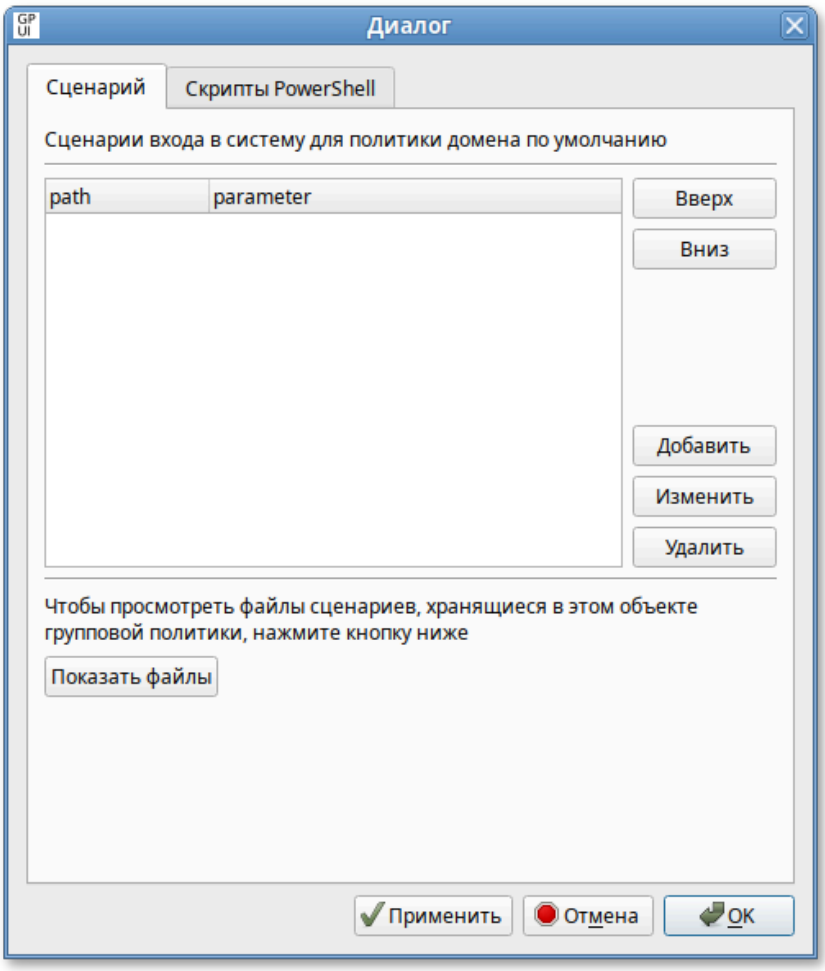


Рис. 338 – Диалоговое окно свойств политики

Пример добавления сценария для ОС Windows (можно указать локальный скрипт на компьютере клиента) (рис. 339).

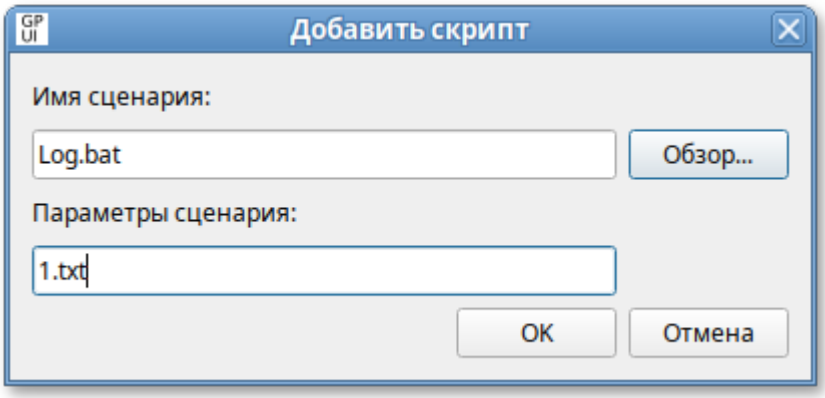


Рис. 339 – Пример добавления сценария для ОС Windows

При назначении нескольких сценариев они будут применяться в заданном порядке. Чтобы переместить сценарий в списке вверх/вниз, следует выбрать его в списке и нажать кнопку «Вверх»/«Вниз». Для того чтобы изменить параметры сценария, нужно выбрать его в списке и нажать кнопку «Изменить». Кнопка «Удалить» предназначена для удаления сценария из списка.

На вкладке «Скрипты PowerShell» можно добавить сценарии с расширением `*.ps1`.

9.2.5.6.3. Включение экспериментальных групповых политик

Политики управления logon-скриптами относятся к экспериментальным, поэтому на машинах с ОС Альт СП где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 9.2.5.4.7).

Также можно включить/отключить механизм групповых политик управления logon-скриптами, включив/отключив политики «Модуль выполнения сценариев для компьютеров» или «Модуль выполнения сценариев для пользователей» («Компьютер» → «Административные шаблоны» → «Система ALT» → «Групповые политики» → «Механизмы GPUpdate») (рис. 340).

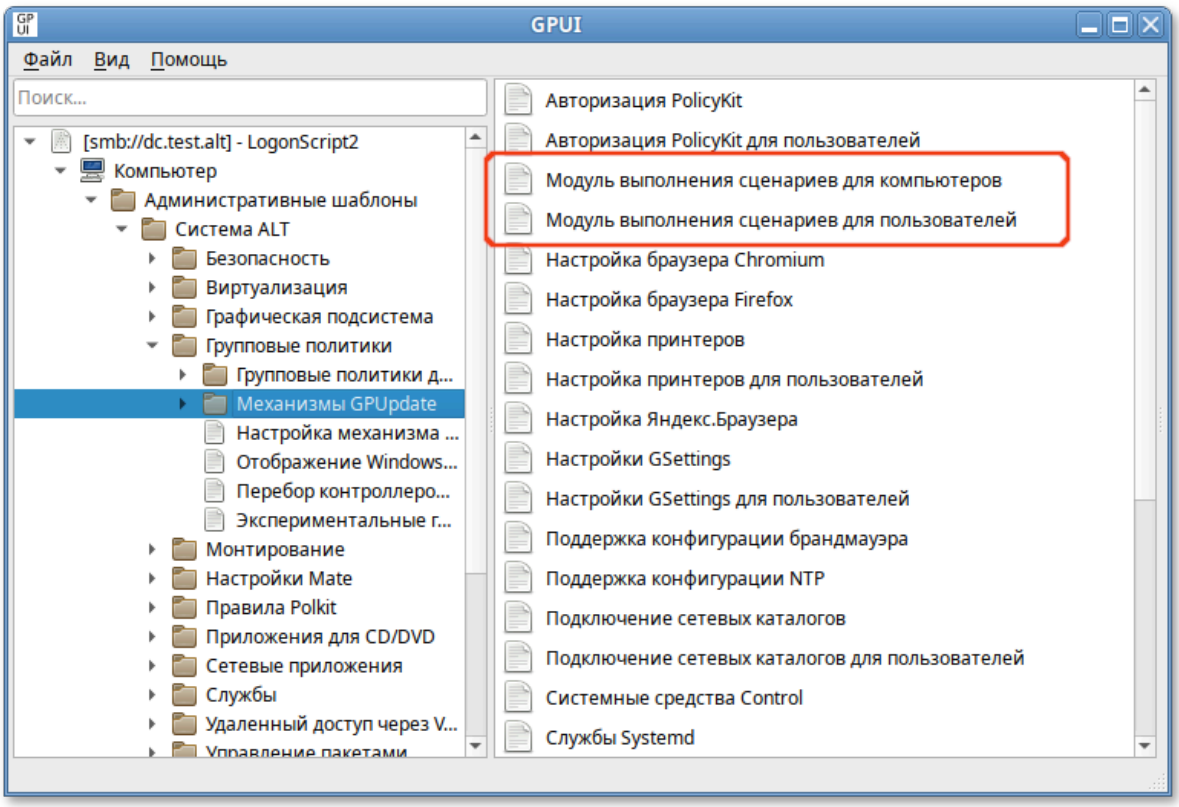


Рис. 340 – Включение экспериментальных групповых политик

9.2.5.6.4. Файлы настроек политики

Файлы сценариев входа и выхода пользователя (за исключением локальных) хранятся в каталогах: `{GUID GPT}\User\Scripts\Logon` и `{GUID GPT}\User\Scripts\Logoff`. Настройки политики для сценариев входа и выхода пользователя хранятся в файле `{GUID GPT}\User\Scripts\scripts.ini`. В файле `scripts.ini` перечисляются все скрипты, выполняемые в сценариях входа и выхода пользователя из системы. Сценарии входа начинаются с преамбулы `[Logon]`, сценарии выхода начинаются с преамбулы [Logoff].

Пример файла `scripts.ini`:

```
[Logon]
0CmdLine=date.sh
0Parameters=test
1CmdLine=test.sh
1Parameters=new
[Logoff]
0CmdLine=touch.sh
0Parameters=
1CmdLine=Logoff.bat
1Parameters=1.txt
2CmdLine=C:\share\Logon.bat
2Parameters=
```

Файлы сценариев запуска и завершения работы компьютера (за исключением локальных) хранятся в каталогах: `{GUID GPT}\Machine\Scripts\Shutdown` и `{GUID GPT}\Machine\Scripts\Startup`. Настройки политики для сценариев входа и выхода пользователя хранятся в файле `{GUID GPT}\User\Scripts\scripts.ini`. В файле `scripts.ini` перечисляются все скрипты, выполняемые в сценариях запуска и завершения работы компьютера. Сценарии запуска компьютера начинаются с преамбулы [Startup], сценарии завершения работы начинаются с преамбулы [Shutdown].

Пример файла `scripts.ini`:

```
[Startup]
0CmdLine=hello.bat
0Parameters=
1CmdLine=notescript.vbs
1Parameters=
2CmdLine=notescript2.vbs
2Parameters=
3CmdLine=touch.bat
```

```
3Parameters=
[Shutdown]
0CmdLine=touch.bat
0Parameters=
```

Файл `scripts.ini` закодирован в формате UTF-16LE (little-endian).

9.3. Решение проблем

Прежде чем разбираться, почему групповые политики не применяются как ожидается, необходимо убедиться, что инфраструктура AD работает штатно. Работа групповых политик в домене зависит от корректности работы контроллеров домена и репликации между ними.

Не рекомендуется использовать сложную структуру групповых политик и создавать дополнительные политики без необходимости. Рекомендуется использовать единую схему наименования политик. Имя групповой политики должно давать однозначное понимание того, для чего она нужна.

9.3.1. Область действия и статус групповой политики

В каждой групповой политике есть два независимых раздела с настройками:

- «Компьютер» – параметры, применяемые к компьютеру;
- «Пользователь» – параметры пользователей.

Если параметр политики настраивается в секции «Компьютер», групповая политика должна быть привязана к OU с компьютерами. Соответственно, если настраиваемый параметр относится к конфигурации пользователя, нужно назначить политику на OU с пользователями.

Примечание. Чтобы применить пользовательские настройки к компьютерам, нужно включить политику замыкания (см. п. 9.3.4).

Если групповая политика настраивает только параметры пользователя или только параметры компьютера, неиспользуемый раздел можно отключить. Это снизит трафик групповой политики и позволит уменьшить время обработки групповой политики на клиентах.

Статус групповой политики можно проверить в ADMC в свойствах подразделения на вкладке «Групповая политика» (рис. 341).

Изменение статуса групповой политики возможно в свойствах на вкладке «Атрибуты» (рис. 342).

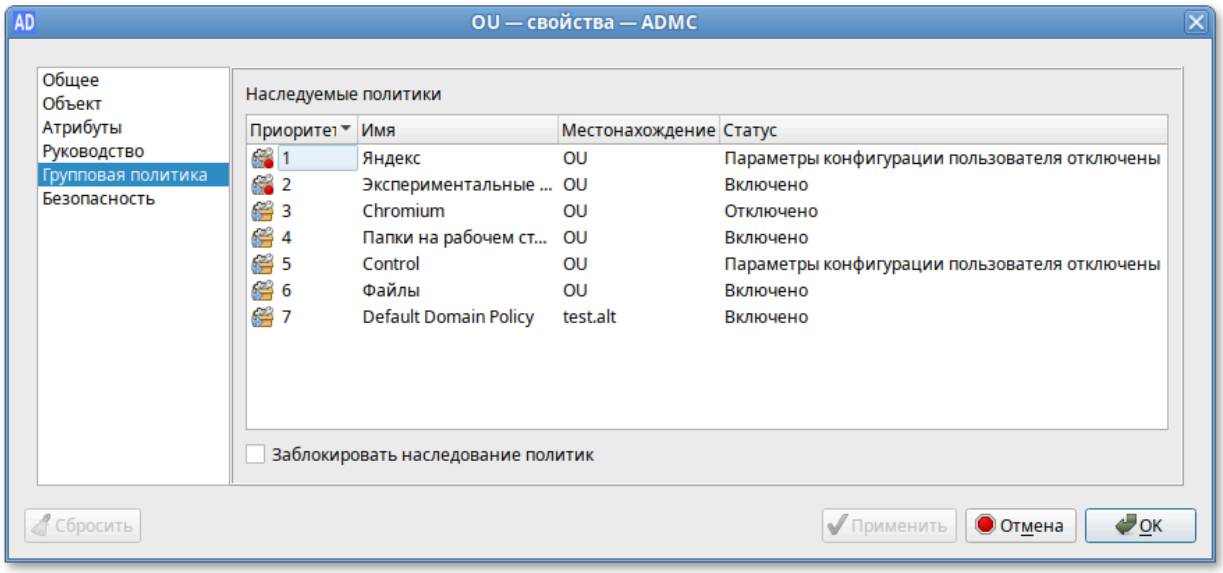


Рис. 341 – Вкладка «Групповая политика»

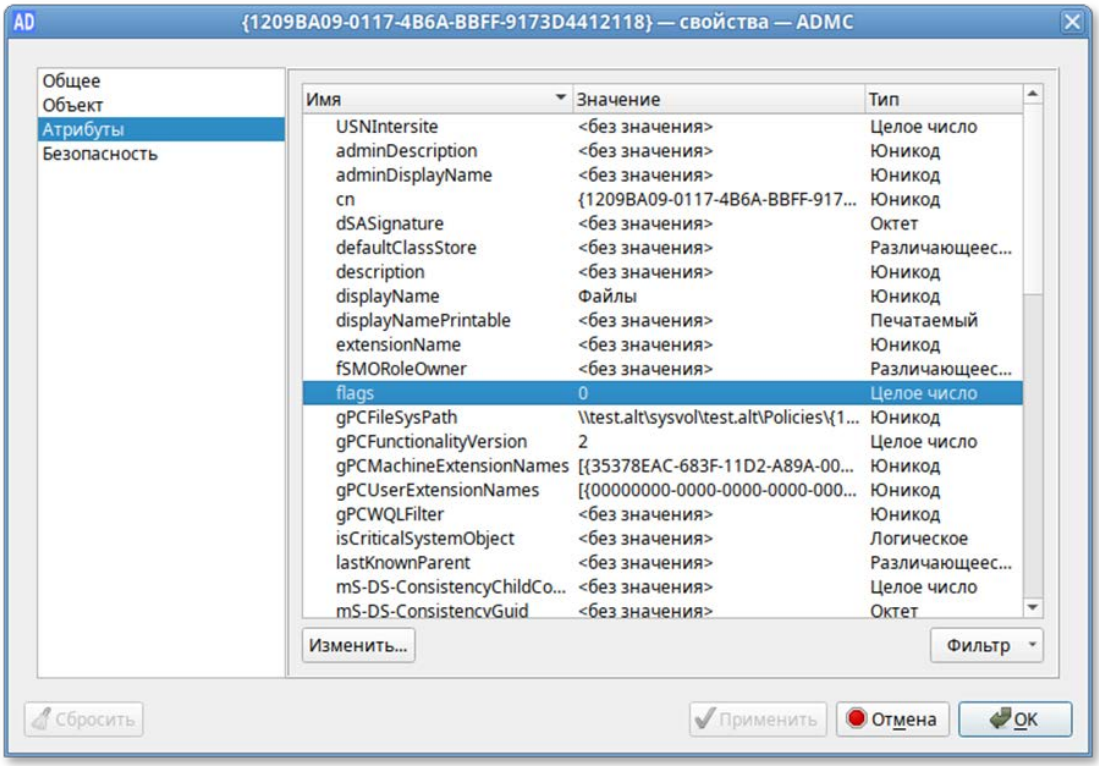


Рис. 342 – Вкладка «Атрибуты»

Состояние объекта групповой политики указывается в значении атрибута `flags`. Данный атрибут может принимать следующие значения:

- значение «0» – объект GPO включен (все настройки политики применяются к целевым объектам AD);
- значение «1» – отключен раздел «Конфигурация пользователя» (не применяются настройки пользовательских политик);
- значение «2» – отключен раздел «Конфигурация компьютера» (не применяются настройки из параметров GPO компьютера);
- значение «3» – объект GPO полностью отключен (все настройки политики не применяются).

9.3.2. Наследование групповых политик

По умолчанию политики высокого уровня применяются ко всем вложенным объектам в иерархии домена.

Увидеть какие политики применяются к подразделению и местонахождение политики можно в ADMC при выборе подразделения на вкладке «Наследуемые политики» (рис. 343).

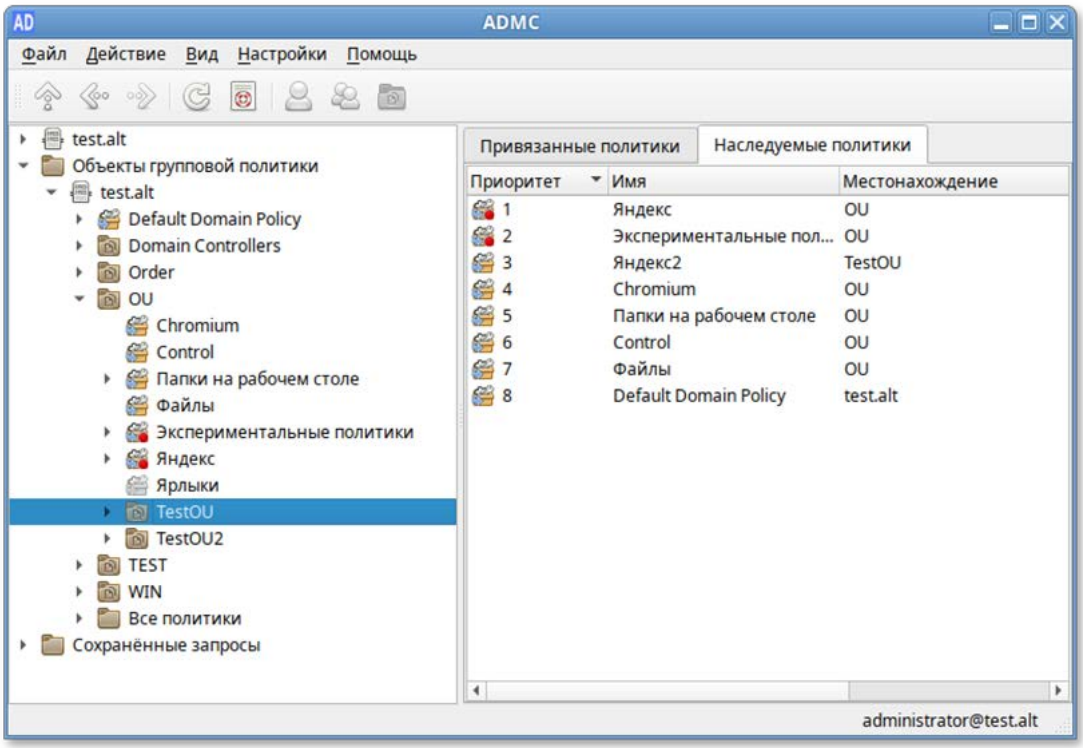


Рис. 343 – Вкладка «Нумерованные политики»

Также наследуемые политики можно увидеть на вкладке «Групповая политика» свойств подразделения (рис. 344).

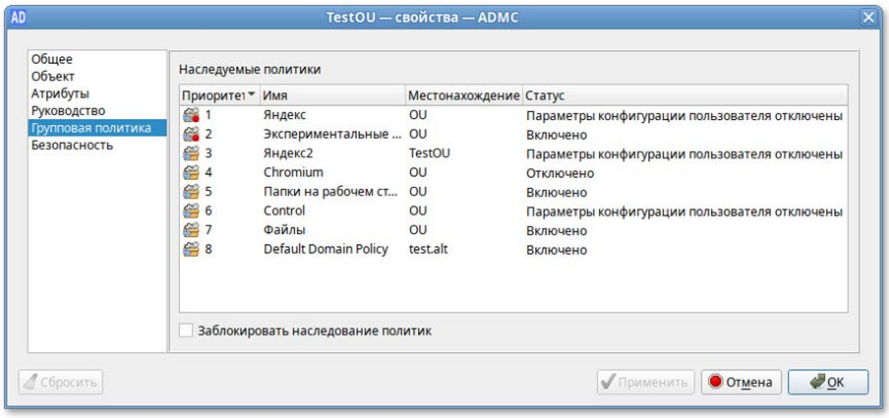


Рис. 344 – Вкладка «Групповая политика»

Каждый объект групповой политики можно настроить на блокирование наследования политик более высокого уровня (см. п. 9.2.4.11.3). Таким образом, политика подразделения может блокировать параметры политик домена и сайта. Блокирование наследования предохраняет объекты групповой политики, связанные с доменами или подразделениями родительского уровня, от автоматического наследования на дочернем уровне (рис. 345).

Так как администратор домена может не согласиться с тем, что администратор подразделения блокирует параметры политики домена, существует возможность запретить переопределение параметров с помощью отметки «Принудительно».

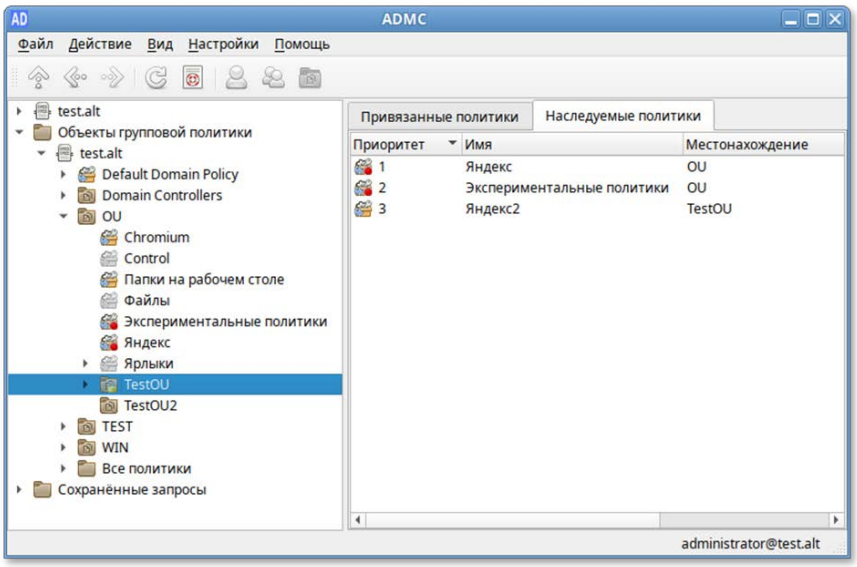


Рис. 345 – Политики подразделения с блокированием наследования

9.3.3. Порядок применения групповых политик

Групповые политики обрабатываются в следующем порядке:

- объект локальной групповой политики;
- объекты групповой политики, связанные с доменом (в рамках возможностей и ограничений поддержки леса доменов в Samba, как в наборе клиентских компонентов);
- объекты групповой политики, связанные с OU:сначала обрабатываются объекты групповой политики, связанные с OU, находящейся на самом высоком уровне в иерархии Active Directory, затем объекты групповой политики, связанные с дочерним подразделением и т. д. Последними обрабатываются объекты групповой политики, связанные с OU, в которой находится пользователь или компьютер.

Последние политики имеют наивысший приоритет. Т. е. если параметр включен на уровне политики домена, но на целевом OU данный параметр отключается другой политикой – это означает, что нужный параметр в результате будет отключен на клиенте (выиграет ближайшая политика к объекту в иерархии AD).

Если на OU назначено несколько групповых политик, то они обрабатываются в том порядке, в котором были назначены. Политики обрабатываются в обратном порядке (политика с номером 1 будет обработана последней) (рис. 346).

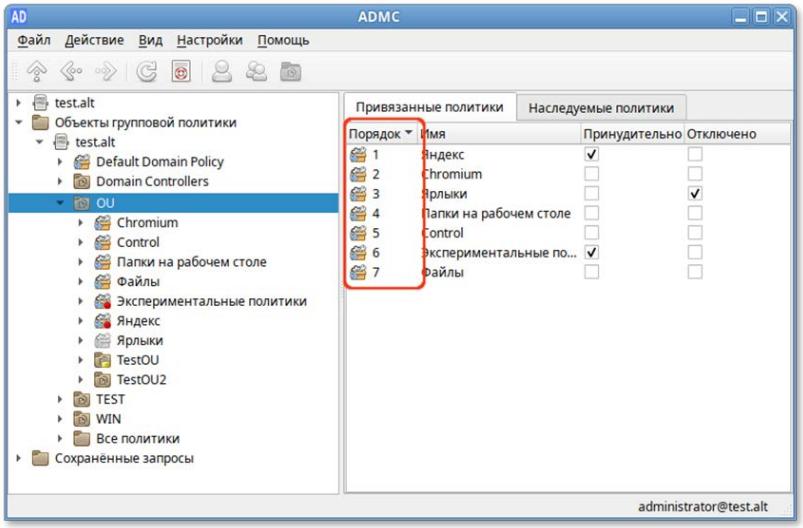


Рис. 346 – Порядок выполнения групповых политик

При необходимости этот порядок можно изменить, выбрав в контекстном меню политики пункт «Переместить вверх» или «Переместить вниз» (рис. 347).

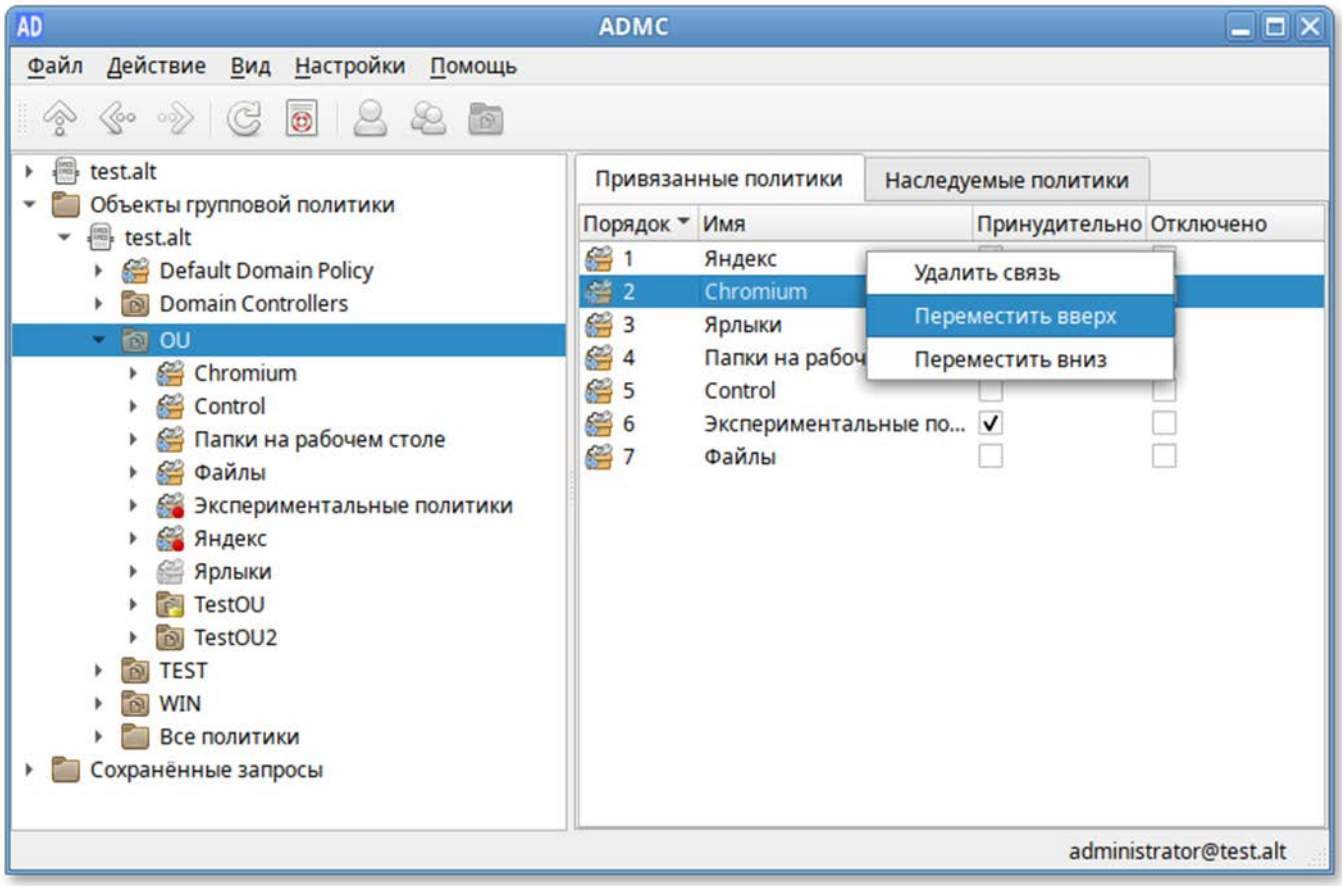


Рис. 347 – Контекстное меню политики

При использовании параметра «Принудительно» у групповой политики выигрывает та политика, которая находится выше в иерархии домена, например, политика Default Domain Policy будет выигрывать у всех других групповых политик, если у нее активирован этот параметр.

У каждого объекта групповой политики, который привязан к организационному контейнеру AD можно включить или отключить связь (применение политики). Для этого нужно выбрать опцию «Удалить связь/Добавить связь» в меню политики. При отключении связи политика перестает применяться к клиентам, но ссылка на объект групповой политики не удаляется из иерархии. Активировать данную связь можно в любой момент.

9.3.4. Замыкание групповой политики

По умолчанию групповая политика применяется к пользователю или компьютеру способом, который зависит от того, где и пользователь, и объекты компьютера находятся в Active Directory. В некоторых случаях может потребоваться применить к пользователям политику в зависимости от расположения объекта компьютера.

На компьютерах, расположенных в организационном подразделении (Organization Unit, OU), машинные объекты групповой политики применяются по порядку во время запуска компьютера. Пользовательские объекты групповой политики, пользователей из OU, применяются во время входа, независимо от того, на каком компьютере пользователь входит в систему.

Если пользовательская учетная запись находится в OU, на которое распространяется действие пользовательской политики, то применяться эти настройки будут при входе пользователя в систему независимо от того, в какое OU входит компьютер. Такое поведение может быть нежелательным, например, вполне разумно иметь одни пользовательские настройки для сервера, другие – для локального компьютера.

Политику замыкания можно использовать для применения пользовательских групповых политик в зависимости от того, на каком компьютере пользователь входит в систему.

Эта политика может принимать два значения:

- режим «Слияние» (Merge) – при входе пользователя в систему к компьютеру будут применяться политики, основанные на расположении пользователя, а затем политики, привязанные к компьютеру. При возникновении конфликтов между пользовательскими и машинными политиками, машинные политики будут иметь более высокий приоритет;
- режим «Замена» (Replace) – к пользователю будут применяться только политики, назначенные на OU, в котором содержится компьютер, на который пользователь выполнил вход.

В качестве примера рассмотрим домен с двумя организационными подразделениями – OU1 и OU2. В первом находятся объекты учетных записей пользователей и их локальные компьютеры, во втором – объекты серверов (рис. 348).

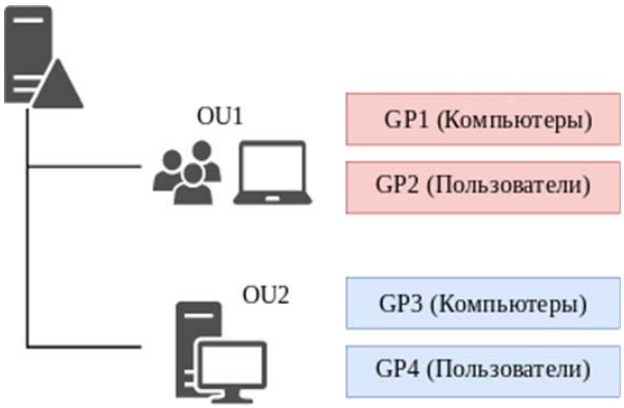


Рис. 348 – Схема деления домена

Если пользователь осуществляет вход в систему на локальном компьютере, то он оказывается под действием политики GP1 локального компьютера (которая была применена при его включении) и политики GP2 пользователя (примененной при входе в систему). Если пользователь осуществляет вход на сервер, то будут действовать политика сервера GP3 и политика пользователя GP2.

Если же включить политику замыкания (см. п. 9.3.4), то при входе на сервер будут действовать политика сервера GP3 и политика пользователя GP2+GP4 (в режиме «Слияние») или только GP4 (в режиме «Замена»). При возникновении любых конфликтов настроек между политиками OU пользователя и OU сервера в режиме «Слияние» политика в OU сервера будет иметь более высокий приоритет.

9.3.5. Диагностика применения GPO на стороне клиента

9.3.5.1. Коды ошибок

Для диагностики применения групповых политик на стороне клиента используются утилиты gpoa (на машинах Альт), gpresult (на машинах Windows).

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

1) получить и применить настройки для текущей машины:

```
# groa --loglevel 0
```

2) получить и применить настройки для пользователя:

```
# groa --loglevel 0 <имя_пользователя>
```

9.3.5.2. Коды ошибок

Сообщения, сопутствующие кодам ошибок, могут изменяться (переводиться, исправляться), но сам код уникален для определенной части программы, что позволяет однозначно идентифицировать проблему (таблица 37).

Таблица 37 – Коды ошибок и их описание

Код	Описание	Решение
E00001	Недостаточно прав для запуска программы gpupdate	Необходимо повысить уровень привилегий. Может помочь запуск программы от имени администратора
E00002	Программа gpupdate не будет запущена из-за предыдущих ошибок	
E00003	Ошибка работы бэкэнда, которая привела к досрочному прекращению обработки групповых политик. Этот код характеризует серьезные ошибки, которые обрабатываются на самом высоком уровне	Возможно, это ошибка в коде и необходимо создать отчет об ошибке, чтобы разработчики узнали о ней
E00004	Ошибка во время работы фронтенда	Высокоуровневая ошибка при инициализации фронтенда или во время работы appliers. С большой вероятностью может оказаться ошибкой в коде
E00005	Не получилось запустить appliers политик для обновления групповых политик компьютера	Проверить, что машина все еще в домене, демон oddjobd доступен через D-Bus и у пользователя достаточно прав для запуска ПО
E00006	Показать список доступных бэкэндов	Проверить, что машина все еще в домене, демон oddjobd доступен через D-Bus и у пользователя достаточно прав для запуска ПО
E00007	Невозможно инициализировать бэкэнд Samba в силу неполадок компонентов, связанных с Samba	Необходимо проверить инсталляцию Samba на машине, убедиться, что машина введена в домен и домен доступен
E00008	Невозможно инициализировать бэкэнд no-domain для выполнения процедуры бутстрапа групповых политик	Возможно, было произведено вмешательство в локальную политику или произошел misconfiguration. Необходимо проверить целостность пакета local-policy и настройки домена в Alterator.
E00009	Произошла ошибка при попытке запуска adp	Необходимо обратиться к руководству по устранению неполадок проекта ADP

Продолжение таблицы 37

Код	Описание	Решение
E00010	Произошел сбой при попытке получить имя домена Active Directory	Необходимо проверить работу доменной службы имен (DNS), а также доступность доменного LDAP. Для доступа к LDAP необходим работоспособный Kerberos, так что стоит проверить и его конфигурацию
E00011	Во время работы applier с пониженным уровнем привилегий произошла неполадка	Возможно, что в используемой групповой политике заданы параметры, для установки которых требуются права администратора. Это необходимо проверить и исправить объект групповой политики соответственно
E00012	Высокоуровневая ошибка инициализации бэкэнда	Необходимо проверить наличие условий для запуска бэкэнда. В случае с Samba – удостовериться, что машина введена в домен
E00013	У пользователя, запустившего программу, недостаточно прав для обновления настроек машины	Запустить программу с правами администратора
E00014	Не прошла проверка наличия билета Kerberos. Билет Kerberos нужен для доступа к сервисам домена	Проверить конфигурацию Kerberos в файле /etc/krb5.conf. Попытаться получить билет Kerberos вручную
E00015	Запрос на получение имени домена Active Directory через LDAP не прошел	Проверить возможность получения Kerberos ticket для машины. Проверить работу DNS и возможность обратиться к доменному LDAP
E00016	Утилита wbinfo не отдает SID для пользователя, для которого выполняется обновление групповых политик	Проверить целостность программы wbinfo Проверить, что машина введена в домен.
E00017	Невозможно получить список групповых политик для репликации на используемое имя пользователя	Следует удостовериться, что пользователь для которого происходит попытка получить список групповых политик, существует в домене. Также необходимо удостовериться, что проблема не вызвана misconfiguration домена
E00018	Не получилось прочитать содержимое настройки XDG_DESKTOP_DIR	Необходимо удостовериться, что XDG в системе сконфигурирован корректно и пользователь, для которого вычитывается настройка, существует
E00019	Произошла ошибка во время работы applier для пользователя	Необходимо удостовериться, что это не misconfiguration в используемой GPO. Возможно это ошибка. В таком случае необходимо создать отчет об ошибке, чтобы разработчики узнали о ней
E00020	Произошла ошибка во время работы applier для пользователя с пониженными привилегиями	Необходимо удостовериться, что это не misconfiguration в используемой GPO. Возможно это ошибка. В таком случае необходимо создать отчет об ошибке, чтобы разработчики узнали о ней
E00021	Не был получен ответ от D-Bus при попытке запустить gpoa для текущего пользователя	Следует удостовериться, что D-Bus работает корректно и демон oddjobd запущен.

Окончание таблицы 37

Код	Описание	Решение
		Необходимо удостовериться, что у текущего пользователя достаточно прав для обращения к D-Bus
E00022	Не был получен ответ от D-Bus при попытке запустить gpoa для машины	Необходимо удостовериться, что D-Bus работает корректно и демон oddjobd запущен
E00023	Не был получен ответ от D-Bus при попытке запустить gpoa для пользователя	Следует удостовериться, что D-Bus работает корректно и демон oddjobd запущен. Необходимо удостовериться, что у текущего пользователя достаточно прав для обращения к D-Bus
E00024	Ошибка во время работы машинного applier	Необходимо проверить настройки applier вручную, чтобы убедиться, что соответствующая часть ОС не поломана
E00025	Ошибка во время инициализации пользовательского applier	Необходимо проверить, что машина является частью домена и контроллер домена доступен. Следует удостовериться, что пользователь существует и что соответствующая часть ОС не поломана

9.3.6. Диагностика проблем при работе с политикой скриптов

На контроллере домена:

1) проверить работоспособность загружаемого скрипта в дистрибутиве ОС Альт СП;
2) убедиться, что кодировка файла со скриптом – UTF8, без BOM;
3) убедиться, что скрипт расположен в каталоге (GPT) применяемого объекта групповой политики (GPO);
4) убедиться, что включена групповая политика «Экспериментальные групповые политики» или политика «Управление logon-скриптами» (см. 9.2.5.6.3);
5) убедиться, что целевой компьютер, входит в подразделение (OU), к которому привязан объект групповой политики GPO.

На компьютере пользователя:

1) проверить версию `gpupdate` (политики скриптов выполняются с релиза 0.9.11-alt1);
2) убедиться, что механизм применения политик (gpupdate) запущен:

```
# gpupdate-setup status
```

3) убедиться, что служба скриптов запущена:

```
# systemctl status gpupdate-scripts-run.service
```

4) проверить содержимое каталога и права для загруженных скриптов:

```
# ls -Rl /var/cache/gpupdate_scripts_cache/
```

5) проверить состояние службы запуска скриптов пользователя (от пользователя):

```
$ systemctl --user status gpupdate-scripts-run-user.service
```

6) вывести журнал применения политик:

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

10. ДОМЕННАЯ ИНФРАСТРУКТУРА НА БАЗЕ SAMBA

10.1. Основные сведения о логической модели AD

Домен – группа компьютеров, пользователей, принтеров и других объектов, совместно использующих общую БД каталога.

Дерево доменов – иерархическая система доменов, имеющая единый корень (корневой домен).

Лес доменов – множество деревьев доменов, находящихся в различных формах доверительных отношений.

Сервер – компьютер, выполняющий определенные роли в домене.

Контроллер домена – сервер, хранящий каталог и обслуживающий запросы пользователей к каталогу. Помимо хранения данных контроллер домена может выступать в качестве одной из FSMO-ролей.

Организационное подразделение (OU) – субконтейнер в домене, который может содержать различные объекты AD: другие контейнеры, группы, аккаунты пользователей и компьютеров. OU представляет собой единицу административного управления внутри домена, на который администратор может назначить объекты групповых политик и назначить разрешения другим пользователем.

Группа (ы) – объекты, являющиеся участниками системы безопасности (security principals) и предназначенные для управления доступом к ресурсам. Каждой группе присваивается уникальный идентификатор безопасности (Security Identifier, SID), который сохраняется в течение всего срока службы.

10.2. Создание контроллера домена Active Directory на базе Samba

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).

⚠ 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.

⚠ 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.

10.2.1. Подготовка системы к установке сервера Samba AD DC

В этом подразделе перечислены требования для установки сервера Samba AD DC. Перед установкой необходимо убедиться, что система соответствует этим требованиям.

Примечание. Для установки сервера Samba AD DC нужны привилегии суперпользователя.

Примечание. При применении Samba в качестве DC AD в условиях реальной эксплуатации рекомендуется использовать два или более DC для обеспечения отказоустойчивости.

10.2.1.1. Системные требования к серверу Samba AD DC

10.2.1.1.1. RAM

Для демонстрационной/тестовой системы рекомендуется 2 Гбайт.

Для производственной установки рекомендуется не менее 4 Гбайт ОЗУ, а затем 2 Гбайт на каждую дополнительную 1000 пользователей.

Примечание. Параметр, который оказывает наибольшее влияние на требования к памяти, – это количество одновременных открытий сеансов.

10.2.1.1.2. Размеры хранилища

10 Гбайт достаточно для доменов с несколькими сотнями пользователей.

Также, при планировании размера хранилища, необходимо учесть:

- уровни журналов и политику хранения журналов;
- использование изображений/аватаров для идентификации пользователей;
- количество пользователей, машин и групп;
- место под резервные копии.

10.2.1.1.3. CPU

Для нескольких сотен пользователей достаточно 4 vCPUs.

Некоторые процессы Samba не являются многопоточными, поэтому увеличение числа процессоров не повысит производительность.

Чтобы сбалансировать нагрузку, необходимо создать второй контроллер домена в репликации с первым и применить политику балансировки нагрузки на уровне клиента.

Необходимое количество контроллеров домена зависит от нескольких параметров:

- количество сторонних приложений LDAP, подключенных к AD;
- качество кода сторонних LDAP-приложений, подключенных к AD;
- количество запросов к файловым серверам.

10.2.1.1.4. DNS

Не следует использовать существующий домен, если вы не являетесь владельцем домена. Рекомендуется использовать зарезервированный домен верхнего уровня RFC2606 (`https://tools.ietf.org/html/rfc2606`) для частных тестовых установок, например, alt.test.

Имя домена для разворачиваемого DC должно состоять минимум из двух компонентов, разделенных точкой.

ВАЖНО

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

Примечание. Имя контроллера домена Samba AD не должно превышать 15 символов (ограничение связано с `sAMAccountName` в Active Directory).

10.2.1.2. Требования к портам

Служба samba, предоставляющая функции AD DC, требует, чтобы на контроллере домена были открыты следующие порты (таблица 38).

Таблица 38 – Порты, используемые Samba AD DC

Служба	Порт	Протокол	Примечание
DNS	53	TCP и UDP	Может быть предоставлен внутренним DNS-сервером Samba или DNS-сервером Bind9
Kerberos	88	TCP и UDP	
NTP	123	UDP (опционально)	Если на контроллере домена настроен и работает NTP
End Point Mapper (DCE/RPC Locator Service)	135	TCP	
NetBIOS Name Service	137	UDP	
NetBIOS Datagram	138	UDP	
NetBIOS Session	139	TCP	
LDAP	389	TCP и UDP	
SMB over TCP	445	TCP	
Kerberos	464	TCP и UDP	Используется `kadmin` для установки и смены пароля
LDAPS	636	TCP	Если в файле `smb.conf` установлено `tls enabled = yes` (по умолчанию)
Global Catalog	3268	TCP	
Global Catalog SSL	3269	TCP	Если в файле `smb.conf` установлено `tls enabled = yes` (по умолчанию)
Dynamic RPC Ports	49152-65535	TCP	Диапазон соответствует диапазону портов, используемому в Windows Server 2008 и более поздних версиях. Чтобы вручную установить диапазон портов в Samba 4.7 и более поздних версиях, необходимо указать параметр `rpc server port` в файле `smb.conf`. Подробности смотрите в описании параметра на справочной странице `man smb.conf`

10.2.2. Создание домена

Samba поддерживает следующие серверные части DNS:

1) SAMBA_INTERNAL – встроенный сервер имен:

- используется по умолчанию при подготовке нового домена, присоединении к существующему домену или переносе домена NT4 в AD;
- прост в настройке и не требует дополнительного ПО или знаний о DNS;
- следует использовать для простых настроек DNS;

2) BIND9_DLZ – использует samba4 AD для хранения информации о зоне:

- требуется BIND 9.8 или более поздняя версия, установленная и настроенная локально на контроллере домена (DC) Samba Active Directory (AD);
- необходимы знания о DNS-сервере BIND и о том, как настроить службу;
- следует использовать для сложных сценариев DNS, которые нельзя настроить во внутреннем DNS.

Примечание. Внутренний DNS-сервер Samba не управляет кешем, поэтому он будет отправлять запрос серверу пересылки для каждого DNS-запроса, который не соответствует его домену. Бэкенд Bind-DLZ использует кэш Bind для рекурсивных запросов. Запросы на сам домен каждый раз передаются модулю DLZ, кэша на этом уровне у него нет.

ВАЖНО

Бэкенд `DNS BIND9_FLATFILE` не поддерживается.

10.2.2.1. Параметры команды разворачивания домена

Команда `samba-tool domain provision` имеет множество опций, которые можно использовать для предоставления дополнительной информации при интерактивной установке сервера. Их также можно использовать в скриптах.

Ниже описаны некоторые опции (таблица 39). Для получения более подробной информации следует обратиться к man странице samba-tool(8).

Таблица 39 – Основные опции для samba-tool domain provision

Опция	Описание
`-d DEBUGLEVEL, --debuglevel=DEBUGLEVEL`	Включить отладку
`--interactive`	Запрашивать ввод данных у пользователя (интерактивное создание домена)
`--domain=DOMAIN`	Имя домена NetBIOS (имя рабочей группы)
`--domain-guid=GUID`	Установить domainguid (иначе используется случайное значение)
`--domain-sid=SID`	Установить domainsid (иначе используется случайное значение)
`--ntds-guid=GUID`	Установить GUID объекта NTDS (иначе используется случайное значение)
`--host-name=HOSTNAME`	Установить имя хоста
`--host-ip=IPADDRESS`	Установить IPv4 IP-адрес
`--host-ip6=IP6ADDRESS`	Установить IPv6 IP-адрес
`--adminpass=PASSWORD`	Пароль основного администратора домена (иначе используется случайное значение)
`--krbtgtpass=PASSWORD`	Пароль krbtgtpass (иначе используется случайное значение)
`--dns-backend=NAMESERVER-BACKEND`	Бэкенд DNS-сервера: SAMBA_INTERNAL – встроенный сервер имен (по умолчанию), BIND9_FLATFILE – использует текстовую базу данных bind9 для хранения информации о зоне, BIND9_DLZ – использует samba4 AD для хранения информации о зоне, NONE – полностью пропускает настройку DNS (не рекомендуется)
`--dnspass=PASSWORD`	Пароль dns (иначе используется случайное значение)
`--server-role=ROLE`	Позволяет указать тип серверной роли: domain controller, dc (по умолчанию), member server, member или standalone
`--use-rfc2307`	Позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux
`--machinepass=PASSWORD`	Пароль для машины (иначе используется случайное значение)
`--plaintext-secrets`	Сохранять конфиденциальные данные в виде обычного текста на диске (по умолчанию конфиденциальные данные шифруются)
`--realm=REALM`	Задает область Kerberos (LDAP), и DNS имя домена
`--option=OPTION`	Позволяет установить параметры smb.conf из командной строки
`-s FILE, --configfile=FILE`	Файл конфигурации

10.2.2.2. Установка пакетов

Samba поддерживает серверные части Heimdal и MIT Kerberos.

Установить пакет task-samba-dc для Samba DC на базе Heimdal Kerberos:

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

или task-samba-dc-mitkrb5 для Samba DC на базе MIT Kerberos:

```
# apt-get install task-samba-dc-mitkrb5
```

Примечание. Samba на базе Heimdal Kerberos использует KDC несовместимый с MIT Kerberos, поэтому на контроллере домена на базе Heimdal Kerberos из пакета samba-dc, для совместимости с клиентской библиотекой libkrb5, в `krb5.conf` (в блоке – libdefaults) необходимо отключить использование ядерного кеша ключей – `KEYRING:persistent:%{uid}`:

```
# control krb5-conf-ccache default
```

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
```

10.2.2.3. Внутренний DNS-сервер Samba (SAMBA_INTERNAL)

Контроллер домена (DC) Samba Active Directory (AD) предоставляет внутренний DNS-сервер, который поддерживает основные функции, необходимые для AD. Он прост в настройке и не требует дополнительного программного обеспечения или знаний о DNS. Создание домена с внутренним DNS-сервером рекомендуется для простых настроек DNS.

Внутренний DNS Samba имеет следующие недостатки:

- нельзя использовать как кэширующий сервер;
- не поддерживает рекурсивные запросы;
- не поддерживает подпись транзакции с общим ключом (TSIG) (shared-key transaction signature);
- нет зоны-заглушки (stub zones);
- не поддерживает zone transfers;
- не поддерживает балансировку нагрузки циклического перебора между контроллерами домена (Round Robin load balancing among DC's).

Внутренний DNS-сервер может разрешать только DNS-зоны Active Directory (AD). Чтобы включить рекурсивные запросы других зон, следует в параметре dns forwarder в файле smb.conf указать один или несколько IP-адресов DNS-серверов, поддерживающих рекурсивное разрешение. Например:

```
dns forwarder = 192.168.0.190
```

Примечание. Samba 4.5 и более поздние версии в параметре `dns forwarder` поддерживают несколько IP-адресов, разделенных пробелами. Старые версии поддерживают один IP-адрес. Обращение ко второму и последующим DNS-серверам произойдет только в том случае, если первый не вернул никакого ответа.

Примечание. Внешний DNS-сервер можно указать при создании домена.

При создании домена с внутренним DNS-сервером нужно использовать параметр `--dns-backend=SAMBA_INTERNAL` или не указывать этот параметр вообще.

10.2.2.3.1. Выбор имени домена

Должно быть установлено правильное имя узла и домена для сервера. Для этого в файл `/etc/sysconfig/network` необходимо добавить строку:

```
HOSTNAME=dc1.test.alt
```

И выполнить команды:

```
# 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.

10.2.2.3.2. Настройка файла `/etc/resolvconf.conf`

Для корректного распознавания всех локальных DNS-запросов в файле `/etc/resolvconf.conf` должна присутствовать строка:

```
name_servers=127.0.0.1
```

Если этой строки в файле `/etc/resolvconf.conf` нет, то в конец этого файла следует добавить строку:

```
name_servers=127.0.0.1
```

и перезапустить сервис resolvconf:

```
# resolvconf -u
```

10.2.2.3.3. Восстановление к начальному состоянию Samba

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

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

⚠ Перед созданием домена необходимо обязательно удалить `/etc/samba/smb.conf`:

```
rm -f /etc/samba/smb.conf
```

10.2.2.3.4. Интерактивное создание домена

Для запуска интерактивной установки необходимо выполнить команду:

```
# samba-tool domain provision
```

В ответе на первые два вопроса нужно указать доменное имя и имя рабочей группы:

```
Realm [TEST.ALT]:
Domain [TEST]:
```

Примечание. Чтобы принять значение по умолчанию, необходимо нажать «Enter».

Далее нужно указать тип серверной роли и бэкенд DNS-сервера:

```
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
```

В DNS forwarder IP address нужно указать внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена:

```
DNS forwarder IP address (write 'none' to disable forwarding) [127.0.0.1]:  8.8.8.8
```

Задать пароль для администратора:

```
Administrator password:
Retype password:
```

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трех групп из четырех 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.

Начнется процесс конфигурации:

```
Looking up IPv4 addresses
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 and extended rights
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
The Kerberos KDC configuration for Samba AD is located at
/var/lib/samba/private/kdc.conf
A Kerberos configuration suitable for Samba AD 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 Samba AD server will be ready to use
Server Role:           active directory domain controller
Hostname:              dc1
NetBIOS Domain:        TEST
DNS Domain:            test.alt
DOMAIN SID:            S-1-5-21-3617232745-2316959539-2936900449
```

10.2.2.3.5. В пакетном режиме

Пример команды создания контроллера домена test.alt в пакетном режиме:

`# 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 --use-rfc2307`

Для пакетной установки необходимо указать следующие параметры:

- `--realm REALM_NAME` – имя области Kerberos (LDAP), и DNS имя домена;

- `--domain=DOMAIN` – имя домена (имя рабочей группы);

- `--adminpass=PASSWORD` – пароль основного администратора домена;

- `dns forwarder` – внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена;
- `--server-role=ROLE` – тип серверной роли;
- `--dns-backend=NAMESERVER-BACKEND` – бэкенд DNS-сервера;
- `--use-rfc2307` – позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux.

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трех групп из четырех 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.

Примечание. Полный список параметров можно увидеть, запустив команду:

```
# samba-tool domain provision --help
```

10.2.2.3.6. 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 (рис. 349);
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» (рис. 350);

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трех групп из четырех 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.

Имя компьютера: dc.test.alt

Интерфейсы

enp0s3

Сетевая карта: Intel Corporation 82540EM Gigabit Ethernet Controller
провод подсоединён
MAC: 08:00:27:c6:49:01

Версия протокола IP: IPv4 Включить

Конфигурация: Вручную

IP-адреса: 192.168.0.122/24 Удалить

Добавить ↑ IP: /24 (255.255.255.0) Добавить

Шлюз по умолчанию: 192.168.0.1

DNS-серверы: 127.0.0.1 8.8.8.8

Домены поиска:

(несколько значений записываются через пробел)

Дополнительно...

Создать объединение... Удалить объединение... Настроить объединение...

Создать сетевой мост... Удалить сетевой мост... Настроить сетевой мост...

Применить Сбросить

Рис. 349 – Окно инициализации домена в веб-интерфейсе ЦУС

Имя домена: test.alt

Примечание: имя домена должно соответствовать RFC 1035:

1. Имя домена должно состоять из одного или нескольких компонентов, разделённых точками.
2. Компоненты имени домена должны начинаться со строчной или прописной латинской буквы, заканчиваться на латинскую букву или цифру, содержать латинские буквы, цифры и символ «-».
3. Компонент имени домена не должен превышать 63 символов.
4. Имя домена не должно содержать компоненты «localhost», «localdomain» и «local», которые зарезервированы для служебных целей.
5. **Рекомендуется указывать домен как минимум из двух компонентов, разделённых точками.**

Примеры: domain.loc, school-33.domain, department.company

Тип домена:

ALT-домен

(домен, основанный на OpenLDAP и MIT Kerberos. Рекомендуется для аутентификации рабочих станций под управлением ALT Linux)

*Этот тип невозможно использовать, поскольку не установлен пакет **alt-domain-server**.*

Active Directory

(домен для контроллера домена Samba AD. Рекомендуется для аутентификации рабочих станций под управлением и Windows и Linux)

Дополнительные параметры:

DNS-серверы: 8.8.8.8 (адреса IP внешних серверов DNS)

Пароль администратора: •••••••• (пароль администратора домена)

Повторите пароль: •••••••• (повторите фразу)

Текущее состояние:

Служба: %(_ 'NOT OK (samba service is stopped)')
Имя домена: --
Realm: --
Имя DC: --
Сервер LDAP: --
Сервер KDC: --

FreeIPA

(домен для контроллера домена FreeIPA. Рекомендуется для аутентификации рабочих станций под управлением Linux)

*Этот тип невозможно использовать, поскольку не установлен пакет **freeipa-server, freeipa-server-dns**.*

Только DNS

(обслуживание только запросов DNS)

Внимание: изменение имени домена вступит в силу только после перезагрузки компьютера

Восстановить файл конфигурации по умолчанию (krb5.conf).

Применить Сбросить

Рис. 350 – Окно модуля «Домен»

3) после успешного создания домена, будет выведена информация о домене (рис. 351);

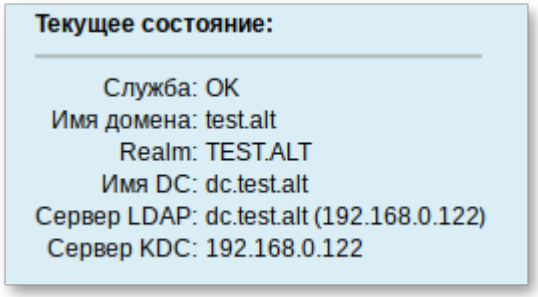


Рис. 351 – Информационное окно «Текущее состояние»

4) перегрузить сервер.

10.2.2.3.7. Запуск службы

Установить службу по умолчанию и запустить ее:

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

Примечание. Если служба после установки никаким способом не запускается, необходимо перезагрузить сервер.

Примечание. Пример файла `/etc/samba/smb.conf` после создания домена с SAMBA_INTERNAL:

```
 Global parameters
[global]
        dns forwarder = 8.8.8.8
        netbios name = DC1
        realm = TEST.ALT
        server role = active directory domain controller
        workgroup = TEST
        idmap_ldb:use rfc2307 = yes

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No

[netlogon]
        path = /var/lib/samba/sysvol/test.alt/scripts
        read only = No
```

10.2.2.4. Домен с BIND9_DLZ

Работа с внешним сервером DNS осуществляется с помощью бэкенда BIND9_DLZ и используется в следующих случаях:

- сложная схема зон DNS;

- поддержка больше одного сервера форвардинга (параметр dns forwarder на бэкенде INTERNAL работает только с одним адресом).

Если планируется настроить контроллер домена (DC) Samba Active Directory (AD) с использованием серверной части BIND9_DLZ, необходимо сначала установить и настроить DNS-сервер BIND.

На сервере должны быть установлены пакеты bind и bind-utils:

```
# apt-get install bind bind-utils
```

П р и м е ч а н и е . Во избежании появлении ошибки при запуске bind:

```
мая 03 14:25:13 dc1 named[3825]: samba_dlz: Failed to configure zone 'test.alt'
мая 03 14:25:13 dc1 named[3825]: loading configuration: already exists
мая 03 14:25:13 dc1 named[3825]: exiting (due to fatal error)
мая 03 14:39:44 dc1 named[4309]: Loading 'AD DNS Zone' using driver dlopen
```

не следует, при установке системы, задавать полное имя для DC (dc1.test.alt).

П р и м е ч а н и е . Пакет bind содержит различные утилиты, связанные с DNS, например:

- `named-checkconf` – проверка синтаксиса файлов конфигурации;
- `named-checkzone` – проверка файлов зон DNS;
- `rndc` – инструмент управления службой DNS.

Пакет bind-utils содержит различные утилиты, связанные с DNS, например:

- `dig` – многофункциональный инструмент для опроса DNS-серверов;
- `host` – преобразовать имя хоста в IP-адрес;
- `nslookup` – получить информацию DNS об удаленном сервере;
- `nsupdate` – инструмент для динамического обновления записей DNS.

Основные файлы настройки DNS:

- `/etc/named.conf` – основной файл конфигурации, содержит в себе ссылки на остальные конфигурационные файлы;
- `/etc/bind/options.conf` – файл для глобальных настроек службы;
- `/etc/bind/rndc.conf` – получить информацию DNS об удаленном сервере;
- `/etc/bind/local.conf` – файл для настроек зоны DNS;
- `/var/lib/samba/bind-dns/named.conf` – инструмент для динамического обновления записей DNS.

В таблице 40 описаны некоторые параметры конфигурационного файла `/etc/bind/options.conf`. Для получения более подробной информации следует обратиться к man странице `named.conf(5)`.

Таблица 40 – Основные параметры конфигурационного файла `/etc/bind/options.conf`

Опция	Описание
directory	Указывает каталог расположения таблиц зон
listen-on	Позволяет указать сетевые интерфейсы, которые будет прослушивать служба
allow-query	IP-адреса и подсети от которых будут обрабатываться запросы
allow-transfer	Устанавливает возможность передачи зон для slave-серверов
allow-query-cache	
allow-recursion	IP-адреса и подсети от которых будут обрабатываться рекурсивные запросы
tkey-gssapi-keytab	
minimal-responses	
max-cache-ttl	
forward	Позволяет указать каким образом сервер обрабатывает запрос клиента. При значении first DNS-сервер будет пытаться разрешать имена с помощью DNS-серверов, указанных в параметре forwarders. Если разрешить имя с помощью данных серверов не удалось, то попытаться разрешить имя самостоятельно. Если указать значение none, сервер не будет пытаться разрешить имя самостоятельно
forwarders	DNS-сервер, на который будут перенаправляться запросы клиентов
type	Тип зоны

Настройка BIND9 для работы с Samba AD:

1) отключить chroot:

```
# control bind-chroot disabled
```

2) отключить KRB5RCACHETYPE:

```
# grep -q KRB5RCACHETYPE /etc/sysconfig/bind || echo 'KRB5RCACHETYPE="none"' >> /etc/sysconfig/bind
```

3) подключить плагин BIND_DLZ:

```
# grep -q 'bind-dns' /etc/bind/named.conf || echo 'include "/var/lib/samba/bind-dns/named.conf";' >> /etc/bind/named.conf
```

4) отредактировать файл `/etc/bind/options.conf`:

- в раздел «options» добавить строки:

```
tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";
minimal-responses yes;
```

- в параметре `forwarders` указать сервера, куда будут перенаправляться запросы, на которые нет информации в локальной зоне (если этой информации нет в файле `/etc/bind/resolvconf-options.conf`):

```
forward first;
```

```
forwarders { 8.8.8.8; };
```

- в параметр `listen-on` добавить IP-адрес DNS-сервера, на котором он будет принимать запросы;
- раскомментировать параметр `allow-query` и указать в нем подсети, из которых разрешено подавать запросы;
- раскомментировать параметр `allow-recursion` и указать в нем подсети из которых будут обрабатываться рекурсивные запросы;
- в раздел «logging» добавить строку:

```
category lame-servers {null;};
```

Пример файла `/etc/bind/options.conf`:

```
options {
        version "unknown";
        directory "/etc/bind/zone";
        dump-file "/var/run/named_dump.db";
        statistics-file "/var/run/named.stats";
        recursing-file "/var/run/recursing";


        // disables the use of a PID file
        pid-file none;
        tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";
        minimal-responses yes;

        listen-on { 127.0.0.1; 192.168.0.152; };
        listen-on-v6 { ::1; };

        include "/etc/bind/resolvconf-options.conf";

        allow-query { localnets; 192.168.0.0/24; };
        allow-recursion { localnets; 192.168.0.0/24; };

        //max-cache-ttl 86400;

};

logging {
        category lame-servers {null;};
};
```

5) в файле `/etc/bind/resolvconf-options.conf` в параметре `forwarders` должен быть указан DNS-сервер, на который будут перенаправляться запросы клиентов;
6) выполнить остановку bind:

```
# systemctl stop bind
```

Если в роли DNS-сервера Samba используется Bind, то при создании домена нужно использовать параметр `--dns-backend=BIND9_DLZ`.

10.2.2.4.1. Восстановление к начальному состоянию Samba

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

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

⚠ Перед созданием домена необходимо обязательно удалить `/etc/samba/smb.conf`:

```
rm -f /etc/samba/smb.conf
```

10.2.2.4.2. Интерактивное создание домена

Для запуска интерактивной установки необходимо выполнить команду:

```
# samba-tool domain provision
```

В ответе на первые два вопроса нужно указать доменное имя и имя рабочей группы:

```
Realm [TEST.ALT]:
Domain [TEST]:
```

Примечание. Чтобы принять значение по умолчанию, необходимо нажать «Enter».

Далее нужно указать тип серверной роли и бэкенд DNS-сервера:

```
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]: BIND9_DLZ
```

Задать пароль для администратора:

```
Administrator password:
Retype password:
```

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трех групп из четырех 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.

Начнется процесс конфигурации:

```
Looking up IPv4 addresses
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 and extended rights
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
See /var/lib/samba/bind-dns/named.conf for an example configuration include file for BIND
and /var/lib/samba/bind-dns/named.txt for further documentation required for secure DNS updates
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
The Kerberos KDC configuration for Samba AD is located at /var/lib/samba/private/kdc.conf
A Kerberos configuration suitable for Samba AD 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 Samba AD server will be ready to use
Server Role:           active directory domain controller
Hostname:              dc1
NetBIOS Domain:        TEST
DNS Domain:            test.alt
DOMAIN SID:            S-1-5-21-3684382553-2825304832-3399765044
```

10.2.2.4.3. В пакетном режиме

Пример команды создания контроллера домена test.alt в пакетном режиме:

```
# samba-tool domain provision --realm=test.alt --domain test --adminpass='Pa$$word' --dns-backend=BIND9_DLZ --server-role=dc
```

Для пакетной установки необходимо указать следующие параметры:

`--realm REALM_NAME` – имя области Kerberos (LDAP), и DNS имя домена;

- `--domain=DOMAIN` – имя домена (имя рабочей группы);
- `--adminpass=PASSWORD` – пароль основного администратора домена;
- `--server-role=ROLE` – тип серверной роли;
- `--dns-backend=NAMESERVER-BACKEND` – бэкенд DNS-сервера;
- `--use-rfc2307` – позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux.

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трех групп из четырех 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.

Примечание. Полный список параметров можно увидеть, запустив команду:

```
# samba-tool domain provision --help
```

10.2.2.4.4. Запуск службы

Установить службы `samba` и `bind` по умолчанию и запустить их:

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

Примечание. Если служба `samba` после установки никаким способом не запускается, необходимо перезагрузить сервер.

Примечание. Пример файла `/etc/samba/smb.conf` после создания домена с BIND9_DLZ:

```
# Global parameters
[global]
        netbios name = DC1
        realm = TEST.ALT
        server role = active directory domain controller
        server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl, winbindd, ntp_signd, kcc, dnsupdate
        workgroup = TEST

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No

[netlogon]
        path = /var/lib/samba/sysvol/test.alt/scripts
        read only = No
```

10.2.2.4.5. Проверка зон

Следующие примеры запрашивают службу DNS о локальном хосте (127.0.0.1).

Проверка зоны перенаправления localhost:

```
# host -t A localhost 127.0.0.1
```

```
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:
localhost has address 127.0.0.1
```

Проверка реверсивной зоны `0.0.127.in-addr.arpa`:

```
# host -t PTR 127.0.0.1 127.0.0.1
```

```
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:
1.0.0.127.in-addr.arpa domain name pointer localhost.
```

10.2.3. 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]
dc = 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
```

10.2.4. Проверка работоспособности домена

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  : DC1
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 4.16.10)
SMB1 disabled -- no workgroup available
```

Создаваемые по умолчанию общие ресурсы netlogon и sysvol нужны для функционирования сервера AD и создаются в `smb.conf` в процессе развертывания/модернизации.

Проверка конфигурации DNS:

1) проверка наличия 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
```

2) проверка имен хостов:

- адрес `_kerberos._udp.*` адрес домена с точкой:

```
# host -t SRV _kerberos._udp.test.alt.
_kerberos._udp.test.alt has SRV record 0 100 88 dc1.test.alt
```

- адрес `_ldap._tcp.*` адрес домена с точкой:

```
# host -t SRV _ldap._tcp.test.alt.
_ldap._tcp.test.alt has SRV record 0 100 389 dc1.test.alt.
```

- адрес `адрес хоста.*` адрес домена с точкой:

```
# host -t A dc1.test.alt.
dc1.test.alt has address 192.168.0.122
```

Если имена не находятся, следует проверить выключение службы bind (если не включен плагин BIND9_DLZ).

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

```
# kinit administrator@TEST.ALT
```

```
Password for administrator@TEST.ALT:
Warning: Your password will expire in 41 days on Ср 24 мая 2023 09:56:24
```

Просмотр полученного билета:

```
# klist
```

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

Valid starting       Expires              Service principal
13.04.2023 09:27:40  13.04.2023 19:27:40  krbtgt/TEST.ALT@TEST.ALT
    renew until 14.04.2023 09:27:36
```

10.2.5. Заведение дополнительного DC

Системные требования к дополнительному DC такие же, как и для основного сервера Samba AD DC (см. п. 10.2.1.1).

Примечание. В терминологии контроллеров домена нет понятия PDC/BDC, т.е. все контроллеры равны, но один из них выступает владельцем ролей FSMO.

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

Все действия выполняются на узле dc2.test.alt (192.168.0.123), 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 удален):

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

4) на существующем контроллере домена завести IP-адрес для дополнительного DC:

⚠ Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

```
# samba-tool dns add 192.168.0.122 test.alt DC2 A 192.168.0.123 -Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

5) на дополнительном 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 дополнительном DC в `/etc/resolv.conf` обязательно должен быть добавлен первый DC 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
```

6) для проверки настройки запросить билет Kerberos для администратора домена:

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

⚠ Имя домена должно быть указано в верхнем регистре.

7) убедиться, что билет получен:

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

Valid starting       Expires              Service principal
19.04.2023 09:10:42  19.04.2023 19:10:42  krbtgt/TEST.ALT@TEST.ALT
    renew until 26.04.2023 09:10:38
```

8) ввести дополнительный 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"
```

При успешном завершении будет выведена информация о присоединении к домену:

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

Примечание. При использовании dns internal, необходимо указать значение `dns forwarder`, чтобы на новом сервере была настроена пересылка запросов. Форвардером может быть как вышестоящий DNS-сервер организации, так и публичные от google или yandex.

Если первый контроллер домена создавался с ключом `--rfc2307`, то и для текущего необходимо это учесть, указав параметр:

```
--option='idmap_ldb:use rfc2307 = yes'
```

9) сделать службу samba запускаемой по умолчанию и запустить ее:

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

Примечание. Для получения дополнительной информации о параметрах команды `samba-tool domain join` можно воспользоваться командой:

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

10.2.6. Контроллер домена на чтение (RODC)

Основная цель контроллера домена, доступного только на чтение (RODC – read-only domain controller), – возможность безопасной установки собственного контролера домена в удаленных филиалах, в которых сложно обеспечить физическую защиту сервера. Контроллер домена RODC содержит копию базы Active Directory, доступную только на чтение. Это означает, что никто, даже при получении физического доступа к такому контроллеру домена, не сможет изменить данные в AD (в том числе сбросить пароль администратора домена).

Основные отличия RODC от обычных контроллеров домена, доступных для записи (RWDC):

- RODC хранит копию базы AD, доступную только для чтения. Клиенты не могут вносить изменения в базу такого контролера домена;
- RODC не реплицирует данные AD на другие контроллеры домена (RWDC) (используется односторонняя репликация);
- контроллер RODC хранит полную копию базы AD, за исключением хэшей паролей объектов AD и других атрибутов, содержащих чувствительную информацию;
- при получении контроллером RODC запроса на аутентификацию от пользователя, он перенаправляет этот запрос на ближайший RWDC контроллер;
- контроллер RODC может кэшировать учетные данные некоторых пользователей (это ускоряет аутентификацию и позволяет пользователям авторизоваться на контроллере домена, даже при отсутствии связи с RWDC);
- DNS служба на RODC работает только на чтение.

Требования, которые должны быть выполнены для разворачивания RODC:

- на сервере должен быть назначен статический IP;
- уровень леса и домена должен соответствовать 2008R2. Это можно проверить, выполнив следующую команду на контролере домена:

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

```
Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
```

- в качестве DNS сервера должен быть указан ближайший RWDC контроллер.

10.2.6.1. Установка и настройка RODC

Все действия выполняются на узле rodc.test.alt (192.168.0.124), 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 удален):

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

4) На существующем контроллере домена завести IP-адрес для RODC:

⚠ Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

```
# samba-tool dns add 192.168.0.122 test.alt DC2 A 192.168.0.124 -Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

5) На RODC установить следующие параметры в файле конфигурации клиента Kerberos `/etc/krb5.conf`):

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

[realms]
TEST.ALT = {
kdc = rodc.test.alt
kdc = dc1.test.alt
default_domain = TEST.ALT
}
```

Примечание. На RODC в `/etc/resolv.conf` должен быть добавлен первый DC 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
```

6) Для проверки настройки запросить билет Kerberos для администратора домена:

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

⚠ Имя домена должно быть указано в верхнем регистре.

---

7) Убедиться, что билет получен:

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

Valid starting       Expires              Service principal
18.05.2023 09:58:43  18.05.2023 19:58:43  krbtgt/TEST.ALT@TEST.ALT
    renew until 25.05.2023 09:58:40
```

8) Ввести дополнительный DC в домен test.alt в качестве контроллера домена, доступного только для чтения (RODC):

```
# samba-tool domain join test.alt RODC -Uadministrator@TEST.ALT
--realm=test.alt --option="dns forwarder=8.8.8.8"
```

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

```
Joined domain TEST (SID S-1-5-21-578923263-1107570656-1287136478) as an RODC
```

Примечание. При использовании dns internal, необходимо указать значение `dns forwarder`, чтобы на новом сервере была настроена пересылка запросов. Форвардером может быть как вышестоящий DNS-сервер организации, так и публичные от google или yandex.

Если первый контроллер домена создавался с ключом `--rfc2307`, то и для текущего необходимо это учесть, указав параметр:

```
--option='idmap_ldb:use rfc2307 = yes'
```

9) Сделать службу samba запускаемой по умолчанию и запустить ее:

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

Тестирование репликации пароля пользователя на сервере RODC:

1) на DC1 создать пользователя и добавить его в группу Allowed RODC Password Replication Group (пароли пользователей/групп, входящих в группу Allowed RODC Password Replication Group разрешено реплицировать на RODC):

```
samba-tool user create ivanov --given-name='Иван Иванов'\
--mail-address='ivanov@test.alt'
samba-tool user setexpiry ivanov --noexpiry
samba-tool group addmembers 'Allowed RODC Password Replication Group' ivanov
```

2) на RODC проверить возможность загрузки кэша пароля, выполнив команду:

```
# samba-tool rodc preload ivanov --server=dc1.test.alt
Replicating DN CN=Иван Иванов,CN=Users,DC=test,DC=alt
Exop on[CN=Иван Иванов,CN=Users,DC=test,DC=alt] objects[1] linked_values[0]
```

10.2.6.2. Политики репликации и кэширования паролей на RODC

На RODC можно задать список пользователей, чьи хэши паролей можно или нельзя реплицировать на данный контролер домена.

Примечание. Все пользователи в кэше RODC смогут аутентифицироваться на этом контроллере домена, даже если отсутствует связь с RWDC.

Пример получения билета при отсутствии связи с RWDC (пользователь ivanov есть в кэше RODC, а пользователь kim – нет):

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

$ kinit kim
kinit: A service is not available that is required to process the request while getting initial credentials
```

По умолчанию в домене создаются две новые глобальные группы:

1) «Allowed RODC Password Replication Group»;

2) «Denied RODC Password Replication Group».

Первая группа по умолчанию пуста, а во второй содержатся административные группы безопасности, пароли пользователей которых нельзя

реплицировать и кэшировать на RODC. В группу Denied RODC Password Replication Group по умолчанию входят группы (рис. 352):

- «Cert Publishers»;
- «Domain Admins»;
- «Domain Controllers»;
- «Enterprise Admins»;
- «Group Policy Creator Owners»;
- «Read-only Domain Controllers»;
- «Schema Admins»;
- учетная запись «krbtgt».

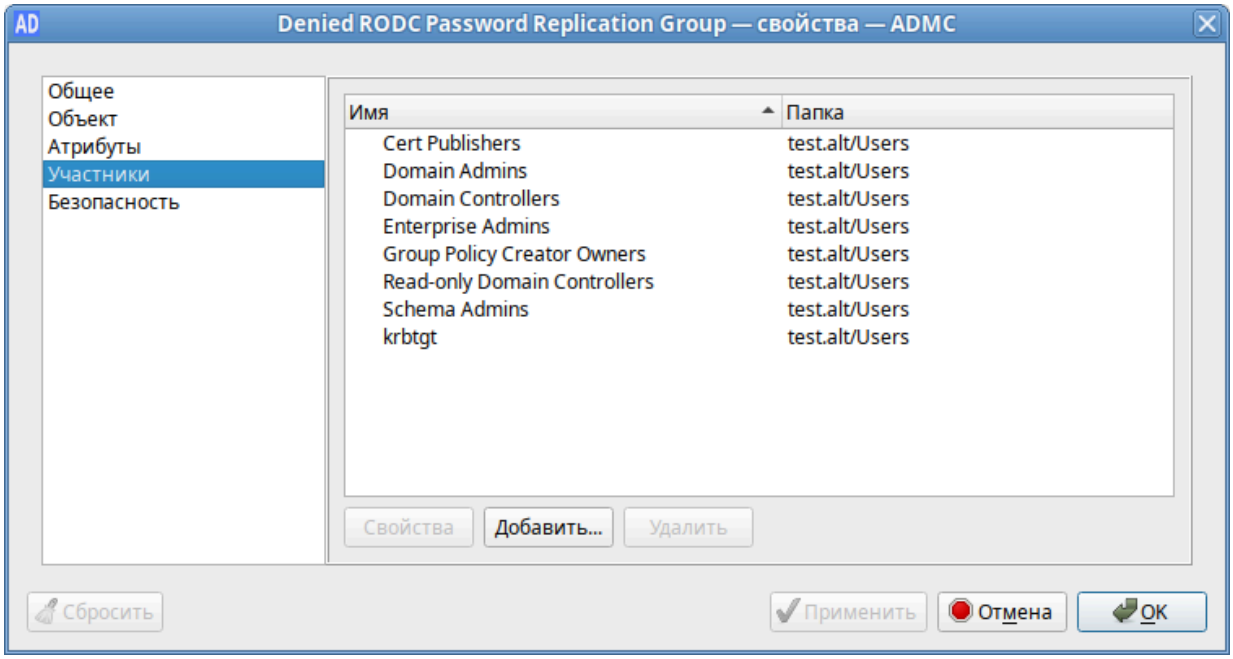


Рис. 352 – Окно участников группы «Denied RODC Password Replication Group»

В группу «Allowed RODC Password Replication Group» обычно добавляются группы пользователей филиала, в котором находится RODC.

10.2.7. Изменение DNS бэкенда контроллера домена Active Directory

Samba позволяет переключаться между бэкендом INTERNAL_DNS и BIND9_DLZ на контроллере домена Active Directory без потери данных.

10.2.7.1. Миграция с Samba INTERNAL на BIND9_DLZ

Для переключения с Samba INTERNAL на BIND9_DLZ на контроллере домена необходимо выполнить следующие шаги:

1) установить и настроить DNS-сервер BIND (см.п. 10.2.2.4);
2) остановить службу samba:

```
# systemctl stop samba
```

3) выполнить миграцию:

```
# samba_upgradedns --dns-backend=BIND9_DLZ
```

4) отключить модуль SAMBA_INTERNAL в файле `/etc/samba/smb.conf`:
   - если в файле нет параметра `server services`, добавить в секцию `global` строку:

     ```
     server services = -dns
     ```

   - если в секции `global` есть параметр `server services`, удалить опцию `dns`, например:

     ```
     server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl, winbindd, ntp_signd, kcc, dnsupdate
     ```

5) запустить службу bind и сделать ее запускаемой по умолчанию:

```
# systemctl enable --now bind
```

6) запустить службу samba:

```
# systemctl start samba
```

10.2.7.2. Миграция с BIND9_DLZ на Samba INTERNAL

Для переключения с BIND9_DLZ на Samba INTERNAL на контроллере домена необходимо выполнить следующие шаги:

1) остановить службу bind и убрать ее из автозагрузки:

```
# systemctl disable --now bind
```

2) остановить службу samba:

```
# systemctl stop samba
```

3) выполнить миграцию:

```
# samba_upgradedns --dns-backend=SAMBA_INTERNAL
```

4) отключить модуль BIND9_DLZ в файле `/etc/samba/smb.conf`:

- если в параметре server services есть только опция -dns, удалить этот параметр из файла (удалить всю строку):

  `server services = -dns`

- если в секции `global` есть параметр `server services`, добавить в него опцию `dns`, например:

  `server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl, winbindd, ntp_signd, kcc, dnsupdate, dns`

5) запустить службу `samba`:

```
# systemctl start samba
```

Примечание. Так как INTERNAL DNS – это одна из настроек по умолчанию для параметра `server services`, удаление параметра `server services` включает все серверы по умолчанию, включая DNS-сервер.

10.2.8. Отладочная информация

10.2.8.1. Настройка уровня журналирования Samba

Дополнительные сведения см. в п. 10.6.1.1.

10.2.8.2. Управление процессами

Для проверки выполнения процессов Samba можно использовать утилиту ps:

```
# ps axf | grep -E "samba|smbd|winbindd"
…
3078 ?  S   0:00 /usr/sbin/samba --no-process-group
3091 ?  S   0:00  \_ /usr/sbin/samba --no-process-group
3092 ?  S   0:00  | \_ /usr/sbin/samba --no-process-group
3096 ?  S   0:00  |  \_ /usr/sbin/samba --no-process-group
3101 ?  Ss 0:00   |   \_ /usr/sbin/smbd -D --option=server role check:inhibit=yes --foreground
3138 ?  S  0:00   |  \_ /usr/sbin/smbd -D --option=server role check:inhibit=yes --foreground
3139 ?  S  0:00   |  \_ /usr/sbin/smbd -D --option=server role check:inhibit=yes --foreground
3149 ?  S  0:00   |   \_ /usr/sbin/smbd -D --option=server role check:inhibit=yes --foreground
3150 ?  S  0:00   |   \_ /usr/sbin/smbd -D --option=server role check:inhibit=yes --foreground
…
3127 ?   Ss   0:00   | \_ /usr/sbin/winbindd -D --option=server role check:inhibit=yes --
foreground
3140 ?   S   0:00   | \_ /usr/sbin/winbindd -D --option=server role check:inhibit=yes --
foreground
…
```

Все процессы `samba`, `smbd` и `winbindd` должны быть дочерними процессами одного процесса `samba`.

Если структура процесса не отображается:

- следует проверить файлы журнала Samba. Для подробного вывода можно увеличить уровень журнала (см. п. 10.6.1.1);

- можно запустить Samba в интерактивном режиме и посмотреть на результат:

```
# samba -i
```

10.2.8.3. DNS

10.2.8.3.1. Устранение неполадок, связанных с серверной частью DNS

10.2.8.3.1.1 Внутренний DNS-сервер Samba (SAMBA_INTERNAL)

Если клиенты не могут разрешать записи из зоны DNS AD, необходимо убедиться, что на клиенте указан IP-адрес DNS-сервера, способного разрешать зону AD DNS.

Если конфигурация клиента правильная, следует убедиться, что DNS-сервер Samba работает.

Если DNS-сервер Samba не запускается, необходимо убедиться, что ни один другой процесс не использует TCP- и UDP-порт 53:

- проверить файлы журнала Samba на наличие ошибок, связанных с DNS;
- убедиться, что никакой другой процесс не прослушивает TCP- и UDP-порт 53, например:

```
# ss -tulpn | grep ":53"
```

Если порт 53 занят другим процессом, необходимо:

- остановить службу, прослушивающую порт 53, и отключить ее автоматический запуск во время загрузки;
- перезапустить Samba.

10.2.8.3.1.2 Samba с BIND9_DLZ

Каталог `/var/lib/samba/bind-dns` создается только в том случае, если произошло одно из следующих трех событий:

- при создании контроллера домена использовался параметр `--dns-backend=BIND9_DLZ`;
- при подключении к домену использовался параметр `--dns-backend=BIND9_DLZ`;
- домен был обновлен до Bind9 с помощью команды `samba_upgradedns` и опции `--dns-backend=BIND9_DLZ`.

10.2.9. Удаление контроллера домена

В некоторых ситуациях необходимо навсегда удалить контроллер домена из Active Directory. Если для обычного участника домена достаточно просто удалить соответствующую учетную запись, то чтобы удалить контроллер из домена требуется понизить его роль (demoting).

Если роль контроллера домена будет понижена неправильно, домен может стать нестабильным. Например:

- могут начаться сбои репликации;
- оставшиеся контроллеры домена могут замедлять свою работу из-за тайм-аутов и неудачных попыток репликации;
- вход в систему доменных пользователей может завершиться ошибкой или занять больше времени.

10.2.9.1. Понижение роли онлайн-контроллера домена

Если удаляемый контроллер домена все еще работает правильно, для понижения его роли необходимо выполнить следующие действия (в примере понижается роль DC3):

1) авторизоваться на контроллере домена под локальным пользователем;
2) убедиться, что контроллер не владеет никакими ролями FSMO:

```
# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
InfrastructureMasterRole owner: CN=NTDS Settings,CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
RidAllocationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainNamingMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
```

Если контроллеру домена принадлежит одна или несколько ролей FSMO,

передать их другому контроллеру домена;

3) вывести `objectGUID` контроллера домена:

```
# ldbsearch -H /var/lib/samba/private/sam.ldb '(invocationId=*)' --cross-ncs objectguid | grep -A1 DC3
dn: CN=NTDS Settings,CN=DC3,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
objectGUID: 512f03b4-7042-434d-93c0-61dd6a2ea895
```

4) для того чтобы убедиться, что все записи DNS были удалены после понижения роли контроллера домена, необходимо знать имя хоста, IP-адрес и objectGUID контроллера домена;

5) понизить DC:

```
# samba-tool domain demote -Uadministrator
Using dc1.test.alt as partner server for the demotion
Password for [TEST\administrator]:
Deactivating inbound replication
Asking partner server dc1.test.alt to synchronize from us
Changing userControl and container
Removing Sysvol reference: CN=DC3,CN=Enterprise,CN=Microsoft System Volumes,CN=System,CN=Configuration,DC=test,DC=alt
Removing Sysvol reference: CN=DC3,CN=test.alt,CN=Microsoft System Volumes,CN=System,CN=Configuration,DC=test,DC=alt
Removing Sysvol reference: CN=DC3,CN=Domain System Volumes (SYSVOL share),CN=File Replication Service,CN=System,DC=test,DC=alt
Removing Sysvol reference: CN=DC3,CN=Topology,CN=Domain System Volume,CN=DFSR-GlobalSettings,CN=System,DC=test,DC=alt
updating ForestDnsZones.test.alt keeping 2 values, removing 1 values
updating test.alt keeping 6 values, removing 1 values

…
Demote successful
```

6) остановить службу `samba`:

```
# systemctl stop samba
```

7) если этот контроллер работал, как доменный сервер DNS:

- остановите службу DNS:

```
# systemctl stop bind
```

- убедитесь, что члены домена и контроллеры домена больше не используют этот хост для разрешения зон AD DNS.

10.2.9.2. Понижение автономного контроллера домена

В определенных ситуациях, например, при сбое оборудования, из домена необходимо удалить контроллер домена, который больше недоступен. В этом случае понизить уровень контроллера домена, можно на оставшемся работающий контроллер домена Samba.

ВАЖНО

Эта процедура должна выполняться только в том случае, если контроллер домена, который нужно понизить, больше не подключен к AD, и его нельзя понизить так, как описано в п. 10.2.9.1. Это гарантирует, что все изменения, такие как изменения пароля, будут реплицированы на другой контроллер домена. В противном случае такие изменения будут потеряны. Вы можете получить список изменений с помощью Samba-инструмента ldapcmp. При описанной ниже процедуре все изменения (например, изменения паролей) не будут реплицированы на работающий DC.

ВАЖНО

Нельзя понизить статус автономного удаленного контроллера домена с контроллера домена, на котором работает Samba 4.4 или более ранней версии.

Для понижения статуса неработающего контроллера домена необходимо выполнить следующие действия (в примере понижается статус DC3):

1) авторизоваться на работающем контроллере домена;
2) убедиться, что понижаемый контроллер не владеет никакими ролями FSMO:

```
# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
InfrastructureMasterRole owner: CN=NTDS Settings,CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
RidAllocationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainNamingMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
```

Если понижаемому контроллеру домена принадлежит одна или несколько

ролей FSMO, захватить их локальным контроллером домена;

3) убедиться, что понижаемый контроллер домена отключен;

4) вывести `objectGUID` контроллера домена:

```
# ldbsearch -H /var/lib/samba/private/sam.ldb '(invocationId=*)' --cross-ncs objectguid | grep -A1 DC3
dn: CN=NTDS Settings,CN=DC3,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
objectGUID: 512f03b4-7042-434d-93c0-61dd6a2ea895
```

Для того чтобы убедиться, что все записи DNS были удалены после понижения роли контроллера домена, необходимо знать имя хоста, IP-адрес и objectGUID контроллера домена;

Примечание. Команды выполняются на действующем контроллере домена.

5) понизить статус удаленного контроллера домена:

```
# samba-tool domain demote --remove-other-dead-server=DC3
```

6) если пониженный контроллер работал как доменный сервер DNS, убедиться, что члены домена и контроллеры домена больше не используют этот хост для разрешения зон AD DNS.

ВАЖНО

Не следует подключать к сети контроллер, выведенный по данной процедуре. Иначе ваш домен станет несогласованным.

10.2.9.3. Проверка

Действия, описанные в этом разделе, предназначены только для проверки и ручного удаления оставшихся записей, если процесс понижения контроллера не удался.

На машине, введенной в домен, запустить модуль удаленного управления базой данных конфигурации (ADMC) (подробнее см. п. 9.2.4). Выбрать запись Domain Controllers и убедиться, что пониженный контроллер домена был удален (рис. 353).

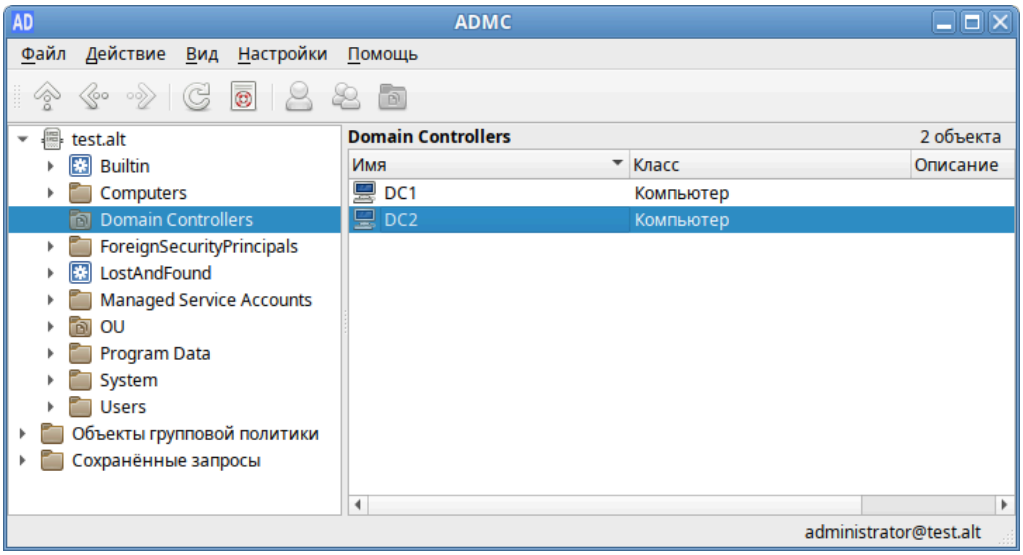


Рис. 353 – Модуль удаленного управления базой данных конфигурации (ADMC)

Проверить, что контроллер домена был понижен, можно также в RSAT (см. п. 10.7.10). Для этого на машине Windows введенной в домен:

1) открыть приложение «Active Directory – пользователи и компьютеры», перейти к записи «Контроллеры домена» и убедиться, что пониженный контроллер домена был удален (рис. 354).

   Если запись все еще присутствует в списке, ее можно удалить вручную, выбрав в контекстном меню записи пункт «Удалить»;

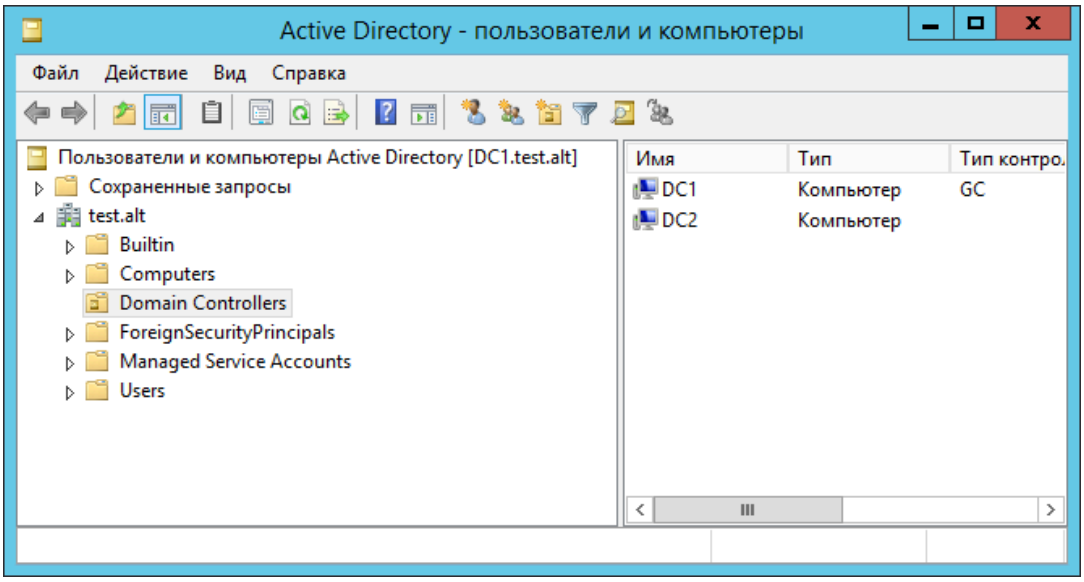


Рис. 354 – Окно приложения «Active Directory – пользователи и компьютеры»

2) открыть приложение «Active Directory – сайты и службы», и убедиться, что контроллер домена с пониженным статусом больше не указан ни в одной записи сайта Active Directory (рис. 355).

Если запись все еще присутствует в списке, ее можно удалить вручную, выбрав в контекстном меню записи пункт «Удалить»;

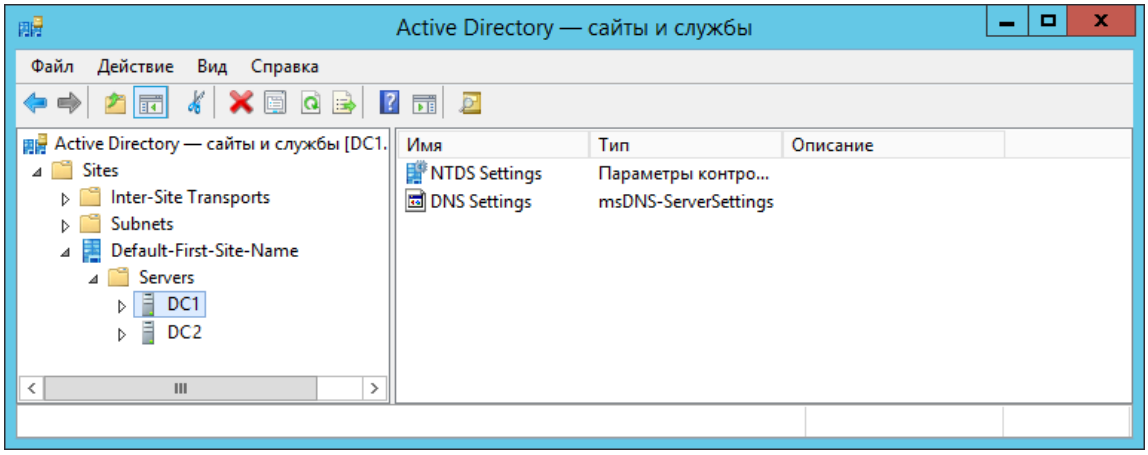


Рис. 355 – Окно приложения «Active Directory – сайты и службы»

3) открыть приложение «DNS», и убедиться, что имя хоста, IP-адрес и objectGUID контроллера домена больше не используются ни в одной записи DNS в любой зоне AD DNS (рис. 356).

Если записи все еще присутствуют в списке, их можно удалить вручную, выбрав в контекстном меню записи пункт «Удалить».

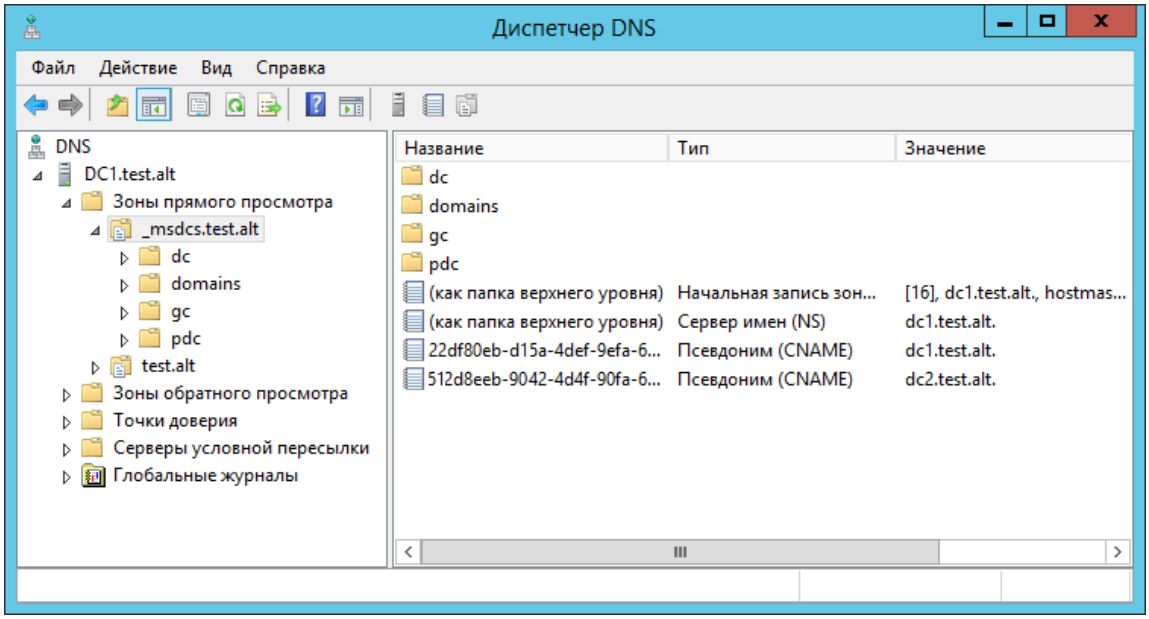


Рис. 356 – Окно «Диспетчер DNS»

10.2.10. Управление политиками паролей домена

В AD настройки пароля управляют:

- минимальные требования к длине и сложности пароля;
- длина истории паролей: предотвращает повторное использование пользователем предыдущего пароля;
- минимальный и максимальный срок действия пароля: как часто пользователь может/должен менять свой пароль;
- блокировка учетной записи: пороговое значение неудачных попыток входа в систему перед блокировкой учетной записи пользователя и продолжительность блокировки.

Управление политиками паролей домена производится на контроллере домена.

10.2.10.1. Глобальные парольные политики

Просмотр текущих параметров политик паролей:

```
# samba-tool domain passwordsettings show
Password information for domain 'DC=test,DC=alt'

Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 7
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

Изменить параметр политик паролей:

```
# samba-tool domain passwordsettings set <параметр>
```

Возможные параметры:

- `--complexity=on|off|default` – должен ли пароль отвечать требованиям сложности (по умолчанию on);
- `--store-plaintext=on|off|default` – хранить пароли используя обратимое шифрование (по умолчанию off);

- --history-length=целое число|default – число хранимых предыдущих паролей пользователей (требование неповторяемости паролей) (по умолчанию 24);
- --min-pwd-length=целое число|default – минимальное количество символов в пароле (по умолчанию 7);
- --min-pwd-age=целое число|default – минимальный срок действия пароля (по умолчанию 1);
- --max-pwd-age=целое число|default – максимальный срок действия пароля (по умолчанию 43);
- --account-lockout-duration=целое число|default – интервал времени (в минутах), в течение которого возможность аутентификации для пользователя, превысившего количество попыток входа, будет заблокирована (по умолчанию 30);
- --account-lockout-threshold=целое число|default – допустимое количество неудачных попыток ввода пароля перед блокировкой учетной записи (по умолчанию 0 – никогда не блокировать);
- --reset-account-lockout=целое число|default – интервал времени (в минутах), по истечении которого записанное количество попыток начинается заново (по умолчанию 30).

Изменить минимальную длину пароля и количество неудачных попыток входа в систему:

```
# samba-tool domain passwordsettings set --min-pwd-length=7 --account-lockout-threshold=3
Minimum password length changed!
Account lockout threshold changed!
All changes applied successfully!
```

Примечание. Определить, что учетная запись пользователя заблокирована после нескольких неудачных попыток входа в систему можно, если badPwdCount достиг своего порога и для пользователя существует параметр lockoutTime:

```
# samba-tool user show ivanov
…
badPwdCount: 3
badPasswordTime: 133287267974607690
lockoutTime: 133287267974607690
…
```

Чтобы разблокировать пользователя, необходимо отредактировать объект учетной записи пользователя, установив для атрибута `lockoutTime` значение 0:

```
# samba-tool user edit ivanov
Modified User 'ivanov' successfully

# samba-tool user show ivanov
…
badPasswordTime: 133287277878749270
lockoutTime: 0
…
```

Разблокировать пользователя также можно в модуле удаленного управления базой данных конфигурации (ADMC) (подробнее см. п. 9.2.4) (рис. 357).

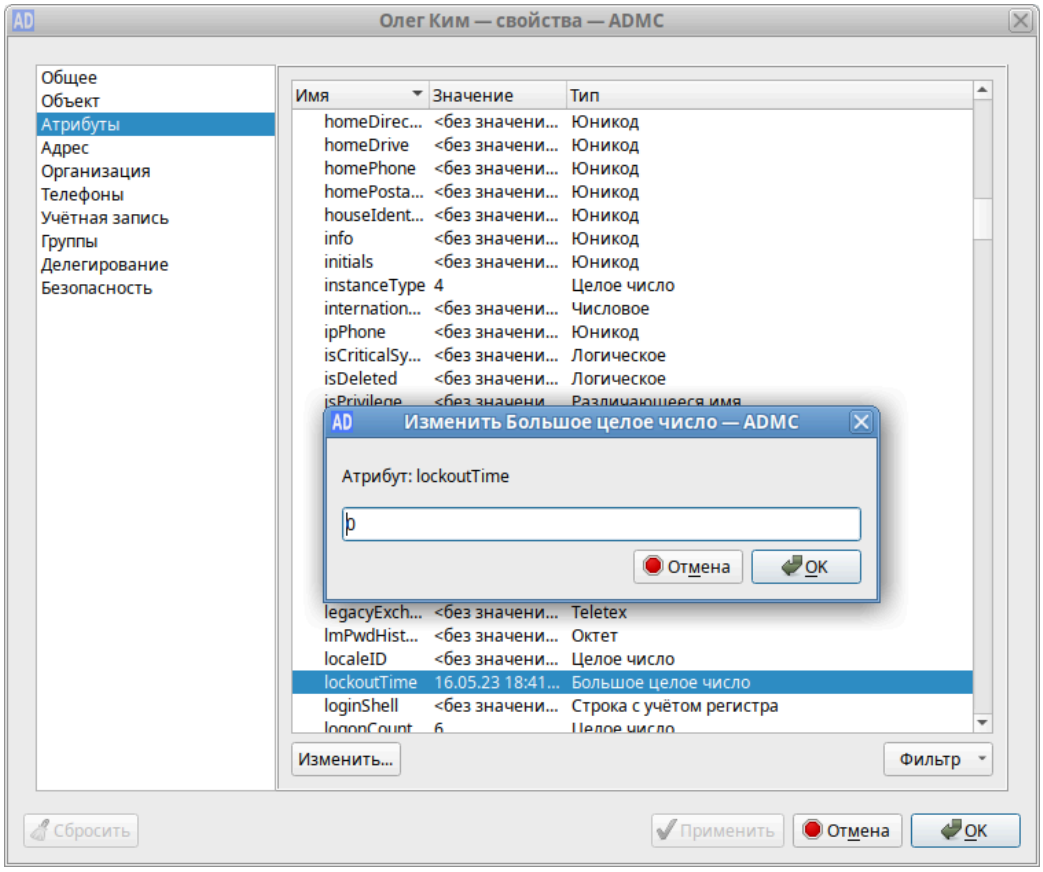


Рис. 357 – Окно модуля удаленного управления конфигурации (ADMC)

10.2.10.2. Объекты настроек паролей (PSO)

PSO позволяют администраторам AD переопределять параметры политики паролей домена и настраивать более точные параметры паролей для конкретных пользователей или групп пользователей. Например, для определенных пользователей можно установить требование минимальной длины пароля, ослабить ограничения сложности для других пользователей и т.д. PSO могут применяться к

группам или к отдельным пользователям.

Изменить PSO:

```
# samba-tool domain passwordsettings pso <подкоманда>
```

Доступные подкоманды:

1) `apply` – применить политику паролей PSO к пользователю или группе;
2) `create` – создать новый объект настроек пароля (PSO);
3) `delete` – удалить объект настроек пароля (PSO);
4) `list` – вывести список всех объектов настроек пароля (PSO);
5) `set` – изменить объект настроек пароля (PSO);
6) `show` – показать детали объекта настроек пароля;
7) `show-user` – отобразить настройки пароля, которые применяются к пользователю;
8) `unapply` – обновить PSO, чтобы он больше не применялся к пользователю или группе.

Создание правила пароля для пользователя ivanov:

```
# samba-tool domain passwordsettings pso create PwPolicyUser 1 --min-pwd-length=10
Not all password policy options have been specified.
For unspecified options, the current domain password settings will be used as the default values.
PSO successfully created: CN=PwPolicyUser,CN=Password Settings Container,CN=System,DC=test,DC=alt
Password information for PSO 'PwPolicyUser'
Precedence (lowest is best): 1
Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 10
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

```
# samba-tool domain passwordsettings pso apply PwPolicyUser ivanov
The following PSO settings apply to user 'ivanov'.
```

```
Password information for PSO 'PwPolicyUser'

Precedence (lowest is best): 1
Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 10
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30

Note: PSO applies directly to user (any group PSOs are overridden)
```

К одному и тому же пользователю может применяться множество различных PSO (напрямую или через группы). Если несколько PSO применяются к одному и тому же пользователю, в основном вступает в силу PSO с наименьшим приоритетом. Однако PSO, которые применяются непосредственно к пользователю, всегда превосходят PSO, унаследованные через членство в группе. Чтобы увидеть, какой PSO действует для данного пользователя, используется команда настройки пароля домена `samba-tool pso show-user`:

```
# samba-tool domain passwordsettings pso show-user kim
No PSO applies to user 'kim'. The default domain settings apply.
Refer to 'samba-tool domain passwordsettings show'.
```

Если для пользователя не создано правила, будет применяться правило по умолчанию.

Примечание. Необходимо одновременно настраивать политику паролей для всех остальных пользователей, иначе есть риск снижения производительности при настройке PSO и применении их к пользователям. Например:

```
# samba-tool domain passwordsettings pso create PwPolicyAdmins 1 --min-pwd-length=16
# samba-tool domain passwordsettings pso apply PwPolicyAdmins "domain admins"
# samba-tool domain passwordsettings pso create PwPolicyUsers 3 --min-pwd-length=8
# samba-tool domain passwordsettings pso apply PwPolicyUsers "domain admins"
# samba-tool domain passwordsettings pso create PwPolicyService 2 --min-pwd-length=24
# samba-tool domain passwordsettings pso apply PwPolicyService "domain admins"
```

Если объектов PSO вообще нет, производительность не снижается.

Расчет PSO включает в себя расчет членства пользователя в группах, что является довольно дорогостоящим расчетом. Если PSO применяется непосредственно к пользователю (а не к группе), то дорогостоящие групповые вычисления пропускаются. Однако применение PSO непосредственно к пользователям делает управление PSO более сложным по сравнению с применением PSO к группам.

10.3. Репликация

Репликация Active Directory – метод, посредством которого изменения в базе службы каталогов на одном контроллере домена передаются другим контроллерам.

В Samba все, что хранится внутри AD, реплицируется между контроллерами домена (пользователи, группы и записи DNS).

В настоящее время Samba не поддерживает протокол репликации распределенной файловой системы (DFS-R), используемый для репликации Sysvol. Методы решения этой проблемы см. в п. 10.3.3.

10.3.1. Настройка репликации

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

⚠ Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

Команда репликации:

```
# samba-tool drs replicate <destinationDC> <sourceDC> <NC> [options]
```

Процедура двусторонней репликации:

1) репликация с первого контроллера домена на второй:

```
# samba-tool drs replicate dc2.test.alt dc1.test.alt dc=test,dc=alt -Uadministrator
Password for [TEST\administrator]:
Replicate from dc1.test.alt to dc2.test.alt was successful.
```

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

2) репликация на первый контроллер домена со второго:

```
# samba-tool drs replicate dc1.test.alt dc2.test.alt dc=test,dc=alt -Uadministrator
Password for [TEST\administrator]:
Replicate from dc2.test.alt to dc1.test.alt was successful.
```

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 можно запустить команду на DC (подробнее см. п. 10.3.2):

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

Примечание. Если репликация на Windows не работает, следует добавить в Active Directory Sites and Services новое соединение Active Directory, реплицировать на DC, подождать минут 5 и попробовать реплицировать с Samba на Windows.

10.3.2. Проверка статуса репликации

10.3.2.1. Отображение статуса репликации на контроллере домена Samba

Команда `samba-tool drs showrepl` отображает установленные связи с другими контроллерами домена в лесу AD. Соединения отображаются с точки зрения контроллера домена, на котором запускается команда.

Пример:

```
# samba-tool drs showrepl
Default-First-Site-Name\DC2
DSA Options: 0x00000001
DSA object GUID: 899a8050-fd2f-44f6-9f19-53f7f63b0348
DSA invocationId: ac8f1710-0f0b-401a-aa8b-4bdf30517f6b

==== INBOUND NEIGHBORS ====

DC=DomainDnsZones,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ Wed Apr 19 11:09:03 2023 EET was successful
        0 consecutive failure(s).
        Last success @ Wed Apr 19 11:09:03 2023 EET

CN=Configuration,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
```

```
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ Wed Apr 19 11:09:03 2023 EET was successful
        0 consecutive failure(s).
        Last success @ Wed Apr 19 11:09:03 2023 EET

DC=ForestDnsZones,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ Wed Apr 19 11:09:03 2023 EET was successful
        0 consecutive failure(s).
        Last success @ Wed Apr 19 11:09:03 2023 EET

DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ Wed Apr 19 11:09:04 2023 EET was successful
        0 consecutive failure(s).
        Last success @ Wed Apr 19 11:09:04 2023 EET

CN=Schema,CN=Configuration,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ Wed Apr 19 11:09:04 2023 EET was successful
        0 consecutive failure(s).
        Last success @ Wed Apr 19 11:09:04 2023 EET

==== OUTBOUND NEIGHBORS ====

DC=DomainDnsZones,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
        Last success @ NTTIME(0)

CN=Configuration,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
        Last success @ NTTIME(0)

DC=ForestDnsZones,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
        Last success @ NTTIME(0)

DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
        Last success @ NTTIME(0)
```

```
CN=Schema,CN=Configuration,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
        Last success @ NTTIME(0)

==== KCC CONNECTION OBJECTS ====

Connection --
    Connection name: a46c895e-658b-463e-9ab5-a1c237fca4b1
    Enabled        : TRUE
    Server DNS name : dc1.test.alt
    Server DN name : CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
        TransportType: RPC
        options: 0x00000001
Warning: No NC replicated for Connection!
```

Связи отображаются в разделах `INBOUND NEIGHBORS` и `OUTBOUND NEIGHBORS`. В каждом разделе должно быть по 5 пунктов:

```
CN=Schema,CN=Configuration,DC=test,DC=alt
DC=ForestDnsZones,DC=test,DC=alt
DC=test,DC=alt
DC=DomainDnsZones,DC=test,DC=alt
CN=Configuration,DC=test,DC=alt
```

В разделе `INBOUND NEIGHBORS` в пункте `Last attempt` должны стоять актуальные дата и время, идентичные указанным в строке `Last success` (отображает время последней репликации).

Должно быть `0 consecutive failure(s)`.

Если в разделе `INBOUND NEIGHBORS` есть записи:

```
Last attempt @ NTTIME(0) was successful
…
Last success @ NTTIME(0)
```

необходимо подождать (соединение устанавливается).

В разделе `KCC CONNECTION OBJECTS` был приведен список всех контроллеров домена, чьи KCC установили соглашения о репликации с текущим контроллером домена. В случае, когда контроллер домена только-только был добавлен в домен и запущен, может пройти до 15 минут до того, как соглашения будут установлены.

Примечание. Предупреждение:
`No NC replicated for Connection!`

можно игнорировать. Оно появляется из-за того, что при регистрации нового DC Samba неверно устанавливает некоторые флаги репликации.

Так же можно проверить репликацию LDAP:

```
# samba-tool ldapcmp ldap://dc1.test.alt ldap://dc2.test.alt -Uadministrator
Password for [TEST\administrator]:

* Comparing [DOMAIN] context...

* Objects to be compared: 274

* Result for [DOMAIN]: SUCCESS

* Comparing [CONFIGURATION] context...

* Objects to be compared: 1625

* Result for [CONFIGURATION]: SUCCESS

* Comparing [SCHEMA] context...

* Objects to be compared: 1739

* Result for [SCHEMA]: SUCCESS

* Comparing [DNSDOMAIN] context...

* Objects to be compared: 41

* Result for [DNSDOMAIN]: SUCCESS

* Comparing [DNSFOREST] context...

* Objects to be compared: 18

* Result for [DNSFOREST]: SUCCESS
```

Данная команда сравнит значения атрибутов объектов всего каталога на DC1 и DC2. В ряде случаев атрибуты объектов на разных контроллерах могут отличаться, и в выводе команды, это будет видно. Но не во всех случаях это будет признаком проблемы с репликацией.

10.3.2.2. Отображение статусов репликации на контроллере домена Windows

Для отображения статуса входящей репликации на контроллере домена Windows можно использовать утилиту `repadmin`:

```
> repadmin /showrepl
```

Windows не поддерживает отображение статусов исходящих подключений репликации. Чтобы обойти эту проблему, можно отобразить статусы входящих подключений на контроллерах домена Samba, на которые реплицируется контроллер домена Windows:

1) найти в AD всех партнеров репликации Windows DC. Например, чтобы отобразить партнеров по репликации контроллера домена с именем WindowsDC:

```
# ldbsearch -H /var/lib/samba/private/sam.ldb '(fromServer=*CN=WindowsDC*)' --cross-ncs dn
# record 1
dn: CN=a46c895e-658b-463e-9ab5-a1c237fca4b1,CN=NTDS Settings,CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt

# returned 1 records
# 1 entries
# 0 referrals
```

В этом примере возвращается один партнер по репликации (имя хоста: DC2). Имя хоста партнера по репликации является частью возвращаемого отличительного имени (DN);

2) на каждом контроллере домена Samba, полученном на предыдущем шаге, выполнить команду `samba-tool drs showrepl` для отображения статуса репликации каталога.

Необходимо убедиться, что каждый реплицируемый контейнер каталогов указан для контроллера домена Windows в разделе `INBOUND NEIGHBORS` на контроллере домена Samba, а статусы успешны.

10.3.3. Двунаправленная репликация SysVol

Каталог Sysvol присутствует на всех контроллерах домена AD и используется для хранения логон скриптов и объектов групповых политик. Отсутствие репликации этого каталога приведет к неправильной работе групповых политик и сценариев входа.

Samba в своем текущем состоянии не поддерживает репликацию SysVol через DFS-R (репликация распределенной файловой системы) или более старую FRS (службу репликации файлов), используемую в Windows Server 2000/2003 для

репликации SysVol. В настоящее время для репликации SysVol можно использовать один из следующих обходных путей:

- двунаправленная репликация SysVol на основе Rsync/Unison (только Samba DC);
- двунаправленная репликация SysVol на основе Rsync/osync (только Samba DC).

ВАЖНО

Необходимо синхронизировать `idmap.ldb` из контроллера домена, имеющего роль FSMO PDC_Emulator, со всеми другими контроллерами домена. Это гарантирует, что все контроллеры домена будут использовать одни и те же идентификаторы. Если файл `idmap.ldb` не синхронизируется, на каждом контроллере домена будут разные идентификаторы.

10.3.3.1. Настройка двунаправленной репликации SysVol на базе Rsync/Unison

Исходные данные:

- все команды выполняются от пользователя root;
- первый контроллер домена – DC1;
- второй контроллер домена – DC2 (уже присоединен к домену);
- sysvol расположен в `/var/lib/samba/` как на DC1, так и на DC2;
- rsync расположен в `/usr/bin/rsync`;
- unison расположен в `/usr/bin/unison`;
- журнал sysvolsync пишется в файл `/var/log/sysvol-sync.log`.

Примечание. Предварительно должно быть настроено беспарольное межсерверное взаимодействие (подробнее, см. п. 10.7.12).

На первом контроллере домена (DC1):

1) установить пакеты rsync и unison:

```
# apt-get install rsync unison
```

2) при низких скоростях в сети, `unison` может некорректно работать, поэтому при повторной его работе будет использоваться ранее созданное подключение по ssh, для этого:

```
# mkdir ~/.ssh/ctl
# cat < < EOF > ~/.ssh/ctl/config
```

```
Host *
ControlMaster auto
ControlPath ~/.ssh/ctl/%h_%p_%r
ControlPersist 1
EOF
```

3) создать каталог `/root/.unison/`:

```
# mkdir /root/.unison
```

4) для определения политики синхронизации создать файл конфигурации unison `/root/.unison/default.prf` с следующим содержимым:

```
# Список каталогов, которые будут синхронизированы
root = /var/lib/samba
root = ssh://root@DC2.test.alt//var/lib/samba
# Список подкаталогов, которые нужно синхронизировать
path = sysvol

auto=true
batch=true
perms=0
rsync=true
maxthreads=1
retry=3
confirmbigdeletes=false
servercmd=/usr/bin/unison
# использовать rsync только для больших файлов??
copythreshold=1000
copyprog = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --inplace --
compress
copyprogrest = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --
partial --inplace --compress
copyquoterem = true
copymax = 1

# Сохранять журнал с результатами работы в отдельном файле
logfile = /var/log/sysvol-sync.log
```

5) создать файл для записи журнала репликации (необходимо настроить ротацию логов для этого файла, так как размер журнала не контролируется): # `touch /var/log/sysvol-sync.log`

На втором контроллере домена (DC2) установить пакеты rsync и unison:

```
# apt-get install rsync unison
```

Сделать резервную копию каталога sysvol, и запустить команду синхронизации:

```
# /usr/bin/rsync -XAavz --log-file /var/log/sysvol-sync.log --delete-after -f"+ */" -f"- *" /var/lib/samba/sysvol root@dc2.test.alt:/var/lib/samba && /usr/bin/unison
```

Утилита rsync создает структуры каталогов с расширенными атрибутами, а затем утилита unison копирует только эти расширенные атрибуты файлов.

На DC1 включить синхронизацию по расписанию:

```
# crontab -e
*/5 * * * * /usr/bin/unison -silent
```

Повторная синхронизация каталога:

- отключить синхронизацию по расписанию на DC1;
- rsync и unison не должны выполняться в данный момент (можно проверить командой ps -aux);
- удалить хеш-файлы на DC1 и DC2 в /root/.unison;
- проверить sysvol и повторить синхронизацию;
- убедиться, что синхронизация выполнена успешно;
- включить синхронизацию по расписанию на DC1.

Если контроллеров домена больше чем два, можно создать больше заданий для cron на DC1:

1) скопировать файл /root/.inison/default.prf в другой файл, например: /root/.inison/sync_dc2.prf;
2) в файле /root/.inison/dc2.prf изменить значение параметра root;
3) повторить шаги 1 и 2 для всех контроллеров домена;
4) изменить задание на синхронизацию по расписанию на DC1:

```
* * * * * /usr/bin/unison sync_dc2 -silent
* * * * * /usr/bin/unison sync_dc3 -silent
…
```

10.3.3.2. Настройка двунаправленной репликации SysVol на базе Rsync/osync

Исходные данные:

- все команды выполняются от пользователя root;

- первый контроллер домена – DC1;
- второй контроллер домена – DC2 (уже присоединен к домену);
- sysvol расположен в `/var/lib/samba/` как на DC1, так и на DC2;
- rsync расположен в `/usr/bin/rsync`;
- osync расположен в `/usr/bin/osync`;
- журнал sysvolsync пишется в файл `/var/log/osync_*.log`;
- настроено беспарольное взаимодействие между rootами всех контроллеров домена (см. п. 10.7.12).

На первом контроллере домена (DC1):

1) установить пакеты rsync и osync:

```
# apt-get install rsync osync
```

2) отредактировать файл `/etc/osync/sync.conf`:

```
#!/usr/bin/env bash
INSTANCE_ID="sync_sysvol"
 # Путь до SysVol на текущем сервере
INITIATOR_SYNC_DIR="/var/lib/samba/sysvol"
 # Путь до SysVol на удаленном сервере
TARGET_SYNC_DIR="ssh://root@DC2:22//var/lib/samba/sysvol"
 # ssh ключ root
SSH_RSA_PRIVATE_KEY="/root/.ssh/id_ed25519"
 # Удаленные хосты которые osync пингует перед стартом
REMOTE_3RD_PARTY_HOSTS=""
 # Сохранять xattr
PRESERVE_ACL=yes
 # Сохранять xattr
PRESERVE_XATTR=yes
 # Сохранять резервную копию удаленных файлов
SOFT_DELETE=yes
DESTINATION_MAILS="your@test.alt"
REMOTE_RUN_AFTER_CMD="/usr/bin/samba-tool ntacl sysvolreset"
```

На втором контроллере домена (DC2) установить пакет rsync:

```
# apt-get install rsync
```

Сделать резервную копию `sysvol` и запустить команду синхронизации:

```
# /usr/bin/osync.sh /etc/osync/sync.conf --dry --verbose
```

Если команда выполнилась без ошибок, можно удалить параметр `--dry` и запустить команду синхронизации снова:

```
# /usr/bin/osync.sh /etc/osync/sync.conf --verbose
```

В результате sysvol будет синхронизирован на обоих серверах.

Примечание. Если в файле sysvol параметры SOFT_DELETE (сохранять резервные копии удаленных файлов) и CONFLICT_BACKUP (сохранять резервные копии файлов на целевой реплике, если они обновлены из исходной реплики) установлены в значение yes, то на источнике и получателе репликации необходимо создать каталоги .osync_workdir/deleted и .osync_workdir/backup:

```
# mkdir /var/lib/samba/sysvol/.osync_workdir/deleted
# mkdir /var/lib/samba/sysvol/.osync_workdir/backup
```

На DC1 включить синхронизацию по расписанию:

```
# crontab -e
*/5 * * * * root  /usr/local/bin/osync.sh /etc/osync/sync.conf --silent
```

Если при попытке синхронизировать каталог возникают проблемы необходимо:

- отключить синхронизацию по расписанию на DC1;
- убедиться, что rsync и osync не выполняются в данный момент (можно проверить, выполнив команду ps -aux| grep sync);
- удалить хеш-файлы .osync_workdir на DC1 и DC2 в /var/lib/samba/sysvol/;
- проверить sysvol и повторить синхронизацию;
- убедиться, что синхронизация выполнена успешно;
- включить синхронизацию по расписанию на DC1.

Если контроллеров домена больше чем два, можно создать больше заданий для cron на DC1:

1) скопировать файл /etc/osync/sync.conf в другой файл, например: /etc/osync/sync_dc3.conf;
2) в файле /etc/osync/sync_dc3.conf изменить значение параметра TARGET_SYNC_DIR;
3) повторить шаги 1 и 2 для всех контроллеров домена;
4) изменить задание на синхронизацию по расписанию на DC1:

```
# crontab -e
*/5 * * * * root  /usr/local/bin/osync.sh /etc/osync/sync.conf --silent
*/5 * * * * root  /usr/local/bin/osync.sh /etc/osync/sync_dc3.conf --silent
…
```

10.4. Клиент сети Active Directory

10.4.1. SSSD vs Winbind

Существует несколько способов прямого подключения системы Linux к AD. В этом разделе описаны функции и возможности двух вариантов интеграции: решение на основе Samba winbind и решение на базе SSSD.

Машины под управлением ОС Альт рекомендуется вводить в домен AD с помощью SSSD, но есть несколько исключений:

1) если в сети уже развернуты системы Linux, которые уже используют Samba winbind для целей интеграции;
2) если используется AD с включенным протоколом NTLM (так как SSSD не поддерживает протокол NTLM);
3) если SSSD не поддерживает определенную функцию, которую поддерживает winbind (например, SSSD не поддерживает доверительные отношения AD между лесами при прямом подключении к AD).

Ниже рассмотрены преимущества и недостатки интеграции на основе Samba Winbind и на базе SSSD (рис. 358, рис. 359).

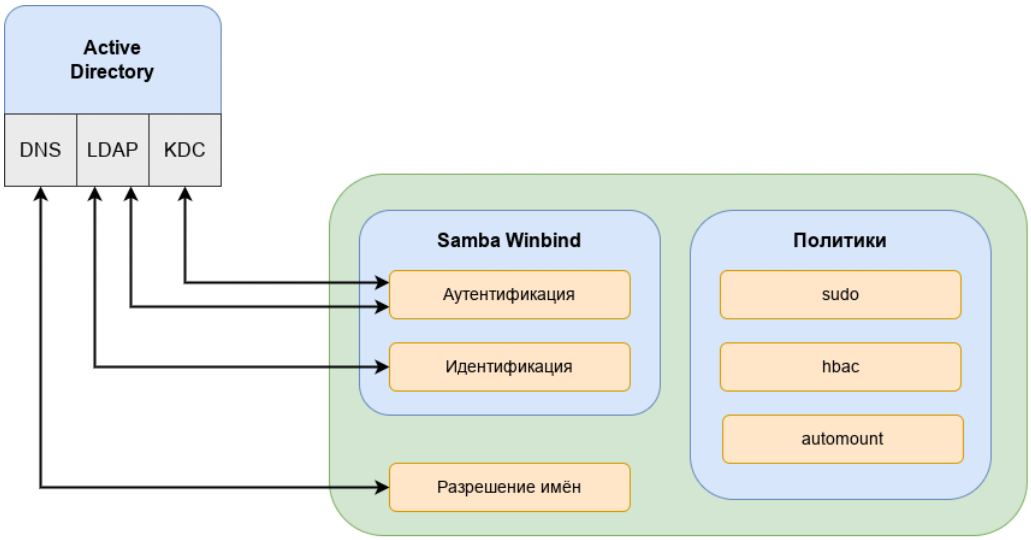


Рис. 358 – Схема интеграции на основе Samba Winbind

Преимущества варианта интеграции с использованием Samba Winbind:

- Samba Winbind эмулирует клиент Windows в системе Linux и использует преимущества собственных протоколов Windows и расширений протокола LDAP;
- Winbind понимает концепцию доменов и лесов, а также работает с доверием между доменами и лесами;
- Winbind может обнаруживать серверы, используя DNS;
- Winbind может переключиться на другой сервер, если контроллер домена AD становится недоступным;
- Winbind может динамически выполнять сопоставление идентификаторов на основе идентификаторов объектов AD (SID) или использовать атрибуты POSIX, хранящиеся в AD (если эти расширения были загружены);
- Winbind хорошо интегрируется с клиентом Samba FS и CIF;
- безопасность соединения основана на идентификации клиентской системы и ключах Kerberos, выданных этой системе.

Ограничения Samba Winbind:

- политики не управляются централизованно и должны распространяться вне группы;
- может подключаться только к AD.

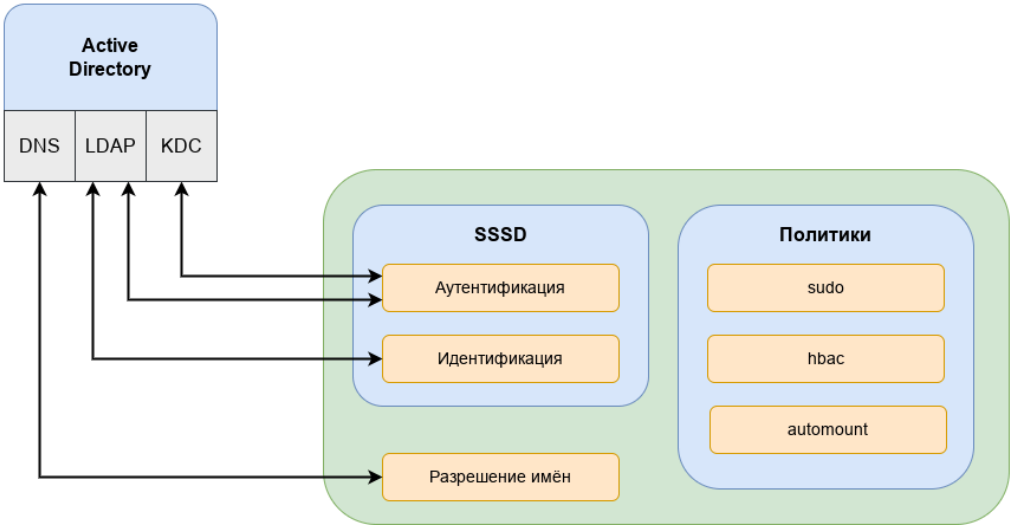


Рис. 359 – Схема интеграции на базе SSSD

SSSD – это группа служб, которые являются частью ядра операционной системы Linux и работают вместе для обеспечения аутентификации, поиска удостоверений и возможностей управления доступом для системы Linux. SSSD может взаимодействовать с AD, FreeIPA, Samba DC или любыми другими стандартными реализациями сервера LDAP и/или Kerberos.

Единственным серьезным ограничением для интеграции с использованием SSSD, является поддержка (старого) протокола NTLM. SSSD не реализует этот протокол, потому что по современным стандартам NTLM больше не является безопасным для развертывания. Наилучшей практикой является отказ от использования NTLM.

Преимущества SSSD (рис. 360):

- возможность загрузки и применения политик управления доступом на основе хоста с использованием объектов групповой политики, управляемых в AD;
- может взаимодействовать с разными источниками идентификации, а не только с AD;
- поддерживает очистку DNS (т. е. обнаруживает, были ли удалены или обновлены записи DNS для серверов);
- предоставляет расширенные интерфейсы идентификации на локальной шине сообщений (D-Bus). Этот интерфейс можно использовать для лучшей интеграции приложений, работающих в ОС Linux, с корпоративными источниками идентификации, такими как AD и FreeIPA.

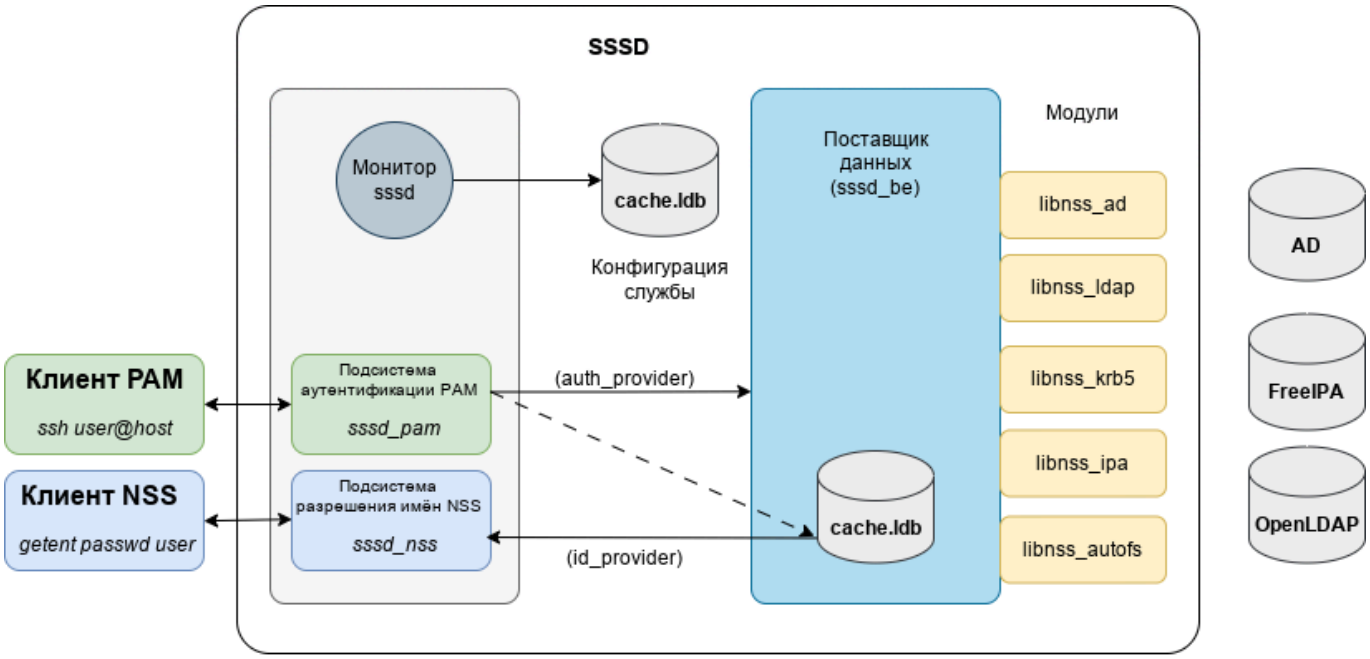


Рис. 360 – Схема интеграции конфигураций на базе SSSD

Сравнение Winbind и SSSD представлено в таблице 41.

Т а б л и ц а 41 – Сравнение Winbind и SSSD

Категория	Описание	Winbind	SSSD
Аутентификация	Проверка подлинности с использованием Kerberos	Да	Да
	Проверка подлинности LDAP	Да	Да
	Поддержка нескольких доменов AD	Да	Да
	Поддержка лесов AD	Да	Да
	Поддержка гетерогенных сетей AD/FreeIPA	Нет	Да
Безопасность	Простота настройки безопасной конфигурации	Нет	Да
	Система имеет идентификатор и ее ключ используется для защиты доступа к центральному серверу	Да	Да
	Поддержка NTLM	Да	Нет
Поиск и сопоставление идентификаторов	Динамическое сопоставление идентификаторов AD SID	Да	Да
	Использование преимуществ конкретных расширений и протоколов AD	Да	Да
DNS	Обновление и очистка DNS AD	Нет	Да
	Поддержка сайтов AD DNS	Да	Да
Обмен файлами	Интеграция с Samba FS	Да	Да
	Интеграция с клиентом CIFS	Да	Да
Служба печати	Сервер печати CUPS с использованием Kerberos	Да	Да
Политики	Централизованное управление контролем доступа на основе хоста через GPO	Нет	Да

Окончание таблицы 41

Категория	Описание	Winbind	SSSD
Интеграция с другими сервисами и приложениями	Интеграция с основными утилитами, такими как SSH, sudo, automount	Нет	Да
	Расширенные интерфейсы идентификации по локальной шине сообщений D-Bus	Нет	Да
	Специальные функции для приложений (Docker, Cockpit, GSS Proxy и др.)	Нет	Да

10.4.2. Подготовка системы к вводу в домен

10.4.2.1. Установка пакетов

Установить пакет task-auth-ad-sssd:

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

10.4.2.2. Синхронизация времени

Синхронизация времени с контроллером домена производится автоматически.

10.4.2.3. Настройка DNS

AD использует DNS для обнаружения других контроллеров домена и служб, таких как Kerberos. Поэтому, члены и серверы домена AD должны иметь возможность разрешать зоны AD DNS.

Для ввода компьютера в домен, на нем должен быть доступен сервер DNS, имеющий записи про контроллер домена Active Directory. При получении IP-адреса по DHCP данные о сервере DNS также должны быть получены от DHCP-сервера.

Ниже приведен пример настройки сетевого интерфейса со статическим IP-адресом.

10.4.2.3.1. Настройка клиентов для использования DNS-серверов вручную

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

В Центре управления системой «Сеть» → «Ethernet интерфейсы» задать имя компьютера, указать в поле «DNS-серверы» DNS-сервер домена и в поле «Домены поиска» – домен для поиска.

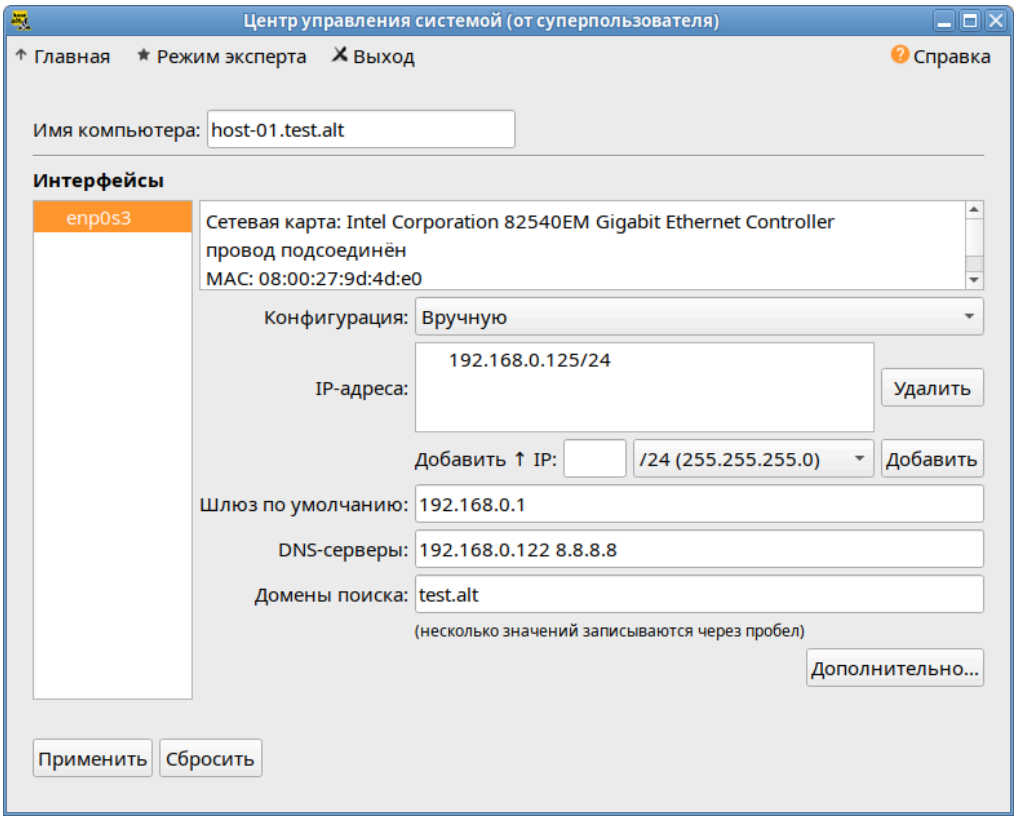


Рис. 361 – Окно «Центр управления системой»

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

В консоли:

1) задать имя компьютера:

```
# hostnamectl set-hostname host-01.test.alt
```

2) 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;

3) 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;

4) 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
```

10.4.2.3.2. Проверка разрешения DNS

Для проверки того, что настройки DNS верны и машины могут разрешать IP-адреса и имена, можно использовать команды `nslookup` и `host`.

Прямой поиск:

```
# nslookup dc1.test.alt

Server:        192.168.0.122
Address:  192.168.0.1222#53

Name:     dc1.test.alt
Address: 192.168.0.122

# host dc1.test.alt
dc1.test.alt has address 192.168.0.122
```

Обратный поиск:

```
# nslookup 192.168.0.122

122.0.168.192.in-addr.arpa name = dc1.alt.test.

# host 192.168.0.122
122.0.168.192.in-addr.arpa domain name pointer dc1.alt.test.
```

Обратите внимание, что в Samba AD обратная зона не настраивается автоматически.

AD использует записи SRV для поиска служб, таких как Kerberos и LDAP. Проверка разрешения SRV-записей:

```
$ nslookup
> set type=SRV
> _ldap._tcp.test.alt
```

```
Server:        192.168.0.122
Address:  192.168.0.122#53

_ldap._tcp.test.alt service = 0 100 389 dc2.test.alt.
_ldap._tcp.test.alt service = 0 100 389 dc1.test.alt.
> exit
```

или:

```
$ host -t SRV _ldap._tcp.test.alt
_ldap._tcp.test.alt has SRV record 0 100 389 dc1.test.alt.
_ldap._tcp.test.alt has SRV record 0 100 389 dc2.test.alt.
```

10.4.3. Ввод клиентских машин в Active Directory

10.4.3.1. Параметры команды system-auth

Для ввода клиентских машин в домен Active Directory, в дистрибутивах ОС Альт СП используется команда `system-auth`:

```
# system-auth <Действие> <Опции>
```

В таблице 42 приведено описание опций этой команды.

Таблица 42 – Опции команды system-auth

Параметр	Описание
Действие	
`status`	Показать текущую схему аутентификацию
`list`	Вывести список доступных схем аутентификации
`write`	Установить заданные параметры аутентификации
Опция	
`-d`	Включить отладку
`--winbind`	Использовать Samba Winbind для подключения системы к AD (если этот параметр не указан, будет использован SSSD)
`--gpo`	Включить групповые политики на машине
`--createcomputer=OU/SubOU`	Субконтейнер в AD (организационная единица/подразделение), куда будет помещена машина при вводе в домен
`--windows2003`	Ввести станцию в домен windows 2003
`--version`	Вывести версию программы

Примеры использования:

- вывести текущую схему аутентификации:

```
# system-auth status
ad TEST.ALT HOST-01 TEST
```

- использовать локальную аутентификацию:

```
# system-auth write local
```

- использовать аутентификацию AD (по умолчанию используется билет Kerberos):

```
# system-auth write ad <Домен> <Имя компьютера> <Рабочая группа> <Имя пользователя> [<Пароль>] [--windows2003] [--createcomputer="COMPUTEROU/SubCOMPUTEROU/SubSubCOMPUTEROU"] [--winbind] [--gpo]
```

10.4.3.2. Подключение к AD с помощью SSSD

В этом разделе описывается использование демона служб безопасности системы (SSSD) для подключения системы к Active Directory (AD).

SSSD используется для доступа к пользовательскому каталогу для аутентификации и авторизации через общую структуру с кэшированием пользователей, чтобы разрешить автономный вход в систему. SSSD легко настраивается.

Он обеспечивает интеграцию подключаемых модулей аутентификации (PAM) и службы переключения имен (NSS), базу данных для хранения локальных пользователей, а также расширенных пользовательских данных, полученных с центрального сервера.

Дополнительные ресурсы:

```
man realm
man sssd-ad
man sssd
```

10.4.3.2.1. Ввод в домен в командной строке

Для ввода компьютера в домен необходимо выполнить команду:

```
# system-auth write ad test.alt host-01 test 'administrator' 'Pa$$word'
Joined 'HOST-01' to dns domain 'test.alt'
```

Перезагрузить рабочую станцию.

10.4.3.2.2. Ввод в домен в Центре управления системой

Для ввода компьютера в домен в «Центре управления системой» необходимо выбрать пункт «Пользователи» → «Аутентификация».

В окне модуля «Аутентификация» следует выбрать пункт «Домен Active Directory», заполнить поля («Домен», «Рабочая группа», «Имя компьютера»),

выбрать пункт «SSSD» (в единственном домене) и нажать кнопку «Применить» (рис. 362).

В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку «ОК» (рис. 363).

При успешном подключении к домену, отобразится соответствующая информация (рис. 364).

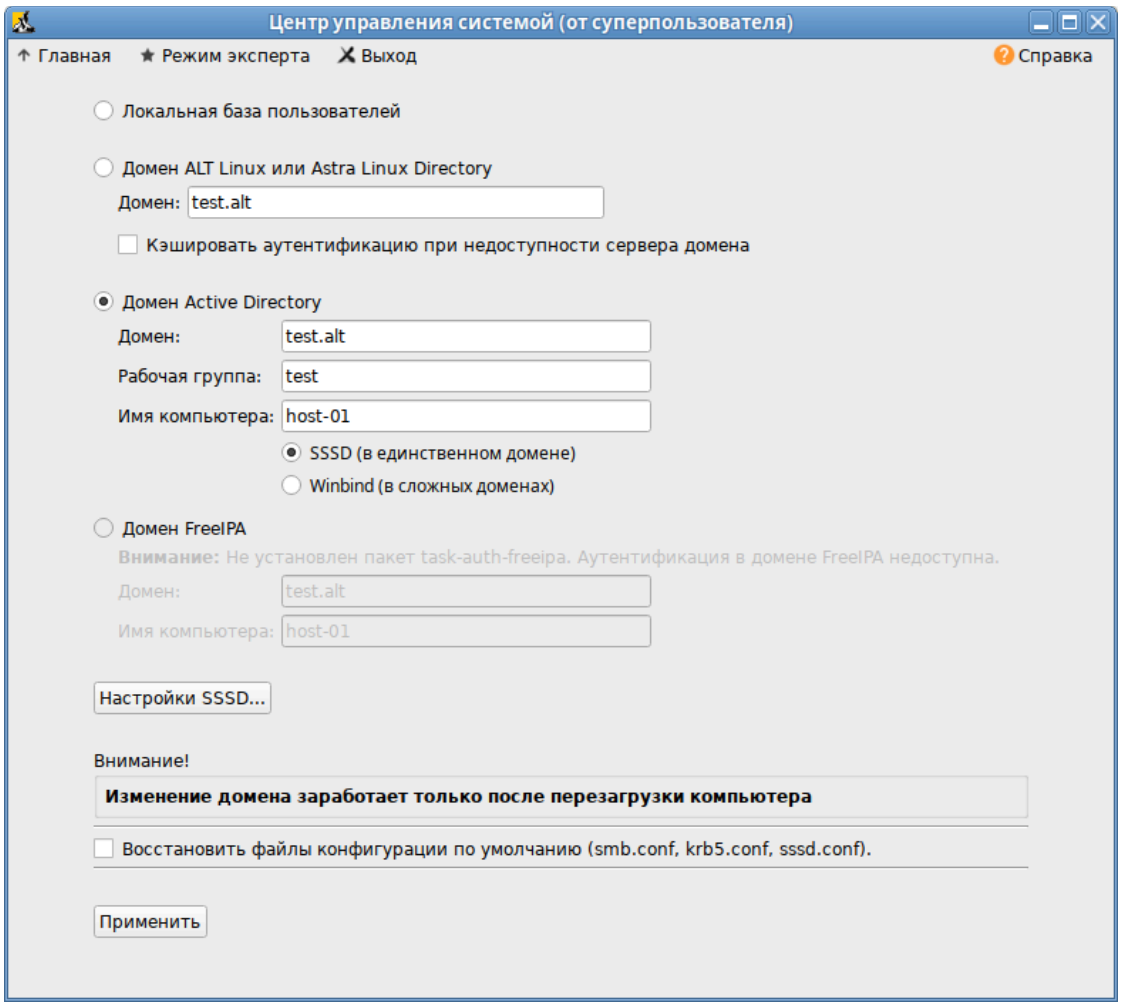


Рис. 362 – Окно модуля «Аутентификация»

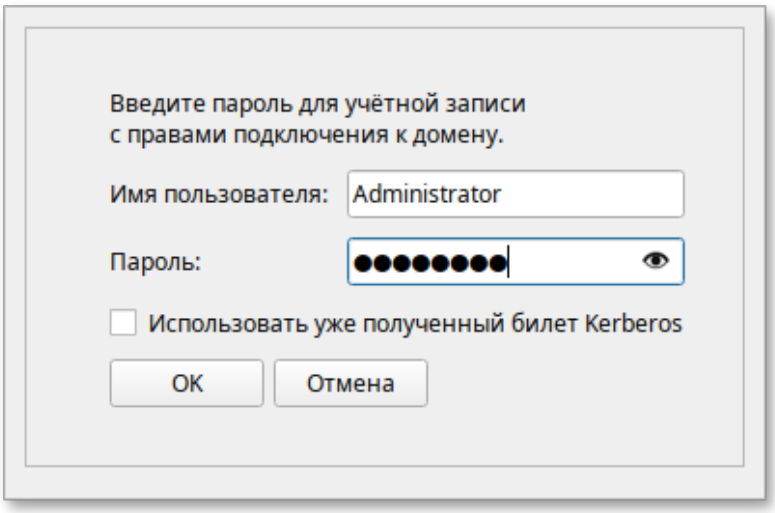


Рис. 363 – Окно ввода имени пользователя и пароля

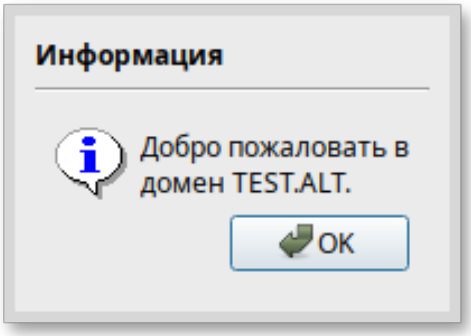


Рис. 364 – Информационное окно

Перезагрузить рабочую станцию.

10.4.3.2.3. Проверка клиента

Отображение сведений о пользователе AD (ivanov – пользователь в домене):

```
# getent passwd ivanov
ivanov:*:1187401105:1187400513:Иван
Иванов:/home/TEST.ALT/ivanov:/bin/bash

# net ads info
LDAP server: 192.168.0.122
LDAP server name: dc1.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
LDAP port: 389
Server time: Пн, 17 апр 2023 13:19:38 EET
KDC server: 192.168.0.122
Server time offset: 129
Last machine account password change: Вт, 11 окт 2022 10:11:52 EET
```

```
# net ads testjoin
Join is OK
```

Примечание. Список пользователей можно посмотреть на сервере командой:

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

Примечание. О настройке SSSD см. п. 10.6.1 и см. п. 10.5.5.2 в ЦУС.

10.4.3.3. Подключение к AD с помощью Samba Winbind

В этом разделе описывается использование Samba Winbind для подключения системы к Active Directory (AD).

Samba Winbind эмулирует клиент Windows в системе Linux и взаимодействует с серверами AD.

Дополнительные ресурсы:

- man realm;

- man winbindd.

10.4.3.3.1. Ввод в домен в командной строке

Для ввода компьютера в домен необходимо выполнить команду:

```
# system-auth write ad test.alt host-02 test 'administrator' 'Pa$$word' --winbind
Joined 'HOST-02' to dns domain 'test.alt'
```

Перезагрузить рабочую станцию.

10.4.3.3.2. Ввод в домен в «Центре управления системой»

Для ввода компьютера в домен в ЦУС выбрите пункт «Пользователи» → «Аутентификация».

В окне модуля «Аутентификация» следует выбрать пункт «Домен Active Directory», заполнить поля («Домен», «Рабочая группа», «Имя компьютера»), выбрать пункт «Winbind (в сложных доменах)» и нажать кнопку «Применить» (рис. 365).

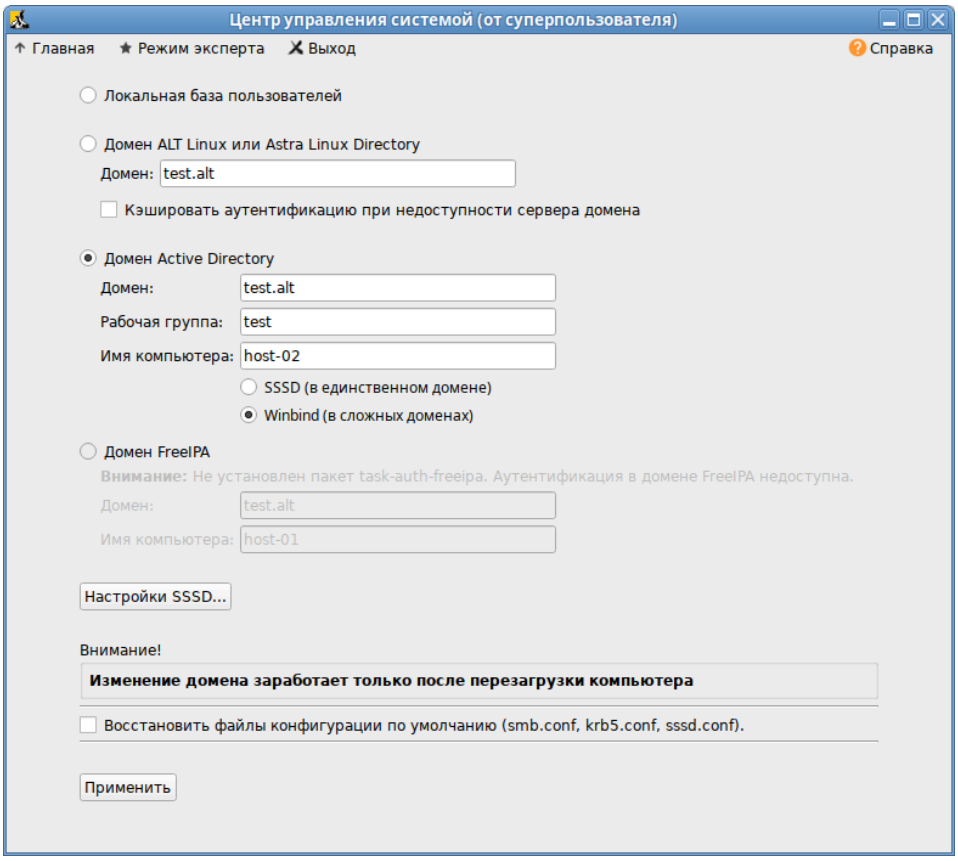


Рис. 365 – Окно ЦУС

В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку «ОК» (рис. 366).

При успешном подключении к домену, отобразится соответствующая информация (рис. 367).

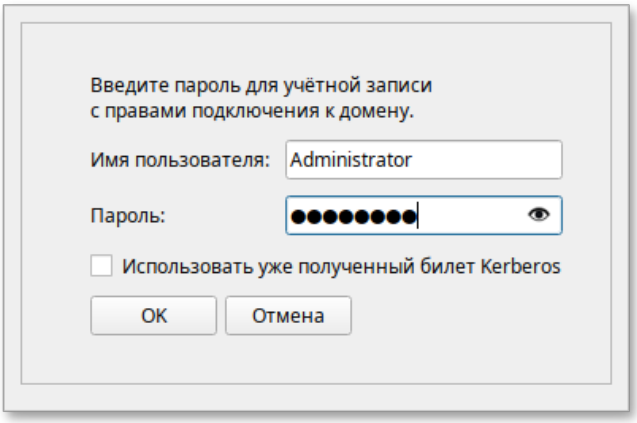


Рис. 366 – Окно ввода имени пользователя и пароля

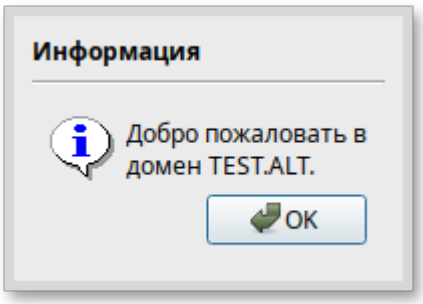


Рис. 367 – Информационное окно

Перезагрузить рабочую станцию.

10.4.3.3.3. Проверка клиента

Отображение сведений о пользователе AD (ivanov – пользователь в домене):

```
# getent passwd ivanov
ivanov:*:10000:10001::/home/TEST.ALT/ivanov:/bin/bash

# net ads info
LDAP server: 192.168.0.122
LDAP server name: dc1.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
LDAP port: 389
Server time: Пн, 17 апр 2023 13:20:46 EET
KDC server: 192.168.0.122
Server time offset: 129
Last machine account password change: Пн, 17 апр 2023 12:36:35
EET

# net ads testjoin
Join is OK
```

Примечание. Список пользователей можно посмотреть на сервере командой:

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

10.4.4. Отладочная информация

10.4.4.1. Настройка уровня журналирования Samba

Дополнительные сведения см. в п. 10.6.1.1.

10.4.4.2. Ошибка при подключении к IP-адресу 127.0.0.1

Используя настройки по умолчанию, команда net подключается к IP-адресу 127.0.0.1. Если Samba не прослушивает петлевой интерфейс, соединение не устанавливается. Например:

```
# net rpc rights list -U administrator
Could not connect to server 127.0.0.1
Connection failed: NT_STATUS_CONNECTION_REFUSED
```

Чтобы решить эту проблему, необходимо настроить Samba для дополнительного прослушивания интерфейса loopback.

Примечание. Чтобы временно обойти проблему, можно передать параметр `-I <IP-адрес>` или `-S <Имя хоста>` в команду `net`:

```
# net rpc rights list -U administrator -I 192.168.0.122
Password for [TEST\administrator]:
SeMachineAccountPrivilege  Add machines to domain
 SeTakeOwnershipPrivilege   Take ownership of files or other objects
 …
```

10.4.4.3. getent не показывает доменных пользователей и группы

Используя команду `getent passwd` и `getent group` нельзя увидеть доменных пользователей и группы. Этот функционал отключен по умолчанию для того чтобы сократить нагрузку на серверы. Поэтому для проверки необходимо указать точное имя пользователя:

```
# getent passwd <имя_пользователя>
```

Примечание. Список пользователей можно посмотреть на сервере командой:

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

Если команда `getent passwd <имя_пользователя>` ничего не возвращает, следует попробовать выполнить команду:

```
# getent passwd <рабочая_группа>\<имя_пользователя>
```

Например:

```
# getent passwd "TEST\ivanov"
```

Если эта команда работает, а первая нет, то необходимо добавить следующую строку в файл `smb.conf`:

```
winbind use default domain = yes
```

10.4.5. Повторная регистрация клиента

В этом разделе рассмотрена процедура повторной регистрации клиента в AD с тем же именем хоста. Повторная регистрация может потребоваться, если клиентский компьютер был уничтожен и потерял связь с серверами AD, например, из-за аппаратного сбоя клиента.

10.4.6. Удаление клиента AD

Чтобы вывести систему из домена, можно воспользоваться командой `realm leave`. Эта команда удалит конфигурацию домена из SSSD и локальной системы:

```
# realm leave test.alt
```

По умолчанию удаление выполняется от имени администратора (для AD – administrator). Если для присоединения к домену использовалась учетная запись другого пользователя, может потребоваться выполнить удаление от имени этого пользователя. Чтобы указать пользователя следует использовать параметр `-U`:

```
# realm leave test.alt -U <пользователь>
```

Сначала команда пытается подключиться без использования учетных данных, но при необходимости запрашивает пароль.

Следует обратить внимание, что, когда клиент удаляется из домена, учетная запись компьютера не удаляется из каталога; удаляется только конфигурация локального клиента. Если необходимо удалить учетную запись компьютера, следует запустить команду с параметром `--remove`:

```
# realm leave --remove test.alt
```

Для получения дополнительной информации см. справочную страницу man realm (8).

П р и м е ч а н и е . После вывода из домена, схема аутентификации пользователей в системе должна переключиться на локальную базу:

```
# control system-auth
local
```

П р и м е ч а н и е . Для того чтобы в окне входа отображался список доступных пользователей необходимо в файле `/etc/lightdm/lightdm.conf` закомментировать строку в группе `[SeatDefaults]`:

```
#greeter-hide-users=true
```

10.4.7. Настройка аутентификации доменных пользователей на DC

ВАЖНО

На текущий момент (samba 4.16.10, gpupdate 0.9.12.2) данный метод не позволяет применять групповые политики на контроллере домена.

ВАЖНО

На текущий момент (samba 4.16.10, sssd 2.8.1) для каталога `/var/lib/samba/sysvol` SID'ы домена не корректно транслируются в UNIX user id и group id.

Контроллер домена в рамках доменной инфраструктуры является, в том числе, еще одной машиной и имеет соответствующий машинный аккаунт. После применения настроек, описанных в этом разделе, машина с контроллером домена сможет выполнять, в том числе, и функции обычного члена домена, такие как:

- аутентификация доменными пользователями (в том числе по ssh);
- применение групповых политик;
- все, что поддерживает обычная клиентская машина (в качестве клиента SSSD или Winbind).

ВАЖНО

В качестве клиента на контроллере домена рекомендуется использовать Winbind. Использование SSSD не желательно.

10.4.7.1. Winbind

10.4.7.1.1. Установка пакетов

На контроллере домена необходимо установить пакеты task-auth-ad-winbind и gpupdate:

```
# apt-get install task-auth-ad-winbind gpupdate
```

10.4.7.1.2. Изменение файлов конфигурации

10.4.7.1.2.1 Настройка Kerberos (krb5.conf)

В файле `/etc/krb5.conf` должны быть заданы следующие параметры:

```
dns_lookup_realm = false
default_realm = TEST.ALT
```

Пример файла `/etc/krb5.conf`:

```
[logging]

[libdefaults]
 dns_lookup_kdc = true
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = TEST.ALT

[realms]

[domain_realm]
```

10.4.7.1.2.2 Настройка Samba (smb.conf)

В файле `/etc/samba/smb.conf` должны быть заданы следующие параметры:

```
kerberos method = dedicated keytab
dedicated keytab file = /etc/krb5.keytab
```

Значения остальных параметров в файле должно соответствовать аналогичному файлу на обычных клиентах домена.

Пример файла `/etc/samba/smb.conf`:

```
[global]
        dns forwarder = 8.8.8.8
        netbios name = DC1
        kerberos method = dedicated keytab
        dedicated keytab file = /etc/krb5.keytab
        realm = TEST.ALT
        server role = active directory domain controller
        workgroup = TEST
        idmap_ldb:use rfc2307 = yes
        template shell = /bin/bash
        template homedir = /home/TEST.ALT/%U

        wins support = no
        winbind use default domain = yes
        winbind enum users = no
        winbind enum groups = no
        winbind refresh tickets = yes
        winbind offline logon = yes

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No

[netlogon]
        path = /var/lib/samba/sysvol/test.alt/scripts
        read only = No
```

10.4.7.1.2.3 Настройка NSS (nsswitch.conf)

В файле `/etc/nsswitch.conf` должны быть заданы следующие параметры:

```
passwd: files winbind systemd
shadow: tcb files winbind
group: files [SUCCESS=merge] winbind role systemd
```

Пример файла `/etc/nsswitch.conf`:

```
passwd:     files winbind systemd
shadow:     tcb files winbind
group:      files [SUCCESS=merge] winbind role systemd
gshadow:    files

hosts:      files myhostname dns

ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files

automount:  files
aliases:    files
```

10.4.7.1.3. Настройка аутентификации

Необходимо переключить PAM-стек на использование для аутентификации winbind-модуля:

```
# control system-auth winbind
```

10.4.7.2. SSSD

10.4.7.2.1. Установка пакетов

На контроллере домена должны быть установлены пакеты task-auth-ad-sssd и gpupdate:

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

10.4.7.2.2. Изменение файлов конфигурации

10.4.7.2.2.1 Настройка Kerberos (krb5.conf)

В файле `/etc/krb5.conf` должны быть заданы следующие параметры:

```
includedir /etc/krb5.conf.d/
dns_lookup_realm = false
default_realm = TEST.ALT
```

Пример файла /etc/krb5.conf:

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

[logging]

[libdefaults]
 dns_lookup_kdc = true
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = TEST.ALT

[realms]

[domain_realm]
```

10.4.7.2.2.2 Настройка SSSD (sssd.conf)

В файле /etc/sssd/sssd.conf должны быть заданы следующие параметры:

```
user = root

ad_maximum_machine_account_password_age = 0
```

Значения остальных параметров в файле должно соответствовать аналогичному файлу на обычных клиентах домена.

Пример файла /etc/sssd/sssd.conf:

```
[sssd]
config_file_version = 2
services = nss, pam

# Managed by system facility command:
## control sssd-drop-privileges unprivileged|privileged|default
user = root

# SSSD will not start if you do not configure any domains.
domains = TEST.ALT
[nss]

[pam]
[domain/TEST.ALT]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad
default_shell = /bin/bash
fallback_homedir = /home/%d/%u
debug_level = 0
; cache_credentials = false
ad_gpo_ignore_unreadable = true
```

```
ad_gpo_access_control = permissive
ad_update_samba_machine_account_password = true
ad_maximum_machine_account_password_age = 0
```

10.4.7.2.2.3 Настройка Samba (smb.conf)

В файле `/etc/samba/smb.conf` должны быть заданы следующие параметры:

```
idmap config * : range = 200000-2000200000
idmap config * : backend = sss
```

Значения остальных параметров в файле должно соответствовать аналогичному файлу на обычных клиентах домена.

Пример файла `/etc/samba/smb.conf`:

```
[global]
        dns forwarder = 8.8.8.8
        netbios name = DC1
        realm = TEST.ALT
        server role = active directory domain controller
        workgroup = TEST
        idmap_ldb:use rfc2307 = yes

        template shell = /bin/bash
        template homedir = /home/TEST.ALT/%U

        kerberos method = system keytab
        wins support = no
        winbind use default domain = yes
        winbind enum users = no
        winbind enum groups = no
        winbind refresh tickets = yes
        winbind offline logon = yes

        idmap config * : range = 200000-2000200000
        idmap config * : backend = sss

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No

[netlogon]
        path = /var/lib/samba/sysvol/test.alt/scripts
        read only = No
```

10.4.7.2.2.4 Настройка NSS (nsswitch.conf)

В файле `/etc/nsswitch.conf` должны быть заданы следующие параметры:

```
passwd: files sss systemd
shadow: tcb files sss
group: files [SUCCESS=merge] sss role system
```

Пример файла `/etc/nsswitch.conf`:

```
passwd:     files sss systemd
shadow:     tcb files sss
group:      files [SUCCESS=merge] sss role systemd
gshadow:    files

hosts:      files myhostname dns

ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files

automount:  files
aliases:    files
```

10.4.7.2.3. Настройка аутентификации

Необходимо переключить PAM-стек на использование для аутентификации sss-модулей:

```
# control system-auth sss
```

10.4.7.3. Генерация keytab-файла

Необходимо сгенерировать системный keytab-файл для машинного аккаунта контроллера домена. Для этого следует выполнить следующую команду:

```
# net ads keytab create
```

10.4.7.4. Службы

Необходимо отключить сервис `nscd`:

```
# systemctl disable --now nscd
```

Если используется схема с SSSD клиентом, необходимо запустить и включить автоматический запуск для службы `sssd`:

```
# systemctl enable --now sssd
```

10.4.7.5. Настройка ролей

Необходимо указать, какие локальные роли каким группам домена соответствуют:

- обычные пользователи домена (Domain Users) соответствуют локальной роли users: `# roleadd 'domain users' users`

- администраторы домена (Domain Admins) соответствуют локальной роли localadmins:

```
# roleadd 'domain admins' localadmins
```

ВАЖНО

В русскоязычных версиях MS Windows Server встроенные группы Domain Users и Domain Admins имеют русифицированные названия «Пользователи домена» и «Администраторы домена».

10.4.7.6. Групповые политики

Для включения поддержки групповых политик необходимо выполнить:

```
# gpupdate-setup enable --local-policy ad-domain-controller
```

ВАЖНО

Работа групповых политик на контроллере домена с SSSD клиентом может быть не стабильной.

10.4.7.7. Настройка SSH

Разрешить удаленный доступ по ssh только Администраторам домена:

```
# control sshd-allow-groups enabled
# control sshd-allow-groups-list remote
```

При необходимости можно разрешить аутентификацию по Kerberos билетам:

```
# control sshd-gssapi-auth enabled
```

Для применения настроек необходимо перезапустить сервис `sshd`:

```
# systemctl restart sshd
```

Примечание. Данные настройки можно применить с помощью механизма групповых политик control. Подробнее см. п. 9.2.5.4.2.

10.4.8. Настройка обновления паролей аккаунтов машин

После завершения процедуры ввода в домен каждая машина получает специальный аккаунт вида MACHINE01$. Такой аккаунт, ассоциированный с машиной, а не с конкретным пользователем, позволяет машине выполнять в домене действия от своего имени. Например, запрашивать информацию о пользователях, получать машинные групповые политики и т. д.

Как и у любого другого пользователя, у машинного пользователя есть свой пароль, генерируемый автоматически в процессе ввода машины в домен. В отличии

от обычных пользователей, у машинных аккаунтов нет ограничения на время жизни пароля, но машина имеет возможность поменять его самостоятельно. По умолчанию машины с MS Windows 2000 и старше меняют пароль раз в 30 дней. Информация о последней смене пароля хранится в атрибуте машинного аккаунта pwdlastset.

10.4.8.1. Локальная политика смены пароля

Сменой пароля пароля учетной записи компьютера можно управлять с помощью групповых политик. Для этого нужно отредактировать параметр политики домена по умолчанию (Default domain policy) «Член домена: максимальный срок действия пароля учетной записи компьютера», который располагается в подразделе «Конфигурация компьютера» → «Политики» → «Конфигурация Windows» → «Параметры безопасности» → «Локальные политики» → «Параметры безопасности» (Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options) (рис. 368).

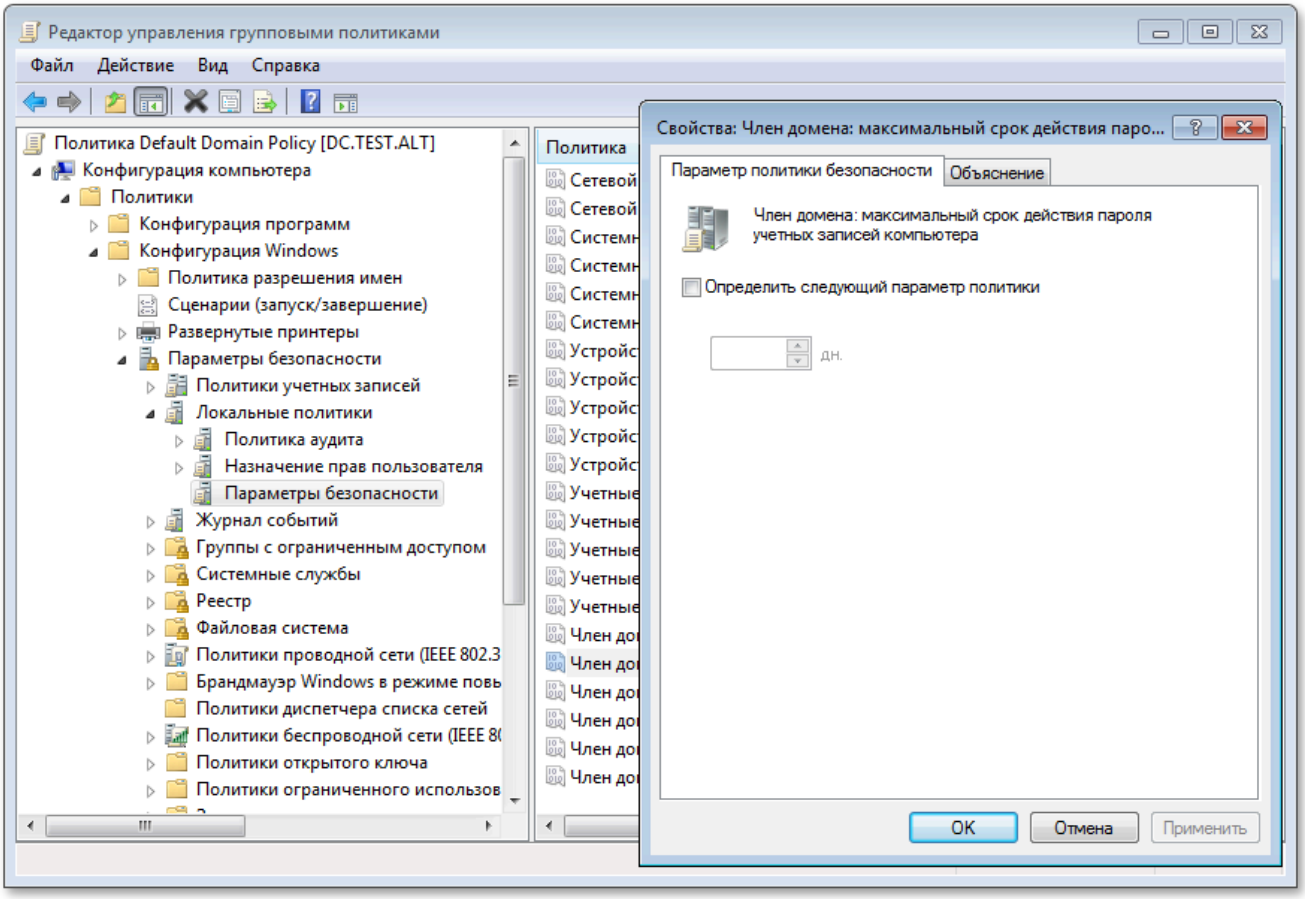


Рис. 368 – Окно параметра «Член домена»

П р и м е ч а н и е . На данный момент в ADMC (admc 0.11.2), нет возможности настроить данные параметры групповой политики. Необходимо использовать оснастку RSAT «Управление групповыми политиками» (см. п. 10.7.10).

Этот параметр безопасности определяет, как часто член домена будет пытаться изменить пароль учетной записи компьютера. Значение по умолчанию: 30 дней.

С помощью параметра «Член домена: отключить изменение пароля учетных записей компьютера» можно отключить обновления пароля машинного аккаунта совсем, но делать этого не рекомендуется.

ВАЖНО

Указанные выше параметры корректно работают на машинах с ОС MS Windows 2000 и старше.

ВАЖНО

На машинах с ОС Альт СП (sssd 2.8.1) данные параметры игнорируются.

10.4.8.2. Включение обновления пароля

10.4.8.2.1. ОС Windows

Для включения периодического обновления пароля учетной записи компьютера на машинах под управлением ОС Windows 2000 и старше дополнительных действий не требуется. Периодичность обновления настраивается с помощью соответствующей групповой политики.

10.4.8.2.2. ОС Альт СП

За обновление пароля машинного аккаунта на машинах под управлением ОС Альт СП отвечают сервисы `sssd` и `winbind`.

10.4.8.2.2.1 Winbind

Winbind, на текущий момент (samba-winbind 4.16.10), не умеет после смены пароля учетной записи компьютера обновлять системный keytab-файл (`/etc/krb5.keytab`). Поэтому, во избежание конфликтов с sssd, следует отключить этот функционал.

Для отключения периодического обновления пароля учетной записи компьютера необходимо в файл `/etc/samba/smb.conf` в секцию `[global]` добавить параметр `machine password timeout = 0`:

```
[global]
machine password timeout = 0
```

10.4.8.2.2.2 SSSD

`sssd` для обновления пароля учетной записи компьютера использует утилиту adcli. Необходимо убедиться, что пакет adcli установлен в системе:

```
# apt-get install adcli
```

Периодичностью обновления пароля учетной записи компьютера можно управлять с помощью параметра `ad_maximum_machine_account_password_age` (секция `[domain/<Домен>]`) в `/etc/sssd/sssd.conf`. Значение по умолчанию: 30 дней.

Для корректного функционирования обновления пароля учетной записи компьютера `sssd` необходим доступ на запись в файл `/etc/krb5.keytab`. Для этого недостаточно привилегий пользователя _sssd, от которого обычно и запускается `sssd`. Необходимо запускать `sssd` с правами суперпользователя. Для этого следует в файле `/etc/sssd/sssd.conf` в секции `[sssd]` изменить значение параметра `user` на root:

```
[sssd]
user = root

[domain/<Домен>]
ad_update_samba_machine_account_password = true
```

ВАЖНО

При вводе компьютера в домен с помощью ЦУС следующие параметры прописываются в конфигурационные файлы по умолчанию:

- `/etc/samba/smb.conf:`
  `machine password timeout = 0`
- `/etc/sssd/sssd.conf:`
  `ad_update_samba_machine_account_password = true`

10.4.8.3. Отключение обновления пароля

10.4.8.3.1. ОС Windows

Для отключения периодического обновления пароля учетной записи компьютера на машинах под управлением ОС Windows 2000 и старше достаточно включить параметр групповой политики «Default domain policy» «Член домена: отключить изменение пароля учетных записей компьютера».

10.4.8.3.2. ОС Альт СП

Для отключения периодического обновления пароля учетной записи компьютера на машинах под управлением ОС Альт СП необходимо:

- в файле `/etc/sssd/sssd.conf` (секция `[domain/<Домен>]`) значение параметра `ad_maximum_machine_account_password_age` установить равным 0:

```
[domain/<Домен>]
ad_maximum_machine_account_password_age = 0
```

- в файле `/etc/samba/smb.conf` (секция `[global]`) значение параметра `machine password timeout` установить равным 0:

```
[global]
machine password timeout = 0
```

10.4.8.4. Диагностика

10.4.8.4.1. Дата последней смены пароля

Дата последней смены пароля учетной записи компьютера хранится в базе данных AD. Запросить ее можно одним из способов:

- на введенной в домен машине выполнить команду:

```
# net ads info
…
Last machine account password change: Ср, 12 апр 2023 09:59:36 EET
```

- если машина уже потеряла доверие в домене, то выполнить эту же команду от доменного пользователя:

```
# net ads info -U <user>
```

Дата последней смены пароля учетной записи компьютера будет показана в параметре:

`Last machine account password change.`

10.4.8.4.2. Потеря доверия между машиной и доменом

Для проверки того, имеет ли машина возможность аутентифицироваться в домене можно выполнить следующие действия:

- убедиться, что keytab-файла (`/etc/krb5.keytab`) содержит корректную информацию:

```
# klist -ke
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------
------
   1 host/work.test.alt@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 host/WORK@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 host/work.test.alt@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 host/WORK@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 host/work.test.alt@TEST.ALT (DEPRECATED:arcfour-hmac)
   1 host/WORK@TEST.ALT (DEPRECATED:arcfour-hmac)
   1 restrictedkrbhost/work.test.alt@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 restrictedkrbhost/WORK@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 restrictedkrbhost/work.test.alt@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 restrictedkrbhost/WORK@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 restrictedkrbhost/work.test.alt@TEST.ALT (DEPRECATED:arcfour-hmac)
   1 restrictedkrbhost/WORK@TEST.ALT (DEPRECATED:arcfour-hmac)
   1 WORK$@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 WORK$@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 WORK$@TEST.ALT (DEPRECATED:arcfour-hmac)
```

- попытаться получить билет Kerberos для учетной записи компьютера (в примере WORK$), используя файл `/etc/krb5.keytab`:

```
# kinit -k WORK\$@TEST.ALT
```

- убедиться, что билет успешно получен и удалить его:

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

Valid starting       Expires              Service principal
21.04.2023 12:25:37  21.04.2023 22:25:37  krbtgt/TEST.ALT@TEST.ALT
    renew until 28.04.2023 12:25:37

# kdestroy -p WORK\$@TEST.ALT
```

ВАЖНО

Следует убедиться, что имя машины в keytab-файле (`/etc/krb5.keytab`) соответствует реальному имени машины (см. вывод команды `hostnamectl`).

10.4.8.5. Восстановление работоспособности

Если диагностика показала, что машина потеряла доверие с доменом, то, для восстановления работоспособности, необходимо выполнить следующие действия:

- обновить систему:

```
# apt-get update && apt-get dist-upgrade
```

- удалить файл `/etc/krb5.keytab`;
- повторно ввести машину в домен используя ЦУС;
- убедиться, что конфигурационные файлы соответствуют одному из сценариев: «Включение обновления пароля» или «Отключение обновления пароля»;
- перезагрузить машину.

10.5. Доверительные отношения (Трасты)

Доверительные отношения (trusts) позволяют аутентифицироваться под пользователями не только текущего домена, но и доверенных.

10.5.1. Настройка доверия

10.5.1.1. Общие сведения

Доверительные отношения реализуются в рамках механизма аутентификации. Суть доверительных отношений между двумя доменами сводится к тому, что доверяющий домен (trusting domain) доверяет процесс аутентификации доверенному домену (trusted domain). Пользователь, аутентифицированный доверенным доменом, может получить доступ к ресурсам в доверяющем домене (рис. 369).

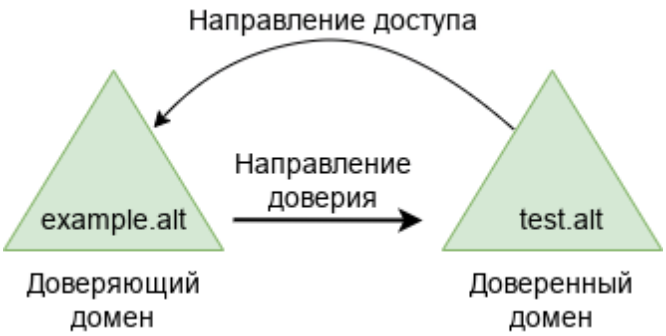


Рис. 369 – Схема доверительных отношений в рамках механизма аутентификации

Отношения доверия обеспечивают доступ к ресурсам в одном или двух направлениях:

- одностороннее доверие – позволяет пользователям и группам из домена А получать доступ к ресурсам в домене Б, но не наоборот. Домен А доверяет домену Б, но домен Б не доверяет домену А. При создании такого доверия нужно указать направление (входящее или исходящее);
- двустороннее доверие – позволяет пользователям и группам из домена А получать доступ к ресурсам в домене Б и наоборот. Запросы проверки подлинности могут передаваться между двумя доменами в обоих направлениях. Домен А доверяет домену Б, а домен Б доверяет домену А.

Транзитивность определяет, можно ли расширить доверие за пределы двух доменов, для которых оно сформировано:

- транзитивное доверие можно использовать для расширения отношений доверия на другие домены;
- нетранзитивное доверие можно использовать для запрета отношений доверия с другими доменами.

Типы доверия:

- доверие леса (Forest) – связывает леса и все их домены (это двухсторонние или односторонние отношения доверия между разными лесами, всегда являющиеся транзитивными);
- внешнее доверие (External) – устанавливается между двумя доменами напрямую вне леса (для установки двухстороннего доверия нужно использовать два разнонаправленных доверия, которыми надо связать все требуемые пары доменов).

10.5.1.2. Особенности доверительных отношений в Samba

Поддерживается:

- доверие леса (это доверие может быть установленным между двумя Samba-доменами или Samba-доменом и Windows-доменом);
- внешние доверительные отношения между доменом AD и доменом в стиле NT;

- добавление пользователей и групп доверенного домена в группы доверяющего домена (при этом необходимо использовать SID пользователей и групп, имя пользователя или имя группы использовать невозможно);
- в RSAT можно увидеть foreignSecurityPrincipal для всех добавленных пользователей и групп из доверенного домена.

Особенности и ограничения:

- не применяются правила фильтрации SID;
- нельзя добавить пользователей и группы доверенного домена в доменные группы доверяющего домена по имени;
- для входа в доверенный домен через SSSD надо использовать тип связи `External`, а не `Forest`;
- обе стороны траста должны полностью доверять друг другу (администратор из домена А может управлять всеми объектами в домене Б и наоборот);
- не поддерживается выборочная аутентификация;
- нельзя создать доверительные отношения между доменами в одном дереве с одним и тем же пространством имен верхнего уровня. NetBIOS имена доменов должны отличаться (домен MYDOMAIN.WIN и MYDOMAIN.NEW будут иметь одинаковое короткое имя – MYDOMAIN, это приведет к невозможности установки доверительных отношений).

Для управления доверием можно использовать инструмент командной строки samba-tool (таблица 43).

Т а б л и ц а 43 – Команды управления доверием

Команда	Описание	Примечание
`domain trust create <домен>`	Создать доверие домена или леса	Можно использовать следующие опции: `--type=TYPE` – тип доверия (`external`, `forest`); `--direction=DIRECTION` – направление доверия (`incoming`, `outgoing`, `both`); `--create-location=LOCATION` – где создать объект доверенного домена (`local`, `both`); `--quarantined=yes|no` – применять к доверию специальные правила фильтрации SID (если `--type=external` по умолчанию `yes`, если `--type=forest` по умолчанию `no`); `-U USERNAME` – имя пользователя

Окончание таблицы 43

Команда	Описание	Примечание
`domain trust modify <домен>`	Изменить доверие домена или леса	
`domain trust delete <домен>`	Удалить доверие домена или леса	Можно использовать следующие опции: `--delete-location=LOCATION` – где удалить объект доверенного домена (`local`, `both`); `-U USERNAME` – имя пользователя
`domain trust list`	Вывести список доверительных отношений домена	
`domain trust show <домен>`	Показать сведения о доверенном домене	
`domain trust validate <домен>`	Проверить доверие к домену	Можно использовать следующие опции: `--validate-location=LOCATION` – проверить объект доверенного домена (`local`, `both`); `-U USERNAME` – имя пользователя

10.5.2. Настройка DNS

Перед настройкой доверия необходимо убедиться, что серверы видят друг друга и правильно разрешают доменные имена.

10.5.2.1. Два домена Samba

Доменные имена, относящиеся к версии Samba, представлены в таблице 44.

Таблица 44 – Исходные данные

Имя домена	Контроллер домена	IP-адрес	ОС контроллера домена	Версия Samba
TEST.ALT	dc1.test.alt	192.168.0.122	ALT Server SP	4.16.10
EXAMPLE.ALT	s1.example.alt	192.168.0.172	ALT Server SP	4.16.10

10.5.2.1.1. Настройка переадресации DNS на DC с BIND9_DLZ

Если используется dns_backend BIND9_DLZ, добавить информацию о зоне в конец файла `/etc/bind/options.conf`.

На контроллере домена dc1.test.alt добавить строки:

```
zone "example.alt" {
      type forward;
      forwarders { 192.168.0.172; };
};
```

На контроллере домена s1.example.alt:

```
zone "test.alt" {
      type forward;
      forwarders { 192.168.0.122; };
};
```

Перезапустить службу DNS:

```
# systemctl restart bind.service
```

Примечание. Если удаленный DNS-сервер не использует DNSSEC и включить проверку DNSSEC на удаленном DNS-сервере нельзя, можно отключить DNSSEC на сервере AD. Для этого необходимо в файл `/etc/bind/options.conf` в секцию `options` добавить параметры:

```
dnssec-enable no;
dnssec-validation no;
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

10.5.2.1.2. Настройка переадресации DNS на DC с SAMBA_INTERNAL

Если используется DC с dns_backend SAMBA_INTERNAL, самый простой способ заставить работать разрешение имен – настроить DNS-прокси между двумя доменами. DNS-прокси будет перенаправлять запрос между доменами и внешним DNS-серверами. В примере, в качестве DNS-прокси используется отдельный сервер (IP-адрес 192.168.0.150) с настроенным bind9.

На каждом контроллере домена:

1) указать DNS-прокси, как сервер пересылки в файле `/etc/samba/smb.conf` (в параметре `dns forwarder`). Например:

```
dns forwarder = 192.168.0.150 8.8.8.8
```

2) перезапустить службу samba:

```
# systemctl restart samba
```

На сервере bind9 отредактировать файл `/etc/bind/options.conf`:

- отключить проверку DNSSEC, для этого в секцию `options` добавить параметры:

```
dnssec-enable no;
dnssec-validation no;
```

- в конец файла добавить информацию о зонах:

```
zone "example.alt" {
      type forward;
      forwarders { 192.168.0.172; };
};

zone "test.alt" {
      type forward;
      forwarders { 192.168.0.122; };
};
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

10.5.2.1.3. Проверка конфигурации DNS

Для проверки настройки следует убедиться, что на обоих контроллерах домена разрешаются SRV-записи:

- на контроллере домена dc1.test.alt:

```
# host -t srv _kerberos._tcp.example.alt
_kerberos._tcp.example.alt   has   SRV   record   0   100   88
s1.example.alt.
# host -t srv _kerberos._tcp.test.alt
_kerberos._tcp.test.alt has SRV record 0 100 88 dc1.test.alt.
```

- на контроллере домена s1.example.alt:

```
# host -t srv _kerberos._tcp.example.alt
_kerberos._tcp.example.alt has SRV record 0 100 88 s1.example.alt.
# host -t srv _kerberos._tcp.test.alt
_kerberos._tcp.test.alt has SRV record 0 100 88 dc1.test.alt.
```

Проверить возможность получения билета Kerberos:

- на контроллере домена dc1.test.alt:

```
# kinit administrator@EXAMPLE.ALT
Password for administrator@EXAMPLE.ALT:
# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_eFyZ8Tr
Default principal: administrator@EXAMPLE.ALT

Valid starting       Expires              Service principal
25.04.2023 15:38:17  26.04.2023 01:38:17  krbtgt/EXAMPLE.ALT@EXAMPLE.ALT
    renew until 26.04.2023 15:38:14
```

- на контроллере домена s1.example.alt:

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

Valid starting       Expires              Service principal
25.04.2023 15:17:50  26.04.2023 01:17:50  krbtgt/TEST.ALT@TEST.ALT
    renew until 26.04.2023 15:17:46
```

ВАЖНО

realm должен быть записан заглавными буквами.

10.5.2.2. Samba DC и Windows Server с AD

Исходные данные Samba DC и Windows Server с AD представлены в таблице 45.

Таблица 45 – Исходные данные

Имя домена	Контроллер домена	IP-адрес	ОС контроллера домена	Версия Samba
TEST.ALT	dc1.test.alt	192.168.0.122	ALT Server SP	4.16.10
WIN.ALT	DC1.win.alt	192.168.0.190	Windows Server 2012	

10.5.2.2.1. Windows Server с AD

На AD сервере создать сервер условной пересылки для зоны Samba домена.

В графическом интерфейсе:

1) открыть «Диспетчер DNS» (DNS Manager);
2) в разделе «Серверы условной пересылки» (Conditional Forwarders) добавить новый сервер пересылки, указав FQDN или IP-адрес сервера Samba (рис. 370);
3) сохранить настройки.

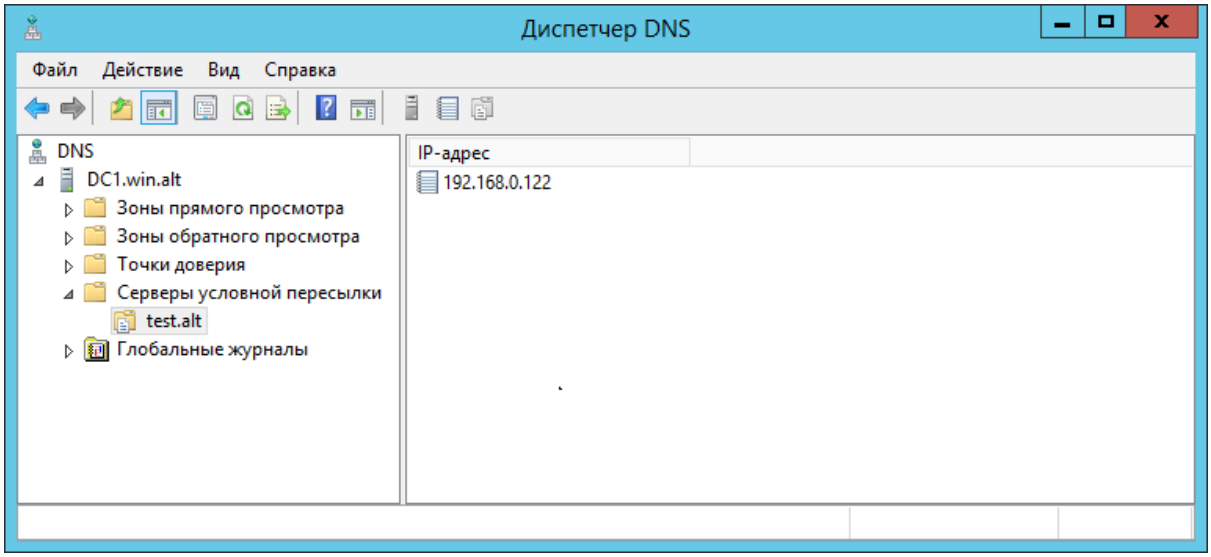


Рис. 370 – Окно «Диспетчер DNS»

В командной строке:

```
C:\> dnscmd 127.0.0.1 /ZoneAdd test.alt /Forwarder 192.168.0.122
DNS Server 127.0.0.1 created zone test.alt:

Command completed successfully
```

выполнить следующую команду в сеансе PowerShell, для настройки пересылки DNS:

```
PS C:\Windows\system32> Add-DnsServerConditionalForwarderZone -Name test.alt -MasterServers 192.168.0.122 -ReplicationScope Forest
```

10.5.2.2.2. Samba DC с BIND9_DLZ

Если используется dns_backend BIND9_DLZ, добавить в конец файла `/etc/bind/options.conf` (или `/etc/bind/ddns.conf`) строки:

```
zone "win.alt" {
      type forward;
      forwarders { 192.168.0.190; };
};
```

и перезапустить службу DNS:

```
# systemctl restart bind.service
```

Примечание. Если удаленный DNS-сервер не использует DNSSEC и включить проверку DNSSEC на удаленном DNS-сервере нельзя, можно отключить DNSSEC на сервере AD. Для этого необходимо в файл `/etc/bind/options.conf` в секцию `options` добавить параметры:

```
dnssec-enable no;
dnssec-validation no;
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

10.5.2.2.3. Samba DC с SAMBA_INTERNAL

Если используется DC с dns_backend SAMBA_INTERNAL, самый простой способ заставить работать разрешение имен – настроить DNS-прокси между двумя доменами. DNS-прокси будет перенаправлять запрос между доменами и внешним DNS-серверами. В примере, в качестве DNS-прокси используется отдельный сервер (IP-адрес 192.168.0.150) с настроенным bind9.

На контроллере домена:

- указать DNS-прокси, как сервер пересылки в файле `/etc/samba/smb.conf` (в параметре dns forwarder). Например:

```
dns forwarder = 192.168.0.150 8.8.8.8
```

- перезапустить службу samba:

```
# systemctl restart samba
```

На сервере bind9 отредактировать файл `/etc/bind/options.conf`:

- отключить проверку DNSSEC, для этого в секцию `options` добавить параметры:

```
dnssec-enable no;
dnssec-validation no;
```

- в конец файла добавить информацию о зонах:

```
zone "win.alt" {
      type forward;
      forwarders { 192.168.0.190; };
};
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

10.5.2.2.4. Проверка конфигурации DNS

Перед настройкой доверия необходимо убедиться, что серверы могут разрешать себя и друг друга.

На Samba DC:

1) запись, отвечающая за работу сервисов Kerberos через UDP и LDAP через TCP:

```
# dig +short -t SRV _kerberos._udp.test.alt
0 100 88 dc1.test.alt.
# dig +short -t SRV _ldap._tcp.test.alt
0 100 389 dc1.test.alt.
```

В выводе команд должен быть отображен список всех серверов;

2) наличие записей для работы сервисов AD на DNS-сервере Samba:

```
# dig +short -t SRV _kerberos._tcp.dc._msdcs.win.alt
0 100 88 dc1.win.alt.
# dig +short -t SRV _ldap._tcp.dc._msdcs.win.alt
0 100 389 dc1.win.alt.
```

3) проверить возможность получения билета Kerberos:

```
# kinit administrator@WIN.ALT

Password for administrator@WIN.ALT:
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@WIN.ALT

Valid starting       Expires              Service principal
27.04.2023 17:42:28  28.04.2023 03:42:28  krbtgt/WIN.ALT@WIN.ALT
    renew until 28.04.2023 17:42:25
```

Проверить наличие записей DNS-сервере AD:

1) запустить утилиту nslookup.exe для поиска служебных записей:

```
C:\> nslookup.exe
> set type=SRV
```

2) ввести доменное имя для служебных записей Kerberos через UDP и LDAP через TCP:

```
> _kerberos._udp.test.alt
_kerberos._udp.test.alt       SRV service location:
    priority                = 0
    weight                  = 100
    port                    = 88
    svr hostname            = dc1.test.alt
…
test.alt
    primary name server = dc1.test.alt
    responsible mail addr = hostmaster.test.alt
    serial = 7
    refresh = 900 (15 mins)
    retry = 600 (10 mins)
    expire = 86400 (1 days)
    default TTL = 3600 (1 hours)
> _ldap._tcp.test.alt
_ldap._tcp.test.alt       SRV service location:
    priority                = 0
    weight                  = 100
    port                    = 389
    svr hostname            = dc1.test.alt
…
```

10.5.3. Создание двухстороннего транзитивного подключения

10.5.3.1. Два домена Samba

На контроллере домена dc1.test.alt:

```
# samba-tool domain trust create EXAMPLE.ALT --type=forest --direction=both --create-location=both -U administrator@EXAMPLE.ALT
LocalDomain Netbios[TEST] DNS[test.alt] SID[S-1-5-21-1455776928-3410124986-2843404052]
RemoteDC                    Netbios[S1]                    DNS[s1.example.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,FULL_SECRET_DOMAIN_6]
Password for [administrator@EXAMPLE.ALT]:
RemoteDomain   Netbios[EXAMPLE]   DNS[example.alt]   SID[S-1-5-21-3274802069-598906262-3677769431]
Creating remote TDO.
Remote TDO created.
Setting supported encryption types on remote TDO.
Creating local TDO.
Local TDO created
Setting supported encryption types on local TDO.
Setup local forest trust information...
```

```
Namespaces[2] TDO[example.alt]:
TLN: Status[Enabled]                  DNS[*.example.alt]
DOM: Status[Enabled]                        DNS[example.alt] Netbios[EXAMPLE]
SID[S-1-5-21-3274802069-598906262-3677769431]
Setup remote forest trust information...
Namespaces[2] TDO[test.alt]:
TLN: Status[Enabled]                  DNS[*.test.alt]
DOM: Status[Enabled]                   DNS[test.alt] Netbios[TEST] SID[S-1-5-
21-1455776928-3410124986-2843404052]
Validating outgoing trust...
OK: LocalValidation: DC[\\s1.example.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
Validating incoming trust...
OK: RemoteValidation: DC[\\dc1.test.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
Success
```

ВАЖНО

Для входа в доверенный домен через SSSD надо использовать тип связи `external`, а не `forest`.

Проверка доверия:

- просмотр доверия с dc1.test.alt:

```
[root@dc1 ~]# samba-tool domain trust show EXAMPLE.ALT
LocalDomain   Netbios[TEST]   DNS[test.alt]   SID[S-1-5-21-1455776928-
3410124986-2843404052]
TrustedDomain:

NetbiosName:    EXAMPLE
DnsName:        example.alt
SID:            S-1-5-21-3274802069-598906262-3677769431
Type:           0x2 (UPLEVEL)
Direction:      0x3 (BOTH)
Attributes:     0x8 (FOREST_TRANSITIVE)
PosixOffset:    0x00000000 (0)
kerb_EncTypes:  0x18 (AES128_CTS_HMAC_SHA1_96,AES256_CTS_HMAC_SHA1_96)
Namespaces[2] TDO[example.alt]:
TLN: Status[Enabled]                 DNS[*.example.alt]
DOM: Status[Enabled]                  DNS[example.alt] Netbios[EXAMPLE]
SID[S-1-5-21-3274802069-598906262-3677769431]
```

- просмотр доверия с s1.example.alt:

```
[root@s1 ~]# samba-tool domain trust show TEST.ALT
LocalDomain Netbios[EXAMPLE] DNS[example.alt] SID[S-1-5-21-3274802069-
598906262-3677769431]
TrustedDomain:

NetbiosName:    TEST
DnsName:        test.alt
SID:            S-1-5-21-1455776928-3410124986-2843404052
Type:           0x2 (UPLEVEL)
Direction:      0x3 (BOTH)
```

```
Attributes:     0x8 (FOREST_TRANSITIVE)
PosixOffset:    0x00000000 (0)
kerb_EncTypes:  0x18 (AES128_CTS_HMAC_SHA1_96,AES256_CTS_HMAC_SHA1_96)
Namespaces[2] TDO[test.alt]:
TLN: Status[Enabled]                  DNS[*.test.alt]
DOM: Status[Enabled]                        DNS[test.alt] Netbios[TEST]
SID[S-1-5-21-1455776928-3410124986-2843404052]
```

- список трастов:

```
[root@dc1 ~]# samba-tool domain trust list
Type[Forest]   Transitive[Yes] Direction[BOTH]     Name[example.alt]
```

В разных доменах могут быть разные результаты. Результат зависит от типа траста, который установлен с этим доменом.

Если после настройки доверия возникли проблемы с доступом пользователей из трастового домена в свой домен, тогда следует проверить, действительно ли установлен траст:

```
[root@dc1 ~]# samba-tool domain trust validate EXAMPLE.ALT -
Uadministrator@EXAMPLE.ALT
LocalDomain   Netbios[TEST]   DNS[test.alt]   SID[S-1-5-21-1455776928-
3410124986-2843404052]
LocalTDO   Netbios[EXAMPLE]   DNS[example.alt]   SID[S-1-5-21-3274802069-
598906262-3677769431]
OK:     LocalValidation:     DC[\\s1.example.alt]     CONNECTION[WERR_OK]
TRUST[WERR_OK] VERIFY_STATUS_RETURNED
OK: LocalRediscover: DC[\\s1.example.alt] CONNECTION[WERR_OK]
RemoteDC                 Netbios[S1]                 DNS[s1.example.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,F
ULL_SECRET_DOMAIN_6]
Password for [administrator@EXAMPLE.ALT]:
OK:     RemoteValidation:     DC[\\dc1.test.alt]     CONNECTION[WERR_OK]
TRUST[WERR_OK] VERIFY_STATUS_RETURNED
OK: RemoteRediscover: DC[\\dc1.test.alt] CONNECTION[WERR_OK]
```

10.5.3.2. Samba DC и Windows Server с AD

Настройка на стороне Windows:

1) открыть «Диспетчер серверов», выбрать «Средства» → «Active Directory – домены и доверие» (рис. 371);

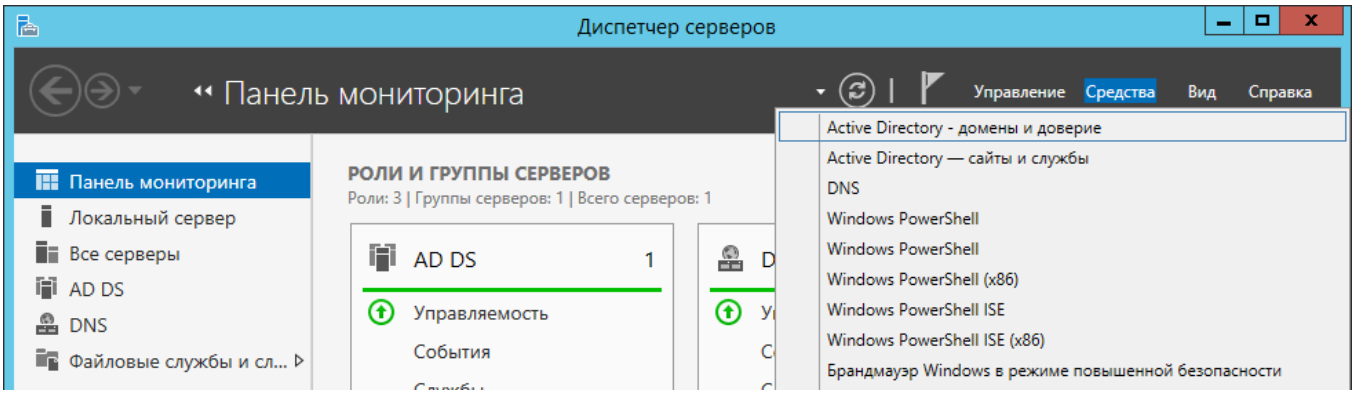


Рис. 371 – Окно «Диспетчер серверов»

2) в открывшемся окне в контекстном меню домена выбрать пункт «Свойства» (рис. 372);

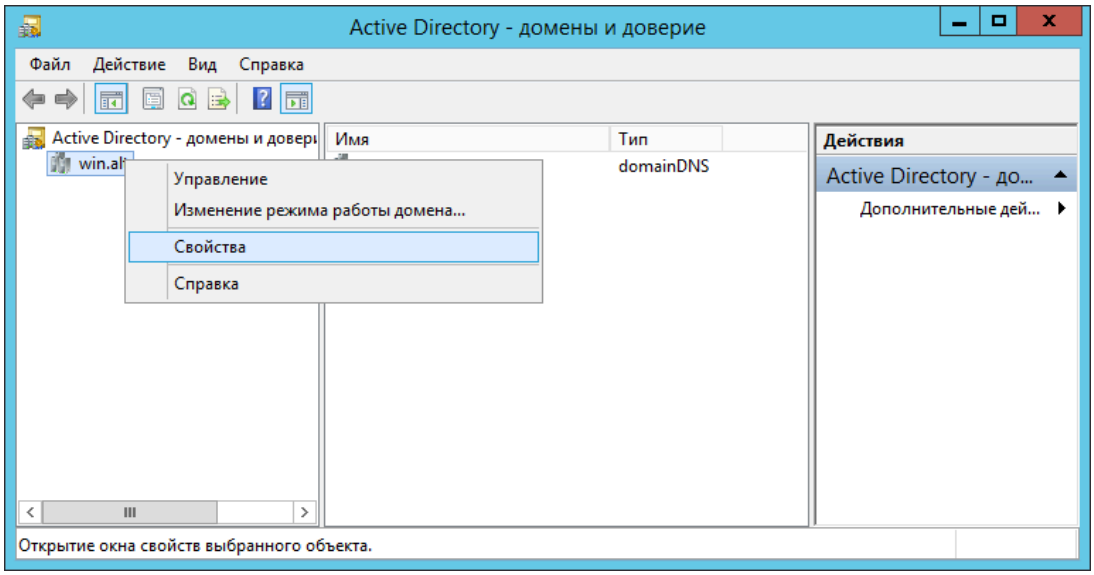


Рис. 372 – Окно «Active Directory – домены и доверие»

3) откроется окно свойств домена. Необходимо перейти во вкладку «Отношения доверия» и нажать кнопку «Создать отношение доверия…» (рис. 373);

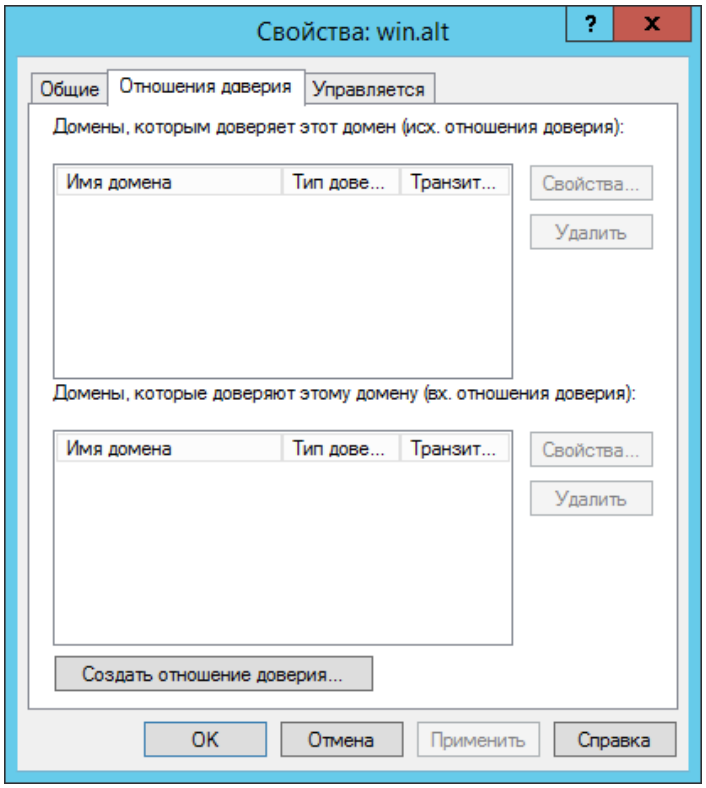


Рис. 373 – Окно свойств домена

4) будет запущен «Мастер создания отношения доверия» (рис. 374);

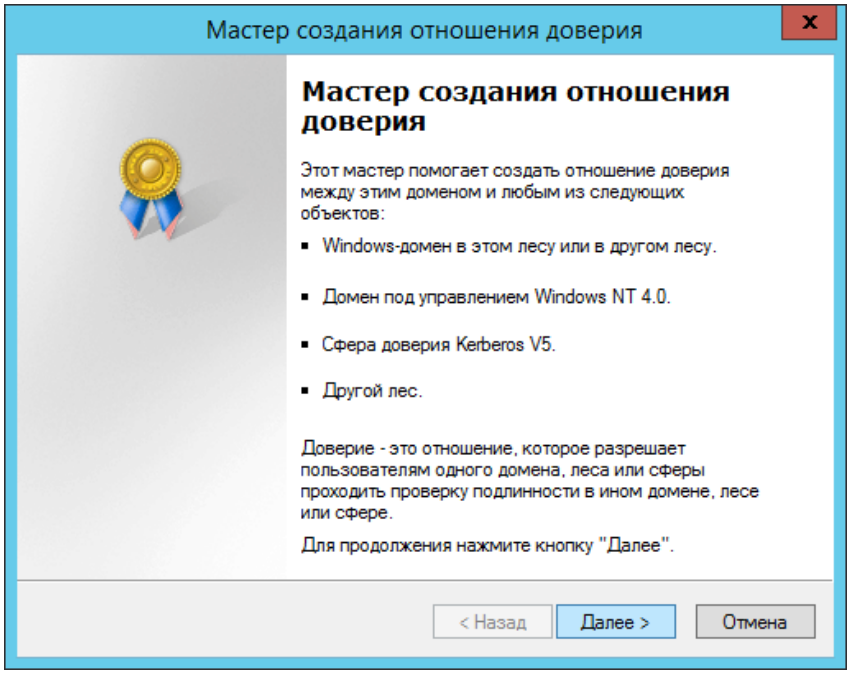


Рис. 374 – Окно «Мастер создания отношения доверия»

5) на втором шаге создания отношения доверия необходимо ввести имя домена Samba DC (в примере TEST.ALT) (рис. 375);

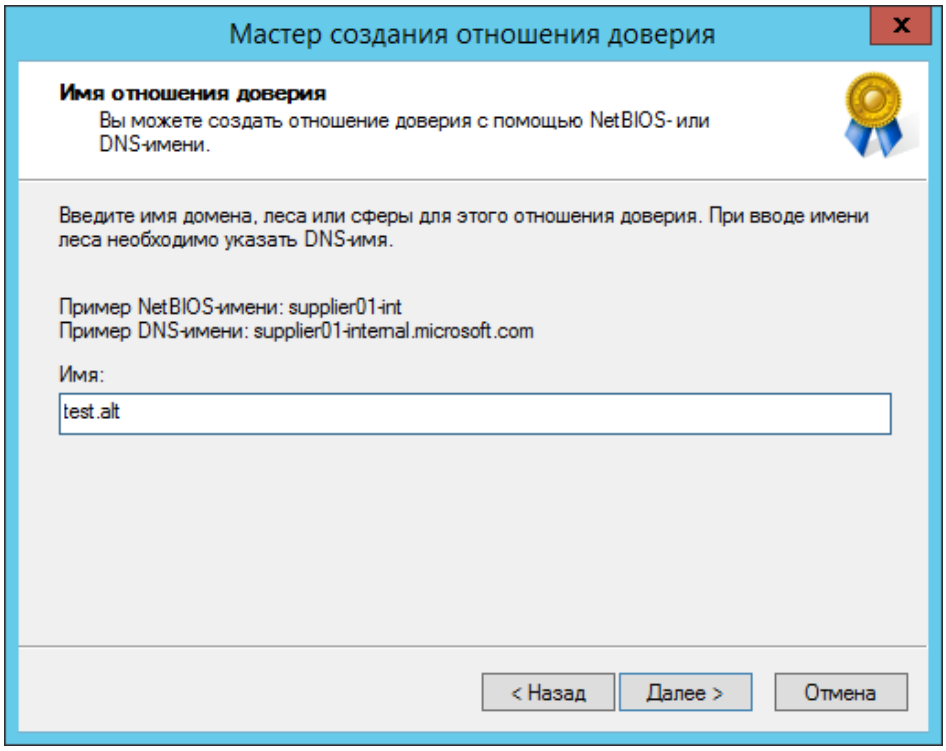


Рис. 375 – Окно ввода имени домена Samba DC

6) на следующем шаге следует выбрать тип доверия (рис. 376);

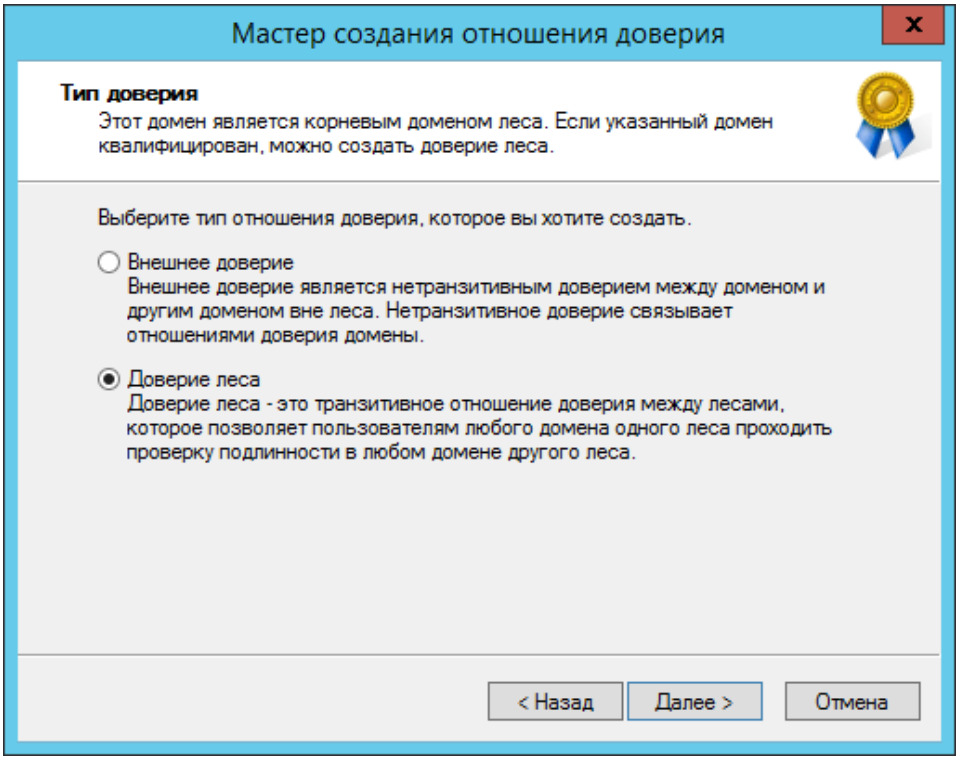


Рис. 376 – Окно выбора типа доверия

7) далее выбирается направление доверия (рис. 377);

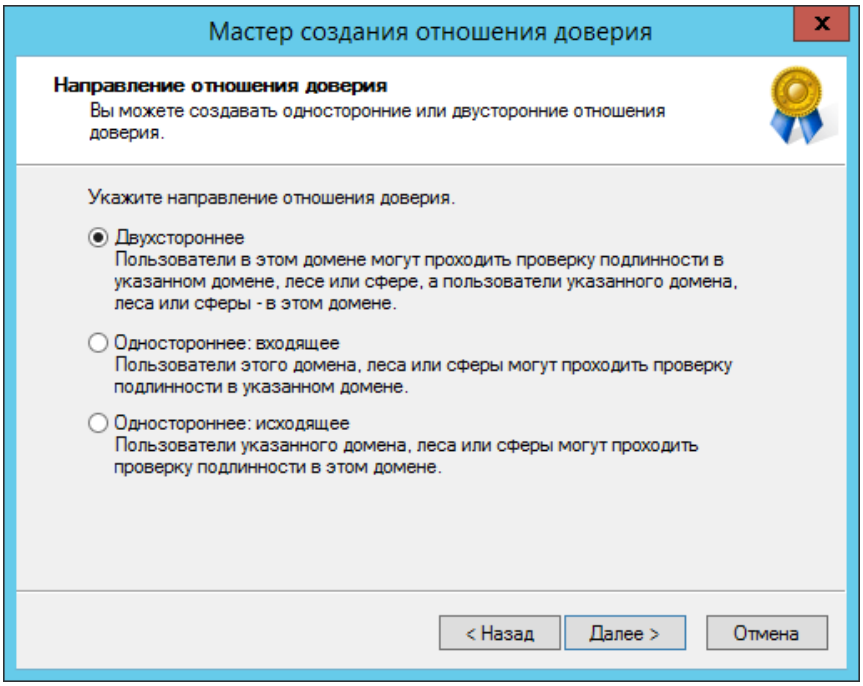


Рис. 377 – Окно выбора направления доверия

8) в открывшемся окне «Стороны отношения доверия» нужно выбрать, на каком из доменов применяется настройка. Если есть права администратора для обоих доменов, можно выбрать пункт «Для данного и указанного домена» (рис. 378);

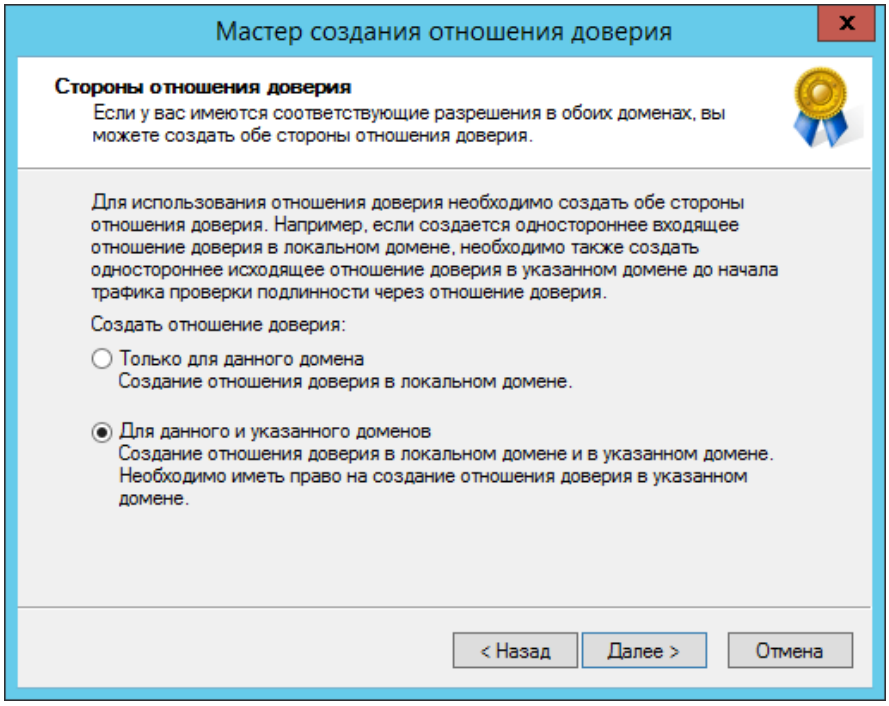


Рис. 378 – Окно выбора настройки доверия

Примечание. Если выбрать параметр «Только для данного домена» (рис. 379), необходимо задать «Пароль отношения доверия» (Trust Secret Key), который в дальнейшем будет использоваться при создании доверительного отношения на стороне Samba DC (рис. 380).

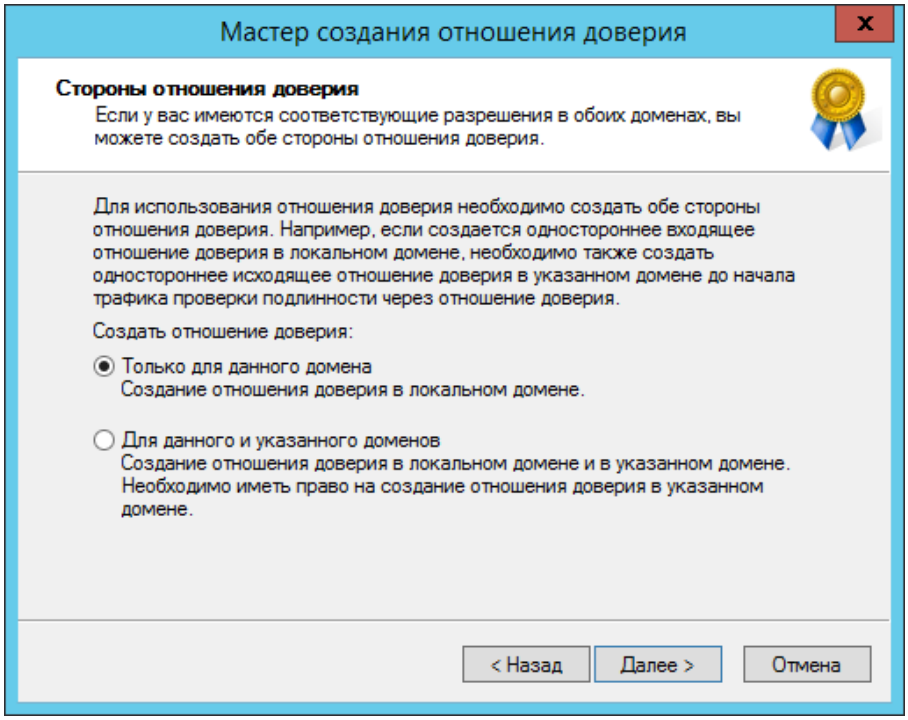


Рис. 379 – Окно выбора параметра «Только для данного домена»

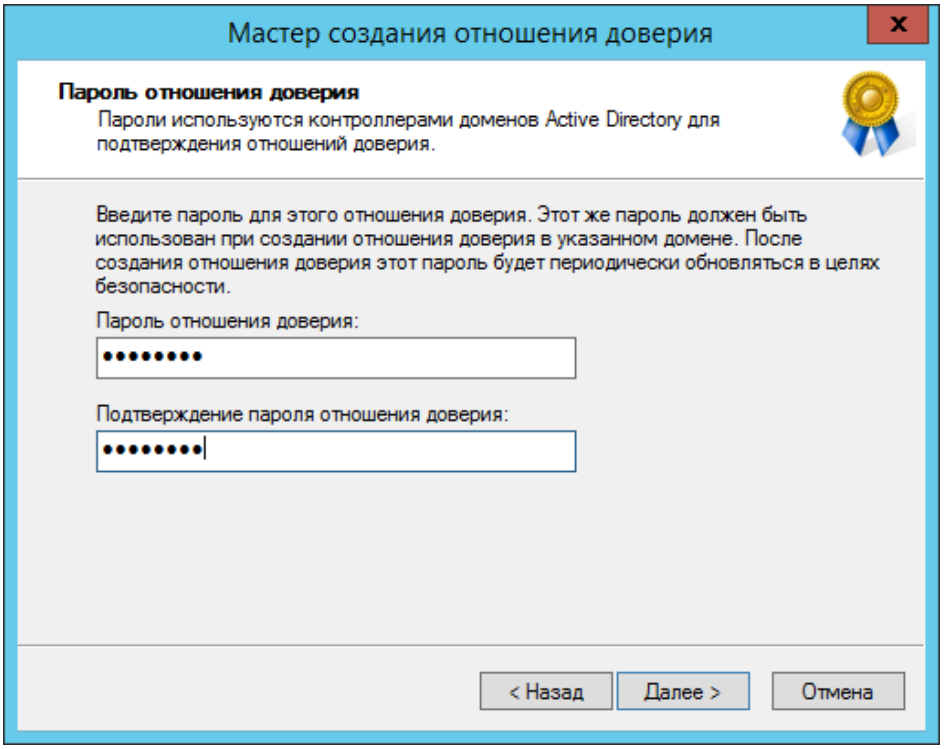


Рис. 380 – Окно ввода пароля «Пароль отношения доверия»

9) на следующем этапе мастер свяжется с удаленным доменом (если он доступен), и запросит имя и пароль пользователя с правами установки доверительных отношений в домене (рис. 381);

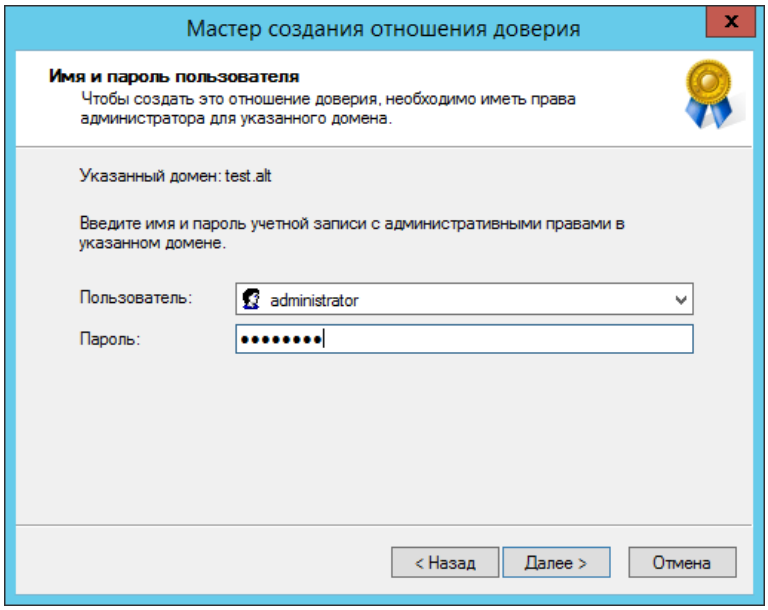


Рис. 381 – Окно ввода имени пользователя и пароля

10) далее на шаге «Уровень проверки подлинности исходящего доверия – Локальный лес» следует выбрать «Проверка подлинности в лесу» (рис. 382);

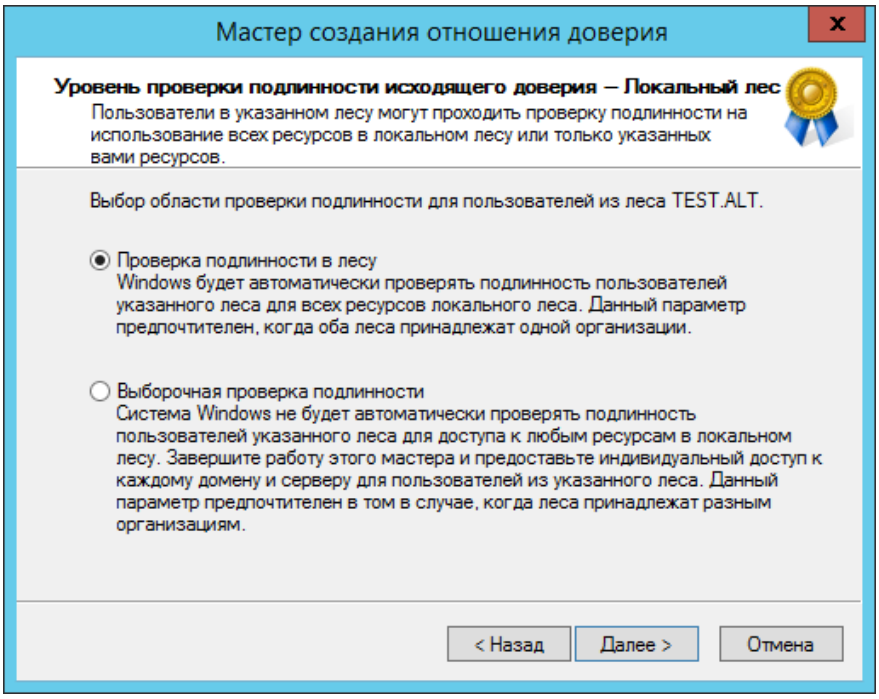


Рис. 382 – Окно выбора области проверки подлинности

11) на шаге «Уровень проверки подлинности исходящего доверия – Указанный лес» также следует выбрать пункт «Проверка подлинности в лесу»;

12) в окне «Выбор доверия завершен» мастер выдаст уведомление о том, что готов создать новое отношение доверия, и покажет краткую сводку с выбранными параметрами. Если согласиться с параметрами, то должно появиться уведомление о том, что создание доверия завершено (рис. 383);

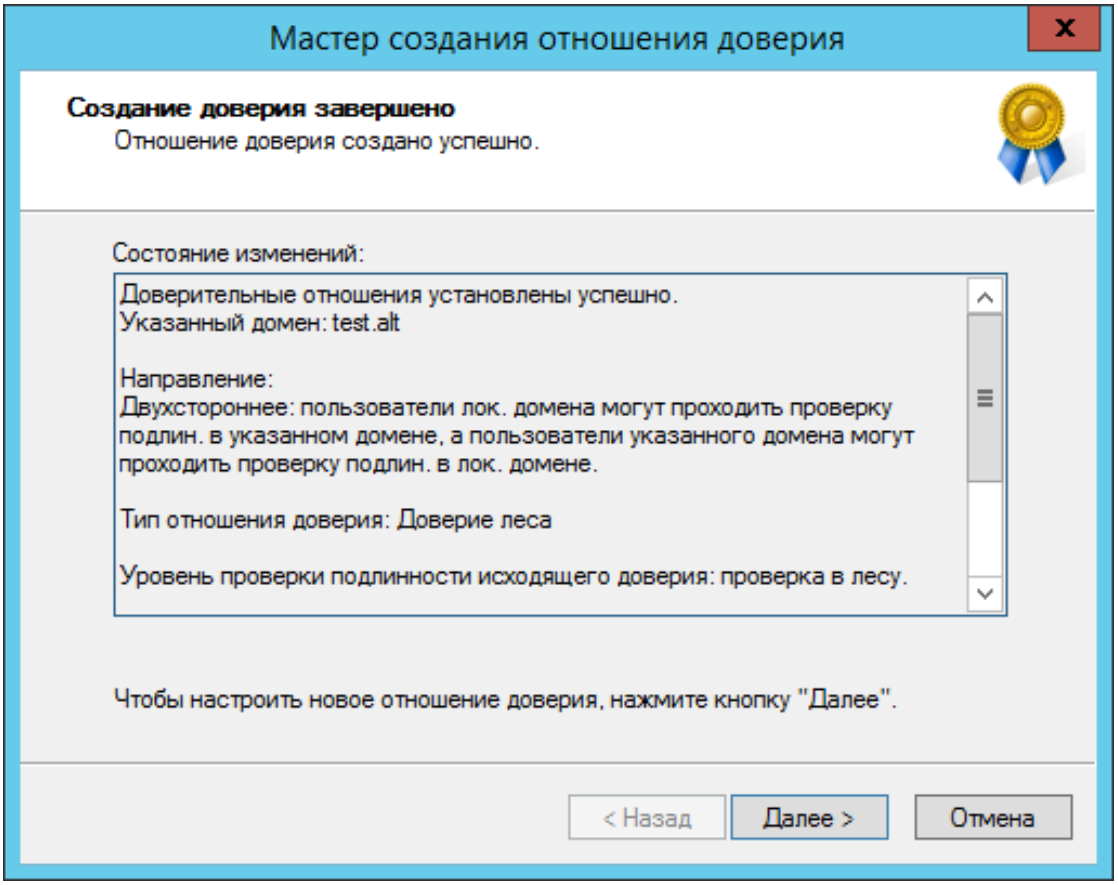


Рис. 383 – Окно «Создание доверия завершено»

13) после нажатия кнопки «Далее» появится окно «Подтверждение исходящего доверия», а после него «Подтверждение входящего доверия». Здесь можно оставить выбранным пункт «Нет, не подтверждаю это исходящее/входящее отношение доверие», так как на стороне Samba DC доверие еще не создавалось (рис. 384).

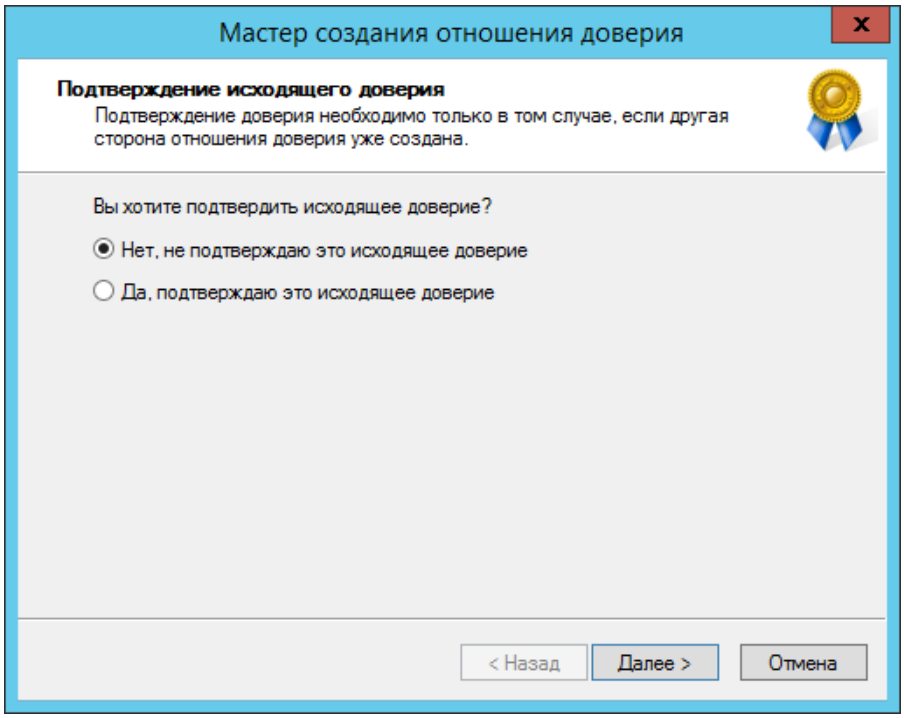


Рис. 384 – Окно подтверждения доверия

В результате будут получены двухсторонние доверительные отношения между доменами (рис. 385).

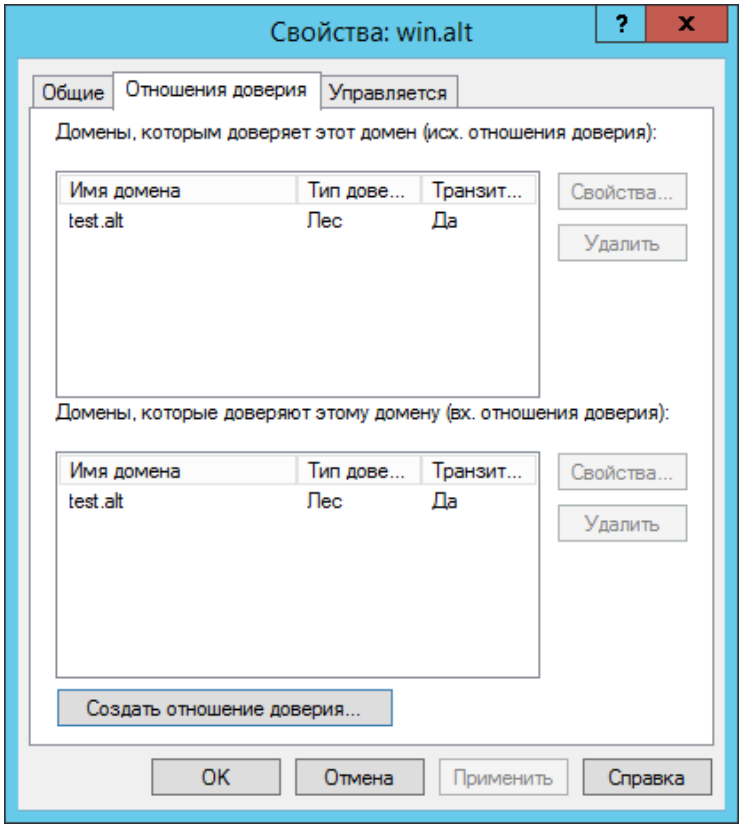


Рис. 385 – Окно установленных доверительных отношения между доменами

На стороне Samba DC для создания доверия необходимо выполнить команду:

```
# samba-tool domain trust create win.alt --type=forest --direction=both --create-location=both -Uadministrator@WIN
```

ВАЖНО

Для входа в доверенный домен через SSSD надо использовать тип связи `external`, а не `forest`.

При появлении запроса введите пароль администратора. Если все настроено верно, будет установлено доверие к домену AD.

```
LocalDomain    Netbios[TEST]    DNS[test.alt]    SID[S-1-5-21-3848605173-1839566900-710408900]
RemoteDC                  Netbios[DC1]                  DNS[DC1.win.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,FULL_SECRET_DOMAIN_6,ADS_WEB_SERVICE,DS_8,__unknown_00008000__]
Password for [administrator@WIN]:
RemoteDomain    Netbios[WIN]    DNS[win.alt]    SID[S-1-5-21-212759798-1661061060-862600140]
Creating local TDO.
Local TDO created
Setting supported encryption types on local TDO.
Setup local forest trust information...
Namespaces[2] TDO[win.alt]:
TLN: Status[Enabled]                  DNS[*.win.alt]
DOM: Status[Enabled]                    DNS[win.alt] Netbios[WIN] SID[S-1-5-21-212759798-1661061060-862600140]
Validating outgoing trust...
OK:      LocalValidation:      DC[\\DC1.win.alt]      CONNECTION[WERR_OK] TRUST[WERR_OK] VERIFY_STATUS_RETURNED
Validating incoming trust…
OK:     RemoteValidation:     DC[\\dc1.test.alt]     CONNECTION[WERR_OK] TRUST[WEER_OK] VERIFY_STATUS_RETURNED
Success.
```

В случае использования Trust Secret Key в параметре `--create-location` нужно заменить опцию `both` на `local`, Samba DC прежде чем создать доверительные отношения сначала запросит Trust Key (??Incoming Trust Password/Outgoing Trust Password), созданный ранее при настройке в Windows.

```
# samba-tool domain trust create win.alt --type=forest --direction=both --create-location=local -Uadministrator@WIN
New Incoming Trust Password:
Retype Incoming Trust Password:
New Outgoing Trust Password:
Retype Outgoing Trust Password:
LocalDomain    Netbios[TEST]    DNS[test.alt]    SID[S-1-5-21-3848605173-1839566900-710408900]
```

```
RemoteDC                  Netbios[DC1]                  DNS[DC1.win.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,…]
Password for [administrator@WIN]:
…
```

Проверка доверия с `dc1.test.alt`:

- просмотр доверия:

```
# samba-tool domain trust show WIN.ALT
LocalDomain   Netbios[TEST]   DNS[test.alt]   SID[S-1-5-21-3848605173-
1839566900-710408900]
TrustedDomain:

NetbiosName:    WIN
DnsName:        win.alt
SID:            S-1-5-21-212759798-1661061060-862600140
Type:           0x2 (UPLEVEL)
Direction:      0x3 (BOTH)
Attributes:     0x8 (FOREST_TRANSITIVE)
PosixOffset:    0x00000000 (0)
kerb_EncTypes:  0x18 (AES128_CTS_HMAC_SHA1_96,AES256_CTS_HMAC_SHA1_96)
Namespaces[2] TDO[win.alt]:
TLN: Status[Enabled]                  DNS[*.win.alt]
DOM: Status[Enabled]                   DNS[win.alt] Netbios[WIN] SID[S-
1-5-21-212759798-1661061060-862600140]
```

- список трастов:

```
# samba-tool domain trust list
Type[Forest]   Transitive[Yes] Direction[BOTH]     Name[win.alt]
```

В разных доменах могут быть разные результаты. Результат зависит от типа траста, который установлен с этим доменом.

Если после настройки доверия возникли проблемы с доступом пользователей из трастового домена в свой домен, тогда следует проверить, действительно ли установлен траст:

```
# samba-tool domain trust validate win.alt -Uadministrator@WIN
LocalDomain   Netbios[TEST]   DNS[test.alt]   SID[S-1-5-21-3848605173-
1839566900-710408900]
LocalTDO  Netbios[WIN]  DNS[win.alt]  SID[S-1-5-21-212759798-1661061060-
862600140]
OK:     LocalValidation:     DC[\\DC1.win.alt]     CONNECTION[WERR_OK]
TRUST[WERR_OK] VERIFY_STATUS_RETURNED
OK: LocalRediscover: DC[\\DC1.win.alt] CONNECTION[WERR_OK]
RemoteDC                  Netbios[DC1]                  DNS[DC1.win.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,F
ULL_SECRET_DOMAIN_6,ADS_WEB_SERVICE,DS_8,__unknown_00008000__]
Password for [administrator@WIN]:
OK:    RemoteValidation:     DC[\\dc2.test.alt]     CONNECTION[WERR_OK]
TRUST[WERR_OK] VERIFY_STATUS_RETURNED
OK: RemoteRediscover: DC[\\dc2.test.alt] CONNECTION[WERR_OK]
```

10.5.4. Управление пользователями и группами

Теперь можно назначать пользователей и группы из доверяющего домена в группу доверенного домена. Так как настроено двустороннее доверие, можно назначать пользователей и группы в обоих направлениях.

Примечание. Предварительно необходимо создать несколько пользователей и групп в обоих доменах.

10.5.4.1. Список пользователей и групп

С помощью команды `wbinfo` нельзя получить список пользователей и групп из доверяющего домена, можно получить список пользователей и групп только из своего домена. Пример:

- команды выполняются на контроллере домена dc1.test.alt:

```
# wbinfo -u --domain=EXAMPLE.ALT
# wbinfo -u --domain=TEST.ALT
TEST\administrator
TEST\guest
TEST\krbtgt
TEST\dns-dc1
TEST\ivanov
```

- команды выполняются на контроллере домена s1.example.alt:

```
# wbinfo -u --domain=EXAMPLE.ALT
EXAMPLE\administrator
EXAMPLE\guest
EXAMPLE\krbtgt
EXAMPLE\dns-s1
EXAMPLE\kim
# wbinfo -u --domain=TEST.ALT
```

Для получения списка всех пользователей можно выполнить LDAP-запрос с помощью команды `samba-tool`. Пример получения списка пользователей из обоих доменов на контроллере домена dc1.test.alt:

```
# samba-tool user list -H ldap://s1 -Uadministrator@EXAMPLE.ALT
Password for [administrator@EXAMPLE.ALT]:
dns-s1
krbtgt
Administrator
Guest
kim
# samba-tool user list -H ldap://dc1 -Uadministrator@TEST.ALT
Password for [administrator@TEST.ALT]:
```

```
dns-dc1
krbtgt
Guest
Administrator
ivanov
```

Получение дополнительной информации о доменах (в примере команды выполняются на контроллере домена dc1.test.alt):

```
# wbinfo --all-domains
BUILTIN
TEST
EXAMPLE

# wbinfo --own-domain
TEST

# wbinfo --trusted-domains
BUILTIN
TEST
EXAMPLE

# wbinfo --online-status
BUILTIN : active connection
TEST : active connection
EXAMPLE : active connection
```

Получение SID пользователей и групп (в примере команды выполняются на контроллере домена dc1.test.alt):

```
# wbinfo -n TEST\\ivanov
S-1-5-21-1455776928-3410124986-2843404052-1105 SID_USER (1)

# wbinfo -n EXAMPLE\\kim
S-1-5-21-3274802069-598906262-3677769431-1104 SID_USER (1)

# wbinfo -n TEST\\office
S-1-5-21-1455776928-3410124986-2843404052-1107 SID_DOM_GROUP (2)

# wbinfo -n EXAMPLE\\office2
S-1-5-21-3274802069-598906262-3677769431-1107 SID_DOM_GROUP (2)

# wbinfo -i TEST\\ivanov
TEST.ALT\ivanov:*:3000022:100::/home/TEST.ALT/ivanov:/bin/false

# wbinfo -i EXAMPLE\\kim
EXAMPLE\kim:*:3000020:3000021::/home/EXAMPLE/kim:/bin/false
```

10.5.4.2. Тестирование аутентификации

С помощью команды `wbinfo` можно протестировать процесс аутентификации разных пользователей из обоих доменов.

`wbinfo` попытается авторизовать пользователя. Первой проверкой будет аутентификация по паролю с открытым текстом. Этот тип аутентификации применяется, когда пользователь входит в систему локально (plaintext не означает, что пароль будет отправлен без шифрования, это просто название процесса входа в систему). Вторая проверка – аутентификация по паролю запрос/ответ. Этот тип аутентификации использует NTLM или Kerberos.

Проверка методов аутентификации (в примере команды выполняются на контроллере домена dc1.test.alt):

```
# wbinfo -a TEST\\ivanov
Enter TEST\ivanov's password:
plaintext password authentication succeeded
Enter TEST\ivanov's password:
challenge/response password authentication succeeded

# wbinfo -a EXAMPLE\\kim
Enter EXAMPLE\kim's password:
plaintext password authentication succeeded
Enter EXAMPLE\kim's password:
challenge/response password authentication succeeded
```

Посмотреть какие контроллеры домена отвечают за аутентификацию:

```
# wbinfo --ping-dc
checking the NETLOGON for domain[TEST] dc connection to "dc1.test.alt" succeeded

# wbinfo --ping-dc --domain=EXAMPLE.ALT
checking the NETLOGON for domain[EXAMPLE.ALT] dc connection to "s1.example.alt" succeeded
```

Назначение пользователей и групп из доверенных доменов в группу доверяющего домена:

```
# wbinfo -n EXAMPLE\\kim
S-1-5-21-3274802069-598906262-3677769431-1104 SID_USER (1)

# samba-tool group addmembers office S-1-5-21-3274802069-598906262-3677769431-1104
Added members to group office

# wbinfo -n EXAMPLE\\office2
S-1-5-21-3274802069-598906262-3677769431-1107 SID_DOM_GROUP (2)
```

```
# samba-tool group addmembers office S-1-5-21-3274802069-598906262-3677769431-1107
Added members to group office

# samba-tool group listmembers office
S-1-5-21-3274802069-598906262-3677769431-1104
ivanov
S-1-5-21-3274802069-598906262-3677769431-1107
```

10.5.4.3. Просмотр доверия в Windows

Модуль RSAT (см. п. 10.7.10) «Active Directory – домены и доверие» (Active Directory – Domain and Trusts) позволяет проверить состояние отношений доверия между доменами (рис. 386).

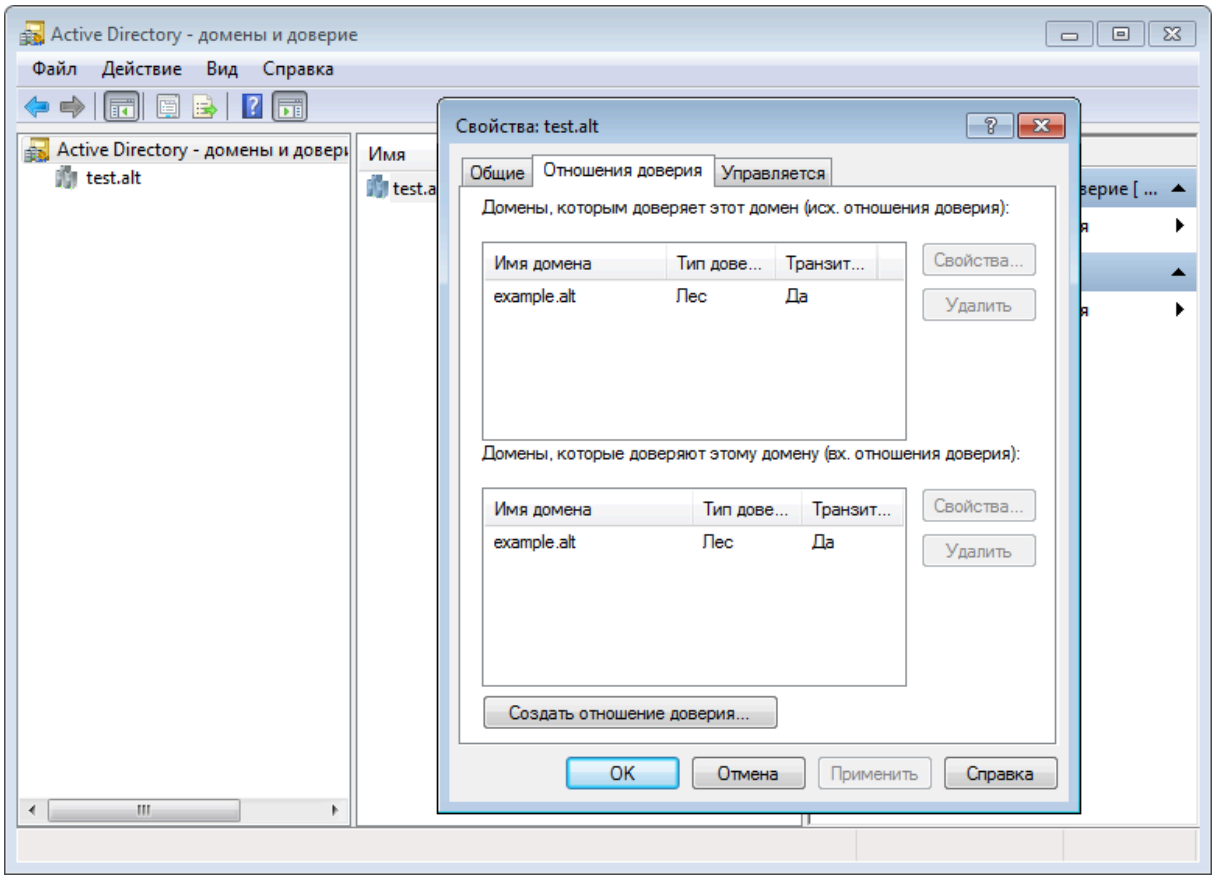


Рис. 386 – Окно установленных доверительных отношения между доменами

В модуле RSAT «Active Directory – пользователи и компьютеры» (Active Directory – Users and Computers) можно просмотреть список пользователей группы (рис. 387).

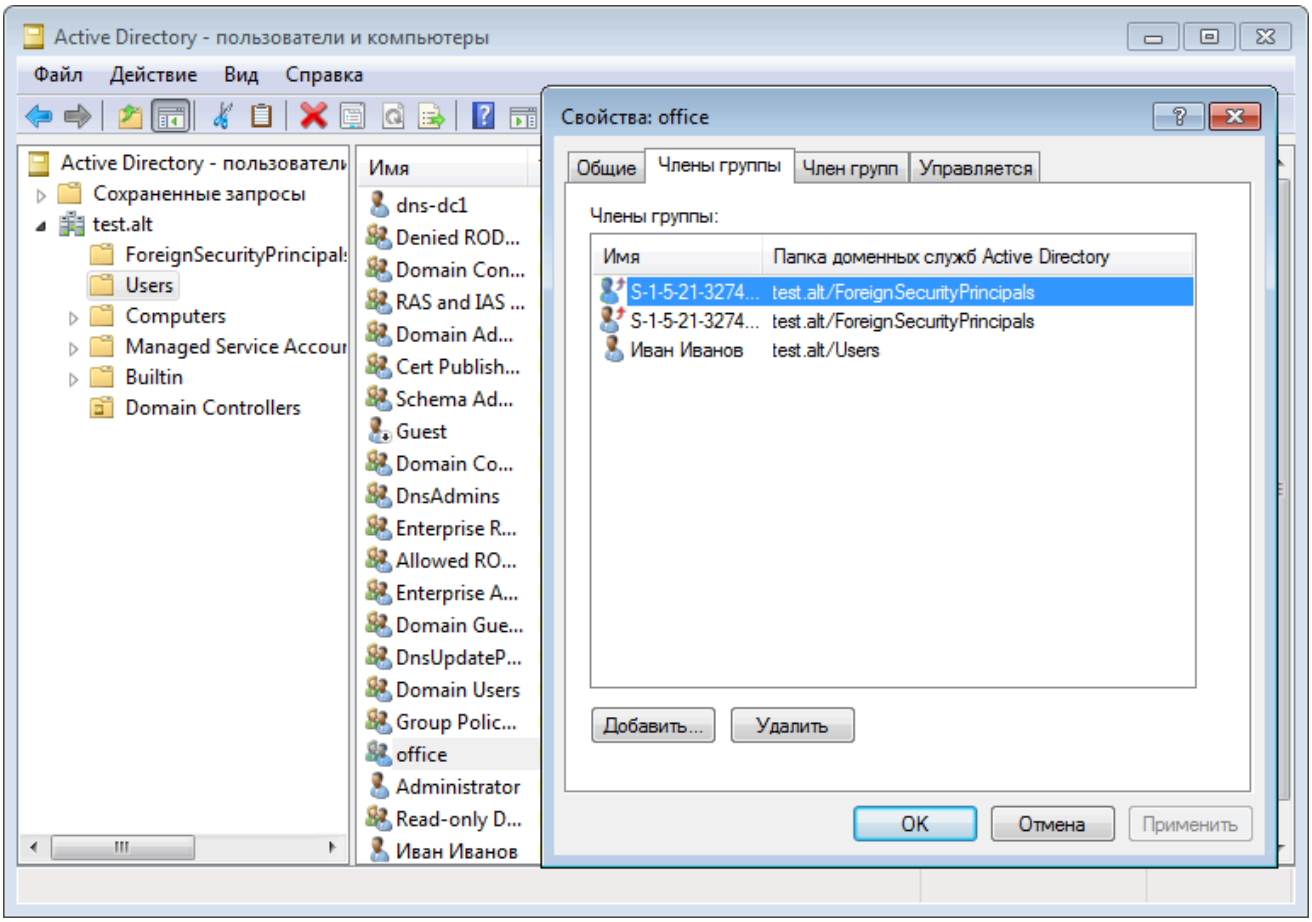


Рис. 387 – Окно списка пользователей «Члены группы»

10.5.5. Использование трастов на LINUX-клиентах

Если необходимо использовать пользователей из обоих доменов (установлены двухсторонние доверительные отношения с типом связи `Лес`), то рабочую станцию с ОС Альт СП следует вводить в домен через winbind (см. п. 10.4.3.3).

10.5.5.1. Настройка winbind

На машине, введенной в домен, необходимо в файле `smb.conf` установить ID-маппинг для обоих доменов (backend = rid/tdb).

Пример файла `smb.conf` на машине, введенной в домен example.alt:

```
[global]
        security = ads
        realm = EXAMPLE.ALT
        workgroup = EXAMPLE
        netbios name = WORK1
        template shell = /bin/bash
        kerberos method = system keytab
```

```
        wins support = no
        winbind use default domain = yes
        winbind enum users = no
        winbind enum groups = no
        template homedir = /home/EXAMPLE.ALT/%U
        winbind refresh tickets = yes
        winbind offline logon = yes
        idmap config * : range = 10000-20000000
        idmap config * : backend = tdb

        idmap config EXAMPLE : backend = rid
        idmap config EXAMPLE : range = 10000-20000000
        idmap config TEST : backend = rid
        idmap config TEST : range = 10000-20000000
```

После перезапуска smbd, nmbd, winbind можно проверить, есть ли возможность просматривать пользователей из обоих доменов:

```
# net rpc trustdom list -Uadministrator
Password for [EXAMPLE\administrator]:
Trusted domains list:

TEST                S-1-5-21-1455776928-3410124986-2843404052

Trusting domains list:

TEST                S-1-5-21-1455776928-3410124986-2843404052


# wbinfo -n TEST\\ivanov
S-1-5-21-1455776928-3410124986-2843404052-1105 SID_USER (1)

# wbinfo -n EXAMPLE\\kim
S-1-5-21-3274802069-598906262-3677769431-1104 SID_USER (1)
```

Проверка с помощью getent:

```
# getent group TEST\\office
TEST\office:*:11107:

# getent group EXAMPLE\\office2
office2:*:11107:

# getent passwd TEST\\ivanov
```

```
TEST\ivanov:*:11105:10513::/home/EXAMPLE.ALT/ivanov:/bin/bash

# getent passwd EXAMPLE\\kim
kim:*:10000:10001:Олег Ким:/home/EXAMPLE.ALT/kim:/bin/bash
```

Проверка входа по SSH пользователями из обоих доменов:

```
$ ssh TEST\\ivanov@192.168.0.126
TEST\ivanov@192.168.0.126's password:
[TEST\ivanov@work1 ~]$ exit
выход
Connection to 192.168.0.126 closed.

$ ssh EXAMPLE\\kim@192.168.0.126
EXAMPLE\kim@192.168.0.126's password:
[kim@work1 ~]$ exit
выход
Connection to 192.168.0.126 closed.
```

10.5.5.2. Настройка SSSD

На машине, введенной в домен, необходимо в файл /etc/sssd/sssd.conf добавить доверенный домен:

```
[domain/EXAMPLE.ALT/TEST.ALT]
use_fully_qualified_names = false
```

После перезапуска sssd можно проверить, есть ли возможность просматривать пользователей из обоих доменов:

```
# getent passwd ivanov
ivanov:*:1855401105:1855400513:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash

# getent passwd kim
```

10.5.6. Удаление доверия

10.5.6.1. На стороне Samba

Пример удаления доверия на контроллере домена dc1.test.alt:

```
# samba-tool domain trust delete EXAMPLE.ALT -U administrator@EXAMPLE.ALT
LocalDomain Netbios[TEST] DNS[test.alt] SID[S-1-5-21-1455776928-3410124986-2843404052]
RemoteDC Netbios[S1] DNS[s1.example.alt] ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,FULL_SECRET_DOMAIN_6]
```

```
Password for [administrator@EXAMPLE.ALT]:
RemoteDomain   Netbios[EXAMPLE]   DNS[example.alt]   SID[S-1-5-21-3274802069-598906262-3677769431]
RemoteTDO deleted.
```

Проверка:

```
# samba-tool domain trust list
```

10.5.6.2. На стороне Windows Server с AD

Удаление доверия:

1) открыть «Диспетчер серверов», выбрать «Средства» → «Active Directory – домены и доверие» (рис. 388);

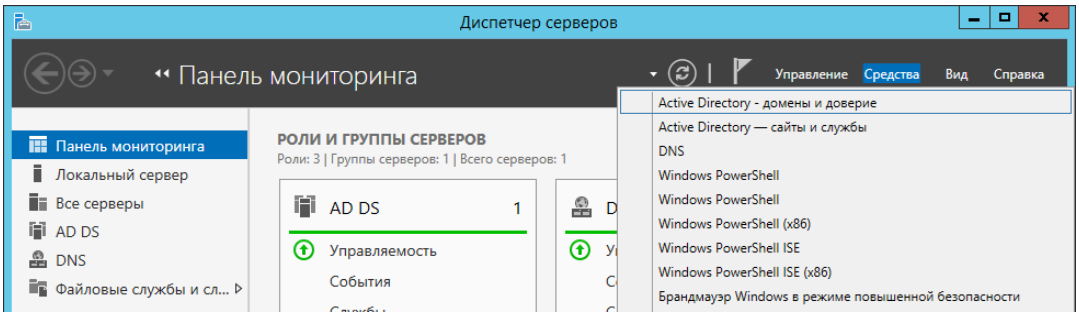


Рис. 388 – Окно «Диспетчер серверов»

2) в открывшемся окне в контекстном меню домена выбрать пункт «Свойства» (рис. 389);

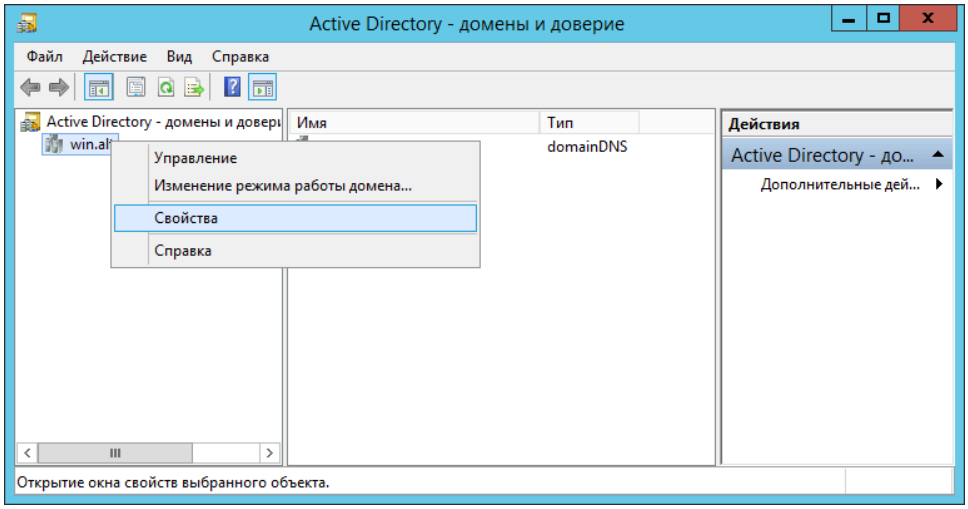


Рис. 389 – Окно «Active Directory – домены и доверие»

3) откроется окно свойств домена. Необходимо перейти во вкладку «Отношения доверия» и нажать кнопку «Создать отношение доверия…» (рис. 390);

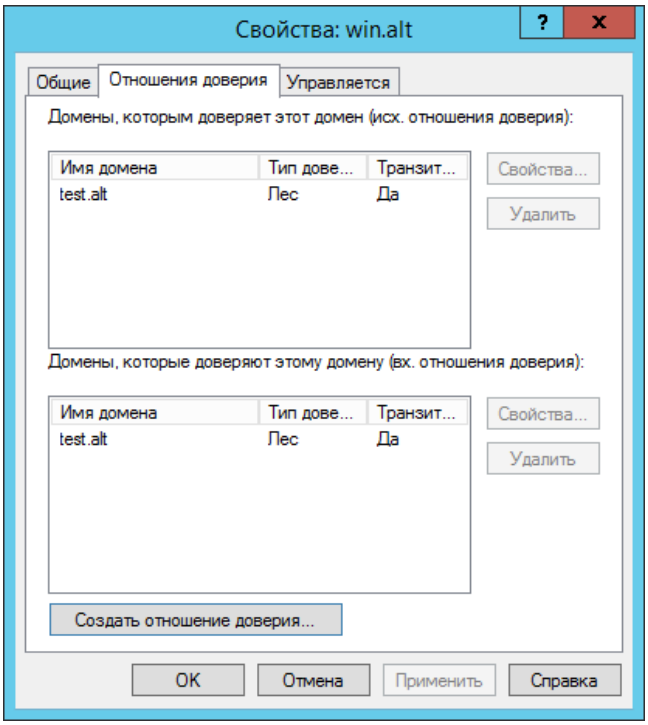


Рис. 390 – Вкладка «Отношения доверия»

4) в группе «Домены, которым доверяет этот домен (исх. отношения доверия)» или группе «Домены, которые доверяют этому домену (вх. отношения доверия)» выбрать доверие, которое требуется удалить, а затем нажать кнопку «Удалить»;

5) в открывшемся окне выбрать пункт, где нужно удалить доверие, и нажать кнопку «ОК» (рис. 391).

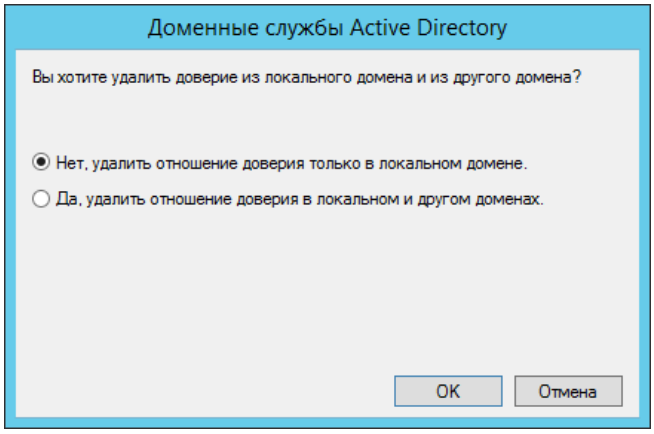


Рис. 391 – Окно выбора пункта удаления доверия

Если выбран параметр «Нет, удалить отношение доверия только в локальном домене», рекомендуется повторить эту процедуру для домена второй стороны.

Если выбран параметр «Да, удалить отношение доверия в локальном и другом доменах», необходимо ввести учетную запись и пароль администратора для домена второй стороны.

10.6. Конфигурирование Samba

10.6.1. Журналирование в Samba

Файлы журналов службы Samba находятся в каталоге `/var/log/samba/`.

10.6.1.1. Уровни журналирования

10.6.1.1.1. Установка уровня журналирования в файле `smb.conf`

Установить уровень журналирования для Samba можно, используя параметр `log level` в файле `/etc/samba/smb.conf`. Для разных классов отладки можно указывать разные уровни журналирования и отдельные файлы журналов.

Чтобы настроить ведение журналов для определенных классов так, чтобы они входили в другой файл, а не в файл журнала, вы можете добавить @PATH к классу.

Примеры:

- установить уровень журнала для всех классов отладки на 3:

```
log level = 3
```

- установить общий уровень журнала на 3 и для классов passdb и auth на 5:

```
log level = 3 passdb:5 auth:5
```

- установить уровень журнала для класса winbind на 1 и писать логи в файл `/var/log/winbind.log`:

```
log level = 3 winbind:1@/var/log/winbind.log
```

Получить дополнительную информацию и список классов отладки можно на справочной странице smb.conf(5) (man smb.conf).

10.6.1.1.2. Установка уровня журналирования при выполнении команд

Команды Samba используют уровень журналирования, установленный в параметре `log level` в файле `/etc/samba/smb.conf`. Это значение можно переопределить, используя опцию `-d` для всех команд Samba.

Например:

```
$ net usershare add Share2 /tmp/share2 -d 5
```

10.6.1.2. Настройка ведения журнала аудита

Samba поддерживает ведение журнала событий аутентификации и авторизации, а также ведение журнала изменений базы данных AD DC. Это позволяет регистрировать, например, неудачные запросы аутентификации или сбросы пароля.

Ведение журнала аудита является локальной настройкой, эту функцию необходимо включить на каждом сервере Samba. События регистрируются на сервере Samba, на котором произошло событие. Чтобы хранить все журналы на централизованном сервере, следует настроить централизованный сервер системных журналов, настроить Samba для регистрации в syslog и настроить syslog для отправки журналов на централизованный сервер.

Описание параметров `logging`, `syslog` и `syslog only` можно посмотреть на справочной странице smb.conf(5) (man smb.conf).

Примечание. Samba генерирует некоторые журналы на узле в конфигурации файлового сервера и члена домена, но полная поддержка доступна только в AD DC.

Samba поддерживает протоколирование успешных событий авторизации, но не неуспешных событий авторизации. Samba может регистрировать как успешные, так и неуспешные события аутентификации.

Примечания:

1. Аутентификация происходит, когда Samba проверяет комбинацию имени пользователя и пароля.
2. Авторизация происходит при запуске сеанса.

Журнал аудита Samba поддерживает стандартный формат и формат JSON. Можно включить каждый формат по отдельности или оба вместе, используя разные классы отладки журнала.

В зависимости от уровня журналирования Samba регистрирует разные события. Чтобы ограничить количество записей в журнале, можно увеличить уровень журналирования только для классов отладки, связанных с аудитом.

Для управления уровнем журнала аудита можно использовать следующие классы отладки:

- `auth_audit` – стандартный формат журнала;
- `auth_json_audit` – формат JSON.

Пример включения ведения журнала аудита аутентификации (установить уровень журнала по умолчанию – 1, включить регистрацию неудачных и успешных запросов аутентификации – 3):

1) установить в секции `[global]` файла `/etc/samba/smb.conf`:

```
log level = 1 auth_audit:3 auth_json_audit:3
```

2) перезапустить службу Samba.

Пример записей о неуспешной и успешной попытках аутентификации пользователя на контроллере домена Samba с использованием стандартного формата журнала:

```
[2023/04/13 11:51:20.341735, 2]
../../auth/auth_log.c:647(log_authentication_event_human_readable)
  Auth: [Kerberos KDC,ENC-TS Pre-authentication] user
[(null)]\[petrov\\@TEST.ALT@TEST.ALT] at [Thu, 13 Apr 2023 11:51:20.341726 EET] with
[aes256-cts-hmac-sha1-96] status [NT_STATUS_WRONG_PASSWORD] workstation [(null)]
remote host [ipv4:192.168.0.125:49382] mapped to [TEST]\[petrov]. local host [NULL]

[2023/04/13 11:51:32.859080, 3]
../../auth/auth_log.c:647(log_authentication_event_human_readable)
  Auth: [Kerberos KDC,ENC-TS Pre-authentication] user
[(null)]\[petrov\\@TEST.ALT@TEST.ALT] at [Thu, 13 Apr 2023 11:51:32.859051 EET] with
[aes256-cts-hmac-sha1-96] status [NT_STATUS_OK] workstation [(null)] remote host
[ipv4:192.168.0.125:52630] became [TEST]\[petrov] [S-1-5-21-1723588197-2340999690-
1379671080-1106]. local host [NULL]
```

Пример записей о неуспешной и успешной попытках аутентификации пользователя на контроллере домена Samba с использованием формата JSON:

```
[2023/04/13 11:46:08.614095, 2]
../../auth/auth_log.c:647(log_authentication_event_human_readable)
  Auth: [Kerberos KDC,ENC-TS Pre-authentication] user
[(null)]\[petrov\\@TEST.ALT@TEST.ALT] at [Thu, 13 Apr 2023 11:46:08.614055 EET] with
[aes256-cts-hmac-sha1-96] status [NT_STATUS_WRONG_PASSWORD] workstation [(null)]
remote host [ipv4:192.168.0.125:42738] mapped to [TEST]\[petrov]. local host [NULL]
  {"timestamp": "2023-04-13T11:46:08.614338+0200", "type": "Authentication",
"Authentication": {"version": {"major": 1, "minor": 2}, "eventId": 4625, "logonId":
"10c3af2c9c39fef4", "logonType": 3, "status": "NT_STATUS_WRONG_PASSWORD",
"localAddress": null, "remoteAddress": "ipv4:192.168.0.125:42738",
"serviceDescription": "Kerberos KDC", "authDescription": "ENC-TS Pre-authentication",
"clientDomain": null, "clientAccount": "petrov\\@TEST.ALT@TEST.ALT", "workstation":
null, "becameAccount": "petrov", "becameDomain": "TEST", "becameSid": "S-1-5-21-
```

1723588197-2340999690-1379671080-1106", "mappedAccount": "petrov", "mappedDomain": "TEST", "netlogonComputer": null, "netlogonTrustAccount": null, "netlogonNegotiateFlags": "0x00000000", "netlogonSecureChannelType": 0, "netlogonTrustAccountSid": null, "passwordType": "aes256-cts-hmac-sha1-96", "duration": 6096}}

```
[2023/04/13 11:48:45.902778, 3] ../../auth/auth_log.c:647(log_authentication_event_human_readable)
Auth: [Kerberos KDC,ENC-TS Pre-authentication] user [(null)]\[petrov\\@TEST.ALT@TEST.ALT] at [Thu, 13 Apr 2023 11:48:45.902759 EET] with [aes256-cts-hmac-sha1-96] status [NT_STATUS_OK] workstation [(null)] remote host [ipv4:192.168.0.125:52840] became [TEST]\[petrov] [S-1-5-21-1723588197-2340999690-1379671080-1106]. local host [NULL]
```

{"timestamp": "2023-04-13T11:48:45.902942+0200", "type": "Authentication", "Authentication": {"version": {"major": 1, "minor": 2}, "eventId": 4624, "logonId": "71c99af1de51eaf6", "logonType": 3, "status": "NT_STATUS_OK", "localAddress": null, "remoteAddress": "ipv4:192.168.0.125:52840", "serviceDescription": "Kerberos KDC", "authDescription": "ENC-TS Pre-authentication", "clientDomain": null, "clientAccount": "petrov\\@TEST.ALT@TEST.ALT", "workstation": null, "becameAccount": "petrov", "becameDomain": "TEST", "becameSid": "S-1-5-21-1723588197-2340999690-1379671080-1106", "mappedAccount": "petrov", "mappedDomain": "TEST", "netlogonComputer": null, "netlogonTrustAccount": null, "netlogonNegotiateFlags": "0x00000000", "netlogonSecureChannelType": 0, "netlogonTrustAccountSid": null, "passwordType": "aes256-cts-hmac-sha1-96", "duration": 9023}}

Пример включения ведения журнала аудита базы данных DC AD (установить уровень журнала по умолчанию – 1, включить ведение журнала изменений базы данных в формате JSON):

1) установить в секции `[global]` файла `/etc/samba/smb.conf`:

   `log level = 1 dsdb_json_audit:5 dsdb_password_json_audit:5 dsdb_group_json_audit:5 dsdb_transaction_json_audit:5`

2) перезапустить службу Samba.

10.6.1.3. Интерпретация журналов аудита JSON

Если включено ведение журнала аудита в формате JSON, сведения о различных событиях регистрируются в формате JSON. Каждое событие имеет множество атрибутов. Внешний слой атрибутов состоит из трех элементов: метки времени, типа события и объекта данных:

```
{
  "timestamp": 2023-04-13T11:48:45.902942+0200,
  "type": одно из значений "Authentication", "Authorization", "dsdbChange",
          "dsdbTransaction", "passwordChange", "replicatedUpdate",
          "groupChange",
  type: { data }
}
```

Примечание. Некоторые атрибуты по-прежнему будут присутствовать в журнале, даже если они неприменимы. Например, если NETLOGON не используется (согласно `serviceDescription`), для параметра `netlogonComputer` будет установлено значение «null», для параметра `netlogonNegotiateFlags` будет установлено значение «0x00000000», а другие поля сетевого входа будут иметь аналогичные пустые значения.

Таблица 46 – Аутентификация

Атрибут	Значение
`authDescription`	Тип аутентификации, в том числе: - «simple bind/TLS», «simple bind»: простая привязка LDAP с каналом TLS или без него; - «guest»: анонимный запрос SMB1; - «bare-NTLM»: SMB, использующий протокол NT1; - «plaintext»: обычный текст SMB1; - «interactive»: как если бы физически находились на рабочей станции; - «network»: проверка подлинности запроса/ответа по сети; - «Unknown Auth Description», «Unknown Pre-authentication»: события KDC; - «ServerAuthenticate»: запрос/ответ компьютера при входе в систему с использованием NETLOGON; - «LDAP Modify»: смена пароля (не событие аутентификации, но регистрируется здесь, чтобы администратор не пропустил его)
`becameAccount`	Имя учетной записи, под которой выполнен вход (может отличаться от учетной записи, предоставленной клиентом)
`becameDomain`	Имя домена, в который произведен вход
`becameSid`	SID аутентифицированной учетной записи
`clientAccount`	Сообщаемое клиентом имя учетной записи
`clientDomain`	Имя домена, о котором сообщает клиент
`duration`	Сколько времени заняла аутентификация в микросекундах
`eventId`	Идентификатор события Windows, указывающий в общих чертах, что произошло
`localAddress`	Адрес сервера и используемый порт
`logonId`	Случайный 64-битный идентификатор, помогающий отслеживать события входа в систему на разных этапах
`logonType`	Тип входа в Windows, для Samba один из: - 2: интерактивный, то есть на этом компьютере; - 3: по сети; - 8: NetworkCleartext с использованием нехешированных паролей
`mappedAccount`	Имя учетной записи клиента, преобразованное в имя учетной записи AD
`mappedDomain`	Клиентский домен, преобразованный в доменное имя AD
`netlogonComputer`	Заявленное имя компьютера в аутентификации NETLOGON RPC
`netlogonNegotiateFlags`	Флаги параметров согласования NETLOGON
`netlogonSecureChannelType`	Тип используемого канала NETLOGON

Окончание таблицы 46

Атрибут	Значение
`netlogonTrustAccount`	Учетная запись, используемая для аутентификации NETLOGON
`netlogonTrustAccountSid`	SID, принадлежащий доверенной учетной записи NETLOGON
`passwordType`	Алгоритм/протокол пароля (например, «HMAC-SHA256», «NTLMv2», «arcfour-hmac-md5»)
`remoteAddress`	Заявленный адрес (и порт) удаленного клиента
`serviceDescription`	Тип службы, например, LDAP, SMB2, NETLOGON, Kerberos KDC
`status`	Сообщение NT STATUS. Для успешной аутентификации это будет «NT_STATUS_OK». Неудачная аутентификация может иметь здесь «NT_STATUS_OK», если аутентификация не удалась после регистрации этого сообщения, но обычно имеет код ошибки. Некоторые типы сообщений: - NT_STATUS_ACCESS_DENIED: доступ запрещен по неустановленным причинам, но, вероятно, из-за неправильных учетных данных; - NT_STATUS_WRONG_PASSWORD: неверный пароль; - NT_STATUS_NO_SUCH_USER: неверный пользователь; - NT_STATUS_NO_SUCH_DOMAIN: неверный домен; - NT_STATUS_ACCOUNT_RESTRICTION: учетная запись защищена или иным образом ограничена; - NT_STATUS_INVALID_SYSTEM_SERVICE: выбранная служба аутентификации недоступна; - NT_STATUS_NO_MEMORY: сервер не может завершить аутентификацию и заявляет о нехватке памяти
`workstation`	Заявленное имя клиентской рабочей станции

Таблица 47 – Успешные события авторизации

Атрибут	Значение
`account`	Имя авторизуемой учетной записи
`accountFlags`	Битовое поле атрибутов учетной записи
`authType`	Строка, описывающая тип авторизации (например, «krb5», «NTLMSSP», «simple bind»)
`domain`	Домен
`localAddress`	Адрес сервера и используемый порт
`logonServer`	Сервер, на котором выполнена аутентификация
`remoteAddress`	Видимый адрес клиента
`serviceDescription`	Тип службы, например, «LDAP», «SMB2», «DCE/RPC»
`sessionId`	GUID, идентифицирующий сеанс
`sid`	SID авторизованной учетной записи
`transportProtection`	Тип защиты канала (например, «SMB», «TLS», «SEAL», «NONE»)

10.6.2. Создание keytab-файла

SPN (Service Principal Name) – уникальный идентификатор экземпляра сервиса. SPN используется аутентификацией Kerberos для сопоставления экземпляра сервиса с учетной записью сервиса (service logon account). Это позволяет клиентским приложением аутентифицироваться в роли сервиса даже не зная имени пользователя.

До того, как аутентификация Kerberos сможет использовать SPN для аутентификации сервиса, SPN должен быть привязан к учетной записи, которая будет использоваться для входа. К учетной записи может быть привязано несколько SPN. SPN может быть привязан только к одной учетной записи. Если учетная запись, привязанная к SPN, изменяется, то необходимо заново выполнить привязку.

Можно иметь столько SPN, сколько необходимо. Когда клиент хочет воспользоваться сервисом, он находит экземпляр сервиса и составляет SPN для этого экземпляра, далее использует этот SPN для аутентификации. Если клиент не может найти правильный SPN, он не сможет запросить билет службы.

П р и м е ч а н и е . Если клиент не может найти правильный SPN, он не сможет запросить билет службы. Поэтому формирование SPN было глобально нормализовано:

- для файлового сервера могут использоваться следующие SPN (их можно добавить столько, сколько нужно):
  `HOST/fileserver.test.alt`
  `HOST/fileserver`
  `HOST/fileserver@TEST.ALT`
  `CIFS/fileserver.test.alt`
- для веб-сервера (подробнее см. п. 10.7.5.1):
  `HTTP/web.test.alt`
- для прокси-сервера:
  `HTTP/proxy.test.alt`
- на практике можно сопоставить SPN с IP-адресом, но это не рекомендуется:
  `HOST/192168.0.129@TEST.ALT`

Keytab-файл – это файл, содержащий пары Kerberos принципалов и их ключей (полученных с использованием Kerberos пароля). Эти файлы используются для аутентификации в системах, использующих Kerberos, без ввода пароля. Если пароль принципала изменится, то keytab-файл необходимо будет сгенерировать заново.

ВАЖНО

Каждый кто имеет разрешения на чтения keytab-файла может воспользоваться любыми ключами в нем. Чтобы предотвратить нежелательное использование, необходимо ограничивать права доступа при создании keytab-файла.

10.6.2.1. Создание SPN и генерация keytab с помощью samba-tool

Добавить имена SPN для пользователя можно с помощью команды samba-tool:

```
samba-tool spn add host/fdqn@KerberosRealm <sAMAccount name>
```

После добавления SPN можно сгенерировать keytab, выполнив команду:

```
samba-tool domain exportkeytab <имя>.keytab --principal=[<sAMAccount name> | <SPN>]
```

В результате выполнения этой команды будет создан keytab-файл `<имя>.keytab`, содержащий UPN или SPN, в зависимости от того, что было указано в параметре `--principal`.

Получить дополнительную информацию можно на справочной странице samba-tool (8) (man samba-tool).

Примечание. В команде нужно использовать или <sAMAccount name> или <SPN>, но не оба параметра сразу.

Пример:

- привязать к пользователю SPN:

```
# samba-tool spn add HTTP/test.alt webauth
```

- создать keytab:

```
# samba-tool domain exportkeytab /tmp/web.keytab --principal=HTTP/test.alt
Export one principal to /tmp/keytab
```

- проверка:

```
# klist -ke /tmp/web.keytab
Keytab name: FILE:/tmp/web.keytab
KVNO Principal
----  ---------------------------------------------------------------
----------------
   2 HTTP/test.alt@TEST.ALT (DEPRECATED:arcfour-hmac)
```

Также можно проверить авторизацию в домене по имени SPN с помощью keytab-файла. Для этого на контроллере домена получить билет Kerberos:

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

И выполнить команду:

```
kinit -5 -V -k -t /tmp/web.keytab HTTP/test.alt
Using default cache: /tmp/krb5cc_0
Using principal: HTTP/test.alt@TEST.ALT
Using keytab: /tmp/web.keytab
Authenticated to Kerberos v5
```

П р и м е ч а н и е . Если при проверке авторизации возникает ошибка:

```
kinit: Client not found in Kerberos database while getting initial credentials
```

необходимо в ADMC изменить для пользователя webauth значение параметра `userPrincipalName` на значение `servicePrincipalName + REALM` (в данном примере нужно поменять webauth на HTTP/test.alt@TEST.ALT).

10.7. Администрирование Samba

10.7.1. Управление пользователями и группами

10.7.1.1. В ADMC

Для управления пользователями и группами в AD можно использовать модуль удаленного управления базой данных конфигурации (ADMC). Подробнее см. п. 9.2.4.

10.7.1.2. samba-tool

Для управления пользователями и группами в AD можно использовать инструмент командной строки samba-tool.

Команды управления пользователями представлены в таблице 48.

Т а б л и ц а 48 – Команды управления пользователями инструмента samba-tool

Команда	Описание	Примечание
`user add <имя пользователя> [<пароль>]`	Создать нового пользователя в AD	
`user create <имя пользователя> [<пароль>]`	Создать нового пользователя в AD	Команда доступна только в целях совместимости. Рекомендуется вместо этой команды использовать команду `samba-tool user add`

Продолжение таблицы 48

Команда	Описание	Примечание
`user delete` <имя пользователя> [<опции>]	Удалить существующего пользователя	
`user disable` <имя пользователя>	Отключить пользовательский аккаунт	
`user edit` <имя пользователя>	Редактировать объект пользовательского аккаунта AD	В опции `-editor =` <редактор> можно указать редактор (по умолчанию `vi`)
`user enable` <имя пользователя>	Включить пользовательский аккаунт	
`user setprimarygroup` <имя пользователя> <имя группы>	Установить основную группу для учетной записи пользователя	
`user getgroups` <имя пользователя>	Вывести список групп, в которые входит учетная запись пользователя напрямую	
`user list`	Вывести список пользователей	По умолчанию выводятся sAMAccountNames пользователей. Можно использовать следующие опции: - `--full-dn` – показать различающиеся имена пользователей (CN) вместо sAMAccountNames; - `-b BASE_DN|--base-dn=BASE_DN` – вывести пользователей с указанным базовым DN; - `--hide-expired` – не выводить просроченные учетные записи пользователей; - `--hide-disabled` – не выводить отключенные учетные записи пользователей
`user show` <имя пользователя>	Вывести пользовательский объект AD	В опции `--attributes=USER_ATTRS` можно указать, разделенный запятыми, список атрибутов
`user move` <имя пользователя> <контейнер>	Переместить учетную запись пользователя в указанную организационную единицу или контейнер	Имя пользователя указывается в команде в формате sAMAccountName. Имя организационной единицы или контейнера можно указать как полное DN или без компонента domainDN.
`user password`	Изменить пароль учетной записи пользователя, указанной при аутентификации.	

Окончание таблицы 48

Команда	Описание	Примечание
`user setexpiry <имя пользователя>`	Установить срок действия для учетной записи пользователя	
`user setpassword <имя пользователя>`	Установить или сбросить пароль учетной записи пользователя	
`user unlock <имя пользователя>`	Разблокировать учетную запись пользователя в домене AD	
`user getpassword <имя пользователя>`	Получить атрибуты пароля учетной записи пользователя	
`user rename <имя пользователя>`	Переименовать пользователя и изменить его атрибуты	По умолчанию выводятся sAMAccountNames пользователей. Для удаления атрибута следует использовать пустое значение атрибута. Имя пользователя указывается в команде в формате sAMAccountName. Можно использовать следующие опции: - `--surname=SURNAME` – новая фамилия; - `--given-name=GIVEN_NAME` – новое имя; - `--initials=INITIALS` – новые инициалы; - `--force-new-cn=NEW_CN` – новый CN (вместо использования комбинации имени, инициалов и фамилии); - `--reset-cn` – установить CN на комбинацию имени, инициалов и фамилии по умолчанию; - `--display-name=DISPLAY_NAME` – новое отображаемое имя; - `--mail-address=MAIL_ADDRESS` – новая электронная почта; - `--samaccountname = SAMACCOUNTNAME` – новое имя для входа (sAMAccountName); - `--upn=UPN` – новое основное имя пользователя.
`user syncpasswords --cache-ldb-initialize`	Синхронизировать пароли всех учетных записей пользователей с помощью дополнительного сценария	Эта команда должна выполняться только на одном контроллере домена (обычно на PDC)

10.7.1.2.1. Примеры

Создать пользователя ivanov:

```
# samba-tool user create ivanov --given-name='Иван Иванов'
--mail-address='ivanov@test.alt'
New Password:
Retype Password:
User 'ivanov' added successfully
```

Разблокировать пользователя ivanov:

```
# samba-tool user setexpiry ivanov --noexpiry
Expiry for user 'ivanov' disabled.
```

Просмотреть доступных пользователей:

```
# samba-tool user list
Guest
ivanov
Administrator
krbtgt
```

Отключить пользователя:

```
# samba-tool user disable ivanov
```

Изменить пароль пользователя:

```
# samba-tool user setpassword ivanov
```

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

10.7.1.3. Команды управления группами

Команды управления группами представленны в таблице 49.

Т а б л и ц а 49 – Команды управления группами инструмента samba-tool

Команда	Описание	Примечание
group add <имя группы> [<опции>]	Создать новую группу	
group create <имя группы> [<опции>]	Создать новую группу	Доступна только в целях совместимости. Рекомендуется вместо этой команды использовать команду samba-tool group add
group addmembers <имя группы> <участник> [<опции>]	Добавить участников в группу	
group delete <имя группы> [<опции>]	Удалить группу AD	
group edit <имя группы>	Редактировать объект группы AD	В опции --editor=<редактор> можно указать редактор (по умолчанию vi)
group list	Вывести список групп	
group listmembers <имя группы> [<опции>]	Вывести список участников данной группы	По умолчанию выводятся sAMAccountNames участников. Если sAMAccountName недоступен, будет использоваться CN. Можно использовать следующие опции: - --full-dn – показать различающиеся имена участников (CN) вместо sAMAccountNames; - --hide-expired – не выводить членов группы с истекшим сроком действия; - --hide-disabled – не выводить отключенных членов группы
group move <имя группы> <контейнер> [<опции>]	Переместить группу в указанную организационную единицу или контейнер	Имя группы указывается в команде в формате sAMAccountName. Имя организационной единицы или контейнера можно указать как полное DN или без компонента domainDN
group removemembers <имя группы> <участник> [<опции>]	Удалить участника из группы	
group show <имя группы> [<опции>]	Вывести группу и ее атрибуты	В опции --attributes=USER_ATTRS можно указать, разделенный запятыми, список атрибутов
group stats [<опции>]	Показать статистику для общих групп и членства в группах	
group rename <имя группы> [<опции>]	Переименовать группу и изменить ее атрибуты	По умолчанию выводятся sAMAccountNames групп. Для удаления атрибута следует использовать пустое значение атрибута. Имя группы указывается в команде в формате sAMAccountName.

Окончание таблицы 49

Команда	Описание	Примечание
		Можно использовать следующие опции: - `--force-new-cn=NEW_CN` – новый CN (вместо использования sAMAccountName); - `--reset-cn` – установить CN равным sAMAccountName; - `--mail-address=MAIL_ADDRESS` – новая электронная почта; - `--samaccountname=SAMACCOUNTNAME` – новое имя для входа (sAMAccountName).

10.7.1.3.1. Примеры

Добавить группу:

```
# samba-tool group add office
```

Добавить UNIX-группу:

```
# samba-tool group add groupname --nis-domain=samdom --gid-number=<next available GID>
```

Удалить группу:

```
# samba-tool group delete office
```

Добавить пользователя в группу:

```
# samba-tool group addmembers "Domain Users" user
# samba-tool group addmembers "Domain Users" user,user1,user2
```

Удалить пользователя из группы:

```
# samba-tool group removemembers "Domain Users" user
```

Вывести пользователей группы:

```
# samba-tool group listmembers "Domain Users" | grep Ivanov
```

10.7.2. Резервное копирование и восстановление Samba AD DC

Резервные копии Samba позволяют восстановить домен Samba AD в случае сбоя работы. Резервное копирование отдельных контроллеров домена не выполняется.

Если контроллер домена используется и в качестве файлового сервера (что не рекомендуется), потребуется также создать отдельные резервные копии этих данных.

Есть несколько разновидностей резервного копирования:

- online – выполняется клонирование работающей базы данных DC. По функциональности это похоже на присоединение нового контроллера домена к сети;
- offline (локальный) – резервные копии Samba создаются в том виде, в котором они появляются на диске. Сюда входят метаданные репликации, которые являются локальными для этого конкретного контроллера домена и которые не включаются в online резервные копии. Резервную копию также можно создать, когда контроллер домена находится в автономном режиме (т.е. процесс samba фактически не запущен).
- rename (локальный) – создается файл резервной копии с переименованным доменом (предназначен только для временной замены).

Резервные копии можно создать, используя команду `samba-tool domain backup`. При этом будет создан файл резервной копии `.tar.bz2`, который будет содержать полную резервную копию домена (на основе данного контроллера домена). Этот файл резервной копии можно использовать для восстановления домена с помощью команды `samba-tool domain backup restore`.

Примечание. Следует иметь ввиду, что файл резервной копии – это резервная копия домена, а не контроллера домена. Восстановление файла резервной копии создаст новый DC с информацией о домене. Чтобы восстановить последующие контроллеры домена, необходимо присоединить новые контроллеры домена к восстановленному контроллеру домена.

10.7.2.1. Создание резервной копии в режиме онлайн/оффлайн режимах

Схема создания резервной копии представлена на рис. 392.

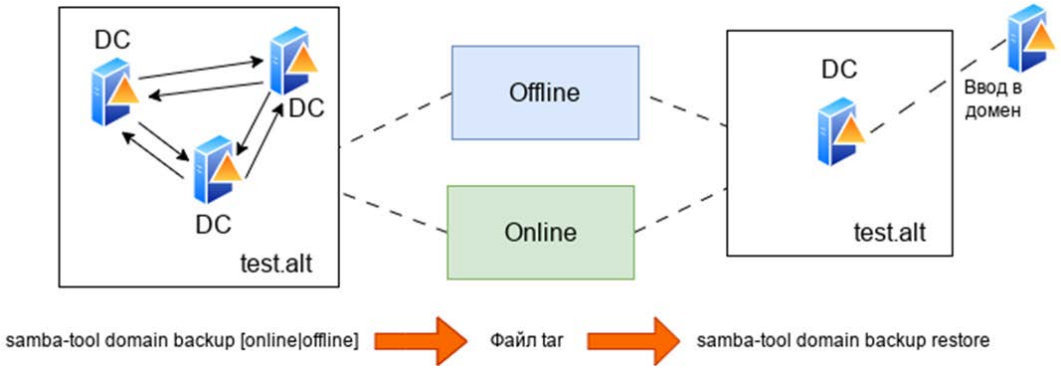


Рис. 392 – Схема создания резервной копии

10.7.2.1.1. Онлайн режим

Для создания резервной копии в режиме онлайн (online), следует выполнить команду:

```
# samba-tool domain backup online --targetdir=<output-dir> --server=<DC-server> -UAdministrator
```

Эту команду можно запустить как локально на контроллере домена, так и удаленно на другом компьютере. При удаленном запуске можно указать параметр `--configfile`, чтобы в резервную копию были включены правильные настройки `smb.conf` (т. к. локальный файл `smb.conf` может не существовать или его настройки могут отличаться от настроек контроллера домена).

Пример создания резервной копии в режиме онлайн на контроллере домена:

```
# mkdir /var/samba-backup-online
# samba-tool domain backup online --targetdir=/var/samba-backup-online --server=dc1 –Uadministrator
Password for [TEST\Administrator]:
workgroup is TEST
realm is test.alt
Looking up IPv4 addresses
Looking up IPv6 addresses
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
A Kerberos configuration suitable for Samba AD has been generated at /var/samba-backup-online/tmpxqc6dwts/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!
...
Creating backup file /var/samba-backup-online/samba-backup-test.alt-2023-04-17T20-09-56.883910.tar.bz2..
```

10.7.2.1.2. Создание резервной копии в автономном режиме

Для создания автономной (offline) резервной копии, следует на контроллере домена выполнить команду:

```
# samba-tool domain backup offline --targetdir=<output-dir>
```

Примечание. Несмотря на название этого резервного копирования, контроллеру домена не нужно быть в автономном режиме при выполнении этой команды. Инструмент просто выполняет резервное копирование локальных файлов и имеет достаточную блокировку, чтобы гарантировать безопасное создание резервной копии.

Пример создания резервной копии в автономном режиме на контроллере домена:

```
# mkdir /var/samba-backup-offline
# samba-tool domain backup offline --targetdir=/var/samba-backup-offline
running backup on dirs: /var/lib/samba/private /var/lib/samba /etc/samba
Starting transaction on /var/lib/samba/private/secrets
Starting transaction on /var/lib/samba/private/sam.ldb
   backing up /var/lib/samba/private/sam.ldb

…
   adding misc file etc/lmhosts
   adding misc file etc/smb.conf
Backup succeeded.
```

10.7.2.1.3. Восстановление домена

Для восстановления домена из резервной копии необходимо выполнить следующие шаги:

1) остановить samba на всех старых контроллерах домена. Этот шаг можно пропустить если используется не rename резервная копия;
2) запустить команду samba-tool domain backup restore, чтобы восстановить базу данных домена на одном новом контроллере домена;
3) запустить samba на новом dc;
4) повторно добавить старые контроллеры домена в сеть, присоединив их к восстановленному DC, например, командой:

```
samba-tool domain join <dns-realm> DC --server=<restored-dc>
```

Если используется rename резервная копия, также потребуется перенастроить сетевые устройства, так чтобы трафик перенаправлялся в восстановленный домен, а не в неисправный/исходный домен.

Примечание. Из файла резервной копии восстанавливается весь домен, а не конкретный контроллера домена. Шаг с командой `samba-tool domain backup restore` выполняется только один раз, при этом домен воссоздается на одном контроллере домена. Затем все старые контроллеры домена должны быть повторно присоединены к восстановленному контроллеру домена.

10.7.2.1.4. Восстановление из файла резервной копии

Этап восстановления из файла резервной копии аналогичен разворачиванию домена, который выполнялся при первой настройке сети Samba, за исключением того, что резервная копия содержит в себе все объекты базы данных, которые были добавлены с момента создания домена. Как и при создании нового домена, при запуске команды восстановления домена потребуется указать новый контроллер домена. Этот контроллер домена не должен был существовать ранее в сети Samba.

Команда восстановления:

```
# samba-tool domain backup restore --backup-file=<tar-file> \
--newservername=<DC-name> --targetdir=<new-samba-dir>
```

Следует обратить внимание, что указанный целевой каталог должен быть пустым (или не должен существовать). Т. е. нецелесообразно восстанавливать базу данных домена в место установки по умолчанию (например, `/var/lib/samba`). Вместо этого рекомендуется восстановить базу данных домена в другой целевой каталог, а затем, при запуске samba, использовать параметр `-s` (или `--configfile`), например:

```
# samba -s <targetdir>/etc/smb.conf
```

Указание восстановленного `smb.conf` гарантирует, что Samba будет использовать файлы базы данных в правильном месте.

Восстановленный DC будет добавлен на сайт «Default-First-Site-Name». Этот сайт будет создан в восстановленной БД, если он еще не существует. Можно указать альтернативный сайт для добавления восстановленного контроллера домена с помощью параметра `--site`.

Перед запуском samba на восстановленном контроллере домена следует еще раз проверить правильность восстановленных настроек `smb.conf`.

Пример восстановления данных из резервной копии:

```
# mkdir /var/lib/samba/new
# samba-tool domain backup restore
--backup-file=/home/user/samba-backup-test.alt-2023-04-17T20-09-
56.883910.tar.bz2
--newservername=newdc  --targetdir=/var/lib/samba/new
Adding new DC to site 'Default-First-Site-Name'
Updating basic smb.conf settings...
…
Backup file successfully restored to /var/lib/samba/new
Please check the smb.conf settings are correct before starting samba.
```

10.7.2.1.5. Рекомендуемая стратегия

Восстановление файла резервной копии имеет несколько неудобств:

- необходимость использовать другой каталог для установки по умолчанию;
- необходимо указать имя сервера DC, отличное от того, что было ранее в сети.

Свести эти неудобства к минимуму можно, используя временный сервер (или виртуальную машину) для восстановления контроллера домена:

1) выполнить восстановление из файла резервной копии на временный контроллер домена и запустить Samba;
2) повторно по одному присоединить исходные контроллеры домена к временному контроллеру домена (во время присоединения можно повторно использовать одно и то же имя сервера и место установки по умолчанию);
3) после присоединения всех исходных контроллеров домена к восстановленному домену, можно удалить временный контроллер домена (например, с помощью команды `samba-tool domain demote`). В этом случае сеть контроллеров домена будет точно такой же, как и раньше.

10.7.2.1.5.1 Пример разворачивания домена (SAMBA_INTERNAL) из резервной копии на ВМ

1) Подготовить узел:
   - установить пакет task-samba-dc (или task-samba-dc-mitkrb5):

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

- остановить конфликтующие службы:

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

- очистить базы и конфигурацию Samba:

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba/*
# rm -rf /var/cache/samba
```

2) Скопировать файл резервной копии на ВМ и выполнить восстановление домена из файла резервной копии:

```
# samba-tool domain backup restore\
--backup-file=/home/user/samba-backup-test.alt-2023-04-17T20-09-56.883910.tar.bz2\
--newservername=newdc --targetdir=/var/lib/samba
Adding new DC to site 'Default-First-Site-Name'
Updating basic smb.conf settings...
…
Backup file successfully restored to /var/lib/samba
Please check the smb.conf settings are correct before starting samba.
```

3) Скопировать файл `smb.conf` из каталога `/var/lib/samba/etc/` в каталог `/etc/samba/`:

```
# cp /var/lib/samba/etc/smb.conf /etc/samba/
```

4) Запустить Samba:

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

5) Заменить файл `/etc/krb5.conf` файлом из каталога `/var/lib/samba/private/`:

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

6) Проверить работоспособность домена (см. п. 10.2.4):

```
# samba-tool domain info 127.0.0.1
Forest           : test.alt
Domain           : test.alt
Netbios domain   : TEST
DC name          : newdc.test.alt
DC netbios name  : NEWDC
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
# smbclient -L localhost -Uadministrator
Password for [TEST\administrator]:
    Sharename       Type      Comment
    ---------       ----      -------
    sysvol          Disk
    netlogon        Disk
```

```
    share           Disk      Commonplace
    Free            Disk
    IPC$            IPC       IPC Service (Samba 4.16.10)
SMB1 disabled -- no workgroup available
# host -t SRV _kerberos._udp.test.alt.
_kerberos._udp.test.alt has SRV record 0 100 88 newdc.test.alt.
```

10.7.2.2. Переименованная резервная копия

Создание резервной копии в режиме переименования (рис. 393) может применяться для:

1) запуска временного альтернативного домена на случай катастрофического отказа основного домена. На альтернативный/переименованный домен можно переключиться с минимальными усилиями. Затем можно запустить два домена одновременно, не мешая друг другу (переименованный/альтернативный домен будет предоставлять основные сетевые службы Samba, в это же время на исходных контроллерах домена можно устранять неполадки);
2) создания реалистичного лабораторного домена: домен переименовывается и удаляются конфиденциальные данные (на данный момент только самые важные), чтобы создать предпроизводственную среду для тестирования.

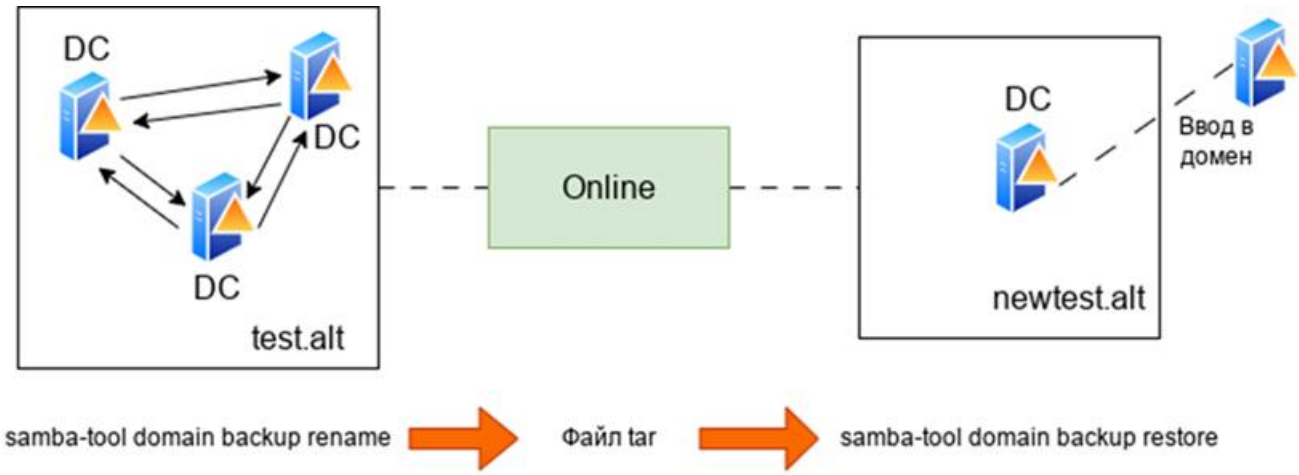


Рис. 393 – Схема создания резервной копии в режиме переименования

Переименование домена выполняется в два этапа:

1) создание переименованной резервной копии домена: samba-tool делает клон работающей базы данных DC, в процессе клонирования переименовывает домен и создает файл резервной копии;
2) восстановление резервной копии домена: samba-tool берет файл резервной копии и заполняет файлы, необходимые для запуска нового контроллера домена Samba.

10.7.2.2.1. Создание переименованной резервной копии

Команда для создания переименованной (rename) резервной копии:

```
# samba-tool domain backup rename <new-domain-netbios> <newdomain-dns-realm>
 --server=<dc-to-backup> --targetdir=<output-dir> --no-secrets -UAdministrator
```

где:

- `new-domain-netbios` – новое имя NETBIOS;
- `newdomain-dns-realm` – новая область DNS;
- `output-dir` – каталог, куда будет записан сгенерированный файл резервной копии.

Пример:

```
# mkdir /var/samba-backup-rename
# samba-tool domain backup rename NEWTEST newtest.alt\
--server=dc1\ --targetdir=/var/samba-backup-rename\
--no-secrets -UAdministrator
New realm for backed up domain: newtest.alt
New base DN for backed up domain: DC=newtest,DC=alt
New domain NetBIOS name: NEWTEST
Password for [TEST\Administrator]:
Provisioning the new (renamed) domain...
…
INFO 2023-04-17 20:19:06,012 pid:4195 /usr/lib64/samba-dc/python3.9/\
samba/netcmd/domain_backup.py #815: Deleting old DNS zone DC=test.alt,
CN=MicrosoftDNS, DC=DomainDnsZones, DC=newtest,DC=alt
ERROR(ldb): uncaught exception - No Deleted Objects container for DN
DC=_msdcs,DC=test.alt,CN=MicrosoftDNS,DC=DomainDnsZones,DC=newtest,DC=a
lt
  File "/usr/lib64/samba-dc/python3.9/samba/netcmd/__init__.py", line
186, in _run
    return self.run(*args, **kwargs)
  File "/usr/lib64/samba-dc/python3.9/samba/netcmd/domain_backup.py",
line 925, in run
    self.delete_old_dns_zones(logger, samdb, old_realm)
  File "/usr/lib64/samba-dc/python3.9/samba/netcmd/domain_backup.py",
line 816, in delete_old_dns_zones
    samdb.delete(dn, ["tree_delete:1"])
```

⚠ Параметр `--no-secrets` исключает из резервной копии конфиденциальную информацию о паролях (например, такие атрибуты, как `unicodePwd`, `lmPwdHistory` и т. д.) для всех пользователей в домене. При этом, файл резервной копии по-прежнему содержит конфиденциальную информацию, такую как имена учетных записей пользователей.

В случае, если команда создания резервной копии запускается на узле, который будет использоваться в качестве нового контроллера домена (он должен быть подключен к рабочему домену), рекомендуется иметь файл `smb.conf`, максимально соответствующий производственному контроллеру домена, и передать его команде резервного копирования (с помощью параметра `--configfile=smb.conf`). Это гарантирует, что резервная копия будет содержать `smb.conf`, точно соответствующий домену.

Если команда создания резервной копии запускается на другом узле, (например, на рабочем контроллере домена), необходимо скопировать сгенерированный файл резервной копии на узел, который будет использоваться в качестве нового контроллера домена.

10.7.2.2.2. Восстановление данных из резервной копии

Команда восстановления из резервной копии:

```
# mkdir /var/lib/samba/newtest
# samba-tool domain backup restore--targetdir=/var/lib/samba/newtest\
--newservername=NEWDC1\
--backup-file=/home/user/samba-backup-test.alt-2023-04-17T20-09-
56.883910.tar.bz2
```

Примечания:

1. Целевой каталог должен быть пустым (или не должен существовать). Поэтому нецелесообразно восстанавливать базу данных домена в место установки по умолчанию (например, `/var/lib/samba/`). Однако можно указать подкаталог (например, `/var/lib/samba/newtest/`).

2. Новый контроллер домена не может использовать то же имя сервера, что и контроллер домена в исходной сети.

10.7.2.2.3. Сброс пароля

Во время резервного копирования/восстановления пароль для учетной записи администратора сбрасывается на случайно сгенерированный пароль. Для его изменения можно просто обновить базу данных на локальном диске, выполнив команду:

```
# samba-tool user setpassword Administrator
--newpassword=<пароль>-H /var/lib/samba/newtest/private/sam.ldb
```

Для тестирования аутентификации пользователей можно либо добавить дополнительные «тестовые» учетные записи пользователей/машин, либо «командовать» некоторыми учетными записями, скопированными из рабочего домена. Для учетных записей, скопированных из рабочего домена, не будут установлены пароли, поэтому на этом этапе также можно сбросить пароли для выбранных учетных записей. Или можно сделать это позже, когда Samba действительно запустится на новом контроллере домена.

10.7.2.2.4. Запуск Samba

Перед запуском samba на новом контроллере домена, необходимо проверить правильность настроек `smb.conf` (например, `/var/lib/samba/newtest/etc/smb.conf`) и `/etc/krb5.conf`.

При запуске samba необходимо указать восстановленный `smb.conf` (это гарантирует, что Samba загрузит правильные файлы базы данных для нового домена). Например:

```
# samba -s /var/lib/samba/newtest/etc/smb.conf
```

При первом запуске samba могут быть зарегистрированы ошибки DNS. Это связано с тем, что `samba_dnsupdate` запускается автоматически и добавляет записи DNS для нового домена.

После запуска samba можно проверить правильность работы нового контроллера домена, например:

```
# ldbsearch -H ldap://NEWDC1 –Uadministrator
```

10.7.2.2.5. Обновление подсетей сайта

Новый домен будет содержать все сайты AD рабочего домена, но ни один из рабочих контроллеров домена. Однако подсети, которые используют эти сайты, скорее всего, больше не будут иметь смысла для экспериментального домена.

10.7.2.3. Отладочная информация

Если команда резервного копирования или восстановления завершится с ошибкой, то они могут оставить после себя временный каталог (указанный в параметре `--targetdir`). Это может помочь понять, почему произошел сбой. Необходимо удалить этот каталог перед повторным запуском команды восстановления.

Создание резервной копии:

1) резервное копирование следует запускать от имени пользователя root. Онлайн-резервное копирование может быть успешным для пользователя без полномочий root, но при попытке восстановить данные из такой резервной копии могут возникнуть проблемы;
2) для резервных копий, выполненных в режиме «онлайн» или «переименования», следует проверить правильность используемых учетных данных и сведений о сервере. Например:
   ```
   # ldbsearch -H ldap://<server> -UAdministrator
   ```
3) чтобы узнать больше информации о причине сбоя можно увеличить уровень журналирования. Например, добавить в команду параметр `--debug=3`;
4) работа команд для выполнения резервного копирования в режиме «онлайн» или «переименование» очень похожа на присоединение к контроллеру домена. Если известно, что присоединение к контроллеру домена в вашей сети не удается, то эти команды также вряд ли будут работать. Сообщения «Committing SAM database» и «Cloned domain <domain>», говорят о том, что часть резервного копирования, подобная присоединению, скорее всего, выполнена успешно;

5) инструменты резервного копирования не работают напрямую с контроллером домена Windows (в основном простое резервное копирование файлов sysvol не удается из-за блокировки службы DFSR). Если у вас смешанный домен контроллера домена, следует создать резервную копию контроллера домена Samba, а не контроллера домена Windows. Если у вас домен Windows, можно на время резервного копирования на контроллере домена остановить службу DFSR «Репликация DFS».

Восстановление из резервной копии:

1) команду восстановления необходимо запускать от имени пользователя root;
2) имя, указанное в параметре `--newservername`, не должно существовать в исходном домене. В противном случае будет получена ошибка вида:

```
Adding CN=NEWDC,OU=Domain Controllers,DC=test,DC=alt
ERROR(ldb): uncaught exception - Entry CN=NEWDC, OU=Domain Controllers, DC=test, DC=alt already exists
  File "/usr/lib64/samba-dc/python3.9/samba/netcmd/__init__.py", line 186, in _run
    return self.run(*args, **kwargs)
  File "/usr/lib64/samba-dc/python3.9/samba/netcmd/domain_backup.py", line 562, in run
    ctx.join_add_objects(specified_sid=dom_sid(str(sid)))
  File "/usr/lib64/samba-dc/python3.9/samba/join.py", line 674, in join_add_objects
    ctx.samdb.add(rec, controls=controls)
```

Если команда резервного копирования выполнялась локально на контроллере домена, то файл резервной копии должен содержать файл `smb.conf` контроллера домена. Однако `smb.conf` в файле резервной копии может содержать конфигурацию «интерфейсов», которая не соответствует IP-адресам на DC, на котором разворачиваются данные из резервной копии. Избежать этой проблемы можно, указав аргумент `--host-ip` во время восстановления (это имеет значение только для переименованных резервных копий).

10.7.3. Роли FSMO

FSMO, или Flexible single-master operations (операции с одним исполнителем) – это операции, выполняемые контроллерами домена AD, которые требуют обязательной уникальности сервера для каждой операции. В зависимости от типа операции уникальность FSMO подразумевается в пределах одного домена или леса доменов. Различные типы FSMO могут выполняться как на одном, так и на нескольких контроллерах домена. Выполнение FSMO сервером называют ролью сервера, а сами сервера – хозяевами операций.

Active Directory – это центральный репозиторий, в котором хранятся все объекты и соответствующие им атрибуты. Это иерархическая база данных с поддержкой нескольких источников. Большинство операций в AD можно выполнять на любом контроллере домена. Служба репликации AD скопирует изменения на остальные контролеры домена, обеспечив идентичность базы AD на всех контролерах одного домена. Один из способов разрешения конфликтов заключается в том, что сохраняются изменения, внесенные последними. Изменения, внесенные остальными контроллерами домена, игнорируются.

Однако существует несколько операций (например, изменение схемы AD), при которых конфликты недопустимы. В AD некоторые обновления выполняются на одном специальном контроллере домена, а затем реплицируются на все остальные. AD использует роли, назначенные контроллерам домена, для этих специальных задач. Так как роль не привязана к одному контроллеру домена, она называется ролью FSMO. В настоящее время существует семь ролей FSMO с разными областями действия:

- эмулятор PDC/PDC Emulator (один на домен);
- хозяин RID/RID Master (один на домен);
- хозяин схемы/Schema Master (один на лес);
- хозяин именования доменов/Domain Naming Master (один на лес);
- хозяин инфраструктуры/Infrastructure Master (один на домен);
- хозяин зоны DNS домена/Domain DNS Zone Master role (один на домен);
- хозяин зоны DNS леса/Forest DNS Zone Master role (один на лес).

10.7.3.1. Семь ролей FSMO

Ниже описаны роли FSMO, их функции и требования к доступности. Эти сведения позволяют определить последствия, когда контроллер домена, владеющий этой ролью, находится в автономном режиме.

10.7.3.1.1. Эмулятор PDC

Владелец роли эмулятора PDC отвечает за следующие задачи в домене:

1) является сервером точного времени для клиентов в домене. Для аутентификации Kerberos необходима точная синхронизация времени. Эмулятор PDC корневого домена в лесу является по умолчанию сервером точного времени для эмуляторов PDC в дочерних доменах;
2) изменения паролей, внесенные другими контроллерами домена в домене, реплицируются преимущественно в эмулятор PDC. В случае недоступности эмулятора PDC информация об изменении пароля все равно распространится по домену, просто произойдет это несколько медленнее;
3) выполняет все функции, предоставляемые PDC в стиле NT4;
4) обрабатывает блокировки учетных записей. Сбои аутентификации на любом контроллере домена в домене, вызванные неправильным паролем, перенаправляются в эмулятор PDC до того, как сообщение о сбое из-за неправильного пароля будет передано пользователю. При успешной аутентификации учетной записи сразу после неудачной попытки, о ней уведомляется эмулятор PDC и сбрасывает счетчик неудачных попыток в ноль;
5) консоль управления групповыми политиками по умолчанию соединяется с эмулятором PDC, и изменения политик происходят на нем же. Если эмулятор PDC недоступен, то будет нужно указать редактору, к какому контроллеру домена подключиться;
6) в больших средах контроллер домена, которому принадлежит роль эмулятора PDC, может иметь высокую загрузку ЦП из-за сквозной аутентификации, смены пароля и синхронизации времени.

На каждый домен приходится один эмулятор PDC.

Этот контроллер домена должен, по возможности, быть доступен всегда, потому что для Kerberos требуется точное время на всех машинах в домене. Если клиенты настроены на использование другого источника времени и в сети нет клиентов до Windows 2000, временное отсутствие может быть менее критичным.

Для поиска эмулятора PDC можно использовать команду host:

```
# host -t SRV _ldap._tcp.pdc._msdcs.<домен>
```

Например:

```
# host -t SRV _ldap._tcp.pdc._msdcs.test.alt
_ldap._tcp.pdc._msdcs.test.alt has SRV record 0 100 389 dc1.test.alt.
```

10.7.3.1.2. Хозяин RID

Владелец роли FSMO хозяина RID отвечает за обработку запросов пула RID от всех DC в домене. Он также отвечает за перемещение объектов в другой домен и удаление их из домена.

Все объекты безопасности, например, учетные записи и группы пользователей/компьютеров имеют уникальный идентификатор безопасности (SID). SID объектов содержит идентификатор безопасности (SID) домена, одинаковый для всех объектов в домене, и относительный идентификатор (RID), уникальный для каждого идентификатора безопасности субъекта безопасности, созданного в домене.

Каждому контроллеру домена в домене выделяется пул относительных идентификаторов RID, которые разрешено назначать созданным субъектам безопасности. По умолчанию это диапазон из 500 уникальных RID для всего домена, назначаемых хозяином RID каждому контроллеру домена. Если объект безопасности создается на контроллере домена, то RID берется из этого пула, что гарантирует его уникальность в домене. Если выделенный пул RID контроллера домена оказывается ниже порогового значения (ниже 50 %), контроллер домена выполняет запрос дополнительных идентификаторов RID к хозяину RID в домене. Хозяин RID в домене отвечает на запрос, извлекая идентификаторы RID из невыделенного пула RID домена и назначая их пулу запрашивающего контроллера домена.

На каждый домен приходится один хозяин RID.

Этот контроллер домена должен быть активен, при создании нового контроллера домена в домене, чтобы назначить ему пул RID. Также хозяин RID должен быть доступен, когда существующие контроллеры домена обновляют свой резервный пул RID.

С другой стороны, если хозяин RID находится в автономном режиме, то на каждом контроллере домена можно создавать новые объекты безопасности, пока локальный пул RID не станет пустым. Если пулы RID на всех контроллерах домена опустеют, создание дополнительных объектов станет невозможно. Также пока хозяин RID домена находится в автономном режиме невозможно присоединиться к дополнительным контроллерам домена.

10.7.3.1.3. Хозяин схемы

Контроллер домена, обладающий ролью хозяина схемы, является единственным в лесу AD, кому разрешено обновлять схему каталога. После завершения обновления изменения реплицируются на все другие контроллеры домена в лесу.

Схема каталога (контекст именования схемы) или `LDAP://cn=schema,cn=configuration,dc=<домен>` существует на всех контроллерах домена. Обновления выполняются только на хозяине схемы. После завершения обновления схема реплицируется из хозяина схемы во все остальные контроллеры домена каталога.

В каждом лесу есть один хозяин схемы.

Этот контроллер домена должен быть подключен к сети при выполнении обновлений схемы.

10.7.3.1.4. Хозяин именования доменов

Хозяин именования доменов отвечает за внесение изменений в пространство доменных имен в масштабах леса. Только этот контроллер домена может добавлять или удалять домены, доверительные отношения с внешними каталогами и разделами приложений в (из) леса.

Информация об именах доменов хранится в разделе «Контекст именования конфигурации» в `CN=Partitions, CN=Configuration, DC=<домен>`.

Этот раздел существует на всех контроллерах домена, но обновляется только на хозяине именования доменов.

На каждый лес приходится один хозяин именования доменов.

Этот контроллер домена должен быть подключен к сети, когда устанавливаются доверительные отношения с внешними каталогами и доменами, а разделы приложений добавляются или удаляются из леса.

10.7.3.1.5. Хозяин инфраструктуры

Контроллер домена, которому принадлежит роль хозяина инфраструктуры, отвечающий за обновление идентификатора безопасности (SID) и различающегося имени объекта в ссылке на междоменный объект. Это используется, например, если пользователь из одного домена добавляется в группу безопасности другого домена.

На каждый домен приходится один хозяин инфраструктуры.

Если этот контроллер домена временно отключен, междоменные изменения невозможны.

10.7.3.1.6. Хозяин зоны DNS домена

Контроллер домена, которому принадлежит роль хозяина зоны DNS домена, отвечает за координацию добавления или удаления любых зон DNS, интегрированных в AD, на контроллерах домена с DNS-серверами, на которых размещен домен.

На каждый домен приходится один хозяин зоны DNS-домена.

10.7.3.1.7. Хозяин зоны DNS леса

Контроллер домена, которому принадлежит роль хозяина зоны DNS леса, отвечает за координацию добавления или удаления записей всего леса на DNS-серверах, на которых размещена зона DNS верхнего уровня. Эти записи содержат имена серверов глобального каталога (GC).

На каждый домен приходится один хозяин зоны DNS леса.

10.7.3.2. Просмотр и передача ролей FSMO

По возможности следует передавать роли FSMO штатным образом и не использовать принудительную передачу (захват роли). Для штатной передачи роли требуется, чтобы контроллер домена, которому в данный момент принадлежит роль, работал и был подключен к сети. В этом случае при передаче роли старый контроллер домена узнает, что он больше не владеет ролью.

Если контроллер домена сломан (например, из-за аппаратного дефекта) и больше никогда не будет возвращен в сеть, можно использовать принудительную передачу (захватить роль на оставшемся контроллере домена). Если старый контроллер домена будет снова подключен к сети, это вызовет конфликты и приведет к неконсистентному AD (т. к. старый контроллер домена не заметит изменения и по-прежнему будет считать себя владельцем роли).

Роли FSMO можно передавать с помощью инструмента командной строки `samba-tool` или в модуле удаленного управления базой данных конфигурации (ADMC).

10.7.3.2.1. ADMC

Для просмотра текущего владельца роли необходимо выбрать пункт меню «Файл» → «Мастера Операций» (рис. 394). В открывшемся окне в списке слева выбрать роль и в поле «Текущий мастер» будет показан владелец роли.

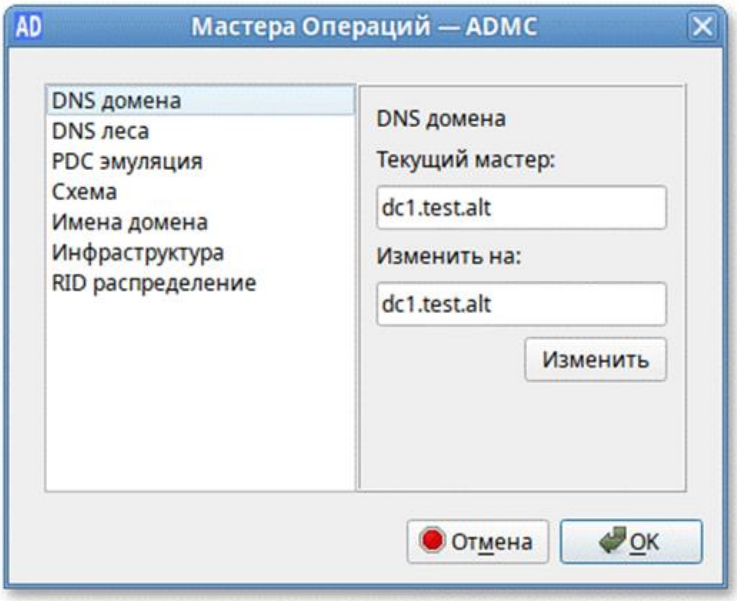


Рис. 394 – Мастера операций

Список возможных ролей:

- «DNS домена» – хозяин зоны DNS домена;
- «DNS леса» – хозяин зоны DNS леса;
- «PDC эмуляция» – эмулятор PDC;
- «Схема» – хозяин схемы;
- «Имена домена» – хозяин именования доменов;
- «Инфраструктура» – хозяин инфраструктуры;
- «RID распределение» – хозяин RID.

Для штатной передачи роли необходимо выполнить следующие действия:

1) в окне «Параметры подключения» – «ADMC» («Файл» → «Параметры подключения») выбрать контроллер домена, который должен стать новым владельцем роли и нажать кнопку «ОК» (рис.395);

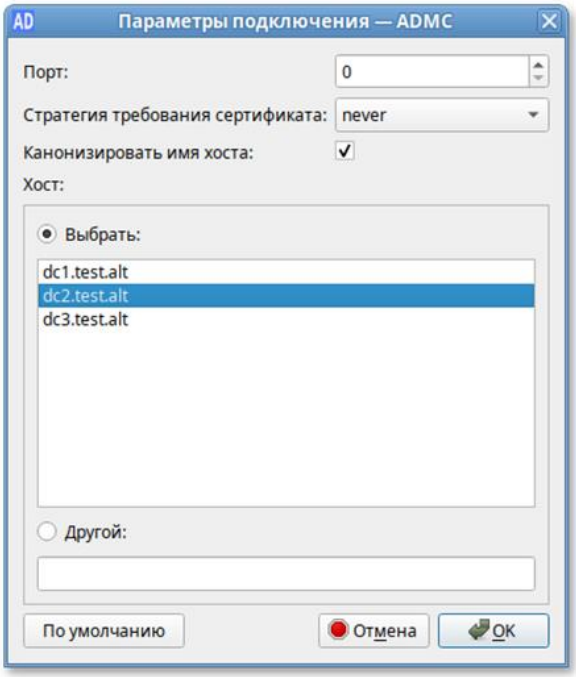


Рис. 395 – Выбор контроллера домена

2) в окне «Мастера Операций» – «ADMC» («Файл» → «Мастера Операций») выбрать роль (при этом в поле «Текущий мастер» будет показан текущий владелец роли, а в поле «Изменить на» – контроллер домена, который должен стать новым владельцем роли) и нажать кнопку «Изменить» (рис. 396).

Владелец роли будет изменен.

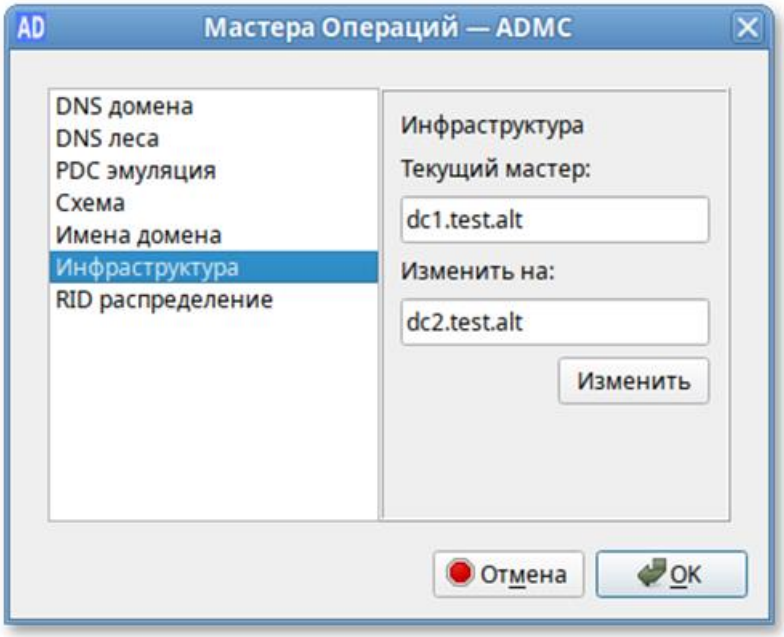


Рис. 396 – Изменение владельца роли

10.7.3.2.2. Инструмент samba-tool

Просмотр текущего состояния (команда выполняется на контроллере домена):

```
# samba-tool fsmo show
```

```
SchemaMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
InfrastructureMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
RidAllocationMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
PdcEmulationMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
DomainNamingMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
DomainDnsZonesMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
ForestDnsZonesMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
```

Для штатной передачи роли необходимо на контроллере домена, который должен стать новым владельцем роли выполнить команду:

```
# samba-tool fsmo transfer --role=<роль>
```

Список возможных ролей:

- `rid` – хозяин RID;

- `pdc` – эмулятор PDC;

- `infrastructure` – хозяин инфраструктуры;

- schema – хозяин схемы;

- naming – хозяин именования доменов;

- domaindns – хозяин зоны DNS домена;

- forestdns – хозяин зоны DNS домена;

- all – все роли.

Пример штатной передачи роли (команда выполняется на DC2):

```
# samba-tool fsmo transfer --role=infrastructure
FSMO transfer of 'infrastructure' role successful
```

Проверка:

```
# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name,CN=Sites,CN=Configuration, DC=test, DC=alt
InfrastructureMasterRole owner: CN=NTDS Settings, CN=DC2, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
RidAllocationMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
PdcEmulationMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
DomainNamingMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
DomainDnsZonesMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
ForestDnsZonesMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
```

Для принудительной передачи роли (если контроллер домена вышел из строя) необходимо на контроллере домена, который должен стать новым владельцем роли выполнить команду:

```
# samba-tool fsmo seize --role=<роль>
```

Примечания:

1. Если роль была передана принудительно, старый контроллер домена больше никогда не должен подключаться к сети.

2. При передаче ролей domaindns и forestdns необходимо предоставить аутентификацию.

3. В ранних версиях samba-tool была ошибка, не позволявшая захватить роль naming:

```
# samba-tool fsmo seize --role=naming
ERROR (ldb): uncaught exception – Failed FSMO transfer: WERR_BADFILE
```

4. В этом случае необходимо использовать «еще более принудительную передачу»:

```
# samba-tool fsmo seize --force --role=naming
```

10.7.4. Настройка Samba для привязки к определенным интерфейсам

Если на сервере настроено несколько сетевых интерфейсов, можно настроить Samba для привязки только к определенным интерфейсам.

Например, для того чтобы привязать все службы Samba к устройству enp0s3 и loopback (lo) необходимо добавить следующие параметры в раздел [`global`] файла `smb.conf`:

```
bind interfaces only = yes
interfaces = lo enp0s3
```

и перезапустить службу Samba:

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

Примечания:

1. В параметре interfaces вместо имен интерфейсов можно указывать IP-адреса.
2. Некоторые утилиты подключаются к петлевому IP-адресу, если имя хоста не указано. Поэтому всегда нужно указывать Samba прослушивать петлевые (lo) устройства.

10.7.5. Аутентификация других сервисов в Samba AD

10.7.5.1. Настройка аутентификации Kerberos для веб-сервера Apache

В этом разделе показано, как обеспечить прозрачную авторизацию пользователей домена на веб-сайте, размещенном на веб-сервере Apache2.

В качестве веб-сервера используется отдельный сервер (web.test.alt, IP-адрес 192.168.0.150), введенный в домен.

Примечание. Веб-сервер может быть присоединен или не присоединен к домену, это не имеет значения.

Добавить зону обратного просмотра для подсети 192.168.0.0/24, в которой располагается веб-сервер:

```
# samba-tool dns zonecreate dc1 0.168.192.in-addr.arpa -Uadministrator
Password for [TEST\administrator]:
Zone 0.168.192.in-addr.arpa created successfully
```

где `dc1` – имя контроллера домена.

Если требуется более одной обратной зоны (при использовании нескольких подсетей), следует запустить приведенную выше команду еще раз, но с данными для другой подсети.

Обратная зона работает напрямую без перезапуска Samba или BIND.

Добавить зону обратного просмотра для веб-сервера:

```
# samba-tool dns add dc1 0.168.192.in-addr.arpa 150 PTR web.test.alt -Uadministrator
```

10.7.5.1.1. Создание keytab-файла

Нужно настроить SPN (имена участников-служб) для имени сервера, на которое разрешается любой веб-сайт. Если виртуальный хостинг не используется, веб-адрес и имя машины будут одинаковыми. Для создания SPN на контроллере домена выполнить команды:

```
# samba-tool user create --random-password webauth
# samba-tool user setexpiry webauth
# samba-tool spn add HTTP/web.test.alt webauth
```

Создать Kerberos keytab файл для Apache2:

```
# samba-tool domain exportkeytab /tmp/httpd.keytab --principal=HTTP/web.test.alt@TEST.ALT
Export one principal to /tmp/httpd.keytab
```

Перенести полученный файл `keytab` на веб-сервер в `/etc/httpd2/conf/`, установить права на него, так чтобы apache мог читать, но не изменять keytab-файл:

```
# chown root:apache /etc/httpd2/conf/httpd.keytab
# chmod 640 /etc/httpd2/conf/httpd.keytab
```

10.7.5.1.2. Настройка Apache2

Для настройки Apache2 необходимо выполнить следующие действия:

1) на веб-сервере установить пакет apache2-mod_auth_gssapi и включить необходимые модули:

```
# apt-get install apache2-mod_auth_gssapi
# a2enmod auth_gssapi
# a2enmod authn_core
# a2enmod authz_user
# service httpd2 condreload
```

2) добавить в конфигурацию Apache строки:

```
<Location "/login.html">
        AuthType GSSAPI
        AuthName "GSSAPI Login"
        #GssapiBasicAuth On
        GssapiCredStore keytab:/etc/httpd2/conf/httpd.keytab
        GssapiAllowedMech krb5
        Require valid-user
</Location>
```

3) перезапустить Apache:

```
# systemctl restart httpd2
```

10.7.5.1.3. Проверка аутентификации

Тестовый сайт должен быть доступен по адресу `http://<полное_доменное_имя_веб-сервера>`.

На рабочей станции, введенной в домен, получить билет Kerberos:

```
$ kinit ivanov
Password for ivanov@TEST.ALT:
$ klist
Ticket cache: KEYRING:persistent:500:krb_ccache_5VitJSL
Default principal: ivanov@TEST.ALT

Valid starting       Expires              Service principal
28.04.2023 15:54:41  29.04.2023 01:54:41 krbtgt/TEST.ALT@TEST.ALT
    renew until 05.05.2023 15:54:38
```

Попытаться прочитать содержимое сайта, используя аутентификацию Kerberos:

```
$ curl --negotiate -u : http://web.test.alt/login.html
<html><body><h1>It works!</h1></body></html>
```

Получить содержимое страницы.

Удалить билеты Kerberos:

```
$ kdestroy
$ klist
```

Попытаться прочитать содержимое сайта используя аутентификацию Kerberos:

```
$ curl --negotiate -u : http://web.test.alt/login.html
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">

<head>
<title>Authentication required!</title>
</head>

<body>
<h1>Authentication required!</h1>
…
<h2>Error 401</h2>
<address>
```

```
  <a href="/">web.test.alt</a><br />
  <span>Apache/2.4.57 (Unix) mod_auth_gssapi/1.6.3 OpenSSL/1.1.1u</span>
</address>
</body>
</html>
```

Содержимое страницы не доступно.

10.7.5.2. Настройка аутентификации Kerberos для веб-сервера Nginx

В этом разделе показано, как обеспечить прозрачную авторизацию пользователей домена на веб-сайте, размещенном на веб-сервере Nginx.

В качестве веб-сервера используется отдельный сервер (web.test.alt, IP-адрес 192.168.0.150), введенный в домен.

П р и м е ч а н и е . Веб-сервер может быть присоединен или не присоединен к домену, это не имеет значения.

Добавить зону обратного просмотра для подсети 192.168.0.0/24, в которой располагается веб-сервер:

```
# samba-tool dns zonecreate dc1 0.168.192.in-addr.arpa –Uadministrator

Password for [TEST\administrator]:
Zone 0.168.192.in-addr.arpa created successfully
```

где `dc1` – имя контроллера домена.

Если требуется более одной обратной зоны (при использовании нескольких подсетей), следует запустить приведенную выше команду еще раз, но с данными для другой подсети.

Обратная зона работает напрямую без перезапуска Samba или BIND.

Добавить зону обратного просмотра для веб-сервера:

```
# samba-tool dns add dc1 0.168.192.in-addr.arpa 150 PTR web.test.alt
```

10.7.5.2.1. Создание keytab-файла

Нужно настроить SPN (имена участников-служб) для имени сервера, на которое разрешается любой веб-сайт (таким образом, фактическое имя сервера, на которое указывает CNAME, является полным). Если виртуальный хостинг не используется, веб-адрес и имя машины будут одинаковыми. Для этого на контроллере домена:

```
# samba-tool user create --random-password nginxauth
# samba-tool user setexpiry nginxauth
# samba-tool spn add HTTP/web.test.alt nginxauth
```

Создать Kerberos keytab файл для Nginx:

```
# samba-tool domain exportkeytab /tmp/nginx.keytab --principal=HTTP/web.test.alt@TEST.ALT
Export one principal to /tmp/nginx.keytab
```

10.7.5.2.2. Настройка Nginx

Для работы прозрачной доменной аутентификации (SSO) в Nginx необходимо установить пакеты nginx и nginx-spnego:

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

Модуль SPNEGO для Nginx – это программный компонент для возможности прохождения аутентификации (Single Sign-On или SSO) через сервер LDAP.

Включить модуль http_auth_spnego:

```
# ln -s /etc/nginx/modules-available.d/http_auth_spnego.conf /etc/nginx/modules-enabled.d/
```

Перенести полученный на контроллере домене файл `keytab` на веб-сервер в `/etc/nginx`. Установить права на файл `keytab`:

```
# chmod 644 /etc/nginx/nginx.keytab
```

Nginx должен иметь права на чтение файла `keytab`, но не на его изменение.

Настроить аутентификацию в секции «Server» файла конфигурации сайта:

```
server {
    …
    location /
    {
        root /var/www/html;
        auth_gss on;
        auth_gss_realm TEST.ALT; #имя kerberos области
        auth_gss_keytab /etc/nginx/nginx.keytab; #путь к keytab-файлу
        auth_gss_service_name HTTP/web.test.alt; #имя используемого SPN
        auth_gss_allow_basic_fallback off;
    }
}
```

Описание опций:

- `auth_gss` – включение/отключение аутентификации;
- `auth_gss_keytab` – абсолютный путь к файлу keytab, содержащему учетные данные службы;
- `auth_gss_realm` – имя области Kerberos;
- `auth_gss_service_name` – имя субъекта-службы, используемое при получении учетных данных;

- `auth_gss_allow_basic_fallback` – включить/отключить базовую аутентификацию. При включенной базовой аутентификации (по умолчанию), если SSO не проходит (машина не в домене) разрешает обычный ввод логина и пароля. Если используется SPNEGO без SSL, рекомендуется отключить базовую аутентификацию, так как в этом случае пароль будет отправлен в виде открытого текста.

Перезапустить nginx:

```
# systemctl restart nginx
```

Если нужно авторизовать только определенный набор пользователей, можно использовать в параметре `auth_gss_authorized_principal`. Можно указывать несколько записей, по одной на строку:

```
auth_gss_authorized_principal <username>@<realm>
auth_gss_authorized_principal <username2>@<realm>
```

Список пользователей также можно указать с помощью шаблона регулярного выражения в параметре `auth_gss_authorized_principal_regex`. Этот параметр можно использовать вместе с параметром `auth_gss_authorized_principal`:

```
auth_gss_authorized_principal <username>@<realm>
auth_gss_authorized_principal_regex ^(<username>)/(<group>)@<realm>$
```

10.7.5.2.3. Проверка аутентификации

Тестовый сайт должен быть доступен по адресу `http://<полное_доменное_имя_веб-сервера>`.

На рабочей станции, введенной в домен, получить билет Kerberos:

```
$ kinit ivanov
Password for ivanov@TEST.ALT:
$ klist
Ticket cache: KEYRING:persistent:500:krb_ccache_5VitJSL
Default principal: ivanov@TEST.ALT

Valid starting       Expires              Service principal
28.04.2023 15:54:41  29.04.2023 01:54:41  krbtgt/TEST.ALT@TEST.ALT
    renew until 05.05.2023 15:54:38
```

Попытаться прочитать содержимое сайта использую аутентификацию Kerberos:

```
$ curl --negotiate -u : http://web.test.alt
<html><body><h1>It works!</h1></body></html>
```

Получено содержимое страницы.

Удалить билеты Kerberos:

```
$ kdestroy
$ klist
```

Попытаться прочитать содержимое сайта использую аутентификацию Kerberos:

```
$ curl --negotiate -u : http://web.test.alt

<html>
<head><title>401 Authorization Required</title></head>
<body>
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.22.1</center>
</body>
</html>
```

Содержимое страницы не доступно.

10.7.5.3. Настройка веб-браузеров для SSO

Предварительно необходимо ввести компьютер в домен (см. п. 10.4) и убедиться, что доменный пользователь получает билет Kerberos.

Для работы SSO в веб-браузерах необходимо произвести некоторые настройки.

Порядок действий:

1) в адресной строке ввести `about:config`, чтобы отобразить список текущих параметров конфигурации (необходимо будет нажать кнопку «Принять риск и продолжить»);
2) в поле «Фильтр» ввести «negotiate», чтобы ограничить список параметров»;
3) выбрать параметр `network.negotiate-auth.trusted-uris`;
4) указать в этом параметре имя kerberos области (realm), включая предшествующую точку (.). Если нужно добавить несколько доменов, их необходимо указать через запятую (рис. 397).

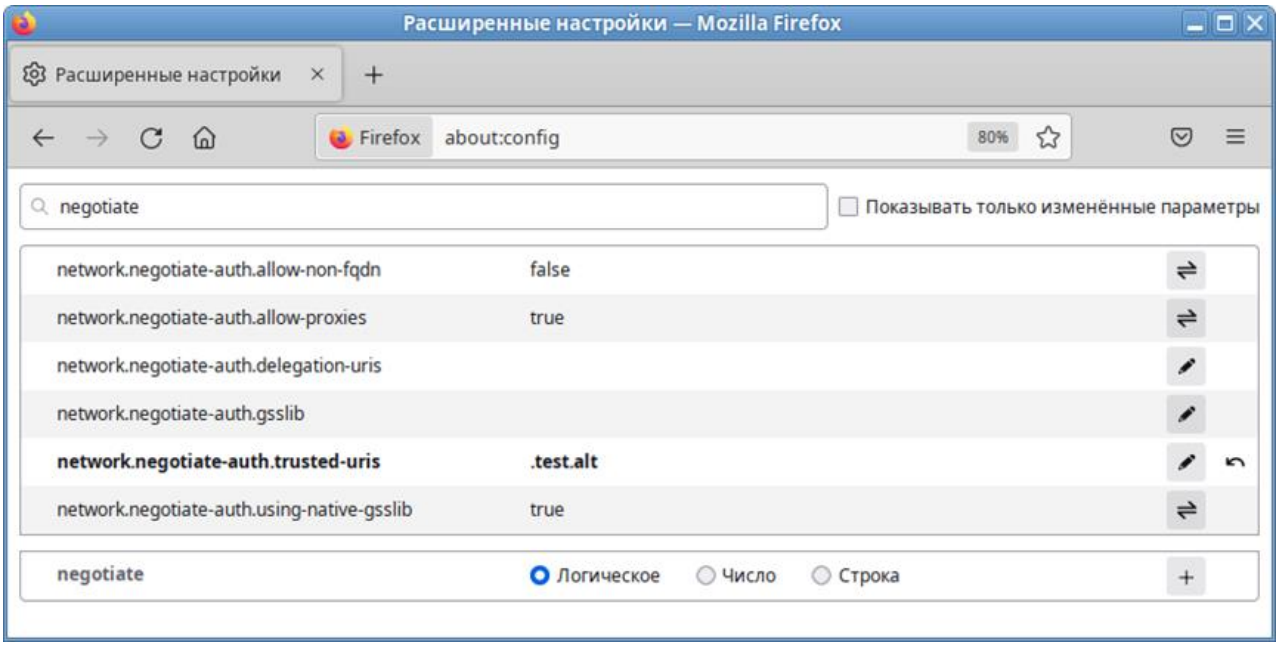


Рис. 397 – Ограниченный список параметров конфигурации

В ряде случаев может потребоваться отредактировать еще несколько параметров:

1) параметр `network.automatic-ntlm-auth.trusted-uris` выставить в kerberos realm: `.test.alt`;
2) параметр `network.negotiate-auth.delegation-uris` выставить в kerberos realm: `.test.alt`;
3) параметр `network.automatic-ntlm-auth.allow-non-fqdn` выставить в: `true`;
4) параметр `network.negotiate-auth.allow-non-fqdn` выставить в: `true`.

Вместо выставления этих параметров можно создать файл `/usr/lib64/firefox/browser/defaults/preferences/prefs.js` со следующим содержимым:

```
pref("network.negotiate-auth.trusted-uris",".test.alt");
pref("network.automatic-ntlm-auth.trusted-uris",".test.alt");
pref("network.automatic-ntlm-auth.allow-non-fqdn","true");
pref("network.negotiate-auth.allow-non-fqdn","true");
pref("network.negotiate-auth.delegation-uris",".test.alt");
```

Эти параметры могут быть распространены через групповые политики для Firefox:

- параметр `network.negotiate-auth.trusted-uris` – политика SPNEGO;
- параметр `network.automatic-ntlm-auth.trusted-uris` – политика NTLM;
- параметр `network.negotiate-auth.delegation-uris` – политика «Делегированная авторизация»;
- параметр `network.automatic-ntlm-auth.allow-non-fqdn` – политика «Разрешить неполное доменное имя» (Non FQDN);
- параметр `network.negotiate-auth.allow-non-fqdn` – политика «Разрешить неполное доменное имя» (Non FQDN).

10.7.5.3.1. Настройка Chromium

В файл `/etc/chromium/policies/managed/policies.json` добавить строку:

```
{
    "AuthServerAllowlist": "*.test.alt"
}
```

Где `.test.alt` – имя kerberos области (realm).

Для применения настроек необходимо перезапустить веб-браузер. Результат применения параметров политики для Chromium можно проверить, указав в адресной строке URL: `chrome://policy`.

Этот параметр может быть распространен через групповые политики для Chromium: политика «Список разрешенных серверов для аутентификации».

Примечание.Для проверки работы аутентификации без изменения настроек веб-браузера можно запустить веб-браузер из командной строки, выполнив команду:

```
$ chromium-browser --auth-server-whitelist="*.test.alt"
```

10.7.6. Distributed File System

Распределенная файловая система (Distributed File System, DFS) – серверная технология Microsoft, предназначенная для упрощения доступа к общим файловым ресурсам, распределенным по сети. С помощью DFS можно объединять в единую логическую структуру файловые ресурсы, физически находящиеся на различных серверах, а также производить между ними репликацию.

Функционал DFS образуют две составляющих: пространство DFS-имен – DFS-N (DFS-Namespace) и механизм репликации – DFS-R (DFS-Replication).

Samba поддерживает DFS-N, но пока не поддерживает DFS-R.

10.7.6.1. Пространство DFS-имен

Пространство DFS-имен – это единый виртуальный каталог, содержащий ссылки на общие каталоги, расположенные на разных файловых серверах. Пространство имен состоит из корня (root), ссылок (folders) и целевых объектов (folder targets). Пространство имен DFS может быть двух типов: автономное (Stand-alone) и доменное (Domain-based).

Автономный вариант работает на одном сервере и приводит к тому, что имена DFS содержат имя этого сервера, они выглядят как общие ресурсы, предоставляемые этим сервером (можно создать распределенную файловую систему не используя доменные службы AD).

При доменном варианте имена DFS содержат только имя домена, а не имя какого-либо конкретного сервера (имя сервера пространства имен скрыто от пользователей, проще замена сервера пространства имен или перенос пространства имен на другой сервер) (рис. 398).

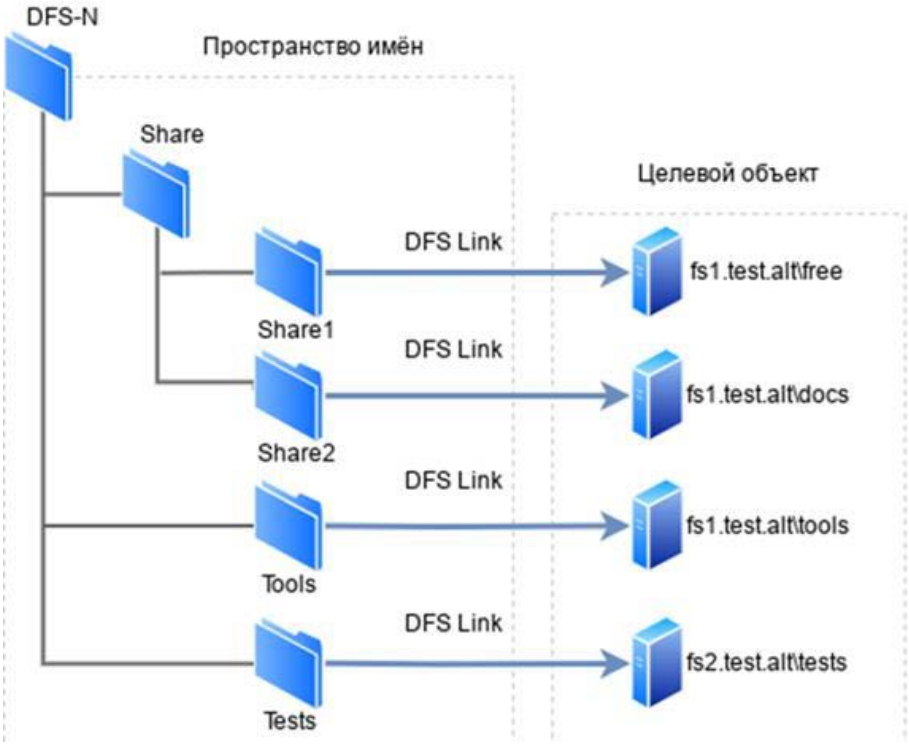


Рис. 398 – Структура дерева

Корень пространства имен (Namespace root) – это базовая точка, от которой начинается отсчет пространства имен. В зависимости от типа корень доступен по адресу `\\ServerName\RootName` (Stand-alone) или `\\DomainName\RootName` (Domain-based).

Каталог – ссылка в пространстве имен DFS, указывающая на целевой объект. Каталог без конечных объектов (например, каталог Share) образуют структуру и иерархию в пространстве имен, а каталоги с целевыми объектами (например, каталог Share1) предоставляют пользователям доступ к фактическому содержимому.

Целевой объект (Folder targets) – ссылка на общий файловый ресурс, находящийся на определенном файловом сервере. Одна ссылка может указывать как на один, так и на несколько целевых объектов.

10.7.6.2. Настройка DFS на сервере Samba

Прежде, чем перейти к добавлению пространства имен, необходимо создать хотя бы один сетевой каталог на любом из серверов, добавленных в домен.

Сервер Samba можно сделать сервером DFS, задав логический параметр `host msdfs` в файле `/etc/samba/smb.conf`.

Корень DFS назначается с помощью логического параметра `root msdfs`. Если для этого параметра установлено значение `yes`, Samba будет воспринимать открытый для общего доступа ресурс как корневой DFS. Ссылки DFS, указываемые в открытом для доступа каталоге, имеют вид: `msdfs:serverA\shareA,serverB\shareB` и т. д. Корневой каталог DFS в Samba содержит ссылки DFS в виде символических ссылок.

Для создания нового пространства имен необходимо выполнить следующие действия:

1) создать каталог, в котором будут настроены ссылки DFS на другие серверы в сети (в примере `/media/dfsroot`):

   ```
   # mkdir /media/dfsroot
   ```

2) в файле `/etc/samba/smb.conf` в секцию [`global`] добавить параметр:

   ```
   host msdfs = yes
   ```

   и добавить секцию [`dfs`], с указанием корня:

```
[dfs]
        path = /media/dfsroot
        msdfs root = yes
```

3) в каталоге `/media/dfsroot` настроить ссылки DFS на общие ресурсы в сети:

```
# cd /media/dfsroot
# ln -s msdfs:dc1.test.alt\\free linka
# ln -s msdfs:web.test.alt\\tests linkb
```

4) перезапустить samba:

```
# systemctl restart samba
```

5) дерево DFS теперь доступно по адресу `//test.alt/dfs/`. При доступе к ссылкам linka или linkb (которые отображаются для клиента как каталоги) пользователи напрямую переходят к соответствующим общим ресурсам в сети.

Проверка:

```
$  smbclient //test.alt/dfs/linka -U 'ivanov'
Password for [TEST\ivanov]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon May 22 10:13:28 2023
  ..                                  D        0  Mon May 22 10:13:06 2023
  dc.txt                              N        5  Mon May 22 15:57:14 2023

        48254668 blocks of size 1024. 40859796 blocks available
smb: \> exit
```

Примечание. Для доступа к ресурсам DFS по имени домена с использованием аутентификации Kerberos необходимо добавить к имени сервера псевдоним – имя домена. Это можно сделать, выполнив на контроллере домена команду:

```
# samba-tool spn add cifs/cifs/<имя_домена> <имя_сервера>$
```

Например:

```
# samba-tool spn add cifs/test.alt dc1$
```

Подключиться к данному пространству можно, набрав в адресной строке следующий адрес: `smb://<имя_домена>/<имя_пространства_имен>` (рис. 399).

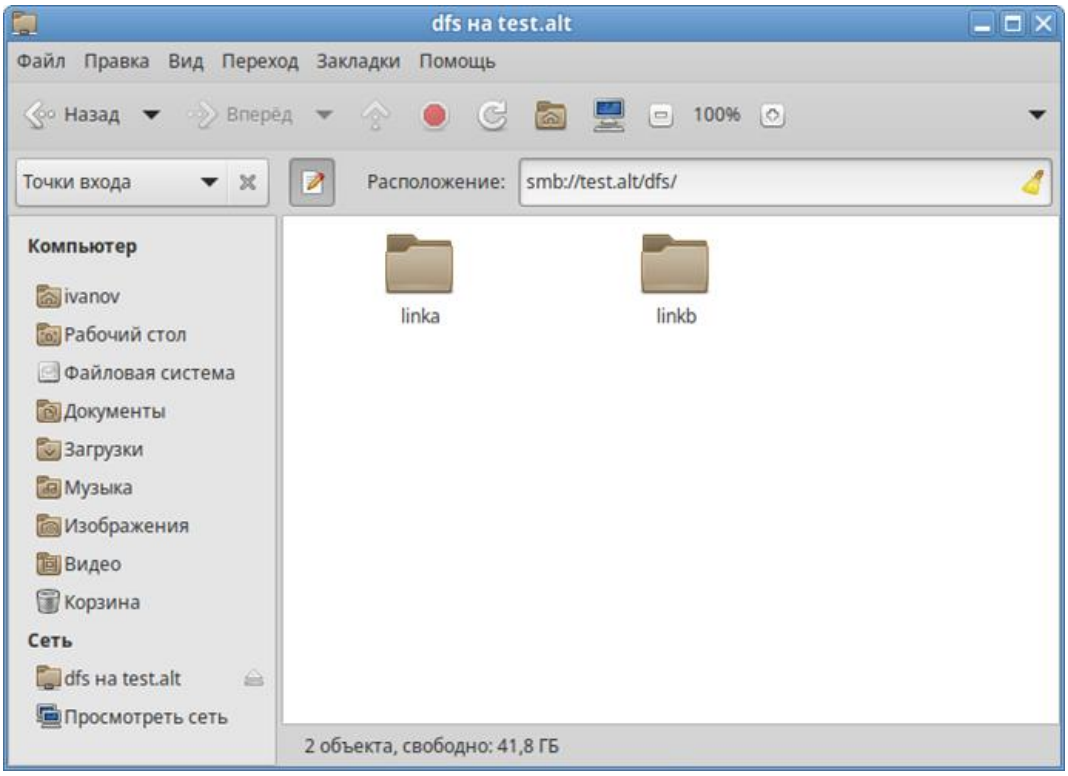


Рис. 399 – Подключение к пространству

10.7.7. Настройка SSSD

10.7.7.1. Журналирование SSSD

10.7.7.1.1. Файлы журналов SSSD

Каждая служба SSSD записывает логи в свой собственный файл журнала в каталоге `/var/log/sssd/`. Например, для машины в домене AD `test.alt`, файлы журналов SSSD могут выглядеть следующим образом:

```
# ls -l /var/log/sssd/
итого 1660
-rw------- 1 _sssd _sssd       0 мая 18 12:55 gpo_child.log
-rw------- 1 _sssd _sssd       0 мая 18 12:55 krb5_child.log
-rw------- 1 _sssd _sssd       0 мая 18 12:54 ldap_child.log
-rw------- 1 root  root      261 июн 19 10:10 sssd_ifp.log
-rw------- 1 root  root     3955 июн 19 09:34 sssd.log
-rw------- 1 _sssd _sssd 1677605 июн 19 11:18 sssd_nss.log
-rw------- 1 _sssd _sssd    1134 июн 19 09:34 sssd_pac.log
-rw------- 1 _sssd _sssd    3067 июн 19 09:34 sssd_pam.log
-rw------- 1 _sssd _sssd       0 мая 18 12:54 sssd_TEST.ALT.log
```

где:

- `krb5_child.log` – файл журнала для недолговечного вспомогательного процесса, участвующего в аутентификации Kerberos;

- `ldap_child.log` – файл журнала для недолговечного вспомогательного процесса, участвующего в получении билета Kerberos для связи с сервером LDAP$;
- `sssd_<domain.name>.log` – Для каждого раздела [`domain`] в файле `sssd.conf` служба SSSD записывает информацию о взаимодействии с LDAP-сервером в отдельный файл журнала;
- `sssd.log` – Файл журнала для мониторинга SSSD и связи его с ответчиком и внутренними процессами;
- `sssd_ifp.log` – Файл журнала для ответчика InfoPipe, который предоставляет общедоступный интерфейс D-Bus, доступный через системную шину;
- `sssd_nss.log` – Файл журнала для ответчика Name Services Switch (NSS), который извлекает информацию о пользователях и группах;
- `sssd_pac.log` – Файл журнала для ответчика Microsoft Privilege Attribute Certificate (PAC), который собирает PAC из билетов AD Kerberos и извлекает информацию о пользователях AD из PAC, что позволяет избежать ее запроса непосредственно из AD;
- `sssd_pam.log` – Файл журнала для ответчика Pluggable Authentication Module (PAM);
- `sssd_ssh.log` – Файл журнала для процесса ответчика SSH.

10.7.7.1.2. Уровни журналирования SSSD

Уровни журналирования SSSD представлены в таблице 50.

Таблица 50 – Уровни журналирования SSSD

Уровень	Описание
0 (0x0010)	Фатальные ошибки. Ошибки, которые не позволяют запустить службу SSSD или вызывает завершение работы сервиса
1 (0x0020)	Критические ошибки. Ошибки, которые не завершают работу службы SSSD, но означает, что как минимум одна из основных функций не работает должным образом
2 (0x0040)	Серьезные ошибки. Ошибки, сообщающие о том, что определенный запрос или операция завершились неудачно. Это уровень журналирования по умолчанию

Окончание таблицы 50

Уровень	Описание
3 (0x0080)	Незначительные ошибки. Ошибки, которые могут стать причиной ошибок 2-го уровня (ошибок при выполнении действий)
4 (0x0100)	Настройки конфигурации
5 (0x0200)	Данные функций
6 (0x0400)	Сообщения трассировки для функций действий
7 (0x1000)	Сообщения трассировки для функций внутреннего управления
8 (0x2000)	Содержимое переменных внутренних функций
9 (0x4000)	Информация трассировки крайне низкого уровня
9 (0x20000)	Быстродействие и статистические данные. Из-за способа обработки запросов на внутреннем уровне, записанное в журнал время выполнения запроса может быть больше, чем оно было на самом деле
10 (0x10000)	Информация трассировки libldb еще более низкого уровня. Практически никогда не требуется

Установка уровня журнала также включает все уровни ниже него. Например, установка уровня журнала на 6 также включает уровни с 0 по 5.

Чтобы вести журнал для необходимых уровней журналирования, указанных в представлении битовых масок, следует просто сложить их номера. Например, чтобы вести журнал для фатальных, критических, серьезных ошибок и для данных функций, следует использовать значение 0x0270.

10.7.7.1.3. Настройка уровня журналирования для SSSD в файле `sssd.conf`

Чтобы включить подробное журналирование, сохраняющееся при перезапуске службы SSSD, следует добавить опцию `debug_level=<целое_число>` в каждую секцию файла `/etc/sssd/sssd.conf`.

Где `<целое_число>` – число от 0 до 10. Уровни до 3 регистрируют крупные сбои, а уровни начиная с 8 и выше предоставляют большое количество подробных сообщений журнала. Уровень 6 является хорошей отправной точкой для отладки проблем.

Пример настройки уровня журналирования в файле `/etc/sssd/sssd.conf`:

```
[sssd]
debug_level = 6
config_file_version = 2
services = nss, pam

[domain/TEST.ALT]
debug_level = 6
```

```
id_provider = ad
…

[nss]
debug_level = 6

[pam]
debug_level = 6
```

Чтобы загрузить новые параметры конфигурации необходимо перезапустить службу SSSD:

```
# systemctl restart sssd
```

10.7.7.1.4. Настройка уровня журналирования для SSSD с помощью команды `sssctl`

Изменить уровень журналирования службы SSSD можно с помощью команды `sssctl debug-level <целое_число>`.

Где `<целое_число>` – число от 0 до 10. Уровни до 3 регистрируют крупные сбои, а уровни начиная с 8 и выше предоставляют большое количество подробных сообщений журнала. Уровень 6 является хорошей отправной точкой для отладки проблем.

Просмотр текущего уровня журналирования:

```
# sssctl debug-level
sssd                      0x0070
nss                       0x0070
pam                       0x0070
pac                       0x0070
domain/TEST.ALT           0x0070
```

Установка нового уровня журналирования:

```
# sssctl debug-level 6
# sssctl debug-level
sssd                      0x07f0
nss                       0x07f0
pam                       0x07f0
pac                       0x07f0
domain/TEST.ALT           0x07f0
```

Примечание. Уровень журналирования, заданный с помощью команды `sssctl debug-level` будет действовать до перезапуска службы `sssd`.

10.7.7.2. Настройки SSSD в ЦУС

Настройки SSSD в ЦУС представлены на рис. 400 и таблице 51.

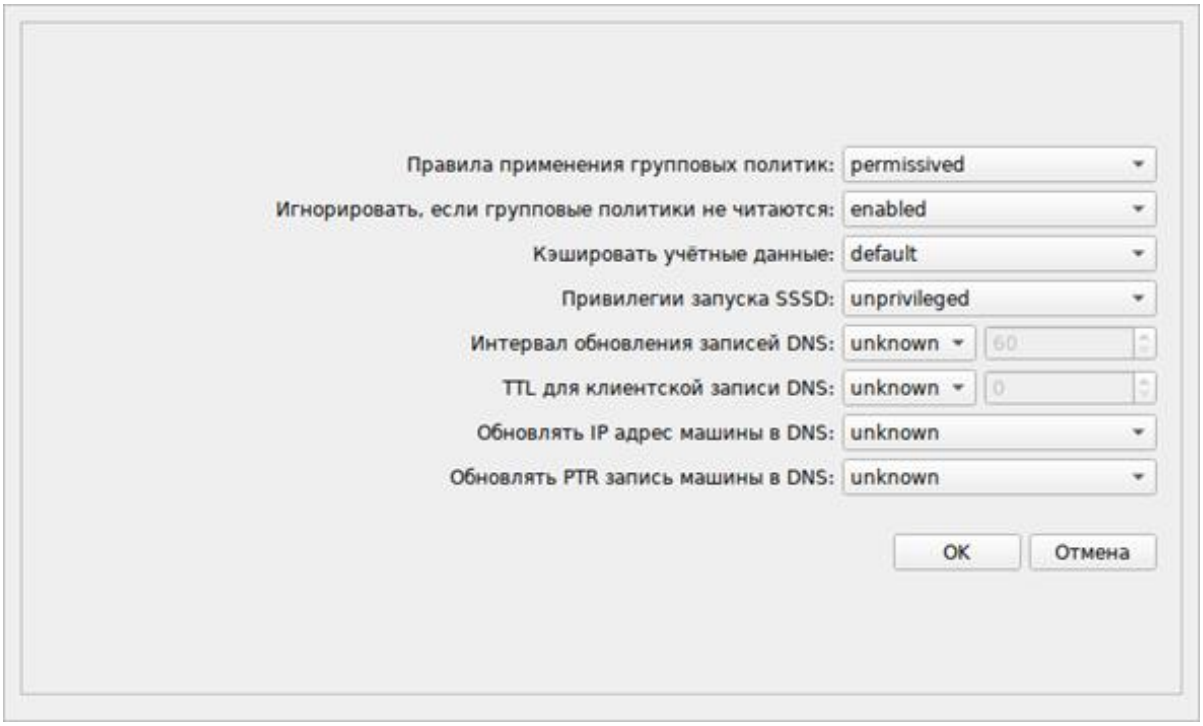


Рис. 400 – Настройки SSSD в ЦУС

Таблица 51 – Настройки SSSD в ЦУС

Настройка	Опция в файле `/etc/sssd/sssd.conf`	Описание	Режимы
Правила применения групповых политик	`ad_gpo_access_control`	Определяет в каком режиме будет осуществляться контроль доступа в SSSD основанный на групповых политиках Active Directory (GPO)	`enforced` (принудительный режим) – правила управления доступом в SSSD основанные на GPO выполняются, ведется логирование. `permissived` (разрешающий режим) – правила управления доступом в SSSD основанные на GPO не выполняются, ведется только логирование. Такой режим необходим администратору, чтобы оценить, как срабатывают новые правила. `disabled` (отключить) – правила управления доступом в SSSD основанные на GPO не логируются и не выполняются.

Продолжение таблицы 51

Настройка	Опция в файле `/etc/sssd/sssd.conf`	Описание	Режимы
			`default` (по умолчанию) – настройка контроля доступом в SSSD основанное на GPO сброшена на значение по умолчанию в пакете
Игнорировать, если групповые политики не читаются	`ad_gpo_ignore_unreadable`	Определяет будут ли проигнорированы правила управления доступом в SSSD основанные на групповых политиках, если недоступен какой-либо шаблон (GPT) объекта групповой политики (GPO)	`enabled` (включить) – игнорировать правила управления доступом через групповые политики, если шаблоны групповых политик не доступны для SSSD. `disabled` (отключить) – запретить доступ пользователям SSSD AD, которым назначены групповые политики, если шаблоны групповых политик не доступны. `default` (по умолчанию) – настройка игнорирования политик, при недоступности шаблонов групповых политик сброшена на значение по умолчанию в пакете
Кэшировать учетные данные	`cache-credentials`	Определяет, будут ли учетные данные удаленных пользователей сохраняться в локальном кэше SSSD	`enabled` (включить) – сохранение в локальном кэше SSSD учетных данных пользователей включено. `disabled` (отключить) – сохранение в локальном кэше SSSD учетных данных пользователей отключено. `default` (по умолчанию) – настройка сохранения в локальном кэше SSSD учетных данных пользователей сброшена на значение по умолчанию в пакете
Привилегии запуска SSSD	`control sssd-drop-privileges`	Позволяет сбросить права службы SSSD, чтобы избежать работы от имени суперпользователя (root)	`privileged` (привилегированный) – служба SSSD запущена от имени привилегированного суперпользователя (root).

Продолжение таблицы 51

Настройка	Опция в файле `/etc/sssd/sssd.conf`	Описание	Режимы
			`unprivileged` (непривилегированный) – служба SSSD запущена от имени непривилегированного пользователя (_sssd). `default` (по умолчанию) – режим привилегий службы SSSD задан по умолчанию в пакете
Интервал обновления записей DNS	`dyndns_refresh_interval`	Определяет, как часто серверная часть должна выполнять периодическое обновление DNS в дополнение к автоматическому обновлению, выполняемому при подключении серверной части к сети. Этот параметр является применимым только в том случае, если для `dyndns_update` установлено значение `true`.	`enabled` (включить) – задать интервал. `disabled` (отключить) – установить значение по умолчанию (86400) `unknown`
TTL для клиентской записи DNS	`dyndns_ttl`	Срок жизни, применяемый к DNS-записи клиента при ее обновлении. Если `dyndns_update` имеет значение `false`, это не имеет никакого эффекта	`enabled` (включить) – задать TTL. `disabled` (отключить) – установить значение по умолчанию (3600) `unknown`
Обновлять IP-адрес машины в DNS	`dyndns_update`	Позволяет включить или отключить автоматическое обновление DNS-записей (защищенных с помощью GSS-TSIG) с IP-адресом клиента через SSSD	`enabled` (включить) – автоматическое обновление DNS-записи клиента через SSSD включено. `disabled` (отключить) – автоматическое обновление DNS-записи клиента через SSSD отключено. `default` (по умолчанию) – настройка автоматического обновления DNS-записи

Окончание таблицы 51

Настройка	Опция в файле `/etc/sssd/sssd.conf`	Описание	Режимы
			клиента через SSSD задана по умолчанию в пакете `unknown`
Обновлять PTR-запись машины в DNS-записей	`dyndns_update_ptr`	Определяет будет ли обновляться клиентская PTR-запись (защищенная с помощью GSS-TSIG) при обновлении DNS-записей клиента. Применимо, только если `dyndns_update` и меет значение `true`.	`enabled` (включить) – автоматическое обновление DNS-записи обратной зоны через SSSD включено. `disabled` (отключить) – автоматическое обновление DNS-записи обратной зоны через SSSD отключено. `default` (по умолчанию) – настройка автоматического обновления DNS-записи обратной зоны задана по умолчанию в пакете `unknown`

10.7.7.3. Включение автономной аутентификации

По умолчанию SSSD не кэширует учетные данные пользователей. При обработке запросов на аутентификацию SSSD всегда обращается к поставщику идентификационных данных. Если провайдер недоступен, аутентификация пользователя не проходит.

Чтобы пользователи могли пройти аутентификацию, даже когда провайдер идентификации недоступен, можно включить кэширование учетных данных, установив параметр `cache_credentials` в значение `true` в файле `/etc/sssd/sssd.conf`.

Чтобы пользователи могли пройти аутентификацию, даже когда провайдер идентификации недоступен, можно включить кэширование учетных данных, установив параметр `cache_credentials` в значение `true` в разделе домена.

Дополнительно можно использовать параметр `offline_credentials_expiration` в разделе [`pam`], чтобы установить ограничение по времени (в днях), в течении которого пользователи смогут аутентифицироваться в автономном режиме с момента последнего успешного входа.

Пример настройки возможности автономной аутентификации пользователей в течение 5 дней с момента последнего успешного входа:

```
[pam]
offline_credentials_expiration = 5
[domain/TEST.ALT]
cache_credentials = true
```

10.7.8. Файловый сервер

Samba можно настроить как файловый сервер. Samba также можно настроить как сервер печати для совместного доступа к принтеру.

10.7.9. Монтирование общих ресурсов samba

Рассматриваемые ниже способы позволяют подключать файловые ресурсы (file shares) для доменного пользователя без повторного ввода пароля (SSO, Single Sign-On).

10.7.9.1. Подключение с использованием gio

Примечание. Способ актуален для дистрибутивов, использующих gio (например, Simply Linux, Альт Рабочая станция).

Недостаток этого способа – необходимо открыть ресурс в файловом менеджере (Caja, Pcmanfm). Однако можно открывать любые ресурсы на любых серверах, входящие в домен Active Directory.

Установить необходимые пакеты:

```
# apt-get install fuse-gvfs gvfs-backend-smb libgio
```

Включить пользователя в группу `fuse`:

```
# gpasswd -a <пользователь> fuse
```

Разрешить для всех доступ к `fuse` под root:

```
# control fusermount public
```

Войти под доменным пользователем.

Открыть ресурс в файловом менеджере (например, по адресу `smb://server/sysvol`). Ресурс смонтирован по пути `/var/run/<uid_пользователя>/gvfs`

или

`/var/run/user/<uid_пользователя>/gvfs/smb-share:server=сервер, share=ресурс`.

Другой вариант (полезно для скриптов в автозапуске):

```
gio mount smb://server/sysvol/
```

Примечание. Если необходимо открывать что-то с ресурса в WINE, в `winecfg` следует добавить диск с путем `/var/run/uid_пользователя/gvfs`.

10.7.9.2. Подключение с использованием pam_mount

При этом способе сетевой ресурс подключается с заданного сервера автоматически при каждом входе доменным пользователем.

Установить пакеты pam_mount и cifs-utils:

```
# apt-get install pam_mount cifs-utils
```

Примечание. Для того, чтобы файловые ресурсы, подключенные с помощью pam_mount, корректно отключались при завершении сеанса, следует установить пакет systemd-settings-enable-kill-user-processes и перезагрузить систему:

```
# apt-get install systemd-settings-enable-kill-user-processes
```

Прописать `pam_mount` в схему аутентификации по умолчанию. Для этого в конец файла `/etc/pam.d/system-auth` добавить строки:

```
session     [success=1 default=ignore] pam_succeed_if.so   service = systemd-user quiet
session    optional        pam_mount.so disable_interactive
```

Установить правило монтирования ресурса в файле `/etc/security/pam_mount.conf.xml` (перед тегом `<cifsmount>`):

```
<volume     uid="10000-2000200000"     fstype="cifs"     server="dc1.test.alt" path="sysvol" mountpoint="~/share"
options="sec=krb5i,cruid=%(USERUID),nounix,uid=%(USERUID),gid=%(USERGID),file_mode=0664,dir_mode=0775" />
```

где:

- `uid="10000-2000200000"` – диапазон присваиваемых для доменных пользователей UID (подходит для Winbind и для SSSD);
- `server="dc1.test.alt"` –имя сервера с ресурсом;
- `path="sysvol"` – имя файлового ресурса;
- `mountpoint="~/share"` – путь монтирования в домашней папке пользователя.

Опционально можно добавить:

`sgrp="group_name"` – имя группы, при членстве пользователя в которой, папка будет примонтирована.

Параметр `sec=krb5i` более безопасный, но требует больше вычислительных ресурсов. Вместо него можно указать `sec=krb5`.

⚠ В параметре server необходимо указывать настоящее имя сервера, а не имя домена.

⚠ По умолчанию для монтирования используется `smb` версии 1.0, если он отключен, то необходимо указать в параметрах версию 2 или 3:

```
<volume uid="10000-2000200000" fstype="cifs" server="dc1.test.alt"
path="sysvol" mountpoint="~/share"
options="sec=krb5i,vers=2.0,cruid=%(USERUID),nounix,uid=%(USERUID),gid
=%(USERGID),file_mode=0664,dir_mode=0775" />
```

⚠ Для проверки можно попробовать смонтировать ресурс в сессии: `mount.cifs //dc1.test.alt/sysvol /mnt/ -o vers=2.0,user=Ivanov`

⚠ Также можно проверить доступность ресурса с помощью `smbclient`, например: `smbclient -L dc1.test.alt -U ivanov -m SMB2`

10.7.9.3. Подключение с использованием Autofs

При этом способе заданный ресурс подключается автоматически при каждом обращении пользователя и отключается после определенного времени бездействия (определяется конфигурацией Autofs).

Принцип работы:

- задается каталог, в котором будет происходить подключение, например, `/mnt/auto/`;
- при необходимости обратиться к сетевой файловой системе, следует обратиться к каталогу с именем этой ФС в этом каталоге. Например, `/mnt/auto/server/share/`;
- при обращении будет произведена попытка смонтировать соответствующий сетевой ресурс;

- при отсутствии обращения, после заданного таймаута, сетевой ресурс будет отмонтирован;
- AutoFS использует для конфигурирования шаблоны `/etc/auto*`. Основной шаблон называется auto.master, он может указывать на один или несколько других шаблонов для конкретных типов носителей. Пример содержимого файла `/etc/auto.master`:

```
# Format of this file:
# mountpoint map options
# For details of the format look at autofs(8).
/mnt/auto       /etc/auto.tab   -t 5
/mnt/net        /etc/auto.avahi -t 120
```

Первое значение в каждой строке определяет базовый каталог, в который носители будут монтироваться, второе значение – файл конфигурации или скрипт, который будет использован.

Примечание. Параметр `-t` (`--timeout`) устанавливает количество секунд, после истечения которых каталоги будут размонтированы. Значение 0 отключает таймаут. Значения параметра по умолчанию задаются в файле `/etc/autofs.conf`.

Базовый каталог будет создан, если он не существует. Он станет точкой монтирования, отображающей в себе динамически подключаемые носители, что означает, что существующее содержимое базового каталога будет недоступно пока autofs работает.

Пример настройки автоматического подключения сетевых файловых ресурсов Windows (Samba) при входе пользователя:

1) добавить в `/etc/auto.master` строку:

```
/mnt/samba /etc/auto.smb -t 120
```

где:

- `/mnt/samba` – каталог в котором будут подключаться сетевые файловые системы;
- `/etc/auto.smb` – стандартный скрипт, входящий в состав пакета autofs;
- `120` – таймаут подключения при отсутствии обращения.

2) включить и запустить сервис autofs:

```
# systemctl enable --now autofs
```

3) для автоматического подключения ресурсов достаточно обратиться к ресурсу по имени хоста, например:

```
$ ls /mnt/samba/<имя_хоста>
```

Или в диспетчере файлов (рис. 401).

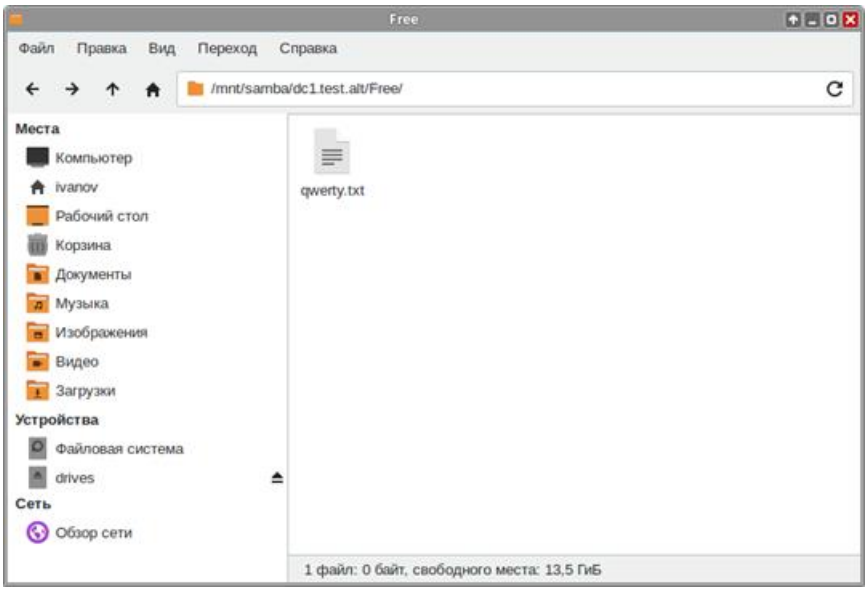


Рис. 401 – Диспетчер файлов

Пример настройки автоматического подключения сетевых файловых ресурсов Windows (Samba) при входе пользователя в систему для дистрибутивов с KDE (Альт Рабочая станция К, Альт Образование):

1) установить пакет kde5-autofs-shares:

```
# apt-get install kde5-autofs-shares
```

2) добавить в `/etc/auto.master` строку:

```
/mnt/samba /etc/auto.smb -t 120
```

где:

- `/mnt/samba` – каталог в котором будут подключаться сетевые файловые системы;
- `/etc/auto.smb` – скрипт, входящий в состав пакета autofs;
- `120` – таймаут подключения при отсутствии обращения;

3) включить и запустить сервис autofs:

```
# systemctl enable --now autofs
```

4) в диспетчере файлов Dolphin по адресу `smb://test.alt` («Сеть» → «Общие папки Samba») найти нужный ресурс Windows (Samba);

5) в контекстном меню подключаемого ресурса выбрать пункт «Подключение» (рис. 402).

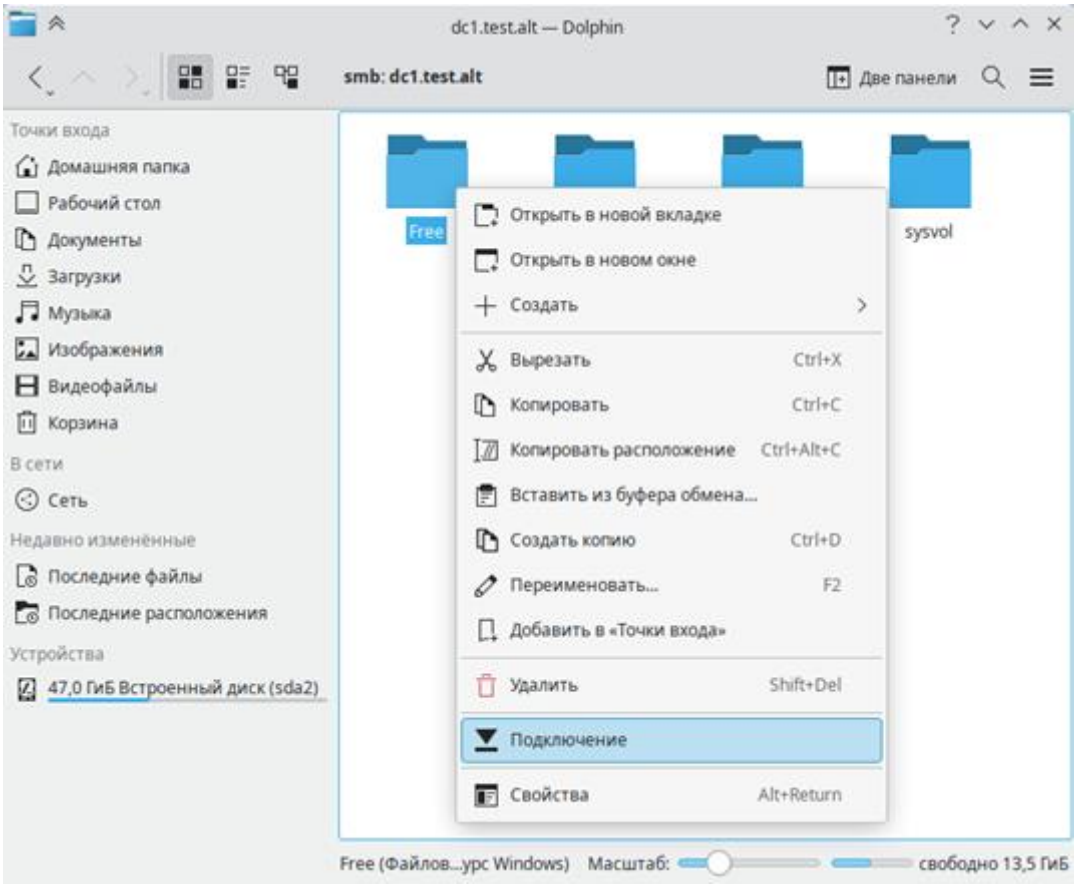


Рис. 402 – Вызов контекстного меню

Данный ресурс будет подключаться автоматически при входе в систему (рис. 403).

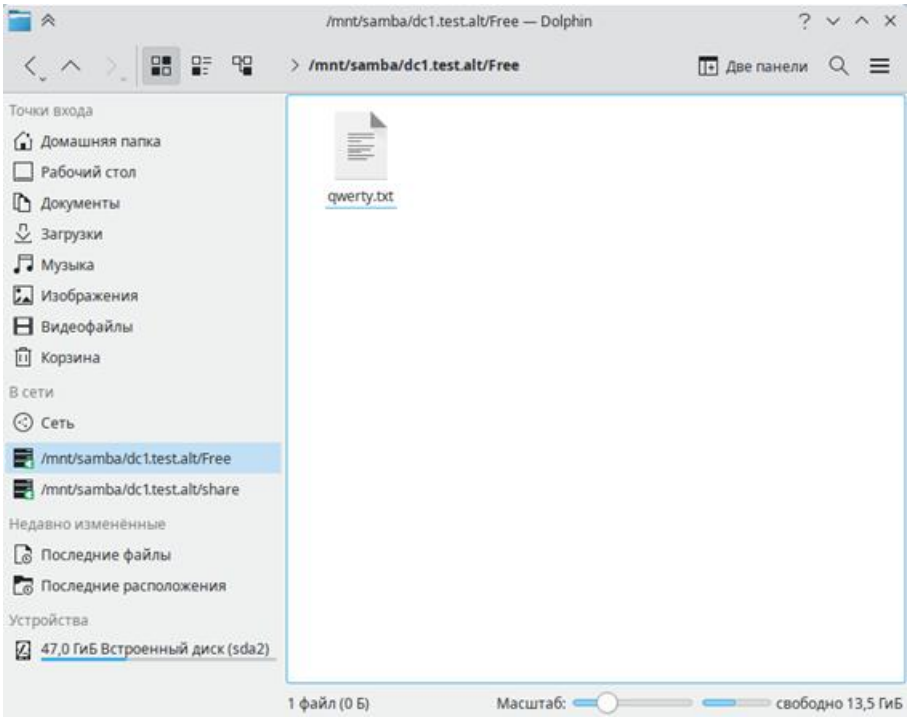


Рис. 403 – Автоматическое подключения ресурса

Примечание. Список ресурсов для подключения хранится в файле `~/.autofs.shares`.

ВАЖНО
Данный способ работает только для ресурсов с гостевым доступом или ресурсов с авторизацией Kerberos.

10.7.10. Установка RSAT

Для администрирования Active Directory из Windows можно использовать средства удаленного администрирования сервера Microsoft (RSAT).

10.7.10.1. Windows Server

В ОС Windows Server средства удаленного администрирования сервера Microsoft (RSAT) включены по умолчанию.

Для установки необходимо выполнить следующие пункты:

1) запустить Диспетчер серверов;

2) на Windows Server 2012, 2012 R2, и 2016:

- выбрать «Управление» → «Добавить роли и компоненты» (рис. 404);

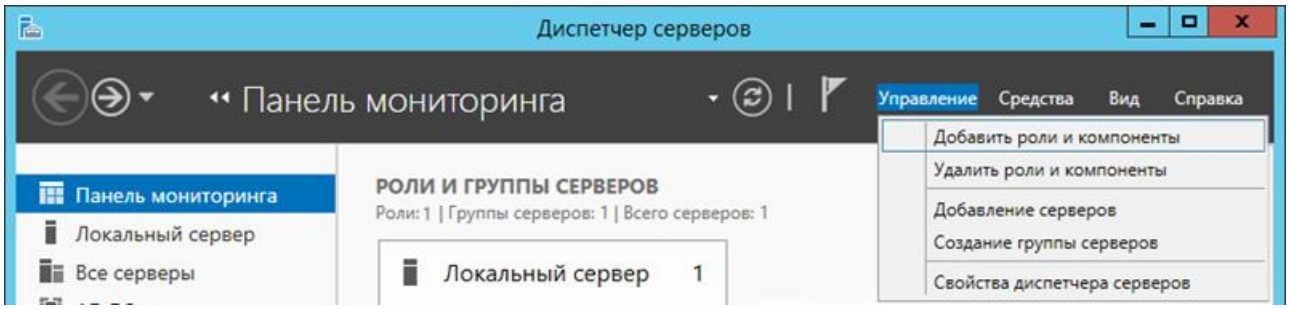


Рис. 404 – Панель мониторинга

- в открывшемся окне «Мастер добавления ролей и компонентов» выбрать пункт «Установка ролей или компонентов» (рис. 405);
- выбрать хост, на котором будут установлены компоненты (рис. 406);
- Нажать кнопку «Далее»;

3) на Windows Server 2008 и 2008 R2 в дереве навигации выбрать «Компоненты» и нажать «Добавить компоненты».

4) выбрать компоненты для установки (рекомендуемые компоненты см. в таблице 52).

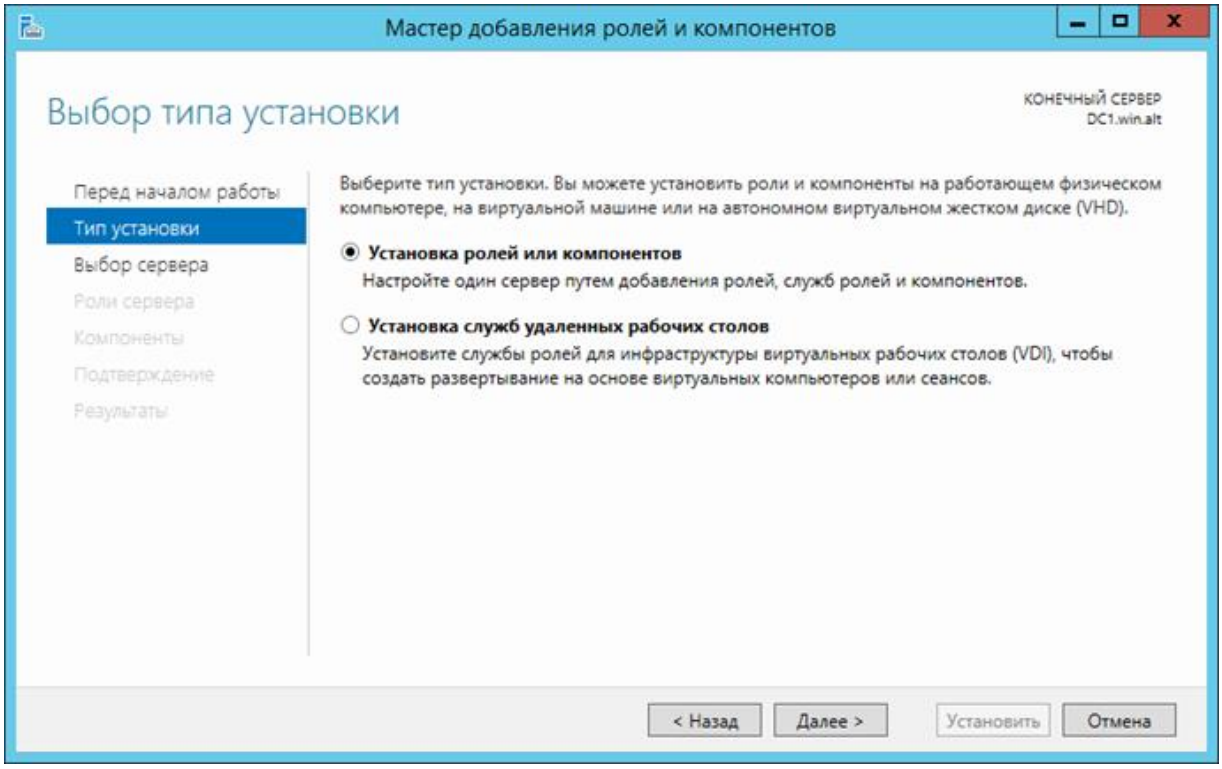


Рис. 405 – Выбор типа установки

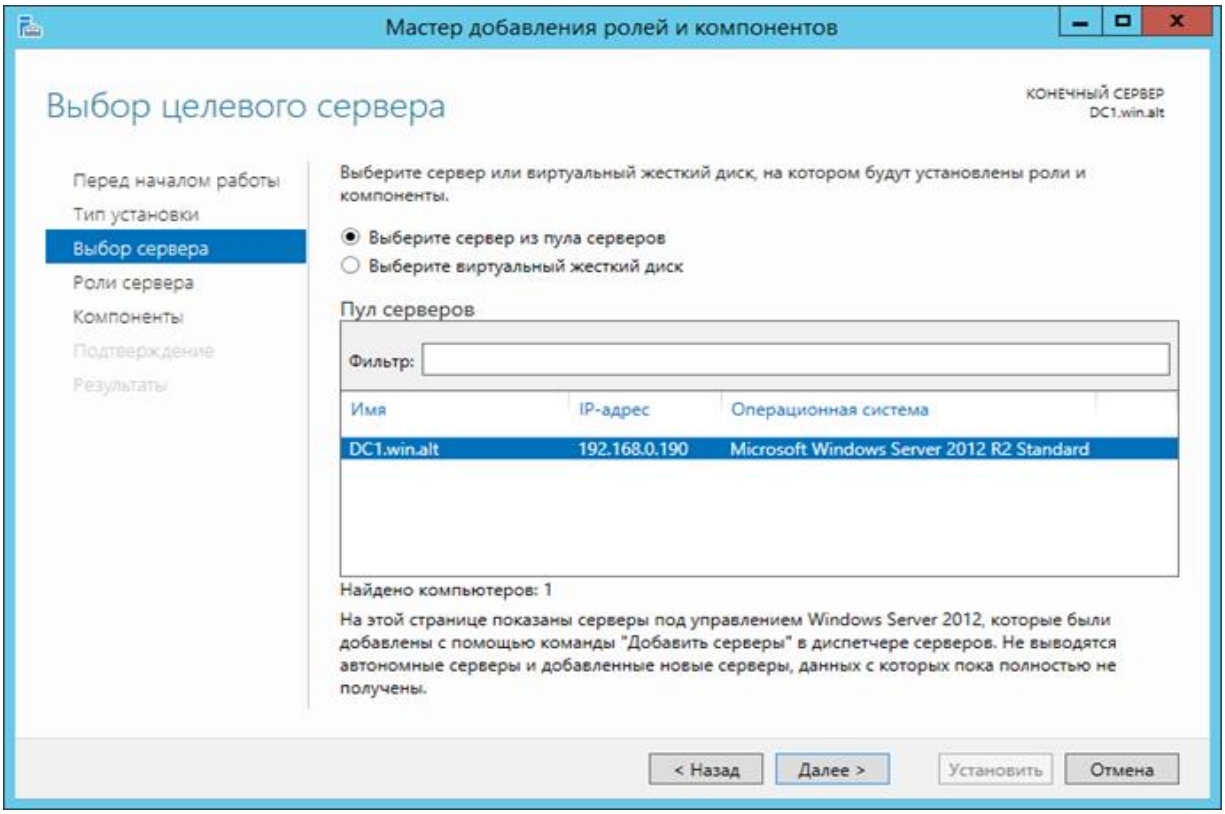


Рис. 406 – Выбор целевого сервера

Т а б л и ц а 52 – Рекомендуемые компоненты для администрирования

Компонент	Описание
Group Policy Management	Предоставляет оснастки для групповой политики: средство управления (GPMC), редактор управления (gpedit) и начальный редактор GPO
AD DS Snap-Ins and Command-Line Tools	Предоставляет оснастку «Пользователи и компьютеры Active Directory» (ADUC) и «Сайты и службы Active Directory» (ADSS)
Server for NIS	Добавляет вкладку Атрибуты UNIX в свойства объектов ADUC. Позволяет настраивать атрибуты RFC2307. Эта функция не поддерживается в Windows Server 2016
Active Directory Module for Windows PowerShell	Включает командлеты Active Directory (AD) PowerShell
DNS Server tools	Оснастка MMC DNS для удаленного управления DNS

10.7.10.2. Windows 10 (1809 и более поздние версии)

В Windows 10 1809 и более поздних версиях RSAT устанавливается в качестве дополнительной функции. Для установки компьютер должен иметь доступ в Интернет.

Для установки RSAT выполнить следующие действия:

1) перейти в раздел «Settings» → «Apps» → «Optional Features» → «View features» («Параметры Windows» → «Приложения» → «Дополнительные возможности» → «Добавить компонент») (рис. 407);

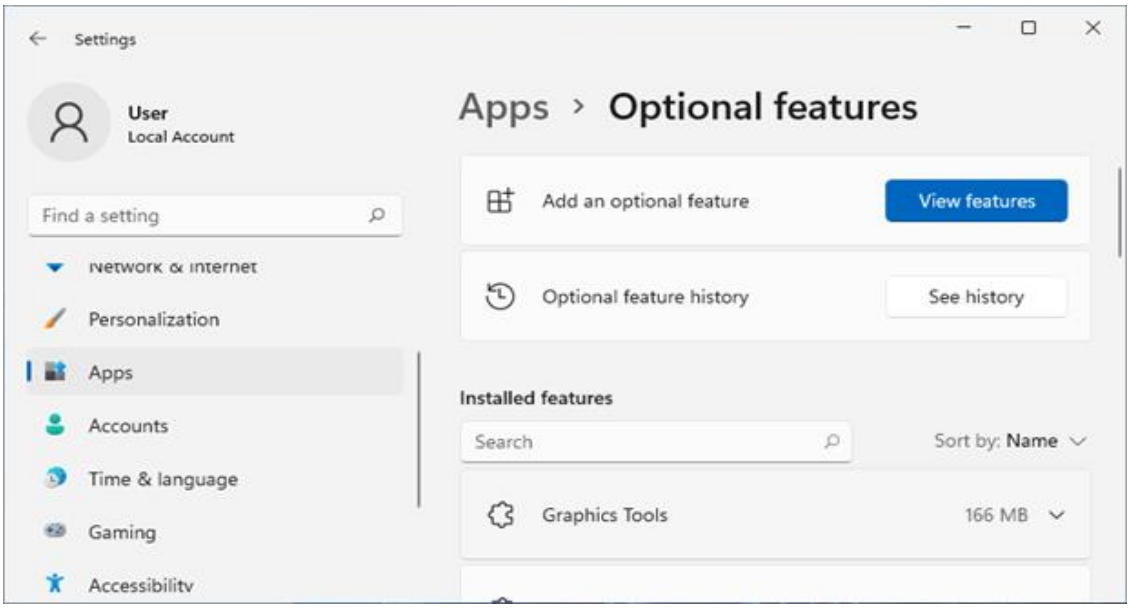


Рис. 407 – Дополнительные возможности

2) выбрать нужные компоненты RSAT (рекомендованнын компоненты RSAt представленны в таблице 53) и нажать кнопку «Next» (рис. 408);

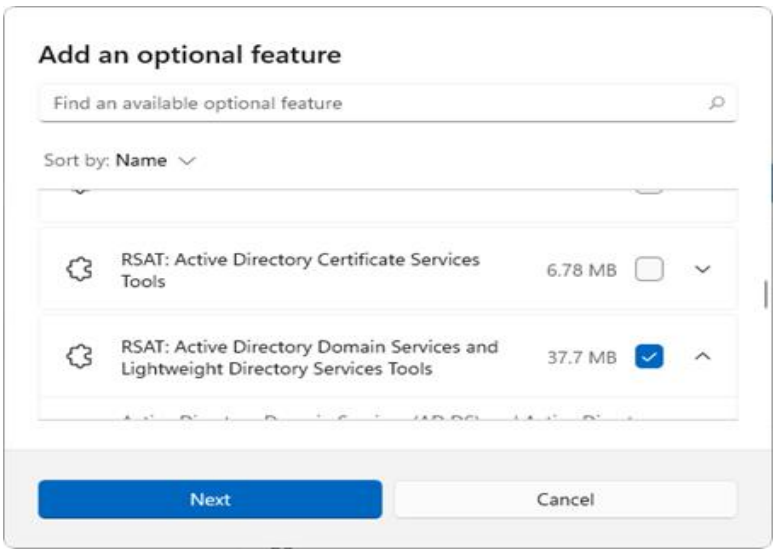


Рис. 408 – Добавление компонентов

3) нажать кнопку «Install».

Т а б л и ц а 53 – Рекомендуемые компоненты RSAT

Компонент	Описание
RSAT: Group Policy Management Tools	Включают консоль управления групповыми политиками (gpmc.msc), редактор управления групповыми политиками (gpme.msc) и редактор GPO инициализирующей программы групповой политики (gpedit.msc)
RSAT: Active Directory Domain Services and Lightweight Directory Services Tools	Предоставляет оснастку «Пользователи и компьютеры Active Directory» (ADUC) и «Сайты и службы Active Directory» (ADSS)
RSAT: DNS Server Tools	Включает оснастку «Диспетчер DNS» для удаленного управления DNS и программу командной строки dnscmd.exe
RSAT: Remote Desktop Services Tool	Добавляет вкладку Профиль служб удаленных рабочих столов в свойства объекта пользователя ADUC и устанавливает оснастку MMC «Удаленные рабочие столы» для администрирования RDP-сервера (tsmmc.msc).

10.7.10.3. Windows Vista и 7

До версии Windows 10 1809 пакет удаленного администрирования серверов RSAT устанавливается в виде MSU обновления, которое нужно скачать с серверов Microsoft.

Для установки RSAT необходимо выполнить следующие действия:

1) перейти в «Панель управления» → «Программы» → «Включение или отключение компонентов Windows» (рис. 409).

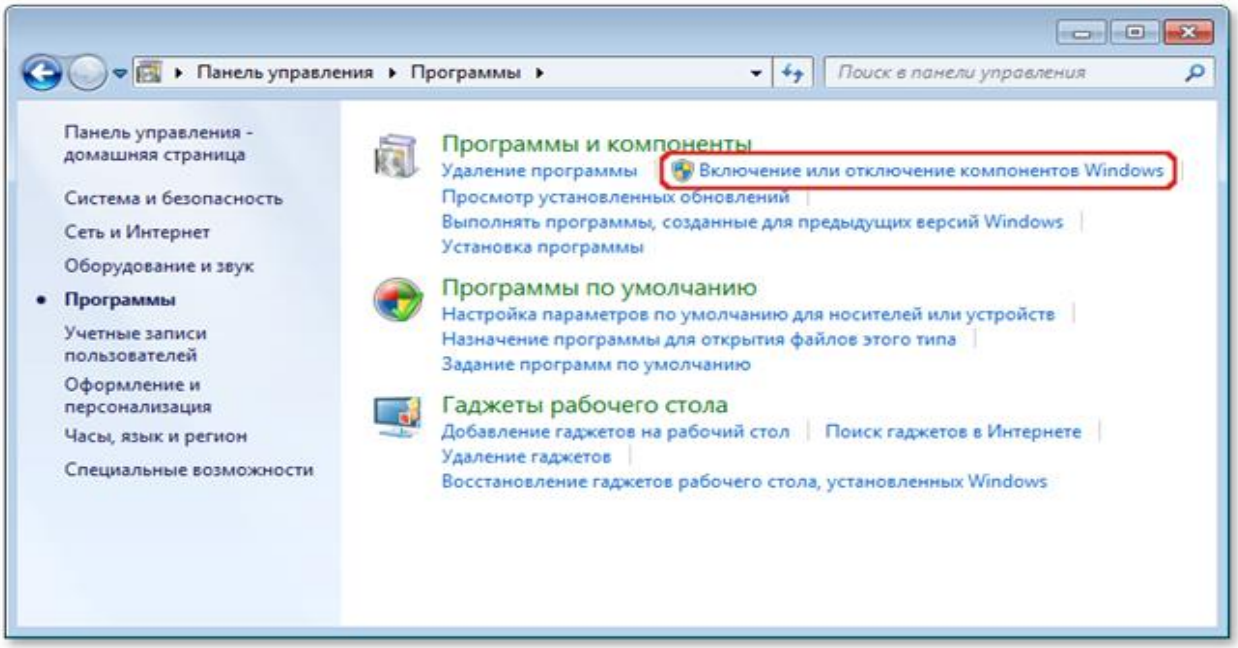


Рис. 409 – «Включение или отключение компонентов Windows»

2) включить компоненты, представленные на рис. 410 и описанные в таблице 54.

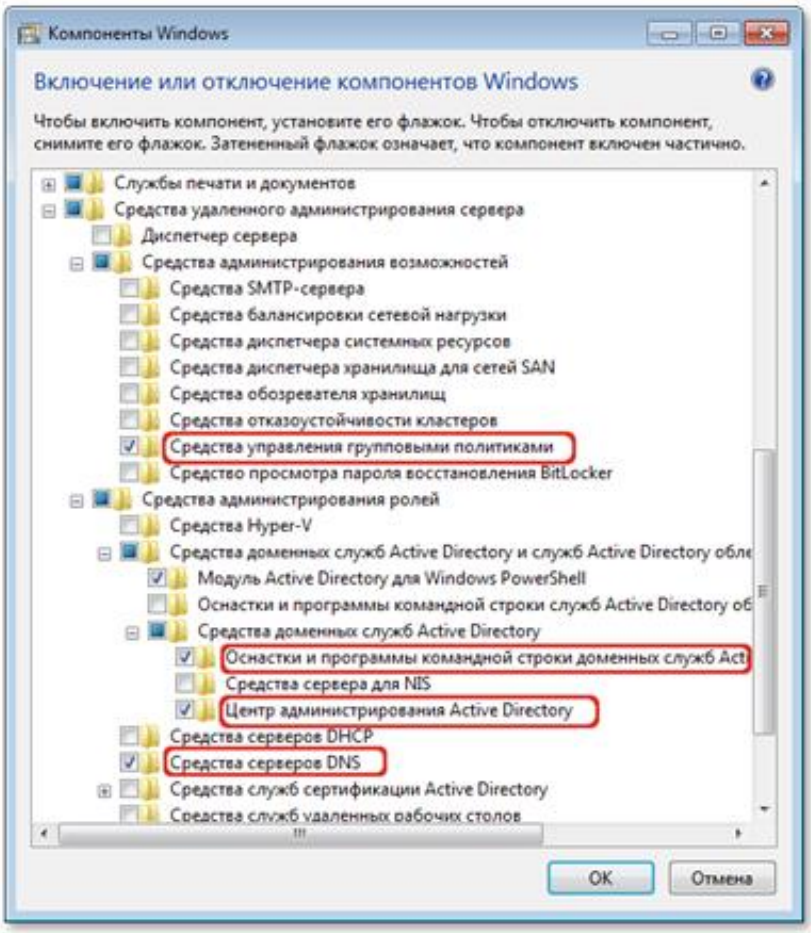


Рис. 410 – Компоненты для включения

Т а б л и ц а 54 – Рекомендуемые компоненты Windows

Компонент	Описание
Group Policy Management Tools (Средства управления групповыми политиками)	Включают консоль управления групповыми политиками (gpmc.msc), редактор управления групповыми политиками (gpme.msc) и редактор GPO инициализирующей программы групповой политики (gpedit.msc)
AD DS Tools (Оснастки и программы командной строки доменных служб Active Directory)	Предоставляет оснастку «Пользователи и компьютеры Active Directory» (ADUC) и «Сайты и службы Active Directory» (ADSS)
Server for NIS Tools (Средства сервера для NIS)	Средства сервера для сетевых информационных служб добавляет вкладку Атрибуты UNIX (UNIX Attributes) в свойства объектов ADUC. Позволяет настраивать атрибуты RFC2307. Включает программу командной строки ypclear.exe

Окончание таблицы 54

Компонент	Описание
Active Directory Module for Windows PowerShell (Модуль Active Directory для Windows PowerShell)	Обеспечивает централизованную среду для управления службами каталогов
DNS Server tools (Средства серверов DNS)	Включает оснастку «Диспетчер DNS» для удаленного управления DNS и программу командной строки dnscmd.exe
Remote Desktop Services Tool(Средства служб удаленных рабочих столов)	Добавляет вкладку Профиль служб удаленных рабочих столов в свойства объекта пользователя ADUC и устанавливает оснастку ММС «Удаленные рабочие столы» для администрирования RDP-сервера (tsmmc.msc).

3) Нажать кнопку «ОК».

10.7.11. Инструменты командной строки

Основные инструменты командной строки представлены в таблице 55.

Т а б л и ц а 55 – Основные инструменты

Утилита	Описание
`samba-tool`	Основная утилита управления Samba
`wbinfo`	Позволяет получить информацию от демона winbindd
`net`	Инструмент администрирования Samba и удаленных серверов CIFS
`adcli`	Инструмент для выполнения действий в домене Active Directory
`ldapsearch`	Утилита для поиска информации в LDAP
`testparm`	Проверка корректности содержимого основного файла конфигурации Samba – `/etc/samba/smb.conf`

10.7.11.1. Команда `samba-tool`

Для управления Samba AD DC в состав пакета Samba входит инструмент командной строки `samba-tool` (таблица 56).

Т а б л и ц а 56 – Основные команды `samba-tool`

Команда	Описание
`computer`	Управление учетными записями компьютеров
`contact`	Управление контактами
`dbcheck`	Проверка локальной базы данных AD на наличие ошибок
`delegation`	Управление делегированием
`dns`	Управление параметрами доменной службы DNS
`domain`	Управление параметрами домена
`drs`	Управление службой репликации каталогов (Directory Replication Services, DRS)

Окончание таблицы 56

Команда	Описание
`dsacl`	Управление групповыми политиками
`forest`	Управление ролями (Flexible Single Master Operations, FSMO)
`fsmo`	Управление конфигурацией леса
`gpo`	Управление списками контроля доступа DS
`group`	Управление группами
`ldapcmp`	Сравнение двух баз данных ldap
`ntacl`	Вывод списка процессов
`processes`	Управление списками контроля доступа ACL
`ou`	Управление организационными подразделениями (OU)
`rodc`	Управление контроллером домена (Read-Only Domain Controller, RODC)
`schema`	Управление и запрос схемы
`sites`	Управление сайтами
`spn`	Управление службой принципалов (Service Principal Name, SPN)
`testparm`	Проверка конфигурационного файла на корректность синтаксиса
`time`	Получение показаний текущего времени сервера
`user`	Управление пользователями
`visualize`	Графическое представление состояния сети Samba

Получить дополнительную информацию можно на справочной странице `samba-tool` (`man samba-tool`).

Пример получения дополнительной информации о подкоманде:

```
$ samba-tool fsmo –help
```

10.7.11.2. Команда `wbinfo`

Команда `wbinfo` создает запросы и возвращает информацию к (от) демона winbindd.

Параметры команды `wbinfo` представленны в таблице 57.

Таблица 57 – Параметры команды wbinfo

Параметр	Описание	Пример
-a| --authenticate username %password	Попытаться аутентифицировать пользователя через winbindd Проверяет два метода аутентификации: plaintext password (применяется при входе пользователя в систему локально), challenge/response password (использует NTLM или Kerberos).	$ wbinfo -a TEST\\ivanov Enter TEST\ivanov's password: plaintext password authentication succeeded Enter TEST\ivanov's password: challenge/response password authentication succeeded
--allocate-gid	Получить новый GID из idmap	
--allocate-uid	Получить новый UID из idmap	
--all-domains	Вывести список всех доменов (доверенных и собственный)	$ wbinfo --all-domains BUILTIN TEST EXAMPLE
-c| --change-secret	Изменить пароль доверительной учетной записи. Может использоваться вместе с доменом для изменения паролей учетных записей междоменного доверия.	
--ccache-save <имя_пользователя>%<пароль>	Сохранить имя пользователя и пароль для ccache	
--change-user-password <имя_пользователя>	Изменить пароль пользователя (будет запрошен старый и новый пароль)	
--dc-info <домен>	Вывести текущий контроллер домена для домена	$ wbinfo --dc-info TEST dc1.test.alt (192.168.0.122)
--domain <домен>	Определяет домен, в котором будут выполняться любые указанные операции	
-D|--domain-info <домен>	Показать информацию об указанном домене	$ wbinfo -D TEST Name : TEST Alt_Name : test.alt SID : S-1-5-21-578923263-1107570656-1287136478 Active Directory : Yes Native : Yes Primary : Yes
--dsgetdcname <домен>	Найти DC для домена	$ wbinfo --dsgetdcname TEST \\dc1.test.alt \\192.168.0.122 1 d75c7b83-9472-4646-adb2-52b3d6968eb6 test.alt test.alt 0xe00013fd Default-First-Site-Name Default-First-Site-Name
--gid-info <gid>	Получить информацию о группе по gid	$ wbinfo --gid-info 10000 domain admins:*:10000:

Продолжение таблицы 57

Параметр	Описание	Пример
--group-info <группа>	Получить информацию о группе по имени группы	$ wbinfo --group-info "TEST\\domain admins" domain admins:*:10000:
-g|--domain-groups	Вывести список доменных групп	$ wbinfo -g … TEST\domain admins TEST\domain users TEST\domain guests TEST\domain computers …
--get-auth-user	Эта функция была перенесена в утилиту net	
--getdcname <домен>	Вывести имя контроллера домена для указанного домена	$ wbinfo --getdcname TEST DC1
-G|--gid-to-sid <gid>	Преобразовать идентификатор группы UNIX в SID Windows NT. Если указанный gid не относится к диапазону gid idmap, операция завершится ошибкой.	$ wbinfo -G 10000 S-1-5-21-578923263-1107570656-1287136478-512
-i|--user-info <имя_пользователя>	Вывести информацию о пользователе	$ wbinfo -i TEST\\ivanov ivanov:*:10000:10001:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash
-I|--WINS-by-ip ip	Вывести NetBIOS-имя, связанное с IP-адресом	$ wbinfo -I 192.168.0.135 192.168.0.135 WORK135
-K|--krb5auth <имя_пользователя>%<пароль>	Попытаться аутентифицировать пользователя через Kerberos	$ wbinfo -K TEST\\ivanov Enter TEST\ivanov's password: plaintext kerberos password authentication for [TEST\ivanov] succeeded (requesting cctype: FILE)
--krb5ccname KRB5CCNAME	Запросить определенный тип кэша учетных данных Kerberos, используемый для аутентификации	
--lanman	Использовать криптографию Lanman для аутентификации пользователей	
--logoff	Выйти из системы	
--logoff-uid UID	Определяет идентификатор пользователя, используемый во время запроса на выход из системы	
--logoff-user <имя_пользователя>	Определяет имя пользователя, используемое во время запроса на выход из системы	
--lookup-sids SID1,SID2...	Поиск SID	$ wbinfo --lookup-sids S-1-5-21-578923263-1107570656-1287136478-512 S-1-5-21-578923263-1107570656-1287136478-512 -> <none>\Domain Admins 2
-m|--trusted-domains	Вывести список доверенных доменов	$ wbinfo --trusted-domains BUILTIN TEST EXAMPLE

Продолжение таблицы 57

Параметр	Описание	Пример
-n|--name-to-sid <имя>	Вывести SID, связанный с указанным именем. Если домен не указан, используется домен, указанный в параметре workgroup smb.conf	$ wbinfo -n TEST\\ivanov S-1-5-21-578923263-1107570656-1287136478-1103 SID_USER (1)
-N|--WINS-by-name <name>	Вывести IP-адрес, связанный с именем NetBIOS, указанным в параметре name	$ wbinfo -N WORK135 192.168.0.135 WORK135
--ntlmv1	Использовать криптографию NTLMv1 для аутентификации пользователей	
--ntlmv2	Использовать криптографию NTLMv2 для аутентификации пользователей	
--online-status <домен>	Показать, поддерживает ли winbind в настоящее время активное соединение или нет. Если домен не указан, будет выведен статус текущего домена	$ wbinfo --online-status BUILTIN : active connection TEST : active connection
--own-domain	Вывести собственный домена	$ wbinfo --own-domainTEST
--pam-logon <имя_пользователя>%<пароль>	Попытаться аутентифицировать пользователя так же, как это сделал бы pam_winbind	$ wbinfo --pam-logon ivanov Enter ivanov's password: plaintext password authentication succeeded
-p|--ping	Проверяет запущен ли winbindd	$ wbinfo -p Ping to winbindd succeeded
-P|--ping-dc	Проверить безопасное соединение с контроллером домена	$ wbinfo -P checking the NETLOGON for domain[TEST] dc connection to "dc1.test.alt" succeeded
-r|--user-groups <имя_пользователя>	Получить список идентификаторов групп, к которым принадлежит пользователь. Доступно только при наличии пользователя на контроллере домена	$ wbinfo -r ivanov 10001 10003
-R|--lookup-rids rid1, rid2, rid3..	Преобразовать RID в имена	
--remove-gid-mapping GID,SID	Удалить существующее сопоставление GID и SID из базы данных	
--remove-uid-mapping UID,SID	Удалить существующее сопоставление UID и SID из базы данных	
-s|--sid-to-name sid	Преобразовать SID в имя	$ wbinfo -s S-1-5-21-578923263-1107570656-1287136478-1103 TEST\ivanov 1
--separator	Вывести активный разделитель winbind	$ wbinfo --separator \

Продолжение таблицы 57

Параметр	Описание	Пример
--sequence	Команда устарела, вместо нее следует использовать параметр --online-status	
--set-auth-user <имя_пользователя>%<пароль>	Эта функция была перенесена в утилиту net	
--set-gid-mapping GID,SID	Создать сопоставление GID и SID в базе данных	
--set-uid-mapping UID,SID	Создать сопоставление UID и SID в базе данных	
-S|--sid-to-uid sid	Преобразовать SID в идентификатор пользователя	$ wbinfo -S S-1-5-21-578923263-1107570656-1287136478-1103 10000
--sid-aliases sid	Получить псевдонимы SID для заданного SID	
--sid-to-fullname sid	Преобразовать SID в полное имя пользователя (ДОМЕН\имя пользователя)	$ wbinfo --sid-to-fullname S-1-5-21-578923263-1107570656-1287136478-1103 TEST\Иван Иванов 1
--sids-to-unix-ids sid1,sid2,sid3...	Преобразовать SID в Unix ID	$ wbinfo --sids-to-unix-ids S-1-5-21-578923263-1107570656-1287136478-1103 S-1-5-21-578923263-1107570656-1287136478-1103 -> uid 10000
-t|--check-secret	Проверить, что доверительная учетная запись рабочей станции, созданная при добавлении сервера Samba в домен Windows NT, работает. Может использоваться вместе с доменом для проверки учетных записей междоменного доверия	
-u|--domain-users	Вывести список доменных пользователей	$ wbinfo -u administrator krbtgt ivanov guest
--uid-info uid	Получить информацию о пользователе по идентификатору	$ wbinfo --uid-info 10000 ivanov:*:10000:10001:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash
--usage	Вывести краткую справку о программе	
--user-domgroups sid	Вывести группы пользователей домена	$ wbinfo --user-domgroups S-1-5-21-578923263-1107570656-1287136478-1103 S-1-5-21-578923263-1107570656-1287136478-1103 S-1-5-21-578923263-1107570656-1287136478-513

Окончание таблицы 57

Параметр	Описание	Пример
`--user-sidinfo sid`	Получить информацию о пользователе по sid	`$ wbinfo --user-sidinfo S-1-5-21-578923263-1107570656-1287136478-1103` `ivanov:*:10000:10001:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash`

`--user-sids sid`	Получить SID групп пользователя	`$ wbinfo --user-sids S-1-5-21-578923263-1107570656-1287136478-1103`
		`S-1-5-21-578923263-1107570656-1287136478-1103`
		`S-1-5-21-578923263-1107570656-1287136478-513`
		`S-1-5-32-545`

`-U|--uid-to-sid uid`	Преобразовать идентификатор пользователя UNIX в SID	`$ wbinfo -U 10000` `S-1-5-21-578923263-1107570656-1287136478-1103`
`-Y|--sid-to-gid sid`	Преобразовать SID в идентификатор группы UNIX	`$ wbinfo -Y S-1-5-21-578923263-1107570656-1287136478-513` `10001`

10.7.11.3. Команда `net`

`net` – инструмент администрирования Samba и удаленных серверов CIFS.

Синтаксис:

`net <протокол> <функция> <дополнительные_параметры> <параметры_цели>`

где `<протокол>` – протокол, используемый при выполнении команды. Возможные значения: `ads` (Active Directory), `rap` (Win9x/NT3) или `rpc` (WindowsNT4/2000/2003/2008/2012). Если протокол не указан, `net` пытается определить его автоматически.

Параметры команды net представлены в таблице 58.

Таблица 58 – Параметры команды `net`

Команда	Описание
`info`	Вывод информации о домене
`join`	Присоединение машины к домену
`testjoin`	Проверка, действителен ли пароль учетной записи компьютера
`leave`	Удалить локальную машину из домена AD
`status`	Вывод информации об учетной записи компьютера
`user`	Список/изменение пользователей
`group`	Список/изменение групп
`dns`	Выполнить динамическое обновление DNS

Окончание таблицы 58

Команда	Описание
`password`	Изменить пароль пользователей
`changetrustpw`	Изменить пароль доверительной учетной записи
`printer`	Список/изменение записей принтера
`search`	Выполнить поиск LDAP с использованием фильтра
`dn`	Выполнить поиск LDAP по DN
`sid`	Выполнить поиск LDAP по SID
`workgroup`	Показать имя рабочей группы
`lookup`	Найти контроллер домена AD с помощью поиска CLDAP
`keytab`	Управление локальным файлом keytab
`spnset`	Управление именами участников-служб (SPN)
`gpo`	Управление объектами групповой политики
`kerberos`	Управление keytab Kerberos
`enctypes`	Список/изменение enctypes

Получить дополнительную информацию можно на справочной странице `net`.

Пример получения дополнительной информации о подкоманде:

```
# net time --help
```

Получение информации о домене:

```
# net ads info
LDAP server: 192.168.0.132
LDAP server name: dc1.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
LDAP port: 389
Server time: Чт, 08 июн 2023 11:48:01 EET
KDC server: 192.168.0.132
Server time offset: -171
Last machine account password change: Вт, 16 мая 2023 09:26:46 EET
```

Получение информации об учетной записи компьютера:

```
# net ads status -U administrator
```

10.7.11.4. Команда `adcli`

`adcli` – инструмент для выполнения действий в домене Active Directory. Основные команды `adcli` представлены в таблице 59.

Таблица 59 – Основные команды `adcli`

Команда	Описание
`info домен`	Вывести информацию о домене
`join домен`	Присоединить данную машину к домену (создает учетную запись компьютера в домене и настраивает keytab для этой машины. Не настраивает службу аутентификации, например, sssd).
`update`	Обновляет пароль учетной записи компьютера на контроллере домена для локальной машины, записывает новые ключи в keytab и удаляет старые ключи
`testjoin`	Проверить, действителен ли пароль учетной записи компьютера
`create-user [--domain=домен] пользователь`	Создать учетную запись пользователя
`delete-user [--domain=домен] пользователь`	Удалить учетную запись пользователя
`passwd-user [--domain=домен] пользователь`	Установить (повторно) пароль пользователя
`create-group [--domain=домен] группа`	Создать группу
`delete-group [--domain=домен] группа`	Удалить группу
`add-member [--domain=домен] группа пользователь или компьютер…`	Добавить пользователей в группу
`remove-member [--domain=домен] группа пользователь…`	Удалить пользователей из группы
`preset-computer [--domain=домен] компьютер…`	Предустановить учетные записи компьютеров (предварительно создает одну или несколько учетных записей компьютеров в домене, чтобы позже компьютеры могли использовать их при присоединении к домену. При этом, машины могут присоединяться с помощью одноразового пароля или автоматически без пароля).
`reset-computer [--domain=домен] компьютер`	Сбросить учетную запись компьютера (если соответствующая машина присоединена к домену, ее членство будет нарушено).
`delete-computer [--domain=домен] компьютер`	Удалить учетную запись компьютера
`show-computer [--domain=домен] компьютер`	Показать атрибуты учетной записи компьютера, хранящиеся в AD
`create-msa [--domain=домен]`	Создать управляемую учетную запись службы (MSA) в заданном домене AD (это бывает нужно, если компьютер не должен присоединяться к домену Active Directory, но к нему необходим LDAP доступ)

Получить дополнительную информацию можно на справочной странице `adcli`.

Пример получения дополнительной информации о подкоманде:

```
# adcli testjoin --help
```

Получение информации о домене:

```
# adcli info test.alt
```

```
[domain]
domain-name = test.alt
domain-short = TEST
domain-forest = test.alt
domain-controller = dc1.test.alt
domain-controller-site = Default-First-Site-Name
domain-controller-flags = pdc gc ldap ds kdc timeserv closest writable
good-timeserv full-secret
domain-controller-usable = yes
domain-controllers = dc1.test.alt dc2.test.alt
[computer]
computer-site = Default-First-Site-Name
```

Показать атрибуты учетной записи компьютера:

```
# adcli show-computer -D test.alt win2012
```

```
Password for Administrator@TEST.ALT:
sAMAccountName:
 WIN2012$
userPrincipalName:
 - not set -
msDS-KeyVersionNumber:
 1
msDS-supportedEncryptionTypes:
 28
dNSHostName:
 win2012.test.alt
servicePrincipalName:
 HOST/win2012.test.alt
 RestrictedKrbHost/win2012.test.alt
 HOST/WIN2012
 RestrictedKrbHost/WIN2012
 Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/win2012.test.alt
operatingSystem:
 Windows Server 2012 R2 Standard
operatingSystemVersion:
 6.3 (9600)
operatingSystemServicePack:
 - not set -
pwdLastSet:
 133294743593838200
userAccountControl:
 4096
description:
 - not set –
```

Создать группу `testldap` в подразделении OU:

```
# adcli create-group -D test.alt -O OU=OU,dc=test,dc=alt testldap
Password for Administrator@TEST.ALT
```

10.7.11.5. Утилита ldapsearch

ldapsearch – утилита для поиска информации в LDAP.

Синтаксис:

`ldapsearch <параметры> <фильтр> <атрибуты>`

ldapsearch открывает соединение с сервером LDAP, подключается к нему и выполняет поиск с помощью фильтра.

Если утилита ldapsearch найдет одну или несколько записей, то значения указанных атрибутов этих записей будут переданы в стандартный поток вывода. Если в этом списке указан знак *, возвращаются все пользовательские атрибуты. Если в этом списке указан знак +, возвращаются все операционные атрибуты. Если атрибуты не указаны, то возвращаются все пользовательские атрибуты.

Если утилита `ldapsearch` найдет одну или несколько записей, то значения указанных атрибутов этих записей будут переданы в стандартный поток вывода. Если атрибуты не указаны, то возвращаются все атрибуты.

Результаты поиска отображаются в виде расширенной версии LDIF. Формат вывода контролируется с помощью параметра `-L`.

Параметры команды `ldapsearch` представлены в таблице 60.

Таблица 60 – Параметры команды `ldapsearch`

Параметр	Описание
Параметры поиска	
`-a {never|always|search|find}`	Задает способ преобразования псевдонимов. Может принимать значения: never (по умолчанию), always, search или find, указывающие, соответственно, что псевдонимы не преобразуются, преобразуются всегда, преобразуются при поиске, либо преобразуются только при определении базового объекта для поиска
`-A`	Получить только атрибуты (без значений)
`-b basedn`	Позволяет переопределить заданную по умолчанию начальную точку поиска
`-c`	Режим продолжения операции (не останавливать поиск при ошибках)
`-E [!]ext [=extparam]`	Указывает расширения поиска. Знак «!» обозначает критичность расширения. Общие расширения: - `[!]domainScope` (диапазон домена); - `!dontUseCopy`; - `[!]mv=<filter>` (RFC 3876 фильтр совпавших значений); - `[!]pr=<size>[/prompt|noprompt]` (RFC 2696 постраничный вывод результатов/запрос вывода);

Продолжение таблицы 60

Параметр	Описание
	- [!]sss=[-]<attr[:OID]>[/[-]<attr[:OID]>...] (RFC 2891 сортировка на стороне сервера); - [!]subentries[=true|false] (RFC 3672 подзаписи); - [!]sync=ro[/<cookie>] (RFC 4533 LDAP Sync refreshOnly); - [!]sync=rp[/<cookie>][/<slimit>] (LDAP Sync refreshAndPersist); - [!]vlv=<before>/<after>(/<offset>/<count>|:<value>) (ldapv3-vlv-09 вид виртуального списка); - [!]deref=derefAttr:attr[,...][;derefAttr:attr[,...][;...]]; - [!]<oid>[=:<b64value>] (общий контроль; нет обработки ответа)
-f file	Считать серию строк из файла file и выполнить по одному поиску LDAP для каждой строки. В этом случае заданный в командной строке фильтр filter интерпретируется как шаблон, в котором первое и только первое вхождение %s заменяется строкой из файла file. Любые другие вхождения символа % в шаблоне будут рассматриваться как ошибка. Если требуется, чтобы в поисковом фильтре присутствовал символ «%», он должен быть закодирован как \25 (смотрите RFC 4515). Если в качестве значения file указан символ «-», то строки считываются со стандартного ввода
-F prefix	URL-префикс для временных файлов (по умолчанию: file://path, где path либо /tmp/.private/<user>, либо значение, указанное в параметре -T)
-l limit	Ограничение на время поиска (в секундах). Значение 0 (ноль) или none означает, что ограничений нет. Значение max означает максимальное допустимое протоколом значение (целое число)
-L[LL]	Управление выводом результатов поиска в формате обмена данными LDAP (LDAP Data Interchange Format): - -L – вывести ответы в формате LDIFv1; - -LL – отключить вывод комментариев; - -LLL – отключить вывод версии LDIF
-M[M]	Включить элемент управления Manage DSA IT. -MM делает этот элемент управления критичным
-P {2|3}	Версия протокола LDAP (по умолчанию 3)
-s {base|one|sub|children}	Задает область поиска. Может принимать одно из следующих значений: base, one, sub (по умолчанию) или children, что означает поиск только по базовому объекту, на одном уровне, по всему поддереву и по дочерним записям соответственно
-S attr	Отсортировать возвращаемые записи по атрибуту attr. По умолчанию возвращаемые записи не сортируются. Если в качестве attr задана строка нулевой длины (""), записи сортируются по компонентам их уникального имени Distinguished Name. По умолчанию ldapsearch выводит записи по мере их получения. При использовании параметра -S все данные сначала получаются, потом сортируются, потом выводятся
-t[t]	При указании одного -t полученные непечатаемые значения записываются в набор временных файлов (полезно при работе со значениями, содержащими несимвольные данные, такими как jpegPhoto или audio). При указании второго -t все полученные значения записываются в файлы
-T path	Временные файлы записываются в указанный в path каталог (по умолчанию /tmp/.private/<user>)

Продолжение таблицы 60

Параметр	Описание
-u	Включить в вывод форму удобного для пользователя имени (User Friendly Name, UFN) уникального имени (Distinguished Name, DN)
-z limit	Ограничить количество возвращаемых в результате поиска записей значением limit. Значение 0 (ноль) или none означает, что ограничений нет. Значение max означает максимальное допустимое протоколом значение (целое число)
Общие параметры	
-d debuglevel	Установить уровень отладки LDAP
-D binddn	Использовать указанное в binddn уникальное имя Distinguished Name при подсоединении к каталогу LDAP. При SASL-подсоединениях сервер будет игнорировать это значение
-e [!]ext[=extparam]	Указывает общие расширения. Знак «!» обозначает критичность расширения. Общие расширения: - [!]assert=<filter> (RFC 4528; фильтр RFC 4515) - [!]authzid=<authzid> (RFC 4370; "dn:<dn>" или "u:<user>") - [!]chaining[=<resolveBehavior>[/<continuationBehavior>]] - [!]manageDSAit (RFC 3296) - [!]noop - ppolicy - [!]postread[=<attrs>] (RFC 4527; разделенный запятыми список атрибутов) - [!]preread[=<attrs>] (RFC 4527; разделенный запятыми список атрибутов) - [!]relax - [!]sessiontracking - abandon, cancel, ignore (сигнал SIGINT посылает abandon/cancel, либо в ответ на него посылается ignore; если расширение помечено как критичное, сигнал SIGINT не принимается; ненастоящие элементы управления
-h host	Сервер LDAP
-H URI	Указывает URI (возможно, несколько), ссылающийся на LDAP-сервер (серверы). В URI допускаются поля: протокол/хост/порт
-I	Использовать интерактивный режим SASL
-n	Демонстрируется, что будет сделано, но реальный поиск не выполняется. Используется для отладки совместно с параметром -v
-N	Не использовать обратное разрешение DNS для получения канонического имени хоста SASL
-O props	Параметры безопасности SASL
-o opt[=optparam]	Указывает опции общего назначения. Возможные опции: - nettimeout=<timeout> (в секундах, либо «none» или «max») - ldif-wrap=<width> (в символах, либо «no» для предотвращения переноса строк)
-p порт	Порт, на котором сервер LDAP принимает запросы. Номер порта по умолчанию – 389. Если номер порта не задан, и указан параметр -Z, то применяется номер порта LDAP SSL по умолчанию, равный 636

Окончание таблицы 60

Параметр	Описание
`-Q`	Использовать тихий режим SASL. Запросы не выводятся никогда
`-R realm`	Задает realm аутентификационного идентификатора для SASL. Форма realm зависит от того, какой механизм аутентификации в действительности используется
`-U authcid`	Идентификатор аутентификации SASL. Форма идентификатора зависит от того, какой механизм аутентификации в действительности используется
`-v`	Использовать тихий режим SASL. Запросы не выводятся никогда
`-V[V]`	Вывести информацию о версии. При указании -VV, после вывода информации о версии осуществляется выход. При указании -V, после вывода информации о версии выполняется поиск согласно заданным критериям
`-w passwd`	Использовать указанное значение passwd в качестве пароля для простой аутентификации
`-W`	Запрашивать ввод пароля для простой аутентификации (используется для того, чтобы не указывать пароль в командной строке)
`-x`	Использовать простую аутентификацию
`-X authzid`	Идентификатор авторизации SASL («dn:<dn>» или «u:<user>»)
`-y file`	Считать пароль из файла file. В качестве пароля используется все содержимое файла. Поэтому файл не должен содержать символа переноса строки
`-Y mech`	Задает механизм SASL, который будет использоваться для аутентификации. Если параметр не указан, программа выберет лучший из известных серверу механизмов
`-Z[Z]`	Запустить запрос TLS (`-ZZ` для запроса успешного ответа)

10.7.11.5.1. Фильтр

Фильтр должен быть указан в строковом формате фильтров. Если фильтр не указан, используется фильтр по умолчанию (objectClass=*).

Синтаксис LDAP-фильтра имеет вид:

```
<Атрибут><оператор сравнения><значение>
```

Вместо имени атрибута можно использовать его идентификатор (Attribute-Id). Тело фильтра должно быть заключено в скобки.

Примеры LDAP-фильтров представлены в таблице 61.

Таблица 61 – Примеры LDAP-фильтров

Запрос	LDAP фильтр
Все пользователи:	`(sAMAccountType=805306368)`
Отключенные (Disabled) пользователи:	`(&(sAMAccountType=805306368)` `(useraccountcontrol:1.2.840.113556.1.4.803:=2))`
Заблокированные (Locked) пользователи:	`(&(sAMAccountType=805306368)(badPwdCount>=4))`

Окончание таблицы 61

Запрос	LDAP фильтр
Пользователи, у которых в настройках указано «Пароль никогда не истекает»	(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=65536))
Пользователи которые не меняли пароль с 5 мая 2023 года	(&(objectCategory=person)(pwdLastSet<=133278047990000000))
Пользователи с незаполненным полем mail	(&(objectCategory=group)(!(mail=*)))
Пользователи, которые должны сменить пароль при следующем входе в систему	(&(sAMAccountType=805306368)(pwdLastSet=0))
Пользователи с ограниченным сроком действия учетной записи	(&(sAMAccountType=805306368)(accountExpires>=1)(accountExpires<=9223372036854775806))
Пользователи, созданные за определенный период (формат даты: YYYY MM DD HH mm ss.s Z)	(&(sAMAccountType=805306368)(whenCreated>=20230401000000.0Z<=20230701000000.0Z))
Все компьютеры	(objectCategory=computer)
Все контроллеры домена	(&(objectCategory=computer)(userAccountControl:1.2.840.113556.1.4.803:=8192))
Контроллеры домена, доступные только для чтения	(&(objectCategory=computer)(userAccountControl:1.2.840.113556.1.4.803:=67108864))
Группы в которых нет пользователей	(&(objectCategory=group)(!(member=*)))
Группы с ключевым словом admin в имени	(&(objectCategory=group)(samaccountname=*admin*))
Все группы безопасности (Security)	(&(objectCategory=group)(groupType:1.2.840.113556.1.4.803:=2147483648))
Все члены группы Sales (без учета вложенности)	(memberOf=CN=Sales,CN=Users,DC=test,DC=alt)
Все члены группы Sales (с учетом вложенности)	(memberOf:1.2.840.113556.1.4.1941:=CN=Sales,CN=Users,DC=test,DC=alt)
Все группы, в которые входит пользователь testldap	(&(objectCategory=group)(member=CN=testldap,CN=Users,DC=test,DC=alt)))
Все подразделения (OU)	(objectCategory=organizationalUnit)
Все объекты групповой политики	(objectCategory=groupPolicyContainer)
Все отношения доверия	(objectClass=trustedDomain)
Объекты, связанные с ролями FSMO	(fsMORoleOwner=*)
PDC Emulator	(&(objectClass=domainDNS)(fSMORoleOwner=*))
RID Master	(&(objectClass=rIDManager)(fSMORoleOwner=*))
Объект AD с определенным SID	(objectSID=S-1-5-21-1723588197-2340999690-1379671080-1105)

10.7.11.5.2. Формат вывода

Если найдена одна или несколько записей, то каждая запись передается в поток вывода в следующем формате:

```
Отличительное имя (DN)
имя_атрибута: значение
имя_атрибута: значение
имя_атрибута: значение
…
```

Записи разделяются пустыми строками.

Если задан параметр `-t` вместо реальных значений атрибутов будут выводиться URI временных файлов, в которые эти значения помещаются. Если задан параметр `-A`, то будут выводиться только имена атрибутов.

Примечания:

1. Значение атрибута записывается в 7-битной кодировке ASCII и отделяется от его имени символом «:». Значения, не подходящие под эту кодировку, записываются в кодировке base64 и отделяются от имени атрибута символами «::»:

```
имя_атрибута:: base64_значение_атрибута
```

Например:

```
dn::Q0490JfQsNC50YbQtdCy0LAg0J7Qu9GM0LPQsCxDTj1Vc2VycyxEQz10ZXN0LERDPWFsdA==cn:
: 0JfQsNC50YbQtdCy0LAg0J7Qu9GM0LPQsA==
…
$  echo "0JfQsNC50YbQtdCy0LAg0J7Qu9GM0LPQsA==" | base64 -d
Зайцева Ольга
```

2. Чтобы отобразить строки в кодировке base64 можно использовать следующую команду:

```
$  ldapsearch  -LLL  -D  testldap@test.alt  -x  -W  |  perl  -MMIME::Base64  -
MEncode=decode   -n   -00   -e   's/\n   +//g;s/(?<=::   )(\S+)/decode("UTF-
8",decode_base64($1))/eg;print'
```

10.7.11.5.3. Примеры

Вывести всех пользователей, фамилия которых начинается с буквы «К»:

```
$ ldapsearch -LLL -H ldap://192.168.0.122:389 \
-D testldap@test.alt -b "dc=test,dc=alt" \
-x -W "(&(sAMAccountName=*)(sn=К*))" cn sn
```

где:

- `-H ldap://192.168.0.122:389` – сервер LDAP;
- `-D testldap@test.alt` – пользователь с правом чтения в каталоге LDAP;
- `-b "dc=test,dc=alt"` – контейнер AD, в котором будет выполняться поиск;
- `-x` – использовать простую аутентификацию;
- `-W` – спросить пароль;

- «(&(sAMAccountName=*)(sn=К*))» – выражение, по которому будут отфильтрованы результаты;
- cn sn – поля, которые необходимо вывести.

Параметры по умолчанию можно задать в файле /etc/openldap/ldap.conf, например:

```
BASE    dc=test,dc=alt
URI     ldap://dc1.test.alt
```

Команда с использованием базы поиска и URI по умолчанию:

```
$ ldapsearch -LLL -D testldap@test.alt \
-x -W "(&(sAMAccountName=*)(sn=К*))" cn sn
```

Вывести фамилию и электронную почту всех пользователей, из подразделения OU, у которых непустое поле mail:

```
$ ldapsearch -LLL -H ldap://192.168.0.122:389 \
-D testldap@test.alt -b "ou=OU,dc=test,dc=alt" -s one \
-x -W "(&(sAMAccountName=*)(mail=К*))" sn mail
```

В данном примере не будут выведены записи только из подразделения OU, но не из его дочерних подразделений.

Считать последовательность строк из файла new.filter и выполнить функцию поиска LDAP для каждой строки:

```
$ ldapsearch -H ldap://192.168.0.122:389 \ -D testldap@test.alt -b "dc=test,dc=alt" -x -W -f new.filter "(samaccountname=%s)" cn
```

Содержимое файла new.filter:

```
z*
ivanov
k*
*k
```

Команда выполняет поиск по поддереву для каждого фильтра, начиная с samaccountname=z*. Когда этот поиск завершается, начинается поиск для фильтра cn=ivanov и т. д.

Пример вывода вышеуказанной команды с параметром `-n`:

```
 LDAPv3
# base <dc=test,dc=alt> with scope subtree
# filter pattern: (samaccountname=%s)
# requesting: dn
#

#
# filter: (samaccountname=z*)
#

#
# filter: (samaccountname=ivanov)
#

#
# filter: (samaccountname=k*)
#

#
# filter: (samaccountname=*k)
#
```

10.7.11.6. Команда `sssctl`

`sssctl` – это инструмент командной строки, который предоставляет унифицированный способ получения информации о состоянии Security System Services Daemon (SSSD).

Утилиту `sssctl` можно использовать для сбора информации:

- состоянии домена;

- аутентификации пользователя;

- доступа пользователей к клиентам определенного домена;

- информация о кэшированном содержимом.

С помощью утилиты `sssctl` можно:

- управлять кэшем SSSD;

- управлять журналами;

- проверить конфигурационные файлы.

Основные команды `sssctl` представлены в таблице 62.

Таблица 62 – Основные команды `sssctl`

Команда	Описание
Статус SSSD	
`domain-list`	Вывести список доступных доменов
`domain-status` `домен`	Вывести информацию о домене
`user-checks` `пользователь`	Вывести информацию о пользователе и проверить аутентификацию
`access-report` `домен`	Создание отчета о правилах управления доступом для домена, которые применяются к клиентскому компьютеру (работает только для домена FreeIPA)
Информация о кэшированном содержимом	
`user-show` `пользователь`	Информация о кэше пользователя
`group-show` `группа`	Информация о кэше группы
`netgroup-show` `группа`	Информация о кэше сетевой группы
Инструменты для работы с локальными данными	
`client-data-backup`	Резервное копирование локальных данных
`client-data-restore`	Восстановление локальных данных из резервной копии
`cache-remove`	Резервное копирование локальных данных и удаление кэшированного содержимого
`cache-upgrade`	Выполнить обновление кеша
`cache-expire`	Сделать недействительными кешированные объекты
`cache-index` `действие`	Управление индексами кеша
Инструменты для управления журналированием	
`logs-remove`	Удалить существующие файлы журналов SSSD
`logs-fetch файл`	Архивировать файлы журналов SSSD в tarball
`debug-level` `[уровень]`	Изменить или вывести уровень журналирования SSSD
`analyze`	Анализ зарегистрированных данных
Инструменты для проверки файлов конфигурации	
`config-check`	Выполнить статический анализ конфигурации SSSD
`cert-show` `сертификат`	Вывести информацию о сертификате
`cert-map` `сертификат`	Показать пользователей, привязанных к сертификату

Получить дополнительную информацию можно на справочной странице `sssctl`.

Пример получения дополнительной информации о подкоманде:

```
# sssctl user-show --usage
```

или

```
# sssctl user-show --help
```

Получение информации о домене:

```
# sssctl domain-status TEST.ALT
```

```
Online status: Online

Active servers:
AD Global Catalog: dc1.test.alt
AD Domain Controller: dc1.test.alt

Discovered AD Global Catalog servers:
- dc1.test.alt
Discovered AD Domain Controller servers:
- dc1.test.alt
```

Показать информацию о кэше пользователя:

```
# sssctl user-show kim
```

```
Name: kim
Cache entry creation date: 12/28/22 13:39:46
Cache entry last update time: 06/19/23 09:55:29
Cache entry expiration time: Expired
Initgroups expiration time: Expired
Cached in InfoPipe: No
```

Создать группу `testldap` в подразделении OU:

```
# sssctl user-checks kim
```

```
user: kim
action: acct
service: system-auth
SSSD nss user lookup result:
 - user name: kim
 - user id: 1187401107
 - group id: 1187400513
 - gecos: Олег Ким
 - home directory: /home/TEST.ALT/kim
 - shell: /bin/bash
SSSD InfoPipe user lookup result:
 - name: kim
 - uidNumber: 1187401107
 - gidNumber: 1187400513
 - gecos: Олег Ким
 - homeDirectory: not set
 - loginShell: not set
testing pam_acct_mgmt
pam_acct_mgmt: Success
PAM Environment:
 - no env –
```

10.7.11.7. Команда `testparm`

С помощью команды `testparm` можно проверить содержимое файла конфигурации `/etc/samba/smb.conf`.

Пример проверки настройки Samba:

```
$ testparm

Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed

Server role: ROLE_ACTIVE_DIRECTORY_DC

Press enter to see a dump of your service definitions

# Global parameters
[global]
    dns forwarder = 8.8.8.8
    ldap server require strong auth = No
    passdb backend = samba_dsdb
    realm = TEST.ALT
    server role = active directory domain controller
    workgroup = TEST
    rpc_server:tcpip = no
    rpc_daemon:spoolssd = embedded
    rpc_server:spoolss = embedded
    rpc_server:winreg = embedded
    rpc_server:ntsvcs = embedded
    rpc_server:eventlog = embedded
    rpc_server:srvsvc = embedded
    rpc_server:svcctl = embedded
    rpc_server:default = external
    winbindd:use external pipes = true
    idmap_ldb:use rfc2307 = yes
    idmap config * : backend = tdb
    map archive = No
    vfs objects = dfs_samba4 acl_xattr

[dfs]
    msdfs root = Yes
    path = /media/dfsroot

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

[netlogon]
    path = /var/lib/samba/sysvol/test.alt/scripts
    read only = No

[free]
    guest ok = Yes
    path = /mnt/win/free
    read only = N
```

10.7.12. Конфигурационные файлы

`/etc/samba/smb.conf` – файл конфигурации Samba.

`/etc/krb5.conf` – файл конфигурации Kerberos.

10.7.12.1. Файл `sssd.conf`

`/etc/sssd/sssd.conf` – файл конфигурации SSSD.

Для работы с Active Directory в SSSD имеется специальный AD-провайдер `sssd-ad`.

Минимальный конфигурационный файл (`/etc/sssd/sssd.conf`) для `sssd-ad`:

```
[sssd]
config_file_version = 2
services = nss, pam

# Managed by system facility command:
## control sssd-drop-privileges unprivileged|privileged|default
user = _sssd

# SSSD will not start if you do not configure any domains.

domains = TEST.ALT
[nss]

[pam]
[domain/TEST.ALT]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad
default_shell = /bin/bash
fallback_homedir = /home/%d/%u
debug_level = 0
;cache_credentials = true
ad_gpo_ignore_unreadable = true
ad_gpo_access_control = permissive
ad_update_samba_machine_account_password = true
```

Получить подробную информацию можно на справочной странице `man sssd.conf`.

10.7.12.2. Файл `resolv.conf`

`/etc/resolv.conf` – файл конфигурации ресолвера (механизма преобразования имен хостов в адреса IP).

Файл конфигурации ресолвера (resolver) содержит информацию, которая считывается функциями разрешения имен при первом их вызове процессом.

Файл разработан в удобочитаемом формате, и содержит список ключевых слов со значениями, которые предоставляют различного рода информацию для функций разрешения имен. Файл настройки считается надежным источником информации DNS (например, информация об AD-бите DNSSEC будет возвращаться в неизменном виде из этого источника).

Если этот файл не существует, то будет опрашиваться только служба имен на локальной машине; доменное имя определяется из имени узла, а список поиска будет содержать это доменное имя.

Обычно в файле `/etc/resolv.conf` указан как минимум 1 сервер имен, на который будут перенаправляться все DNS запросы:

```
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
nameserver 192.168.197.241
```

ВАЖНО

Файл `/etc/resolv.conf` не должен редактироваться. Его автоматически генерирует `resolvconf`. Редактировать можно файл `/etc/net/ifaces/<interface>/resolv.conf`.

Поддерживаются следующие параметры настройки:

1) `nameserver` (IP-адрес сервера имен)

Интернет-адрес сервера имен, на который надо переправлять все запросы, либо адрес IPv4 (в точечной нотации), либо адрес IPv6 в нотации с двоеточием (и, возможно, с точками) в соответствии с RFC 2373. Может быть указано до `MAXNS` (в настоящее время 3) серверов имен, ключевое слово должно быть указано для каждого сервера. Если указано несколько серверов, библиотека распознавателя запрашивает их в указанном порядке. Если в файле нет строк `nameserver`, по умолчанию используется сервер имен на локальном компьютере. Используемый алгоритм заключается в том, чтобы попробовать обратиться к первому указанному серверу имен, и, если время ожидания запроса истекло,

попробовать обратиться к следующему серверу, и т. д. пока не будет исчерпан список серверов, а затем повторять попытки, пока не будет сделано максимальное количество повторных попыток;

2) options

Позволяют изменять некоторые внутренние переменные функций определения имен. Синтаксис:

options параметр …

где параметр может иметь следующие значения:

- attempts:n

  Задает количество попыток, которое преобразователь предпримет, отправляя запрос на свои серверы имен, прежде чем закончить работу и вернуть ошибку. По умолчанию используется RES_DFLRETRY (в настоящее время равно 2). Значение этого параметра скрыто, ограничено числом 5;

- debug

  Устанавливает RES_DEBUG в _res.options (эффективно, только если glibc был собран с поддержкой отладки);

- edns0 (начиная с glibc 2.6)

  Задает значение RES_USE_EDNSO в _res.options. Включает поддержку расширений DNS, описанных в RFC 2671;

- inet6

  Задает значение RES_USE_INET6 в _res.options. Это приводит к выполнению запроса AAAA перед запросом A внутри функции gethostbyname, и отображению ответов IPv4 в «туннелированной форме» IPv6, если записи AAAA не были найдены, но существует набор записей A. Начиная с glibc 2.25, эта опция устарела; приложения должны использовать getaddrinfo, а не gethostbyname;

- `ip6-bytestring` (с glibc 2.3.4 до glibc 2.24)

  Задает значение RES_USE_BSTRING в `_res.options`. Это приводит к поиску обратной записи IPv6, с использованием формата значимых битов, описанного в RFC 2673; если этот параметр не установлен (по умолчанию);
- `ndots:n`

  Задает минимальное количество точек, которые должны обязательно присутствовать в имени, переданном функции `res_query` (см. resolver(3)), прежде чем будет сделан первоначальный абсолютный запрос. По умолчанию `n` равно 1, поэтому если в имени есть точки, сначала имя пытаются разрешить как абсолютное, прежде чем добавлять к нему элементы из списка поиска. Значение этой опции скрыто и ограничено числом 15;
- `no-check-names`

  Задает значение RES_NOCHECKNAME в `_res.options`, что приводит к отключению в современном BIND проверки в поступающих именах узлов и почтовых именах недопустимых символов, таких как символы подчеркивания (_), не-ASCII или управляющие символы;
- `no-reload` (начиная с glibc 2.16)

  Задает значение RES_NORELOAD в `_res.options`. Эта опция отключает автоматическую перезагрузку измененного файла конфигурации;
- `no-tld-query` (начиная с glibc 2.14)

  Задает значение RES_NOTLDQUERY в `_res.options`. Этот параметр указывает `res_nsearch()` не пытаться разрешить неполное имя, как если бы оно было доменом верхнего уровня. Данный параметр может привести к проблемам, если в качестве TLD указано «localhost», а не localhost в одном или более элементах списка поиска.

Данный параметр не действует, если не установлен RES_DEFNAMES или RES_DNSRCH;

- `rotate`

  Задает значение RES_ROTATE в `_res.options`, что приводит к циклическому выбору указанных серверов имен. Без этой опции распознаватель всегда будет запрашивать первый сервер имен в списке и использовать последующий сервер имен только в случае сбоя первого. Эта опция позволяет распределить нагрузку между разными серверами имен;

- `single-request-reopen` (начиная с glibc 2.9)

  Задает RES_SNGLKUPREOP в `_res.options`. Для разрешения имен используется единый сокет для запросов A и AAAA. Некоторое оборудование ошибочно возвращает только один ответ. Когда это происходит, клиент продолжает ждать второго ответа.

  Указание этого параметра изменяет это поведение так, что если два запроса с одного порта не обрабатываются правильно, то сокет будет закрыт и открыт новый перед посылкой второго запроса;

- `single-request` (начиная с glibc 2.10)

  Задает значение RES_SNGLKUP в `_res.options`. По умолчанию `glibc`, начиная с версии 2.9, выполняет поиск по IPv4 и IPv6 параллельно.

  Некоторые приложения DNS-серверов не могут обработать такие запросы должным образом и делают паузу между ответами на запрос. Этот параметр отключает данное поведение, что заставляет `glibc` делать запросы IPv6 и IPv4 последовательно (за счет некоторого замедления процесса разрешения имени);

- `timeout:n`

  Задает промежуток времени, который функции определения имен будут ждать ответа от удаленного сервера имен перед тем как повторить запрос другому серверу имен.

Это время может не совпадать с общим временем, затраченным на любой вызов API-интерфейса преобразователя, и нет гарантии, что один вызов API-интерфейса преобразователя соответствует одному тайм-ауту. Измеряется в секундах, значение по умолчанию – RES_TIMEOUT (в настоящее время равно 5). Значение этой опции скрыто и ограничено числом 30;

- `trust-ad` (начиная с glibc 2.31)

  Задает значение RES_TRUSTAD в `_res.options`. Этот параметр управляет поведением бита AD распознавателя-заглушки. Если проверяющий преобразователь устанавливает в ответе бит AD, это означает, что данные в ответе были проверены в соответствии с протоколом DNSSEC. Чтобы полагаться на бит AD, локальная система должна доверять как распознавателю, проверяющему DNSSEC, так и сетевому пути к нему, поэтому требуется явное согласие. Если активна опция `trust-ad`, тупиковый распознаватель устанавливает бит AD в исходящих DNS-запросах (чтобы включить поддержку бита AD) и сохраняет бит AD в ответах. Без этой опции бит AD в запросах не устанавливается и всегда удаляется из ответов, прежде чем они будут возвращены приложению. Это означает, что приложения могут доверять биту AD в ответах, если параметр `trust-ad` установлен правильно.

  В glibc версии 2.30 и более ранних AD не устанавливается автоматически в запросах и без изменений передается приложениям в ответах;

- `use-vc` (начиная с glibc 2.14)

  Задает значение RES_USEVC в `_res.options`. Данный параметр включает принудительное использование TCP для запросов DNS;

- search (список поиска)

  По умолчанию список поиска содержит одну запись – имя локального домена. Он определяется по локальному имени хоста, возвращаемому функцией gethostname; локальным доменным именем считается все, что следует после первого знака «.». Если имя хоста не содержит «.», предполагается, что корневой домен является именем локального домена.

  Это поведение можно изменить, перечислив имена доменов, в которых нужно вести поиск, после ключевого слова search через пробел или символ табуляции. При разрешении запросов имен, в которых меньше точек чем указано в ndots (по умолчанию 1), будет использован каждый компонент пути поиска пока не будет найдено соответствующее имя. Для сред с несколькими субдоменами см. параметры ndots:n выше, чтобы избежать атак типа «человек посередине» и ненужного трафика для корневых DNS-серверов. Обратите внимание, что этот процесс может быть медленным и будет генерировать много сетевого трафика, если серверы для перечисленных доменов не являются локальными, и что время ожидания запросов истечет, если сервер для одного из доменов недоступен.

  При наличии нескольких директив search используется только список поиска из последнего экземпляра.

  Список поиска может содержать не более шести доменов и не может быть длиннее 256 символов. В glibc 2.25 и более ранних версиях список поиска мог содержать не более шести доменов и не мог быть длиннее 256 символов. Начиная с glibc 2.26 список поиска не ограничен.

  Директива domain – это устаревшее название директивы search, которая обрабатывает только одну запись в списке поиска;

- `sortlist`

  Позволяет сортировать адреса, возвращаемых функцией gethostbyname. Список сортировки задается в виде пар IP-адрес/сетевая маска. Маску сети указывать не обязательно, по умолчанию используется естественная маска сети. IP-адрес и маска сети разделяются косой чертой. В списке можно указывать до 10 пар.

  Пример:
  `sortlist 130.155.160.0/255.255.240.0 130.155.0.0`

Ключевое слово `search` системного файла `resolv.conf` можно переопределить для каждого процесса, задав для переменной среды LOCALDOMAIN список доменов поиска, разделенных пробелами.

Ключевое слово options системного файла `resolv.conf` можно переопределить для каждого процесса, задав для переменной среды RES_OPTIONS список параметров преобразователя, разделенных пробелами.

Любые изменения, внесенные вручную в файл конфигурации `/etc/resolv.conf`, обязательно будут перезаписаны при изменениях в сети или перезагрузке системы.

Ключевое слово и значение должны находиться в одной строке, и кроме того, строка должна начинаться с ключевого слова (например, `nameserver`). Значение следует за ключевым словом, разделенным пробелом.

Строки, начинающиеся с точки с запятой (;) или решетки (#), считаются комментариями.

`Resolvconf` – это платформа для обновления системной информации о серверах DNS. Он настраивается как посредник между программами, которые предоставляют эту информацию и программами, которые используют эту информацию.

Обновить файл `/etc/resolv.conf`, чтобы внести изменения в DNS:

```
# resolvconf -u
```

Пример файла `/etc/resolv.conf`:

```
search test.alt example.test
nameserver 192.168.0.122
nameserver 8.8.8.8
```

Запись search позволяет использовать в качестве адреса только хост-имя для компьютеров в домене `test.alt`. Например, чтобы обратиться системе `work.test.alt`, пользователь должен ввести в качестве адреса только хост-имя, `work`. Когда преобразователь пытается разрешить доменное имя, например, `work`, он сначала формирует полное доменное имя, используя имя домена `test.alt`, в `work.test.alt` и выполняет DNS-запрос, используя это полное доменное имя. Если это не удается, то преобразователь пробует следующий в очереди домен и запрашивает IP-адрес `work.example.test`.

При этом, когда преобразователь пытается разрешить доменное имя `work.ru`, он сначала запросит `work.ru` как абсолютное доменное имя. Если DNS не сможет разрешить его, то только тогда преобразователь объединит его с поисковым доменом, чтобы сформировать `work.ru.test.alt`, и повторит запрос.

Решение о том, выполняется ли первый запрос как абсолютное доменное имя или нет, полностью зависит от количества точек, присутствующих в доменном имени. По умолчанию доменное имя, содержащее по крайней мере 1 точку, заставит преобразователь запрашивать его дословно, не объединяя его с какими-либо поисковыми доменами. Количество точек для первого запроса абсолютного доменного имени настраивается в значении параметра `ndots`.

10.8. Примечания

10.8.1. Настройка беспарольного доступа по ssh

Генерация SSH-ключа (на DC1):

```
# ssh-keygen -t ed25519
```

На вопрос о файле для сохранения ключа нажать «Enter» (по умолчанию).

На вопрос о пароле к ключу также нажать «Enter» (не указывать пароль).

Скопировать публичную часть SSH-ключа на второй контроллер домена (DC2) для пользователя user:

```
# ssh-copy-id -i ~/.ssh/id_ed25519.pub user@dc2.test.alt
```

Проверка, что ключ был скопирован на DC2:

```
# ssh user@dc2.test.alt
[user@dc2 ~]$ su -
```

```
Password:
[root@dc2 ~]# cat /home/user/.ssh/authorized_keys >>.ssh/authorized_keys
[root@dc2 ~]# exit
выход
[user@dc2 ~]$ exit
выход
Connection to dc2 closed.
```

Теперь есть возможность удаленно выполнять команды на DC2 с привилегиями администратора.

10.8.2. Центр управления системой

Центр управления системой (ЦУС, альтератор) 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 состоит из независимых диалогов-модулей. Каждый модуль отвечает за настройку определенной функции или свойства системы.

Запустить ЦУС в графической среде можно следующими способами:

1) в графической среде MATE: «Система» → «Администрирование» → «Центр управления системой»;
2) в графической среде XFCE, KDE: «Меню запуска приложений» → «Настройки» → «Центр управления системой»;
3) из командной строки: командой acc.

Запуск ЦУС (рис. 411) требует административных прав, и, если запустить его от обычного пользователя, он запросит пароль администратора (root) (рис. 412).

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

Для запуска веб-ориентированного интерфейса, должен быть установлен пакет alterator-fbi:

```
# apt-get install alterator-fbi
```

И запущены сервисы `ahttpd` и `alteratord`:

```
# systemctl enable --now ahttpd
# systemctl enable --now alteratord
```

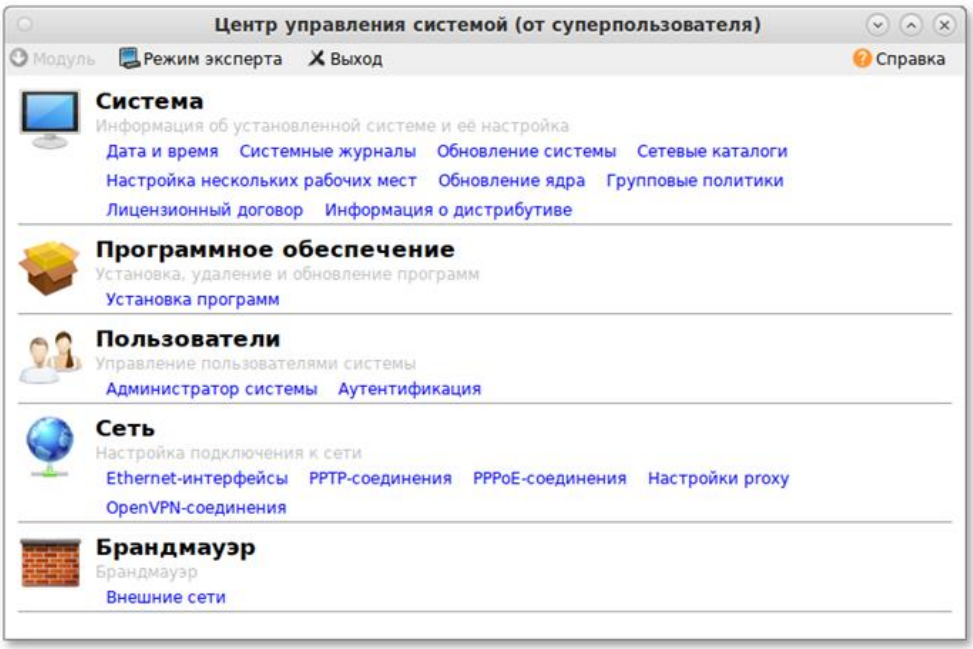


Рис. 411 – Центр управления системой

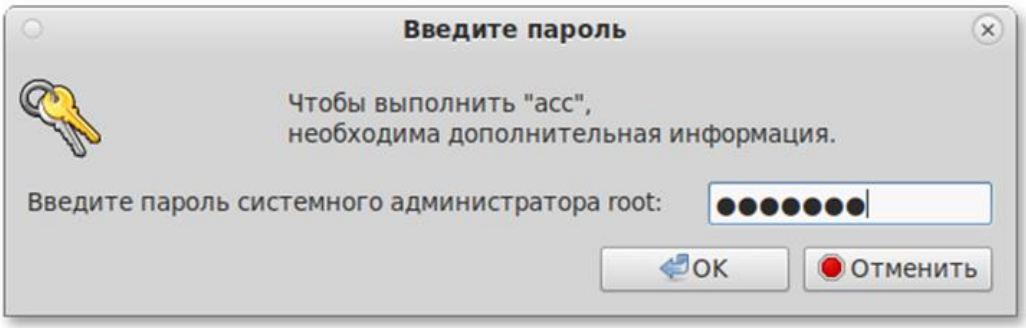


Рис. 412 – Запрос пароля администратора

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

При запуске центра управления системой необходимо ввести в соответствующие поля имя пользователя (root) и пароль пользователя (рис. 413).

После этого будут доступны все возможности ЦУС на той машине, к которой было произведено подключение через веб-интерфейс (рис. 414).

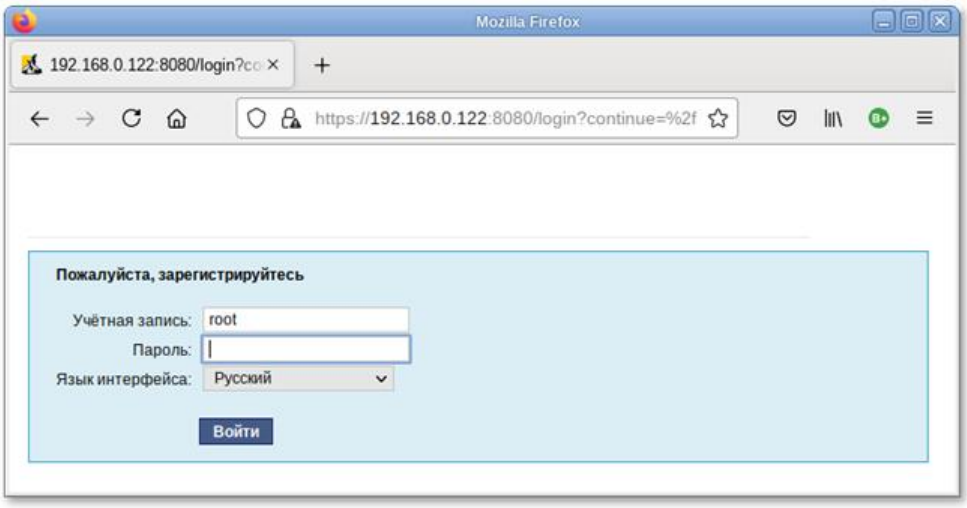


Рис. 413 – Работа с ЦУС из веб-браузера

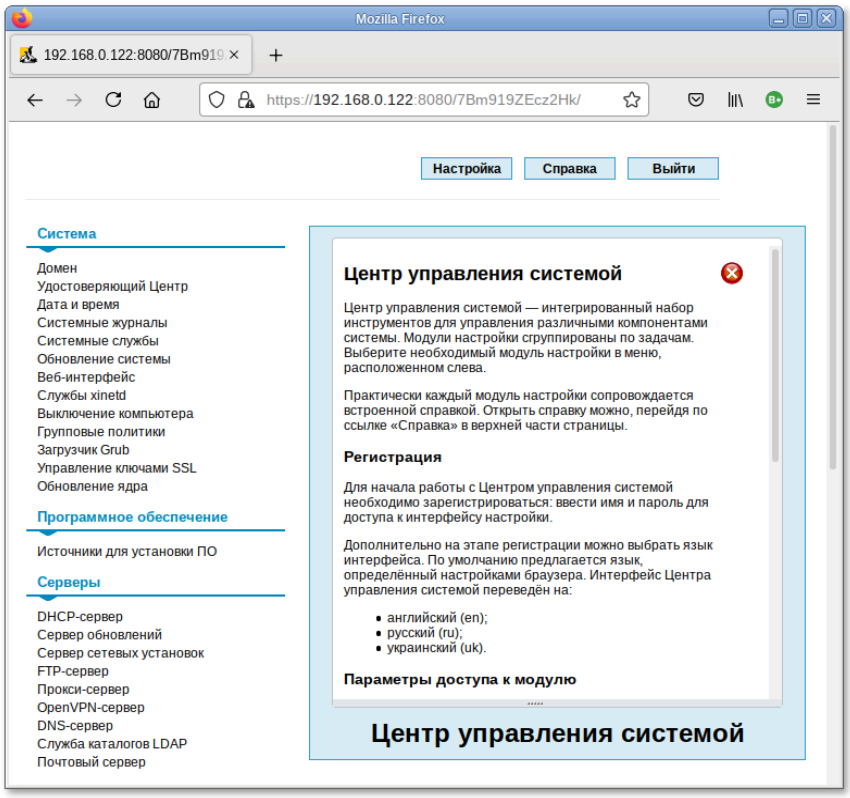


Рис. 414 – Возможности ЦУС в веб-браузере

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
```

11. SOGO

SOGo – сервер групповой работы, аналогичный Microsoft Exchange, с веб-интерфейсом и доступом по MAPI для Microsoft Outlook.

SOGo обеспечивает веб-интерфейс на основе AJAX и поддерживает различные нативные клиенты с помощью стандартных протоколов.

Возможности SOGo:

- общие почтовые папки, календари и адресные книги;
- веб-интерфейс, аналогичный Outlook Web Access;
- поддержка протоколов CalDAV, CardDAV, GroupDAV, Microsoft ActiveSync, IMAP и SMTP;
- доступ по MAPI для Microsoft Outlook, не требующий внешних модулей;
- делегирование, уведомления, резервирование, поддержка категорий и почтовых фильтров;
- поддержка нескольких почтовых ящиков в веб-интерфейсе;
- Single sign-on с помощью CAS, WebAuth или Kerberos.

⚠ MAPI over HTTPS не поддерживается.

11.1. Установка

Для установки SOGo на ОС Альт СП Сервер (64 бит, AArch64 (ARMv8)) нужно выполнить команду (драйвер к PostgreSQL будет установлен автоматически):

```
# apt-get install task-sogo
```

11.2. Подготовка среды

Подготовить к запуску и настроить службы PostgreSQL:

- создать системные базы данных:

```
# /etc/init.d/postgresql initdb
```

- запустить службу:

```
# service postgresql start
```

- создать пользователя sogo и базу данных sogo (под правами root):

```
# su - postgres -s /bin/sh -c 'createuser --no-superuser --no-
createdb --no-createrole sogo'
# su - postgres -s /bin/sh -c 'createdb -O sogo sogo'
# service postgresql restart
```

Настройка Samba DC:

1) пользователи расположены в домене Active Directory, расположенном на контроллере с Samba DC. Нужно предварительно развернуть сервер Samba AD DC (см. п. 10.2);

2) создать в домене пользователя sogo с паролем `Pa$$word` (при запросе дважды ввести пароль):

```
# samba-tool user create sogo
# samba-tool user setexpiry --noexpiry sogo
```

Настройка SOGo (настраивается на домен `test.alt`):

1) заполнить файл конфигурации `/etc/sogo/sogo.conf`:

```
{
    SOGoProfileURL = "postgresql://sogo@/sogo/sogo_user_profile";
 OCSFolderInfoURL = "postgresql://sogo@/sogo/sogo_folder_info";
 OCSSessionsFolderURL = "postgresql://sogo@/sogo/sogo_sessions_folder";
 OCSEMailAlarmsFolderURL = "postgresql://sogo@/sogo/sogo_alarms_folder";
 SOGoEnableEMailAlarms = YES;
 SOGoDraftsFolderName = Drafts;
 SOGoSentFolderName = Sent;
 SOGoTrashFolderName = Trash;
 SOGoIMAPServer                                                          =
"imaps://localhost:993/?tlsVerifyMode=allowInsecureLocalhost";
 SOGoMailingMechanism = sendmail;
 SOGoForceExternalLoginWithEmail = NO;
 NGImap4ConnectionStringSeparator = "/";
 SOGoUserSources =  (
          {
        id = sambaLogin;
             displayName = "SambaLogin";
              canAuthenticate = YES;
        type = ldap;
             CNFieldName = cn;
        IDFieldName = cn;
        UIDFieldName = sAMAccountName;
        hostname = "ldaps://127.0.0.1";
        baseDN = "CN=Users,DC=test,DC=alt";
        bindDN = "CN=sogo,CN=Users,DC=test,DC=alt";
        bindPassword = "Pa$$word";
        bindFields = (sAMAccountName);
    },
    {
        id = sambaShared;
        displayName = "Shared Addressbook";
        canAuthenticate = NO;
        isAddressBook = YES;
        type = ldap;
```

```
        CNFieldName = cn;
        IDFieldName = mail;
        UIDFieldName = mail;
        hostname = "ldaps://127.0.0.1";
        baseDN = "CN=Users,DC=test,DC=alt";
        bindDN = "CN=sogo,CN=Users,DC=test,DC=alt";
        bindPassword = "Pa$$word";
        filter = "((NOT isCriticalSystemObject='TRUE') AND (mail='*') AND (NOT
objectClass=contact))";
    },
    {
        id = sambaContacts;
        displayName = "Shared Contacts";
        canAuthenticate = NO;
        isAddressBook = YES;
        type = ldap;
        CNFieldName = cn;
        IDFieldName = mail;
        UIDFieldName = mail;
        hostname = "ldaps://127.0.0.1";
        baseDN = "CN=Users,DC=test,DC=alt";
        bindDN = "CN=sogo,CN=Users,DC=test,DC=alt";
        bindPassword = "Pa$$word";
        filter   =   "((((objectClass=person)   AND   (objectClass=contact)   AND
((uidNumber>=2000) OR (mail='*')))
                 AND    (NOT    isCriticalSystemObject='TRUE')    AND    (NOT
showInAdvancedViewOnly='TRUE') AND (NOT uid=Guest))
                 OR  (((objectClass=group)  AND  (gidNumber>=2000))  AND  (NOT
isCriticalSystemObject='TRUE') AND (NOT showInAdvancedViewOnly='TRUE')))";
        mapping = {
            displayname = ("cn");
        };
    }
  );
  SOGoSieveScriptsEnabled = YES;
  SOGoLanguage = Russian;
  SOGoTimeZone = Europe/Moscow;
  SOGoFirstDayOfWeek = 1;
}
```

2) включить службы по умолчанию и перезапустить их:

```
# for s in samba postgresql memcached sogo httpd2;do chkconfig
$s on;service $s restart;done
```

Возможные ошибки будут записаны в файл журнала `/var/log/sogo/sogo.log`.

11.3. Включение веб-интерфейса

Для включения веб-интерфейса нужно выполнить команды:

```
# a2enmod proxy
# a2enmod proxy_http
# a2enmod authn_core
# a2enmod authn_file
# a2enmod auth_basic
# a2enmod authz_user
```

```
# a2enmod env
# a2enmod dav
# a2enmod headers
# a2enmod rewrite
# a2enmod version
# a2enmod setenvif
# a2ensite SOGo
# service httpd2 restart
# service sogo restart
```

Веб-интерфейс доступен по адресу: `http://<адрес_сервера>/SOGo/`.

Примечание. Если при входе в веб-интерфейс возникает ошибка «Неправильный логин или пароль» и в логах `/var/log/sogo/sogo.log` есть ошибки вида:

```
Jul 06 16:14:51 sogod [12257]: [ERROR] <0x0x5578db070b40[LDAPSource]>
Could not bind to the LDAP server ldaps://127.0.0.1 (389) using the
bind DN: CN=sogo,CN=Users,DC=test,DC=alt
```

следует в файл `/etc/openldap/ldap.conf` добавить опцию `TLS_REQCERT allow` и перезапустить службы samba и sogo:

```
# service samba restart
# service sogo restart
```

11.4. Настройка электронной почты

⚠ Предварительно должен быть настроен DNS (см. п. 13).

Для использования электронной почты в SOGo нужно настроить аутентификацию в Active Directory для Postfix и Dovecot.

В примере используется следующая конфигурация (рис. 415):

- имя домена: test.alt;
- размещение почты: `/var/mail/<имя_домена>/<имя_пользователя>` (формат maildir);
- доступ на чтение почты: IMAP (порт 993), SSL;
- доступ на отправку почты: SMTP (порт 465), SSL/STARTTLS;
- данные аутентификации: email с доменом (например, petrov@test.alt) или имя пользователя.

⚠ Доступ к серверу LDAP осуществляется по протоколу ldap без шифрования. Для SambaDC нужно отключить ldaps в `/etc/samba/smb.conf` в секции `[global]`: `ldap server require strong auth = no` и перезапустить samba:

```
# service samba restart
```

Предварительно нужно создать пользователя vmail (пароль `Pa$$word`) с не истекающей учетной записью:

```
# samba-tool user create -W Users vmail
# samba-tool user setexpiry vmail --noexpiry
```

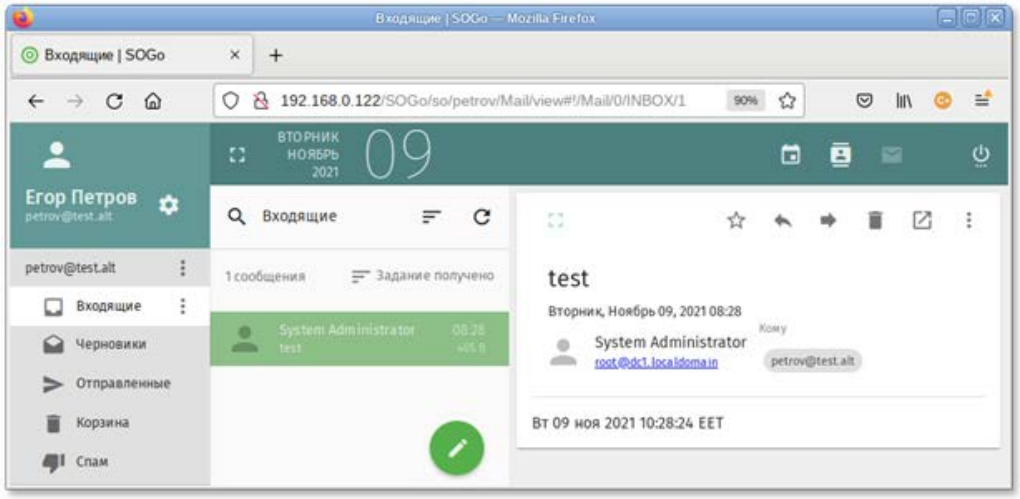


Рис. 415

11.4.1. Настройка Postfix

Установить пакет postfix-ldap:

```
# apt-get install postfix-ldap
```

В каталоге `/etc/postfix` изменить файлы для домена `test.alt`:

- изменить содержимое файла `main.cf`:

```
# Global Postfix configuration file.  This file lists only a small subset
# of all parameters.  For the syntax, and for a complete parameter list,
# see the postconf(5) manual page.  For a commented and more complete
# version of this file see /etc/postfix/main.cf.dist
mailbox_command    =    /usr/libexec/dovecot/dovecot-lda    -f    "$SENDER"    -a
"$RECIPIENT"
inet_protocols = ipv4

# Mappings
virtual_mailbox_base = /var/mail
virtual_mailbox_domains = test.alt
virtual_mailbox_maps = ldap:/etc/postfix/ad_local_recipients.cf
virtual_alias_maps = ldap:/etc/postfix/ad_mail_groups.cf
virtual_transport = dovecot
local_transport = virtual
```

```
local_recipient_maps = $virtual_mailbox_maps

# SSL/TLS
smtpd_use_tls = yes
smtpd_tls_security_level = encrypt
#smtpd_tls_security_level = may
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain = test.alt
smtpd_sasl_path = private/auth
smtpd_sasl_type = dovecot
smtpd_sender_login_maps = ldap:/etc/postfix/ad_sender_login.cf
smtpd_tls_auth_only = yes
smtpd_tls_cert_file = /var/lib/ssl/certs/dovecot.cert
smtpd_tls_key_file = /var/lib/ssl/private/dovecot.key
smtpd_tls_CAfile = /var/lib/ssl/certs/dovecot.pem

smtpd_recipient_restrictions = permit_mynetworks, reject_unauth_destination,
per-mit_sasl_authenticated, reject
smtpd_sender_restrictions = reject_authenticated_sender_login_mismatch
```

- файл `/etc/postfix/mydestination` должен быть пустым;

- в файл `master.cf` нужно добавить строки:

```
dovecot   unix  -       n       n       -       -       pipe
  flags=DRhu   user=mail:mail   argv=/usr/libexec/dovecot/deliver   -d
${recipient}
smtps     inet  n       -       n       -       -       smtpd
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
```

- создать файл `ad_local_recipients.cf`:

```
version = 3
server_host = test.alt:389
search_base = dc=test,dc=alt
scope = sub
query_filter                                                          =
(&(|(mail=%s)(otherMailbox=%u@%d))(sAMAccountType=805306368))
result_filter = %s
result_attribute = mail
special_result_attribute = member

bind = yes
bind_dn = cn=vmail,cn=users,dc=test,dc=alt
bind_pw = Pa$$word
```

- создать файл `ad_mail_groups.cf`:

```
version = 3
server_host = test.alt:389
search_base = dc=test,dc=alt
timeout = 3
scope = sub
query_filter = (&(mail=%s)(sAMAccountType=268435456))
result_filter = %s
result_attribute = mail
special_result_attribute = member
```

```
bind = yes
bind_dn = cn=vmail,cn=users,dc=test,dc=alt
bind_pw = Pa$$word
```

- создать файл `ad_sender_login.cf`:

```
version = 3
server_host = test.alt:389
search_base = dc=test,dc=alt
scope = sub
query_filter = (&(objectClass=user)(|(sAMAccountName=%s)(mail=%s)))
result_attribute = mail

bind = yes
bind_dn = cn=vmail,cn=users,dc=test,dc=alt
bind_pw = Pa$$word
```

- перезапустить службу postfix: # `service postfix restart`

Проверка конфигурации Postfix (в выводе не должно быть никаких сообщений):

```
# postconf >/dev/null
```

Проверка пользователя почты petrov:

```
# postmap -q petrov@test.alt ldap:/etc/postfix/ad_local_recipients.cf
petrov@test.alt
```

Проверка входа:

```
# postmap -q petrov@test.alt ldap:/etc/postfix/ad_sender_login.cf
petrov@test.alt
```

Проверка общего адреса e-mail:

```
# samba-tool group add --mail-address=sales@test.alt Sales
Added group Sales
# samba-tool group addmembers Sales ivanov,petrov
Added members to group Sales
# postmap -q sales@test.alt ldap:/etc/postfix/ad_mail_groups.cf
sales@test.alt,ivanov@test.alt,petrov@test.alt
```

11.4.2. Настройка Dovecot

Установить Dovecot:

```
# apt-get install dovecot
```

Изменить файлы для домена `test.alt`:

- создать файл `/etc/dovecot/dovecot-ldap.conf.ext`:

```
hosts            = test.alt:3268
ldap_version     = 3
auth_bind        = yes
dn               = cn=vmail,cn=Users,dc=test,dc=alt
dnpass           = Pa$$word
```

```
base             = cn=Users,dc=test,dc=alt
scope            = subtree
deref            = never

user_filter = (&(objectClass=user)(|(mail=%Lu)(sAMAccountName=%Lu)))
user_attrs  = =uid=8,gid=12,mail=user
pass_filter = (&(objectClass=user)(|(mail=%Lu)(sAMAccountName=%Lu)))
pass_attrs = mail=user
```

- изменить файл /etc/dovecot/conf.d/10-auth.conf:

```
#auth_username_format = %Lu
#auth_gssapi_hostname = "$ALL"
#auth_krb5_keytab = /etc/dovecot/dovecot.keytab
#auth_use_winbind = no
#auth_winbind_helper_path = /usr/bin/ntlm_auth
#auth_failure_delay = 2 secs
auth_mechanisms = plain
!include auth-ldap.conf.ext
```

- изменить файл /etc/dovecot/conf.d/10-mail.conf:

```
mail_location              =              maildir:/var/mail/%d/%n:UTF-
8:INBOX=/var/mail/%d/%n/Inbox
mail_uid = mail
mail_gid = mail
first_valid_uid = 5
first_valid_gid = 5
```

- изменить файл /etc/dovecot/conf.d/10-master.conf:

```
service imap-login {
  inet_listener imap {
    port = 0
  }
  inet_listener imaps {
  }
}
service pop3-login {
  inet_listener pop3 {
    port = 0
  }
  inet_listener pop3s {
    port = 0
  }
}
service lmtp {
  unix_listener lmtp {
  }
}
service imap {
}
service pop3 {
}
service auth {
  unix_listener auth-userdb {
  }
  unix_listener /var/spool/postfix/private/auth {
    mode = 0600
```

```
    user = postfix
    group = postfix
  }
}
service auth-worker {
}
service dict {
  unix_listener dict {
  }
}
```

- изменить файл `/etc/dovecot/conf.d/15-lda.conf`:

```
protocol lda {
  hostname = test.alt
  postmaster_address = administrator@test.alt
}
```

- изменить файл `/etc/dovecot/conf.d/15-mailboxes.conf`:

```
namespace inbox {
  inbox = yes
  mailbox Drafts {
    auto = subscribe
    special_use = \Drafts
  }
  mailbox Junk {
    auto = subscribe
    special_use = \Junk
  }
  mailbox Trash {
    auto = subscribe
    special_use = \Trash
  }
  mailbox Sent {
    auto = subscribe
    special_use = \Sent
  }
  mailbox "Sent Messages" {
    special_use = \Sent
  }
}
```

- перезапустить службу dovecot: `# service dovecot restart`

Проверка конфигурации Dovecot (в выводе не должно быть никаких сообщений):

```
# doveconf >/dev/null
```

11.4.3. Безопасность

Так как конфигурационные файлы содержат пароль пользователя LDAP, их нужно сделать недоступным для чтения прочим пользователям:

```
# chown dovecot:root /etc/dovecot/dovecot-ldap.conf.ext
# chmod 0640 /etc/dovecot/dovecot-ldap.conf.ext
```

```
# chown root:postfix /etc/postfix/ad_local_recipients.cf
/etc/postfix/ad_mail_groups.cf /etc/postfix/ad_sender_login.cf
# chmod 0640 /etc/postfix/ad_local_recipients.cf
/etc/postfix/ad_mail_groups.cf /etc/postfix/ad_sender_login.cf
```

Перезапустить службы:

```
# service dovecot restart
# service postfix restart
```

11.4.4. Проверка конфигурации

Проверка SMTP:

```
# date | mail -s test petrov@test.alt
# mailq
-Queue ID-     -Size-   ----Arrival Time----       -Sender/Recipient-
0C33E20196     146      Fri Feb 16 16:39:37       root
                                                  ivanov@test.alt
```

Проверка IMAP (выход по «Ctrl+D»):

```
# openssl s_client -crlf -connect test.alt:993
...
tag login petrov@test.alt Pa$$word
tag OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID
ENABLE
IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS
THREAD=ORDEREDSUBJECT
MULTIAPPEND URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE
UIDPLUS
LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT
SEARCHRES
WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE] Logged in
```

12. FREEIPA

FreeIPA – это комплексное решение по управлению безопасностью Linux-систем, 389 Directory Server, MIT Kerberos, NTP, DNS, Dogtag, состоит из веб-интерфейса и интерфейса командной строки.

FreeIPA является интегрированной системой проверки подлинности и авторизации в сетевой среде Linux, FreeIPA-сервер обеспечивает централизованную проверку подлинности, авторизацию и контроль за аккаунтами пользователей сохраняя сведения о пользователе, группах, узлах и других объектах, которые требуются для обеспечения сетевой безопасности.

12.1. Установка сервера FreeIPA

Для установки сервера FreeIPA (Сервер 64 бит, AArch64 (ARMv8)) со встроенным DNS-сервером и доменом `EXAMPLE.TEST` в локальной сети `192.168.135.0/24` выполнить следующие действия:

1) отключить ahttpd, работающий на порту 8080, во избежание конфликтов с разворачиваемым tomcat и отключить HTTPS в Apache2:

```
# service ahttpd stop
# a2dissite 000-default_https
# a2disport https
# service httpd2 condreload
```

2) установить пакеты:

```
# apt-get install freeipa-server freeipa-server-dns
```

3) задать имя сервера:

```
# hostnamectl set-hostname ipa.example.test
```

4) запустить скрипт настройки сервера:

- в пакетном режиме:

```
# ipa-server-install -U --hostname=$(hostname) -r EXAMPLE.TEST -n example.test -p 12345678 -a 12345678 --setup-dns --no-forwarders --no-reverse
```

- или интерактивно:

```
# ipa-server-install
```

ВНИМАНИЕ!

Пароли должны быть не менее 8 символов.

Обратите внимание на ответы на вопрос, не совпадающий с предложенными:

`Do you want to configure integrated DNS (BIND)? [no]: yes`

Остальные вопросы нужно выбрать по умолчанию (можно просто нажать <Enter>). Так же при установке нужно ввести пароль администратора системы и пароль администратора каталогов.

Для возможности управлять FreeIPA-сервером из командной строки нужно получить билет Kerberos:

```
# kinit admin
```

Добавить в DNS запись о сервере времени, чтобы компьютеры в локальной сети могли к нему подключаться:

```
# ipa dnsrecord-add example.test _ntp._udp --srv-priority=0 --srv-weight=100 --srv-port=123 --srv-target=ipa.example.test.
```

Проверить работу ntp сервера можно командой:

```
# ntpdate -q localhost
server 127.0.0.1, stratum 3, offset 0.000018, delay 0.02568
27 Apr 10:27:00 ntpdate[3491]: adjust time server 127.0.0.1 offset 0.000018 sec
```

П р и м е ч а н и е . Если в выводе присутствуют ошибки следующего вида:

```
[error] CalledProcessError: Command '/sbin/systemctl restart httpd2.service' returned non-zero exit status 1
```

Выполнить команду: `# systemctl restart httpd2`

Отменить установку: `# ipa-server-install -U --uninstall`

и повторить снова.

Веб-интерфейс FreeIPA доступен по адресу:

`https://ipa.example.test/ipa/ui/`

12.2. Установка сервера FreeIPA в режиме CA-less

Для установки сервера FreeIPA (Сервер 64 бит, AArch64 (ARMv8)) со встроенным DNS-сервером и доменом `EXAMPLE.TEST` в режиме CA-less выполнить следующие действия:

1) установить пакеты:

```
# apt-get install freeipa-server freeipa-server-dns
```

2) задать имя сервера:

```
# hostnamectl set-hostname ipa.example.test
```

3) требуется перезагрузка;

4) подготовить сертификаты для сервера FreeIPA: `# mkdir ~/test_ca`

5) создать файл `pwdfiles.txt` с паролем, например, 12345678:

```
# echo 12345678 > ~/test_ca/pwdfile.txt
```

ВНИМАНИЕ!

Пароли должны быть не менее 8 символов.

6) создать базу данных NSS:

```
/usr/bin/certutil -d ~/test_ca -N -f ~/test_ca/pwdfile.txt
```

7) создать noise файл, заполненный случайными числами:

```
# head -c20 /dev/random > ~/test_ca/noise.txt
```

8) выполнить экспорт переменной `CERT_SERIAL`:

```
# export CERT_SERIAL=1
```

9) создать CA сертификат:

```
  # SKID="0x`openssl rand -hex 20`"
  # echo $SKID
# /usr/bin/certutil -d ~/test_ca -S -n "CA" -s "CN=Certificate
Authority" -x -t CT,,C -1 -2 -5 -m $CERT_SERIAL -v 120 -z
~/test_ca/noise.txt -f ~/test_ca/pwdfile.txt –extSKID
```

В ответ на запросы команды дать следующие ответы:

```
Generating key.  This may take a few moments...
     0 - Digital Signature
     1 - Non-repudiation
     2 - Key encipherment
     3 - Data encipherment
     4 - Key agreement
     5 - Cert signing key
     6 - CRL signing key
     Other to finish
> 0
```

```
          0 - Digital Signature
          1 - Non-repudiation
          2 - Key encipherment
          3 - Data encipherment
          4 - Key agreement
          5 - Cert signing key
          6 - CRL signing key
          Other to finish
     > 1
          0 - Digital Signature
          1 - Non-repudiation
          2 - Key encipherment
          3 - Data encipherment
          4 - Key agreement
          5 - Cert signing key
          6 - CRL signing key
          Other to finish
     > 5
          0 - Digital Signature
          1 - Non-repudiation
          2 - Key encipherment
          3 - Data encipherment
          4 - Key agreement
          5 - Cert signing key
          6 - CRL signing key
          Other to finish
     > 9
     Is this a critical extension [y/N]?
     y
     Is this a CA certificate [y/N]?
     y
     Enter the path length constraint, enter to skip [<0 for unlimited
path]: > 0
Is this a critical extension [y/N]?
     y
     Adding Subject Key ID extension.
     Enter value for the key identifier fields,enter to omit:
     0xdd2b9e67d1c2e85fd67884dee68e5375fd294e92 – ($SKID)
     Is this a critical extension [y/N]?
     n
     Is this a critical extension [y/N]?
     n
                    0 - SSL Client
                    1 - SSL Server
                    2 - S/MIME
                    3 - Object Signing
                    4 - Reserved for future use
                    5 - SSL CA
                    6 - S/MIME CA
                    7 - Object Signing CA
                    Other to finish
      > 5
                    0 - SSL Client
                    1 - SSL Server
                    2 - S/MIME
                    3 - Object Signing
                    4 - Reserved for future use
                    5 - SSL CA
                    6 - S/MIME CA
                    7 - Object Signing CA
                    Other to finish
      > 6
                    0 - SSL Client
                    1 - SSL Server
```

```
                2 - S/MIME
                3 - Object Signing
                4 - Reserved for future use
                5 - SSL CA
                6 - S/MIME CA
                7 - Object Signing CA
                Other to finish
 > 7
                0 - SSL Client
                1 - SSL Server
                2 - S/MIME
                3 - Object Signing
                4 - Reserved for future use
                5 - SSL CA
                6 - S/MIME CA
                7 - Object Signing CA
                Other to finish
 > 9
Is this a critical extension [y/N]?
n
```

10) создать `noise` файл, заполненный случайными числами:

```
# head -c20 /dev/random > ~/test_ca/noise.txt
```

11) создать запрос сертификата:

```
# SKID="0x`openssl rand -hex 20`"
# echo $SKID
# /usr/bin/certutil -d ~/test_ca -R -s CN=$HOSTNAME,O=IPA -o
/tmp/servercert.req -k rsa -g 2048 -z ~/test_ca/noise.txt -f
~/test_ca/pwdfile.txt -a --extSKID
Generating key.  This may take a few moments...
Adding Subject Key ID extension. Enter value for the key identifier
fields,enter to omit:
0x748098604e1b028 3d3eb413f7843193fa09668db – ($SKID)
Is this a critical extension [y/N]?
n
```

12) подписать запрос о выдаче сертификата сервера:

```
# export CERT_SERIAL=$(($CERT_SERIAL + 1))
# /usr/bin/certutil -d ~/test_ca -C -c "CA" -i
/tmp/servercert.req -o /tmp/servercert.pem -m $CERT_SERIAL -v
120 -f ~/test_ca/pwdfile.txt -1 -5 –a
```

В ответ на запросы команды дать следующие ответы:

```
    0 - Digital Signature
    1 - Non-repudiation
    2 - Key encipherment
    3 - Data encipherment
    4 - Key agreement
    5 - Cert signing key
    6 - CRL signing key
    Other to finish
> 2
    0 - Digital Signature
    1 - Non-repudiation
    2 - Key encipherment
    3 - Data encipherment
    4 - Key agreement
```

```
    5 - Cert signing key
    6 - CRL signing key
    Other to finish
> 9
    Is this a critical extension [y/N]?
 n
    0 - SSL Client
    1 - SSL Server
    2 - S/MIME
    3 - Object Signin g
    4 - Reserved for future use
    5 - SSL CA
    6 - S/MIME CA
    7 - Object Signing CA
    Other to finish
> 1
    0 - SSL Client
    1 - SSL Server
    2 - S/MIME
    3 - Object Signing
    4 - Reserved for future use
    5 - SSL CA
    6 - S/MIME CA
    7 - Object Signing CA
    Other to finish
> 9
    Is this a critical extension [y/N]?
 n
```

Примечание. Можно создавать отдельные сертификаты для серверов HTTP и Directory.

12.2.1. Экспорт сертификатов в правильные форматы

Далее нужно произвести экспорт сертификатов в правильные форматы.

1) Импортировать полученный сертификат:

```
# /usr/bin/certutil -d ~/test_ca -A -i /tmp/servercert.pem -n
Server-Cert -a -t ,,
```

2) Экспортировать сертификат в PKCS#12:

```
# /usr/bin/pk12util -o ~/test_ca/servercert.p12 -n Server-Cert
-d ~/test_ca -k ~/test_ca/pwdfile.txt -w ~/test_ca/pwdfile.txt
```

3) Экспортировать сертификат CA в формате PEM:

```
# /usr/bin/certutil -d ~/test_ca -L -n "CA" -a >
~/test_ca/cacert.pem
```

4) Установить CA-less IPA:

```
# export PWD=$(cat ~/test_ca/pwdfile.txt)
#проверка правильности создания сертификата
# openssl verify -CAfile ~/test_ca/cacert.pem
/tmp/servercert.pem
# ipa-server-install --http-cert-file ~/test_ca/servercert.p12
--dirsrv-cert-file ~/test_ca/servercert.p12 --http-pin $PWD --
dirsrv-pin $PWD --ca-cert-file ~/test_ca/cacert.pem --no-pkinit
```

Примечание. Можно указать при установке опции `--pkinit-cert-file=Файл` – файл, содержащий сертификат SSL Kerberos KDC и закрытый ключ и `--pkinit-pin=Пароль` – пароль от закрытого ключа Kerberos KDC.

Для возможности управлять FreeIPA-сервером из командной строки нужно получить билет Kerberos:

```
# kinit admin
```

Веб-интерфейс FreeIPA доступен по адресу:

`https://ipa.example.test/ipa/ui/`

12.3. Добавление новых пользователей домена

Для добавления новых пользователей можно воспользоваться веб-интерфейсом FreeIPA. Для этого нужно открыть в веб-браузере адрес `https://ipa.example.test/ipa/ui` и ввести данные администратора для входа в систему (рис. 416). Для входа в веб-интерфейс следует использовать имя admin, и пароль, введенный при установке сервера FreeIPA.

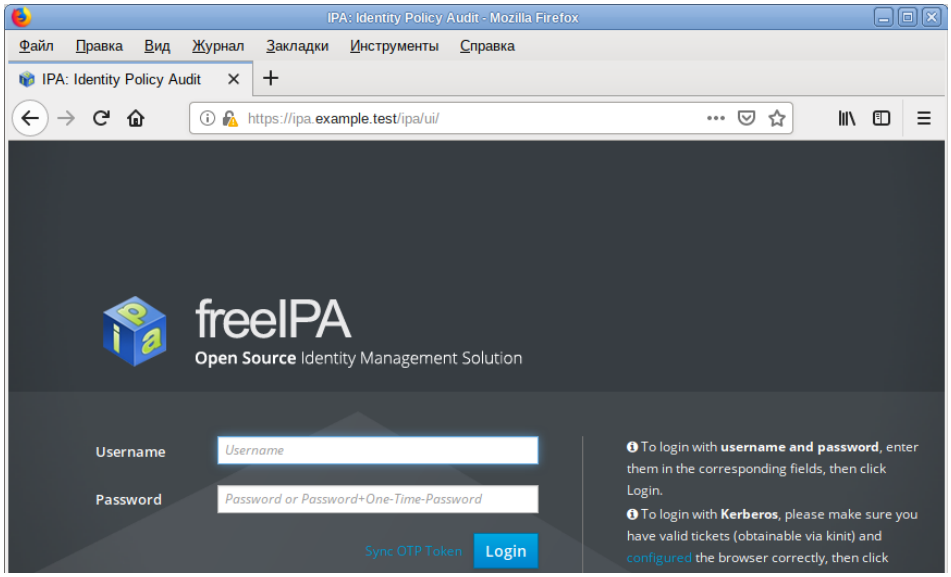


Рис. 416 – Веб-интерфейс FreeIPA

После успешной авторизации можно создать нового пользователя домена. Для этого в окне «Пользователи домена» нужно нажать на кнопку «Добавить» (рис. 417).

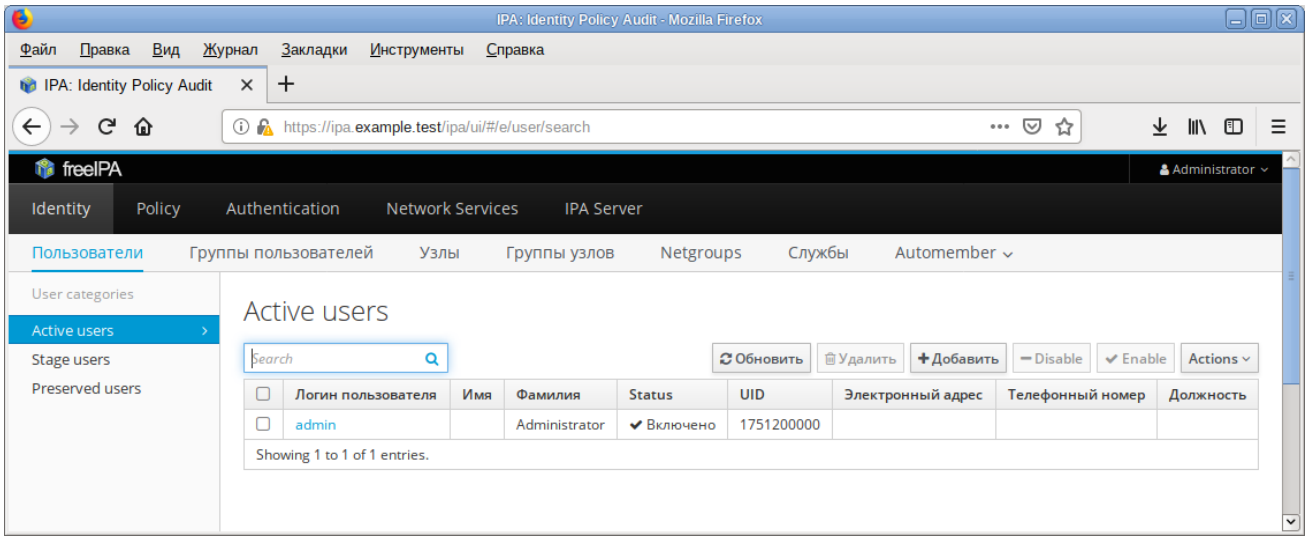


Рис. 417 – Окно «Пользователи домена»

В открывшемся окне нужно ввести данные пользователя и нажать на кнопку «Добавить» (рис. 418).

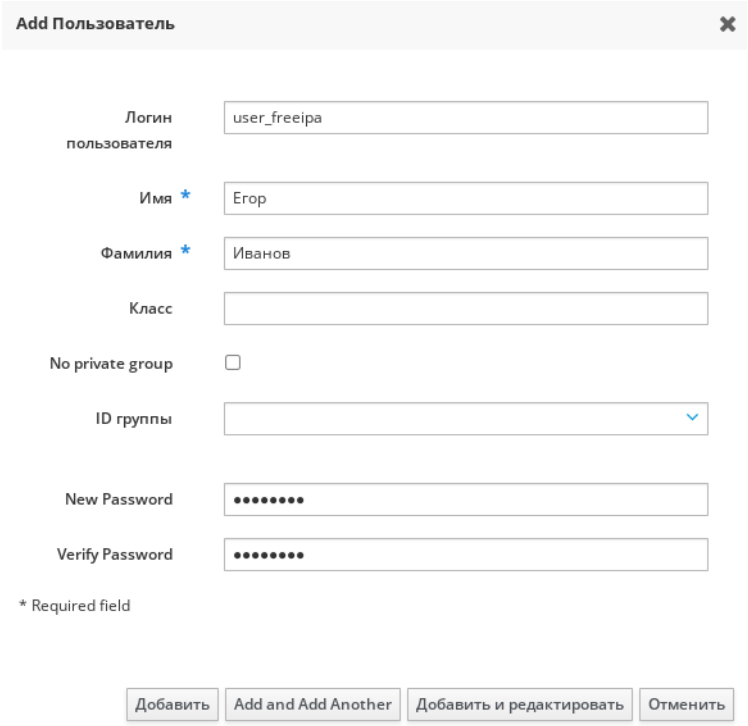


Рис. 418 – Окно добавления нового пользователя домена

Созданный пользователь появится в списке пользователей (рис. 419).

Active users

Search | Обновить | Удалить | Добавить | Disable | Enable | Actions

	Логин пользователя	Имя	Фамилия	Status	UID	Электронный адрес	Телефонный номер	Должность
	admin		Administrator	Включено	1751200000			
	user_freeipa	Егор	Иванов	Включено	1751200001	user_freeipa@example.test		

Showing 1 to 2 of 2 entries.

Рис. 419 – Список пользователей домена

12.4. Ввод рабочей станции в домен FreeIPA – установка клиента и подключение к серверу

Инструкция по вводу рабочей станции под управлением ОС Альт СП Рабочая станция в домен FreeIPA.

12.4.1. Установка FreeIPA клиента

Установить пакеты:

```
# apt-get install freeipa-client libsss_sudo krb5-kinit bind-utils libbind zip
```

Примечание. Установить также пакет task-auth-freeipa на рабочей станции 64/32 бит.

Примечание. Очистить конфигурацию freeipa-client невозможно. В случае если это нужно (например, для удаления, переустановки freeipa-client) следует переустановить систему.

12.4.2. Настройка сети. FreeIPA

Клиентские компьютеры должны быть настроены на использование DNS-сервера, который был сконфигурирован на сервере FreeIPA во время его установки. В сетевых настройках нужно указать использовать сервер FreeIPA для разрешения имен. Эти настройки можно выполнить как в графическом интерфейсе, так и в консоли:

1) в ЦУС в разделе «Сеть» → «Ethernet-интерфейсы» (см. п. 8.5.1) задать имя компьютера, указать в поле DNS-серверы IP-адрес FreeIPA-сервера и в поле «Домены поиска» – домен для поиска (рис. 420);

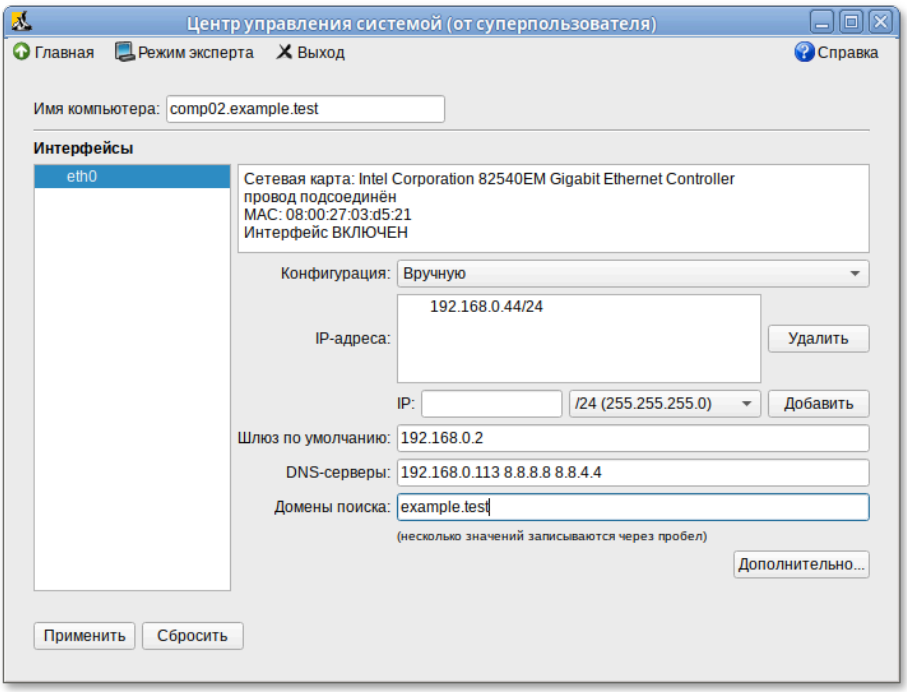


Рис. 420

2) в консоли:

- задать имя компьютера:

```
# hostnamectl set-hostname comp02.example.test
```

- добавить DNS-сервер, для этого нужно создать файл `/etc/net/ifaces/eth0/resolv.conf` со следующим содержимым:

```
nameserver 192.168.0.113
```

где `192.168.0.113` – IP-адрес FreeIPA-сервера;

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

```
interface_order='lo lo[0-9]* lo.* eth0'
search_domains=example.test
```

где:

а) `eth0` – интерфейс на котором доступен FreeIPA-сервер;

б) `example.test` – домен;

- обновить DNS-адреса:

```
# resolvconf -u
```

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

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

```
search example.test
nameserver 192.168.0.113
```

12.4.3. Подключение к серверу в ЦУС

Для ввода рабочей станции в домен FreeIPA, нужно в ЦУС перейти в раздел «Пользователи» → «Аутентификация» (см. п. 8.4.5).

В открывшемся окне следует выбрать пункт «Домен FreeIPA», заполнить поля «Домен» и «Имя компьютера», затем нажать на кнопку «Применить» (рис. 421).

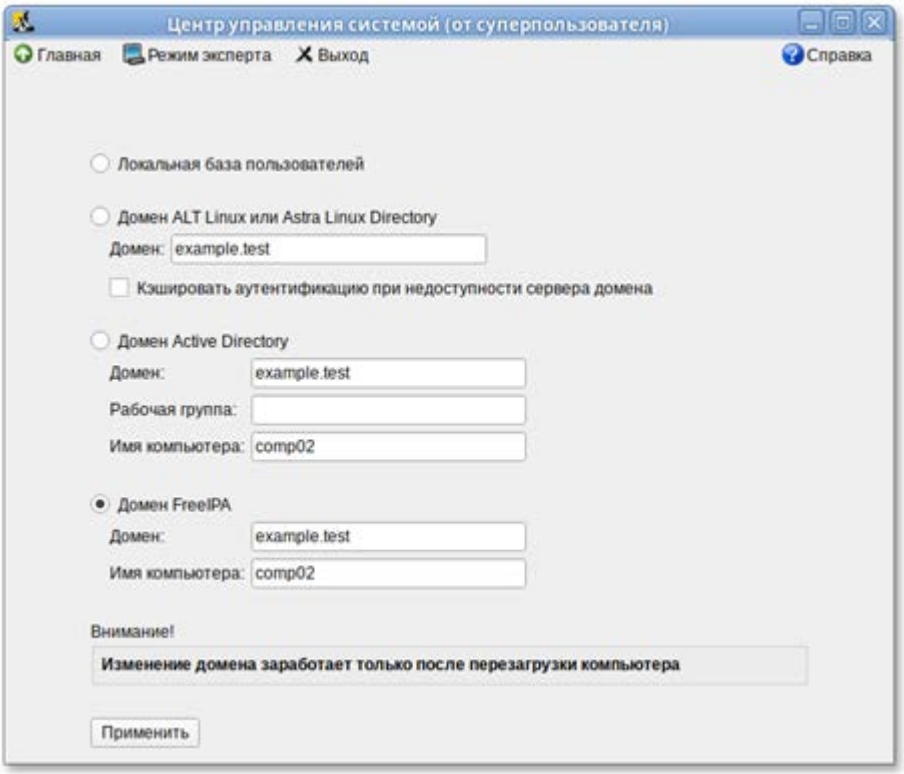


Рис. 421

В открывшемся окне нужно ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать на кнопку «ОК» (рис. 422).

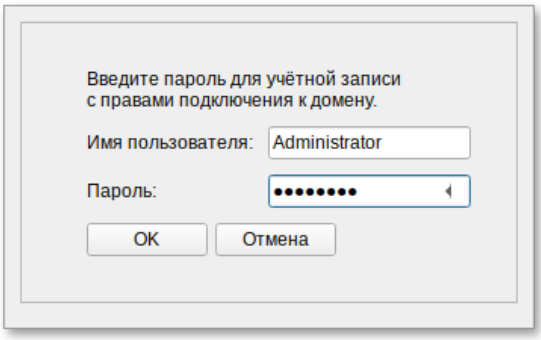


Рис. 422

В случае успешного подключения, будет выведено соответствующее сообщение (рис. 423).

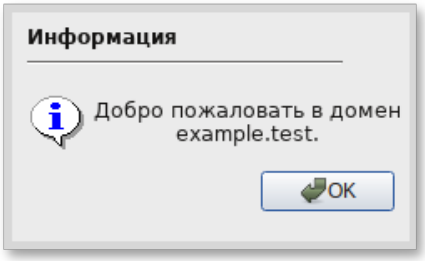


Рис. 423

Перезагрузить рабочую станцию.

12.4.4. Подключение к серверу в консоли

Запустить скрипт настройки клиента в пакетном режиме:

```
# ipa-client-install -U -p admin -w 12345678
```

или интерактивно:

```
# ipa-client-install
```

Если все настроено, верно, скрипт должен выдать такое сообщение:

```
'''Discovery was successful!'''
Client hostname: comp01.example.test
Realm: EXAMPLE.TEST
DNS Domain: example.test
IPA Server: ipa.example.test
BaseDN: dc=example,dc=test
Continue to configure the system with these values? [no]:
```

Нужно ответить `yes`, ввести имя пользователя, имеющего право вводить машины в домен, и его пароль.

ВНИМАНИЕ!

Если при входе в домен возникает такая ошибка:

```
Hostname (comp01.example.test) does not have A/AAAA record.
Failed to update DNS records.
```

Нужно проверить IP-адрес доменного DNS-сервера в файле `/etc/resolv.conf`.

В случае возникновения ошибки, нужно перед повторной установкой запустить процедуру удаления:

```
# ipa-client-install -U --uninstall
```

Для работы sudo-политик для доменных пользователей на клиентской машине нужно разрешить доступ к sudo:

```
# control sudo public
```

12.4.5. Вход пользователя

В окне входа в систему нужно ввести логин учетной записи пользователя FreeIPA и нажать на кнопку «Войти» (рис. 424).

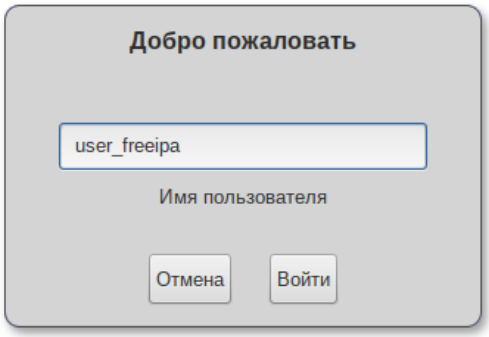


Рис. 424

В открывшемся окне ввести пароль, соответствующий этой учетной записи и нажать на кнопку «Войти».

При первом входе пользователя будет запрошен текущий (установленный администратором) пароль, затем у пользователя запрашивается новый пароль и его подтверждение.

⚠ Если машина до этого была в других доменах или есть проблемы со входом пользователей рекомендуется очистить кэш sssd:

```
# systemctl stop sssd
# rm -f /var/lib/sss/db/*
# rm -f /var/lib/sss/mc/*
# systemctl start sssd
```

12.5. Настройка репликации

На втором контроллере домена нужно установить пакеты:

```
# apt-get install freeipa-client freeipa-server-dns
```

Задать имя сервера:

```
# hostnamectl set-hostname ipabackup.example.test
```

Развернуть и настроить клиента:

```
# ipa-client-install -d --domain=example.test --server=ipa.example.test --realm=EXAMPLE.TEST --principal=admin --password=12345678 --enable-dns-updates -U
```

После выполнения этой операции хост ipabackup.example.test должен появиться в веб-интерфейсе FreeIPA.

Далее нужно настроить репликацию LDAP-каталога:

```
# ipa-replica-install
```

Добавить в DNS второй NTP-сервер:

```
# kinit admin
# ipa dnsrecord-add example.test _ntp._udp --srv-priority=0 --srv-weight=100 --srv-port=123 --srv-target=ipabackup.example.test
```

Настроить репликацию DNS-зон:

```
# ipa-dns-install
```

Настроить репликацию CA:

```
# ipa-ca-install
```

После настройки и репликации контроллеров посмотреть топологию можно в веб-интерфейсе FreeIPA.

12.6. Настройка доверительных отношений с Active Directory

FreeIPA использует Samba для интеграции в AD. Для работы Samba нужен работающий стек IPv6.

Начальные данные:

- IP-адрес IPA-сервера: `192.168.135.130`;

- Имя IPA-сервера: `dcf`;

- Имя IPA-домена: `domf.testf`;

- NetBIOS имя IPA домена: `DOMF`;

- IP-адрес AD DC: `192.168.135.150`;

- Имя AD DC: `dcc`;

- Имя AD домена: `domc.testc`;

- NetBIOS имя AD домена: `DOMC`.

Установить пакеты:

```
# apt-get install freeipa-server-trust-ad python3-module-sss-murmur samba-winbind
```

12.6.1. Предварительная настройка IPA-сервера

Выполнить предварительную настройку IPA-сервера для работы с доверием:

```
# ipa-adtrust-install
```

Скрипт спросит нужно ли конфигурировать slapi-nis плагин для поддержки работы старых клиентов (SSSD < 1.9) с пользователем из доверенного домена:

```
Enable trusted domains support in slapi-nis? [no]:
```

На IPA-сервере существует по крайней мере один пользователь (администратор сервера), поэтому скрипт предложит сгенерировать SID для всех существующих пользователей и групп:

```
Do you want to run the ipa-sidgen task? [no]:
```

Дата и время на серверах должны совпадать.

IPA-сервер в своей работе использует следующие порты:

- TCP ports: 80, 88, 443, 389, 636, 88, 464, 53, 135, 138, 139, 445, 1024 – 1300;

- UDP ports: 88, 464, 53, 123, 138, 139, 389, 445.

Они должны быть открыты и доступны.

Настроить Samba:

```
# net conf setparm global 'dedicated keytab file'
/etc/samba/samba.keytab
# systemctl restart ipa
```

Проверить проходит ли Samba аутентификацию Kerberos со стороны IPA-сервера:

```
# kinit admin
# smbclient -L dcf.domf.testf -k
lp_load_ex: changing to config backend registry
Domain=[DOMF] OS=[Windows 6.1] Server=[Samba 4.5.5]

     Sharename       Type      Comment
     ---------       ----      -------
     IPC$            IPC       IPC Service (Samba 4.5.5)
Domain=[DOMF] OS=[Windows 6.1] Server=[Samba 4.5.5]

     Server               Comment
     ---------            -------

     Workgroup            Master
     ---------            -------
```

Настроить DNS на обоих серверах, чтобы они знали друг о друге:

1) на AD сервере создать сервер условной пересылки для зоны IPA-домена:

```
C:\> dnscmd 127.0.0.1 /ZoneAdd domf.testf /Forwarder 192.168.135.130
```

2) на IPA-сервере так же добавить зону AD домена:

```
# ipa dnsforwardzone-add domc.testc --forwarder=192.168.135.150
--forward-policy=only
```

Если при добавлении зоны перенаправления появляется предупреждение об ошибке проверки DNSSEC, это означает что удаленный DNS-сервер не использует DNSSEC. Рекомендуется включить DNSSEC на удаленном DNS-сервере.

Если включить проверку DNSSEC на удаленном DNS-сервере нельзя, можно отключить DNSSEC на сервере FreeIPA.

Для этого в файле `/etc/bind/ipa-options-ext.conf` следует привести параметры `dnssec-validation` и `dnssec-enable` к виду:

```
dnssec-enable no;
dnssec-validation no;
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

12.6.2. Проверка конфигурации DNS

12.6.2.1. На AD сервере

Проверить наличие записей для работы сервисов IPA на DNS-сервере AD.

1) Запись, отвечающая за работу сервисов Kerberos через UDP и LDAP через TCP:

```
C:\>nslookup.exe
> set type=SRV

> _kerberos._udp.domf.testf.
_kerberos._udp.domf.testf.       SRV service location:
    priority                = 0
    weight                  = 100
    port                    = 88
    svr hostname   = dcf.domf.testf.

> _ldap._tcp.domf.testf.
_ldap._tcp.ipa.example.com       SRV service location:
    priority                = 0
    weight                  = 100
    port                    = 389
    svr hostname   = dcf.domf.testf.
```

2) Запись, отвечающая за имя Kerberos realm IPA домена:

```
C:\>nslookup.exe
> set type=TXT
> _kerberos.domf.testf.
_kerberos.domf.testf.        text =
    "DOMF.TESTF"
```

3) В результате выполнения команды `ipa-adtrust-install` должны появиться записи, отвечающие за работу сервисов MS DC Kerberos через UDP и LDAP через TCP:

```
C:\>nslookup.exe
> set type=SRV
> _kerberos._udp.dc._msdcs.domf.testf.
_kerberos._udp.dc._msdcs.domf.testf.        SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = dcf.domf.testf.
> _ldap._tcp.dc._msdcs.domf.testf.
_ldap._tcp.dc._msdcs.domf.testf.        SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = dcf.domf.testf.
```

4) Далее проверить наличие записей для работы сервисов AD на DNS-сервере AD.

Запись, отвечающая за работу сервисов Kerberos через UDP и LDAP через TCP:

```
C:\>nslookup.exe
> set type=SRV
> _kerberos._udp.dc._msdcs.domc.testc.
_kerberos._udp.dc._msdcs.domc.testc.  SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = dcc.domc.testc.
> _ldap._tcp.dc._msdcs.domc.testc.
_ldap._tcp.dc._msdcs.domc.testc.      SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = dcc.domc.testc.
```

12.6.2.2. На IPA-сервере

Проверить наличие записей для работы сервисов IPA на DNS-сервере IPA.

1) Запись, отвечающая за работу сервисов Kerberos через UDP и LDAP через TCP:

```
# dig +short -t SRV _kerberos._udp.domf.testf.
0 100 88 dcf.domf.testf.

# dig +short -t SRV _ldap._tcp.domf.testf.
0 100 389 dcf.domf.testf.
```

2) Запись, отвечающая за имя Kerberos realm IPA домена:

```
dig +short -t TXT _kerberos.domf.testf.
"DOMF.TESTF"
```

3) После выполнения команды `ipa-adtrust-install` должны появиться записи, отвечающие за работу сервисов MS DC Kerberos через UDP и LDAP через TCP:

```
# dig +short -t SRV _kerberos._udp.dc._msdcs.domf.testf.
0 100 88 dcf.domf.testf.

# dig +short -t SRV _ldap._tcp.dc._msdcs.domf.testf.
0 100 389 dcf.domf.testf.
```

4) Далее проверить наличие записей для работы сервисов AD на DNS-сервере IPA.

Запись, отвечающая за работу сервисов Kerberos через UDP и LDAP через TCP:

```
# dig +short -t SRV _kerberos._udp.dc._msdcs.domc.testc.
0 100 88 dcc.domc.testc.

# dig +short -t SRV _ldap._tcp.dc._msdcs.domc.testc.
0 100 389 dcc.domc.testc.
```

ВНИМАНИЕ!

Если запись `_kerberos._udp.dc._msdcs.domc.testc.` не доступна, проверьте `_kerberos._tcp.dc._msdcs.domc.testc`.

12.6.3. Настройка доверия

Добавление двунаправленных доверительных отношений леса (Forest Trust) с AD (нужно ввести пароль Administrator AD, имя доменного администратора Windows – должно быть на латинице):

```
# kinit admin
# ipa trust-add --type=ad domc.testc --admin Administrator --password --two-way=true
```

Далее нужно запросить сервер AD о его доверенных доменах:

```
# ipa trust-fetch-domains domc.testc
```

При этом IPA создаст нужные id-диапазоны для доверенных доменов.

Если нужно добавить еще один домен `DOME.TESTE`, то нужно настроить DNS на обоих серверах, чтобы они видели друг друга, и выполнить команду еще раз, чтобы IPA-сервер узнал о нем:

```
# ipa trust-fetch-domains domc.testc
```

Найти все доверенные домены можно и с помощью веб-интерфейса. Для это перейти в раздел «IPA Server» → «Trusts» и выбрать нужный домен (рис. 425).

Нажать на кнопку «Fetch domains», это обновит список доверенных доменов (рис. 426).

Для того чтобы увидеть список всех доверенных доменов используйте следующую команду:

```
# ipa trustdomain-find domc.testc
```

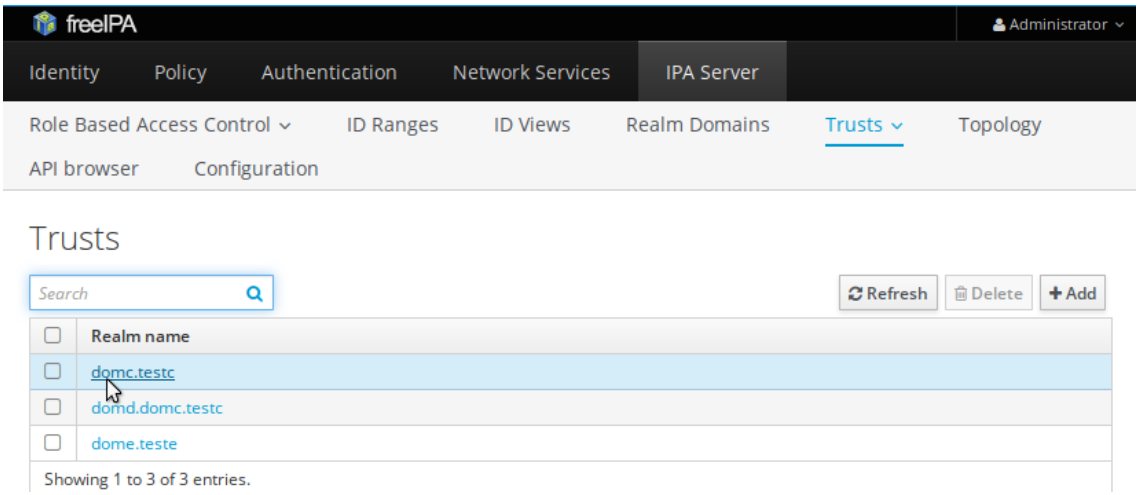


Рис. 425

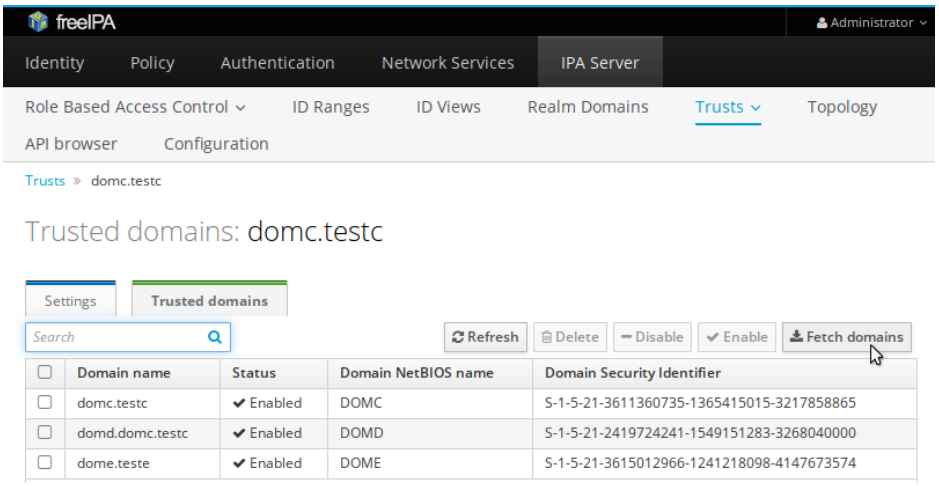


Рис. 426

12.6.4. Проверка конфигурации Kerberos

1) Запросить ticket для IPA пользователя:

```
# kinit admin
```

2) Запросить service ticket для сервиса из IPA домена:

```
# kvno -S host dcf.domf.testf
host/dcf.domf.testf@DOMF.TESTF: kvno = 2
```

3) Запросить service ticket сервиса из AD домена:

```
# kvno -S cifs dcc.domc.testc
cifs/dcc.domc.testc@: kvno = 3
```

Если запрос service ticket для сервиса из AD домена прошел успешно, то должен появиться междоменный ticket-granting ticket, его имя krbtgt/DOMC.TESTC@DOMF.TESTF:

```
# klist
```

12.6.5. Проверка пользователей доверенного домена

Для проверки доступа к пользователям из доверенного домена на рабочей станции IPA выполнить команду:

```
# getent passwd u01domc@domc
u01domc@domc.testc:*:328601108:328601108:u01domc:/home/domc.testc/u01domc:
```

где u01domc это пользователь из AD домена.

Обратите внимание, что не указана оболочка входа. Назначить оболочку входа для пользователей из доверенного домена можно добавив на сервере IPA в файл /etc/sssd/sssd.conf следующую строчку:

```
[domain/domf.testf]
...
default_shell = /bin/bash
...
```

Вывод команды должен стать таким:

```
# getent passwd u01domc@domc
u01domc@domc.testc:*:328601108:328601108:u01domc:/home/domc.testc/u01domc:/bin/bash
```

ВНИМАНИЕ!

1) Для корректной работы сервера IPA с пользователями доверенного домена AD нужно обеспечить доступ сервиса sssd к /etc/krb5.keytab.

2) Для входа AD пользователя в ALT рабочую станцию из IPA имя пользователя вводится в формате DOMC\username или DOMC.TESTC\username или username@domc username@domc.testc.

3) Для входа IPA пользователя в Windows рабочую станцию из AD имя пользователя вводится в формате DOMF.TESTF\username.

13. НАСТРОЙКА СЛУЖБ DNS (BIND)

13.1. Общие сведения

Службы DNS (Bind) в ОС Альт СП отвечают за преобразование доменного имени в IP-адрес и за обратную операцию.

Если локальная сеть не подключена к сети Интернет, вполне возможно, что внутренний DNS-сервер в ней не нужен. За преобразование доменного имени в IP-адрес и обратно в различные механизмы, лишь один из которых базируется на службе доменных имен. В самом простом случае имена всех компьютеров вместе с их адресами можно записать в файл `/etc/hosts`. Порядок просмотра различных пространств имен указывается в файле `/etc/nsswitch.conf`. Строка `hosts: files dns` этого файла предписывает приложениям, пользующимся стандартной функцией `gethostbyname()` сначала обратиться в `/etc/hosts`, а затем отправить запрос к DNS-серверу.

Если задачу преобразования имен в адреса взял на себя провайдер, собственный DNS-сервер также не требуется. В этом случае на всех компьютерах в качестве сервера имен указывается сервер провайдера (поле «nameserver» в файле `/etc/resolv.conf`), к которому и идут все запросы. Даже если внутренняя сеть организована согласно RFC1918 (т. н. интранет) и адреса компьютеров в ней недоступны из внешней сети, DNS-запросы во внешнюю сеть будут выполняться. Между собой компьютерам предлагается общаться с помощью `/etc/hosts` или IP-адресов.

Некоторые службы и системные утилиты, работающие с доменными именами, запускаются в ОС Альт СП с использованием chroot (в каталоге `/var/resolv`), поэтому после изменения упомянутых файлов рекомендуется выполнить команду:

```
update_chrooted conf
```

Собственную службу доменных имен рекомендуется настраивать для решения задач, описанных ниже.

13.2. Уменьшение времени ответа на DNS-запрос абонентов внутренней сети

Если канал подключения к сети Интернет обладает большим временем задержки, то работа с данными, включающими в себя много доменных имен (например, с www-страницами) может замедлиться. Общий объем трафика при этом не вырастет, поскольку система доменных имен – распределенная база данных, поддерживающая механизм кеширования запросов. Первое обращение к кеширующему DNS-серверу приводит к выполнению рекурсивного запроса: опрашивается сервер более высокого уровня, который, если не знает ответа, передаст запрос дальше. Результат запроса сохраняется в кэше, и таким образом все последующие обращения именно к этой записи дальше кеширующего сервера не уйдут. Время жизни (Time To Live, TTL) записи в кэше определяется хозяином запрошенного доменного имени. По истечении TTL запись из кэша удаляется.

13.3. Именование компьютеров в интранет-сети

Решение этой задачи может потребоваться, если среди компьютеров внутренней сети есть свои серверы (например, корпоративный www-сервер), к которым другие компьютеры обращаются по доменному имени.

Поскольку адреса такой сети не пойдут дальше межсетевого экрана, допускается использовать имя какого угодно – в том числе несуществующего – домена и сделать соответствующие записи `/etc/hosts`. Поддержание в актуальном состоянии файла `/etc/hosts` на всех компьютерах – нелегкая задача, и лучше все-таки воспользоваться DNS-сервером.

13.4. Примеры использования DNS-сервера Bind

Решение обеих поставленных задач предоставляется настройкой DNS-сервера Bind.

В ОС Альт СП сервер Bind запускается с использованием `chroot`. В `/etc` от Bind остается символьная ссылка на главный файл настроек `named.conf`. Корневым каталогом является `/var/lib/bind`, где у Bind есть собственный каталог `/etc` содержащий набор включаемых друг в друга конфигурационных файлов, каталоги `/var` и `/dev`.

Примечание. Все пути к файлам и каталогам в настройках Bind начинаются именно из этого каталога, и `/zone` соответствует `/var/lib/bind/zone`.

Чтобы запустить named в кеширующем режиме, достаточно раскомментировать и заполнить раздел настройки forwarders (вышестоящие серверы) в файле `/var/lib/bind/etc/options.conf`.

В связи с возможными ограничениями на право обращаться к серверу с обычными и рекурсивными запросами (настройки `allow-query` и `allow-recursion`), допускается раскомментировать установки по умолчанию. Эти настройки открывают доступ только абонентам локальных сетей, к которым компьютер подключен непосредственно:

```
# grep allow- /var/lib/bind/etc/options.conf
// allow-query { localnets; };
// allow-recursion { localnets; };
```

Использование Bind для полноценного именования компьютеров в локальной сети требует создания двух зон (прямой и обратной), содержащих в виде записей определенного формата информацию о доменных именах компьютеров и об их роли в этих доменах.

Каждая зона должна включать запись типа SOA (StateOfAuthority, сведения об ответственности). В этой записи определяются основные временные и административные параметры домена, в том числе электронный адрес лица, ответственного за домен (администратора) и серийный номер зоны.

Серийный номер – число в диапазоне от 0 до 4294967295 (232); каждое изменение, вносимое в зону, должно сопровождаться увеличением этого номера. Обнаружив увеличение серийного номера, кеширующие и вторичные серверы признают все закешированные записи из этой зоны устаревшими. Удобно использовать формат «годмесяцчисловерсия», где все числа, кроме года, двузначные, а версия может обнуляться раз в день, соответствовать времени (например, по формуле 100*(часы*60+минуты)/(60*24) или иметь сквозную нумерацию (в этом случае появляется сложность с переходом от версии 99 к версии 100, то есть 0).

Даже если серийный номер генерируется автоматически, рекомендуется пользоваться этим форматом, наглядно отражающим время создания зоны.

Пример зоны, не содержащей ничего, кроме записи SOA и обязательной записи типа NS (NameServer), находится в файле `/var/lib/bind/zone/empty`.

Кроме записи типа SOA, в каждой зоне должна быть хотя бы одна запись типа NS, указывающая адрес DNS-сервера, авторитативного в этом домене (как минимум – адрес сервера, на котором запущен named).

Несколько зон включаются в настройку Bind автоматически (файл `/var/lib/bind/etc/rfc1912.conf`). Они нужны для обслуживания сети, привязанной к сетевой заглушке (127.0.0.1/8). Имя домена, который обслуживается зоной, задается в файле настроек, а в самом файле зоны можно использовать относительную адресацию (без «.» в конце имени), благодаря чему операция переименования домена выполняется редактированием одной строки.

В ОС Альт СП рекомендуется добавлять описания зон в конфигурационный файл `/var/lib/bind/etc/local.conf`.

Прямая зона нужна для преобразования доменного имени в IP-адрес – операции, нужной многим программам постоянно. Большинство записей в прямой зоне – типа A (Address) – предназначены именно для этого. Другие часто встречающиеся типы записей – это CNAME (CanonicalName, настоящее имя), позволяющий привязать несколько дополнительных имен к одному, и MX (MaileXchange, обмен почтой), указывающий, куда пересылать почтовые сообщения, в поле адресат которых встречается определенное доменное имя.

Пример прямой зоны для домена `internal.domain.net` (незначащие поля соответствующих файлов заменены на «. . .»):

```
# cat /var/lib/bind/etc/local.conf
. . .
zone "internal.domain.net" {
type master;
file "internal.domain.net";
};
. . .
# cat /var/lib/bind/zone/internal.domain.net
$TTL 1D
@ IN SOA server root.server (
     2013082202 ; serial
```

```
        12H ; refresh
        1H ; retry
        1W ; expire
        1H ; ncache
)
        IN NS server
        MX 10 server
server A 10.10.10.1
www CNAME server
mail CNAME server
jack A 10.10.10.100
jill A 10.10.10.101
```

В этом примере используются правила по умолчанию: если в записи некоторое поле опущено, оно наследуется от предыдущей. Так, вместо A допускается написать INA, а вместо MX – @ IN MX, где @ означает имя домена, указанное в конфигурационном файле.

Как видно из примера, всю работу в сети делает компьютер с адресом 10.10.10.1, он же `server.internal.domain.net`, он же `www.internal.domain.net` и `mail.internal.domain.net`. Несмотря на наличие среди CNAME этого сервера имени «mail», MX-запись указывает на действительный адрес – так рекомендовано RFC (Request for Comments, документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, широко применяемые во всемирной сети).

Для того чтобы преобразовывать IP-адреса в доменные имена, у каждой сети должна быть обратная зона. Если такой зоны нет, и в файле `/etc/hosts` тоже ничего не написано, операция не выполнится. Такое преобразование нужно гораздо реже и в основном по соображениям административным: для того, чтобы выяснить принадлежность компьютера (с которого, допустим, пытаются атаковать сервер) по его IP-адресу. Некоторые почтовые серверы проверяют, содержится ли IP-адрес машины, передающей сообщение, в обратной зоне и похоже ли полученное доменное имя на то, что указано в сообщении, и при несовпадении отказываются принимать письмо.

Обратная зона состоит почти целиком из записей типа PTR (Pointer, указатель). Чтобы не умножать сущностей, решено было не вводить новый способ работы сервера имен и представить обратное преобразование IP-адреса как прямое преобразование доменного имени специального вида.

Например, чтобы выяснить доменное имя компьютера с адресом «1.2.3.4», нужно запросить информацию о доменном имени `4.3.2.1.in-addr.arpa`. Таким образом, каждой подсети класса C (или выше) соответствует определенный домен, в котором можно найти ответ.

Обратная зона для домена, приведенного выше:

```
# cat /var/lib/bind/etc/local.conf

. . .
zone "12.11.10.in-addr.arpa" {
type master;
file "12.11.10.in-addr.arpa";
};
. . .
# cat /var/lib/bind/zone/12.11.10.in-addr.arpa
$TTL 1D
@ IN SOA server.internal.domain.net. root.server.internal.domain.net (
      2013082201 ; serial
      12H ; refresh
      1H ; retry
      1W ; expire
      1H ; ncache
)
      IN NS server.internal.domain.net.
0 PTR internal.domain.net.
1 PTR server.internal.domain.net.
100 PTR jack.internal.domain.net.
101 PTR jill.internal.domain.net.
```

Относительные адреса, использованные в левой части записей PTR, раскрываются в полные следующего вида: `адрес.12.11.10.in-addr.arpa`, а в правой части используются полные, которые могут указывать на имена в разных доменах.

Проверить синтаксическую правильность конфигурационного файла и файла зоны можно с помощью утилит named-checkconf и named-checkzone, входящих в пакет bind. Они же используются при запуске службы командой `service bind start`.

Стоит иметь ввиду, что, в отличие от прямых зон, обратные описывают административную принадлежность компьютеров, но сами принадлежат хозяину сети (как правило, провайдеру).

Существует особого рода затруднение, связанное с работой DNS-сервера уже не во внутренней сети, а в сети Интернет. Связано это с тем, что подсети класса С (сети /24, в которых сетевая маска занимает 24 бита, а адрес компьютера – 8) выдаются только организациям, способным такую подсеть освоить (в сети класса С 254 абонентских IP-адреса, один адрес сети и один широковещательный адрес). Чаще всего выдаются совсем маленькие подсети – от /30 (на два абонентских адреса) до /27 (на 30 адресов) – или другие диапазоны, сетевая маска которых не выровнена по границе байта. Таких подсетей в обратной зоне получится несколько, а возможности просто разделить ее, отдав часть адресов в администрирование хостам, нет. Провайдер в таких случаях пользуется RFC2317, предписывающем в обратной зоне заводить не записи вида PTR, а ссылки CNAME на адреса в «классифицированных» обратных зонах специального вида. Обратное преобразование становится двухступенчатым, зато администрирование каждой классифицированной зоны можно отдать хосту.

DNS-сервер, отвечающий на запросы из глобальной сети, должен быть зарегистрирован в родительском домене. Правила требуют, чтобы при регистрации домена было указано не менее двух DNS-серверов, которые будут его обслуживать.

Из всех зарегистрированных серверов (записей типа NS в родительской зоне) только одна соответствует первичному (master) серверу, а остальные – вторичным (slave). Для внешнего пользователя вторичный сервер не отличается от первичного, отличия состоят только в способе администрирования: все изменения вносятся в зоны первичного сервера, а вторичный только кеширует эти зоны, целиком получая их по специальному межсерверному протоколу. Полученная зона складывается в файл, редактировать который бессмысленно: первичный сервер при изменении зоны рассылает всем своим вторичным указание скачать ее заново. Право на скачивание зоны можно ограничить настройкой allow-transfer (как правило, в ней перечисляются адреса вторичных серверов).

Пример задания вторичного сервера в файле настроек:

```
// We are a slave server for eng.example.com
zone "eng.example.com" {
type slave;
file "slave/eng.example.com";
// IP address of eng.example.com master server
masters { 192.168.4.12; };
};
```

Вторичный сервер рекомендуется размещать в сети, отличной от той, в которой помещается первичный, – так повышается надежность обработки запроса (если один сервер недоступен, возможно, ответит второй) и возрастает скорость распространения записей по кэшам промежуточных серверов.

Проверку работоспособности, доступности и вообще самочувствия DNS-сервера рекомендуется выполнять утилитой dig из пакета bind-utils, которая выдает максимум информации о том, что происходило с запросом (для информации об обратном преобразовании нужно добавить ключ `-x`):

```
dig basealt.ru
; <<>> DiG 9.10.4-P5 <<>> basealt.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32751
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;basealt.ru. IN A
;; ANSWER SECTION:
basealt.ru.  86400 IN A 194.107.17.41
;; Query time: 1177 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Mar 01 10:07:17 MSK 2017
;; MSG SIZE rcvd: 55
```

Можно также использовать утилиту host из того же пакета, например:

```
host basealt.ru
basealt.ru has address 194.107.17.41
```

Для выяснения административной принадлежности тех или иных доменов и сетей можно воспользоваться утилитой whois из одноименного пакета, которая обращается к специальной сетевой базе данных (не имеющей отношения к DNS).

14. 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.

14.1. Установка сервера PostgreSQL

Перед установкой Zabbix должен быть установлен и запущен сервер PostgreSQL, с созданным пользователем zabbix и созданной базой zabbix.

Установить пакеты:

```
# apt-get install postgresql15-server zabbix-server-pgsql
```

где `15` – актуальная версия пакета.

Подготовить к запуску и настроить службы PostgreSQL, для этого нужно 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 путь будет отличаться, версия помечена *):

```
# su - postgres -s /bin/sh -c 'psql -U zabbix -f
/usr/share/doc/zabbix-common-database-pgsql-*/schema.sql zabbix'
# если вы создаете базу данных для Zabbix прокси, следующие
команды выполнять не нужно
# 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'
```

14.2. Установка Apache2

Установить пакеты:

```
# apt-get install apache2 apache2-mod_php8.1
```

Добавить в автозапуск и запустить apache2:

```
# systemctl enable --now httpd2
```

14.3. Установка PHP

Установить пакеты:

```
# apt-get install php8.1-mbstring php8.1-sockets php8.1-gd2 php8.1-xmlreader php8.1-pgsql php8.1-ldap
```

В файле `/etc/php/8.1/apache2-mod_php/php.ini` изменить некоторые опции php:

```
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
```

П р и м е ч а н и е . Актуальная версия PHP может быть другой.

Перезапустить apache2:

```
# systemctl restart httpd2
```

14.4. Установка и настройка Zabbix-сервера

Установить, если еще не установлены, пакеты:

```
# apt-get install zabbix-server-pgsql fping
```

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
```

14.5. Установка веб-интерфейса Zabbix

Установить метапакет:

```
# apt-get install zabbix-phpfrontend-apache2-mod_php8.1
```

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 веб-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.

Для начала установки нужно выбрать язык установки и нажать на кнопку «Далее» (рис. 427), что осуществит переход на страницу проверки предварительных условий.

Нужно доустановить то, что требуется и перейти на следующую страницу.

Здесь нужно ввести параметры подключения к базе данных (параметры подключения нужно указывать такие же, как у Zabbix-сервера). По умолчанию в качестве «Схемы базы данных» («Database schema») нужно указать «public» (рис. 428).

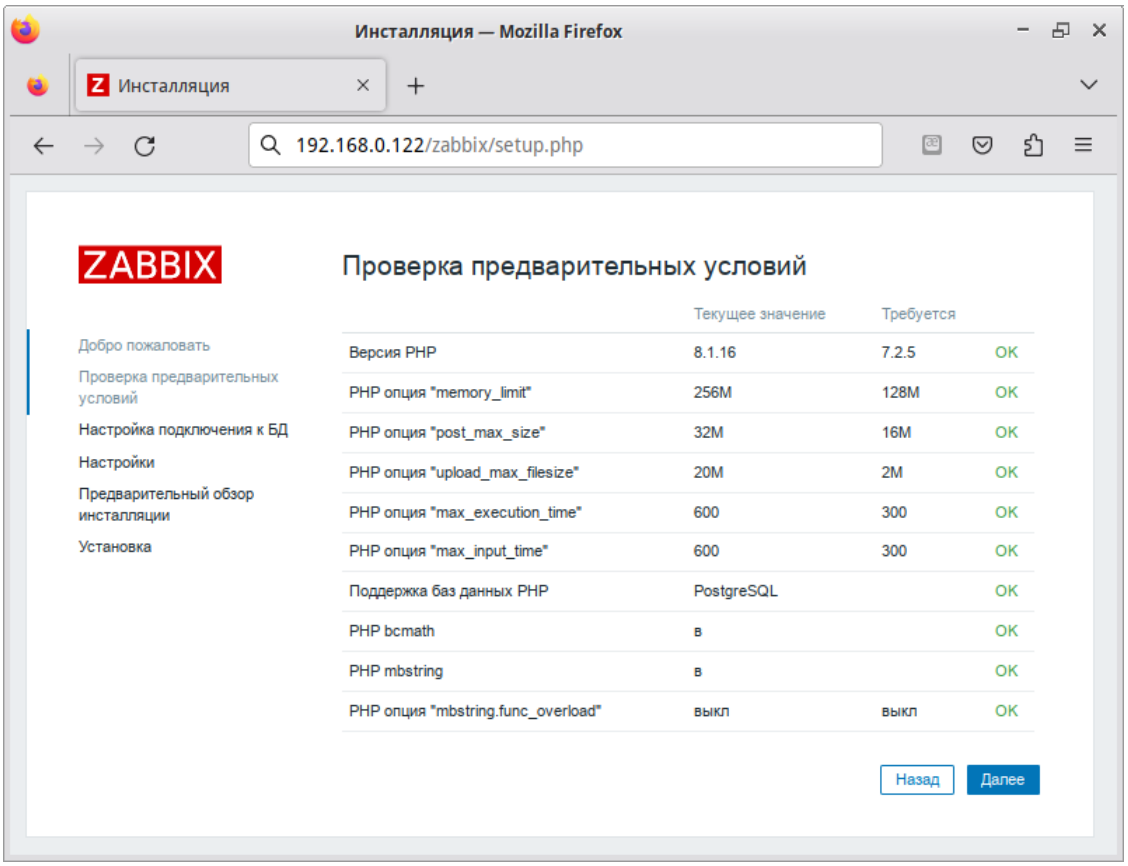


Рис. 427

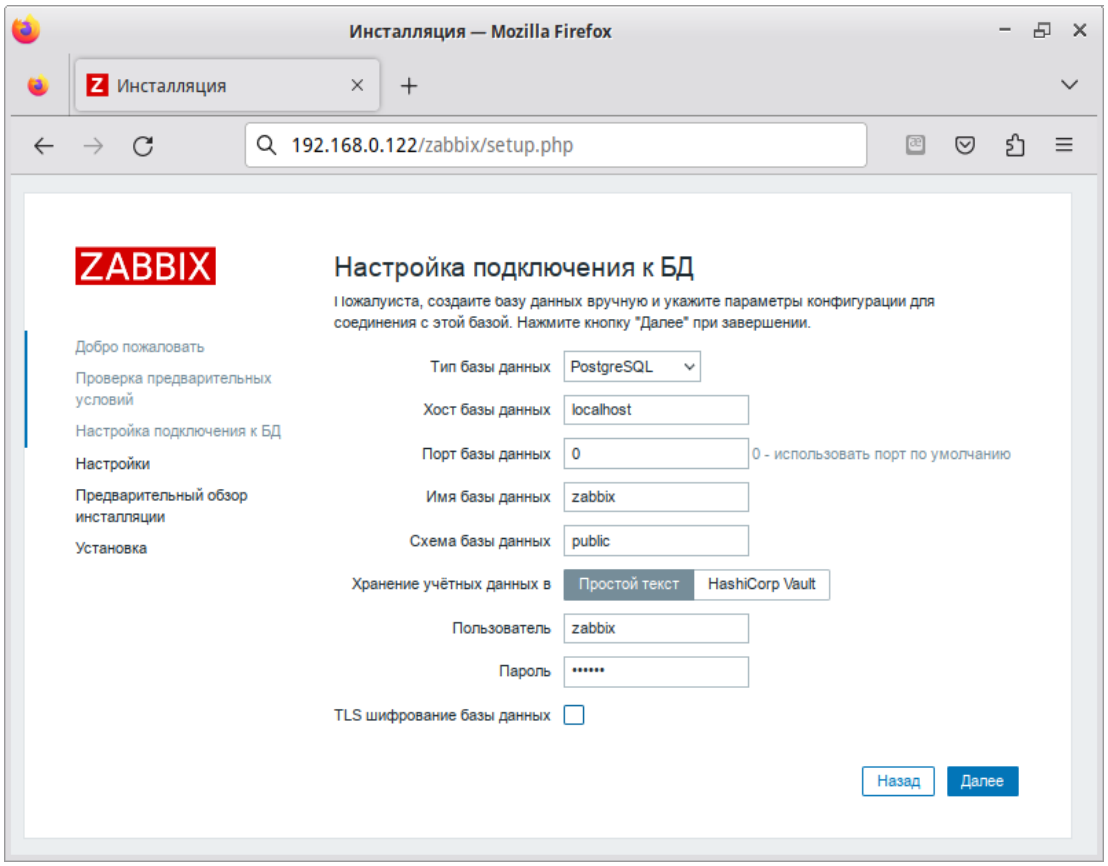


Рис. 428

Примечание. Если выбрана опция «Шифрование TLS базы данных» («Database TLS encryption»), то в форме появятся дополнительные поля для настройки TLS-соединения с базой данных.

Далее нужно задать имя сервера и завершить установку (рис. 429).

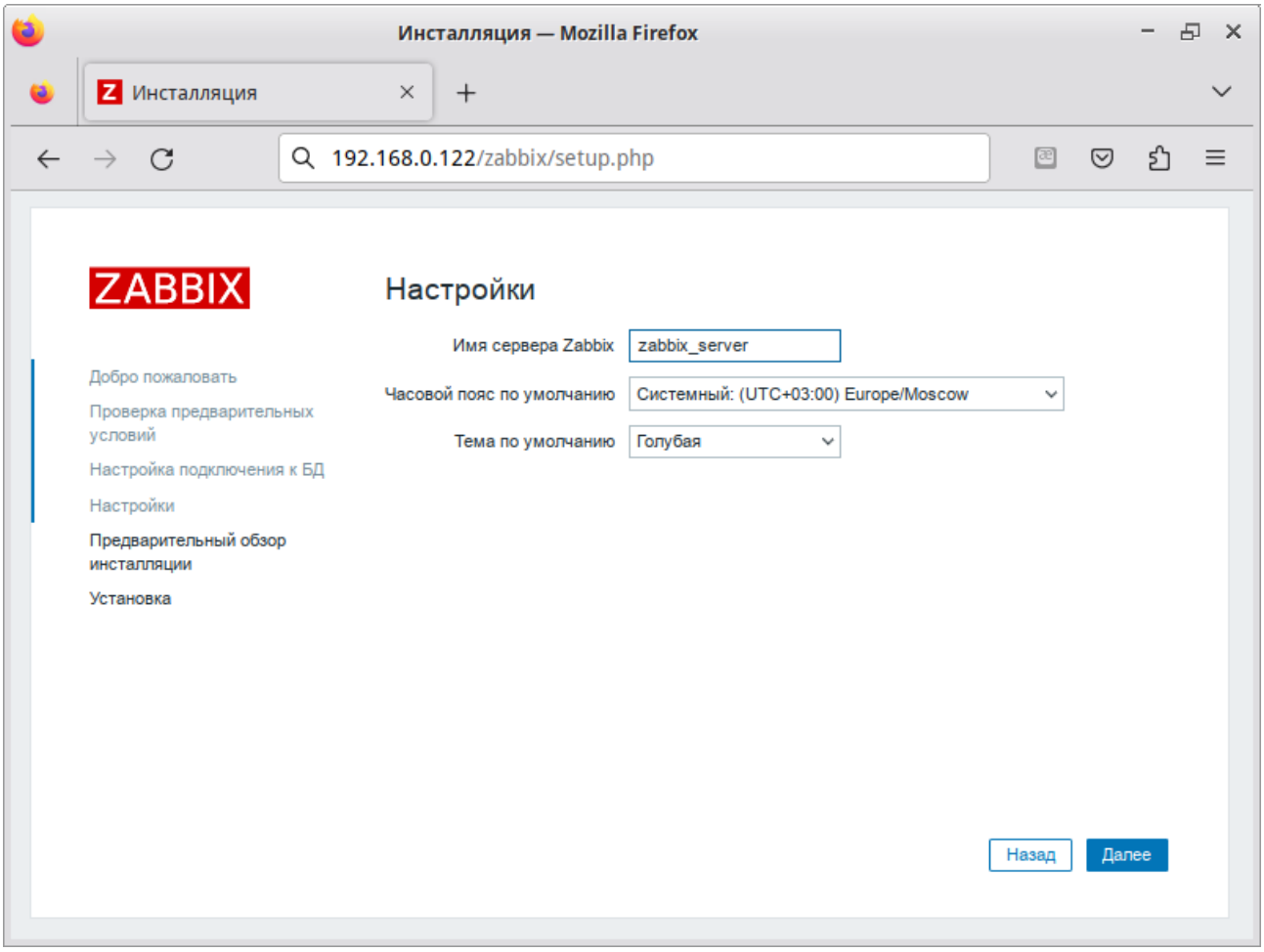


Рис. 429

После окончания установки на экране будет отображаться форма входа в веб-интерфейс управления системой мониторинга (рис. 430) `http://IP-сервера/zabbix`. Параметры доступа по умолчанию:

`Логин: Admin`

`Пароль: zabbix`

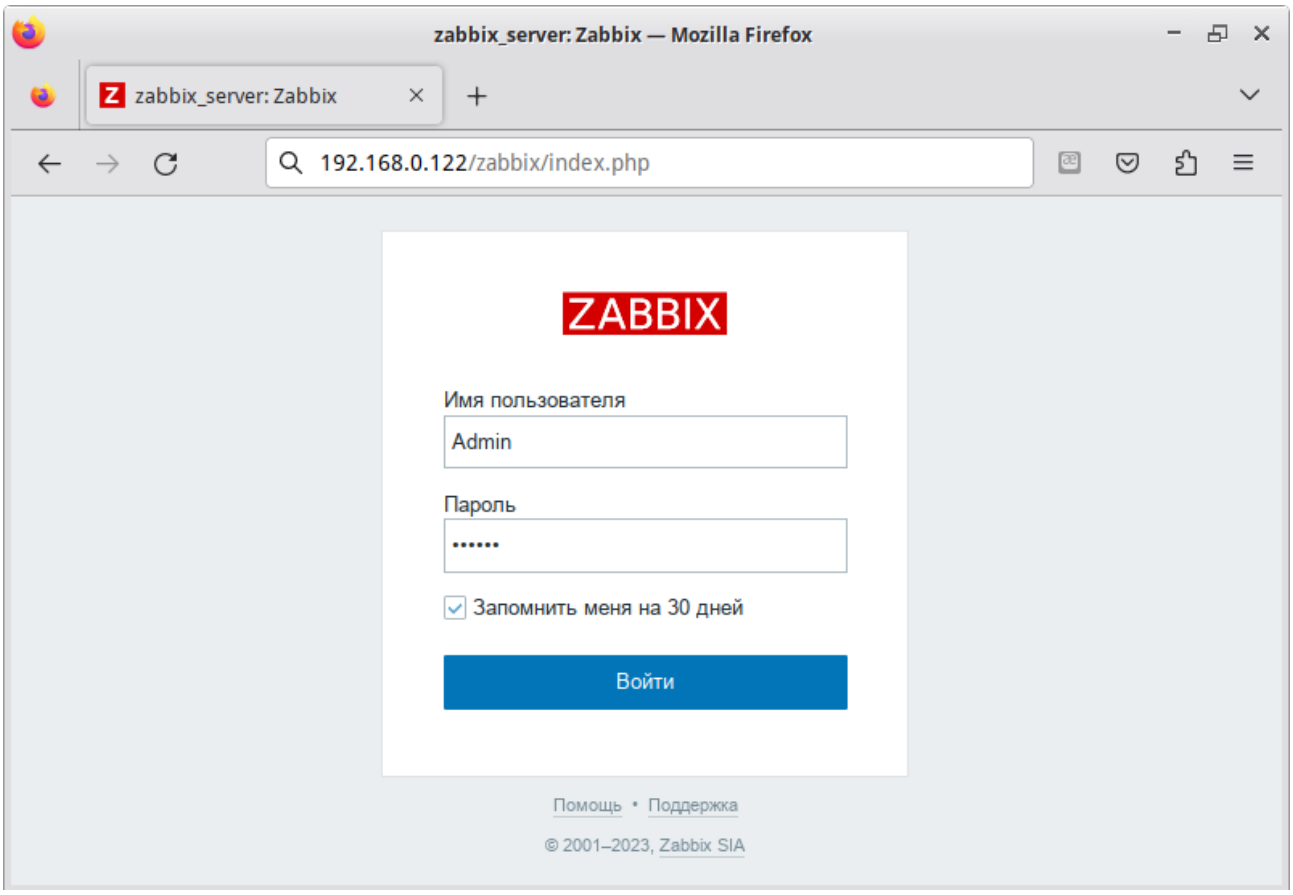


Рис. 430 – Вход в веб-интерфейс управления системой мониторинга

Войдя в систему, нужно сменить пароль администратора, завести других пользователей и затем можно переходить к настройкам 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, Zabbix-сервер использует информацию, получаемую от агентов. Чтобы добавить новый узел, следует установить на узел, который нужно мониторить Zabbix-агент (п. 14.6) и добавить новый хост на Zabbix-сервере (п. 14.7, п. 14.8).

14.6. Установка Zabbix-агента (клиента)

Для установки Zabbix-агента нужно выполнить команду:

```
# 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 параметры сервера:

```
Server=<IP-сервера>
ServerActive=<IP-сервера>
Hostname=HostK.example.test
```

`HostK.example.test` – имя узла мониторинга, которое будет указано на Zabbix-сервере.

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
```

14.7. Добавление нового хоста на Zabbix-сервере

Каждый хост нужно зарегистрировать на Zabbix-сервере, сделать это можно, используя веб-интерфейс.

Информация о настроенных узлах сети в Zabbix доступна в разделе меню «Настройка» → «Узлы сети». Для добавления нового узла сети следует нажать на кнопку «Создать узел сети» (рис. 431).

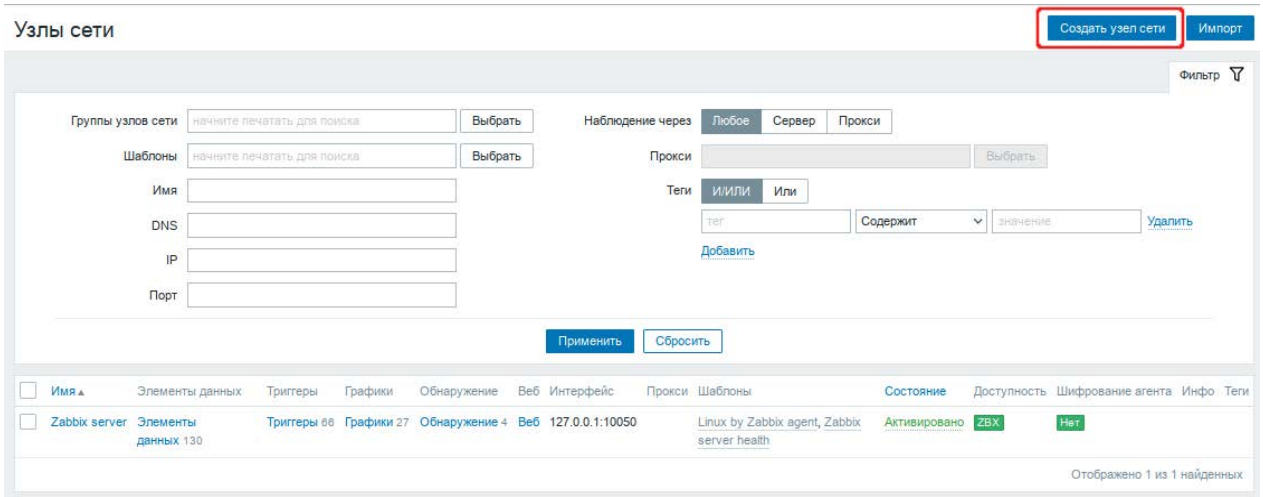


Рис. 431

В открывшемся окне нужно заполнить поля «Имя узла сети» и «IP адрес» согласно данным добавляемого хоста. Затем следует выбрать шаблон «Linux by Zabbix agent», добавить хост в определенную группу, выбрав одну из них из списка, либо создав новую группу (рис. 432).

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, а не индивидуально узлам сети. Поэтому узел сети должен принадлежать хотя бы одной группе.

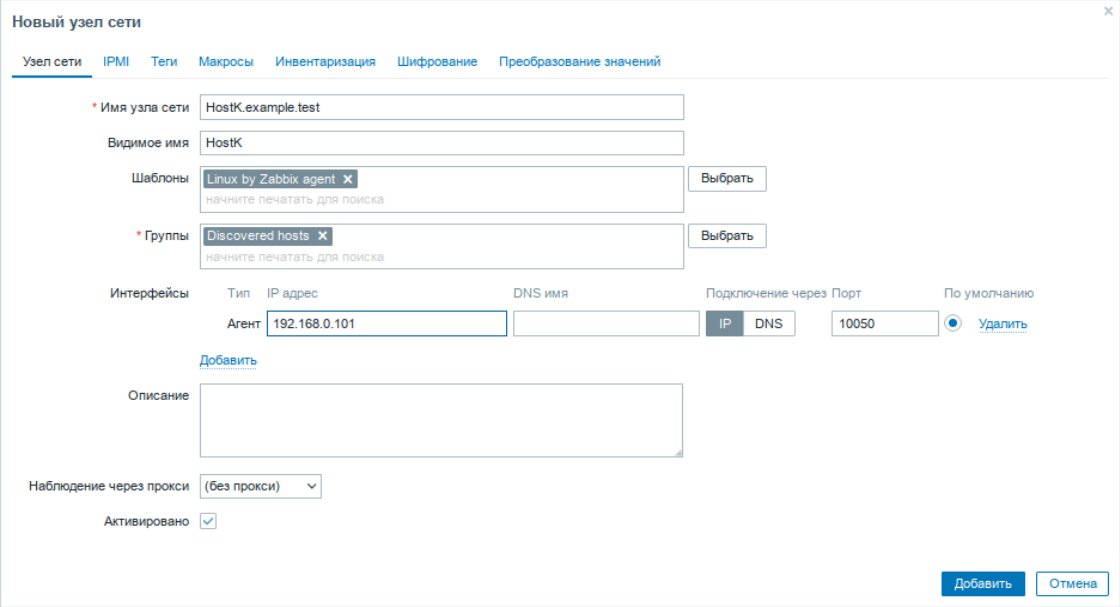


Рис. 432

Получение первых данных может занять до 60 секунд. Для того чтобы просмотреть собранные данные нужно перейти в раздел «Мониторинг» → «Последние данные», выбрать в фильтре нужный узел сети и нажать на кнопку «Применить» (рис. 433).

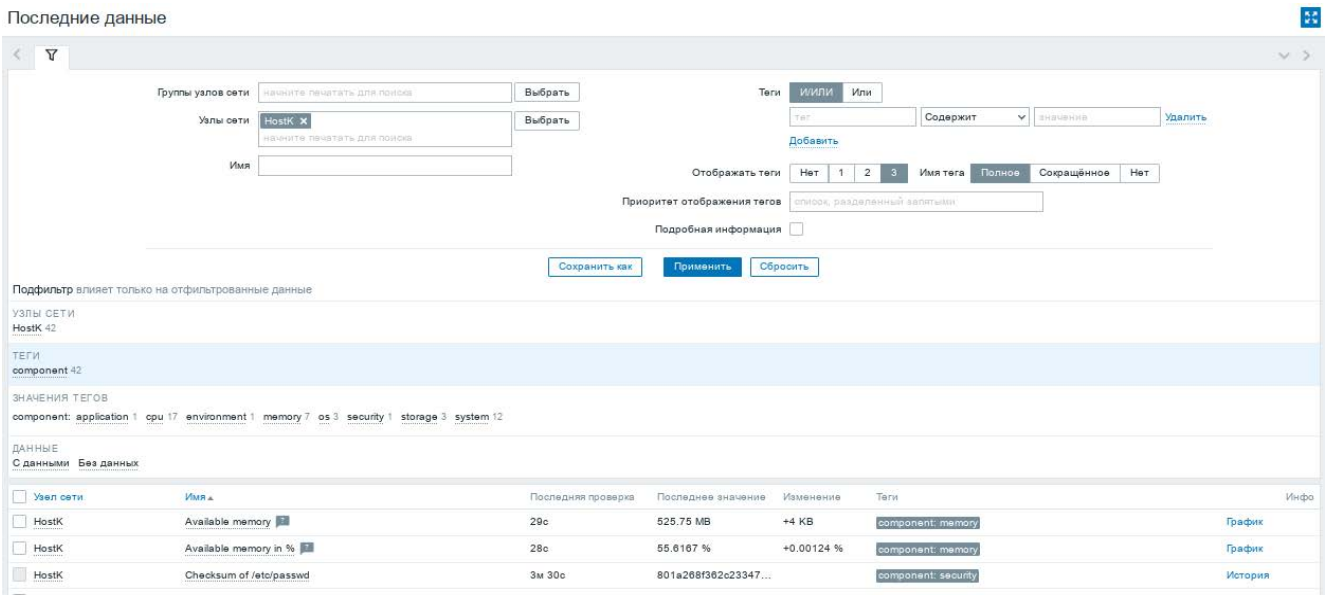


Рис. 433

14.8. 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, перейти в раздел «Настройка» → «Действия» → «Действия авторегистрации»» и нажать на кнопку «Создать действие» (рис. 434).

На открывшейся странице на вкладке «Действия» заполнить поле «Имя». В поле «Условия» следует задать правила, по которым будут идентифицироваться регистрируемые хосты (рис. 435).

На вкладке «Операции» в поле «Операции» следует добавить правила, которые нужно применить при регистрации хоста. Например, для добавления узла, добавления его к группе «Discovered hosts» с присоединением к шаблону «Linux generic by Zabbix agent» (рис. 436).

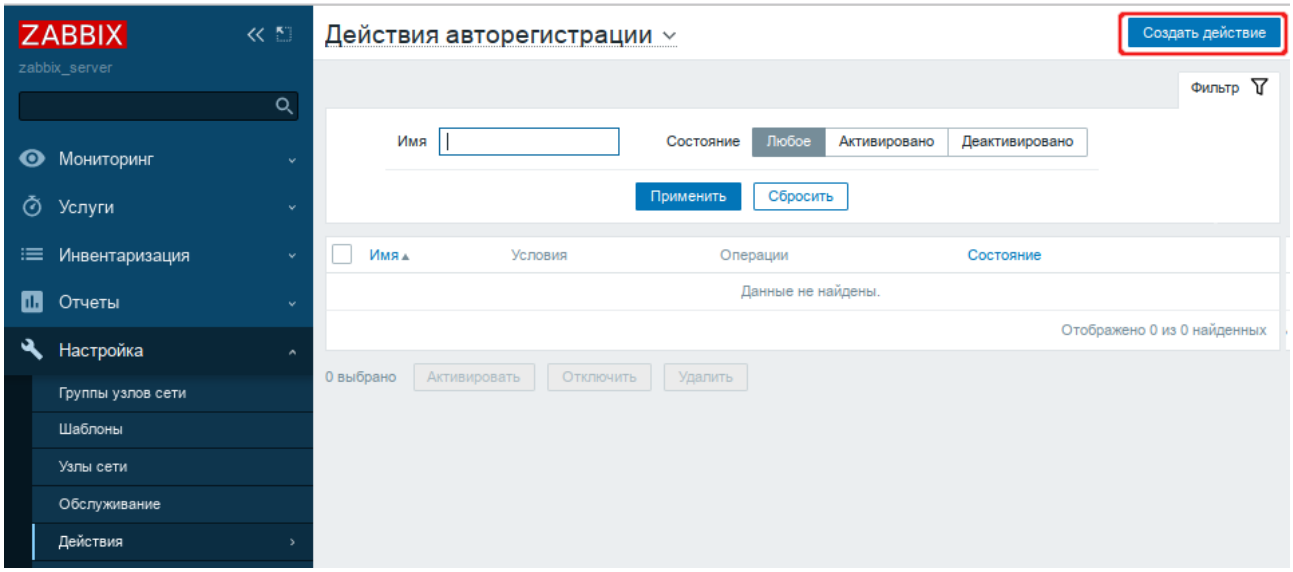


Рис. 434

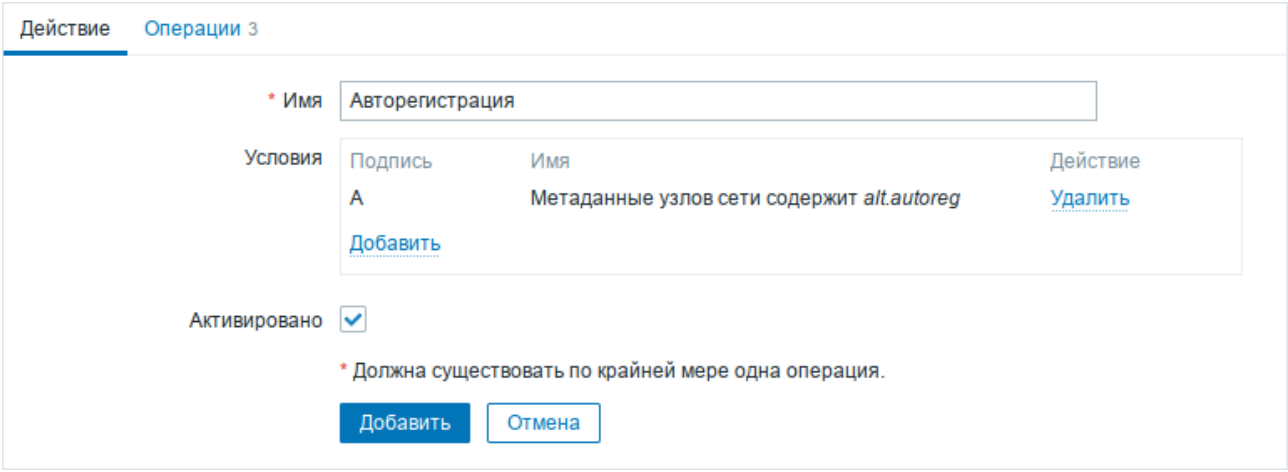


Рис. 435

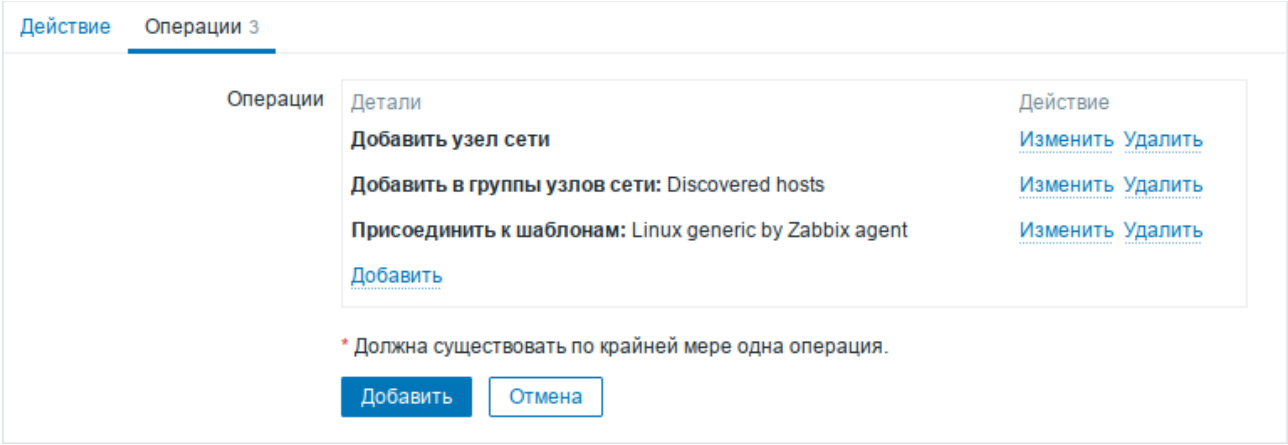


Рис. 436

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:

```
# systemctl restart zabbix_agentd.service
```

15. ОТКАЗОУСТОЙЧИВЫЙ КЛАСТЕР (HIGH AVAILABILITY) НА ОСНОВЕ PACEMAKER

Pacemaker – менеджер ресурсов кластера (Cluster Resource Manager), задачей которого является достижение максимальной доступности управляемых им ресурсов и защита их от сбоев как на уровне самих ресурсов, так и на уровне целых узлов кластера.

Ключевые особенности Pacemaker:

- обнаружение и восстановление сбоев на уровне узлов и сервисов;
- возможность гарантировать целостность данных путем ограждения неисправных узлов;
- поддержка одного или нескольких узлов на кластер;
- поддержка нескольких стандартов интерфейса ресурсов (все, что может быть написано сценарием, может быть кластеризовано);
- независимость от подсистемы хранения – общий диск не требуется;
- поддержка кворумных и ресурсозависимых кластеров;
- автоматически реплицируемая конфигурация, которую можно обновлять с любого узла;
- возможность задания порядка запуска ресурсов, а также их совместимости на одном узле;
- поддерживает расширенные типы ресурсов: клоны (когда ресурс запущен на множестве узлов) и дополнительные состояния (master/slave и подобное);
- единые инструменты управления кластером с поддержкой сценариев.

Архитектура Pacemaker представляет собой три уровня:

- кластеронезависимый уровень – на этом уровне располагаются ресурсы и их скрипты, которыми они управляются и локальный демон, который скрывает от других уровней различия в стандартах, использованных в скриптах;
- менеджер ресурсов (Pacemaker) – реагирует на события, происходящие в кластере: отказ или присоединение узлов, ресурсов, переход узлов в сервисный режим и другие административные действия. Pacemaker исходя из

сложившейся ситуации делает расчет наиболее оптимального состояния кластера и дает команды на выполнения действий для достижения этого состояния (остановка/перенос ресурсов или узлов);

- информационный уровень (Corosync) – на этом уровне осуществляется сетевое взаимодействие узлов, т. е. передача сервисных команд (запуск/остановка ресурсов, узлов и т. д.), обмен информацией о полноте состава кластера (quorum) и т. д.

Узел (node) кластера представляет собой физический сервер или виртуальную машину с установленным Pacemaker. Узлы, предназначенные для предоставления одинаковых сервисов, должны иметь одинаковую конфигурацию.

Ресурсы, с точки зрения кластера, это все используемые сущности – сервисы, службы, точки монтирования, тома и разделы. При создании ресурса потребуется задать его класс, тип, провайдера и собственно имя с дополнительными параметрами. Ресурсы поддерживают множество дополнительных параметров: привязку к узлу (resource-stickiness), роли по умолчанию (started, stoped, master) и т. д. Есть возможности по созданию групп ресурсов, клонов (работающих на нескольких узлах) и т. п.

Связи определяют привязку ресурсов к узлу (location), порядок запуска ресурсов (ordering) и совместное их проживание на узле (colocation).

Ниже приведена инструкция по установке и настройке кластера в ОС Альт СП Сервер (64 бит, AArch64 (ARMv8)).

15.1. Настройка узлов кластера

Рекомендации:

- дата и время между узлами в кластере должны быть синхронизированы;
- должно быть обеспечено разрешение имен узлов в кластере;
- сетевые подключения должны быть стабильными;
- у узлов кластера для организации изоляции (fencing) узла должны присутствовать функции управления питанием/перезагрузкой с помощью IPMI(ILO);

- следующие порты могут использоваться различными компонентами кластеризации: TCP-порты 2224, 3121 и 21064 и UDP-порт 5405 и должны быть открыты/доступны.

Примечание. В примере используется следующая конфигурация:
- ipa – первый узел кластера (IP 192.168.0.145/24);
- ipa2 – второй узел кластера (IP 192.168.0.113/24);
- 192.168.0.251 – виртуальный IP по которому будет отвечать один из узлов.

Дальнейшие действия следует выполнить на всех узлах кластера.

Примечание. Для изменения имени хоста без перезагрузки, можно воспользоваться утилитой hostnamectl:

```
# hostnamectl set-hostname ipa
```

Следует обеспечить взаимно однозначное прямое и обратное преобразование имен для всех узлов кластера. Желательно использовать DNS, в крайнем случае, можно обойтись соответствующими записями в локальных файлах `/etc/hosts` на каждом узле:

```
# echo "192.168.0.145 ipa" >> /etc/hosts
# echo "192.168.0.113 ipa2" >> /etc/hosts
```

Примечание. Перезагрузить ОС после изменения конфигурации.

Проверка правильности разрешения имен:

```
# ping ipa
PING ipa (192.168.0.145) 56(84) bytes of data.
64 bytes from ipa (192.168.0.145): icmp_seq=1 ttl=64 time=0.635 ms
# ping ipa2
PING ipa2 (192.168.0.113) 56(84) bytes of data.
64 bytes from ipa2 (192.168.0.113): icmp_seq=1 ttl=64 time=0.352 ms
```

При настройке ssh-подключения для root по ключу нужно убрать комментарии в файле `/etc/openssh/sshd_config` для строк:

```
PermitRootLogin without-password
PubkeyAuthentication yes
AuthorizedKeysFile                      /etc/openssh/authorized_keys/%u
/etc/openssh/authorized_keys2/%u  .ssh/authorized_keys  .ssh/authorized_k
eys2
PasswordAuthentication yes
```

Кроме того, полезно добавить в `/etc/openssh/sshd_config` директиву:

```
AllowGroups sshusers
```

создать группу sshusers:

```
# groupadd sshusers
```

и добавить туда пользователей, которым разрешено подключаться по ssh:

```
# gpasswd -a <username> sshusers
```

Создать и активировать новый ключ SSH без пароля:

```
# ssh-keygen -t ecdsa -f ~/.ssh/id_ecdsa -N ""
# cp ~/.ssh/id_ecdsa.pub ~/.ssh/authorized_keys
```

ВАЖНО

Незащищенные ключи SSH (без пароля) не рекомендуются для серверов, открытых для внешнего мира.

Установить ключ на другой узел:

```
# ssh-copy-id -i ~/.ssh/id_ecdsa.pub user@ipa2
```

```
user@ipa2 $ su -
ipa2 # cat /home/user/.ssh/authorized_keys >>
/root/.ssh/authorized_keys
ipa2 # exit
user@ipa2 $ exit
```

Убедиться, что теперь можно запускать команды удаленно, без пароля:

```
# ssh ipa2 -- uname -n
```

```
ipa2
```

15.2. Установка кластерного ПО и создание кластера

Для управления кластером Pacemaker можно использовать утилиты pcs или crm (пакет crmsh).

Установить на всех узлах пакеты:

```
# apt-get install corosync resource-agents pacemaker pcs
```

Примечание. Пакет resource-agent содержит агенты ресурсов (набор скриптов) кластера, соответствующие спецификации Open Cluster Framework (OCF), используемые для взаимодействия с различными службами в среде высокой доступности, управляемой менеджером ресурсов Pacemaker. Если есть нужность управлять дополнительными ресурсами, следует установить недостающий пакет resource-agents-*:

```
apt-cache search resource-agents*
```

Пакет pcs (pacemaker/corosync configuration system) – утилита для управления, настройки и мониторинга кластера. Управляется как через командную строку, так и через веб-интерфейс.

При установке Pacemaker автоматически будет создан пользователь hacluster. Для использования pcs, а также для доступа в веб-интерфейс нужно задать пароль пользователю hacluster (одинаковый на всех узлах):

```
# passwd hacluster
```

Запустить и добавить в автозагрузку службу pcsd:

```
# systemctl enable --now pcsd
```

Настроить аутентификацию (на одном узле):

```
# pcs host auth ipa ipa2 -u hacluster
```

```
Password:
ipa: Authorized
ipa2: Authorized
```

После этого кластером можно управлять с одного узла.

Создать кластер:

```
# pcs cluster setup newcluster ipa ipa2
```

```
No addresses specified for host 'ipa', using 'ipa'
No addresses specified for host 'ipa2', using 'ipa2'
Destroying cluster on hosts: 'ipa', 'ipa2'...
ipa2: Successfully destroyed cluster
ipa: Successfully destroyed cluster
Requesting remove 'pcsd settings' from 'ipa', 'ipa2'
ipa: successful removal of the file 'pcsd settings'
ipa2: successful removal of the file 'pcsd settings'
Sending 'corosync authkey', 'pacemaker authkey' to 'ipa', 'ipa2'
ipa: successful distribution of the file 'corosync authkey'
ipa: successful distribution of the file 'pacemaker authkey'
ipa2: successful distribution of the file 'corosync authkey'
ipa2: successful distribution of the file 'pacemaker authkey'
Sending 'corosync.conf' to 'ipa', 'ipa2'
ipa: successful distribution of the file 'corosync.conf'
ipa2: successful distribution of the file 'corosync.conf'
Cluster has been successfully set up.
```

Запустить кластер:

```
# pcs cluster start --all
```

```
ipa: Starting Cluster...
ipa2: Starting Cluster...
```

Настройка автоматического включения кластера при загрузке:

```
# pcs cluster enable --all
```

```
ipa: Cluster Enabled
ipa2: Cluster Enabled
```

Проверка состояния кластера:

```
# pcs status cluster
```

```
Cluster Status:
 Cluster Summary:
   * Stack: corosync
   * Current DC: ipa (version 2.0.3-alt2-4b1f869f0) - partition with quorum
   * Last updated: Mon Jan 25 15:52:33 2021
   * Last change:  Mon Jan 25 12:24:18 2021 by root via cibadmin on ipa2
   * 2 nodes configured
   * 0 resource instances configured
 Node List:
   * Online: [ ipa ipa2 ]

PCSD Status:
  ipa: Online
  ipa2: Online
```

Проверка синхронизации узлов кластера:

```
# corosync-cmapctl | grep members
```

```
runtime.members.1.config_version (u64) = 0
runtime.members.1.ip (str) = r(0) ip(192.168.0.145)
runtime.members.1.join_count (u32) = 1
runtime.members.1.status (str) = joined
runtime.members.2.config_version (u64) = 0
runtime.members.2.ip (str) = r(0) ip(192.168.0.113)
runtime.members.2.join_count (u32) = 2
```

Веб-интерфейс управления кластером расположен по адресу `https://<имя-компьютера>:2224` (в качестве имени компьютера можно использовать имя или IP-адрес одного из узлов в кластере). Потребуется пройти аутентификацию (логин и пароль учетной записи `hacluster`) (рис. 437).

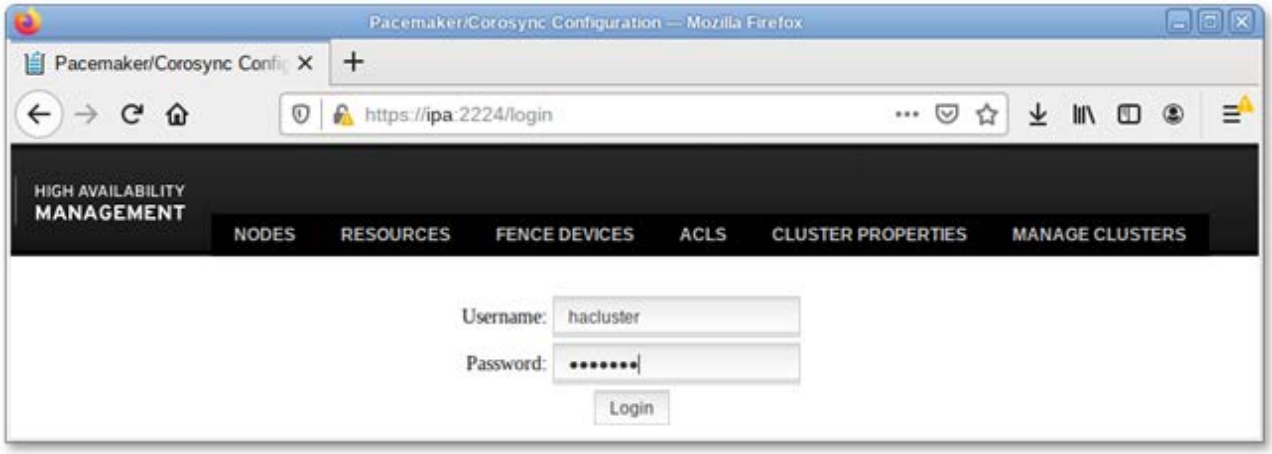


Рис. 437 – Аутентификация

После входа в систему на главной странице отображается страница «Управление кластерами». На этой странице перечислены кластеры, которые в настоящее время находятся под управлением веб-интерфейса. Чтобы добавить существующий кластер в веб-интерфейс, нужно нажать на кнопку «Add Existing» и ввести имя или IP-адрес любого узла в кластере. При выборе кластера отображается информация о кластере (рис. 438).

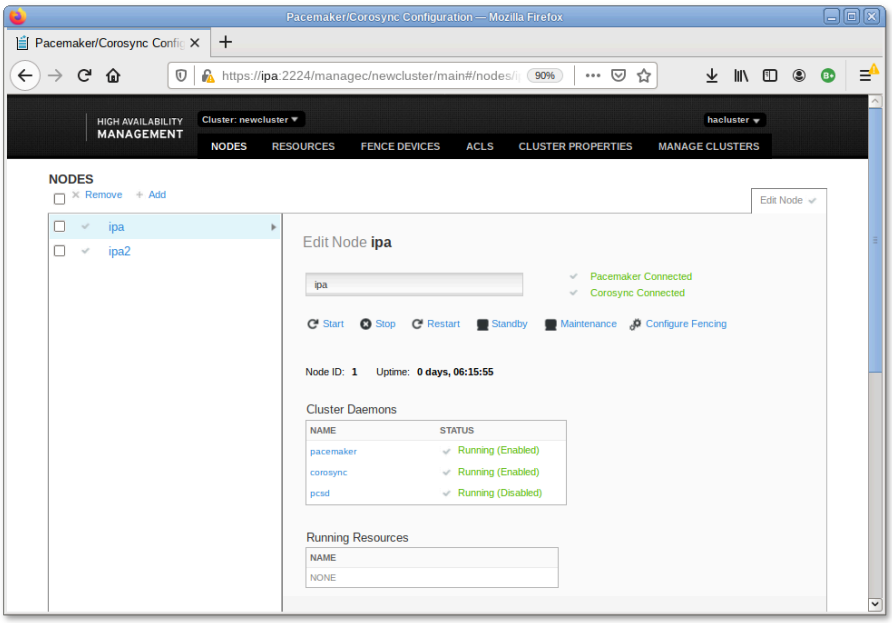


Рис. 438 – Информация о кластере

15.3. Настройка основных параметров кластера

Настройки кластера можно просмотреть, выполнив команду:

```
# pcs property
Cluster Properties:
 cluster-infrastructure: corosync
 cluster-name: newcluster
 dc-version: 2.0.3-alt2-4b1f869f0
 enable-acl: true
 have-watchdog: false
```

15.3.1. Кворум

Кворум определяет минимальное число работающих узлов в кластере, при котором кластер считается работоспособным. По умолчанию, кворум считается неработоспособным, если число работающих узлов меньше половины от общего числа узлов. Так как в данной инструкции узла всего два, то кворума не будет,

поэтому следует отключить эту политику:

```
# pcs property set no-quorum-policy=ignore
```

15.3.2. Настройка STONITH

Для корректной работы узлов с общим хранилищем, нужно настроить механизм STONITH. Этот механизм позволяет кластеру физически отключить не отвечающий на запросы узел, чтобы не повредить данные на общем хранилище. Отключить STONITH, пока он не настроен можно, выполнив команду:

```
# pcs property set stonith-enabled=false
```

ВАЖНО

В реальной системе нельзя использовать конфигурацию с отключенным STONITH. Отключенный параметр на самом деле не отключает функцию, а только лишь эмулирует ее срабатывание при определенных обстоятельствах.

15.3.3. Настройка IPaddr2

Настроим ресурс, который будет управлять виртуальным IP-адресом. Этот адрес будет мигрировать между узлами предоставляя одну точку входа к ресурсам, заставляя работать несколько узлов как одно целое устройство для сервисов.

Команда создания ресурса виртуального IP-адреса с именем ClusterIP с использованием алгоритма ресурсов ocf (каждые 20 минут производить мониторинг работы, в случае выхода из строя узла нужно виртуальный IP переключить на другой узел):

```
# pcs resource create ClusterIP ocf:heartbeat:IPaddr2 ip=192.168.0.251 cidr_netmask=24 op monitor interval=20s
```

Список доступных стандартов ресурсов:

```
# pcs resource standards
lsb
ocf
service
systemd
```

Список доступных поставщиков сценариев ресурсов OCF:

```
# pcs resource providers
heartbeat
pacemaker
redhat
```

Получить список всех агентов ресурсов, доступных для определенного поставщика OCF:

```
# pcs resource agents ocf:heartbeat
```

```
aliyun-vpc-move-ip
anything
AoEtarget
apache
asterisk
…
Xinetd
zabbixserver
ZFS
```

Статус кластера, с добавленным ресурсом:

```
# pcs status
Cluster name: newcluster
Cluster Summary:
  * Stack: corosync
  * Current DC: ipa2 (version 2.0.3-alt2-4b1f869f0) - partition with quorum
  * Last updated: Mon Jan 25 20:46:20 2021
  * Last change:  Mon Jan 25 20:46:11 2021 by root via cibadmin on ipa
  * 2 nodes configured
  * 2 resource instances configured

Node List:
  * Online: [ ipa ipa2 ]

Full List of Resources:
  * ClusterIP   (ocf::heartbeat:IPaddr2):    Started ipa

Daemon Status:
  corosync: active/enabled
  pacemaker: active/enabled
  pcsd: active/enabled
```

Если остановить кластер на узле ipa:

```
# pcs cluster stop ipa
```

```
ipa: Stopping Cluster (pacemaker)...
ipa: Stopping Cluster (corosync)...
```

ClusterIP начнет работать на ipa2 (переключение произойдет автоматически). Проверка статуса на втором узле:

```
# pcs status
```

```
Cluster name: newcluster
Cluster Summary:
  * Stack: corosync
```

```
  * Current DC: ipa (version 2.0.3-alt2-4b1f869f0) - partition
with quorum
  * Last updated: Mon Jan 25 20:56:00 2021
  * Last change:  Mon Jan 25 20:46:11 2021 by root via cibadmin
on ipa
  * 2 nodes configured
  * 2 resource instances configured

Node List:
  * Online: [ ipa2 ]
  * OFFLINE: [ ipa ]

Full List of Resources:
  * ClusterIP   (ocf::heartbeat:IPaddr2):    Started ipa2

Daemon Status:
  corosync: active/enabled
  pacemaker: active/enabled
  pcsd: active/enabaled
```

16. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ОС

16.1. Управление системными сервисами, основные команды

16.1.1. Сервисы

Сервисы – это программы, которые запускаются и останавливаются через инициализированные скрипты, расположенные в каталоге `/etc/init.d`. Многие из этих сервисов запускаются на этапе старта ОС Альт СП.

Каталог `/sbin/service` обеспечивает интерфейс (взаимодействие) пользователя с инициализированными скриптами. В свою очередь, скрипты обеспечивают интерфейс для управления сервисами, предоставляя пользователю опции для запуска, остановки, перезапуска, запроса состояния сервиса и выполнения других воздействий на сервис.

Инициализированный скрипт сервиса openssh имеет следующие опции:

```
/etc/init.d/sshd
Usage: sshd
{start|stop|reload|restart|condstop|condrestart|condreload|check|
status}
```

Текущее состояние всех системных служб в ОС Альт СП можно просмотреть с помощью команды `systemctl`:

```
systemctl
...
sshd.service
loaded active running   OpenSSH server daemon
  systemd-binfmt.service
loaded active exited    Set Up Additional Binary F
  systemd-fsck-root.service
loaded active exited    File System Check on Roo
...
```

Информация о запущенности и включенности сервисов может быть получена или изменена с помощью команды `systemctl`. Например, для службы удаленного доступа ssh установки по умолчанию выглядят следующим образом:

```
/sbin/systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded:   loaded   (/lib/systemd/system/sshd.service;   enabled;
```

```
vendor preset: ena
   Active: active (running) since Mon 2019-04-01 09:48:34 MSK; 4h
0min ago
  Process:   921   ExecStartPre=/usr/sbin/sshd   -t   (code=exited,
status=0/SUCCESS)
  Process: 904 ExecStartPre=/usr/bin/ssh-keygen -A (code=exited,
status=0/SUCCES
 Main PID: 942 (sshd)
   CGroup: /system.slice/sshd.service
           └─942 /usr/sbin/sshd -D
```

Сервис sshd запускается автоматически. Для того чтобы отключить его автоматический запуск сервиса, можно воспользоваться следующей опцией команды `systemctl`:

```
/sbin/systemctl disable sshd
```

Запуск, остановка, перезапуск и перезагрузка настроек служб выполняются соответственно командами:

```
/sbin/systemctl start <служба>
/sbin/systemctl stop <служба>
/sbin/systemctl restart <служба>
/sbin/systemctl reload <служба>
```

16.1.2. Команды

Далее приведены основные команды, использующиеся в ОС Альт СП:

- `ar` – создание и работа с библиотечными архивами;
- `at` – формирование или удаление отложенного задания (см. п. 16.8.2);
- `awk` – язык обработки строковых шаблонов;
- `batch` – планирование команд в очереди загрузки (см. п. 16.8.3);
- `bc` – строковый калькулятор;
- `chfn` – управление информацией учетной записи (имя, описание);
- `chsh` – управление выбором командного интерпретатора (по умолчанию – для учетной записи);
- `cut` – разбивка файла на секции, задаваемые контекстными разделителями;
- `df` – вывод отчета об использовании дискового пространства;
- `dmesg` – вывод содержимого системного буфера сообщений;
- `du` – вычисление количества использованного пространства элементов ФС;

- echo – вывод содержимого аргументов на стандартный вывод;
- egrep – поиск в файлах содержимого согласно регулярным выражениям;
- fgrep – поиск в файлах содержимого согласно фиксированным шаблонам;
- file – определение типа файла;
- find – поиск файла по различным признакам в иерархии каталогов (см. п. 16.5.1);
- gettext – получение строки интернационализации из каталогов перевода;
- grep – вывод строки, содержащей шаблон поиска (см. п. 16.4.4);
- groupadd – создание новой учетной записи группы;
- groupdel – удаление учетной записи группы;
- groupmod – изменение учетной записи группы;
- groups – вывод списка групп;
- gunzip – распаковка файла;
- gzip – упаковка файла;
- hostname – вывод и задание имени хоста;
- install – копирование файла с установкой атрибутов;
- ipcrm – удаление ресурса IPC;
- ipcs – вывод характеристик ресурса IPC;
- kill – прекращение выполнения процесса (см. п. 16.2.6);
- killall – удаление процессов по имени (см. п. 16.2.6);
- lpr – система печати;
- ls – вывод содержимого каталога (см. п. 16.3.1);
- lsb_release – вывод информации о дистрибутиве;
- m4 – запуск макропроцессора;
- md5sum – генерация и проверка MD5-сообщения;
- mknod – создание файла специального типа (см. п. 16.4.6);
- mktemp – генерация уникального имени файла;
- more – постраничный вывод содержимого файла;
- mount – монтирование ФС (см. п. 16.3.12);

- msgfmt – создание объектного файла сообщений из файла сообщений;
- newgrp – смена идентификатора группы;
- nice – изменение приоритета процесса перед его запуском (см. п. 16.2.4);
- nohup – работа процесса после выхода из системы (см. п. 16.2.3);
- od – вывод содержимого файла в восьмеричном и других видах;
- passwd – смена пароля учетной записи (см. п. 20.3);
- patch – применение файла описания изменений к оригинальному файлу;
- pidof – вывод идентификатора процесса по его имени;
- ps – вывод информации о процессах (см. п. 16.2.2);
- renice – изменение уровня приоритета процесса (см. п. 16.2.5);
- rm – удаление файлов или каталогов;
- sed – строковый редактор;
- sendmail – транспорт системы электронных сообщений;
- sh – командный интерпретатор;
- shutdown – команда останова системы;
- srm – безопасная перезапись/переименование/удаление целевого файла;
- su – изменение идентификатора запускаемого процесса (см. п. 20.2.4);
- sync – сброс системных буферов на носители;
- tar – файловый архиватор (см. п. 16.6.1);
- umount – размонтирование ФС;
- useradd – создание новой учетной записи или обновление существующей (см. п. 20.3);
- userdel – удаление учетной записи и соответствующих файлов окружения (см. п. 20.3);
- usermod – модификация информации об учетной записи (см. п. 20.3);
- w – список пользователей, кто в настоящий момент работает в системе и с какими файлами;
- who – вывод списка пользователей системы (см. п. 16.2.1).

Узнать об опциях команд можно с помощью команды man.

16.2. Администрирование многопользовательской и многозадачной среды

16.2.1. Команда who

Для получения списка пользователей, работающих в ОС, используется команда who, которая позволяет вывести в консоль идентификаторы активных пользователей, терминалы и время входа в систему.

Для получения списка пользователей, зарегистрировавшихся в системе, нужно выполнить команду who. Задавая различные опции, с помощью команды who можно получить информацию о времени начала и конца сеансов работы пользователей, перезагрузок, корректировках системных часов, а также о других процессах, порожденных процессом init.

Синтаксис команды who:

```
who [-u] [-T] [-l] [-H] [-q] [-p] [-d] [-b] [-r] [-t] [-a] [-s] [имя файла]
```

Опции команды who приведены в таблице 63.

Таблица 63 – Опции команды who

Опция	Описание
-u	Позволяет вывести информацию о пользователях, которые в настоящее время являются активными (работают в ОС).
-H	Опция, аналогичная опции -u (дополнительно в консоль выводится название столбцов).
-s	Позволяет вывести в консоль имена активных пользователей и терминальных линий, а также время и дату начала сессии пользователей.
-t	Позволяет вывести информацию о последней корректировке системных часов администратором.
-r	Позволяет вывести текущий уровень выполнения процесса init, кроме этого, будут выведены идентификатор процесса, системный код завершения и пользовательский код завершения процесса.
-a	Позволяет обработать файл /etc/utmp или файл, указанный в команде, считая, что все опции (кроме THqs) включены.
-b	Позволяет вывести время и дату последней загрузки системы.
-d	Позволяет вывести информацию обо всех процессах, которые прекратили существование и не были заново порождены процессом init.

Окончание таблицы 63

Опция	Описание
-p	Позволяет вывести список всех других процессов, активных в настоящий момент, которые были порождены процессом init.
-q	Позволяет вывести имена и количество пользователей, работающих в настоящий момент в системе.
-l	Позволяет вывести список линий, на которых система ожидает входа в нее какого-либо пользователя.
-T	Аналогична опции -s с той разницей, что дополнительно в позиции STATE выводится информация о состоянии терминальной линии.

Сообщения, выводимые после выполнения команды who, имеют следующий формат:

NAME [STATE] LINE TIME [IDLE] [PID] [COMMENT] [EXIT]

Информация NAME, LINE и TIME выводится при использовании всех опций, кроме -q, STATE – только при использовании опции -T, IDLE и PID – только при использовании опции -u и -l, COMMENT и EXIT – только при использовании опции -a.

В сообщениях, выводимых после выполнения команды who, фигурируют следующие параметры:

- NAME – имя пользователя;
- STATE – состояние терминальной линии (состояние – возможность передавать сообщения на терминал от кого-либо другого терминала: состояние «+» – свидетельствует о том, что терминалу может передавать сообщения любой другой терминал, состояние «–» – терминалу сообщения передаваться не могут; пользователь root может передавать сообщения во все линии, которым отвечает состояние «+» или «–»; при обнаружении неисправной линии выводится «?»);
- LINE – имя терминальной линии;
- TIME – время и дата начала сеанса работы пользователя в системе;
- IDLE – время, прошедшее со времени последней активной работы пользователя;
- PID – идентификатор процесса входной оболочки пользователя;

- COMMENT – комментарий, характеризующий данную линию (если таковые имеются в файле /etc/inittab – этот файл может содержать, например, сведения о местоположении терминала, телефонном номере комнаты или о типе физического терминала).

Чтобы получить сведения о сеансе, учетной записи и PID запущенного процесса нужно выполнить следующую команду:

```
who -uH
```

На экран монитора будет выведено сообщение следующего вида:

```
ИМЯ        ЛИНИЯ     ВРЕМЯ        IDLE    PID   КОММЕНТАРИЙ
user-name line-name mm-dd hh:mm .      10340 (:0)
```

где:

- user-name – имя пользователя;
- line-name – имя терминальной линии;
- yy-mm-dd hh:mm – дата (в формате гг – мм – дд, гг – год, мм – месяц, дд – день) и время (в формате чч:мм, чч – час, мм – минута) начала сеанса работы пользователя;
- 10340 – PID-идентификатор процесса;
- (:0) – отсутствующий комментарий.

Точка (.) в параметре IDLE свидетельствует о том, что данный терминал находился в активном состоянии не более минуты тому назад.

16.2.2. Команда ps

Для получения информации о состоянии запущенных процессов используется команда ps. Она выдает следующую информацию о процессах: какие из них выполнены, какие вызвали проблемы в системе, как долго выполняется тот или иной процесс, какие он затребовал системные ресурсы, идентификатор процесса (который будет нужен, например, для прекращения работы процесса с помощью команды kill).

Команда ps, запущенная без опций командной строки, выдает список процессов, которые порождены учетной записью администратора.

Наиболее распространенное применение ps – отслеживание работы фоновых и

других процессов в системе. Поскольку в большинстве случаев фоновые процессы никак не взаимодействуют ни с экраном, ни с клавиатурой, команда ps остается основным средством наблюдения за ними.

Синтаксис команды ps:

```
ps [-e] [-d] [-a] [-f] [-l] [-n файл_с_системой] [-t список_терминалов]
[-p список_идентификаторов_процессов]
[-u список_идентификаторов_пользователей]
[-g список_идентификаторов_лидеров_групп]
```

Опции команды ps приведены в таблице 64.

Таблица 64 – Опции команды ps

Опция	Описание
-e	Позволяет вывести информацию обо всех процессах
-d	Позволяет вывести информацию обо всех процессах, кроме лидеров групп
-a	Позволяет вывести информацию обо всех наиболее часто запрашиваемых процессах, то есть обо всех процессах, кроме лидеров групп и процессов, не ассоциированных с терминалом
-f	Позволяет сгенерировать полный листинг
-l	Генерировать листинг в длинном формате
-n файл_с_системой	Считать, что ОС загружена из файла_с_системой, а не из файла /unix
-t список_терминалов	Позволяет вывести информацию только о процессах, ассоциированных с терминалами из заданного списка_терминалов (терминал – это либо имя файла-устройства, например, tty, номер или console, либо просто номер, если имя файла начинается с tty)
-p	Список_идентификаторов_процессов – позволяет вывести информацию только об указанных процессах
-u	Список_идентификаторов_пользователей – позволяет вывести информацию только о процессах с заданными идентификаторами или входными именами пользователей (идентификатор пользователя выводится в числовом виде, а при наличии опции -f – в символьном)
-g	Список_идентификаторов_лидеров_групп – позволяет вывести информацию только о процессах, для которых указаны идентификаторы лидеров групп (лидер группы – это процесс, номер которого идентичен его идентификатору группы)

ps выводит четыре основных поля информации для каждого процесса:

- PID – идентификатор процесса;
- TTY – терминал, с которого был запущен процесс;
- TIME – время работы процесса;
- COMMAND – имя выполненной команды.

При указании опции `-f` команда `ps` пытается определить имя команды и аргументы, с которыми был создан процесс, исследуя пользовательский блок процесса. В случае если это не удается, имя процесса выводится так же, как и при отсутствии опции `–f`, только заключается в квадратные скобки.

В таблице 65 приводятся заголовки колонок листинга, и поясняется смысл их содержимого. Буквы «l» или «f» в скобках означают, что эта колонка появляется соответственно при длинном или полном формате листинга, отсутствие букв означает, что данная колонка выводится всегда. При этом опции `-l` и `-f` влияют только на формат выдачи, но не на список процессов, информация о которых будет предоставлена.

Таблица 65 – Описание заголовков колонок листинга

Заголовок	Значение	Описание
F (l)	Флаги (шестнадцатеричные), логическая сумма которых характеризует процессы следующим образом:	
	00	Процесс терминирован, элемент таблицы процессов свободен.
	01	Системный процесс: всегда в основной памяти.
	02	Процесс трассируется родительским процессом.
	04	Родительский трассировочный сигнал остановил процесс, родительский процесс находится в состоянии ожидания
	08	Процесс не может быть разбужен сигналом
	10	Процесс в основной памяти
	20	Процесс в основной памяти, блокирован до завершения события
	40	Идет сигнал к удаленной системе
	80	Процесс в очереди на ввод/вывод
S (l)	Статус процесса:	
	O	Процесс обрабатывается процессором
	S	Процесс ожидает завершения события
	R	Процесс стоит в очереди на выполнение
	I	Процесс создается
	Z	Процесс завершен, но родительский процесс не ждет этого
	T	Процесс остановлен сигналом, так как родительский процесс трассирует его

Окончание таблицы 65

Заголовок	Значение	Описание
	X	Процесс ожидает получения большего объема основной памяти
UID (f,l)		Идентификатор владельца процесса, при указании опции `-f` выдается входное имя пользователя
PID		Идентификатор процесса (нужен для терминирования процесса)
PPID(f,l)		Идентификатор родительского процесса
C (f,l)		Доля выделенного планировщиком времени центрального процессора
STIME (f)		Время запуска процесса (часы:минуты:секунды). Если процесс запущен более чем 24 часа назад, выводится месяц и день запуска
PRI (l)		Приоритет процесса: большее число означает меньший приоритет
NI (l)		Поправка к приоритету
ADDR (l)		Адрес процесса в памяти
SZ (l)		Размер (в блоках по 512 байт) образа процесса в памяти
WCHAN (l)		Адрес события, которого ожидает процесс (у активного процесса эта колонка пуста)
TTY		Управляющий терминал (обычно – терминал, с которого был запущен процесс). В случае если такового нет, выводится символ «?»
TIME		Истраченное процессом время на выполнение центральным процессором
COMMAND		Имя программы: если указана опция `-f`, выводится полное имя команды и ее аргументы

16.2.3. Команда nohup

Команда nohup применяется для того, чтобы процесс продолжал выполняться даже после выхода из системы, поскольку выполнение стандартного дочернего процесса завершается сразу после прекращения работы родительского, и, если был запущен фоновый процесс, он также прекращает работу при выходе из системы.

При выполнении, команду nohup следует поместить в начало командной строки следующим образом:

```
nohup sort sales.dat &
```

В данном примере nohup заставляет ОС игнорировать выход из нее и продолжать выполнение до тех пор, пока процесс не закончится сам по себе. Будет запущен процесс, который продолжит свое выполнение, не требуя контроля администратора.

16.2.4. Команда `nice`

Команда `nice` позволяет запустить другую команду с предопределенным приоритетом выполнения, предоставляя администратору возможность определять приоритет при выполнении своих задач.

При обычном запуске все задачи имеют один и тот же приоритет, и ОС равномерно распределяет между ними процессорное время. С помощью команды nice можно понизить приоритет какой-либо задачи, предоставив другим задачам больше процессорного времени. Повысить приоритет той или иной задачи имеет право только пользователь с идентификатором root.

Команда `nice` обладает следующим синтаксисом:

```
nice -number command
```

Уровень приоритета определяется параметром `number`, при этом большее его значение означает меньший приоритет команды. Значение по умолчанию равно «10», и `number` представляет собой число, на которое он должен быть уменьшен.

Например, если запущен процесс сортировки:

```
sort sales.dat > sales.srt &
```

Далее, чтобы дать ему преимущество над следующим процессом, нужно запустить следующий процесс с уменьшенным приоритетом:

```
nice -5 lp mail_list &
```

Для того чтобы назначить процессу самый низкий приоритет из возможных, нужно выполнить следующую команду:

```
nice -10 lp mail_list &
```

П р и м е ч а н и е . В случае команды `nice` тире означает знак опции.

Только пользователь с идентификатором root может повысить приоритет того или иного процесса, применяя для этого отрицательное значение аргумента. Максимально возможный приоритет – «20», присвоить его процессу пользователь с идентификатором root может с помощью команды:

```
nice --10 job &
```

Наличие символа «&» в примере достаточно условно, можно изменять приоритеты, как фоновых процессов, так и процессов переднего плана.

16.2.5. Команда renice

Команда renice позволяет изменить приоритет работающего процесса. Формат этой команды подобен формату команды nice:

```
renice -n PID
```

Для изменения приоритета работающего процесса нужно знать его идентификатор, получить который можно с помощью команды ps, например, вызвав:

```
ps -e | grep name
```

В данной команде нужно заменить name именем интересующего процесса. Команда grep отфильтрует только те записи, в которых будет встречаться имя нужной команды. В случае, если нужно изменить приоритет всех процессов пользователя или группы пользователей, в команде renice используется идентификатор пользователя или группы.

Далее приводится пример использования команды renice, предположив, что имя пользователя – pav:

```
ps -ef | grep $LOGNAME
pav 11805 11804 0 Dec 22 ttysb 0:01 sort sales.dat > sales srt
pav 19955 19938 4 16:13:02 ttypo 0:00 grep pav
pav 19938 1 0 16:11:04 ttypo 0-00 bash
pav 19940 19938 42 16:13:02 ttypo 0:33 find . -name core -exec nn
{};
```

Теперь, чтобы понизить приоритет процесса find с идентификатором 19940, нужно ввести:

```
renice -5 19940
```

В случае команды renice работают те же правила, что и в случае команды nice, а именно:

- ее можно использовать только со своими процессами;
- пользователь с идентификатором root может применить ее к любому процессу;
- только пользователь с идентификатором root может повысить приоритет процесса.

16.2.6. Команда `kill` и `killall`

В отдельных ситуациях нужно прекратить выполнение процесса, не дожидаясь его нормального завершения. Это может произойти в следующих случаях:

- процесс использует слишком много времени процессора и ресурсов компьютера;
- процесс работает слишком долго, не давая ожидаемых результатов;
- процесс производит слишком большой вывод информации на экран или в файл;
- процесс привел к блокировке терминала или другой сессии;
- из-за ошибки пользователя или программы используются не те файлы или параметры командной строки;
- дальнейшее выполнение процесса бесполезно.

В случае если процесс работает не в фоновом режиме, нажатие клавиш <Ctrl>+<C> должно прервать его выполнение, но, если процесс фоновый, то прервать его выполнение можно только с помощью команды `kill`, которая посылает процессу сигнал, требующий от процесса завершения. Для этого используются две формы:

```
kill PID(s)
kill -signal PID(s)
```

Для завершения процесса с идентификатором 127 ввести:

```
kill 127
```

Для того чтобы завершить процессы 115, 225 и 325, ввести:

```
kill 115 225 325
```

С помощью опции `-signal` можно, например, заставить процесс перечитать конфигурационные файлы без прекращения работы.

Список доступных сигналов можно получить с помощью команды:

```
kill -l
```

При успешном завершении процесса никакое сообщение не выводится.

Сообщение появится при попытке завершения процесса без наличия соответствующих прав доступа или при попытке завершить несуществующий процесс.

Завершение родительского процесса иногда приводит к завершению дочерних, однако для полной уверенности в завершении всех процессов, связанных с данным, следует указывать их в команде `kill`.

В случае, если терминал оказался заблокированным, можно войти в систему с другого терминала:

```
ps -ef | grep $LOGNAME
```

и завершить работу оболочки на блокированном терминале.

При выполнении команда `kill` посылает процессу соответствующий сигнал. Программы ОС могут посылать и принимать более 20 сигналов, каждый из которых имеет свой номер. Например, при выходе администратора ОС посылает всем его процессам сигнал 1, который заставляет все процессы (кроме запущенных с помощью `nohup`) прекратить работу.

Программы могут быть написаны и таким образом, что будут игнорировать посылаемые им сигналы, включая сигнал 15, который возникает при запуске команды `kill` без указания конкретного сигнала.

Однако сигнал 9 не может быть проигнорирован – процесс все равно будет завершен. Таким образом, если команда `kill PID` не смогла завершить процесс (он виден при использовании команды `ps`), нужно воспользоваться следующей командой:

```
kill -9 PID
```

Команда `kill -9` прекращает процесс, не давая возможности, например, корректно закрыть файлы, что может привести к потере данных. Использовать эту возможность следует только в случае крайней нужности.

Для завершения всех фоновых процессов нужно ввести следующую команду:

```
kill 0
```

Команда `killall` завершает все процессы с данным именем, обладает следующим синтаксисом:

```
killall [имя процесса]
```

Пример использования `killall`:

```
killall httpd
```

Преимущественное право контроля над процессом принадлежит владельцу. Права владельца могут отменяться только пользователем с идентификатором root.

Ядро назначает каждому процессу четыре идентификатора: реальный и эффективный UID, реальный и эффективный GID. Реальные ID используются для учета использования системных ресурсов, а эффективные – для определения прав доступа. Как правило, реальные и эффективные ID совпадают. Владелец процесса может посылать в процесс сигналы, а также понижать приоритет процесса.

Процесс, приступающий к выполнению другого программного файла, осуществляет один из системных вызовов семейства `exec`. Когда такое случается, эффективные UID и GID процесса могут быть установлены равными UID и GID файла, содержащего образ новой программы, если у этого файла установлены биты смены идентификатора пользователя и идентификатора группы.

Системный вызов `exec` – это механизм, с помощью которого такие команды, как `passwd`, временно получают права пользователя с идентификатором root (команде `passwd` они нужны для того, чтобы изменить `/etc/passwd`).

16.3. Основные утилиты для операций с файлами и каталогами

16.3.1. Команда `ls`

Команда `ls` предназначена для вывода информации о файлах или каталогах. Команда `ls` для каждого имени каталога распечатывает список входящих в этот каталог файлов; для файлов – повторяется имя файла и выводится дополнительная информация в соответствии с указанными флагами.

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

Синтаксис:

`ls [параметры]... [файл]...`

Параметры:

1) `-a`, `--all` – вывести список всех файлов (обычно не выводятся файлы, имена которых начинаются с точки);
2) `-A`, `--almost-all` – не показывать подразумеваемые «.» и «..»;
3) `--block-size=РАЗМЕР` – выдает размеры в блоках по `РАЗМЕР` байт. Например, `--block-size=M` для вывода объема в единицах равных 1048576 байтов;
4) `-B`, `--ignore-backups` – не показывать файлы, заканчивающиеся на «~», если они не заданы в командной строке;
5) `-c`, `--time=ctime`, `--time=status` – сортировать содержимое каталога в соответствии со временем изменения состояния файла. Если с помощью опции `-l` задан этот формат, то выдавать время изменения файла вместо времени его модификации. С опцией `-t` показать время последней модификации описания файла и сортировать по имени;
6) `-C`, `--format=vertical` – вывод в несколько колонок с сортировкой по вертикали;
7) `--color[=КОГДА]` – использовать цвета в выводе. `КОГДА` по умолчанию `always`. Также можно использовать `never` и `auto`;
8) `-d`, `--directory` – если аргумент является каталогом, то выводить только его имя, а не содержимое. Часто используется с флагом `-l` для получения сведений о состоянии каталога;
9) `-h`, `--human-readable` – в сочетании с `-l` показывает размеры в удобочитаемом формате (например, 1K 234M 2G);
10) `-i`, `--inode` – показывать индекс каждого файла;
11) `-I`, `--ignore= ШАБЛОН` – не показывать записи, соответствующие `ШАБЛОНУ` командного интерпретатора;
12) `-k`, `--kibibytes` – использовать блоки по 1024 байта;
13) `-l` – вывод в длинном формате;

14) -m – показать записи в список шириной в размер терминала, имена файлов разделяются запятыми;
15) -r, --reverse – изменить порядок сортировки на обратный;
16) -R, --recursive – рекурсивно обойти встретившиеся подкаталоги;
17) -s, --size – выдавать размер файлов в блоках;
18) -S – отсортировать по размеру файлов, большие сначала;
19) --sort=СЛОВО – сортировать по СЛОВУ, а не по имени: none (без сортировки) -U, extension (расширение) -X, size (размер) -S, time (время) -t или version (версия) –v;
20) -t – файлы сортируются по времени последнего изменения (сначала идут самые новые файлы);
21) -U – не сортировать, отображать записи в обычном порядке;
22) -v – сортировать по номерам (версии) в текстовом представлении;
23) -x – вывод в несколько колонок с сортировкой по строкам;
24) -Z, --context – вывести контекст для каждого файла;
25) -1 – отображать по одному файлу в строке.

Режим доступа к файлу при указании флага -l выводится в виде 10 символов. При этом первый символ означает:

1) d – файл является каталогом;
2) b – файл является специальным блочным файлом;
3) c – файл является специальным символьным файлом;
4) p – файл является именованным каналом;
5) - – обычный файл.

Остальные 9 символов делятся на три группы по три символа: права доступа владельца, других пользователей из его группы, всех прочих пользователей. Внутри каждой группы используются три символа, обозначающие права на чтение, запись и выполнение файла соответственно.

Для каталога под правом на выполнение подразумевается право на просмотр в поисках требуемого файла.

Пример:

```
ls -l /util/by
-rwxr-xr-x 1 root sys 50 Jun 22 10:42 /util/by
```

Права обозначаются следующим образом:

1) `r` – право на чтение;
2) `w` – право на запись;
3) `x` – право на выполнение (поиск в каталоге);
4) `-` – данное право доступа отсутствует;
5) `l` – учет блокировки доступа (бит переустановки идентификатора группы равен 1, бит права на выполнение членами группы равен 0). Располагается на месте права на выполнение для членов группы;
6) `s` – право переустанавливать идентификатор группы или идентификатор владельца и право выполнения файла для членов группы или владельца;
7) `S` – неопределенная комбинация бит: право переустанавливать идентификатор владельца есть, а право выполнения файла для владельца отсутствует;
8) `t` – установлен бит навязчивости у файла, который могут выполнять прочие пользователи. Располагается на месте права на выполнение для прочих пользователей;
9) `T` – бит навязчивости установлен, а права на выполнение у прочих пользователей нет. Располагается на месте права на выполнение для прочих пользователей.

Примеры:

1) если файл доступен владельцу для чтения, записи и выполнения, а членам группы и прочим пользователям только для чтения, он имеет режим:
   `-rwxr--r-`
2) файл доступен владельцу для чтения, записи и выполнения, а членам группы и прочим пользователям только для чтения и выполнения. Разрешена переустановка при выполнении идентификатора пользователя на идентификатор владельца файла:
   `-rwsr-xr-x`

3) файл доступен для чтения и записи только владельцу и членам группы; может быть блокирован при доступе:
   `-rw-rwl--`
4) вывести имена всех файлов в текущем каталоге, включая и те, которые начинаются с точки и обычно не выдаются:
   `ls -a`
5) вывести разнообразную информацию: список всех файлов, включая те, которые обычно не выводятся (a); номера описателей файлов будут выведены в левой колонке (i); размеры файлов (в блоках) выводятся во второй колонке (s); наконец, будут выданы числовые идентификаторы владельцев и групп (n):
   `ls –aisn`

Возможные сообщения об ошибках, при использовании команды `ls`:

`ls: невозможно открыть каталог <путь>: Отказано в доступе`

`ls: невозможно получить доступ к <путь>/<файл>: Нет такого файла или каталога`

16.3.2. Команда `cp`

Команда `cp` предназначена для копирования файлов и каталогов.

Синтаксис:

```
cp [ОПЦИЯ]... [-T] ИСТОЧНИК НАЗНАЧЕНИЕ
cp [ОПЦИЯ]... ИСТОЧНИК... КАТАЛОГ
cp [ОПЦИЯ]... -t КАТАЛОГ ИСТОЧНИК...
```

Копирует `ИСТОЧНИК` в `НАЗНАЧЕНИЕ` или несколько `ИСТОЧНИКОВ` в `КАТАЛОГ`.

Основные опции:

1) `--backup[=CONTROL]` – сделать резервную копию каждого целевого файла;
2) `-b` – тоже что и `--backup`, но не принимает аргументы;
3) `-f`, `--force` – если невозможно открыть существующий файл, то удалить его и попробовать еще раз (данная опция игнорируется, если используется совместно с `-n`);
4) `-i`, `--interactive` – спросить перед перезаписью (отменяет ранее указанный ключ `-n`);

5) -H – следовать символьным ссылкам в ИСТОЧНИКЕ;

6) -l, --link – создавать жесткие ссылки вместо копирования;

7) -n, --no-clobber – не перезаписывать существующие файлы (отменяет стоящую перед ней опцию -i);

8) -R, -r, --recursive – копировать каталоги рекурсивно;

9) -s, --symbolic-link – создать символьную ссылку вместо копирования;

10) -u, --update – копировать, только если файл ИСТОЧНИК новее, чем файл назначения или если файл назначения отсутствует;

11) -v, --verbose – выводить имя каждого файла перед копированием.

По умолчанию суффикс для резервных копий «~». Его можно переопределить при помощи опции --suffix или переменной окружения SIMPLE_BACKUP_SUFFIX. Способ контроля версий может быть задан через опцию --backup или через переменную окружения VERSION_CONTROL. Допустимые значения:

1) none, off – никогда не делать резервные копии (даже если задана опция --backup);

2) numbered, t – создать нумерованные резервные копии;

3) existing, nil – если существуют нумерованные резервные копии, то создавать нумерованные резервные копии, если нет, то создавать простые;

4) simple, never – всегда создавать простые резервные копии.

Следующий пример использования команды cp демонстрирует копирование файла srcfile1 в каталог dest_dir: cp srcfile1 dest_dir

16.3.3. Команда rsync

Команда rsync выполняет синхронизацию файлов и каталогов, использует протокол удаленного обновления для ускорения передачи файлов, которые существуют в месте назначения.

Синтаксис:

```
rsync [ОПЦИИ] источник место_назначения
```

Опции:

1) `-v` – подробный режим;
2) `-r` – копировать данные рекурсивно;
3) `-a` – режим архивирования, позволяет копировать данные рекурсивно, с сохранением прав доступа на файлы, символических ссылок и другой информации);
4) `-h` – вывод данных в удобном формате;
5) `-z` – сжатие данных.

Примеры:

1) скопировать или синхронизировать все файлы из одного каталога в другой:
   `rsync –avh /tmp/firstdir /tmp/seconddir`
2) копирование локальных данных на удаленный хост:
   `rsync –avzh /tmp/firstdir user@10.110.2.1:/tmp/seconddir`

Возможные сообщения об ошибках, при использовании команды `sfill`:

```
rsync: change_dir#1 <каталог> failed: Отказано в доступе
rsync: change_dir <каталог> failed: Нет такого файла или каталога
```

16.3.4. Команда `mv`

Команда `mv` – перемещение (переименование) файлов.

Синтаксис:

```
mv [ОПЦИЯ]... [-T] ИСТОЧНИК НАЗНАЧЕНИЕ
mv [ОПЦИЯ]... ИСТОЧНИК... КАТАЛОГ
mv [ОПЦИЯ]... -t КАТАЛОГ ИСТОЧНИК...
```

Переименовать `ИСТОЧНИК` в `НАЗНАЧЕНИЕ` или переместить `ИСТОЧНИК`(и) в `КАТАЛОГ`.

Основные опции:

1) `-i, --interactive` – просит подтверждения на замену существующего файла;
2) `-n, --no-clobber` – не переписывать существующий файл. Если указано несколько опций `-i`, `-f` и `-n`, то действовать будет только последняя;

3) `-u`, `--update` – перемещать только, если файл `ИСТОЧНИК` новее, чем файл назначения или если файл назначения отсутствует;

4) `-v`, `--verbose` – выдавать имя каждого файла перед его переносом.

Возможные сообщения об ошибках, при использовании команды mv:

```
mv: невозможно переместить <файл> в <файл>: Операция не позволена
mv: не удалось выполнить stat для <файл>: Отказано в доступе
mv: не удалось выполнить stat для <файл>: Нет такого файла или каталога
```

16.3.5. Команда `dd`

Команда `dd` предназначена для копирования файла (по умолчанию из стандартного ввода на стандартный вывод), используя заданные размеры блоков для ввода и вывода, и в тоже время, выполняя его преобразование.

Синтаксис:

```
dd [параметр]
```

Основные опции:

1) `if=ФАЙЛ` – читает данные из `ФАЙЛа` вместо стандартного ввода;

2) `of=ФАЙЛ` – пишет данные в `ФАЙЛ` вместо стандартного вывода;

3) `ibs=ЧИСЛО` – читает по `ЧИСЛО` байт за раз. По умолчанию 512;

4) `obs=ЧИСЛО` – пишет по `ЧИСЛО` байт за раз. По умолчанию 512;

5) `bs=ЧИСЛО` – читает и пишет по `ЧИСЛО` байт за раз. По умолчанию 512.

Примеры:

1) Заполнить устройство случайными данными:

```
dd if=/dev/urandom of=/dev/sda bs=4k
```

2) Скопировать раздел в другой раздел:

```
dd if=/dev/sda3 of=/dev/sdb3 bs=4096 conv=notrunc,noerror
```

Возможные сообщения об ошибках, при использовании команды `dd`:

```
dd: не удалось открыть <файл>: Отказано в доступе
```

16.3.6. Команда `s_rm`

Команда `s_rm` выполняет безопасное удаление целевого файла.

Синтаксис:

```
s_rm ФАЙЛ...
```

Возможные сообщения об ошибках, при использовании команды s_rm:

```
Ошибка: файл <файл>: Отказано в доступе
Ошибка: файл <файл>: Нет такого файла или каталога
```

Примечание. Для работы команды s_rm и s_fill должен быть установлен пакет altsp-test-scripts.

16.3.7. Команда s_fill

Команда s_fill выполняет безопасную перезапись свободного пространства на разделе, в котором находится указанная директория и всех свободных индексных дескриптеров указанного каталога.

Синтаксис:

s_fill каталог...

Возможные сообщения об ошибках, при использовании команды s_fill:

```
Ошибка: не достаточно прав для <каталог>: Отказано в доступе
```

16.3.8. 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]

Опция -L заставляет следовать по символическим ссылкам.

Поскольку для выполнения каждой команды создается отдельный процесс, cd не может быть обычной командой; она распознается и выполняется командной оболочкой.

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.

16.3.9. Команда pwd

Команда pwd выводит абсолютный путь текущего (рабочего) каталога.

Синтаксис: `pwd [-LP]`

Опции:

1) `-P` – вывод не будет содержать символических ссылок;
2) `-L` – вывод может содержать символические ссылки.

16.3.10. Команда `mkdir`

Команда `mkdir` предназначена для создания каталогов.

Синтаксис:

```
mkdir [опция]... каталог...
```

Опции:

1) `-m`, `--mode=РЕЖИМ` – установить права доступа для создаваемых каталогов;
2) `-p`, `--parents` – перед созданием нового каталога предварительно создаются все несуществующие вышележащие каталоги. В случае существования каталога не будет выведена ошибка;
3) `-v`, `--verbose` – выводить сообщение для каждого созданного каталога;
4) `-Z`, `--context[=CTX]` – задать контекст для каждого создаваемого каталога. Если CTX не задан, то контекст будет равным типу по умолчанию.

Чтобы создать поддерево каталогов `tmpdir/temp/dir`, надо выполнить команду:

```
mkdir -p tmpdir/temp/dir
```

Возможные сообщения об ошибках, при использовании команды `mkdir`:

```
mkdir: невозможно создать каталог <каталог>: Отказано в доступе
mkdir: невозможно создать каталог <каталог>: Нет такого файла или каталога
```

16.3.11. Команда `rmdir`

Команда `rmdir` предназначена для удаления каталога, при условии, что он пуст.

Синтаксис:

```
rmdir [опция]... каталог...
```

Для команды `rmdir` доступна опция `-p` – при указании пути к каталогу (а не просто имени каталога), команда удалит каталог и его потомков:

```
rmdir –p a/b/c
```

Команда `rmdir` часто заменяется командой `rm -rf`, которая позволяет удалять каталоги, даже если они не пусты.

16.3.12. Команда `mount`

Команда `mount` используется для монтирования файловых систем.

Синтаксис:

```
mount [-lhV]
mount –a [опция]
mount [опция] [--source] <source> | [--target] <directory>
mount [опция] <source> <directory>
```

Опции:

1) `-t` – определение типа файловой системы раздела, предполагаемого для размещения;
2) `-o` – указание параметров монтирования.

Примеры:

1) просмотр примонтированных устройств:

   ```
   mount -l
   ```

2) монтирование разделов жесткого диска:

   ```
   mount –t ext3 /dev/sdb1 /home/user/test
   ```

Возможные сообщения об ошибках, при использовании команды `mount`:

```
mount: точка монтирования <каталог> не существует
```

16.4. Создание, просмотр и редактирование файлов

16.4.1. Команда `cat`

Команда cat позволяет просмотреть файл целиком, копируя файлы в стандартный поток вывода и объединяя их.

Синтаксис:

```
cat [ОПЦИЯ]... [ФАЙЛ]...
```

Опции:

1) `-A`, `--show-all` – тоже что и `-vET`;
2) `-e` – тоже что и `-vE`;
3) `-E`, `--show-ends` – отображать символ «$» в конце каждой строки;
4) `-n`, `--number` – нумеровать выводимые строки;

5) `-s`, `--squeeze-blank` – скрывать повторяющиеся пустые строки в выводе;
6) `-t` – тоже что и `-vT`;
7) `-T`, `--show-tabs` – отображать символ табуляции как `^I`;
8) `-v`, `--show-nonprinting` – использовать `^-` и M-нотацию для всех непечатаемых символов кроме LFD (перевод строки и табуляция) и табуляции.

Если `ФАЙЛ` не задан или задан как «-», то читать из стандартного ввода.

Примеры:

1) вывести содержимое файла `f`, затем со стандартного ввода, затем – содержимое файла `g`:
   `cat f - g`
2) скопировать стандартный ввод на стандартный вывод:
   `cat`

Возможные сообщения об ошибках, при использовании команды `cat`:

```
cat: <файл>: Отказано в доступе
cat: <файл>: Нет такого файла или каталога
```

16.4.2. Команда `less`

Команда `less` позволяет просматривать текст постранично.

```
less [ опции ] файл
```

Опции:

1) `-c` – очистка экран перед тем, как отобразить следующую страницу;
2) `-m` – вывод информации о том, какая часть файла выведена на данный момент (в процентах);
3) `-N` – вывод номеров строк;
4) `-r` – вывод управляющих (непечатаемых) символов;
5) `-s` – объединение несколько пустых строк в одну;
6) `-S` – урезание длинных строк до длины экрана вместо переноса.

Возможные сообщения об ошибках, при использовании команды `less`:

```
<файл>: Отказано в доступе
<файл>: Нет такого файла или каталога
```

16.4.3. Команда echo

Команда echo выводит текст на стандартное устройство вывода.

```
echo [опции] [строка]
```

Опции:

1) -n – не выводить в конце символ новой строки;

2) -e –включить интерпретацию управляющих символов;

3) -E – отключить интерпретацию управляющих символов;

Возможные сообщения об ошибках, при использовании команды echo:

```
<файл>: Отказано в доступе
<файл>: Нет такого файла или каталога
```

16.4.4. Команда grep

Команда grep предназначена для поиска текста, соответствующего регулярному выражению в файлах или потоке вывода.

Синтаксис:

```
grep [ опции ] шаблон_поиска [файл]
```

Опции:

1) -r – рекурсивный поиск во всех каталогах;

2) -n – вывод номеров строк, в которых найдено совпадение;

3) -l – вывод списка файлов, содержащих шаблон;

4) -v – поиск строк, не содержащих шаблон (инверсия);

5) -i – поиск с игнорированием регистра.

16.4.5. Команда touch

Создание и редактирование файлов выполняется командой touch, которая устанавливает время последнего изменения и доступа в текущее системное время у заданного файла. Если файл не существует – он создается.

Синтаксис:

```
touch [опции]... файл
```

Основные опции:

1) -a – изменить только время доступа к файлу;

2) -c, --no-create – не создавать файл;

3) -d, --date=СТРОКА – проанализировать строку и использовать вместо текущего времени;

4) -m – изменить время последней модификации файла;

5) -r, --reference=ФАЙЛ – использовать соответствующий временной штамп от ФАЙЛ в качестве нового значения для изменяемого временного штампа;

6) -t время – использовать заданное время в качестве нового значения для изменяемого временного штампа.

Следующий пример использования команды touch создает файл myfile.txt:

```
touch myfile.txt
```

Возможные сообщения об ошибках, при использовании команды touch:

```
touch: невозможно выполнить touch для <файл>: Отказано в доступе
touch: невозможно выполнить touch для <путь>/<файл>: Нет такого файла или каталога
```

16.4.6. Команда mknod

Утилита mknod создает специальные блочные или символьные файлы. Специальный файл записывается в файловой системе с помощью тройки параметров: один логический и два целых. Логический параметр говорит о том, является ли специальный файл символьным или блочным. Два целых параметра задают старший и младший номера устройства. Специальный файл практически не занимает места на диске и используется только для общения с операционной системой, а не для хранения данных.

Синтаксис:

```
mknod [опции] имя {bc} старший_номер младший_номер
mknod [опции] имя p
```

Основные опции:

1) -m, --mode=РЕЖИМ – установить РЕЖИМ доступа;

2) -Z – установить контекст безопасности равным типу по умолчанию.

Тип устройства может принимать следующие значения:

1) b – создать файл блочного устройства (буферизированный);

2) c – создать файл символьного устройства (небуферизированный);

3) p – создать именованный канал.

Возможные сообщения об ошибках, при использовании команды mknod:

```
mknod: <файл>: Файл существует
```

16.5. Поиск файлов

16.5.1. Команда find

Утилита find используется для поиска файлов.

Синтаксис:

```
find [-H] [-L] [-P] [-Oуровень] [-D help | tree | search | stat |
rates | opt | exec] [путь…] [выражение]
find [путь] [опции] [критерии поиска] [действия над файлами]
```

В качестве пути для поиска можно использовать как абсолютные, так и относительные пути, а также список путей, разделенных пробелом. Путем по умолчанию является текущий подкаталог. Выражение по умолчанию -print.

Основные опции:

1) -d, -depth – поиск в подкаталогах перед поиском в самом каталоге;
2) -L – при поиске следовать по символическим ссылкам;
3) -P – никогда не следовать по символическим ссылкам;
4) -maxdepth N – при поиске проверять не более чем N вложенных уровней каталогов;
5) -mindepth N – не проверять вложенные каталоги уровня N и меньше;
6) -mount – не искать в каталогах других файловых систем.

У команды find может быть несколько критериев поиска (tests). Каждый критерий представляет собой определенное условие проверки, которое возвращает либо true либо false.

В процессе обработки очередного файла команда find по очереди проверяет каждый критерий, и, если очередной критерий возвращает false, тогда команда find переходит к следующему файлу.

Основные критерии поиска:

1) -name шаблон – имя файла (шаблон имени) без указания пути. Рекомендуется всегда заключать шаблон в кавычки;

2) `-atime N` – последний доступ к файлу производился N дней назад. `-atime +1` найдет файлы, доступ к которым осуществлялся как минимум два дня назад;
3) `-mtime N` – последнее изменение файла было N дней назад;
4) `-ctime N` – статус файла последний раз изменялся N дней назад;
5) `-newer другой_файл` – файл был модифицирован позднее, чем другой_файл;
6) `-size [±]N[cwbkMG]` – размер файла равен N блокам, если указано +N, тогда размер файла больше N, -N – меньше. Символ после N означает размер блока (b – 512 байт, c – байт, w – 2 байта, k – Кбайт, M – Мбайт, G – Гбайт);
7) `-type C` – файл имеет тип c, где c есть b (блочный специальный файл), c (символьный специальный файл), d (каталог), p (именованный канал), f (обычный файл), l (символьная ссылка) или s (сокет);
8) `[-perm] [-]восьмеричное_число` – режим доступа к текущему файлу в точности равен `восьмеричному_числу`. Если перед `восьмеричным_числом` указан знак `-`, то для сравнения из режима файла берутся только биты, соответствующие битам `восьмеричного_числа`, равным единице;
9) `-links n` – на файл имеется n ссылок;
10) `-user имя_пользователя` – файл принадлежит пользователю с данным именем. Разрешены цифровые идентификаторы пользователя;
11) `-group имя_группы` – файл принадлежит группе с данным именем. Разрешены цифровые идентификаторы группы.

Критерии можно объединять, используя операторы. Ниже приведены операторы в порядке убывания их приоритета:

- унарная операция отрицания, обозначается ! (! критерий);
- логическое И, обозначается пробелом (критерий1 критерий2);
- логическое ИЛИ, обозначается -o (критерий1-o критерий2).

Когда выполняется команда `find`, можно выполнять различные действия над найденными файлами.

Основные действия:

1) `-exec команда \;` – выполнить команду. Запись команды должна заканчиваться экранированной точкой с запятой. Строка «{}» заменяется текущим маршрутным именем файла;
2) `execdir команда \;` – то же самое что и `exec`, но команда вызывается из подкаталога, содержащего текущий файл;
3) `-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`;
4) `-print` – вывод имени файла на экран.

Примеры:

1) найти в текущем каталоге обычные файлы (не каталоги), имя которых начинается с символа «~»:
   ```
   find . -type f -name "~*" -print
   ```
2) найти в текущем каталоге файлы, измененные позже, чем файл `file.bak`:
   ```
   find . -newer file.bak -type f -print
   ```
3) 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 {} \;
   ```
4) удалить из текущего каталога и его подкаталогов все файлы нулевого размера, запрашивая подтверждение:
   ```
   find . -size 0c -ok rm {} \;
   ```

16.5.2. Команда `whereis`

Команда `whereis` сообщает путь к исполняемому файлу программы, ее исходным файлам (если есть) и соответствующим страницам справочного руководства.

Опции:

1) `-b` – вывод информации только об исполняемых файлах;
2) `-m` – вывод информации только о страницах справочного руководства;
3) `-s` – вывод информации только об исходных файлах.

16.6. Средства архивирования файлов

Команды tar, cpio, gzip представляют собой инструменты создания резервных копий и архивирования ФС.

При создании архива командами tar (п. 16.6.1) и gzip передается список файлов и каталогов, указываемых как параметры командной строки. Любой указанный каталог просматривается рекурсивно.

При создании архива с помощью команды cpio (п. 16.6.2) ей предоставляется список объектов (имена файлов и каталогов, символические имена любых устройств, гнезда доменов UNIX, именованные каналы).

16.6.1. Команда tar

Команда tar предназначена для преобразования файла или группы файлов в архив без сжатия (tarfile).

Синтаксис:

```
tar [Опции] [АРГ]
```

Опции:

1) -c – создает архив;
2) -x – восстанавливает файлы из архива на устройстве, заданном по умолчанию или определенном опцией f;
3) -f name – создает (или читает) архив с name, где name – имя файла или устройства, определенного в /dev, например, /dev/rmt0;
4) -Z – сжимает или распаковывает архив с помощью compress;
5) -z – сжимает или распаковывает архив с помощью gzip;
6) -M – создает многотомный архив;
7) -t – создает список сохраненных в архиве файлов и выводит его на консоль;
8) -v – выводит подробную информацию о процессе.

Упаковка файлов в архив чаще всего выполняется следующей командой:

```
tar -cf [имя создаваемого файла архива] [упаковываемые файлы и (или) директории]
```

Пример использования команды упаковки архива:

```
$ tar -cf moi_dokumenti.tar Docs project.tex
```

Распаковка содержимого архива в текущий каталог выполняется следующей командой:

```
tar -xf [имя файла архива]
```

Далее приводится пример использования команды распаковки архива:

```
$ tar -xf moi_dokumenti.tar
```

Для сжатия файлов используются специальные программы сжатия: gzip, bzip2 и 7z.

16.6.2. Команда `cpio`

Команда `cpio` предназначена для копирования файлов. Ее можно использовать с опцией `-o` для создания резервных архивов и с опцией `-i` – для восстановления файлов. Команда получает информацию от стандартного устройства ввода и посылает выводимую информацию на стандартное устройство вывода.

Команда `cpio` может архивировать любой набор файлов и специальные файлы, хранит информацию более эффективно, чем `tar`, пропускает сбойные сектора или блоки при восстановлении данных, и ее архивы могут быть восстановлены в ОС.

Недостатком команды `cpio` является то, что для обновления архива следует использовать язык программирования оболочки, чтобы создать соответствующий сценарий.

Синтаксис:

```
cpio [Опции] < список-имен [> архив]
```

Опции:

1) `-o` – создание архива в стандартное устройство вывода;
2) `-I` – восстановление файлов из архива, передаваемого на стандартное устройство ввода;
3) `-t` – создание списка содержимого стандартного устройства ввода.

Ниже приводятся примеры использования команды `cpio` для решения различных задач.

Копирование файлов из каталога /home в архив home.cpio выполняется следующим образом:

```
find /home/* | cpio -o > /tmp/home.cpio
```

Восстановление файлов из архива home.cpio с сохранением дерева каталогов и создание списка в файле bkup.index выполняется следующим образом:

```
cpio -id < /tmp/home.cpio > bkup.index
```

Использование команды find для поиска измененных за последние сутки файлов и сохранение их в архив home.new.cpio выполняется следующим образом:

```
find /home -mtime 1 -type f | cpio -o > /tmp/home.new.cpio
```

Восстановление файла /home/dave/notes.txt из архива home.cpio выполняется следующим образом:

```
cpio -id /home/dave/notes.txt < home.cpio
```

Для восстановления файла с помощью cpio следует указывать его полное имя.

Все эти команды могут выполняться автоматически путем их размещения в файле crontab пользователя с идентификатором root.

Пример записи, выполняющей резервное копирование каталога /home ежедневно в 01:30:

```
30 02 *** ls /home : cpio -o > /tmp/home.cpio
```

При нужности выполнения резервного копирования более сложного уровня можно создать соответствующий сценарий оболочки. Запуск подобных сценариев также может быть осуществлен посредством cron.

Создание резервных копий означает определение политики создания резервных копий для снижения потерь и восстановления информации после возможной аварии системы.

16.7. Средства редактирования файлов

16.7.1. Текстовый редактор Vi

Текстовый редактор Vi – системный редактор, назначаемый ОС по умолчанию для работы с текстовыми файлами.

Текстовый редактор Vi имеет модальный интерфейс – одни и те же клавиши в разных режимах работы выполняют разные действия.

В редакторе Vi есть несколько режимов работы:

1) командный режим – перемещение по файлу, удаление текста и другие редактирующие функции. По умолчанию, работа начинается в командном режиме. Перейти в него из любого другого режима `<ESC>`, иногда два раза;
2) режим ввода – ввод текста (удаление и ввод текста происходит в двух разных режимах). Переход в режим ввода из командного режима осуществляется командой `<i>`;
3) режим строчного редактора ED – это специальный режим, в котором редактору даются сложные команды. При вводе этих команд они отображаются в последней строке экрана. Например, команда `<wq>` позволяет записать файл и покинуть редактор Vi, а команда `<q!>` – выйти из редактора Vi без сохранения изменений. В этом режиме обычно вводятся команды, название которых состоит из нескольких символов. Переход в него из командного режима осуществляется командой `<:>`.

Далее описаны операции, которые можно произвести с файлом в командном режиме.

16.7.1.1. Открыть (создать) файл

Управляющая команда открытия файла выглядит следующим образом:

```
vi <имя_файла>
```

Создание файла происходит при помощи той же команды, поскольку создание файла происходит в момент сохранения.

Для открытия или создания нового файла в командном режиме нужно набрать:

```
:e filename
```

Перед этим нужно сохранить предыдущий файл с помощью следующих команд:

- `<:w>` – сохраняет файл с существующим именем;
- `<:sav filename>` – или «Сохранить как».

16.7.1.2. Навигация по файлу

Навигация по файлу происходит с помощью управляющих клавиш на клавиатуре. Также допускается использовать клавиши быстрого перемещения:

- <^> или <0> – в начало текущей строки;
- <$> – в конец текущей строки;
- <w> – на слово вправо;
- <b> – на слово влево.

16.7.1.3. Редактирование файла

Для редактирования текста нужно перейти в режим ввода (нажать <i>).

Основные команды редактирования:

- <R>, <i> – переход в режим ввода, замена текста под курсором;
- <I> – переход в режим ввода с начала текущей строки;
- <o> – переход в режим ввода с новой строки под курсором;
- <O> – переход в режим ввода с новой строки над курсором;
- <a> – переход в режим ввода после курсора;
- <x> – стирание символа под курсором;
- <X> – стирание символа перед курсором;
- <dd> – стирание текущей строки;
- <d<число>d> – стирание выбранного числа строк, начиная с текущей;
- <yy> – копирование текущей строки в неименованный буфер;
- <y<число>y> – копирование выбранного числа строк, начиная с текущей в неименованный буфер;
- <p> – вставка строки из неименованного буфера под курсор;
- <P> – вставка строки из неименованного буфера над курсором;
- <J> – слияние текущей строки со следующей;
- <u> – отмена последней команды;
- <.> – повтор последней команды.

Для перехода в режим строчного редактора ED нужно нажать <Shift>+<:>.

16.7.1.4. Запись в файл и выход из редактора

Запись в файл выполняется следующей командой:

<Esc>:w<Enter>

В случае, если файл заблокирован другим пользователем либо отсутствуют права на запись, нужно использовать следующую команду:

<Esc>:w!<Enter>

При попытке записи без «!» будет выдано соответствующее предупреждение.

Создать новый файл <имя_файла> и записать в него текущее содержимое:

<Esc>:w имя_файла <Enter>

В случае, если файл с таким именем уже существует, редактор выдаст предупреждение. После успешного создания файла и осуществления записи информации в него работа продолжится со старым файлом.

Для выхода из редактора нужно использовать следующую команду:

<Esc>:q<Enter>

В случае, если в файл были внесены изменения, нужно добавлять после команды «!».

Выйти из редактора не сохраняя изменения:

<Esc>:q!<Enter>

Сохранить изменения в файле и выйти:

<Esc>:wq<Enter> или <Esc>ZZ<Enter>.

16.7.1.5. Дополнительные возможности

Текстовый редактор Vi обладает рядом дополнительных возможностей, которые вызываются следующими командами:

- ^G – показать информацию о файле;
- G – перейти в конец файла;
- <number>G – перейти на конкретную строку <number>;
- :<number> – перейти на <number> строк вперед;
- :set number – отобразить слева нумерацию строк (:set nonumber – спрятать нумерацию);
- :set wrap – переносить длинные строки (:set nowrap – не переносить);

- `:colorscheme <name>` – задать цветовую тему (где `<name>` имя темы, `TAB` работает как автодополнение);
- `/мама` – поиск текста «мама» в файле;
- `n` – повторить поиск;
- `:h` или `:help` – список возможной помощи (`:viusage`, `:exusage`).

Привести концы строк в файле к виду `dos` или `unix` соответственно:

```
:set fileformat=dos
:set fileformat=unix
```

Задать размер табуляции в четыре пробела:

```
:set ts=4
```

16.7.2. Редактор Vim

Vim – свободный режимный текстовый редактор, созданный на основе Vi.

16.7.2.1. Основной режим работы

Основной режим работы Vim предназначен для просмотра файлов, ввода команд и перехода из него в другие режимы. В командный режим можно попасть по нажатию клавиши <Esc>.

При нажатии клавиши «:» становится доступна командная строка Vim, в которой вводятся следующие команды:

- команда выхода – `quit` либо `q`;
- команда сохранения – `write` либо `w`, параметром которой может быть имя файла;
- вызов справки – `help` либо `h`.

Для остальных клавиш (и их последовательностей) допускается задавать любые команды либо использовать значения по умолчанию.

Перечисленные ниже команды вводятся в основном режиме (если нет специального уточнения). Все они имеют командностроочные аналоги и могут быть легко переопределены.

16.7.2.2. Визуальный режим работы

Визуальный режим работы предназначен, в первую очередь, для выделения блоков текста. Переход в визуальный режим выполняется с помощью следующих сочетаний клавиш:

- <v> для посимвольного выбора;
- <Shift>+<v> для построчного выбора;
- <Ctrl>+<v> для блочного выбора.

В режиме посимвольного выделения (при переходе по клавише «v») допускается оперировать следующими сущностями:

- слово («w»);
- предложение («s»);
- параграф («p»);
- блок («b»).

Выделение при этом нужно начинать с позиции курсора («a»), или же с начала блока («i»). Например, выделение текущего блока (участка, ограниченного парными элементами) можно произвести следующим образом:

```
<Esc>vib
```

Копирование в буфер выделенного текста осуществляется по «y», вырезание по «d» а вставка, соответственно, «p».

16.7.2.3. Режим редактирования

Режим редактирования предназначен для ввода текста. Переключение на режим редактирования осуществляется нажатием клавиши <Insert>.

16.7.2.4. Переходы

Для перехода на строку с номером n используется команда `G`. Так для перехода к началу текста нужно набрать `1G`, для сотой строки `100G`, а для перехода в конец текста – `$G`.

Для перехода на n символов в нужную сторону используются клавиши навигации на клавиатуре. То есть для перехода на 1000 символов вниз нужно набрать «1000» и нажать клавишу «↓».

Для перемещения по тексту допускается использовать следующие команды:

- «(», «)» – для перемещения по предложениям;
- «{», «}» – для параграфов;
- «[[«, «]]» – для функций;
- «%» – переход к парной скобке;
- «”» – к предыдущему положению;
- <Ctrl>+<O>, <Ctrl>+<I> – соответственно, назад и вперед по истории переходов.

16.7.2.5. Метки

Используются для отметки позиции (<буква>-метка, где меткой является любая буква) и быстрого к ней перехода (<`>-метка). Метки нижнего регистра действительны в пределах данного файла, метки верхнего регистра действуют во всех открытых файлах.

Список всех меток можно получить командой `marks`.

16.7.2.6. Регистры

Регистр отмечается видом <"буква>. К нему применимы все стандартные действия: копирование в него ("<метка>y), вырезание ("<метка>d), и вставка из него ("<метка>p), можете вместо `p` использовать `[p,]p` для вставки соответственно перед, или после курсора).

В режиме редактирования вставка из регистра осуществляется по <Ctrl>+R<метка>. Для добавления данных в регистр используйте заглавную метку.

Также допускается писать в регистр, воспользовавшись командой «q<метка>» и завершив запись по `q`. Таким образом сохраняется макрос, выполнить который можно по «@<метка>».

Регистры с метками «*» и «+» совпадают с X-Window clipboards, «%» – соответствует редактируемому файлу. Для просмотра содержимого всех регистров нужно воспользоваться командой `:registers`, либо `:reg метка1метка2...` для просмотра только выбранных регистров.

16.7.2.7. Фолды

Фолды предназначены для сокрытия строк, ненужных в данный момент.

По умолчанию фолды активированы в режиме ручной расстановки. Все команды для работы с фолдами начинаются с `z`:

- создание фолд выполняется командой `zf`;
- открытие фолд производится командой `zo` либо нажатием навигационной стрелки «→»;
- закрытие кода в существующий фолд – по `zc`.

Для автоматического подключения фолд по отношению к табуляции нужно добавить в файл настроек следующую строку:

```
set foldmethod=indent
```

16.7.2.8. Сессии

Сессии предназначены для сохранения текущего состояния и настройки редактора таким образом, что при следующем запуске работа продолжится с того же места.

Сессии создаются следующей командой:

```
:mksession /path/to/Session.vim
```

Чтение сессий выполняется командой:

```
:so /path/to/Session.vim
```

Для сохранения текущего контекста (текст, положение курсора в коде, текущая расстановка фолдов) нужно использовать команду `:mkview`, а для чтения – `:loadview`.

Автоматическое сохранение и чтение контекста при начале и окончании редактирования файла может быть реализовано следующим кодом (применяется для всех файлов, имеющих точку в имени):

```
au BufWinLeave *.* mkview
au BufWinEnter *.* silent loadview
```

16.7.2.9. Поиск и замена

Поиск по тексту осуществляется следующими командами:

- / – поиск по регулярному выражению вперед;

- ? – поиск по регулярному выражению в обратном направлении;

- n – продолжение поиска далее по тексту;

- N – повторение предыдущего запроса;

- # либо * – поиск слова под установленным курсором.

Для поиска с заменой рекомендуется использовать следующую команду:

`%s/что/на что/gic`

где `%` означает работу со всем текстом (а не с текущей строкой), `g` – глобальная замена (а не первое совпадение), `i` – игнорирование регистра, а `c` – подтверждение каждого действия.

16.7.2.10. Автодополнение, отмена, смена регистра, повтор

Автодополнение производится по содержимому данного файла, а также указанных в переменной dictionary по нажатию клавиш ``.

Для отмены предыдущих действий в режиме автодополнения используется `u`.

Для смены регистра выделенного участка (или буквы под курсором) используется `~`. При этом команда `U` – принудительно устанавливает верхний регистр, а `u` – нижний.

Для повтора прошлой команды используется символ «`.`».

16.7.2.11. Конфигурация

Файл конфигурации используется для настройки различных аспектов поведения и внешнего вида Vim. Комментарии в этом файле начинаются с символа «"» (двойная кавычка) и продолжаются до конца строки. Основным конфигурационным файлом является `~/.vimrc`.

Активация русского шрифта в GUI-режиме, плюс выбор темы для обоих режимов осуществляется, например, следующим кодом:

```
if has("gui_running")
colorscheme ron
set guifont=-cronyx-courier-medium-r-normal-*-*-120-*-*-m-*-koi8-r
endif
if !has("gui_running")
colorscheme elflord
endif
```

В файл конфигурации можно добавить привычное поведение и привычные сочетания клавиш:

```
"Выход по F10
nmap <F10> :q<CR>
imap <F10> <ESC>:q<CR>
"Сохранение по F2
nmap <F2> :w<CR>
imap <F2> <ESC>:w<CR>i<Right>
"Компиляция по F9
nmap <F9> :make<CR>
imap <F9> <ESC>:make<CR>
```

В Vim присутствует подробная документация по настройкам – `:options`.

16.8. Средства настройки отложенного исполнения команд

16.8.1. Служба crond

Для регулярного запуска команд в ОС Альт СП используется служба crond.

Служба crond запускается при загрузке системы и проверяет очередь заданий at и заданий пользователей в файлах crontab. При запуске, служба crond сначала проверяет каталог `/var/spool/cron` на наличие файлов crontab, файлы crontab имеют имена пользователей, соответствующие именам пользователей из `/etc/passwd`. Каждый пользователь может иметь только один файл crontab, записей в файле может быть несколько.

В случае, если задание не было обнаружено, crond переходит в режим ожидания на одну минуту и затем вновь приступает к поискам команды, которую следует запустить в этот момент. Большую часть времени служба crond проводит в режиме ожидания, и для ее работы используется минимум системных ресурсов.

Чтобы определить список задач для cron, используется команда `crontab`.

16.8.1.1. Crontab

Утилита crontab управляет доступом пользователя к службе crond путем копирования, создания, выдачи содержимого и удаления файлов crontab, таблиц заданий. При вызове без опций, crontab копирует указанный файл или стандартный входной поток (если файл не указан) в каталог, в котором хранятся пользовательские таблицы заданий cron. Каждый пользователь может иметь свои

собственные файлы crontab, и, хотя эти файлы доступны в /var/spool/cron, они не предназначены для редактирования напрямую.

Синтаксис:

```
crontab [имя_файла]
crontab [ -elr ] имя_пользователя
```

Опции:

1) -e – редактирует копию файла crontab текущего пользователя или создает пустой файл для редактирования, если соответствующего файла crontab не существует. Когда редактирование завершается, файл устанавливается в качестве пользовательского файла crontab. Переменная среды EDITOR задает редактор, вызываемый при указании опции -e. Все задания в файле crontab должны создаваться с помощью утилиты crontab;
2) -l – отображает текущий файл crontab на стандартный вывод;
3) -r – удаляет текущий файл crontab.

16.8.1.2. Контроль доступа к crontab

Доступ пользователя к crontab разрешен, если:

- имя пользователя указано в файле /etc/cron.d/cron.allow;
- файл /etc/cron.d/cron.allow не существует и имя пользователя не указано в файле /etc/cron.d/cron.deny.

Доступ пользователя к crontab не разрешен, если:

- файл /etc/cron.d/cron.allow существует и имя пользователя в нем не указано;
- файл /etc/cron.d/cron.allow не существует и имя пользователя указано в файле /etc/cron.d/cron.deny.

Правила разрешения и запрещения выполнения заданий применимы к пользователю root, только если существуют файлы allow/deny.

В файлах allow/deny надо задавать по одному имени пользователя в строке.

16.8.1.3. Формат записи файла crontab

Редактировать crontab пользователя можно используя команду:

```
crontab -e
```

Файл crontab состоит из строк, содержащие шесть полей. Поля разделяются пробелами или символами табуляции. Первые пять полей – целочисленные шаблоны, задающие:

- минуту (0 – 59);
- час (0 – 23);
- день месяца (1 – 31);
- месяц года (1 – 12);
- день недели (0 – 6, причем 0=воскресенье).

Каждый из этих шаблонов может представлять собой звездочку (которая обозначает все допустимые значения) или список элементов через запятые. Элемент – число или два числа через дефис (что обозначает закрытый интервал). Обратите внимание, что дни можно указывать в двух полях (день месяца и день недели). Оба поля учитываются, если заданы в виде списка элементов (запись: 30 4 1,15 * 5 приведет к выполнению команды в 4:30 пополуночи первого и пятнадцатого числа каждого месяца, плюс в каждую пятницу). При указании диапазона можно пропускать некоторые его значения, указав шаг в форме «/число». Например: «0-23/2» для поля час означает запуск команды через два часа. Шаг можно указывать также после звездочки: «каждые два часа» соответствует значению «*/2». Для задания полей месяц и день_недели можно использовать имена. Указывайте первые три буквы нужного дня или месяца на английском, регистр букв не имеет значения. Диапазоны или списки имен не разрешены.

Служба crond запускает команды, когда значения полей минута, час, месяц и хотя бы одно из полей число и день_недели, совпадают с текущим временем. Служба crond сверяет директивы с текущим временем раз в минуту.

Вместо первых пяти полей допустимо указание одного из восьми специальных триггеров:

- @reboot – выполнить команду один раз, при запуске cron;
- @yearly – выполнять команду каждое 1 января, «0 0 1 1 *»;
- @annually – эквивалентно @yearly;
- @monthly – выполнять команду в начале каждого месяца, «0 0 1 * *»;

- @weekly – выполнять команду каждое воскресенье, «0 0 * * 0»;
- @daily – выполнять команду в полночь, «0 0 * * *»;
- @midnight – эквивалентно @daily;
- @hourly – выполнять команду раз в час, «0 * * * *».

Шестое поле в строке файла crontab – строка, выполняемая командным интерпретатором в указанные моменты времени. Символ % (процент) в этом поле, если он не замаскирован «\» (обратной косой), преобразуется в символ новой строки.

Только первая строка (до символа % или до конца строки) поля команды выполняется командным интерпретатором. Другие строки передаются команде как стандартный входной поток. Пустые строки, ведущие пробелы и символы табуляции игнорируются. Строки, начинающиеся с символа («#») считаются комментариями и игнорируются. Комментарии не допускаются в тех же строках, где расположены команды cron, так как они будут распознаны как части команды. По этой же причине комментарии не разрешены в строках, задающих переменные среды.

Строка-директива представляет собой либо задание переменной среды, либо команду `cron`.

Демон crond предоставляет каждому командному интерпретатору стандартную среду, задавая переменные `HOME`, `LOGNAME`, `SHELL(=/bin/sh)`, `TZ` и `PATH`. Стандартное значение переменной PATH для пользовательских заданий cron – `/usr/bin`, а для заданий cron пользователя root – `/usr/sbin:/usr/bin`.

Если стандартный выходной поток и стандартный поток ошибок команд не перенаправлены, любые сгенерированные результаты или сообщения об ошибках будут отправлены пользователю по электронной почте.

16.8.1.4. Примеры

Далее приведены примеры использования таблиц crontab в ходе администрирования ОС Альт СП.

16.8.1.4.1. Пример 1

```
$ crontab -e
#minute (0-59),
#| hour (0-23),
```

```
#| | day of the month (1-31),

#| | | month of the year (1-12),
#| | | | day of the week (0-6 with 0=Sunday).
#| | | | | commands
# Каждые 5 минут записывать результат вывода
# команды date в файл date.txt в домашнем каталоге
*/5 * * * * date > ~/date.txt
# Выполнять задание в 18 часов 7 минут 13 числа
# каждого месяца и по пятницам
7 18 13 * 5 /home/www/myscript.pl
# Выполнять задание по воскресеньям в 10 час 30 минут
30 10 * * 0 /home/www/myscript.pl
crontab: installing new crontab
```

Вывод `crontab: installing new crontab` означает, что новый crontab успешно установлен.

16.8.1.4.2. Пример 2

```
# использовать для запуска команд /bin/sh
# не обращая внимание на то, что написано в /etc/passwd
SHELL=/bin/sh
# отправлять вывод выполнения команд по электронной
# почте пользователю 'paul'
# не обращая внимания на то, чей это crontab
MAILTO=paul
#
# запускать пять минут пополуночи, каждый день
5 0 * * * $HOME/bin/daily.job >> $HOME/tmp/out 2>&1
# запускать в 14:15 первого числа каждого месяца
15 14 1 * * $HOME/bin/monthly
# запускать в 22.00 каждый рабочий день
0 22 * * 1-5 mail -s "Уже 10 вечера"
23 0-23/2 * * * echo "запуск в 00:23, 2:23, 4:23 ..., каждый день"
5 4 * * sun echo "запуск в 4:05 каждое воскресенье"
```

16.8.1.5. Дополнительные возможности таблиц

Таблицы crontab обладают следующими дополнительными возможностями:

- при задании дня недели 0 и 7 соответствуют воскресенью;
- допускается указывать одновременно и списки, и диапазоны в одном и том же поле;
- допускается указывать диапазоны с пропусками – например, «1-9/2» соответствует «1,3,5,7,9»;
- допустимо указание месяцев или дней недели по имени;
- в crontab разрешено задавать переменные среды вручную;

- вывод команд отсылается почтой владельцу файла crontab, а также может отправляться кому-либо другому, либо отправка может быть отключена (функция не поддерживается в SysV);
- любая из команд с префиксом «@» может заменять первые пять полей файла.

16.8.2. Команда at

Для запуска одной или более команд в заранее определенное время используется команда at. В ней можно определить время и (или) дату запуска той или иной команды.

Команда at требует двух (или большего числа) параметров – как минимум, следует указать время запуска, и какая команда должна быть запущена. Параметры запуска с помощью команды at указываются в виде списка строк, следующих за ней. Ввод каждой строки завершается нажатием клавиши <Enter>. По окончании ввода всей команды нажать клавиши <Ctrl>+<D> для ее завершения.

Например, если нужно запустить команды в 1:23, следует ввести:

```
at 1:23
lpr /usr/sales/reports/.
echo "Files printed"
```

В указанном примере будут распечатаны все файлы каталога /usr/sales/reports, и пользователю будет выведено сообщение на экран монитора.

После ввода всей команды отобразится следующая запись:

```
job 756603300.a at Tues Jan 21 01:23:00 2007
```

Это означает, что указанные команды будут запущены, как и было задано, в 1:23. В сообщении также приведен идентификатор задания (756603300.a), который понадобится, если нужно отменить задание:

```
at -d 756603300.a
```

В случае, если список команд находится в файле, например, getdone, и нужно запустить все перечисленные в нем команды в 10:00, следует воспользоваться одной из двух форм команды at:

```
at 10:00 < getdone либо at 10:00 -f getdone
```

Обе приведенные команды эквивалентны. Разница заключается в том, что в первой команде используется механизм перенаправления потоков ввода-вывода, во второй команде – дисковый файл.

Кроме времени, в команде `at` может быть также определена дата:

```
at 17:00 Jan 24
lp /usr/sales/reports/
echo "Files printed"
```

Задания, определяемые администратором, помещаются в очередь, которую ОС периодически просматривает. Администратору необязательно находиться в системе для того, чтобы `at` отработала задания, команда будет работать в фоновом режиме.

Для того чтобы просмотреть очередь заданий, нужно ввести следующую команду:

```
at -l
```

В случае, если предыдущие примеры были запущены, то будет выведено:

```
job 756603300.a at Sat Dec 20 01:23:00 2007 job 756604200.a at Sat Jan 24
17:00:00 2008
```

Администратор видит только свои задания по команде `at`.

Для удаления задания из очереди следует запустить `at` с опцией `-d` и номером удаляемого задания следующим образом:

```
at -d 756604200.a
```

Далее представлены варианты использования команды `at`.

Выполнить задание во время `hh:mm` в 24-часовом формате:

```
at hh:mm
```

Выполнить задание во время `hh:mm` в 24-часовом формате в соответствующий день:

```
at hh:mm месяц день год
```

Вывести список заданий в очереди (псевдоним команды – `atq`):

```
at -l
```

Выполнить задание через определенное время, которое задано параметром `count` в соответствующих единицах – неделях, днях, часах или минутах:

```
at now+count time-units
```

Удалить задание с идентификатором job_ID из очереди (псевдоним команды – atrm):

```
at -d job_ID
```

Администратор может применять все эти команды. Для других пользователей права доступа к команде at определяются файлами /etc/at.allow и /etc/at.deny. В случае, если существует файл /etc/at.allow, то применять команду at могут только перечисленные в нем пользователи. В случае, если же такого файла нет, проверяется наличие файла /etc/at.deny, в котором отражено, кому запрещено пользоваться командой at. Также если ни одного из файлов, описывающих доступ к «alt», нет, то команда at доступна только пользователю с идентификатором root.

16.8.3. Команда batch

Команда batch позволяет ОС самой решить, когда наступает подходящий момент для запуска задачи – например, когда система находится в состоянии наименьшей загрузки, и процессы запускаются в фоновом режиме.

Формат команды batch представляет собой список заданий для выполнения, следующих в строках за ней, заканчивается список комбинацией клавиш <Ctrl>+<D>. Также допускается поместить список команд в файл и перенаправить его на стандартный ввод команды batch.

Например, для сортировки набора файлов, печати результатов и вывода сообщения нужно ввести следующие команды:

```
batch
sort /usr/sales/reports ; lp
echo "Files printed"
```

В ответ на это система выдаст:

```
job 7789001234.b at Fri Feb 21 11:43:09 1999
```

Примечание. Дата и время, приведенные в сообщении, соответствуют нажатию клавиш <Ctrl>+<D>.

16.9. Служба передачи файлов FTP

В ОС Альт СП передача файлов обеспечивается с помощью программы lftp. Данная команда реализует протокол передачи файлов FTP. Для копирования файлов нужно знать имя и пароль пользователя, которому принадлежат файлы на сервере

службы FTP.

Для запуска `lftp` нужно в консоли ввести команду:

```
lftp
```

После появления приглашения `lftp :~>` становятся доступными для использования внутренние команды `lftp`.

Основные внутренние команды `lftp`:

- `open` – подключение к серверу;
- `user` – идентификация при удаленном подключении;
- `close` – отключение от сервера;
- `ls` – просмотр списка файлов;
- `lcd` – смена локального каталога;
- `mkdir` – создание нового каталога;
- `lpwd` – просмотр имени каталога на локальном компьютере;
- `get` – копирование файла с сервера;
- `put` – копирование файла на сервер;
- `help` – просмотр списка доступных команд и справки по ним;
- `exit` – выход из `lftp`.

16.10. Защищенный интерпретатор команд SSH

Защищенный интерпретатор команд SSH – клиент-серверная система для организации защищенных туннелей для удаленного доступа к другим компьютерам.

SSH реализует соединение с удаленным компьютером, которое позволяет защититься от следующих угроз:

- прослушивание данных, передаваемых по этому соединению;
- манипулирование данными на пути от клиента к серверу;
- подмена клиента либо сервера путем манипулирования IP-адресами, DNS либо маршрутизацией.

Для создания защищенного туннеля используется программа ssh. Инициировать соединение с сервером можно командой:

```
ssh <имя_клиента>@IP_addr
```

где `IP_addr` – IP-адрес компьютера с запущенной службой sshd.

При использовании идентификации по паролю на сервере должна существовать учетная запись с указанным именем клиента.

Параметры, относящиеся к способу аутентификации, а также все прочие настройки ssh (см. п. 8.12.1) указываются в конфигурационном файле `/etc/ssh/ssh_config`.

Конфигурационные файлы разбиты на разделы, установки которых относятся к отдельному компьютеру, группе компьютеров или ко всем компьютерам, при этом установки разных разделов могут конфликтовать друг с другом. Предпочтение в данном случае будет отдаваться тому параметру, который указан раньше.

16.11. Средство управления процессами xinetd

Средство управления процессами xinetd (далее – сервер xinetd) выполняет функции управления процессами, которые обеспечивают работу сервисов подключения к локальным и глобальным сетям.

Сервер xinetd представляет собой единственный процесс, который выполняет прослушивание всех портов на наличие запросов от других сервисов, перечисленных в файле конфигурации `xinetd.conf` (расположен в директории `/etc`): когда на порт поступает запрос, сервер xinetd запускает соответствующий сервер.

Сервисы, перечисленные в конфигурационном файле сервера xinetd, можно разделить на две группы.

Сервисы из первой группы («multi-threaded») на каждый новый запрос запускают новый серверный процесс.

Для таких сервисов сервер xinetd продолжает прослушивать сеть на соответствующем порту, ожидая новых запросов на порождение нового процесса.

В другую группу («single-threaded») включаются сервисы службы, которые в состоянии обрабатывать новые соединения. В ходе работы с ними сервер xinetd прекращает обработку новых запросов до тех пор, пока серверный процесс не завершит свою работу. Сервисы в этой группе также обычно относят к группе

«datagram-based», работающих с дейтаграммными протоколами передачи данных формата UDP.

Сервер xinetd позволяет сохранять системные ресурсы за счет контроля запуска серверных процессов. Полностью соответствуя назначению запускать требуемые сервисы, сервер xinetd осуществляет также функции контроля доступа и регистрации событий. Кроме того, сервер xinetd не ограничен сервисами, перечисленными в файле `/etc/services`. Также допускается использовать сервер xinetd для запуска сервисов специального назначения.

Синтаксис:

`xinetd [опции]`

Опции:

- `--d` – активирует режим отладки. Указание этой опции приводит к большому количеству отладочных сообщений, которые делают возможным использование отладчика на xinetd;
- `--syslog syslog_facility` – разрешает протоколирование создаваемых xinetd сообщений через syslog с заданным syslogfacility. Поддерживаются следующие имена facility: `daemon, auth, user, local[0-7]` (назначение можно просмотреть в `syslog.conf`). Данная опция неэффективна в режиме отладки, так как все сообщения отправляются на терминал;
- `--filelog файл_журнала` – сообщения, создаваемые xinetd будут помещаться в указанный файл. Сообщения всегда добавляются к уже существующему файлу. Если файл не существует, то он будет создан. Данная опция неэффективна в режиме отладки, так как все сообщения отправляются на терминал;
- `-f файл_настроек` – задает файл, который xinetd использует для настройки. По умолчанию это `/etc/xinetd.conf`;
- `--pidfile pid_файл` – в этот файл записывается идентификатор процесса. Данная опция неэффективна в режиме отладки;
- `--stayalive` – xinetd будет оставаться запущенным, даже если не задано никаких служб;

- `--loop rate` – устанавливает верхнюю величину цикла, по которой определяется, что служба работает с ошибками и по которой она отключается. Величина цикла задается в терминах количества серверов в секунду, которое может быть запущено в обработку (fork). Для этой опции, корректное значение определяется скоростью вашей машины. По умолчанию равно 10;
- `--reuse` – xinetd будет устанавливать опцию сокета SO_REUSEADDR перед привязкой сокета службы к какому-либо интернет-адресу. Это позволяет привязать адрес, даже если есть программа, которая уже использует его, например, в том случае, если некоторые серверы были запущены во время предыдущего запуска xinetd и еще не завершили свою работу. Данная опция не оказывает влияния на службу RPC;
- `--limit proc_limit` – устанавливает ограничение на количество одновременно запущенных процессов, которые может запустить xinetd. Ее назначение предотвращать переполнение таблицы процессов;
- `--logprocs limit` – устанавливает ограничение на количество одновременно запущенных серверов на один идентификатор удаленного пользователя;
- `--shutdownprocs limit` – устанавливает ограничение на количество одновременно запущенных серверов для завершения работы службы;
- `--version` – вывести информацию о версии xinetd;
- `--cc interval` – xinetd будет выполнять периодические проверки своего внутреннего состояния каждые interval секунд.

Опции `syslog` и `filelog` являются взаимноисключающими. Если ни одна из них не задана, то по умолчанию используется `syslog` с `daemonfacility`. Не путайте сообщения xinetd с сообщениями, которые создаются службами. Последние протоколируются только если это задано в файле с настройками.

Сервер xinetd выполняет определенные действия при получении определенных сигналов. Действия, ассоциированные с соответствующими сигналами, могут быть переопределены путем редактирования `config.h` и последующей компиляции.

Сигналы:

- SIGHUP – заставляет выполнить жесткую перенастройку, означающую, что xinetd перечитает файл с настройками и завершит работу серверов для тех служб, которые больше не доступны. Управление доступом выполняется снова на уже запущенных серверах через проверку удаленных подключений, времени доступа и копий серверов. Если количество копий серверов уменьшается, то некоторые произвольно выбранные сервера будут убиты, чтобы соблюсти ограничение; это случится после завершения работы тех серверов, которые попадают под ограничение доступа с удаленных адресов или ограничение времени доступа. Также, если флаг INTERCEPT был сброшен и происходит его установка, то будет завершена работа любых запущенных серверов для служб с этим флагом. Цель такого поведения – убедиться, что после жесткой перенастройки не будет запущено серверов, которые могут принимать пакеты с тех адресов, которые не соответствуют критериями управления доступом;
- SIGQUIT – приводит к завершению работы;
- SIGTERM – завершает работу всех запущенных серверов перед завершением работы xinetd;
- SIGUSR1 – приводит к снятию дампа внутреннего состояния (по умолчанию файл дампа это `/var/run/xinetd.dump`; чтобы изменить данное имя файла нужна правка `config.h` и перекомпиляция);
- SIGIOT – производит внутреннюю проверку того, что структуры данных, используемые программой не повреждены. Когда проверка завершится, xinetd сгенерирует сообщение о том, успешно прошла проверка или нет.

При реконфигурации файлы журналов закрываются и вновь открываются. Это позволяет удалять старые файлы журналов.

16.12. Работа со смарт-картами

Для настройки работы со смарт-картами нужно установить дополнительные пакеты:

1) синхронизировать файлы описаний пакетов с источником пакетов, выполнив команду:

```
# apt-get update
```

2) установить пакеты для поддержки программно-аппаратного комплекса электронно-цифровой подписи и хранения ключевой информации «RUTOKEN», выполнив команду:

```
# apt-get install opensc pcsc-lite pam_pkcs11 librtpkcs11ecp pcsc-lite-ccid openssl-engine_pkcs11 nss-utils
```

И для рабочей станции пакет: `lightdm-gtk-greeter.`

16.12.1. Двухфакторная аутентификация

На токене должны присутствовать ключевая пара и сертификат.

Для генерирования ключевой пары на токене и создания самоподписанного сертификата, используя openssl, нужно выполнить следующие действия (путь зависит от архитектуры, в примере для 64 бит):

1) запустить сервис поддержки смарт-карт, выполнив команду:

```
# systemctl start pcscd
```

2) сгенерировать ключевую пару, выполнив команду:

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

3) сгенерировать сертификат в формате PEM:

```
# openssl
OpenSSL> engine dynamic –pre
SO_PATH:/usr/lib64/openssl/engines-*/libpkcs11.so -pre ID:pkcs11 -pre LIST_ADD:1 -pre LOAD -pre
MODULE_PATH:/usr/lib64/librtpkcs11ecp.so
```

где `engines-*` – текущая версия модулей openssl;

4) конвертировать сертификат из формата PEM в формат CRT:

```
OpenSSL> x509 -in CA.pem -out cert.crt -outform DER
```

5) сохранить сертификат на аутентифицирующий носитель:

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

Для настройки двухфакторной аутентификации нужно выполнить следующие действия:

1) отредактировать файл `/etc/security/pam_pkcs11/pam_pkcs11.conf` для установки аутентификации по «RUTOKEN» следующим образом:

   - закомментировать строку `# use_pkcs11_module = opensc;` и добавить строку `use_pkcs11_module = rutoken;`:

```
# use_pkcs11_module = opensc;
use_pkcs11_module = rutoken;
```

   - после строки `use_pkcs11_module = rutoken;` добавить модуль rutoken:

```
use_pkcs11_module = rutoken;
pkcs11_module rutoken {
ca_dir = /etc/security/pam_pkcs11/cacerts;
crl_dir = /etc/security/pam_pkcs11/crls;
module = /usr/lib64/librtpkcs11ecp.so;
cert_policy = subject;
description = "Rutoken ECP";
slot_description = "none";
}
```

2) включить сервисы поддержки смарт-карт, выполнив команды:

```
# systemctl enable pcscd
# systemctl start pcscd
```

3) включить системную аутентификацию по смарт-картам в графическом интерфейсе, выполнив команду:

```
# control system-auth pkcs11
```

4) добавить информацию об удостоверяющем центре на машину (файл о сертификате создан в начальных условиях):

```
cp CA.pem /etc/security/pam_pkcs11/cacerts/
certutil -A -n 'Root CA' -t 'CT,C,C' -a -d /etc/pki/nssdb/ -i ./CA.pem
```

5) добавить информацию о сертификате в домашний каталог пользователя:

```
mkdir /home/user/.eid/
cat CA.pem > /home/user/.eid/authorized_certificates
```

6) для возможности аутентификации по сертификату в консоли нужно в файл `/etc/pam.d/login` вначале добавить строку:

```
auth       [success=done authinfo_unavail=ignore ignore=ignore default=die] pam_pkcs11.so
```

16.13. Поддержка файловых систем

Файловая система представляет из себя набор правил, определяющих то, как хранятся и извлекаются документы, хранящиеся на устройстве.

Проверка поддержки файловых систем ext2, ext3, ext4, iso9660, fat16, fat32, ntfs:

1) создать раздел объемом менее 4 Гбайт на flash-накопителе (например, `/dev/vdc1`).
2) для создания iso файла установить пакет genisoimage:
   ```
   # apt-get install genisoimage
   ```
3) создать директорию `/mnt/filesystem`, в которую будет монтироваться раздел:
   ```
   # mkdir /mnt/filesystem
   ```
4) отформатировать раздел в проверяемую файловую систему:
   - для ext2:
     ```
     # mkfs.ext2 /dev/vdc1
     ```
   - для ext3:
     ```
     # mkfs.ext3 /dev/vdc1
     ```
   - для ext4:
     ```
     # mkfs.ext4 /dev/vdc1
     ```
   - для fat16:
     ```
     # mkfs.fat -F 16 /dev/vdc1
     ```
   - для fat32:
     ```
     # mkfs.fat -F 32 /dev/vdc1
     ```
   - для ntfs:
     ```
     # mkfs.ntfs /dev/vdc1
     ```
   - для iso9660 – создать iso-файл из каталога `/etc`:
     ```
     # mkisofs -r -jcharset koi8-r -o /root/cd.iso /etc
     ```
5) для проверки поддержки файловых систем ext2, ext3, ext4, fat16, fat32, ntfs:
   - примонтировать раздел с файловой системой в каталог `/mnt/filesystem`:
     ```
     # mount /dev/vdc1 /mnt/filesystem
     ```

- проверить возможность записи файла на текущую файловую систему:

  ```
  # echo test_content > /mnt/filesystem/test.fs
  ```

- проверить командой:

  ```
  # ls -l /mnt/filesystem/test.fs
  -rw-r--r--.  1  root  root  13  май  23  20:10
  /mnt/filesystem/test.fs
  ```

- проверить возможность чтения файла с текущей файловой системой:

  ```
  # cat /mnt/filesystem/test.fs
  ```

6) для проверки поддержки файловой системы iso9660 смонтировать созданный iso файл в каталог `/mnt/filesystem/` (файл образа диска будет примонтирован в режиме «только для чтения»):

   ```
   # mount -o loop,ro /root/cd.iso /mnt/filesystem/
   ```

16.14. Поддержка сетевых протоколов

16.14.1. SMB

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

16.14.2. NFS

16.14.2.1. Настройка сервера NFS

П р и м е ч а н и е . Должен быть установлен пакет nfs-server:

```
# apt-get install nfs-server
```

Запустить NFS-сервер и включить его по умолчанию:

```
# systemctl start nfs
# systemctl enable nfs
```

В файле `/etc/exports` следует указать экспортируемые каталоги (каталоги, которые будет разрешено монтировать с других машин):

```
/mysharedir ipaddr1(rw)
```

Например, разрешить монтировать /home на сервере:

```
# vim /etc/exports
/home 192.168.88.0/24 (no_subtree_check,rw)
```

где:

- `192.168.88.0/24` – разрешение экспорта для подсети 192.168.88.X;

- `rw` – разрешены чтение и запись.

Подробную информацию о формате файла можно посмотреть командой:

```
man exports
```

После внесения изменений в файл `/etc/exports` нужно выполнить команду:

```
# exportfs –r
```

Проверить список экспортируемых файловых систем можно, выполнив команду:

```
# exportfs
/home 192.168.8.0/24
```

16.14.2.2. Использование NFS

Подключение к NFS-серверу можно производить как вручную, так и настроив автоматическое подключение при загрузке.

Для ручного монтирования:

- создать точку монтирования:

```
# mkdir /mnt/nfs
```

- примонтировать файловую систему:

```
# mount -t nfs 192.168.88.218:/home /mnt/nfs
```

где:

а) `192.168.88.3` – IP-адрес сервера NFS;

б) `/mnt/nfs` – локальный каталог куда монтируется удаленный каталог.

- проверить наличие файлов в `/mnt/nfs`:

```
# ls –al /mnt/nfs
```

Должен отобразиться список файлов каталога `/home` расположенного на сервере NFS.

Для автоматического монтирования к NFS-серверу при загрузке нужно добавить следующую строку в файл `/etc/fstab`:

```
192.168.88.218:/home   /mnt/myshare   nfs   intr,soft,nolock,_netdev,x-systemd.automount   0 0
```

Примечание. Прежде чем изменять `/etc/fstab`, попробуйте смонтировать вручную и убедитесь, что все работает.

16.14.3. FTP

В состав дистрибутива ОС Альт СП входит vsftpd (Very Secure FTP Daemon) – полнофункциональный FTP-сервер, позволяющий обслуживать как анонимные запросы, так и запросы от пользователей, зарегистрированных на сервере и имеющих полноценный доступ к его ресурсам.

Для установки vsftpd нужно выполнить следующую команду:

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

16.14.3.1. Организация анонимного доступа на основе vsftpd

В конфигурационном файле сервера `/etc/vsftpd.conf` за разрешение анонимного доступа к серверу vsftpd отвечает параметр `anonymous_enable`, который по умолчанию имеет значение `YES`, т. е. анонимный доступ к серверу разрешен.

При установке vsftpd в системе автоматически создается учетная запись псевдопользователя «novsftpd». Это регистрационное имя не должно использоваться кем-либо для входа в систему, поэтому реальный пароль для него не задается. Вместо командного интерпретатора указывается `/dev/null`.

При установке пакета anonftp автоматически создается каталог, который будет корневым при анонимном подключении, – `/var/ftp` с правами доступа. Владельцем этого каталога является пользователь root. Группой-владельцем каталога является специальная группа ftpadmin, предназначенная для администраторов FTP-сервера.

Если требуется создать в области для анонимного доступа дерево каталогов, следует в каталоге `/var/ftp/pub` установить права доступа 2775. При этом анонимным пользователям FTP-сервера будет предоставлен доступ на чтение к файлам, находящимся в каталоге.

Владельцем каталога следует назначить пользователя root. В качестве группы, которой принадлежит `/var/ftp/pub`, следует назначить группу ftpadmin, включив в нее пользователей, которым нужно изменять содержимое каталогов FTP-сервера.

Примечание. Не рекомендуется работать с содержимым от имени пользователя с идентификатором root.

Чтобы разрешить анонимным пользователям сервера доступ на запись, нужно создать каталог `/var/ftp/incoming` с правами доступа 3773 (группа-владелец – «ftpadmin»), тем самым предоставив анонимным пользователям право записи в этот каталог, но лишив их возможности просмотра его содержимого.

16.14.3.2. Доступ к серверу зарегистрированных пользователей

Чтобы предоставить доступ к FTP-серверу для локально зарегистрированных пользователей, нужно внести изменения в конфигурационный файл `/etc/vsftpd.conf`. Для этого достаточно удалить знак комментария перед директивой `local_enable=YES`. В такой конфигурации клиенты FTP-сервера получат доступ к любым каталогам файловой системы, для которых такой доступ разрешен исходя из прав соответствующих локальных пользователей. Это могут быть как домашние каталоги пользователей, так и системные каталоги. Если в настройках vsftpd разрешена запись, клиенты получат и все права на запись, которыми располагают эти пользователи.

Сервер vsftpd позволяет ограничить возможность пользователей, зарегистрированных локально, перемещаться по дереву каталогов. При этом процесс, работающий с клиентом, будет выполняться в изолированной среде (chrooted environment), и пользователь будет иметь доступ только к своему домашнему каталогу и его подкаталогам.

Чтобы ограничить таким образом доступ к каталогам для отдельных пользователей, нужно удалить знаки комментариев у следующих строк в конфигурационном файле:

```
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
```

В файле `/etc/vsftpd/chroot_list` следует перечислить регистрационные имена пользователей, для которых должна использоваться изолированная среда выполнения. Можно использовать для этого и другой файл, указав его имя в строке `chroot_list_file` конфигурационного файла.

Чтобы ограничить доступ к дереву каталогов для всех пользователей, зарегистрированных локально, следует добавить в конфигурационный файл директиву `chroot_local_user=YES`.

В этом случае имена пользователей, перечисленные в файле `/etc/vsftpd/chroot_list` (при условии, что у строк, указанных выше, удалены знаки комментария), имеют противоположное действие.

Для них не используется изолированная среда выполнения, и перемещение по файловой иерархии не ограничивается домашним каталогом.

Чтобы запретить анонимный доступ к FTP-серверу, нужно поставить знак комментария в начале строки `anonymous_enable=YES` в конфигурационном файле.

16.14.3.3. Дополнительные сведения о настройке сервера

Сервер vsftpd способен осуществлять всю передачу данных в пассивном режиме, что сопряжено со значительно меньшим риском.

Чтобы разрешить использование только пассивного режима, достаточно удалить символ комментария у директивы `port_enable=NO` в конфигурационном файле.

Чтобы разрешить запись файлов на сервер, следует удалить знак комментария у директивы `write_enable=YES`. Этого достаточно для того, чтобы пользователи, зарегистрированные локально, получили возможность загружать файлы в те каталоги, для которых они располагают правами на запись.

Чтобы разрешить запись файлов анонимным пользователям, нужно, кроме этого, удалить знак комментария у строки `anon_upload_enable=YES`. Специальный непривилегированный пользователь, используемый для работы с анонимными клиентами, должен иметь права на запись в один или несколько каталогов, доступных таким клиентам.

Параметры использования vsftpd (в том числе относящиеся к безопасности) могут быть заданы при помощи xinetd.

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.

16.14.3.4. Пример настройки FTP-сервера

Настройте параметры конфигурации xinetd для 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 # лимит адресного пространства
server = /usr/sbin/vsftpd # путь к исполняемому файлу
# only_from = 192.168.0.0 # доступ из всей подсети
# доступ с указанных адресов
# only_from = 207.46.197.100 207.46.197.101
only_from = 0.0.0.0 # неограниченный по адресам доступ
access_times = 2:00-9:00 12:00-24:00 # время, доступа
}
```

Перезапустите xinetd:

```
# systemctl restart xinetd
```

Измените настройку прав доступа в файле `/etc/vsftpd/conf`:

```
local_enable=YES
```

Убедитесь в нормальной работе FTP-сервера:

```
# netstat -ant | grep 21
tcp        0     0 0.0.0.0:21        0.0.0.0:*             LISTEN
FTP-сервер запущен и принимает соединения на 21 порту.
```

Обратитесь к серверу по протоколу FTP:

```
$ lftp user@localhost
Пароль:
lftp user@localhost:~>
```

П р и м е ч а н и е . Пакет lftp должен быть заранее установлен.
Соединение на сервере по протоколу FTP успешно установлено.

16.14.3.5. Подключение рабочей станции

П р и м е ч а н и е . На рабочей станции должен быть установлен пакет lftp:

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

Для создания подключения по протоколу FTP в консоли, на рабочей станции нужно выполнить команду:

```
$ lftp user@192.168.88.218
```

Пароль:

```
lftp user@192.168.8.218:~>pwd
ftp://user@192.168.8.218
```

Для создания подключения по протоколу FTP в графической среде MATE можно запустить файловый менеджер, указать в адресной строке протокол и адрес сервера (рис. 439).

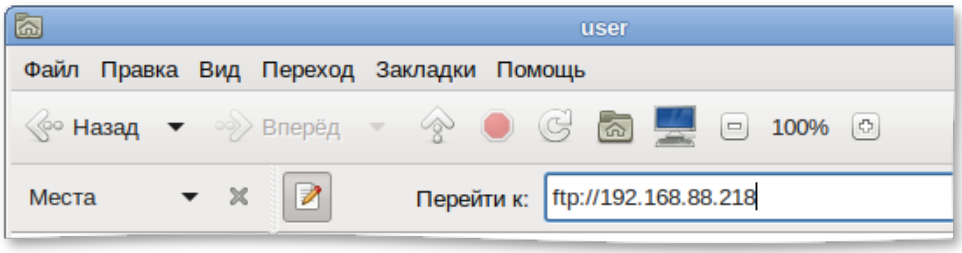


Рис. 439

Нажать клавишу «Enter».

В появившемся окне указать имя пользователя, пароль и нажать на кнопку «Подключиться» (рис. 440).

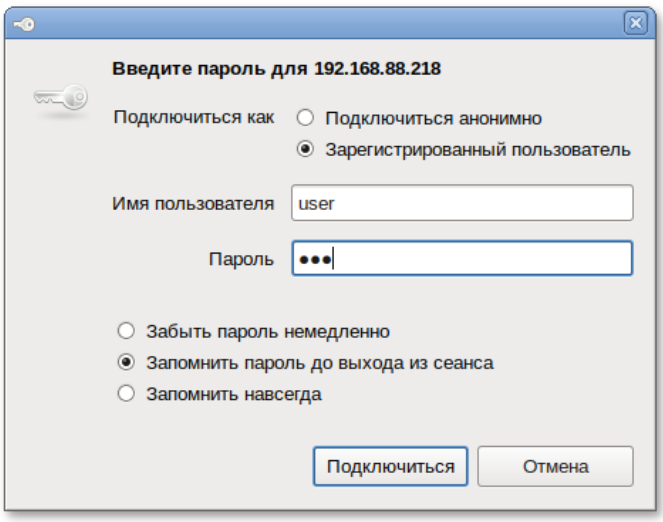


Рис. 440

16.14.4. NTP

16.14.4.1. Настройка сервера NTP

В качестве NTP-сервера/клиента используется сервер времени chrony:

- chronyd – демон, работающий в фоновом режиме. Он получает информацию о разнице системных часов и часов внешнего сервера времени и корректирует локальное время. Демон реализует протокол NTP и может выступать в качестве клиента или сервера.
- chronyc – утилита командной строки для контроля и мониторинга программы. Утилита используется для тонкой настройки различных параметров демона, например, позволяет добавлять или удалять серверы времени.

Выполнить настройку NTP-сервера можно следующими способами:

1) в ЦУС настроить модуль «Дата и время» на получение точного времени с NTP-сервера (см. п. 8.17.7).
2) указать серверы NTP в директиве server или pool в файле конфигурации NTP `/etc/chrony.conf`:

```
allow all #Разрешить NTP-клиенту доступ из локальной сети
pool pool.ntp.org iburst #параметр iburst используется для ускорения начальной синхронизации
```

3) и перезапустить сервис командой:

```
# systemctl restart chronyd
```

Убедиться в нормальной работе NTP-сервера, выполнив команду:

```
# systemctl status chronyd.service
```

Выполнить настройку NTP-сервера можно следующими способами:

1) в ЦУС настроить модуль «Дата и время» на получение точного времени с NTP-сервера (см. п. 8.17.7).
2) раскомментировать директиву `listen` и указать серверы NTP в директиве `servers` в файле конфигурации NTP `/etc/chrony.conf`:

```
allow 192.168.1.0/24
servers pool.ntp.org
```

Примечание. Формат записи `allow _адреса локальной сети_` или можно задать доступ для всех клиентов:
`allow all`

3) и перезапустить сервис командой:

```
# systemctl restart chronyd.service
```

4) убедиться в нормальной работе NTP-сервера, выполнив команду:

```
# systemctl status chronyd.service
```

Примечание. С сервера времени openntpd можно будет обновляться, только после того, как он синхронизируется с другими серверами. Это может занять достаточно продолжительное время.

16.14.4.2. Настройка рабочей станции

Настроить в ЦУС модуль «Дата и время» на получение точного времени с NTP-сервера (в качестве NTP-сервера указать IP-адрес сервера NTP) и нажать на кнопку «Применить» (рис. 441).

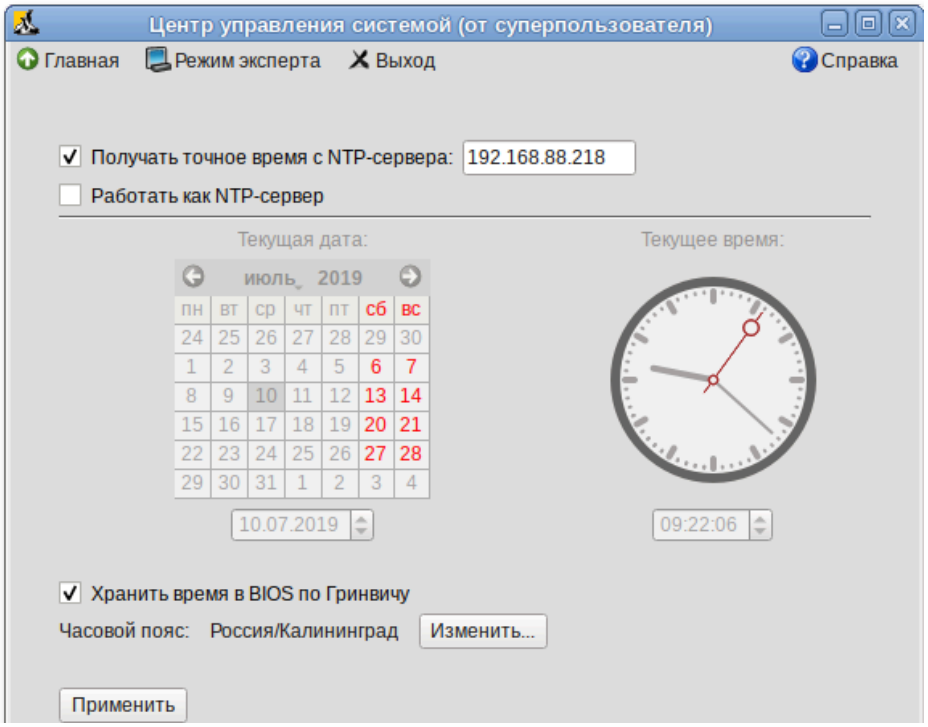


Рис. 441

Проверить текущие источники времени:

```
$ chronyc sources
210 Number of sources = 1
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^? 192.168.88.218                3   8     0   23m   +396us[ -803us] +/-   55ms
```

Проверить статус источников NTP:

```
$ chronyc activity
```

```
200 OK
1 sources online
0 sources offline
0 sources doing burst (return to online)
0 sources doing burst (return to offline)
0 sources with unknown address
```

16.14.5. HTTP(S)

16.14.5.1. Настройка HTTP-сервера

Установить пакет apache2-base:

```
# apt-get install apache2-base
```

Запустить httpd2:

```
# systemctl start httpd2
```

Убедиться, что служба httpd2 запущена:

```
# systemctl status httpd2
```

Создать стартовую страницу для веб-сервера:

```
# echo “Hello, World” >/var/www/html/index.html
```

16.14.5.2. Проверка настройки на рабочей станции

Запустить веб-браузер, перейти по адресу `http://<IP-сервера>:>` (рис. 442).

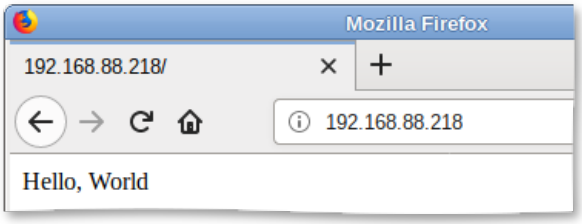


Рис. 442

Также можно выполнить команду:

```
$ curl http://192.168.88.218
Hello, World
```

Происходит обращение к серверу и получение данных по протоколу http.

16.15. Виртуальная (экранная) клавиатура

Onboard – гибкая в настройках виртуальная (экранная) клавиатура.

Виртуальная клавиатура полезна тогда, когда по каким-либо причинам, нет возможности использовать обычную клавиатуру. Так же виртуальная клавиатура может оказаться удобной пользователям сенсорных экранов (touchscreen).

П р и м е ч а н и е . На рабочей станции должен быть установлен пакет onboard:

```
# apt-get install onboard
```

16.15.1. Клавиатура onboard при входе в систему

Для того чтобы появилась возможность использовать виртуальную клавиатуру при входе в систему, нужно в файле `/etc/lightdm/lightdm-gtk-greeter.conf` выставить параметр `keyboard` в значение `onboard --xid`:

```
# vim /etc/lightdm/lightdm-gtk-greeter.conf
[greeter]
...
keyboard=onboard --xid
...
```

На странице входа следует щелкнуть значок  на панели инструментов, а затем отметить пункт «Экранная клавиатура». На экране появится виртуальная клавиатура, ее можно использовать для ввода пароля.

16.15.2. Клавиатура onboard при разблокировке экрана

Для того, чтобы клавиатура работала при разблокировке экрана, следует выставить следующие параметры dconf:

```
org.mate.screensaver.embedded-keyboard-enabled=true
org.mate.screensaver.embedded-keyboard-command="onboard --xid"
```

Установить параметры dconf для конкретного пользователя можно, выполнив команды (под этим пользователем):

```
$ gsettings set org.mate.screensaver embedded-keyboard-enabled true
$ gsettings set org.mate.screensaver embedded-keyboard-command "onboard
--xid"
```

Для того, чтобы выставить настройки dconf глобально для всех пользователей, нужно (все действия выполняются от имени root):

1) создать файл `/etc/dconf/profile/user` следующего содержания:

```
user-db:user
system-db:local
```

2) создать, если он еще не создан, каталог `/etc/dconf/db/local.d`:

```
# mkdir /etc/dconf/db/local.d
```

3) создать файл для локальной базы данных в `/etc/dconf/db/local.d/00_screensaver` следующего содержания:

```
[org/mate/screensaver]
embedded-keyboard-enabled=true
embedded-keyboard-command="onboard --xid"
```

4) обновить системные базы данных, выполнив команду:

```
# dconf update
```

Просмотреть настройки `org.mate.screensaver` можно, выполнив команду:

```
$ gsettings list-recursively org.mate.screensaver
```

```
org.mate.screensaver mode 'single'
org.mate.screensaver status-message-enabled true
org.mate.screensaver lock-dialog-theme 'default'
org.mate.screensaver logout-command ''
org.mate.screensaver user-switch-enabled true
org.mate.screensaver embedded-keyboard-enabled true
org.mate.screensaver idle-activation-enabled true
org.mate.screensaver lock-delay 0
org.mate.screensaver logout-delay 120
org.mate.screensaver cycle-delay 10
org.mate.screensaver lock-enabled false
org.mate.screensaver logout-enabled false
org.mate.screensaver embedded-keyboard-command 'onboard --xid'
org.mate.screensaver themes ['screensavers-gnomelogo-floaters']
org.mate.screensaver power-management-delay 30
```

В результате при разблокировке экрана появится виртуальная клавиатура, ее можно использовать для ввода пароля.

16.15.3. Настройки onboard

Onboard имеет множество настроек, сворачивается в системный трей и (или) в «индикатор действия», имеет несколько тем оформления, с возможностью настройки цвета и формы клавиш (можно создать собственную тему полностью), прозрачности, включения/выключения рамки окна.

Запустить виртуальную клавиатуру Onboard можно, выбрав на панели инструментов меню MATE → «Приложения» → «Стандартные» → «Onboard».

Окно настроек Onboard можно открыть, нажав правой клавишей мыши по значку Onboard  в системном трее и выбрав пункт «Параметры».

В настройках можно:

- подобрать стилевое оформление экранной клавиатуры;

- закрепить к верхнему или нижнему краю экрана рабочего стола;
- включить или отключить звук нажатых клавиш, а также показывать нажатые клавиши;
- изменить раскладку клавиатуры (например, выбрать эргономичную клавиатуру или клавиатуру для небольших экранов).

16.16. Управление печатью

В ОС Альт СП используется система печати CUPS, которая позволяет выполнять следующие действия:

- управляет заданиями на печать;
- исполняет административные команды;
- предоставляет информацию о состоянии принтеров локальным и удаленным программам;
- информирует пользователей, если это требуется.

Система печати CUPS решает задачу монопольной постановки задания в очередь на печать. Данная функция предполагает невозможность вывода документа на печать в обход системы печати.

Существует два способа настройки принтера:

- утилита «Настройка принтера» (пакет system-config-printer);
- веб-интерфейс CUPS (Common UNIX Printing System) (пакет cups).

16.16.1. Устройство CUPS

В состав файлов конфигурации CUPS входят следующие файлы:

- файл конфигурации сервера CUPS (`/etc/cups/cupsd.conf`);
- файлы определения принтеров и классов (`/etc/cups/printers.conf`, `/etc/cups/classes.conf`);
- файлы типа MIME и файлы правил преобразования;
- файлы описания PostScript-принтеров (PPD).

16.16.1.1. Файл конфигурации сервера CUPS

Конфигурационный файл сервера очень похож на файлы конфигурации веб-сервера и определяет все свойства управления доступом. Настраивать

CUPS можно либо непосредственно редактируя файл конфигурации `/etc/cups/cupsd.conf`, либо в веб-интерфейсе CUPS (рис. 443). Веб-интерфейс CUPS можно запустить следующими способами:

- в графической среде MATE: «Приложения» → «Системные» → «Параметры печати»;
- в веб-браузере: `http://localhost:631`.

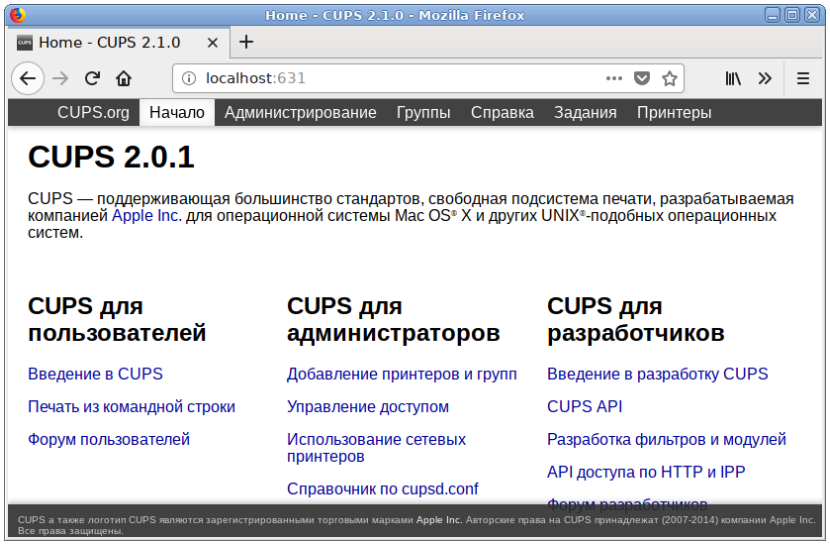


Рис. 443 – Веб-интерфейс CUPS

Если файл `cupsd.conf` редактируется в консоли для применения изменения, нужно перезапустить службу cups, выполнив команду:

```
# systemctl restart cups
```

Если файл `cupsd.conf` редактируется в веб-интерфейсе, то служба cups автоматически перезапускается после нажатия на кнопку «Сохранить изменения».

Файл конфигурации `cupsd.conf` начинается с ряда глобальных директив, которые оформлены в виде пар имя – значение.

`LogLevel` указывает подробность журналирования. Доступные значения: `none` (не записывать логи), `emerg`, `alert`, `crit`, `error`, `warn` (по умолчанию), `notice`, `info`, `debug`, `debug2` (подробный вывод).

`PageLogFormat` определяет формат строк журнала печати (файл `/var/log/cups/page_log`). Последовательности, начинающиеся со знака процента (%), заменяются соответствующей информацией:

- `% {name}` – значение указанного атрибута IPP;

- % C – количество копий для текущей страницы;
- % P – номер текущей страницы;
- % T – текущую дату и время в общий формат журнала;
- % j – идентификатор задания;
- % p – имя принтера;
- % u – имя пользователя.

По умолчанию строка PageLogFormat пустая (журнал печати не пишется). Для ведения журнала печати можно изменить эту строку:

PageLogFormat "%p %u %j %T %P %C %{job-billing} %{job-originating-host-name} %{job-name} %{media} %{sides}"

MaxLogSize задает максимальный размер журналов до их ротации. Значение 0 отключает ротацию.

Listen позволяет указать на каком IP-адресе будет доступен веб-интерфейс (по умолчанию localhost:631), а также прослушиваемый сокет.

Параметры Browsing задают настройки возможности CUPS обнаруживать принтеры в сети. Данная возможность поддерживается на уровне протокола IPP. Обнаружение происходит посредством широковещательных рассылок, что при большом количестве серверов CUPS или при частом отключении/подключении принтеров может порождать дополнительную нагрузку на сеть. Browsing – указывает CUPS предоставлять свои серверы в общий доступ, либо нет. Значения может принимать On или Off соответственно.

Директива DefaultAuthType указывает механизм аутентификации, который будет использоваться для организации доступа (по умолчанию Basic – использовать логины/пароли от локальной системы).

BrowseAllow и BrowseDeny – указывают CUPS на стороне клиента адреса, от которых может приниматься или отвергаться, соответственно, информация о принтерах. Формат директив соответствует директивам Allow и Deny. В качестве аргумента для данной директивы может быть как отдельный IP, так и подсеть в формате 10.0.0.0/24 или 10.0.0.0/255.255.255.0 или 10.0.0.0-10.0.0.255, так и значение

@LOCAL – обозначающее локальную сеть, а также имена хостов. Возможно использование нескольких данных директив.

Директива Order определяет порядок предоставления доступа к CUPS по умолчанию. Значение allow,deny определяет что доступ запрещен, если право на доступ не указано явно. Если директива имеет значение deny,allow, то доступ будет разрешен, если явно не запрещен.

Далее идут параметры, сгруппированные в разделы <Location /...>. Такие директивы определяют доступ к определенным функциям сервера:

- <Location /> – доступ к серверу;
- <Location /admin> – доступ к странице администрирования;
- <Location /admin/conf> – доступ к конфигурационным файлам;
- <Location /jobs> – доступ к заданиям;
- <Location /printer> – доступ к принтерам.

16.16.1.2. Управление политиками операций

Политики операций – это правила, используемые для каждой операции IPP в CUPS. Правила могут включать такие опции, как «пользователь должен предоставить пароль», «пользователь должен находиться в системной группе», «разрешать только из локальной системы» и т. д.

CUPS позволяет полностью переопределить правила для каждой операции и (или) принтера. Каждая политика имеет название и определяет правила контроля доступа для каждой операции IPP.

Политики операций используются для всех запросов IPP, отправленных в планировщик заданий, и оцениваются после правил управления доступом на основе местоположения. Таким образом, политики операций могут только добавлять дополнительные ограничения безопасности к запросу, а не ослаблять их. Для ограничений на уровне сервера нужно использовать правила управления доступом на основе местоположения, а для ограничений на отдельные принтеры, задачи или службы – политики операций.

Политики хранятся в файле `cupsd.conf` в разделах Policy. Каждая политика имеет название, которое используется для ее выбора. Внутри раздела политики находятся один или несколько подразделов Limit, в которых перечислены операции, на которые влияют правила внутри него.

Каждая политика имеет название. В названии политики можно использовать те же символы, что и в названии принтера, в частности все печатные символы, кроме пробела, слэша (/) и решетки (#).

В разделах `< Limit …>` определяется, какие ограничения должна содержать политика. Директивы внутри подраздела `Limit` могут использовать любую из директив ограничения: `Allow`, `AuthType`, `Deny`, `Encryption`, `Require` и `Satisfy`. В таблице 66 перечислены основные примеры для разных правил контроля доступа.

Таблица 66 – Правила контроля доступа

Уровень доступа	Директива
Разрешить всем	`Order allow,deny` `Allow from all`
Разрешить всем в локальной сети	`Order allow,deny` `Allow from @LOCAL`
Запретить всем/Отклонить операции	`Order allow,deny`
Требовать аутентификацию пользователя (Логин, Пароль)	`AuthType Basic`
Требовать CUPS аутентификацию CUPS (lppasswd) Password	`AuthType BasicDigest`
Требовать Kerberos	`AuthType Negotiate`
Только владелец	`Require user @OWNER`
Только администратор	`Require user @SYSTEM`
Члены группы foogroup	`Require user @foogroup`
Пользователи test или test1	`Require user test test1`
Требовать шифрование	`Encryption Required`

Пример политики, которая разрешает доступ только из подсети 10.110.1.x:

```
<Policy mypolicy>
# Операции, связанные с заданиями доступны только владельцам
# членам группы lab999 и администратору...
   <Limit Send-Document Send-URI Hold-Job Release-Job Restart-Job
Purge-Jobs Set-Job-Attributes Create-Job-Subscription Renew-
Subscription Cancel-Subscription Get-Notifications Reprocess-Job
Cancel-Current-Job Suspend-Current-Job Resume-Job Cancel-My-Jobs
Close-Job CUPS-Move-Job>
        Require user @OWNER @lab999 @SYSTEM
        Order allow,deny
```

```
          Allow from 10.110.1.0/24
        </Limit>

        # Все административные операции доступны только администратору
и членам  группы lab999, также необходима процедура аутентификации...
        <Limit  Pause-Printer  Resume-Printer  Set-Printer-Attributes
Enable-Printer     Disable-Printer     Pause-Printer-After-Current-Job
Hold-New-Jobs Release-  Held-New-Jobs  Deactivate-Printer  Activate-
Printer Restart-Printer  Shutdown-Printer  Startup-Printer  Promote-Job
Schedule-Job-After CUPS- Accept-Jobs CUPS-Reject-Jobs CUPS-Set-Default>
          AuthType Default
          Require user @lab999 @SYSTEM
          Order allow,deny
          Allow from 10.110.1.0/24
        </Limit>

        # Все остальные операции доступны из подсети 10.110.1.0/24 с
обязательной аутентификацией пользователей...
        <Limit All>
          AuthType Default
          Order allow,deny
          Allow from 10.110.1.0/24
        </Limit>
      </Policy>
```

После создания политики ее можно использовать двумя способами.

Первый способ – назначить ее в качестве политики по умолчанию для всей системы, используя директиву `DefaultPolicy` в файле `cupsd.conf`. Например:

```
DefaultPolicy mypolicy
```

Второй способ – связать политику с одним или несколькими принтерами. Для этого можно воспользоваться командой `lpadmin (8)` или веб-интерфейсом для изменения политики операций для каждого принтера. Например:

```
# lpadmin -p HP_LaserJet_M1536dnf_MFP -o printer-op-policy=mypolicy
```

16.16.1.3. Файлы описания принтеров и классов

Файлы описания принтеров и классов перечисляют доступные очереди печати и классы. Классы принтеров – наборы принтеров. Задания, посланные классу принтеров, направляются к первому доступному принтеру данного класса. Для редактирования файлов `/etc/cups/printers.conf` и `/etc/cups/classes.conf` можно использовать утилиту lpadmin.

Пример настройки для локального принтера:

```
<DefaultPrinter laserjet>
UUID urn:uuid:7efaaede-819d-3d9a-6270-3fe957597756
Info laserjet
Location host-15.localdomain
MakeModel HP LaserJet m1537dnf MFP pcl3, hpcups 3.19.1
DeviceURI
usb://HP/LaserJet%20M1536dnf%20MFP?serial=00CND9D8YC9C&interface=1
State Idle
StateTime 1553167952
ConfigTime 1553167952
Type 36892
Accepting Yes # принтер принимает задания
Shared Yes
JobSheets none none
QuotaPeriod 0
PageLimit 0
KLimit 0
OpPolicy default
ErrorPolicy stop-printer # остановить принтер при ошибке
Option job-hold-until indefinite
</DefaultPrinter>
```

16.16.1.4. Очередь печати

Очередь печати – механизм, который позволяет буферизовать и организовать задания, посылаемые на принтер. Нужность организации такого механизма обуславливается тем, что принтер является медленно действующим устройством, и задания не могут быть распечатаны мгновенно.

Очевидно, что в многопользовательской среде возникает конкуренция со стороны пользователей при доступе к принтерам, поэтому задания нужно располагать в очереди. Для этого используется буферный каталог `/var/spool/cups/`.

Файлы типов MIME перечисляют поддерживаемые MIME-типы (text/plain, application/postscript) и правила для автоматического обнаружения формата файла. Они используются сервером для определения поля Content-Type для GET- и HEAD-запросов и обработчиком запросов протоколов сетевой печати IPP (Internet Printing Protocol), чтобы определить тип файла.

Правила преобразования MIME перечисляют доступные фильтры. Фильтры используются, когда задание направляется на печать, таким образом, приложение может послать файл удобного (для него) формата системе печати, которая затем преобразует документ в требуемый печатный формат. Каждый фильтр имеет относительную «стоимость», связанную с ним, и алгоритм фильтрования выбирает набор фильтров, который преобразует файл в требуемый формат с наименьшей общей «стоимостью».

Файлы PPD описывают возможности всех типов принтеров. Для каждого принтера имеется один PPD-файл. Файлы PPD для не-PostScript-принтеров определяют дополнительные фильтры посредством атрибута cupsFilter для поддержки драйверов принтеров.

В ОС стандартным языком описания страниц является язык PostScript. Большинство прикладных программ (редакторы, веб-браузеры) генерируют программы печати на этом языке.

Когда нужно напечатать ASCII-текст, программа печати может быть ASCII-текстом. Имеется возможность управления размером шрифтов при печати ASCII-текста.

Управляющая информация используется для контроля доступа пользователя к принтеру и аудита печати. Также имеется возможность печати изображений в форматах GIF, JPEG, PNG, TIFF и документов в формате PDF.

Фильтр – программа, которая читает из стандартного входного потока или из файла, если указано его имя. Все фильтры поддерживают общий набор опций, включающий имя принтера, идентификатор задания, имя пользователя, имя задания, число копий и опции задания. Весь вывод направляется в стандартный выходной поток.

Фильтры предоставлены для многих форматов файлов и включают, в частности, фильтры файлов изображения и растровые фильтры PostScript, которые поддерживают принтеры, не относящиеся к типу PostScript. Иногда несколько фильтров запускаются параллельно для получения требуемого формата на выходе.

Программа backend – это специальный фильтр, который отправляет печатаемые данные устройству или через сетевое соединение. В состав системы печати включены фильтры для поддержки устройств, подключаемых с помощью параллельного и последовательного интерфейсов, а также шины USB.

Клиентские программы используются для управления заданиями и сервером печати.

Управление заданиями включает выполнение следующих действий:

- формирование;
- передачу серверу печати;
- мониторинг и управление заданиями в очереди на печать.

Управление сервером включает выполнение следующих действий:

- запуск/остановку сервера печати;
- запрещение/разрешение постановки заданий в очередь;
- запрещение/разрешение вывода заданий на принтер.

Основные пользовательские настройки содержатся в файлах конфигурации `client.conf` и `~/.cups/lpoptions`.

Для удаленного использования сервера печати нужно от имени пользователя с идентификатором root выполнить следующие команды:

```
cupsctl --remote-admin --remote-printers --remote-any
cupsctl ServerAlias=*
```

В случае использования сервера печати в едином пользовательском пространстве (далее – ЕПП) нужно задание соответствующего типа аутентификации: для работы в ЕПП значение параметра должно быть `DefaultAuthType Negotiate`, без использования ЕПП значение параметра должно быть `DefaultAuthType Basic`.

В файле конфигурации клиента `client.conf` должен быть задан один параметр ServerName, определяющий имя сервера печати, например:

```
ServerName computer.domain
```

В общем случае вывод данных на принтер происходит следующим образом:

1) программа формирует запрос на печать задания к серверу печати;

2) сервер печати принимает подлежащие печати данные, формирует в буферном каталоге файлы с содержимым задания и файлы описания задания, при этом задание попадает в соответствующую очередь печати;
3) сервер печати просматривает очереди печати для незанятых принтеров, находит в них задания и запускает конвейер процессов, состоящий из фильтров и заканчивающийся выходным буфером, информация из которого поступает в принтер посредством драйверов ОС;
4) контроль и мониторинг процесса печати выполняется с помощью программ lpq, lpc, lprm, lpstat, lpmove, cancel.

16.16.2. Установка принтера

Перед началом установки нужно убедиться в том, что в случае локального подключения принтер присоединен к соответствующему порту компьютера и включен, а в случае сетевого подключения принтер корректно сконфигурирован для работы в сети.

Окно «Настройки принтера» можно запустить следующими способами:

- в графической среде: панель инструментов MATE → «Система» → «Администрирование» → «Параметры печати»;
- из командной строки: командой system-config-printer.

Для добавления принтера в диалоговом окне «Настройки принтера» нужно нажать на кнопку «Добавить».

Примечание. Если возникает ошибка «Служба печати недоступна», нужно запустить терминал, и от имени системного администратора root выполнить команду `systemctl restart cups`. После этого следует вернуться к окну «Настройки принтера» и нажать на кнопку «Обновить».

В диалоговом окне «Аутентификация» следует ввести имя, и пароль пользователя, имеющего право изменять настройки принтера, после чего нажать на кнопку «OK» (рис. 444).

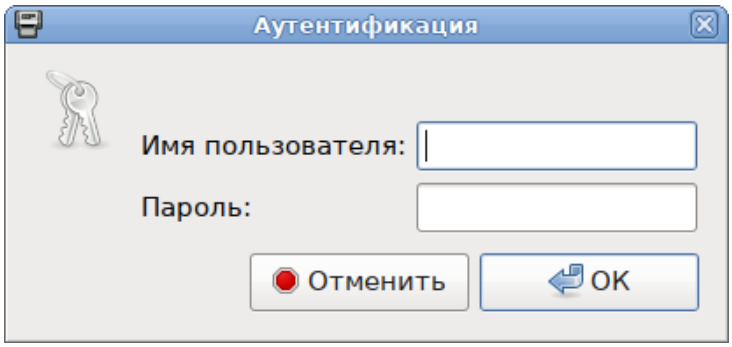


Рис. 444 – Диалоговое окно «Аутентификация»

Далее в открывшемся окне нужно нажать на кнопку «Добавить» и выбрать принтер, который нужно подключить и нажать на кнопку «Далее» (рис. 445).

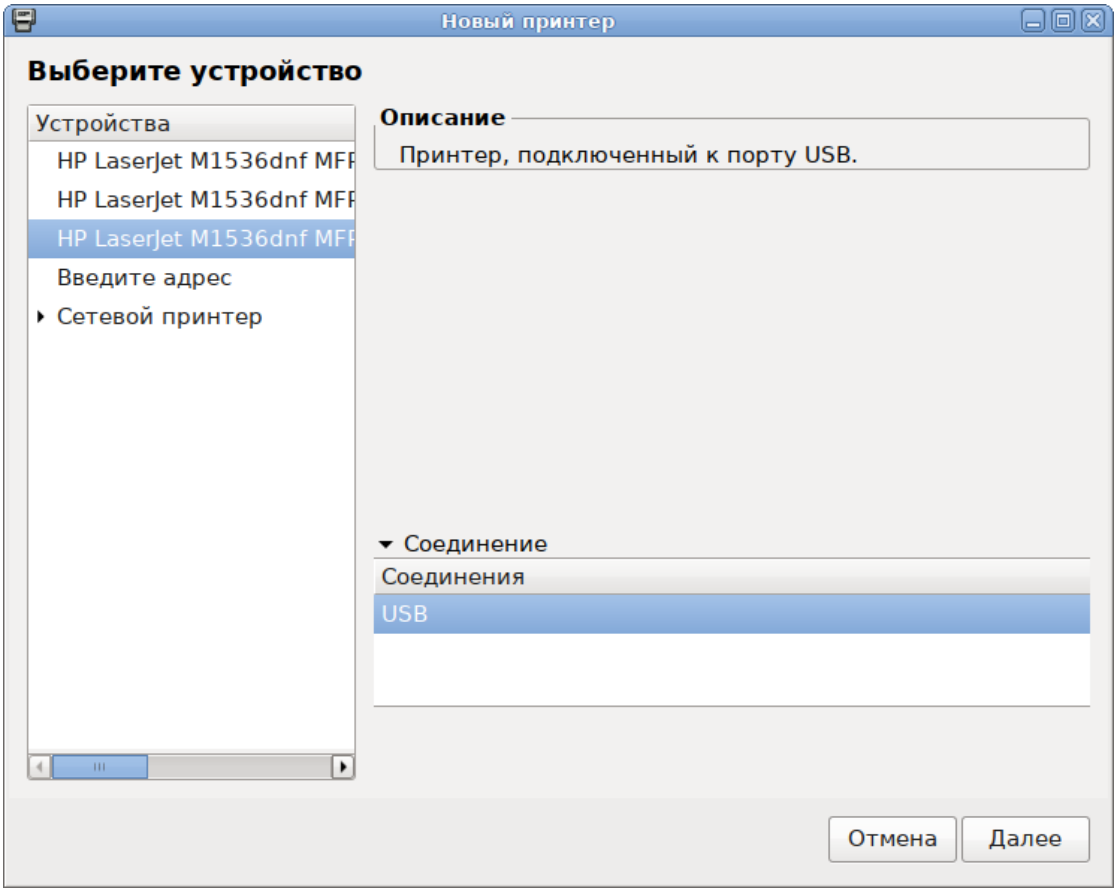


Рис. 445 – Выбор принтера

На следующих шагах настройки принтера нужно выбрать драйвер для принтера. Драйвер можно выбрать из базы данных, содержащей различные файлы описания принтеров (PPD-файлы) от производителей или предоставить файл описания PostScript-принтера (рис. 446).

После выбора драйвера в окне «Новый принтер» можно изменить название и описание принтера (рис. 447).

После нажатия кнопки «Применить» установка принтера завершена, принтер станет доступным для печати (рис. 448).

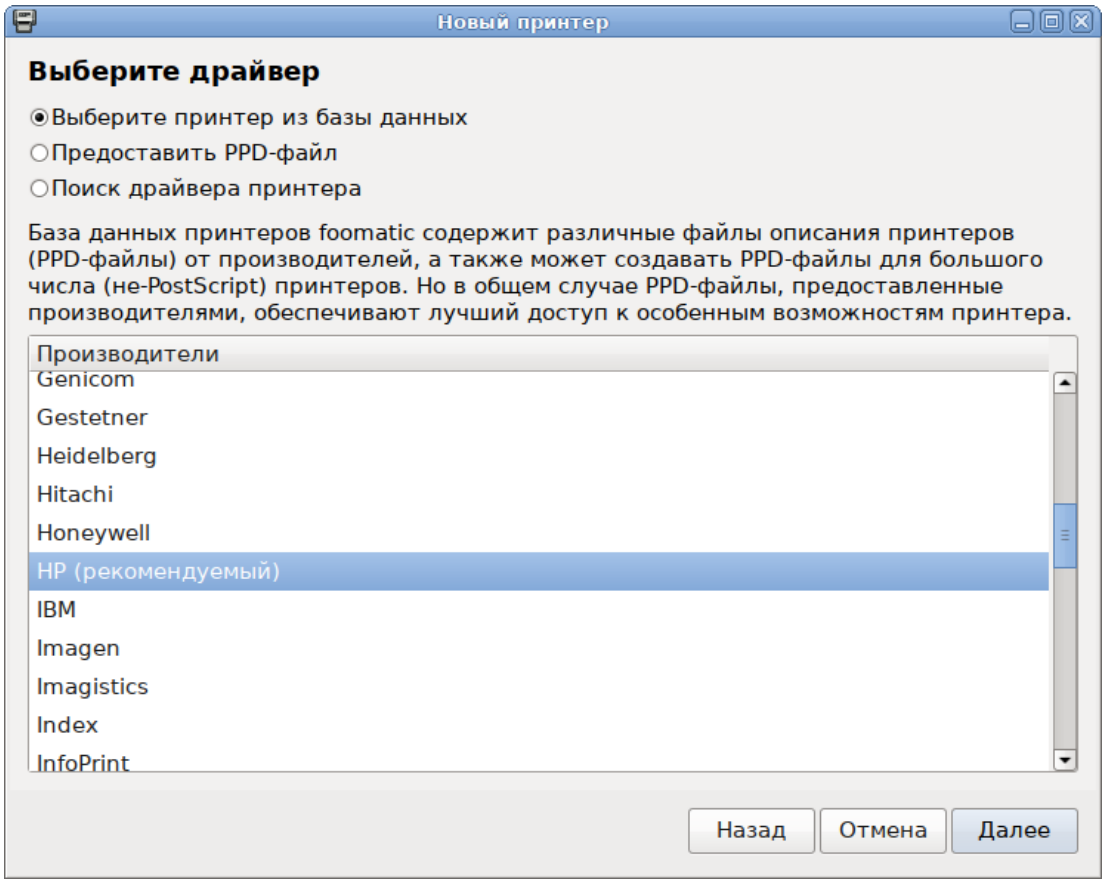


Рис. 446 – Выбор источника драйвера принтера

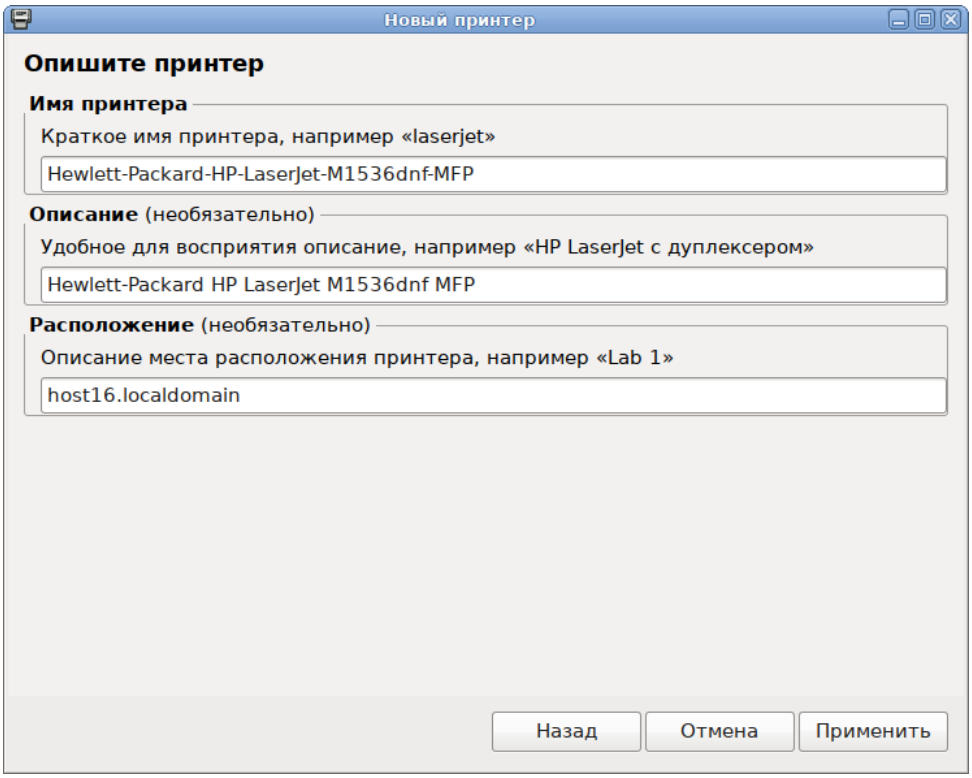


Рис. 447 – Название и описание принтера

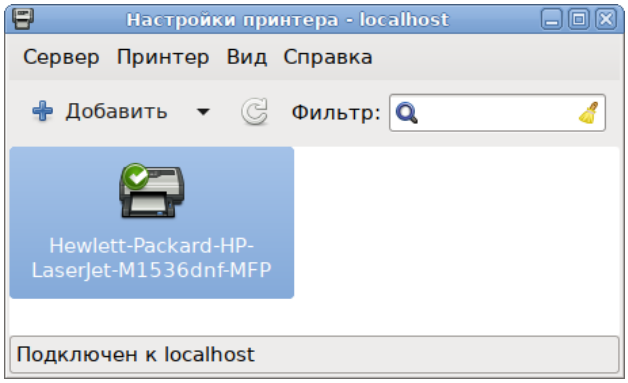


Рис. 448 – Выбор принтера

Изменить настройки принтера (разрешение, размер используемой по умолчанию бумаги, принтер по умолчанию и т. д.) можно в любой момент, выбрав в контекстном меню принтера пункт «Свойства».

16.16.3. Настройка сервера печати для сети

Если в сети имеются несколько принтеров или, когда принтеры не подключены непосредственно к тому компьютеру, на котором работает главный

сервер CUPS, то целесообразно настроить сервер cupsd, так, чтобы он мог принимать задания на печать из сети.

По умолчанию сервер CUPS работает с локально установленными принтерами, для того, чтобы он мог обрабатывать задания из сети, в конфигурационный файл `/etc/cups/cupsd.conf` нужно внести следующие изменения:

- разрешить доступ к серверу – добавить в секцию `Location` директиву `Allow from`:

```
<Location />
    Order allow,deny
    Allow localhost
    Allow from ip-address/netmask
</Location>
```

- включить отображение (обнаружение) общего принтера:

```
Browsing On
BrowseOrder allow,deny
BrowseAllow 192.168.1.* #локальная сеть
BrowseAddress 192.168.1.*:631#локальная сеть
```

Примечание. Включить отображение (обнаружение) общего принтера можно также отметив пункт «Разрешить совместный доступ к принтерам, подключенным к этой системе» в веб-интерфейсе на вкладке «Администрирование».

После внесения изменений нужно перезапустить службу cups:

```
# systemctl restart cups
```

На клиентах также должен быть установлен CUPS. После установки системы печати на клиенте, CUPS-принтеры, присутствующие в сети, автоматически находятся менеджерами принтеров. В качестве альтернативы, можно воспользоваться веб-интерфейсом CUPS на клиентской машине по адресу `http://localhost:631`. Если принтер не был обнаружен автоматически, введите IPP или HTTP-адрес (URI) сетевого CUPS принтера:

```
ipp://server-name-or-ip/printers/printername
```

или

```
http://server-name-or-ip:631/printers/printername
```

Если CUPS клиент не находит в сети принтеры, доступные через сервер CUPS, то иногда может помочь создание или изменение файла `/usr/local/etc/cups/client.conf` с добавлением записи, подобной следующей:

```
ServerName server-ip
```

В этом случае `server-ip` нужно заменить на IP-адрес сервера CUPS в сети.

16.16.4. Команды управления печатью

При печати через локальный сервер печати данные сначала формируются на локальном сервере, как для любой другой задачи печати, после чего посылаются на принтер, подключенный к данному компьютеру.

Вся информация, которая требуется для драйвера принтера (используемое физическое устройство, удаленный компьютер и принтер для удаленной печати), содержится в файлах `/etc/cups/printers.conf` и `/etc/cups/ppd/<имя_очереди>.ppd`.

Примечание. Далее термин «принтер» в этом разделе используется для обозначения принтера, соответствующего одной записи в файле `/etc/cups/printers.conf`. Под термином «физический принтер» подразумевается устройство, с помощью которого производится печать на бумаге. В файле `/etc/cups/printers.conf` может быть несколько записей, описывающих один физический принтер различными способами.

В системе печати CUPS приняты следующие команды для управления печатью:

- `/usr/bin/lpr` – постановка заданий в очередь, совместима с командой lpr системы печати BSD UNIX;
- `/usr/bin/lp` – постановка заданий в очередь, совместима с командой lp системы печати System V UNIX;
- `/usr/bin/lpq` – просмотр очередей печати;
- `/usr/sbin/lpc` – управление принтером, является частичной реализацией команды lpc системы печати BSD UNIX;
- `/usr/bin/lprm` – отмена заданий, поставленных в очередь на печать;
- `/usr/sbin/cupsd` – сервер печати;
- `/usr/sbin/lpadmin` – настройка принтеров и классов принтеров;
- `/usr/sbin/lpmove` – перемещение задания в другую очередь;
- `/usr/bin/fly-admin-printer` – настройка системы печати, установка и настройка принтеров, управление заданиями.

CUPS предоставляет утилиты командной строки для отправления заданий и проверки состояния принтера. Команды `lpstat` и `lpc status` также показывают сетевые принтеры (принтер@сервер), когда разрешен обзор принтеров.

С помощью команды `lp` выполняется передача задачи принтеру, то есть задача ставится в очередь на печать. В результате выполнения этой команды файл передается серверу печати, который помещает его в каталог `/var/spool/cups/`.

Остановить работу сервиса печати можно с помощью команды:

```
# systemctl stop cups
```

Запустить сервис печати можно с помощью команды:

```
# systemctl start cups
```

16.16.4.1. Настройка принтера

Настроить принтер в ОС можно также с помощью команды `lpadmin`. Ее запуск с опцией `-p` выполняется для добавления или модификации принтера:

```
/usr/sbin/lpadmin -p printer [опции]
```

Для `lpadmin` существуют также опции по регулированию политики лимитов и ограничений по использованию принтеров и политики доступа к принтерам.

Для удаления принтера нужно выполнить `lpadmin` с опцией `-x`:

```
/usr/sbin/lpadmin -x printer
```

16.16.4.2. Проверка очереди печати

Команда `lpq` предназначена для проверки очереди печати (используемой `lpd`) и вывода состояния заданий на печать, указанных при помощи номера задания, либо системного идентификатора пользователя, которому принадлежит задание.

`lpq` выводит для каждого задания имя его владельца, текущий приоритет задания, номер задания и размер задания в байтах, без параметров выводит состояние всех заданий в очереди.

16.16.4.3. Удаление задания из очереди печати

Команда `lprm` предназначена для удаления задания из очереди печати. Для определения номера задания нужно использовать команду `lpq`. Для удаления задания нужно быть его владельцем или пользователем с идентификатором root.

Системные каталоги, определяющие работу системы печати ОС, также содержат файлы, которые не являются исполняемыми:

- /etc/cups/printers.conf – содержит описания принтеров в ОС;
- /etc/cups/ppd/<имя_очереди>.ppd – содержит описания возможностей принтера, которые используются при печати заданий и при настройке принтеров;
- /var/log/cups/error_log – содержит протокол работы принтера, в этом файле могут находиться сообщения об ошибках сервера печати или других программ системы печати;
- /var/log/cups/access_log – содержит все запросы к серверу печати;
- /var/log/cups/page_log – содержит сообщения, подтверждающие успешную обработку страниц задания фильтрами и принтером.

16.16.4.4. Настройка сетевого принтера из консоли

Для настройки принтера из консоли нужно выполнить следующие действия:

1) получить права администратора;
2) просмотреть содержимое каталога model на наличие драйверов:

```
ls /usr/share/cups/model
```

Примечание. Для работы с дополнительными драйверами доступных устройств установите пакет printer-driver-splix.

3) если драйвер устройства присутствует перейти к шагу 7) (настройка нового устройства);
4) найти нужное устройство:

```
lpinfo -m | grep название_модели
```

5) просмотреть данные о драйвере устройства:

```
foomatic-ppdfile -A | grep название_модели
```

6) сформировать файл .ppd:

```
foomatic-ppdfile -p 'имя_ppd_драйвера' > /usr/share/cups/model/имя_ppd_файла.ppd
```

7) произвести настройку нового устройства:

- если принтер подключен по сети:

```
lpadmin -p название_принтера -D еще_одно_название -m название_ppd_файла.ppd -v socket://ip_принтера –E
```

- если принтер подключен по usb:

```
lpadmin -p название_принтера -D еще_одно_название -m название_ppd_файла.ppd -v "usb://адрес_принтера" –E
```

8) печать документа:

```
lp -d название_принтера /путь_документ
```

Примечание. Список доступных устройств можно просмотреть, выполнив команду: `lpinfo –v`

Пример вывода:

```
usb://Samsung/M262x%20282x%20Series?serial=ZD1UBJCD5000LVW
```

Список установленных принтеров: `lpstat –p -d`

Пример настройки сетевого принтера Kyocera Ecosys P2235dn:

1) получить права администратора;

2) просмотреть содержимое каталога `/usr/share/cups/model` на наличие драйверов:

```
ls /usr/share/cups/model
```

3) если драйвер устройства присутствует произвести настройку нового устройства (перейти к шагу 7));

4) найти нужное устройство:

```
lpinfo -m | grep Kyocera-P-2
```

5) просмотреть данные о драйвере устройства:

```
foomatic-ppdfile -A | grep Kyocera-P-2
```

6) сформировать файл `.ppd`:

```
foomatic-ppdfile -p ‘Kyocera-P-2000’ > /usr/share/cups/model/Kyocera.ppd
```

7) создать новое устройство:

```
lpadmin -p Kyocera -D Kyocera-P-2000 -m Kyocera.ppd -v socket://10.120.70.90 –E
```

16.17. Управление базами данных

В качестве СУБД в составе ОС Альт СП может использоваться PostgreSQL.

СУБД PostgreSQL предназначена для создания и управления реляционными БД и предоставляет многопользовательский доступ к расположенным в них данным. Данные в реляционной БД хранятся в отношениях (таблицах), состоящих из строк и столбцов. При этом единицей хранения и доступа к данным является строка, состоящая из полей, идентифицируемых именами столбцов. Кроме таблиц, существуют другие объекты БД (виды, процедуры), которые предоставляют доступ к данным, хранящимся в таблицах.

Для работы СУБД на НЖМД выделяется область для хранения БД, называемая «кластером БД». Кластер БД является набором БД, управляемых одним экземпляром сервера СУБД. Настройка работы отдельного экземпляра сервера СУБД так же определяется в рамках кластера соответствующими конфигурационными файлами.

16.17.1. Состав

СУБД PostgreSQL состоит из нескольких компонентов:

- postgresql – сервисная служба, реализующая непосредственно сервер БД;
- libpq – клиентская библиотека, предоставляющая доступ к серверу СУБД;
- набор серверных утилит для управления работой сервера и создания кластеров БД;
- набор клиентских утилит для создания и управления БД.

16.17.2. Настройка

Настройка сервера СУБД осуществляется установкой параметров в конфигурационном файле `postgresql.conf`. В дополнение к файлу `postgresql.conf` в PostgreSQL используется еще два конфигурационных файла, которые контролируют аутентификацию клиента.

По умолчанию все эти три файла находятся в каталоге данных кластера БД или в соответствующем кластеру конфигурационном каталоге, например,

`/etc/postgreslq/x.x/main`. За расположение указанных файлов отвечают конфигурационные параметры, описанные ниже:

- `data_directory` – определяет каталог для хранения данных;
- `config_file` – определяет основной конфигурационный файл сервера (`postgresql.conf`), значение этого параметра может быть задано только в командной строке postgres;
- `hba_file` – определяет конфигурационный файл для аутентификации по узлам (`pg_hba.conf`);
- `ident_file` – определяет конфигурационный файл для аутентификации по методу `ident` (`pg_ident.conf`);
- `external_pid_file` – определяет имя дополнительного файла с идентификатором процесса, который сервер создает для использования программами администрирования сервера.

16.18. Организация терминального доступа XRDP

Для организации и реализации терминального доступа для обработки информации в ОС Альт СП возможно использование XRDP (Remote Desktop Protocol). Программа предоставляет рабочий стол X, обеспечивает графический вход с использованием протокола удаленного рабочего стола RDP. XRDP поддерживает удаленное управление графикой, двустороннюю передачу буфера обмена, перенаправление звука, диска. Передача RDP шифруется с использованием TLS по умолчанию.

16.18.1. Базовая настройка сервера терминалов

Примечание. В настройках сети сервера должен быть указан способ получения IP-адреса: «Вручную», указаны статические настройки сети: IP-адрес, маска, шлюз.

Для настройки сервера терминалов нужно установить пакет xrdp:

```
# apt-get update
# apt-get install xrdp
```

Включить и добавить в автозагрузку сервисы:

```
# systemctl enable --now xrdp xrdp-sesman
```

При использовании в качестве сервера терминалов ОС Альт СП (исполнение Сервер) в профиле установки будет отсутствовать графическая оболочка (о том, как установить графическую оболочку и переключиться в графический режим см. п. 5.7).

16.18.2. Настройка сервера

Параметры настройки сервера хранятся в файле `/etc/xrdp/sesman.ini`, файл конфигурации содержит разделы:

- «Globals» – определяет некоторые глобальные параметры конфигурации;
- «Security» – определяет параметры безопасности;
- «Session» – определяет параметры подключения, управление сеансами;
- «Session» definitions – определяет поддерживаемые типы сеансов. Конфигурация каждого типа сеанса определяется как отдельный раздел по имени типа сеанса Xorg, Xvnc;
- «Logging» – определяет параметры подсистемы логирования;
- «Chansrv» – определяет параметры подключения диска, которые поддерживает RDP.

Фрагмент конфигурационного файла `/etc/xrdp/sesman.ini`:

```
;; MaxSessions - maximum number of connections to an xrdp server
; Type: integer
; Default: 0
MaxSessions=50

;; KillDisconnected - kill disconnected sessions
; Type: boolean
; Default: false
; if 1, true, or yes, kill session after 60 seconds
KillDisconnected=false

;; DisconnectedTimeLimit - when to kill idle sessions
; Type: integer
; Default: 0
; if not zero, the seconds before a disconnected session is killed
; min 60 seconds
DisconnectedTimeLimit=0

;; IdleTimeLimit (specify in second) - wait before disconnect idle
sessions
; Type: integer
; Default: 0
; Set to 0 to disable idle disconnection.
IdleTimeLimit=0
```

```
;; Policy - session allocation policy
; Type: enum [ "Default" | "UBD" | "UBI" | "UBC" | "UBDI" | "UBDC" ]
; "Default" session per <User,BitPerPixel>
; "UBD" session per <User,BitPerPixel,DisplaySize>
; "UBI" session per <User,BitPerPixel,IPAddr>
; "UBC" session per <User,BitPerPixel,Connection>
; "UBDI" session per <User,BitPerPixel,DisplaySize,IPAddr>
; "UBDC" session per <User,BitPerPixel,DisplaySize,Connection>
Policy=Default

[Logging]
LogFile=xrdp-sesman.log
LogLevel=DEBUG
EnableSyslog=1
SyslogLevel=DEBUG
```

Некоторые настройки параметров безопасности сервера, установленные по умолчанию:

- `ListenPort=3350` – порт, который прослушивает xrdp-sesman (если настроен межсетевой экран нужно включить этот порт в разрешенные);
- `TerminalServerUsers=tsusers` – группа, в которую нужно добавить пользователей для организации доступа к серверу. Данная группа создается локально при установке сервера, если рассматривать доменную авторизацию, то нужно внести изменения в файл конфигурации `/etc/sssd/sssd.conf` и в настройках `sesman.ini` вместо локальной группы указать доменную;
- `TerminalServerAdmins=tsadmins` – группа, в которую нужно добавить пользователей для организации административного доступа к серверу;
- `MaxLoginRetry=4` – максимальное количество попыток подключения;
- `MaxSessions=50` – максимальное количество подключений к серверу;
- `KillDisconnected=false` – разрыв сеанса при отключении пользователя;
- `AllowRootLogin=false (true/false)` – управление авторизацией под учетной записью root;
- `FuseMountName=thinclient_drivers` – название монтируемой папки.

Конфигурацию сервера возможно настроить в соответствии с требованиями безопасности.

16.18.3. Настройки доступа пользователей

Для доступа к терминальному сеансу пользователь должен быть включен в группу `tsusers`:

```
# gpasswd -a <пользователь> tsusers
```

Для разрешения монтирования папки пользователь должен быть включен в группу `fuse`:

```
# gpasswd -a <пользователь> fuse
```

16.18.4. Подключение звука

Для возможности прослушивания звука из терминального сеанса локально нужно установить на терминальный сервер пакет pulseaudio-module-xrdp:

```
# apt-get install pulseaudio-module-xrdp
```

16.18.5. Подключение USB-устройств

Для организации инфраструктуры перенаправления USB-устройств на сеанс сервера XRDP нужно установить пакет xrdp-usb, который состоит из двух пакетов:

- терминальный сервер – xrdp-usb-session;
- терминальный клиент – xrdp-usb-terminal.

Пакет xrdp-usb-session позволяет добавлять подключение разрешенных администратором USB-устройств с клиента.

Установка пакета xrdp-usb-session на сервер:

```
# apt-get install xrdp-usb-session
```

Перезапустить службу xrdp-sesman:

```
# systemctl restart xrdp-sesman.service
```

Выполнить настройку клиента:

1) установить пакет xrdp-usb-terminal:

```
# apt-get install xrdp-usb-terminal
```

2) добавить пользователя клиентского компьютера в группу `disk`:

```
# gpasswd -a <пользователь> disk
```

3) перезагрузить систему;

4) убедиться, что служба usbipd запущена:

```
# systemctl status usbipd
```

Далее нужно подключить USB-устройства и настроить разрешения для передачи.

Осуществим просмотр идентификатора подключенного USB-устройства:

```
# lsusb
Bus 002 Device 002: ID 0951:1643 Kingston Technology DataTraveler G3
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 004 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 003 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 001 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
```

Из полученного вывода следует выбрать ID устройства, которое нужно передать при подключении к терминальной сессии, скопировать нужный идентификатор и прописать его в файле `/etc/xrdp-usb`:

```
# Config file for xrdp-usb-terminal
# Add redirected usb ids one per line
# Example
#072f:90cc     # Advanced Card Systems, Ltd : ACR38 SmartCard Reader (072f:90cc)
#072f:*      # All devices from specified vendor
0951:1643  # ID устройства
```

16.18.6. Настройка клиента для подключения к серверу терминалов

Примечание. Следует избегать одновременных сеансов RDP и обычных для одного и того же пользователя. Systemd не позволит полноценно работать в сеансе RDP.

Для подключения к серверу терминалов, на клиентском компьютере должен быть установлен клиент удаленного доступа. Для подключения к серверу терминалов можно использовать программы удаленного доступа FreeRDP, Remmina, Connector и т. д.

Перед подключением нужно на клиенте выполнить команду usbip-export:

```
$ usbip-export
```

Для подключения с использованием xfreerdp (должен быть установлен пакет xfreerdp) нужно выполнить команду:

```
$ xfreerdp /v:192.168.0.148 /u:user /p:password
```

Описание некоторых параметров:

- `/v:<server>[:port]` – ip-адрес или имя сервера;
- `/u:<user>` – пользователь;
- `/p:<password>` – пароль;
- `/w:<width>` – ширина окна;
- `/h:<height>` – высота окна;
- `/f` – полноэкранный режим.

Примечание. Если не указывать пользователя или пароль, появится окно входа.

На рис. 449 показано подключение к терминальной сессии с использованием xfreerdp.

В качестве клиента удаленного доступа также можно использовать программу Remmina. Для этого нужно установить пакеты remmina и remmina-plugins-rdp:

```
# apt-get install remmina remmina-plugins-rdp
```

Для запуска Remmina выбрать в меню «Приложения» → «Интернет» → «Клиент удаленного доступа к рабочему столу».

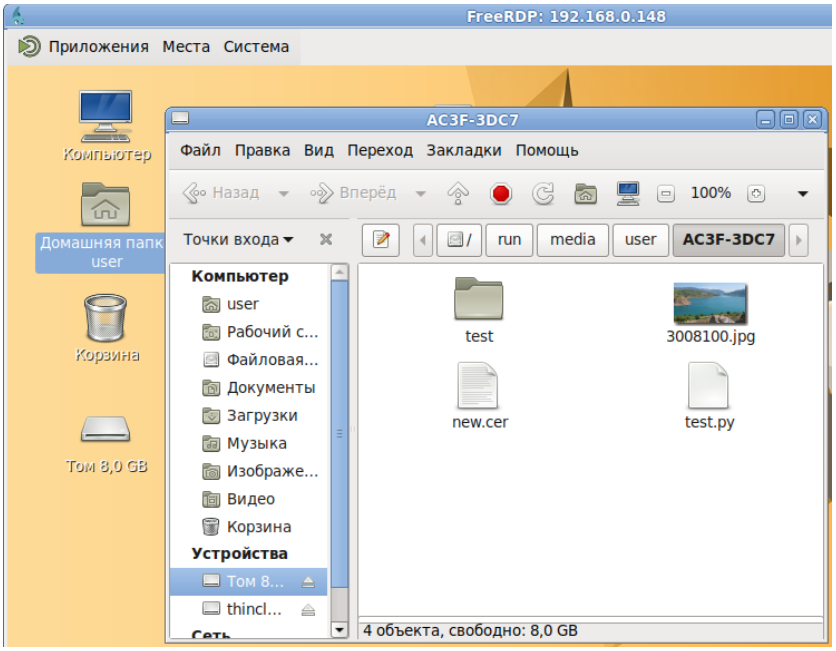


Рис. 449 – FreeRDP. Подключение к удаленному рабочему столу

Для подключения к терминальной сессии в окне Remmina (рис. 452) нажмите кнопку создания нового подключения (рис. 450) и в открывшемся окне (рис. 451)

укажите настройки RDP-подключения (IP-адрес терминального сервера, имя пользователя, пароль и т. д.), нажамите кнопку «Сохранить и подключиться».

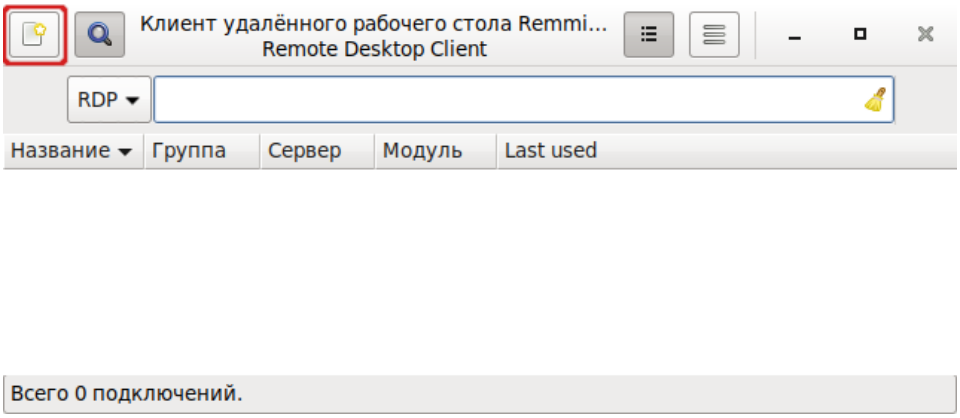


Рис. 450 – Кнопка создания нового подключения

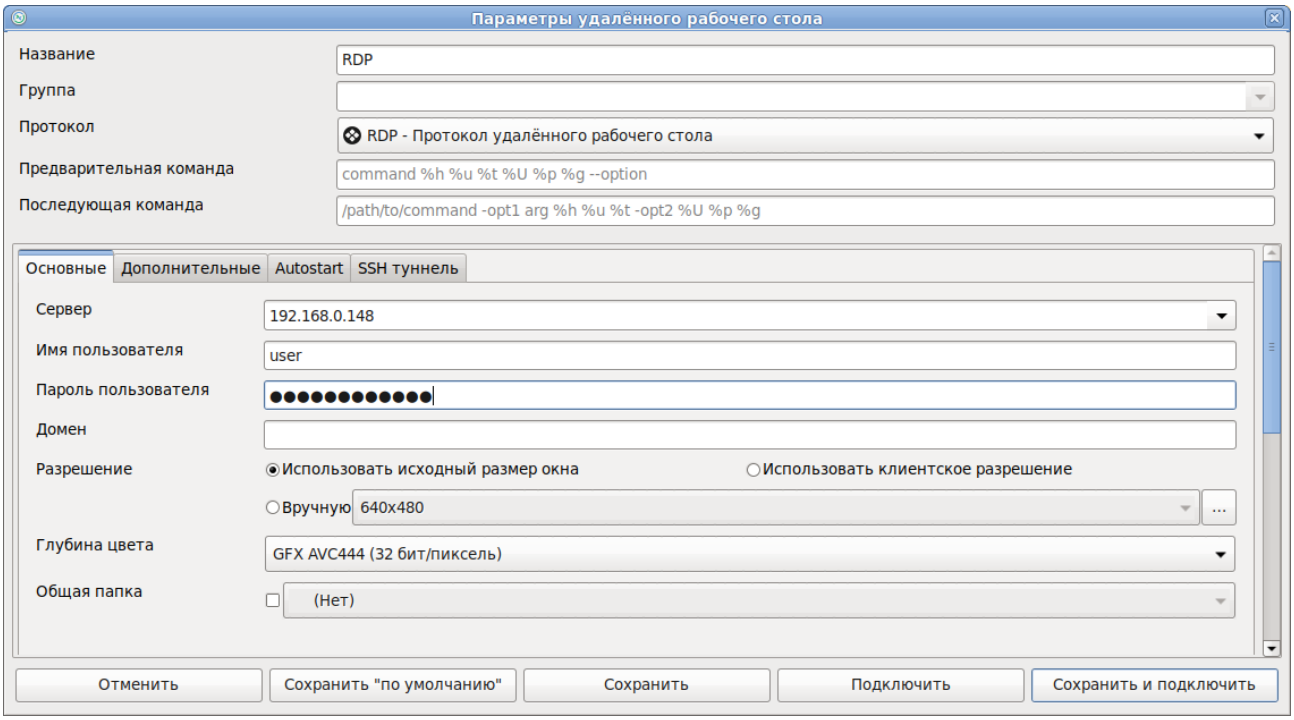


Рис. 451 – Настройки RDP-подключения

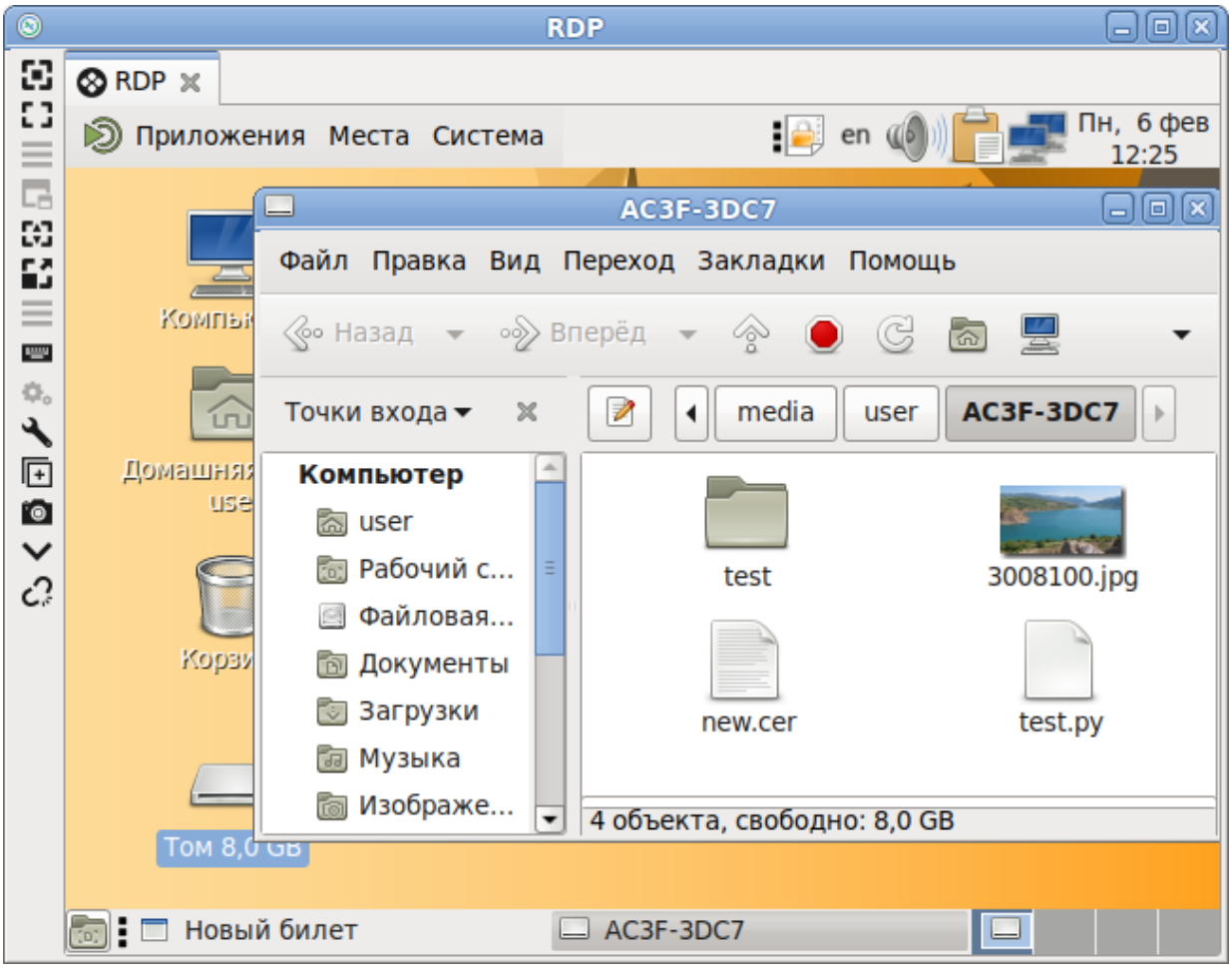


Рис. 452 – Remmina. Подключение к удаленному рабочему столу

П р и м е ч а н и е . Если автоматического монтирования не происходит, следует выполнить команду:

```
$ udisksctl mount -b /dev/sdb1
```

где `/dev/sdb1` – USB-устройство, можно посмотреть в выводе команды lslbk.

В качестве клиента удаленного доступа можно использовать программу Connector. Connector позволяет осуществлять удаленный доступ к компьютерам с различными ОС с использованием распространенных типов подключений, таких как RDP, VNC, NX, XDMCP, SSH, SFTP. Connector реализует интерфейс для пользователя к предустановленным программам для запуска их с введенными параметрами.

Установите пакет connector на клиентский компьютер:

```
# apt-get install connector
```

Для подключения к терминальной сесссии запустите Myconnector – выбрать в меню «Приложения» → «Интернет» → «Connector». В окне подключения (рис. 453) указать IP-адрес терминального сервера. Нажать кнопку «Дополнительные параметры» и в открывшемся окне (рис. 454) указать настройки RDP-подключения. Нажать на кнопку «Подключение».

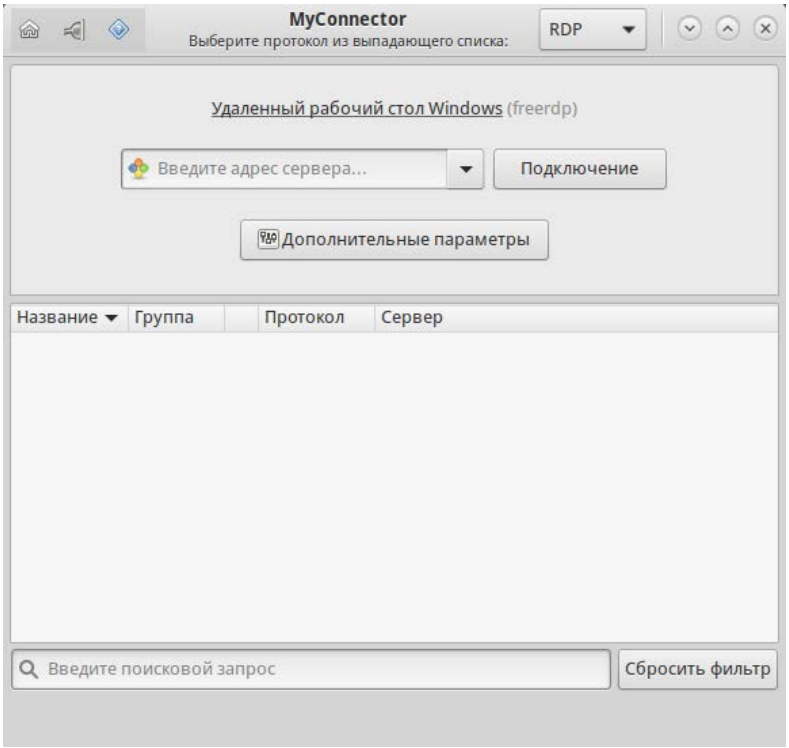


Рис. 453 – Myconnector. Окно подключения

Для просмотра содержимого проброшенного USB-устройства перейти в «Домашний каталог» → «thinclient_drives» → «MEDIA» → «kingston» (рис. 455).

Где:

- thinclient_drives – каталог, указанный в конфигурационном файле `/etc/xrdp/sesman.ini`;
- kingston – наименование USB-устройства.

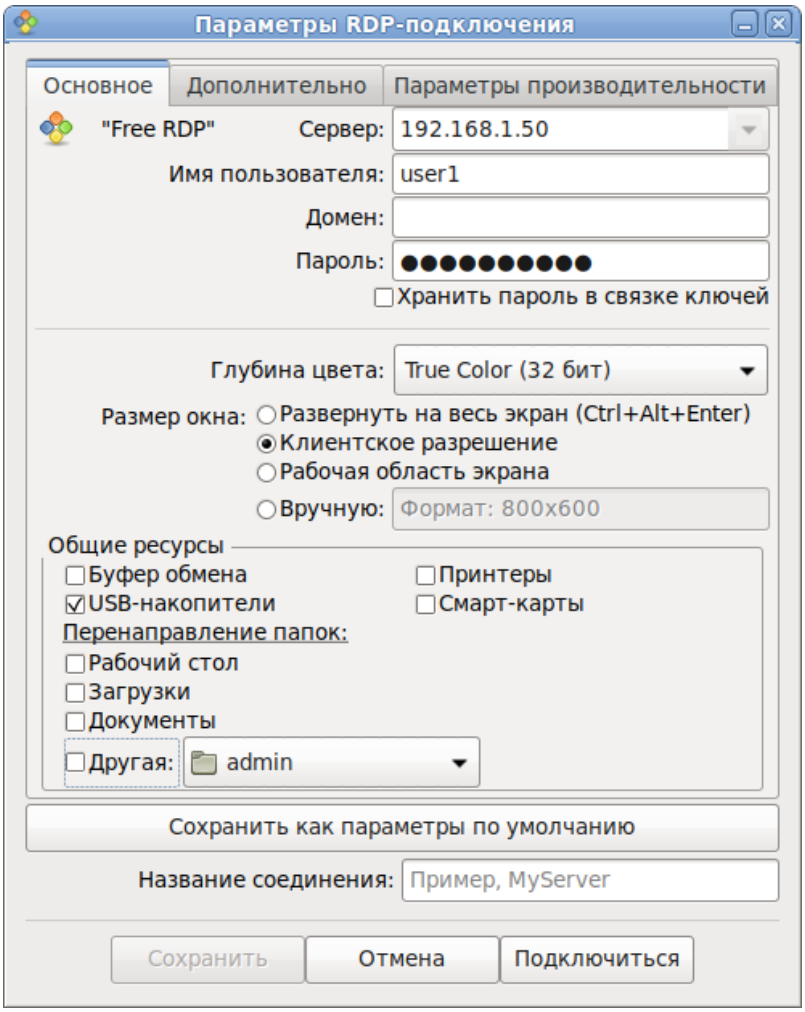


Рис. 454 – Настройки RDP-подключения

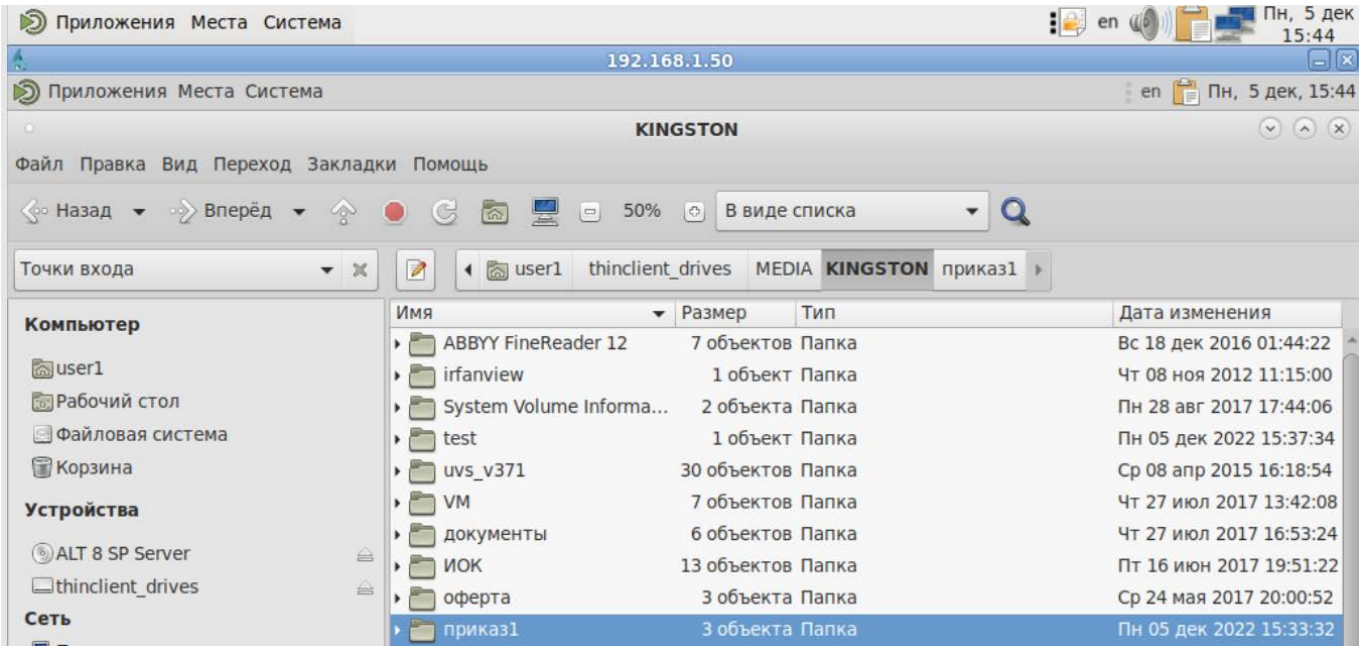


Рис. 455

16.18.7. Управление XRDP

Просмотр информации об активных пользователях:

```
# ps aux |grep xrdp |grep xorg
```

```
user1        5689  0.6  2.5 943524 100112 ?        Sl   17:48   0:09 Xorg :10 -auth .Xauthority -config xrdp/xorg.conf -noreset -nolisten tcp -logfile .xorgxrdp.%s.log
```

В выводе команды видно, что подключен пользователь user1 и его PID 5689.

Следующая команда отключит пользователя user1 и завершит все его процессы:

```
# pkill -9 -u user1
```

16.19. Timeshift

Timeshift – программа для автоматического периодического создания копий системы (снимков/snapshots).

Timeshift предназначен, прежде всего для сохранения системных файлов и настроек. Пользовательские данные по умолчанию не архивируются, поэтому в случае сбоя системы, восстанавливаются системные файлы, а данные пользователей остаются в актуальном состоянии (конечно, если они не были повреждены).

Резервные копии не могут быть восстановлены на уровне отдельных файлов, восстановление всегда происходит в полном объеме настроек Timeshift.

Запустить Timeshift можно из MATE «Меню» → «Приложения» → «Системные» → «Программа для восстановления системы» или из командной строки:

```
$ timeshift-launcher
```

Запуск Timeshift требует прав администратора, поэтому нужно ввести пароль администратора (рис. 456).

При первом запуске Timeshift будет запущен «Мастер установки». Запустить мастер установки или открыть окно настроек резервного копирования также можно, нажав соответствующую кнопку на панели инструментов в окне Timeshift (рис. 457).

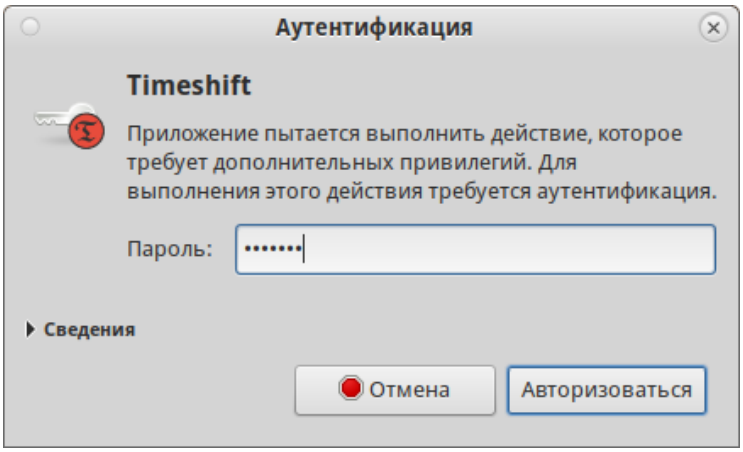


Рис. 456 – Запрос пароля для запуска Timeshift

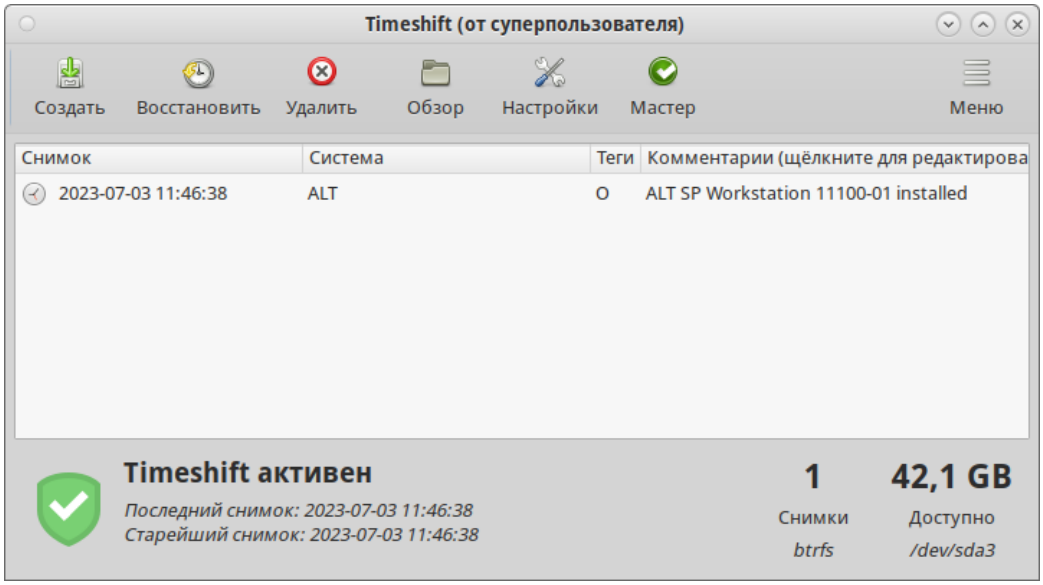


Рис. 457 – Окно программы Timeshift

16.19.1. Настройка резервного копирования

16.19.1.1. Режим RSYNC

Особенности режима RSYNC:

- снимки создаются путем копирования системных файлов при помощи rsync и создания жестких ссылок на неизмененные файлы из предыдущего снимка;
- все файлы копируются при создании первого снимка. Последующие снимки являются инкрементальными. Неизменные файлы будут связаны с предыдущим снимком, если он доступен;
- создание первого снимка может занять до 10 минут;

- системный раздел может быть отформатирован в любой файловой системе. Резервный раздел может быть отформатирован в любой файловой системе Linux, поддерживающей жесткие ссылки. Сохранение снимков на несистемный или внешний диск позволяет восстановить систему, даже если системный диск поврежден;
- можно задать исключения для файлов и каталогов для экономии дискового пространства;
- систему нужно перезагрузить после восстановления снимка.

Тип снимков можно выбрать на вкладке «Тип» окна настроек Timeshift или на первом шаге работы мастера установки. На первом шаге нужно выбрать тип снимков «RSYNC» (рис. 458) и нажать кнопку «Далее».

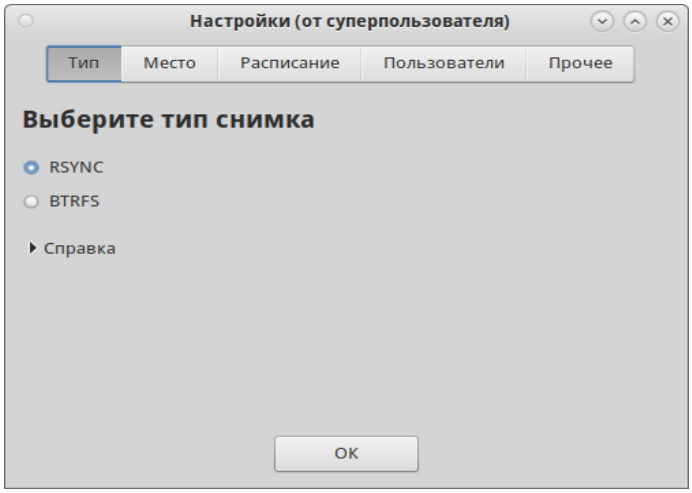


Рис. 458 – Выбор режима RSYNC

На следующем шаге следует выбрать место, где будут храниться снимки (рис. 459). RSYNC снимки имеют большой размер, поэтому желательно хранить их на другом (не системном) диске или разделе. По умолчанию снимки сохраняются в системном (корневом) разделе в `/timeshift`, также можно выбрать другие разделы Linux.

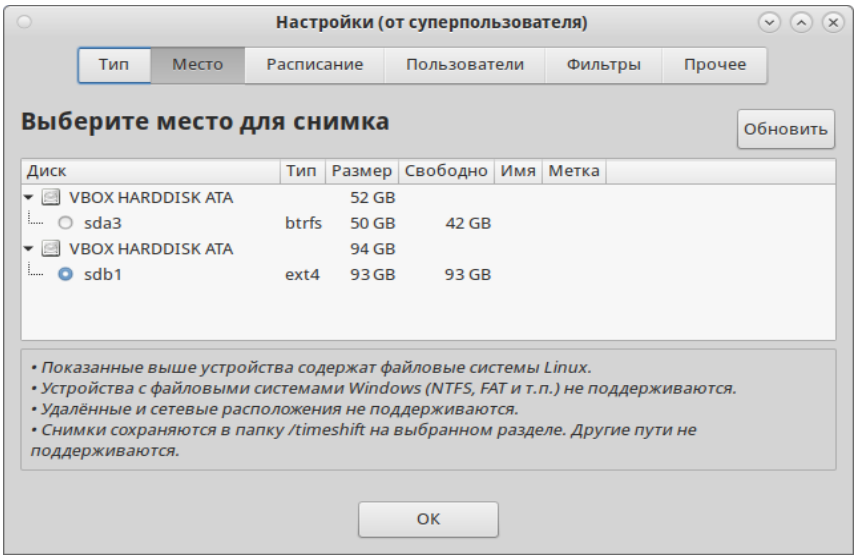


Рис. 459 – Выбор места хранения снимков RSYNC

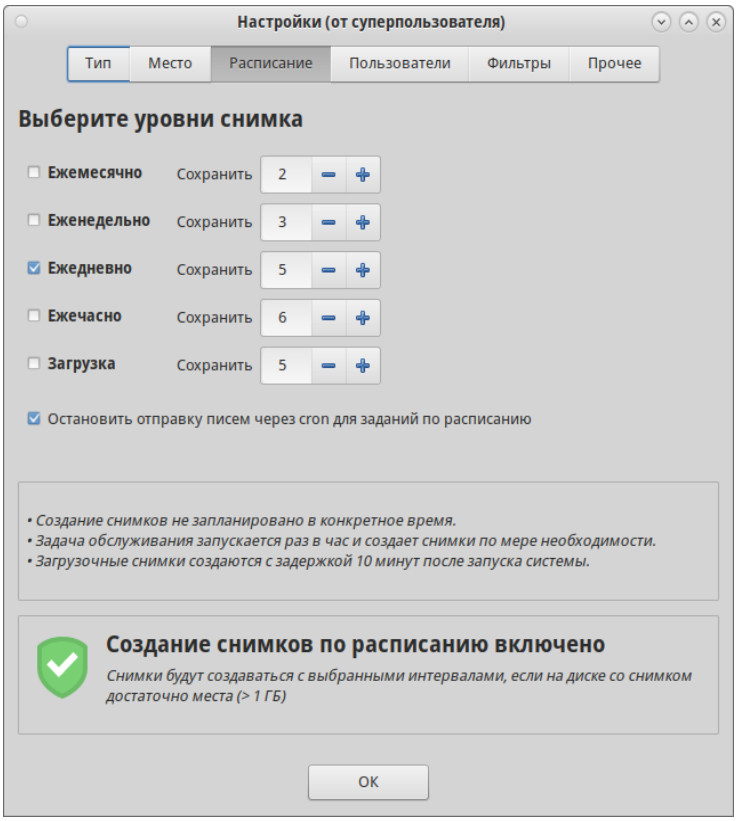


Рис. 460 – Расписание для снимков RSYNC

На вкладке «Фильтры» окна настроек Timeshift можно указать, какие файлы/каталоги включать/исключать из резервного копирования (динамические каталоги исключаются по умолчанию: `/dev`, `/proc`, …).

В данном примере (рис. 461) из резервной копии будут исключены все файлы mp3, все системные журналы, кроме журналов веб-сервера Apache. Просмотреть итоговый список исключений (рис. 462) можно, нажав кнопку «Кратко» на вкладке «Фильтры». Отредактировать шаблон можно, дважды щелкнув левой кнопкой мыши по строке шаблона.

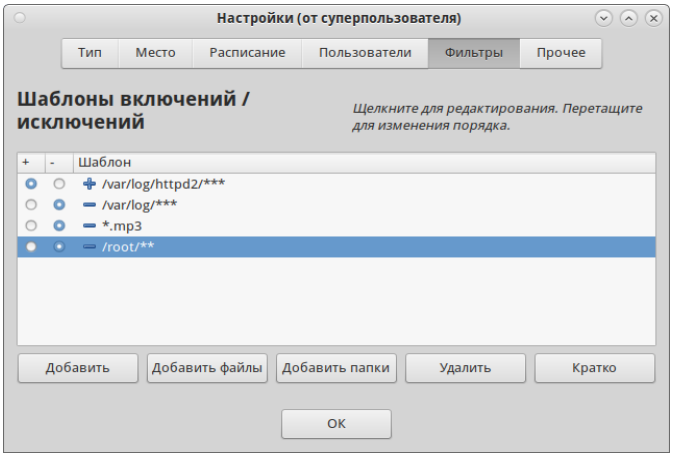


Рис. 461 – Timeshift. Вкладка «Фильтры»

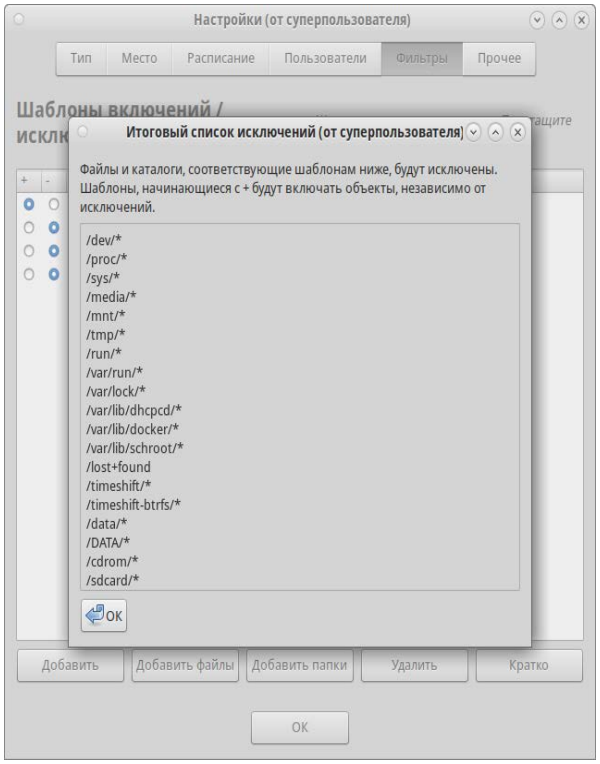


Рис. 462 – Список исключений

16.19.1.2. Режим BTRFS

Особенности режима BTRFS:

- снимки создаются с использованием встроенных средств файловой системы BTRFS;
- снимки создаются и восстанавливаются мгновенно (создание снимков – это атомарная транзакция на уровне файловой системы);
- снимки восстанавливаются путем замены системных подразделов. Поскольку файлы никогда не копируются, не удаляются и не перезаписываются, риск потери данных отсутствует. Существующая система сохраняется как новый снимок после восстановления;
- снимки сохраняются на том же диске, с которого они созданы (системном диске). Хранение на других дисках не поддерживается. Если системный диск выйдет из строя, снимки, хранящиеся на нем, будут потеряны вместе с системой;
- нет возможности исключать файлы и каталоги;
- размер снимков BTRFS изначально равен нулю. При изменении системных файлов, данные записываются в новые блоки данных, которые занимают дисковое пространство (копирование при записи). Файлы в снимке продолжают указывать на исходные блоки данных;
- снимки можно восстановить без немедленной перезагрузки запущенной системы;
- ОС должна быть установлена на раздел BTRFS с разбивкой на подразделы @ и @home. Другие виды разделов не поддерживаются.

Примечание. Для установки ОС на раздел BTRFS с разбивкой на подразделы @ и @home можно при установке системы, на этапе «Подготовка диска» создать следующие подтома (рис. 463):

- подтом @ с точкой монтирования в `/`;
- подтом @home с точкой монтирования в `/home`.

Тип снимков BTRFS можно выбрать на вкладке «Тип» окна настроек Timeshift (рис. 463) или на первом шаге работы мастера установки.

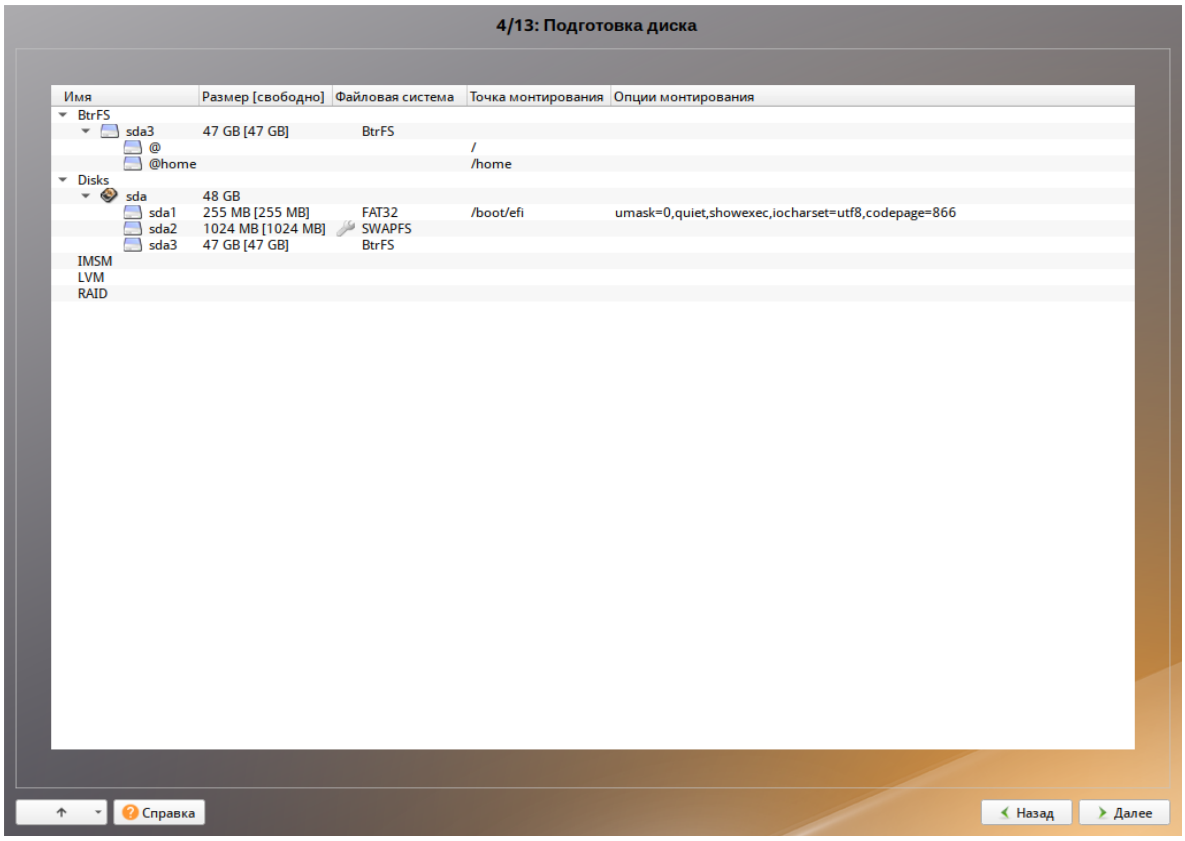


Рис. 463 – Корень системы с файловой системой BTRFS

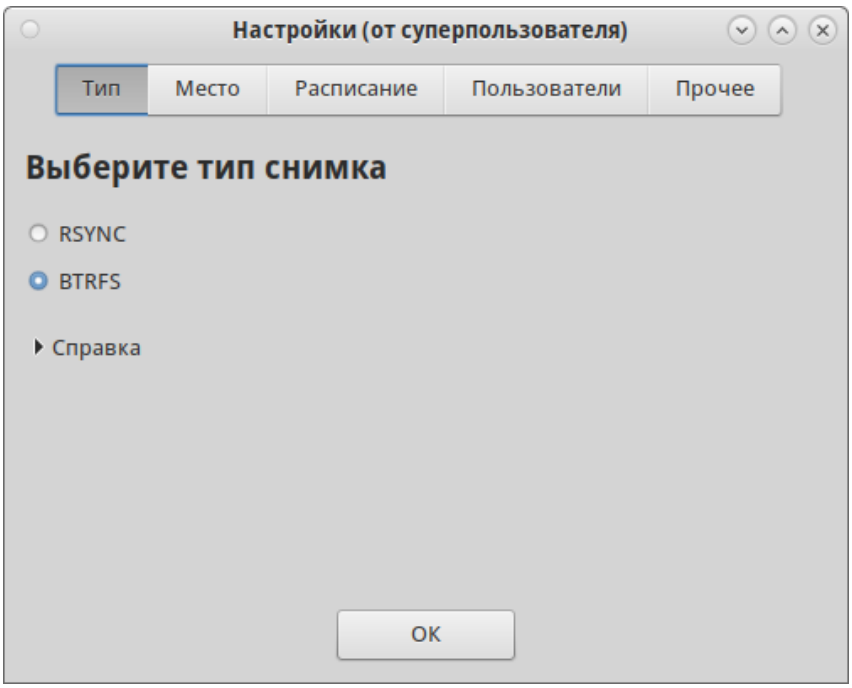


Рис. 464 – Выбор режима BTRFS

Снимки BTRFS сохраняются в системном разделе, другие разделы не поддерживается (рис. 465).

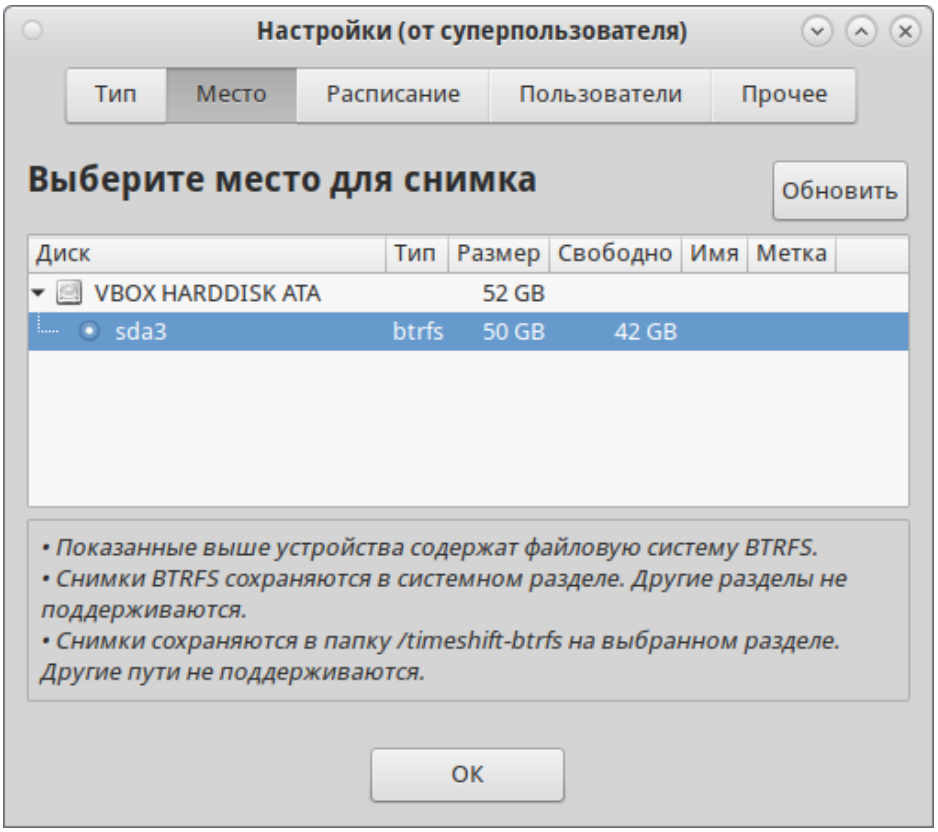


Рис. 465 – Выбор места хранения снимков BTRFS

На вкладке «Расписание» следует выбрать уровни создания снимков (ежемесячно, еженедельно, ежедневно, ежечасно, при загрузке) и указать количество сохраняемых снимков для каждого уровня (рис. 466).

По умолчанию домашние каталоги пользователей не включаются в резервную копию. На вкладке «Пользователи» можно изменить это поведение и включить подраздел @home в создаваемые снимки (рис. 467).

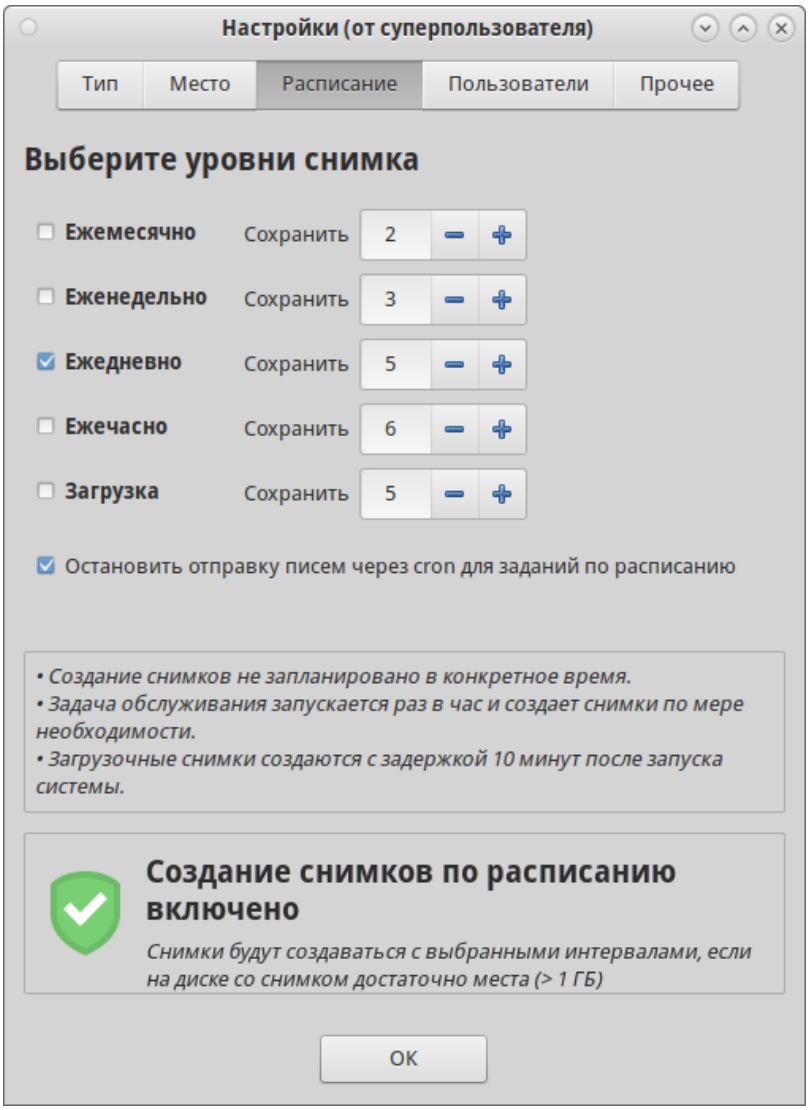


Рис. 466 – Расписание для снимков BTRFS

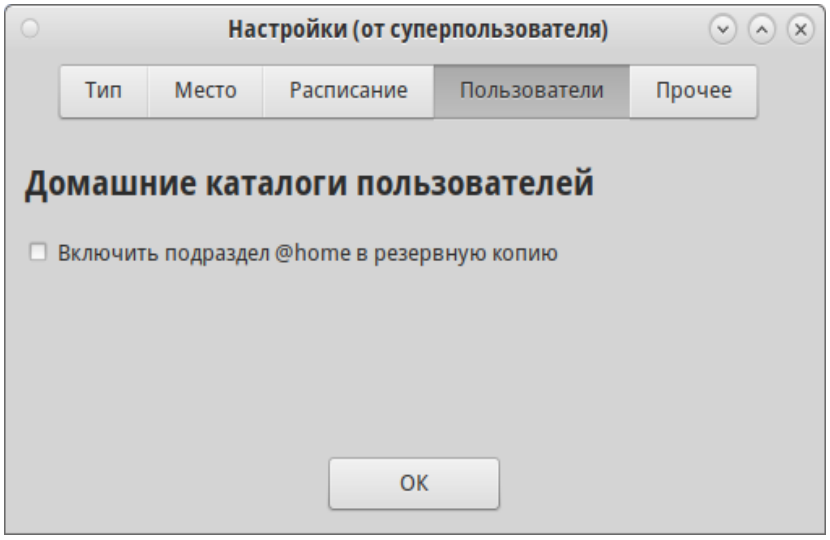


Рис. 467 – Включить подраздел @home в создаваемые снимки

16.19.2. Создание снимков

Снимки будут создаваться автоматически согласно настроенному расписанию.

Для создания снимка в ручном режиме следует нажать кнопку «Создать» на панели инструментов (рис. 468). Резервная копия будет создана на устройстве хранения, который был указан в настройках.

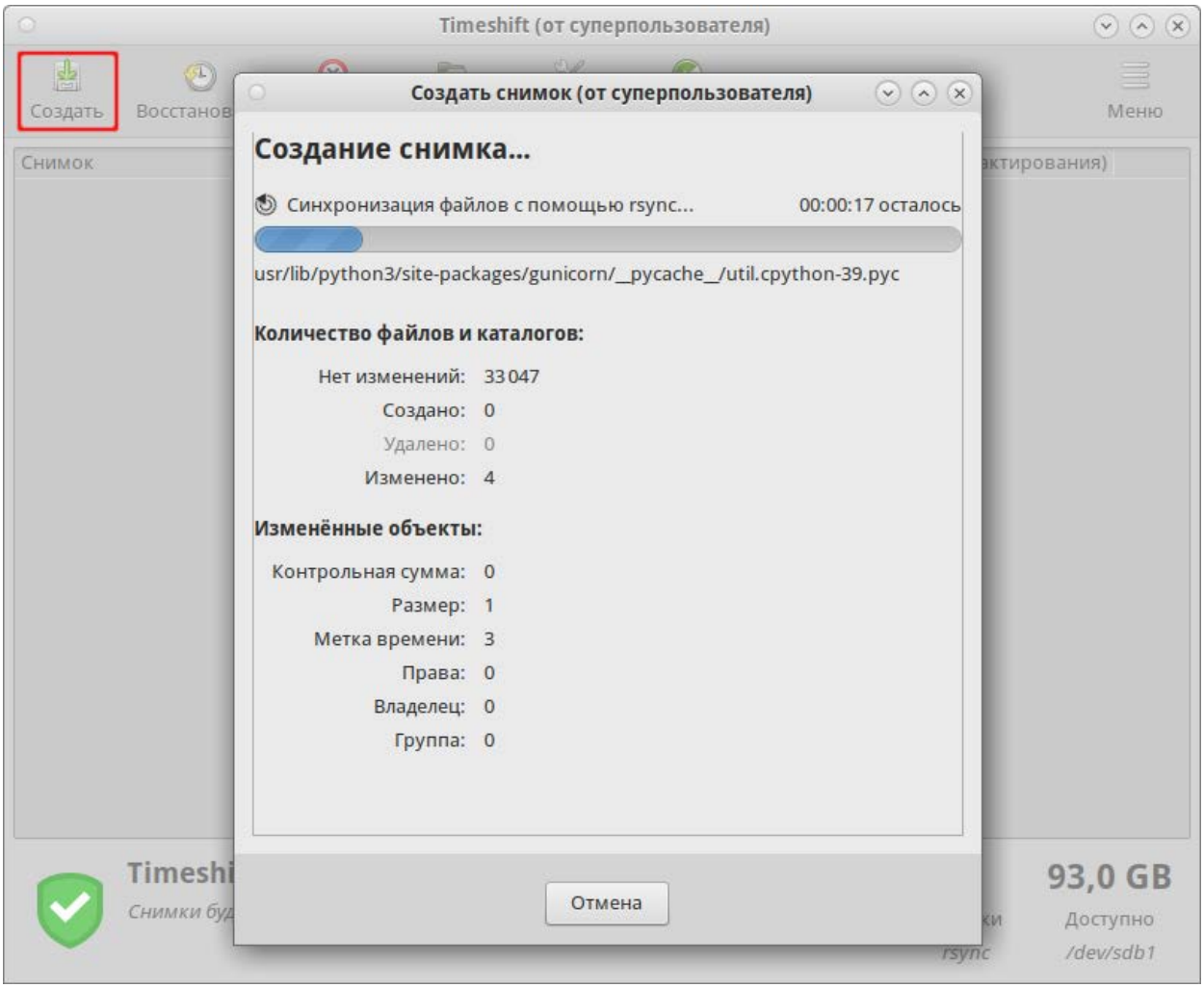


Рис. 468 – Создание снимка в режиме RSYNC

16.19.3. Восстановление системы

Снимки можно восстановить как из работающей системы (оперативное восстановление), так и из другой системы, на которой установлен Timeshift (автономное восстановление).

Для восстановления снимка следует выбрать снимок в главном окне и нажать кнопку «Восстановить» (рис. 469).

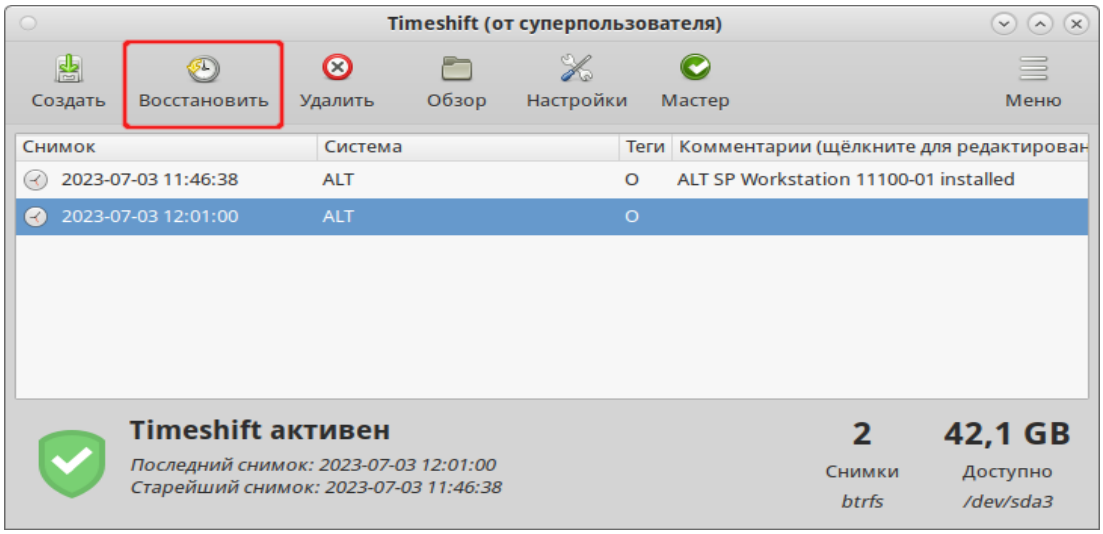


Рис. 469 – Снимки системы и кнопка «Восстановить»

При восстановлении снимка в режиме RSYNC после нажатия кнопки «Восстановить» можно выбрать устройство, куда будут восстановлены файлы (рис. 470), указать нужно ли переустанавливать GRUB, нажав кнопку «Параметры загрузчика» (рис. 471). На следующем шаге будут показаны файлы, которые будут созданы/восстановлены/удалены в процессе восстановления снимка (рис. 472).

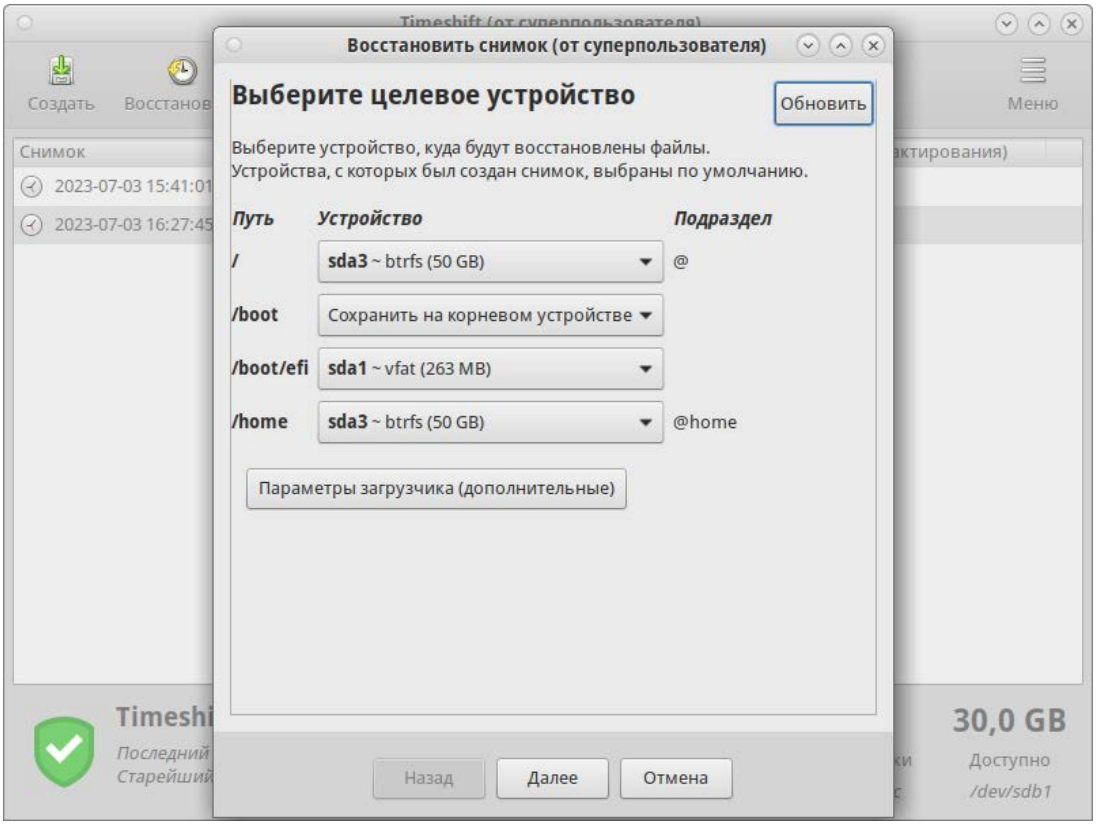


Рис. 470 – Выбор целевого устройства

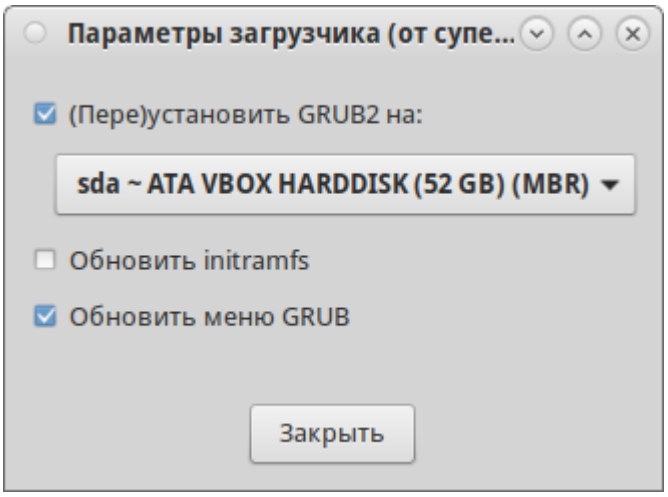


Рис. 471 – Параметры загрузчика

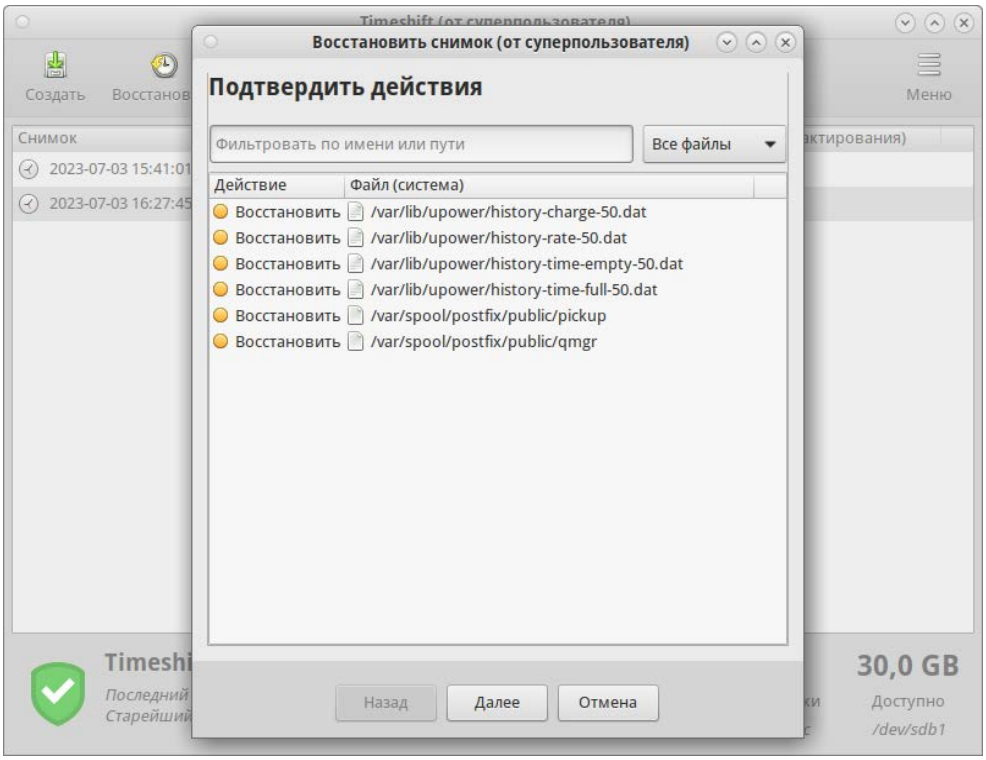


Рис. 472 – Восстановление снимка в режиме RSYNC

Примечание. Если основная система не загружается, то можно загрузиться в режиме восстановления и развернуть снимок в командной строке (рис. 473).

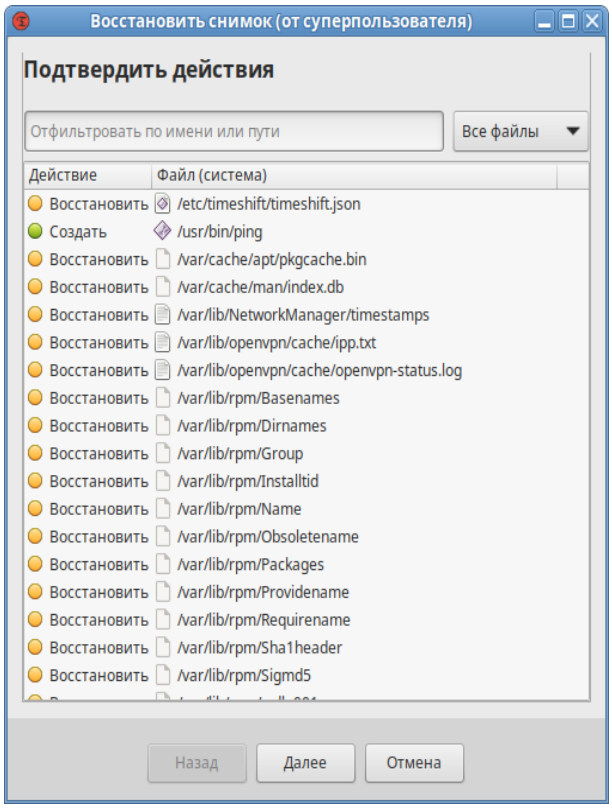


Рис. 473 – Восстановление снимка в режиме RSYNC

16.19.4. Работа с Timeshift в командной строке

Вывод справки о команде:

```
$ timeshift
```

Если параметры не указаны, например, при создании снимка, значения по умолчанию будут загружены из конфигурации приложения.

Просмотр списка снимков:

```
# timeshift --list
```

```
Mounted '/dev/sdb1' at '/run/timeshift/7138/backup'
Device : /dev/sdb1
UUID   : be8e861d-bd39-4b74-b587-d757fa016695
Path   : /run/timeshift/7138/backup
Mode   : RSYNC
Status : OK
2 snapshots, 30.0 GB free

Num     Name                 Tags  Description
------------------------------------------------------------------------
-------
0    >  2023-07-03_15-41-01  O
1    >  2023-07-03_16-27-45  O
```

Пример создания снимка (в режиме RSYNC):

```
# timeshift --create --comments "after update" --tags D
/dev/sdb1 is mounted at: /run/timeshift/backup, options: rw,relatime

------------------------------------------------------------------------
-------
Creating new snapshot...(RSYNC)
Saving to device: /dev/sdb1, mounted at path: /run/timeshift/backup
Linking from snapshot: 2023-07-03_16-27-45
Synching files with rsync...
CCreated control file:
/run/timeshift/7184/backup/timeshift/snapshots/2023-07-03_16-43-46/info.json
RSYNC Snapshot saved successfully (15s)
Tagged snapshot '2023-07-03_16-43-46': ondemand
------------------------------------------------------------------------
-------
Removing snapshots (incomplete):
------------------------------------------------------------------------
-------
Removing '2023-07-03_16-43-46'...
Removed '2023-07-03_16-43-46'
------------------------------------------------------------------------
-------
```

Пример создания (в режиме BTRFS):

```
# timeshift --create --comments "after update" --tags D
Creating new backup...(BTRFS)
Saving to device: /dev/sda3, mounted at path:
/run/timeshift/4294/backup
Created directory: /run/timeshift/4294/backup/timeshift-
btrfs/snapshots/2023-07-03_16-51-23
Created subvolume snapshot: /run/timeshift/4294/backup/timeshift-
btrfs/snapshots/2023-07-03_16-51-23/@
Created control file: /run/timeshift/4294/backup/timeshift-
btrfs/snapshots/2023-07-03_16-51-23/info.json
BTRFS Snapshot saved successfully (0s)
Tagged snapshot '2023-07-03_16-51-23': ondemand
------------------------------------------------------------------------
-------
```

Создание снимка, если он запланирован (есть в расписании):

```
# timeshift --check
```

Восстановить снимок (параметры будут запрошены в интерактивном режиме):

```
# timeshift --restore
```

Восстановить снимок:

```
# timeshift --restore --snapshot '2023-07-03_16-27-45'
```

Восстановить определенный снимок в раздел:

```
# timeshift --restore --snapshot '2023-07-03_16-27-45' --target /dev/sda2
```

Удалить снимок:

```
# timeshift --delete --snapshot '2023-07-03_16-27-45'
```

Если основная система не загружается, то нужно загрузиться в режиме восстановления и выполнить следующие действия (на примере режима RSYNC):

1) установить timeshift:

```
# apt-get update && apt-get install timeshift
```

2) просмотреть список снимков на устройстве:

```
# timeshift --list --snapshot-device /dev/sdb
```

3) запустить восстановление:

```
timeshift --restore --snapshot-device /dev/sdb --snapshot '2023-07-03_16-27-45' --target /dev/sda2 --grub-device /dev/sda
```

4) перезагрузить систему.

16.20. Информация о системе и об аппаратной части компьютера

16.20.1. Команда inxi

inxi – это инструмент командной строки, который позволяет отображать информацию о системе и об аппаратной части компьютера. Часто используется в качестве инструмента отладки для технической поддержки, чтобы быстро определить конфигурации системы и оборудование пользователей.

Установка пакета inxi:

```
# apt-get install inxi
```

Команда:

```
inxi [-AbBCdDEfFGhiIjJlLmMnNopPrRsSuUVwyYzZ]
```

```
inxi [-c <целое число>] [--sensors-exclude SENSORS] [--sensors-use SENSORS] [-t [c|m|cm|mc][целое число]] [-v <целое число>] [-W LOCATION] [--weather-unit {m|i|mi|im}] [-y WIDTH]
```

```
inxi [--edid] [--memory-modules] [--memory-short] [--recommends] [--sensors-default] [--slots]
```

```
inxi [-x|-xx|-xxx|-a] -OPTION(s)
```

В таблице 67 приведены некоторые стандартные опции команды inxi.

Т а б л и ц а 67 – Стандартные опции команды inxi

Ключ	Описание

-A	Выводит информацию об аудио/звуковых устройствах, включая драйвер устройства. Для отображения всех обнаруженных звуковых API/серверов, включая неактивные, нужно использовать ключ -Ax:
	$ inxi -Ax
	Audio:
	  Device-1: Intel Alder Lake PCH-P High Definition Audio vendor: Lenovo
	  driver: sof-audio-pci-intel-tgl bus-ID: 00:1f.3
	  API: ALSA v: k6.1.12-un-def-alt1 status: kernel-api
	  Server-1: JACK v: 1.9.22 status: off
	  Server-2: PulseAudio v: 16.1 status: active

-b	Выводит общую информацию в краткой форме. Аналогично выводу $ inxi -v 2.
-B	Выводит данные батареи системы (при наличии батареи): (ID-x), заряд, состояние, а также дополнительную информацию. $ inxi -B Battery: ID-1: BAT0 charge: 54.5 Wh (100.0%) condition: 54.5/57.0 Wh (95.6%)

-c	Задает цветовую тему для стилизации выводимой информации. Предустановлено 43 темы (0-42):
	$ inxi -c 5
	Просмотреть все предустановленные темы можно, выполнив команду:
	$ inxi -c 94

-C	Выводит данные о процессоре (дополнительные данные доступны с ключами -x, -xxx и -a):
	$ inxi -C
	CPU:
	  Info: 10-core (2-mt/8-st) model: 12th Gen Intel Core i7-1255U bits: 64
	  type: MST AMCP cache: L2: 6.5 MiB
	  Speed (MHz): avg: 2480 min/max: 400/4700:3500 cores: 1: 2873 2: 3438
	  3: 1903 4: 2600 5: 1787 6: 2600 7: 2600 8: 2316 9: 2600 10: 2600 11: 2600
	  12: 1853

-d	Выводит данные накопителей на оптических дисках

-D	Выводит информацию о жестких дисках: идентификатор диска, тип (FireWire, съемный, USB), производитель (если обнаружен), модель и размер. Также показывает общее пространство на дисках и занятое место:
	$ inxi -D
	Drives:
	  Local Storage: total: 1.4 TiB used: 426.1 GiB (29.8%)
	  ID-1: /dev/nvme0n1 vendor: Micron model: MTFDKCD512TFK size: 476.94 GiB
	  ID-2: /dev/nvme1n1 vendor: Western Digital model: WD PC SN740 SDDPTQD-1T00
	  size: 953.87 GiB

-E	Выводит информацию об устройствах bluetooth:
	$ inxi -E
	Bluetooth:
	  Device-1: Intel AX201 Bluetooth driver: btusb type: USB
	  Report: hciconfig ID: hci0 state: up address: 3C:21:9C:AE:28:B4 bt-v: 3.0

Продолжение таблицы 67

Ключ	Описание
-F	Выводит общую информацию. Включает все буквы верхнего регистра, а также -s и -n. Не выводит дополнительные подробные данные, такие как -d -f -l -m -o -p -r -t -u -x, если эти ключи не используются в команде, например: $ inxi –Frmxx

-G	Выводит информацию о графических устройствах, включая сведения о драйверах устройств и дисплеев.
	При использовании ключей -Gxx также выводится информация о мониторах.
	$ inxi -G
	Graphics:
	  Device-1: Intel Alder Lake-UP3 GT2 [Iris Xe Graphics] driver: i915 v: kernel
	  Device-2: Syntek Integrated Camera driver: uvcvideo type: USB
	  Display: x11 server: X.Org v: 1.21.1.8 driver: X: loaded: modesetting
	  unloaded: fbdev,vesa dri: iris gpu: i915 resolution: 1: 1920x1080~60Hz
	  2: 1920x1080~60Hz
	  API: OpenGL v: 4.6 Mesa 23.0.4 renderer: Mesa Intel Graphics (ADL GT2)

-i	Отображает локальные и WAN IP-адреса. По соображениям безопасности, эти данные не отображаются в выводе с -F

-I	Выводит следующую информацию: процессы, время бесперебойной работы, память, оболочка:
	$ inxi -I
	Info:
	  Processes: 338 Uptime: 3h 15m Memory: available: 38.88 GiB
	  used: 9.91 GiB (25.5%) Shell: Bash inxi: 3.3.27
	Для получения дополнительной информации, можно использовать параметры -Ix, -Ixx и -Ia:
	$ inxi -Ia
	Info:
	  Processes: 337 Uptime: 3h 16m wakeups: 4 Memory: available: 38.88 GiB
	  used: 9.94 GiB (25.6%) Init: systemd v: 252 target: graphical (5)
	  default: graphical tool: systemctl Compilers: gcc: 12 Packages: pm: rpm
	  pkgs: N/A note: see --rpm Shell: Bash v: 4.4.23 running-in: xfce4-terminal
	  inxi: 3.3.27

-j	Показывает все активные типы подкачки (раздел, файл, zram).
	Чтобы отобразить метки разделов или UUID (если они доступны и уместны), следует использовать с -l или -u.
	$ inxi -ju
	Swap:
	  ID-1: swap-1 type: partition size: 7.46 GiB used: 0 KiB (0.0%)
	  dev: /dev/nvme0n1p2 uuid: 3cee8e1f-494c-4622-90d9-5f3da9ab2082

-J	Выводит данные USB для подключенных концентраторов и устройств. Концентраторы также показывают количество портов
-l	Выводит метки разделов. Следует использовать с ключами -j, -o, -p и -P. Если ни один из этих ключей не указан, ничего не выводит
-L	Выводит информацию о логическом томе для LVM, LUKS, bcache и т. д.

Продолжение таблицы 67

Ключ	Описание

-m	Выводит информацию о памяти (RAM). Не отображается с ключами -b или -F, если -m не указывается явно. Данный ключ использует dmidecode, который должен запускаться от имени пользователя root:
	`# inxi -m`
	`Memory:`
	`  System RAM: available: 38.88 GiB used: 9.95 GiB (25.6%)`
	`  Array-1: capacity: 256 GiB slots: 8 EC: None`
	`  Device-1: Controller0-ChannelA-DIMM0 type: DDR4 size: 32 GiB`
	`  speed: 3200 MT/s`
	`Device-2: Controller0-ChannelB-DIMM0 type: no module installed`
	`...`

-M	Выводит информацию о машине: устройство, материнская плата, BIOS.
-n	Выводит расширенную информацию о сетевом устройстве.

-N	Выводит информацию о сетевых устройствах, включая драйвер устройства. С ключом -x показывает идентификатор шины, номер порта.
	`$ inxi -N`
	`Network:`
	`  Device-1: Intel Alder Lake-P PCH CNVi WiFi driver: iwlwifi`
	`  Device-2: Intel Ethernet I219-V driver: e1000e`

-o	Выводит информацию о несмонтированном разделе (включая UUID и LABEL, если они доступны)
-p	Выводит полную информацию о всех смонтированных разделах. Чтобы отобразить метки разделов или UUID (если они доступны и уместны), следует использовать с ключами -l или –u.

-P	Выводит основную информацию о разделах (показывает, если обнаружено: / /boot /boot/efi /home /opt /tmp /usr /usr/home /var /var/tmp /var/log):
	`$ inxi -P`
	`Partition:`
	`  ID-1: / size: 460.79 GiB used: 426.1 GiB (92.5%) fs: ext4`
	`  dev: /dev/nvme0n1p3`
	`  ID-2: swap-1 size: 7.46 GiB used: 0 KiB (0.0%) fs: swap`
	`  dev: /dev/nvme0n1p2`

-r	Выводит информацию о репозиториях
-R	Выводит данные RAID. Показывает устройства RAID, состояния, уровни, размер устройства/массива и компоненты

-s	Выводит данные от датчиков (если эти датчики установлены/настроены): температура материнской платы/процессора/графического процессора; скорость вентилятора:
	`$ inxi -s`
	`Sensors:`
	`  System Temperatures: cpu: 48.0 C mobo: N/A`
	`  Fan Speeds (RPM): fan-1: 1800 fan-2: 1800`

-S	Выводит информацию о системе: имя хоста, ядро, окружение рабочего стола, дистрибутив. С ключами -xx также показывает DM

Окончание таблицы 67

Ключ	Описание
-t	Выводит процессы: -t c – только процессор; -t m – только память; -t cm – процессор/память (по умолчанию). Если указано число, показывает данное количество процессов для каждого типа (по умолчанию 5). $ inxi -t cm3 Processes: CPU top: 3 of 348 1: cpu: 27.6% command: virtualboxvm pid: 7152 2: cpu: 17.3% command: virtualboxvm pid: 5544 3: cpu: 7.3% command: x pid: 2700 System RAM: available: 38.88 GiB used: 10.21 GiB (26.3%) Memory top: 3 of 348 1: mem: 1376.0 MiB (3.4%) command: virtualboxvm pid: 5544 2: mem: 1306.8 MiB (3.2%) command: virtualboxvm pid: 7152 3: mem: 808.8 MiB (2.0%) command: telegram pid: 5163
-u	Выводит UUID разделов. Для отображения меток разделов следует использовать с ключами -j, -o, -p и -P. Если ни один из этих ключей не указан, ничего не выводит
-v	Задает уровень детализации. Если номер уровня детализации не указан, предполагается значение 0. Не следует использовать с -b или -F. Поддерживаются уровни 0 – 8: 0 – вызов inxi без параметров; 1 – базовый уровень, включает: -S + базовая информация о центральном процессоре (ЦП) + -G + базовая информация о дисках + -I; 2 – включает информацию: о сетевых устройствах (-N), информацию о машине (-M), данные батареи (-B). То же самое, что и inxi -b; 3 – включает: данные о ЦП (-C), данные батареи (-B), сетевые устройства (-n) (тоже, что и -x); 4 – включает основную информацию о разделах (-P) для /, /home, /var/, /boot. Показывает полную информацию о жестких дисках (-D); 5 – включает: информацию об аудиоустройствах (-A), данные от датчиков (-s), RAM (-m), информацию о bluetooth, метки разделов (-l), все активные типы подкачки (-j), UUID (-u), информацию об оптических устройствах, данные RAID; 6 – включает полную информацию о всех смонтированных (-p) и несмонтированных разделах (-o), оптических устройствах (-d), USB (-J), RAID (тоже, что и -xx); 7 – включает локальные и WAN IP-адреса (-i), информацию о bluetooth, информацию о логических томах (-L), RAID, все данные CPU (тоже, что и -xxx); 8 – включает всю доступную информацию, репозитории (-r), процессы (-tcm), слоты PCI (--slots). $ inxi -v 7

Ключи можно комбинировать, если они не конфликтуют. Например:

```
$ inxi -AG
Graphics:
  Device-1: Intel Alder Lake-UP3 GT2 [Iris Xe Graphics] driver: i915 v:
kernel
  Device-2: Syntek Integrated Camera driver: uvcvideo type: USB
  Display: x11 server: X.Org v: 1.21.1.8 driver: X: loaded: modesetting
```

```
    unloaded: fbdev,vesa dri: iris gpu: i915 resolution: 1: 1920x1080~60Hz
    2: 1920x1080~60Hz
  API: OpenGL v: 4.6 Mesa 23.0.4 renderer: Mesa Intel Graphics (ADL GT2)
Audio:
  Device-1: Intel Alder Lake PCH-P High Definition Audio
    driver: sof-audio-pci-intel-tgl
  API: ALSA v: k6.1.12-un-def-alt1 status: kernel-api
  Server-1: PulseAudio v: 16.1 status: active
```

Для получения более подробных данных о различных параметрах можно использовать один или несколько ключей `-x` (всего три дополнительных уровня данных: `-x`, `-xx`, `-xxx`). Эти ключи можно добавить в любой список опций, например: `-bxx` или `-Sxxx`.

Для получения более технических параметров (параметров администратора) используется ключ `--admin` или `-a`.

Чтобы обеспечить базовую конфиденциальность и безопасность, `inxi` позволяет отфильтровывать такие данные, как MAC-адрес сетевой карты, серийные номера, IP-адрес WAN и LAN, домашний каталог пользователя. Для активации фильтрации используется ключ `-z`, например:

```
$ inxi -iz
Network:
  Device-1: Intel Alder Lake-P PCH CNVi WiFi driver: iwlwifi
  IF: wlp0s20f3 state: up mac: <filter>
  IP v4: <filter> type: dynamic noprefixroute scope: global
  IP v6: <filter> type: noprefixroute scope: global
  IP v6: <filter> type: noprefixroute scope: global
  IP v6: <filter> type: noprefixroute scope: link
  Device-2: Intel Ethernet I219-V driver: e1000e
  IF: enp0s31f6 state: up speed: 1000 Mbps duplex: full mac: <filter>
  IP v4: <filter> type: dynamic noprefixroute scope: global
  IP v6: <filter> type: noprefixroute scope: global
  Message: Output throttled. IPs: 4; Limit: 10; Override: --limit [1-x;-1
    all]
  WAN IP: <filter>
```

Следующая команда проверяет зависимости и программы, которые требуются для работы `inxi`, а затем показывает, какие пакеты нужно установить, чтобы добавить поддержку каждой функции:

```
$ inxi --recommends
```

Пример использования цветовой темы с выводом детальной информации в файл для анализа, команда выполняется от администратора, так как не вся информация доступна пользователю:

```
# inxi -c2 -v8 > inxi.txt
```

16.20.2. Команда `glxinfo`

Команда `glxinfo` позволяет получить информацию о OpenGL и реализации GLX в Xwindows.

Установка пакета:

```
# apt-get install glxinfo
```

Примеры:

- краткий вывод:

```
  $ glxinfo -B
```

- показать информацию об активной видеокарте:

```
 $ glxinfo -B | grep 'Device:'
     Device: Mesa Intel(R) Graphics (ADL GT2) (0x46a8)
```

- получить информацию о поддержке OpenGL renderer:

```
 $ glxinfo  | grep rendering
 direct rendering: Yes
```

- посмотреть информацию по графике intel (NVIDIA):

```
 $ glxinfo | grep OpenGL
```

- узнать версию сервер/клиент, версию драйвера:

```
 $ glxinfo | grep version
```

- просмотреть количество памяти, доступное видеокарте:

```
 $ glxinfo | egrep -i 'device|memory'
 egrep: warning: egrep is obsolescent; using grep -E
     Device: Mesa Intel(R) Graphics (ADL GT2) (0x46a8)
     Video memory: 39808MB
     Unified memory: yes
```

16.21. Xpra

Xpra – это инструмент, который запускает программы X11, обычно на удаленном хосте, и направляет их отображение на локальный компьютер без потери состояния (позволяет отключение и повторное подключение без прерывания перенаправленного приложения).

Xpra может предоставить удаленный доступ, как к отдельным приложениям, так и к новым/существующим сеансам рабочего стола.

Xpra не имеет root-доступа: т. е. приложения, перенаправленные xpra, отображаются на локальном рабочем столе как обычные окна, управляемые локальным оконным менеджером. Xpra также использует собственный протокол, который самонастраивается и относительно нечувствителен к задержкам.

На сервере утилита Xpra запускает в режиме демона нужную программу с заданным идентификатором сеанса, а на клиенте происходит присоединение к сеансу с этим идентификатором.

Доступ к сеансам можно получить по SSH или через защищенные паролем сокеты TCP (с SSL или без).

16.21.1. Установка

Для установки на сервере и на клиенте выполните команду:

```
# apt-get install xpra
```

Можно использовать клиент html5, и в этом случае на клиенте ничего устанавливать не нужно. А на сервере, начиная с xpra версии 4.4.4, нужно дополнительно установить пакет xpra-html5:

```
# apt-get install xpra-html5
```

16.21.2. Режимы работы

16.21.2.1. Запуск приложения

Запуск приложения или бесшовный режим (seamless) – позволяет пересылать клиенту отдельные окна приложений, эти окна появляются на рабочем столе клиента так же, как и другие локальные приложения.

Все операции по управлению окнами выполняются непосредственно клиентской ОС или оконным менеджером, поэтому любые задержки между клиентом и сервером не мешают действиям по управлению окнами (сворачивание, перемещение, изменение размера окна).

Пример запуска приложения xterm удаленно, через SSH, без предварительного запуска xpra на сервере:

```
$ xpra start ssh://user@192.168.0.101 --start="xterm"
```

П р и м е ч а н и е . Xpra и запускаемое приложение должны быть установлены на сервере.

Вместо параметра `--start=команда`, можно использовать параметр `--start-child=команда`, позволяющий учитывать параметр `--exit-with-children`. Если параметр `--exit-with-children=yes`, то сервер xpra будет отслеживать состояние дочерних элементов, запущенных `--start-child`, и автоматически завершится, когда последний из них завершит работу.

Запуск приложения, с предварительным запуском сервера xpra:

1) на сервере: запустить экземпляр сервера xpra, автоматически выбрать дисплей и запустить программу (например, xterm) на этом виртуальном дисплее:

```
$ xpra start --start=kolourpaint
Entering daemon mode; any further errors will be reported to:
'/run/user/500/xpra/1/server.log'
```

2) с клиента подключиться к этому экземпляру сервера:

```
$ xpra attach ssh://user@192.168.0.101/1
```

Локальное подключение:

- запустить экземпляр сервера xpra на дисплее 101 (или автоматически выбрать дисплей) и запустить программу (например, firefox) на этом виртуальном дисплее:

```
$ xpra start :101 --start=firefox
Entering daemon mode; any further errors will be reported to:
'/run/user/500/xpra/101/server.log'
```

- подключиться к этому экземпляру сервера:

```
$ xpra attach :101
```

Подключение с использованием сокетов TCP:

- запустить экземпляр сервера xpra:

```
$ xpra start --start=xterm --bind-tcp=0.0.0.0:10000
Entering daemon mode; any further errors will be reported to:
  '/run/user/500/xpra/S9454/server.log'
Actual display used: :1
Actual log file name is now: '/run/user/500/xpra/1/server.log'
```

- подключиться к серверу, используя выбранный порт:

```
$ xpra attach tcp://192.168.0.109:10000
```

ВНИМАНИЕ!

Использование параметра `--bind-tcp` без использования параметра `tcp-auth` не рекомендуется и представляет серьезную угрозу безопасности (особенно при 0.0.0.0), т.к. кто угодно может подключиться к этому порту и получить доступ к сеансу. Доступ к сеансам Xpra в режиме TCP и websocket можно защитить, используя аутентификацию и шифрование.

16.21.2.2. Запуск новой графической сессии

Режим рабочего стола (desktop) позволяет запустить вложенный сервер X11.

Запуск приложения:

```
$ xpra start-desktop --start=firefox
```

Та же команда, но с запуском сеанса и подключением к нему со стороны клиента:

```
$ xpra attach ssh://user@10.81.1.130/2
```

Где `2` номер дисплея.

Чтобы запустить оконный менеджер (WM) или среду рабочего стола (DE) достаточно в примере выше заменить команду `xterm` командой, которая запускает WM или DE, например:

```
$ xpra start-desktop ssh://user@192.168.0.99 --exit-with-children --start-child=mate-session
```

Подключение:

```
$ xpra attach ssh://user@192.168.0.154:101 --min-size=1200x800 --clipboard-direction=both --clipboard=yes --opengl=no
```

Примечание. Чтобы сеанс завершался при выходе из WM, следует использовать `--start-child` и `--exit-with-children`.

16.21.2.3. Получение управления запущенной графической сессией (shadow режим)

Этот режим позволяет использовать xpra для удаленного доступа к существующему сеансу рабочего стола (обычно подключенному к реальному физическому дисплею).

Примечание. Shadow режим поддерживается на всех платформах, включая MS Windows и Mac OS X, но не на Wayland. В некоторых случаях, использование этого режима, может вызвать высокую нагрузку на процессор как на сервере, так и на клиенте. На большинстве платформ затеняемый дисплей должен быть активен: не заблокирован и не выключен.

Если к машине, к дисплею X11 которой нужно получить удаленный доступ, есть SSH-доступ, можно на клиенте запустить команду:

```
$ xpra shadow ssh://user@HOST/
```

В результате выполнения этой команды будет произведено подключение по SSH к HOST, запущен теневой сервер xpra и произведено подключение к нему. Теневой сервер будет остановлен после отключения.

При этом на сервере в трее появится значок («Exit» – остановить сервер, «Read Only» – запретить управление, только просмотр рабочего стола) (рис. 474).

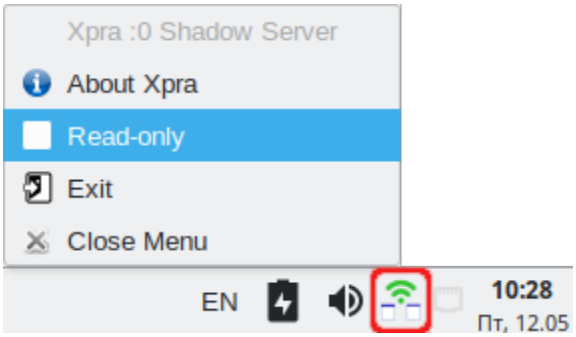


Рис. 474

Если запуск через SSH не поддерживается или нужно запустить теневой сервер вручную и, возможно, настроить дополнительные параметры, можно запустить его из оболочки. Пример запуска управления запущенной графической сессией через TCP-сокеты:

```
$ xpra shadow :0 --bind-tcp=0.0.0.0:9876
```

16.21.3. Использование

16.21.3.1. Некоторые команды xpra

Некоторые команды xpra приведены в таблице 68.

Т а б л и ц а 68 – Команды xpra

Команда	Описание	Пример
xpra start	Запустить новый сервер xpra (при запуске удаленного сервера со строкой подключения `ssh://HOST/DISPLAY` новый сеанс также будет присоединен)	`$ xpra start :7` `$ xpra start --start=gimp`
xpra start-desktop	Запустить вложенный сервер X11, все дочерние команды будут запускаться на вложенном сервере X11	`$ xpra start-desktop --start=xfce4-session`
xpra attach	Подключиться к работающему серверу xpra. Любые приложения, использующие этот сервер, будут перенаправляться на текущий экран	`$ xpra attach :7` `$ xpra attach ssh://user@test/7`
xpra detach	Отсоединить данный дисплей xpra	`$ xpra detach :7`
xpra screenshot	Сделать снимок экрана и сохранить его в файле с указанным именем (снимки экрана можно делать только при подключенном клиенте)	`$ xpra screenshot my.jpg`
xpra version	Вывести версию сервера	`$ xpra version` `4.4.4-r0`
xpra info	Вывести версию, статус и статистику	
xpra top	Отобразить ключевые атрибуты работоспособности сервера	
xpra control	Изменить параметры запущенного сервера. Список команд можно получить, указав «help» в качестве команды (например, `xpra control :1 help`)	`$ xpra control :1 min-quality 20`
xpra stop	Подключиться к работающему серверу xpra и запросить его немедленное завершение. Обычно это приводит к тому, что любые приложения, использующие этот сервер, также прекращают работу	
xpra exit	Подключиться к работающему серверу xpra и запросить его немедленное завершение. В отличие от команды xpra stop, процесс Xvfb и его клиенты X11 (если таковые имеются) останутся запущенными	
xpra showconfig	Вывести конфигурацию xpra. В качестве дополнительных аргументов можно указать определенные параметры, или использовать специальное значение all, чтобы отобразить все параметры	`$ xpra showconfig clipboard-direction` `clipboard-direction = 'both'`
xpra list	Вывести список всех серверов xpra, запущенные текущим пользователем на текущей машине	
xpra shadow	Предоставить доступ к рабочему столу (существующему дисплею X11). Если активен только один дисплей X11 и его номер меньше 10, он может быть обнаружен автоматически. Для этого режима работы настоятельно рекомендуется использовать видеокодек (h264 или vp8)	

Окончание таблицы 68

Команда	Описание	Пример
xpra proxy	Позволяет одному серверу проксировать соединения для нескольких других, потенциально выступая в качестве точки входа для балансировки нагрузки или аутентификации для многих сеансов. Прокси-сервер будет создавать новый процесс для каждого прокси-соединения, этот прокси-процесс создаст неаутентифицированный новый сокет домена unix, который можно использовать с подкомандами info, version и stop	

16.21.3.2. Строка подключения

Локальный дисплей (только для локальных дисплеев локального пользователя):

`:DISPLAY`

Подключение с использованием SSH:

`ssh://[USERNAME[:PASSWORD]@]HOST[:SSH_PORT]/[DISPLAY][?QUERYSTRING]`

`QUERYSTRING` можно использовать для указания прокси-сервера `ssh: ?proxy=ssh://[ИМЯ ПОЛЬЗОВАТЕЛЯ[:ПАРОЛЬ]@]HOST[:SSH_PORT]`. В этом случае xpra установит SSH-соединение с указанным «прокси-сервером» и с этого хоста xpra установит SSH-соединение с сервером xpra.

Для обратной совместимости режим SSH также поддерживает синтаксис:

`ssh:[USERNAME[ PASSWORD]@HOST:DISPLAY`

Пароль нужно указывать только тогда, когда он требуется модулю аутентификации сервера.

Примечание. При подключении по ssh может потребоваться указать системный ssh-клиент:

```
$ xpra start --ssh=ssh ssh://user@192.168.0.101 --start=scratch-desktop
```

Или дописать в файл `~/.xpra/xpra.conf` строку:

```
ssh = ssh
```

В режиме TCP используются номера портов, а не номера дисплеев. Если через один TCP-порт доступно несколько дисплеев (например, при использовании прокси-сервера), то можно также указать номер дисплея:

`tcp://[USERNAME@]HOST:PORT[/DISPLAY]`

Режим SSL (добавляет безопасный уровень сокетов поверх режима TCP):

`ssl://[USERNAME@]HOST:PORT[/DISPLAY]`

Подключиться по протоколу websocket:

`ws://[USERNAME[:PASSWORD]@]HOST:PORT/[DISPLAY]`

Подключиться по защищенному протоколу websocket (websocket с SSL):

`wss://[USERNAME[:PASSWORD]@]HOST:PORT/[DISPLAY]`

16.21.3.3. Дисплей

При запуске xpra сервера (`xpra start`) можно не использовать номер дисплея, в этом случае он будет выбран автоматически. Номер дисплея будет указан в выводе команды, также его можно увидеть, выполнив команду `xpra list`.

В противном случае, при запуске сервера xpra может потребоваться указать номер дисплея. Для этого можно выбрать любое число и поставьте перед ним двоеточие (например, :7, :12 и :3117). Нужно учитывать, что:

- каждый X или xpra сервер, работающие на одном хосте должны использовать уникальный номер дисплея;
- первые несколько цифр (0, 1, 2) обычно используются реальными X серверами.

При указании сервера xpra в клиентской программе (`xpra attach`, `xpra detach`, `xpra stop`, `xpra exit`, `xpra version`, `xpra info`, `xpra list`, `xpra screenshot`) можно использовать указание дисплея в формате `:DISPLAY` при подключении к локальному узлу или одну из форм `ssh://[USER@]HOST/DISPLAY` при подключении к удаленному узлу. Если на узле запущен только один сеанс xpra, то номер дисплея можно не указывать.

Если при запуске сервера был указан параметр `--bind-tcp`, `--bind-ssl` `--bind-udp=[HOST]:PORT`, `--bind-ws`, `--bind-wss` или `--bind-vsock`, то к нему можно подключаться используя следующие строки:

```
tcp://HOST:PORT[/DISPLAY],
udp://HOST:PORT[/DISPLAY],
ssl://HOST:PORT[/DISPLAY],
ws://HOST:PORT[/DISPLAY],
wss://HOST:PORT[/DISPLAY] или vsock://HOST:PORT[/DISPLAY].
```

16.21.3.4. Сеть и аутентификация

Xpra поддерживает разные типы сетевых подключений (`tcp`, `ssl`, `ws`, `wss`, `vnc`, `ssh`, `vsock`, `quic` и т. д.), и большинство из них можно шифровать и мультиплексировать через один порт.

Безопасность зависит от типа подключения клиента `xpra` (`ssl`, `quic` и `ssh` считаются самыми безопасными, поскольку они обеспечивают проверку хоста и шифрование в одном протоколе).

Доступ к сеансам xpra через сокеты TCP можно защитить с помощью модулей аутентификации, но так как они не защищают само сетевое соединение от атак «человек посередине», то для защиты от таких атак можно использовать один из трех вариантов:

- шифрование AES;
- SSL;
- SSH.

16.21.3.4.1. Модули аутентификации

Примечание. При использовании для подключения к серверу SSH разделы шифрование и аутентификация можно пропустить (по умолчанию сокеты, используемые ssh, не используют аутентификацию).

Модули аутентификации приведены в таблице 69.

Таблица 69 – Модули аутентификации

Модуль	Описание	Примечание
allow	Аутентификация всегда успешна (используется имя пользователя, предоставленное клиентом)	Небезопасно, и должно использоваться только для тестирования
none	Аутентификация всегда успешна (используется имя пользователя, под которым работает сервер)	Небезопасно, и должно использоваться только для тестирования
fail	Аутентификация всегда не успешна (пароль не запрашивается)	Полезно для тестирования
reject	Аутентификация всегда не успешна (пароль запрашивается)	Полезно для тестирования

Продолжение таблицы 69

Модуль	Описание	Примечание
env	Пароль сопоставляется с указанной переменной среды (по умолчанию XPRA_PASSWORD).	`--auth=env:name=SOME_OTHER_ENV_VAR_NAME`
password	Пароль сопоставляется с паролем, указанным с помощью опции value	`--auth=password:value=mysecret`

file	Сравнивает пароль с паролем, записанным в файле, указанным с помощью опции filename	`--auth=file:filename=./password.txt`
		Содержимое файла пароля будет рассматриваться как двоичные данные, ограничений на кодировку символов или размер файла нет. Следует остерегаться завершающих символов новой строки, которые будут включены в данные пароля (пример создания файла с паролем:
		`echo -n "mypassword" > password.txt)`

multifile	Сопоставляет имя пользователя и пароль с содержимым файла аутентификации, указанным с помощью опции filename	Файл аутентификации должен содержать учетные данные пользователей в формате: `username|password|uid|gid|displays|env_opts|session_opts` Имя пользователя и пароль не должны содержать символ вертикальной черты (|), который используется в качестве разделителя. Этот модуль устарел, вместо него следует использовать sqlite
pam	Проверяет имя пользователя и пароль с помощью системы PAM	Аутентификация ОС Linux
win32	Проверяет имя пользователя и пароль с помощью win32security	Аутентификация MS Windows
sys	Системная аутентификация	Автоматически выбирает соответствующий системный модуль аутентификации (либо pam, либо win32)
sqlite, mysql, sql	Сверяет имя пользователя и пароль с файлом базы данных sqlite, указанным с помощью параметра filename (sqlite), или с базой данных, указанной с помощью параметра uri (mysql и sql)	Аутентификация будет обработана с использованием следующего запроса (настраивается с помощью параметра password_query): `SELECT password FROM users WHERE username=(?)` Сеансы, доступные для каждого пользователя, будут запрашиваться с помощью запроса (настраивается с помощью параметра session_query): `SELECT uid, gid, displays, env_options, session_options FROM users WHERE username=(?)`
exec	Делегирует процедуру аутентификации внешней команде. Команда указывается с помощью атрибута command	Команда должна вернуть 0, чтобы разрешить доступ, любое другое значение будет запрещать доступ
peercred	Аутентификация SO_PEERCRED	

Окончание таблицы 69

Модуль	Описание	Примечание
hosts	Проверяет хост с помощью системной библиотеки tcp-wrappers	Подробнее см. в hosts.allow и hosts.deny
kerberos-password	Проверяет имя пользователя и пароль с помощью проверки подлинности Kerberos	Модуль не использует билеты Kerberos, и пароль будет отправлен на сервер в виде открытого текста. Следует использовать только для тестирования
kerberos-ticket	Проверяет билет Kerberos, полученный клиентом	
gss	Проверяет билет GSS, полученный клиентом	
u2f	Запрашивает у клиента токен U2F	
ldap	Проверяет имя пользователя и пароль на сервере LDAP, используя библиотеку python-ldap	
ldap3	Проверяет имя пользователя и пароль на сервере LDAP, используя библиотеку python-ldap3	

Предпочтительный способ указания аутентификации – в опции сокета.

Примеры:

```
$ XPRA_PASSWORD=mysecret
$ xpra start --start=xterm --bind-tcp=0.0.0.0:10000,auth=env

$ SOME_OTHER_ENV_VAR_NAME=mysecret
$ xpra start --bind-
tcp=0.0.0.0:10000,auth=env:name=SOME_OTHER_ENV_VAR_NAME

$ xpra start --bind-
tcp=0.0.0.0:10000,auth=password:value=mysecret

$ xpra start --bind-
tcp=0.0.0.0:10000,auth=file:filename=/path/to/mypasswordfile.txt

$ xpra start --bind-
tcp=0.0.0.0:10000,auth=sqlite:filename=/path/to/userlist.sdb
```

Разные сокеты могут использовать разные модули аутентификации:

```
$ xpra start --start=xterm -d auth \
--bind-
tcp=0.0.0.0:10000,auth=hosts,auth=file:filename=password.txt --bind \
--bind-tcp=0.0.0.0:10001,auth=sys
```

16.21.3.5. Журналирование

Журналирование управляется опцией `--debug` (`-d`).

Например, запуск сервера xpra с включенной отладкой фокуса:

```
$ xpra start -d focus --start=xterm
```

Список возможных категорий журналов можно получить, выполнив команду:

```
$ xpra -d help
```

Для записи в журнал событий всех категорий используется значение `all` (следует избегать применение этого значения, так как вывод будет очень подробным и сложным для восприятия).

Добавление к категории знака «-» отключает для данной категории ведение журнала. Например, регистрировать все категории, кроме window и focus:

```
$ xpra start :10 -d all,-window,-focus
```

Категорию журналирования также можно включить с помощью переменных среды. Это может потребоваться, если нет возможности изменить командную строку, или если регистрация должна происходить очень рано.

Например, включить отладку «геометрии» с помощью подкоманды `attach`:

```
XPRA_GEOMETRY_DEBUG=1 xpra attach
```

У запущенного сервера xpra можно изменить параметры журналирования с помощью подкоманды control (эту команду можно использовать как на сервере, так и на клиенте):

```
$ xpra control :DISPLAY debug enable CATEGORY
```

Сервер также может пересылать команды управления отладкой подключенным к нему клиентам:

```
$ xpra control :DISPLAY client debug enable geometry
```

Можно включить сразу несколько категорий:

```
$ xpra control :2 debug enable window geometry screen
```

Включить только регистраторы, которые соответствуют категориям с +:

```
$ xpra control :2  debug disable focus+grab
```

Конфиденциальная информация, такая как пароли и ключи обычно не отображается в журнале, но все же, используя журнал можно собрать достаточно данных, чтобы представлять реальную угрозу.

Хорошей превентивной мерой является отключение удаленного ведения журнала и выключение канала управления сервером.

`xpra shell` – это очень мощная функция отладки, которая обеспечивает полный доступ ко всем структурам данных, хранящимся на клиенте и сервере. По умолчанию эта функция отключена.

16.21.4. Клиент HTML5

Пример запуска экземпляра сервера:

```
$ xpra start --start=xterm --bind-tcp=0.0.0.0:10000 --html=on
```

Или:

```
$ xpra start --start=xterm --bind-ws=0.0.0.0:10000
```

Теперь можно получить доступ к этому сеансу в веб-браузере (рис. 475).

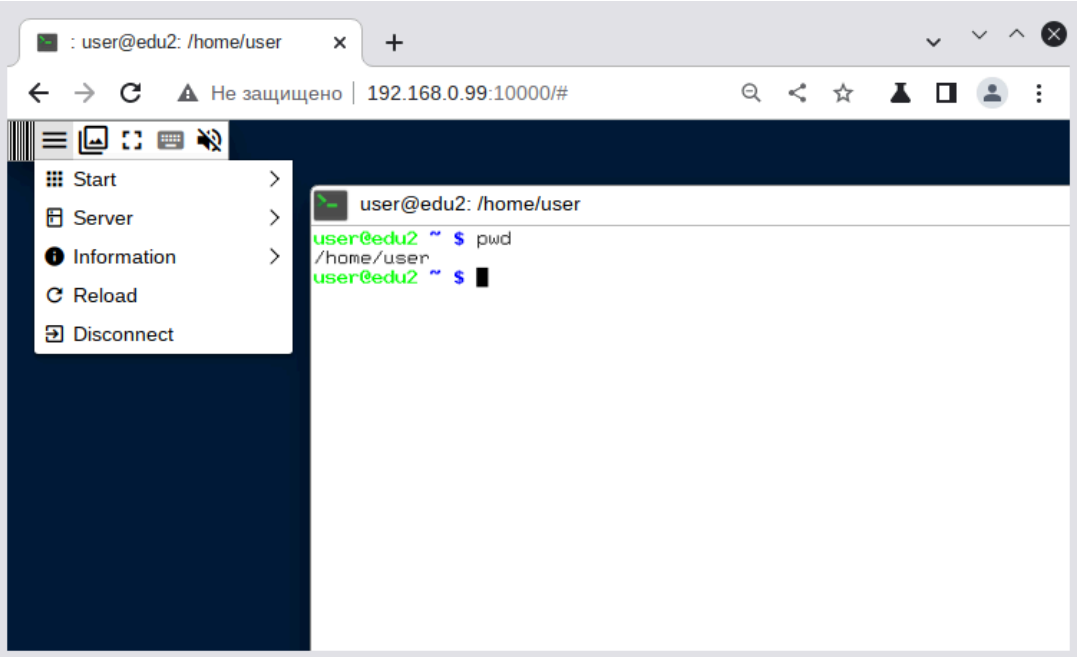


Рис. 475

Параметры подключения можно указать с помощью диалоговой формы подключения (`http://host:port/connect.html`) или указать как параметры URL, например: `http://192.168.0.99:10000/?username=user&keyboard_layout=us`.

Значения по умолчанию можно указать в файле:

`/etc/xpra/html5-client/default-settings.txt`.

Описание параметров подключения приведены в таблице 70.

Таблица 70 – Описание параметров подключения

Параметр	Описание
Параметры подключения	
server	Имя хоста или IP-адрес xpra-сервера
port	Номер порта xpra-сервера
username	Аутентификация на сервере
password	Аутентификация на сервере
ssl	Включить SSL-соединение с сервером xpra
insecure	Разрешить отправку паролей по незашифрованным соединениям (No)
path	Путь WebSocket для подключения (обычно не требуется)
display	Дисплей для подключения (для прокси-серверов)
password	Аутентификация на сервере
encryption	Для включения шифрования, следует указать AES-CBC, AES-CTR или AES-CFB
key	Ключ шифрования AES
sharing	Разрешить другим клиентам подключаться к тому же сеансу (No)
steal	Взять на себя управление сеансом и отключить всех существующих клиентов (Yes)
reconnect	Автоматически переподключаться при обрыве соединения (Yes)
bandwidth_limit	Бюджет пропускной способности в битах в секунду (0 – без ограничений)
override_width	Ширина рабочего стола клиента, ширина окна веб-браузера в пикселях (по умолчанию – ширина окна веб-браузера)
Функции	
keyboard	Включить ввод с клавиатуры
keyboard_layout	Раскладка клавиатуры, которую будет использовать клиент (по умолчанию язык веб-браузера)
clipboard	Включить общий доступ к буферу обмена.
printing	Включить переадресацию принтера
file_transfer	Включить передачу файлов
swap_keys	Поменять местами клавиши Command и Control
scroll_reverse_x	Реверс оси X указателя мыши
floating_menu	Показывать плавающее меню
toolbar_position	Положение панели инструментов по умолчанию (например, top, top-right)
autohide	Скрыть большую часть панели инструментов до наведения на нее указателя
sound	Переадресация звука с сервера («выход динамика»)
video	Разрешить использование программного декодирования видео
Дополнительные параметры	
audio_codec	Используемый аудиоформат (detected)
encoding	Кодировка изображения, например, png, jpeg, webp и т. д. (auto)
remote_logging	Отправлять важные события на сервер
action	Режим подключения, например, start, shadow (connect)
shadow_display	Дисплей, если action=shadow
submit	Показать диагностику при отключении
start	Запустить сервер
exit_with_children	Завершить сессию, когда завершается последняя команда запуска (при запуске нового сеанса)
exit_with_client	Завершить сеанс при закрытии соединения (при запуске нового сеанса)

Значения параметров server, port и ssl отражают соединение, которое использовалось для загрузки клиента HTML5 (то, что указано в строке URL-адреса веб-браузера), и эти значения обычно не нужно изменять.

Примечание. Если в окне клиента при вводе с клавиатуры ничего не происходит, попробуйте изменить раскладку клавиатуры (параметр `keyboard_layout`).

16.21.5. Графический интерфейс

Графический интерфейс xpra («Меню запуска приложений» → «Интернет/Сеть» → «Xpra») (рис. 476).

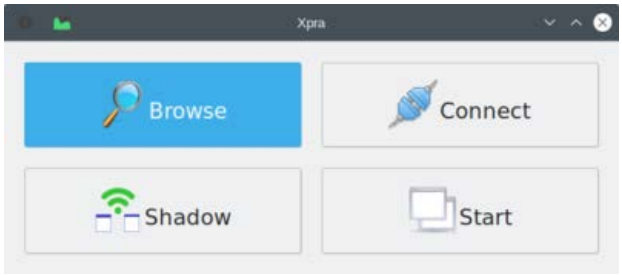


Рис. 476

«Browse» – просмотреть список и подключиться к локальному дисплею (рис. 477).

Рис. 477

«Connect» – подключиться к удаленному серверу (рис. 478).

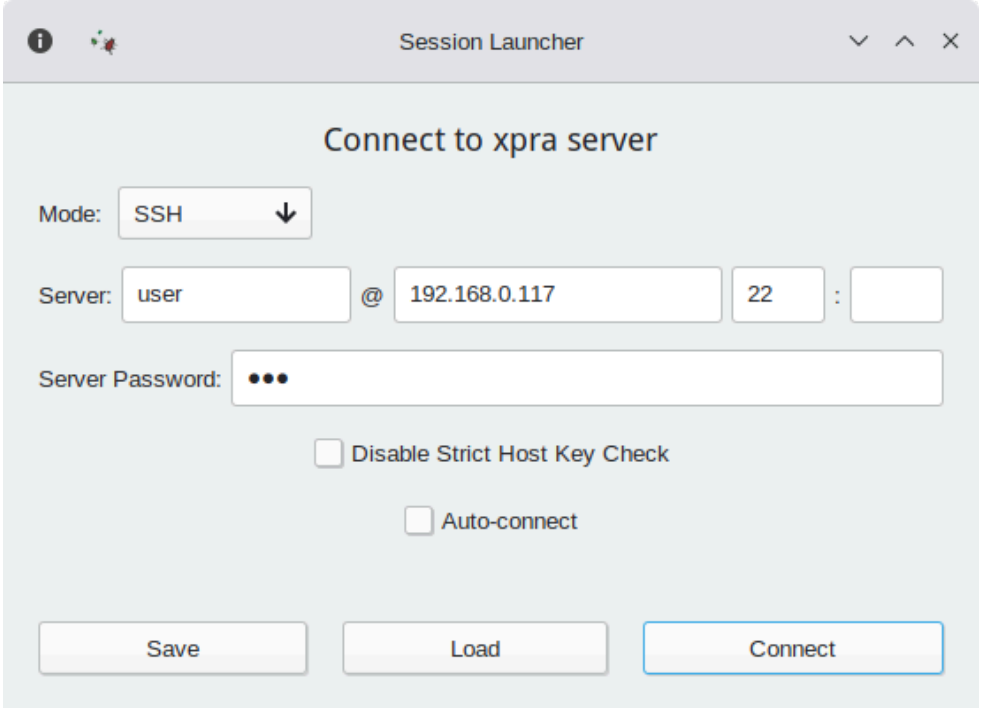


Рис. 478

«Shadow» – предоставить доступ к рабочему столу.

«Start» – запустить сервер xpra (рис. 479).

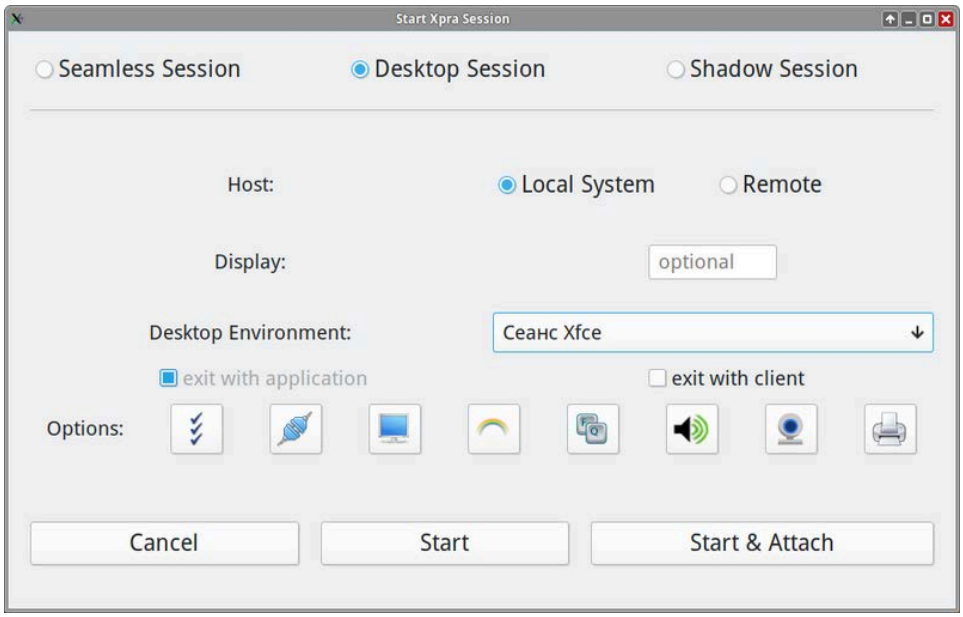


Рис. 479

16.22. Установка корневого сертификата

Для поддержки работы сайтов с российскими сертификатами и установки комплекта корневых сертификатов СА России достаточно установить пакет ca-certificates-digital.gov.ru:

```
# apt-get install ca-certificates-digital.gov.ru
```

В результате в хранилище доверенных сертификатов должны появиться сертификаты «Russian Trusted Root CA» и «Russian Trusted Sub CA»:

```
$ trust  list |grep "Russian Trusted" -B 2 -A 2
pkcs11:id=%E1%D1%81%E5%CE%5A%5F%04%AA%D2%E9%B6%9D%66%B1%C5%FA%AC%2C%87;
type=cert
    type: certificate
    label: Russian Trusted Root CA
    trust: anchor
    category: authority
--
pkcs11:id=%D1%E1%71%0D%0B%2D%81%4E%6E%8A%4A%8F%4C%23%B3%4C%5E%AB%69%0B;
type=cert
    type: certificate
    label: Russian Trusted Sub CA
    trust: anchor
    category: authority
```

Сертификаты «Russian Trusted Root CA» и «Russian Trusted Sub CA» в Chromium-Gost (рис. 480).

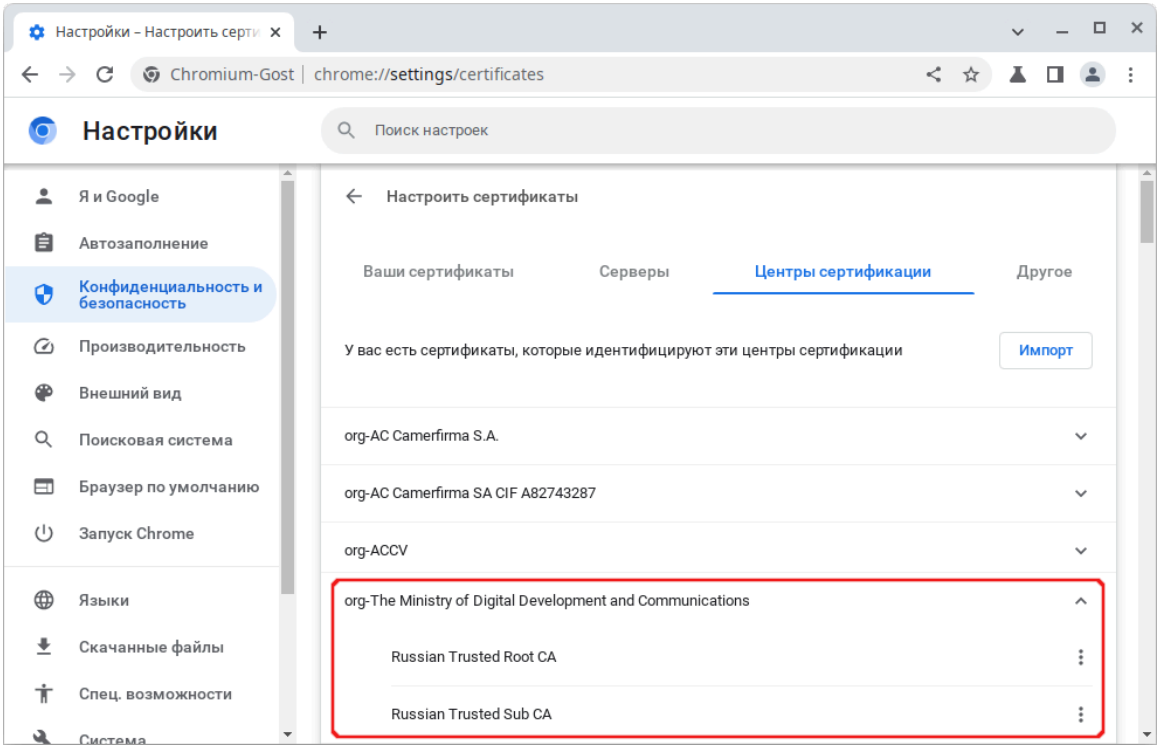


Рис. 480 – Корневые сертификаты СА России в Chromium-Gost

17. УПРАВЛЕНИЕ ПРОГРАММНЫМИ ПАКЕТАМИ

После установки ОС Альт СП при первом запуске доступен тот или иной набор ПО. Количество предустановленных программ зависит от набора программ конкретного дистрибутива или от выбора, сделанного при установке системы. Если интересующие программы не были обнаружены в системе, то имеется возможность доустановить их из разных источников.

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

Для установки, удаления и обновления программ и поддержания целостности системы в ОС семейства Linux используются менеджеры пакетов типа «rpm». Для автоматизации этого процесса и применяется усовершенствованная система управления программными пакетами APT (Advanced Packaging Tool).

⚠ Перед установкой программ внимательно ознакомьтесь с п. 17.4 «Управление установкой (инсталляцией) компонентов программного обеспечения».

Автоматизация достигается созданием одного или нескольких внешних репозиториев, в которых хранятся пакеты программ и относительно которых производится сверка пакетов, установленных в системе. Репозитории могут содержать как официальную версию дистрибутива, обновляемую его разработчиками по мере выхода новых версий программ, так и локальные наработки, например, пакеты, разработанные внутри компании.

Таким образом, 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, руководствуется сведениями о внешнем репозитории для разрешения конфликтов и поиска корректного пути их устранения.

Система APT состоит из нескольких утилит. Чаще всего используется утилита управления пакетами apt-get, которая автоматически определяет зависимости между пакетами и строго следит за их соблюдением при выполнении любой из следующих операций: установка, удаление или обновление пакетов.

17.1. Источники программ (репозитории)

17.1.1. Репозитории для APT

Репозитории, с которыми работает APT, отличаются от обычного набора пакетов наличием мета информации – индексов пакетов, содержащихся в репозитории, и сведений о них. Поэтому, чтобы получить всю информацию о репозитории, APT достаточно получить его индексы.

APT может работать с 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, а расположение в том или ином репозитории не имеет значения. Если потребуется, APT в рамках одной операции установки группы пакетов может пользоваться несколькими репозиториями.

Подключая одновременно несколько репозиториев, нужно следить за тем, чтобы они были совместимы друг с другом по пакетной базе – отражали один определенный этап разработки. Совместимыми являются основной репозиторий дистрибутива и репозиторий обновлений по безопасности к данному дистрибутиву. В то же время смешение среди источников APT репозиториев, относящихся к разным дистрибутивам, или смешение стабильного репозитория с нестабильной веткой разработки (Sisyphus) чревато различными неожиданными трудностями при обновлении пакетов.

APT позволяет взаимодействовать с репозиторием с помощью различных протоколов доступа. Наиболее популярные – HTTP и FTP, однако существуют и некоторые дополнительные методы.

Для того, чтобы APT мог использовать тот или иной репозиторий, информацию о нем нужно поместить в файл.

Файлы описания источников находятся в директории `/etc/apt/sources.list.d/` и имеют расширение `.list`, например:

```
altsp.list
sources.list
```

Так же, есть файл с предопределенным именем: `/etc/apt/sources.list`. Утилита apt-get, в момент работы, просматривает одновременно все эти файлы.

Описания репозиториев заносятся в этот файл в следующем виде:

```
rpm [подпись] метод: путь база название
rpm-src [подпись] метод: путь база название
```

где:

- 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/vendors.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.

Пример синтаксиса, описывающего источники:

```
$ cat /etc/apt/sources.list.d/altsp.list
# update.altsp.su (IVK, Moscow)

# ALT Certified 8
#rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTLinux CF/branch/x86_64 classic
#rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTLinux c10f/branch/x86_64-i586 classic
#rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTLinux c10f/branch/noarch classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux c10f/branch/x86_64 classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux c10f/branch/x86_64-i586 classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux c10f/branch/noarch classic
```

Если первым символом идет символ комментария – строка считается простым текстом, а не описанием источника. У активной записи, в начале строки этот символ отсутствует.

Описание источника состоит из ключевых элементов:

- тип репозитория – применяется пакетная система rpm (все источники описывают rpm-репозитории);
- ключ подписи – пакеты в репозитории подписаны и могут быть проверены, если указать ключ. Списки доступных ключей хранятся в каталоге `/etc/apt/vendors.list` в файлах с расширением `.list`. Так же, есть файл `/etc/apt/vendors.list`. В примере использован ключ [cert8];
- адрес – адрес расположения репозитория. Репозитории доступы несколькими способами (ftp://, http:// и rsync://). После описания способа доступа прописан адрес;
- тип данных – репозиторий может содержать как исполняемые пакеты, так и пакеты для разработчиков или пакеты с данными общего характера. Тип x86_64-i586 показывает, что в данном репозитории находятся исполняемые программы и библиотеки, собранные для 32-х разрядных систем (32bit). При использовании дистрибутива для 64-х разрядных процессоров, тип содержимого будет x86_64. В общем случае, запись источника с выполняемыми программами и библиотеками дополняет источник с типом noarch. Этот источник предоставляет пакеты, идентичные для обеих платформ x86. Как правило, это данные, небинарные библиотеки к Perl, Python и т. п.;
- название – название репозитория.

Для добавления в `sources.list` репозитория на CD/DVD-носителе информации в APT предусмотрена специальная утилита – apt-cdrom. Чтобы добавить запись о репозитории на носителе, достаточно вставить его в привод для чтения (записи) CD (DVD)-носителей информации и выполнить следующую команду:

```
# apt-cdrom add
```

Если используется внешний CD-ROM, то в файле `/etc/fstab` требуется добавить строку:

```
/dev/sr0 /media/ALTLinux udf, iso9660 ro, noauto, user, utf8, nofail, comment=x-gvfs-show 0 0
```

Создать директорию для монтирования:

```
# mkdir /media/ALTLinux
```

Затем использовать команду добавления носителя:

```
# apt-cdrom add
```

После этого в `sources.list` появится запись о подключенном диске примерно такого вида:

```
rpm cdrom:[ ALT 8 SP Workstation]/ ALTLinux main
```

После того как список репозиториев в `sources.list` будет отредактирован, нужно обновить локальную базу данных APT о доступных пакетах, выполнив команду:

```
# apt-get update
```

В случае, если в `sources.list` присутствует репозиторий, содержимое которого может изменяться, то прежде чем работать с APT, нужно синхронизировать локальную базу данных с удаленным сервером:

```
# apt-get update
```

Так происходит с любым постоянно разрабатываемым репозиторием, например, появляются обновления по безопасности (updates).

Локальная база данных создается заново каждый раз, когда в репозитории происходит изменение: добавление, удаление или переименование пакета. Для репозиториев, находящихся на извлекаемых носителях информации и подключенных командой `apt-cdrom add`, синхронизация производится единожды в момент подключения.

При установке определенного 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 начнет 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.

17.1.2. Добавление репозиториев с использованием терминала

17.1.2.1. Скрипт apt-repo

Можно воспользоваться скриптом `apt-repo`, для этого потребуется запустить терминал и вводить команды в него. Для выполнения большинства команд требуются права администратора.

Просмотреть список активных репозиториев можно командой:

`apt-repo list`

Для добавления репозитория в список активных репозиториев используйте команду:

`apt-repo add` `репозиторий`

Для удаления или выключения репозитория используйте команду:

`apt-repo rm` `репозиторий`

Для обновления информации о репозиториях выполните команду:

`apt-repo update`

Для более подробной справки используйте команду:

`man apt-repo`

или `apt-repo --help`

17.1.2.2. Добавление репозиториев вручную

Отредактируйте в любом текстовом редакторе файлы из папки `/etc/apt/sources.list.d/`. Нужны права администратора для изменения этих файлов.

В файле `alt.list` может содержаться примерно такая информация:

```
# update.altsp.su (IVK, Moscow)
# ftp.altlinux.org (ALT Linux, Moscow)

# ALT Certified 9
#rpm  [cert9]  ftp://ftp.altlinux.org/pub/distributions/ALTLinux/cert9f1/branch
x86_64 classic
#rpm  [cert9]  ftp://ftp.altlinux.org/pub/distributions/ALTLinux/cert9f1/branch
x86_64-i586 classic
```

```
#rpm  [cert9]  ftp://ftp.altlinux.org/pub/distributions/ALTLinux/cert9f1/branch
noarch classic

rpm  [cert9]  http://ftp.altlinux.org/pub/distributions/ALTLinux/cert9f1/branch
x86_64 classic
rpm  [cert9]  http://ftp.altlinux.org/pub/distributions/ALTLinux/cert9f1/branch
x86_64-i586 classic
rpm   [cert9]   http://ftp.altlinux.org/pub/distributions/ALTLinux/c9f1/branch
noarch classic
```

По сути, каждая строчка соответствует некому репозиторию. Не активные репозитории – строки, начинающиеся с `#rpm`.

После добавления репозиториев обновите информацию о них: запустите терминал и выполните команду `apt-get update` или `apt-repo update`. Для выполнения этих команд нужны права администратора.

17.1.3. Центр управления системой

Для выбора репозитория в ЦУС меню «Программное обеспечение» → «Источники для установки ПО» в выпадающем списке нужно отметить один из предлагаемых вариантов и нажать на кнопку «Изменить». К предложенному списку можно самостоятельно добавить репозитории, нажав на кнопку «Дополнительно…».

После добавления репозиториев нужно обновить информацию о них в разделе ЦУС «Программное обеспечение» → «Установка программ» кнопка «Обновить».

Информация по установке ПО в ЦУС см. в п. 17.7.1.

17.1.4. Программа управления пакетами Synaptic

Программа Synaptic также может использоваться для выбора репозитория. Для указания конкретного репозитория в меню «Параметры» → «Репозитории» нужно отметить один из предлагаемых вариантов и нажать на кнопку «OK». К предложенному списку можно самостоятельно добавить репозитории, нажав на кнопку «Создать» и введя данные.

После добавления репозиториев нужно обновить информацию о них в программе управления пакетами Synaptic: «Правка» → «Получить сведения о пакетах».

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

17.2. Обновление информации о репозиториях в APT

Практически любое действие с системой APT начинается с обновления данных от активированных источников. Список источников нужно обновлять при поиске новой версии пакета, установке пакетов или обновлении установленных пакетов новыми версиями.

Обновление данных осуществляется командой:

```
# apt-get update
```

Программа загрузит данные с активированных источников в свой кеш. Пример:

```
# apt-get update
Get:1 http://ftp.altlinux.org x86_64 release [896B]
Get:2 http://ftp.altlinux.org x86_64-i586 release [555B]
Get:3 http://ftp.altlinux.org noarch release [690B]
Fetched 2141B in 0s (2476B/s)
Get:1 http://ftp.altlinux.org x86_64/classic pkglist [15.7MB]
Get:2 http://ftp.altlinux.org x86_64/classic release [135B]
Get:3 http://ftp.altlinux.org x86_64-i586/classic pkglist [11.7MB]
Get:4 http://ftp.altlinux.org x86_64-i586/classic release [140B]
Get:5 http://ftp.altlinux.org noarch/classic pkglist [3493kB]
Get:6 http://ftp.altlinux.org noarch/classic release [135B]
Fetched 30.9MB in 33s (910kB/s)
Reading Package Lists... Done
Building Dependency Tree... Done
```

После выполнения этой команды, apt обновит свой кеш новой информацией.

17.3. Поиск пакетов (apt-cache)

Утилита apt-cache предназначена для поиска программных пакетов в репозитории, и позволяет искать не только по имени пакета, но и по его описанию.

Команда `apt-cache search <подстрока>` позволяет найти все пакеты, в именах или описании которых присутствует указанная подстрока. Пример поиска может выглядеть следующим образом:

```
$ apt-cache search ^gimp
```

```
gimp - The GNU Image Manipulation Program
libgimp - GIMP libraries
libgimp-devel - GIMP plugin and extension development kit
gimp-help-en - English help files for the GIMP
gimp-help-ru - Russian help files for the GIMP
gimp-plugin-separateplus - Improved version of the CMYK Separation plug-in [...]
gimp-script-ISONoiseReduction - Gimp script for reducing sensor noise [...]
```

```
gimp-plugin-gutenprint - GIMP plug-in for gutenprint
gimp-plugin-ufraw - GIMP plugin for opening and converting RAW files
[...]
```

Символ «^» в поисковом выражении, указывает на то, что нужно найти совпадения только в начале строки (в данном случае – в начале имени пакета).

Для того чтобы подробнее узнать о каждом из найденных пакетов и прочитать его описание, можно воспользоваться командой `apt-cache show`, которая покажет информацию о пакете из репозитория:

```
$ apt-cache show gimp-help-ru
```

```
Package: gimp-help-ru
Section: Graphics
Installed Size: 37095561
Maintainer: Alexey Tourbin <at@altlinux.org>
Version: 2.6.1-alt2
Pre-Depends: rpmlib(PayloadIsLzma)
Provides: gimp-help-ru (= 2.6.1-alt2)
Obsoletes: gimp-help-common (< 2.6.1-alt2)
Architecture: noarch
Size: 28561160
MD5Sum: 0802d8f5ec1f78af6a4a19005af4e37d
Filename: gimp-help-ru-2.6.1-alt2.noarch.rpm
Description: Russian help files for the GIMP
Russian help files for the GIMP.
```

Команда apt-cache позволяет осуществлять поиск по русскому слову, однако в этом случае будут найдены только те пакеты, у которых есть описание на русском языке.

17.4. Управление установкой (инсталляцией) компонентов программного обеспечения

Установку пакетов может производить только администратор.

ВНИМАНИЕ!

Обновление пакетов выполняется при отсутствии нарушений целостности системы. Проверка целостности системы выполняется:

1) с помощью команды:
   `# integalert`
   При отсутствии изменений вывод команды: `integrity check OK`
2) или просмотром записей osec в системном журнале с помощью команды:
   `# journalctl | grep osec`
   При отсутствии изменений в записях журнала присутствует: `No changes[osec]`

ВНИМАНИЕ!

Если в системе инициализирована система контроля целостности ima-evm (должна быть инициализирована), то установка/обновление пакетов должно происходить посредством команды `updater-start` (см. п. 17.4.1) или штатным методом с использованием команды `integrity-applier` (см. п. 17.4.2).

Подробнее информацию о контроле целостности см. в документе «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03».

Если система контроля целостности не используется, то обновление пакетов нужно производить в следующем порядке:

1) если используется `control++` (черные/белые списки), нужно выключить черные/белые списки, выполнив сброс текущего режима (просмотреть установленный режим можно, выполнив команду `control++ list`, активный режим будет дополнительно отмечен `*`):

   ```
   # control++ --reset
   ```

2) установить пакеты/обновить систему при помощи apt-get;
3) включить установленный ранее режим черного/белого списка, выполнив команду (в зависимости от вывода в шаге 1)):

   ```
   # control++ blacklist
   ```

   или

   ```
   # control++ wl
   ```

4) выполнить команду:

   ```
   # integalert fix
   ```

17.4.1. Команда `updater-start`

Для того чтобы система сохранила все настройки безопасности для установки/обновления пакетов может использоваться команда `updater-start` (из пакета updater).

В результате запуска данной команды будет обновлена система и ядро системы, а также включена система контроля целостности ima-evm. Нужно дождаться завершения работы команды (система будет несколько раз перезагружена).

Примечание. Выполнение команды может занять довольно продолжительное время (время зависит от количества установленных в системе файлов).

Примечание. Если после отработки команды `updater-start` не запускается сервис auditd, нужно переименовать/удалить старый журнал аудита (`/var/log/audit/audit.log`) и потом выполнить команду `systemctl start auditd`:

```
# mv /var/log/audit/audit.log /var/log/audit/audit.log_old
# systemctl start auditd
```

Команда `updater-start` также запускает скрипты из `/etc/updater.d/*` с параметром `remove` перед установкой пакетов и их же с параметром `apply` после.

В частности, если используется `control++` со списками, то в `/etc/updater.d/` нужно положить скрипт, вызывающий `control++` и снимающий списки доустановки пакетов и устанавливающий их после установки.

Последовательность действий:

1) в каталоге `/etc/updater.d` создать файл (с произвольным названием) с содержимым:

```
#!/bin/bash
if [ "$1" == "remove" ] ;
 then
  control++ --reset
 fi
if [ "$1" == "apply" ] ;
 then
  control++ blacklist
 fi
```

2) сделать этот файл исполняемым:

```
# chmod +x /etc/updater.d/<имя_файла>
```

3) запустить обновление:

```
# updater-start
```

4) переименовать файл записи аудита `/var/log/audit/audit.log`:

```
# mv /var/log/audit/audit.log /var/log/audit/audit_old.log
```

5) выполнить запуск аудита:

```
# service auditd start
```

17.4.2. Команда `integrity-applier`

Для того чтобы система сохранила все настройки безопасности установку/обновление пакетов нужно производить в следующем порядке:

1) установить пакеты/обновить систему при помощи `apt-get`;
2) выполнить команду для инициализации контроля целостности:
   `# /usr/bin/integrity-applier`
3) дождаться завершения работы команды (система будет перезагружена четыре раза);
4) переименовать файл записи аудита `/var/log/audit/audit.log`:
   `# mv /var/log/audit/audit.log /var/log/audit/audit_old.log`
5) выполнить запуск аудита:
   `# service auditd start`

17.5. Установка или обновление пакета командой `apt`

Установка пакета с помощью APT выполняется командой:

```
# apt-get install имя_пакета
```

Перед установкой и обновлением пакетов нужно выполнить команду обновления индексов пакетов:

```
# apt-get update
```

Если пакет уже установлен и в подключенном репозитории нет обновлений для данного пакета, система сообщит об уже установленном пакете последней версии. Если в репозитории присутствует более новая версия или новое обновление – программа начнет процесс установки.

`apt-get` позволяет устанавливать в систему другие, пока еще не установленные пакеты, требуемые для работы. Он определяет, какие пакеты нужно установить, и устанавливает их, пользуясь всеми доступными репозиториями.

Установка пакета gimp командой `apt-get install gimp` приведет к следующему диалогу с APT:

```
# apt-get install gimp
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие дополнительные пакеты будут установлены:
icc-profiles libbabl libgegl libgimp libjavascriptcoregtk2 libopenraw
```

```
libspiro libwebkitgtk2 libwmf
Следующие НОВЫЕ пакеты будут установлены:
gimp icc-profiles libbabl libgegl libgimp libjavascriptcoregtk2
libopenraw libspiro libweb-kitgtk2 libwmf
0 будет обновлено, 10 новых установлено, 0 пакетов будет удалено и 0 не
будет обновлено.
Нужно получить 0B/24,6MB архивов.
После распаковки потребуется дополнительно 105MB дискового
пространства.
Продолжить? [Y/n] y
. . .
Получено 24,6MB за 0s (44,1MB/s).
Совершаем изменения...
Preparing...              ######################### [100%]
1: libbabl                ######################### [ 10%]
2: libwmf                 ######################### [ 20%]
3: libjavascriptcoregtk2  ######################### [ 30%]
4: libwebkitgtk2          ######################### [ 40%]
5: icc-profiles           ######################### [ 50%]
6: libspiro               ######################### [ 60%]
7: libopenraw             ######################### [ 70%]
8: libgegl                ######################### [ 80%]
9: libgimp                ######################### [ 90%]
10: gimp                  ######################### [100%]
Running /usr/lib/rpm/posttrans-filetriggers
Завершено.
```

Команда `apt-get install имя_пакета` используется и для обновления уже установленного пакета или группы пакетов. В этом случае `apt-get` дополнительно проверяет, не обновилась ли версия пакета в репозитории по сравнению с установленным в системе.

При помощи APT можно установить и отдельный бинарный rpm-пакет, не входящий ни в один из репозиториев. Для этого достаточно выполнить команду `apt-get install путь_к_файлу.rpm`. При этом APT проведет стандартную процедуру проверки зависимостей и конфликтов с уже установленными пакетами.

В результате операций с пакетами без использования APT может нарушиться целостность ОС Альт СП, и `apt-get` в таком случае откажется выполнять операции установки, удаления или обновления.

Для восстановления целостности ОС Альт СП нужно повторить операцию, задав опцию `-f`, заставляющую `apt-get` исправить нарушенные зависимости, удалить или заменить конфликтующие пакеты. Любые действия в этом режиме обязательно требуют подтверждения со стороны пользователя.

При установке пакетов происходит запись в системный журнал вида:

apt-get: имя-пакета installed

17.6. Удаление установленного пакета командой apt

Для удаления пакета используется команда apt-get remove <имя_пакета>. Удаление пакета с сохранением его файлов настройки производится при помощи следующей команды:

```
# apt-get remove <значимая_часть_имени_пакета>
```

В случае, если при этом нужно полностью очистить систему от всех компонент удаляемого пакета, то применяется команда:

```
# apt-get remove --purge <значимая_часть_имени_пакета>
```

Для того чтобы не нарушать целостность системы, будут удалены и все пакеты, зависящие от удаляемого.

В случае удаления с помощью apt-get базового компонента системы появится запрос на подтверждение операции:

```
# apt-get remove filesystem
Обработка файловых зависимостей... Завершено
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие пакеты будут УДАЛЕНЫ:
basesystem filesystem ppp sudo
Внимание: следующие базовые пакеты будут удалены:
В обычных условиях этого не должно было произойти, надеемся, вы точно
представляете, чего требуете!
basesystem filesystem (по причине basesystem)
0 пакетов будет обновлено, 0 будет добавлено новых, 4 будет
удалено(заменено) и 0 не будет обновлено.
Нужно получить 0B архивов. После распаковки 588kБ будет
освобождено.
Вы делаете нечто потенциально опасное!
Введите фразу 'Yes, do as I say!' чтобы продолжить.
```

Каждую ситуацию, в которой APT выдает такое сообщение, нужно рассматривать отдельно. Однако, вероятность того, что после выполнения этой команды система окажется неработоспособной, очень велика.

При удалении пакетов происходит запись в системный журнал вида:

apt-get: имя-пакета removed

17.7. Альтернативная установка дополнительного ПО

Для установки дополнительного ПО также можно использовать ЦУС либо программу управления пакетами Synaptic.

⚠ Нельзя использовать одновременно два менеджера пакетов, так как это может привести к их некорректной работе.

17.7.1. Установка дополнительного ПО в ЦУС

ЦУС содержит модуль установки пакетов: «Программное обеспечение» → «Установка программ». Для облегчения поиска доступные для установки программы (рис. 481) разделены на группы, выводимые в левой части окна программы. Справа расположен список самих программ с указанием их текущего состояния:

- зеленая метка – пакет уже установлен;
- белая – пакет не установлен.

Объяснение всех обозначений можно увидеть, отметив пункт «Показать статистику».

Для начала установки двойным щелчком мыши нужно отметить неустановленный пакет в правой половине окна и нажать на кнопку «Применить». При нужности менеджер пакетов попросит вставить установочный диск.

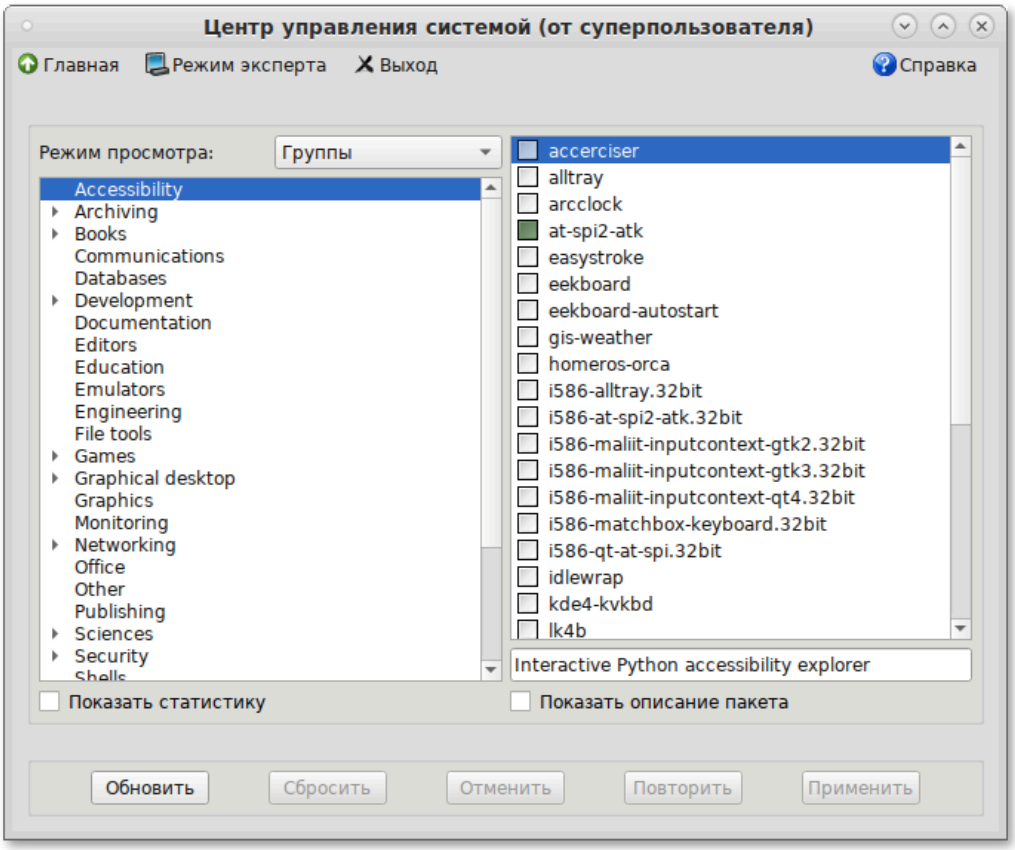


Рис. 481 – ЦУС Программное обеспечение

17.7.2. Программа управления пакетами Synaptic

Программа управления пакетами Synaptic находится на панели инструментов MATE «Меню» → «Приложения» → «Параметры» → «Прочие» → «Менеджер пакетов».

Для облегчения поиска доступные для установки программы (рис. 482) разделены на группы, выводимые в левой части окна программы. Справа расположен список самих программ с указанием их текущего состояния:

- зеленая метка – пакет уже установлен;
- белая – 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, нужно нажать на кнопку «Получить сведения» (или комбинацию клавиш <Ctrl>+<R>), для того чтобы скачать список самых последних версий ПО.

Для начала установки двойным щелчком мыши нужно отметить неустановленный пакет в правой половине окна и нажать на кнопку «Применить».

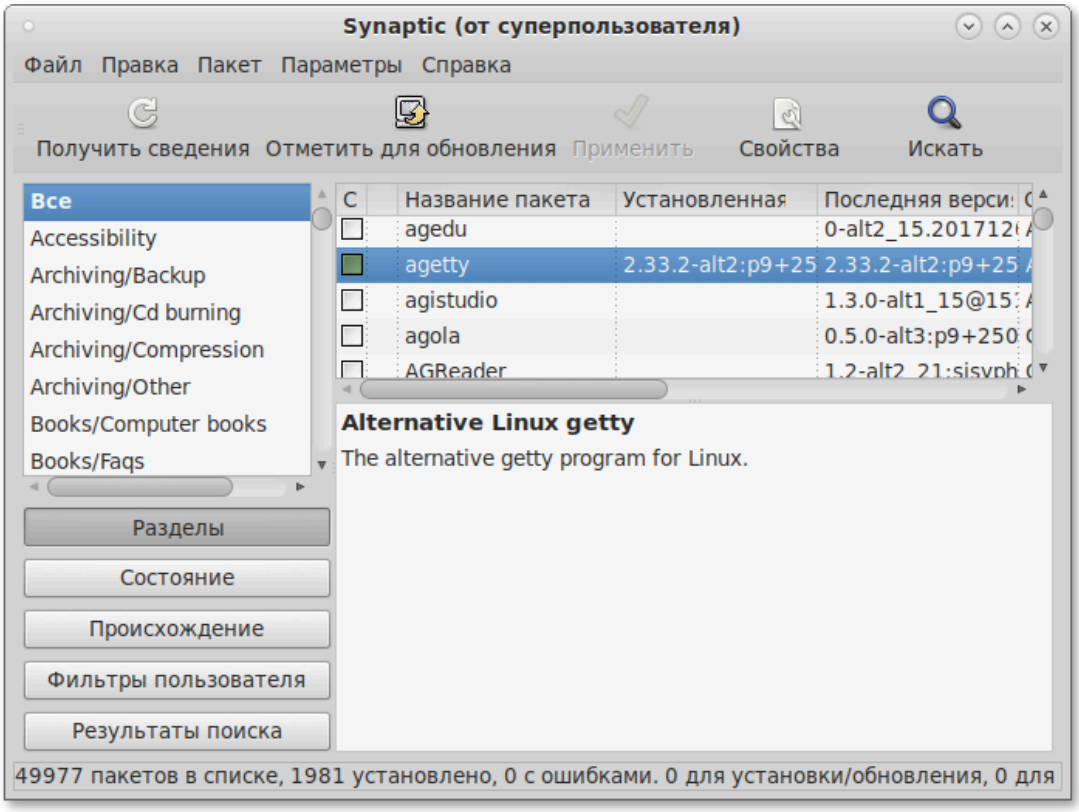


Рис. 482 – Программа управления пакетами Synaptic

17.8. Обновление всех установленных пакетов apt-get

Полное обновление всех установленных в системе пакетов производится при помощи команды:

```
# apt-get dist-upgrade
```

Примечание. Команда `apt-get dist-upgrade` обновит систему, но ядро ОС не будет обновлено (см. п. 17.10).

В случае обновления всего дистрибутива APT проведет сравнение системы с репозиторием и удалит устаревшие пакеты, установит новые версии присутствующих в системе пакетов, отследит ситуации с переименованиями пакетов или изменения зависимостей между старыми и новыми версиями программ. Все, что потребуется поставить (или удалить) дополнительно к уже имеющемуся в системе, будет указано в отчете `apt-get`, которым APT предварит само обновление.

17.9. Обновление всех установленных пакетов Synaptic

Synaptic поддерживает два варианта обновления системы:

1) умное обновление (рекомендуется)

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

2) стандартное обновление

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

По умолчанию Synaptic использует умное обновление. Для того чтобы изменить метод обновления системы, нужно открыть диалоговое окно «Параметры» (Параметры → Параметры) и на вкладке «Основные» в списке «Обновить систему» выбрать требуемый способ.

Для обновления системы:

1) нажать на кнопку «Получить сведения» (или комбинацию клавиш <Ctrl>+<R>), для того чтобы скачать список самых последних версий ПО;
2) нажать на кнопку «Отметить для обновления» (или комбинацию клавиш <Ctrl>+<G>), для того чтобы Synaptic отметил для обновления все пакеты;
3) нажать на кнопку «Применить».

17.10. Обновление ядра и модулей ядра

Для обновления ядра ОС нужно выполнить команду:

```
# update-kernel
```

Примечание. Если индексы сегодня еще не обновлялись перед выполнением команды `update-kernel` нужно выполнить команду `apt-get update`.

Если нужно обновить/установить другой тип ядра, нужно выполнить команду:

```
update-kernel -t <новый тип ядра>
```

где `<новый тип ядра>` – std-def, un-def и т.п.

Примечание. Ключ `-t` и тип ядра (std-def, un-def и т. п.) следует указывать только если нужно обновить ядро другого типа, так как по умолчанию обновляется текущий тип ядра. Узнать версию загруженного ядра можно командой:

```
$ uname –r
```

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.

Установка/обновление модулей ядра выполняется командой:

```
apt-get install kernel-modules-<модуль>-<тип ядра>
```

Например, для установки модуля VirtualBox, если текущий тип ядра std-def, следует выполнить команду:

```
# apt-get install kernel-modules-virtualbox-std-def
```

17.10.1. Графический инструмент обновления ядра

Модуль «Обновление ядра» (пакет alterator-update-kernel) 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.

17.10.1.1. Запуск

Модуль «Обновление ядра» доступен как в графическом интерфейсе ЦУС (п. 7.1.1)(раздел «Система» → «Обновление ядра) (рис. 483), так и в веб-интерфейсе (п. 7.1.2) `https://ip-address:8080` (рис. 484).

Центр управления системой (от суперпользователя)

Главная Режим эксперта Выход Справка

Релиз загруженного ядра: 5.4.68-std-def-alt1.1

Тип загруженного ядра (flavour): std-def

Версия загруженного ядра: 5.4.68

Ядро загружаемое по умолчанию: 5.4.68-std-def-alt1.1

Установленные ядра: std-def-5.4.68-alt1.1

Сделать ядро загружаемым по умолчанию

Замечание:

Чтобы сделать ядро загружаемым по умолчанию, выберите желаемую версию в списке выше и нажмите кнопку 'Сделать ядро загружаемым по умолчанию'. Перезагрузите компьютер, чтобы загрузится с выбранным ядром.

Удалить ядро

Установленные модули

drm-ancient
drm-nouveau
drm-radeon
drm
staging
v4l
bcmwl
e1000e
rtl8723de
rtl8821ce
virtualbox-addition-guest
virtualbox-addition
virtualbox-addition-video
virtualbox

Обновить ядро...

Удалить модуль

Замечание:

Чтобы установить модули или обновить ядро, нажмите кнопку 'Обновить ядро' (Чтобы установить модули нужна последняя версия ядра). Это потребует обновления списка пакетов доступных в репозитории и может занять некоторое время (зависит от скорости интернета).

Рис. 483

ОБНОВЛЕНИЕ ЯДРА

Настройка Справка Выйти

Релиз загруженного ядра: 5.4.68-std-def-alt1.1

Тип загруженного ядра (flavour): std-def

Версия загруженного ядра: 5.4.68

Ядро загружаемое по умолчанию: 5.4.68-std-def-alt1.1

Установленные ядра: std-def-5.4.68-alt1.1

Сделать ядро загружаемым по умолчанию

Notes

Чтобы сделать ядро загружаемым по умолчанию, выберите желаемую версию в списке выше и нажмите кнопку 'Сделать ядро загружаемым по умолчанию'. Перезагрузите компьютер, чтобы загрузится с выбранным ядром.

Удалить ядро

Обновить ядро...

Notes

Чтобы установить модули или обновить ядро, нажмите кнопку 'Обновить ядро' (Чтобы установить модули нужна последняя версия ядра). Это потребует обновления списка пакетов доступных в репозитории и может занять некоторое время (зависит от скорости интернета).

Установленные модули:

drm-ancient
drm-nouveau
drm-radeon
drm
staging
v4l
bcmwl
e1000e
rtl8723de
rtl8821ce

Удалить модуль

Рис. 484

17.10.1.2. Использование модуля

В главном окне модуля отображается ядро, загруженное по умолчанию, список установленных ядер (поле «Установленные ядра»), список установленных модулей ядра.

17.10.1.2.1. Установка/обновление ядра и установка модулей ядра

При обновлении ядра, обновляются и модули ядра, но исходя из списка установленных для текущего ядра пакетов.

Примечание. Для установки модулей требуется последняя версия ядра.

Для того, чтобы обновить ядро или установить модули ядра, нужно нажать кнопку «Обновить ядро…».

Примечание. При нажатии кнопки «Обновить ядро…» локальная база данных пакетов будет синхронизирована с удаленным репозиторием, это может занять некоторое время.

В открывшемся окне будет показано доступное к установке ядро (рис. 485).

В выпадающем списке можно выбрать тип ядра. В окне «Доступные модули» отмечаются модули, которые будут установлены.

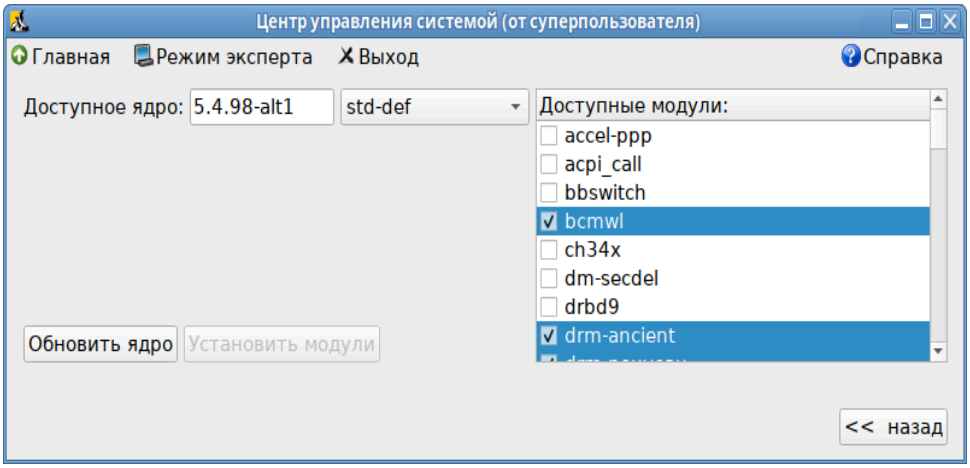


Рис. 485

Чтобы обновить ядро, нужно нажать кнопку «Обновить ядро». Откроется окно, в котором следует нажать кнопку «Да» для того, чтобы обновить ядро, или «Нет», чтобы отказаться от данного действия.

Установленное ядро станет загружаемым по умолчанию.

Если ядро не требует обновления, в окне «Доступные модули» можно отметить модули ядра к установке, и нажать кнопку «Установить модули» (рис. 486).

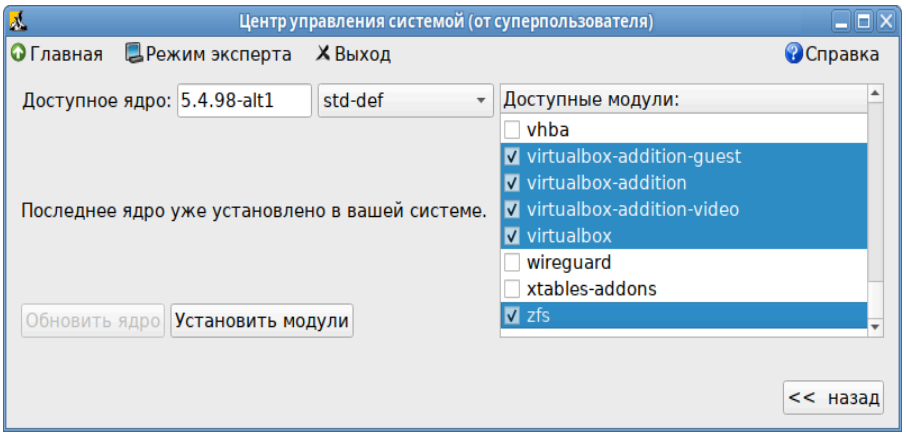


Рис. 486

Новое ядро загрузится только после перезагрузки системы.

17.10.1.2.2. Сделать ядро загружаемым по умолчанию

В дистрибутивах ALT Linux 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» (рис. 487).

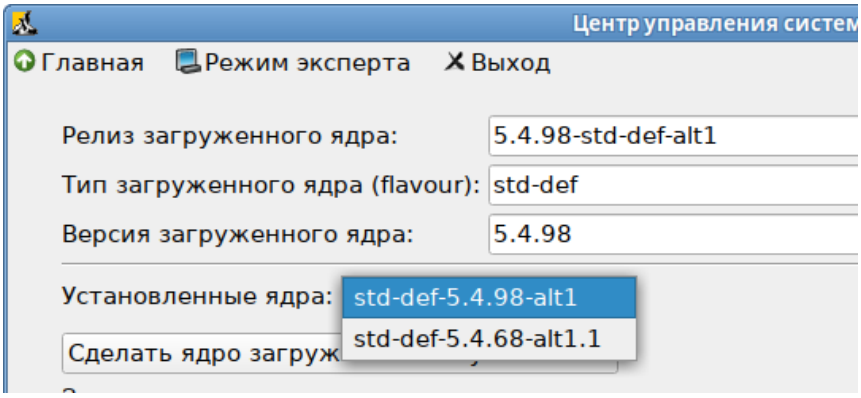


Рис. 487

17.10.1.2.3. Удаление ядра

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».

17.10.1.2.4. Удаление модулей ядра

При установке операционной системы автоматически устанавливаются модули для различных аппаратных средств, включая различные модели видеокарт. Для уменьшения нагрузки при обновлениях неиспользуемые модули можно удалить. Для этого в списке «Установленные ядра» выберите ядро, модули которого хотите удалить, затем в списке «Установленные модули» выделите удаляемые модули и нажмите кнопку «Удалить модуль» (рис. 488).

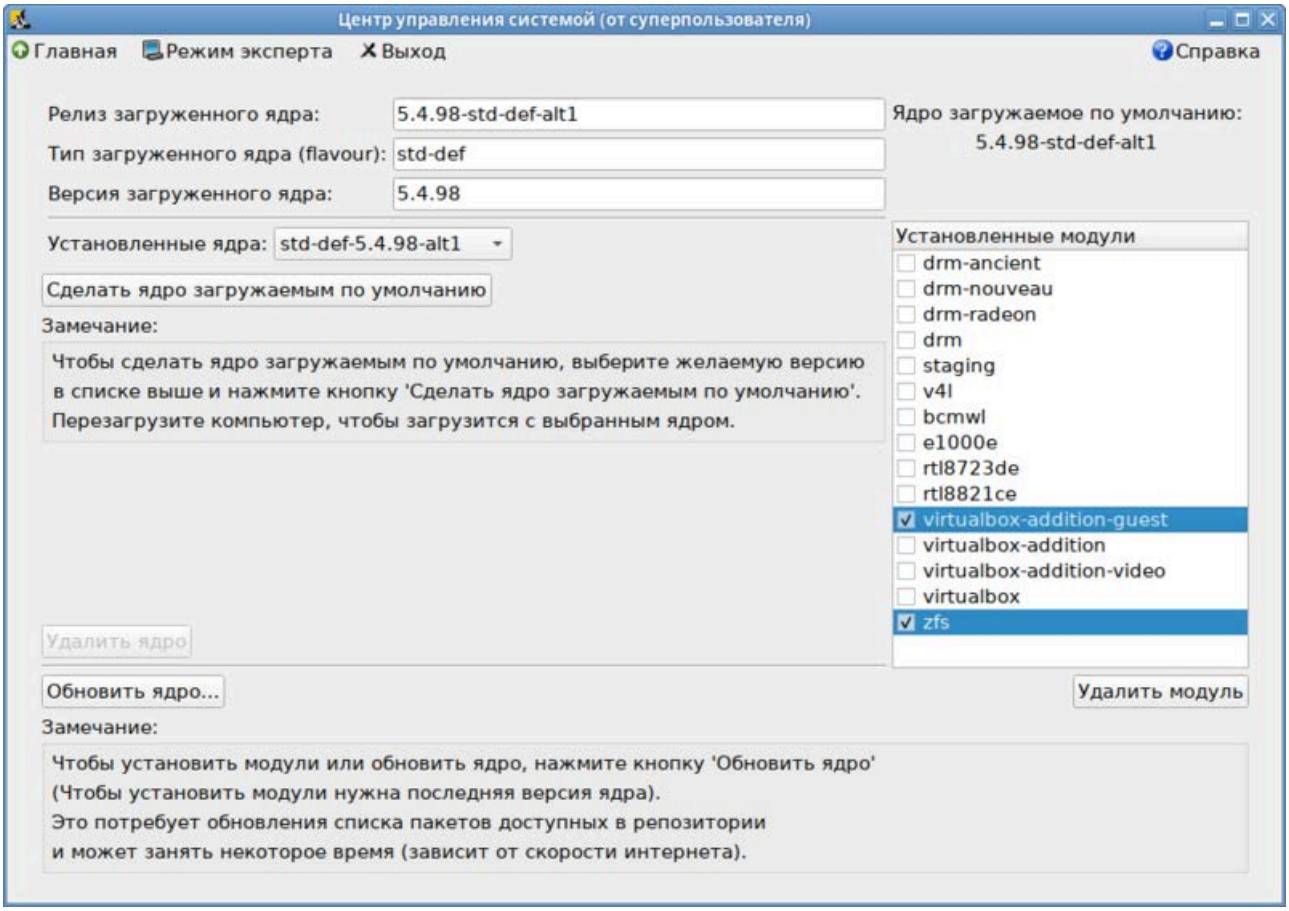


Рис. 488

17.10.2. Удаление старых версий ядра

После успешной загрузки на обновленном ядре можно удалить старое, выполнив команду:

```
# remove-old-kernels
```

17.11. Обновление изолированного окружения (chrooted environment)

Команда `update_chrooted --list` выводит список всех типов модулей для `update_chrooted`, которые установлены в системе:

```
# update_chrooted --list
List of registered types: all conf lib
```

С помощью команды `update_chrooted <имя_типа>` можно выполнить все модули указанного типа.

После изменения общесистемных конфигурационных файлов типа `/etc/resolv.conf`, для того чтобы синхронизировать эти изменения во всех многочисленных `chrooted environments` следует выполнить команду:

```
# update_chrooted conf
```

После изменения системных библиотек следует выполнить команду:

```
# update_chrooted lib
```

Для синхронизации изменений конфигурационных файлов и системных библиотек следует выполнить команду:

```
# update_chrooted all
```

17.12. Проверка подлинности пакетов

Подлинность пакетов при обновлении обеспечивается средствами кодирования, подтверждающих как целостность самих пакетов, так и целостность индексов, описывающих репозитории.

Ключевая информация для проверки подлинности распространяется вместе с дистрибутивом на сертифицированном носителе и защищена от потенциальной подмены при передаче по каналам связи.

Проверить подлинность и целостность пакета можно командой:

```
# rpm -vK имя_пакета
```

17.13. Получение уведомлений о выходе обновлений

Информирование потребителей о мерах, направленных на нейтрализацию выявленных уязвимостей ПИ ОС Альт СП, и выпускаемых обновлениях выполняется путем публикации информации на официальном сайте предприятия-разработчика (`https://altsp.su`) или по электронной почте.

17.14. Обновление систем, не имеющих выхода в Интернет

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

Сервер обновлений – технология, позволяющая настроить автоматическое обновление ПО, установленного на клиентских машинах (рабочих местах), работающих под управлением ОС Альт СП Рабочая станция.

Модуль ЦУС «Сервер обновлений» (пакет alterator-mirror) из раздела «Серверы» предназначен для зеркалирования репозиториев и публикации их для обновлений рабочих станций и серверов. Репозиторий выбирается в соответствии с выбранной веткой для соответствующего дистрибутива (актуальную информацию см. в документе «Формуляр. ЛКНВ.11100-01 30 01» в разделе сведений об изменениях).

Для добавления диска в качестве источника установки следует воспользоваться командой `apt-cdrom add`.

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

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

где `/media/disk/localrepo` – папка-хранилище локального репозитория.

На странице настройки сервера обновлений ЦУС (рис. 489) можно выбрать, как часто выполнять закачку пакетов, можно выставить время, когда начинать зеркалирование (рис. 490).

Так же можно выбрать репозитории, локальные срезы которых нужны. Далее при нажатии на название репозитория, появляются настройки этого репозитория (рис. 491). Нужно выбрать источник (сайт, откуда будет скачиваться репозиторий), архитектуру процессора (если их несколько, то стоит выбрать соответствующие).

Настройка локального репозитория заканчивается нажатием на кнопку «Применить».

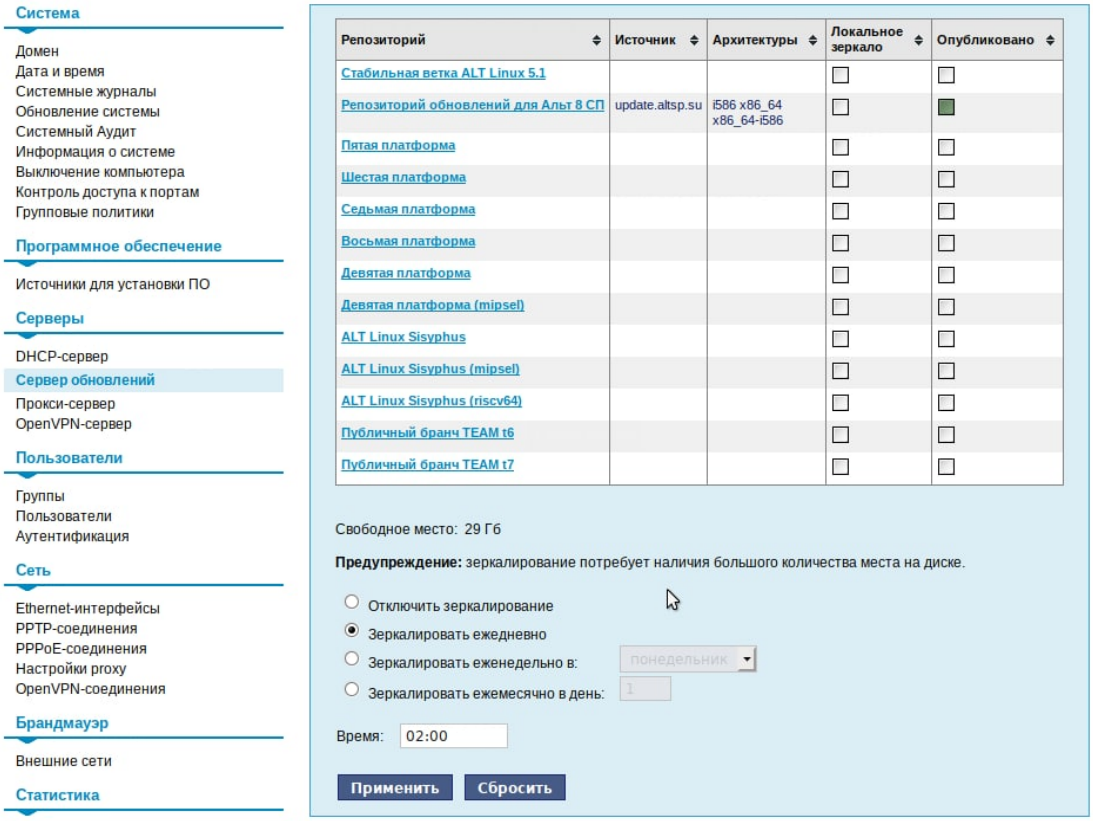


Рис. 489 – Меню «Сервер обновлений»

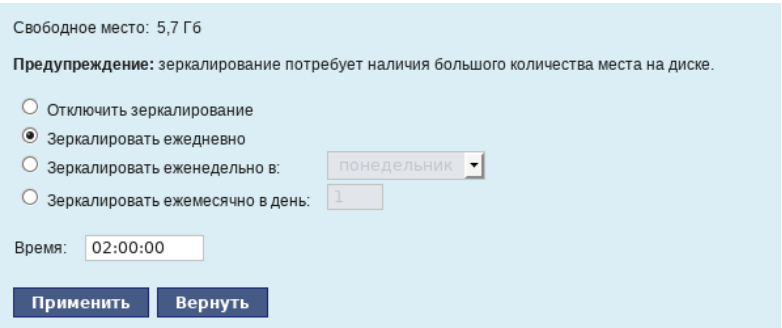


Рис. 490 – Настройка расписания

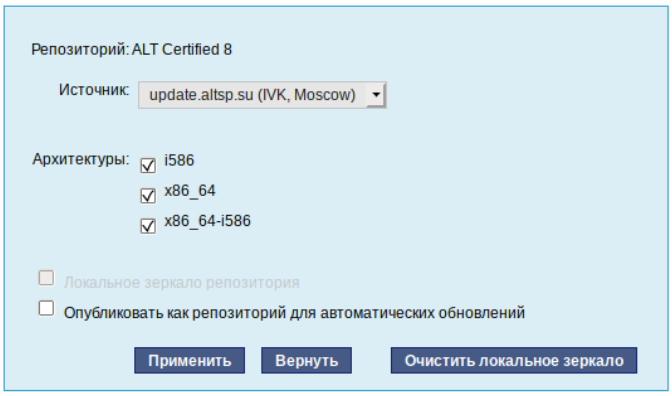


Рис. 491 – Настройки репозитория

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

- локальное зеркало репозитория – в этом режиме на сервере создается копия удаленного репозитория, доступная клиентским машинам по протоколу FTP. Загрузка ПО клиентскими машинами производится с локального сервера. Наличие на локальном сервере зеркала репозитория при большом количестве машин в сети позволяет существенно сэкономить на трафике;
- публикация репозитория – в этом случае реального зеркалирования (загрузки пакетов) не происходит. Публикуется URL внешнего сервера, содержащего репозиторий. Такая публикация позволяет клиентским машинам автоматически настроить свои менеджеры пакетов на использование внешнего сервера. Загрузка ПО клиентским машинам производится с внешнего сервера.

Здесь также можно указать имена каталогов и файлов, которые будут исключены из синхронизации, что позволит уменьшить размер скачиваемых файлов и занимаемое репозиторием место на диске. 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.

Настройка локального репозитория заканчивается нажатием на кнопку «Применить».

Далее нужно отредактировать файл `/etc/httpd2/conf/include/Directory_html_default.conf`, изменив следующие строки:

```
Options Indexes FollowSymLinks MultiViews
AllowOverride None
Order allow,deny
allow from all
```

Эти настройки разрешают серверу apache обрабатывать символические ссылки. Перезапустите apache:

```
# service httpd2 restart
```

Осуществите переход в папку веб-сервера:

```
cd /var/www/html
```

Создайте здесь символическую ссылку на репозиторий:

```
ln -s /srv/public/mirror mirror
```

На клиентских машинах нужно настроить репозитории. Для этого нужно запустить Synaptic, в параметрах выбрать репозитории. И далее настроить URL доступных репозиториев:

```
http://<IP-адрес>/mirror/
```

Так же со стороны клиентских машин на них нужно настроить модуль ЦУС «Обновление системы» (пакет alterator-updates) в соответствии с п. 8.17.4.

17.15. Единая команда управления пакетами (`epm`)

epm – единая команда управления пакетами. Основное предназначение: унифицировать управление пакетами в дистрибутивах с разными пакетными менеджерами. epm упрощает процедуру управления пакетами, особенно полезна для тех, кто работает с множеством дистрибутивов, может использоваться в скриптах и установщиках, сервисных программах, в повседневном администрировании различных систем. Кроме того, в epm добавлены типовые операции, которые, например, в случае использования apt, потребовали бы ввода более одной команды.

Установка выполняется командой:

```
# apt-get install eepm
```

Включает в себя следующую функциональность:

- управление пакетами (установка – удаление – поиск);
- управление репозиториями (добавление – удаление – обновление – список);
- управление системными сервисами (включение – выключение – список).

Список поддерживаемых пакетных менеджеров: rpm, deb, tgz, tbz, tbz2, apk, pkg.gz.

Список команд `epm –help` представлен в таблица 71.

Таблица 71 – Список команд `epm –help`

Описание операции	Команда epm	Команда ОС Альт СП
Установка пакета по названию в систему	`epm -i (package)`	`apt-get install (package)`
Установка файла пакета в систему	`epm -i (package file)`	`apt-get install (package file)`
Удаление пакета из системы	`epm -e (package)`	`apt-get remove (package)`
Поиск пакета в репозитории	`epm -s (text)`	`apt-cache search (text)`
Проверка наличия пакета в системе	`epm -q (package)`	`rpm -qa (pipe) grep (package)`
Список установленных пакетов	`epm -qa`	`rpm -qa`
Поиск по названиям установленных пакетов	`epm -qp <word>`	`grep <word>`
Принадлежность файла к (установленному) пакету	`epm -qf (file)`	`rpm -qf (file)`
Поиск, в каком пакете есть указанный файл	`epm -sf <file>`	
Список файлов в (установленном) пакете	`epm -ql (package)`	`rpm -ql (package)`
Вывести информацию о пакете	`epm -qi (package)`	`apt-cache show (package)`
Обновить дистрибутив	`epm upgrade`	`apt-get dist-upgrade`

Примеры:

`# epms name subtext` – выполняет `epms name | grep subtest`

`# epms name ^subtext` – выполняет `epms name | grep -v subtest`

`# epms "name1 name2"` – выполняет поиск именно такого сочетания.

18. ОГРАНИЧЕНИЕ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ

18.1. Определение параметров уничтожения данных

Для пользователей нужно запретить использование команды `rm`. Для этого нужно выполнить команду:

```
# chmod o-x /bin/rm
```

Команда `srm` предназначена для удаления данных без возможности их восстановления. `srm` выполняет безопасную перезапись/переименование/удаление целевого файла(ов). Использование команды srm аналогично использованию `rm`.

Команда `shred` переписывает несколько раз файл, скрывая его содержимое, для того, чтобы сделать более трудоемким процесс восстановления данных даже в случае использования специального оборудования для восстановления:

```
shred [ОПЦИЯ] ФАЙЛ [...]
```

Стандартные опции для запуска команды:

1) `-f`, `--force` – изменить права для разрешения записи, если нужно;
2) `-n`, `--iterations=N` – переписать N раз вместо указанных (25) по умолчанию;
3) `-s`, `--size=N` – очистить N байт (возможны суффиксы вида K, M, G);
4) `-u`, `--remove` – обрезать и удалить файл после перезаписи;
5) `-v`, `--verbose` – показывать индикатор прогресса;
6) `-x`, `--exact` – не округлять размеры файлов до следующего целого блока;
7) `-z`, `--zero` – перезаписать в конце с нулями, чтобы скрыть перемешивание.

Если файл задан как -, перемешивать стандартный вывод.

Удаляет `ФАЙЛЫ` если указан `--remove (-u)`. По умолчанию файлы не удаляются, так как часто обрабатываются файлы-устройства вроде `/dev/hda`, а такие файлы нельзя удалять.

Команда `sfill` выполняет безопасную перезапись свободного пространства на разделе, в котором находится указанная директория и всех свободных индексных дескрипторов (inode) указанного каталога. Процесс удаления данных выглядит следующим образом:

- 1 проход с 0xff (все данные затираются значением 0xff);
- 5 случайных проходов с `/dev/urandom` используя RNG;
- 27 проходов со значениями Питера Гутмана;
- обрезает файл.

Стандартные опции для запуска команды:

1) `-d` – игнорировать специальные файлы "." и "..";

2) `-f` – быстрый (и небезопасный режим);

3) `-l` – выполнить только два прохода, с 0xff и случайное заполнение;

4) `-l -l` – выполнить только случайное заполнение (один проход);

5) `-r` – выполнить в рекурсивном режиме, удалить все подкаталоги;

6) `-v` – подробный режим;

7) `-z` – последний проход заполняет нулями, а не случайными данными.

Пользователю запрещено определять параметры уничтожения данных. Эти параметры определяет администратор.

Для определения параметров уничтожения данных в системе созданы скрипты с предопределенными настройками уничтожения данных, для их переопределения администратор должен внести правки в файл `/etc/sysconfig/s_rm`.

П р и м е ч а н и е . Должен быть установлен пакет altsp-test-scripts.

Пользователи для удаления данных должны использовать команды `s_rm` и `s_fill`.

18.2. Модуль AltHa

AltHa – это модуль безопасности Linux, может использоваться для настройки блокировки возможности удаления открытого файла.

Модуль в настоящее время имеет три варианта защиты пользовательского пространства:

- игнорировать биты SUID в двоичных файлах (возможны исключения);
- запретить запуск выбранных интерпретаторов в интерактивном режиме;
- отключить возможность удаления открытых файлов в выбранных каталогах.

Для включения модуля AltHa нужно передать ядру параметр `altha=1`: для этого в файле `/etc/sysconfig/grub2` в строке `GRUB_CMDLINE_LINUX_DEFAULT` следует добавить опцию: `altha=1`. Например:

```
# vim /etc/sysconfig/grub2
...
GRUB_CMDLINE_LINUX_DEFAULT='vga=0x314 quiet resume=/dev/disk/by-uuid/187504b7-7f78-486d-b383-1b638370d3eb panic=30 splash altha=1'
```

Обновить загрузчик, выполнив команду:

```
# update-grub
```

Перезагрузить систему.

18.2.1. Запрет бита исполнения (SUID)

При включенном подмодуле altha.nosuid биты SUID во всех двоичных файлах, кроме явно перечисленных, игнорируются в масштабе всей системы.

18.2.1.1. Отключение влияния бита SUID на привилегии порождаемого процесса в консоли

Для включения запрета бита исполнения следует установить значение переменной `kernel.altha.nosuid.enabled` равным 1:

```
# sysctl -w kernel.altha.nosuid.enabled=1
```

И добавить, если это нужно, исключения (список включенных двоичных файлов SUID, разделенных двоеточиями), например:

```
# sysctl -w kernel.altha.nosuid.exceptions="/bin/su:/usr/libexec/hasher-priv/hasher-priv"
```

Проверка состояния режима запрета бита исполнения выполняется командой:

```
# sysctl -n kernel.altha.nosuid.enabled
1
```

Результат выполнения команды:

- 1 – режим включен;

- 0 – режим выключен.

18.2.2. Блокировка интерпретаторов (запрет запуска скриптов)

При включении блокировки интерпретаторов блокируется несанкционированное использование интерпретатора для выполнения кода напрямую из командной строки.

18.2.2.1. Блокировка интерпретаторов в консоли

Для включения режима блокировки интерпретаторов следует установить значение переменной `kernel.altha.rstrscript.enabled` равным 1:

```
# sysctl -w kernel.altha.rstrscript.enabled=1
```

Переменная `kernel.altha.rstrscript.interpreters` должна содержать разделенный двоеточиями список ограниченных интерпретаторов. Для изменения значения переменной `kernel.altha.rstrscript.interpreters` выполнить команду:

```
# sysctl -w kernel.altha.rstrscript.interpreters= "/usr/bin/python:/usr/bin/python3:/usr/bin/perl:/usr/bin/tclsh"
```

Примечание. В этой конфигурации все скрипты, начинающиеся с `#!/usr/bin/env python`, будут заблокированы.

Проверка состояния режима блокировки интерпретаторов выполняется командой:

```
# sysctl -n kernel.altha.rstrscript.enabled
1
```

Результат выполнения команды:

- 1 – режим включен;

- 0 – режим выключен.

Для получения списка заблокированных интерпретаторов выполнить команду:

```
# sysctl -n kernel.altha.rstrscript.interpreters
/usr/bin/python:/usr/bin/python3:/usr/bin/perl:/usr/bin/tclsh
```

18.2.3. Отключение возможности удаления открытых файлов

18.2.3.1. Отключение возможности удаления открытых файлов в консоли

Для отключения возможности удаления открытых файлов следует установить значение переменной `kernel.altha.olock.enabled` равным 1:

```
# sysctl -w kernel.altha.olock.enabled=1
```

Переменная `kernel.altha.olock.dirs` должна содержать разделенный двоеточиями список каталогов, например: `/var/lib/something:/tmp/something`. Для изменения значения переменной `kernel.altha.olock.dirs` следует выполнить команду:

```
# sysctl -w kernel.altha.olock.dirs="/var/lib/something:/tmp/something"
```

Проверка состояния режима выполняется командой:

```
# sysctl -n kernel.altha.olock.enabled
1
```

Результат выполнения команды:

- 1 – режим включен;
- 0 – режим выключен.

При нужности устанавливать эти переменные автоматически при каждой загрузке ОС, нужно добавить их в файл `/etc/sysctl.conf`. После редактирования `sysctl.conf` применить изменения, без перезагрузки ОС, можно выполнив команду:

```
# sysctl -p
```

19. КОНТРОЛЬНЫЕ ХАРАКТЕРИСТИКИ РАЗВЕРНУТОЙ ОС АЛЬТ СП

После установки нужно проверить корректность развертывания ОС Альт СП путем подсчета и сличения контрольных характеристик установленных файлов. Подробнее см. в документе «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03».

В качестве контрольной характеристики файла выступает контрольная сумма.

Подробнее об интегральных контрольных суммах ПИ, расположении пофайловых отчетов подсчета, алгоритме подсчета контрольных сумм приведено в документе «Формуляр. ЛКНВ.11100-01 30 01».

В случае изменения контрольных сумм после применения критических обновлений ОС Альт СП перечень измененных файлов и новые контрольные суммы нужно внести в раздел «Особые отметки» документа «Формуляр. ЛКНВ.11100-01 30 01».

20. ОСНОВЫ АДМИНИСТРИРОВАНИЯ LINUX

20.1. Общие принципы работы ОС

20.1.1. Процессы и файлы

ОС Альт СП 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.

20.1.1.1. 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 нужности интерактивной работы с пользователем (в общем случае) процесс будет «остановлен» ядром, и работа его продолжается только после переведения его в «нормальный» режим работы.

20.1.1.2. 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 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 `./`.

20.1.1.3. 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 ее 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, которые нужны 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 – каталог для регистрации сообщений, системный журнал;
- /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 и т. д.).

20.1.1.4. 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 имен 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 нужна пользователям или некоторым программам, но не имеет значение для shell.

20.1.1.5. Имена дисков и разделов

Все физические устройства компьютера отображаются в каталог `/dev` файловой системы дистрибутива. Диски (в том числе IDE/SATA/SCSI/SAS жесткие диски, USB-диски) имеют имена:

- `/dev/sda` – первый диск;
- `/dev/sdb` – второй диск;
- и т. д.

Диски обозначаются `/dev/sdX`, 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.

20.1.1.6. Разделы 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 подкачки (swap). Размер последнего, как правило, составляет от однократной до двукратной величины оперативной памяти компьютера. Если на диске много свободного места, то можно создать отдельные разделы для каталогов `/usr`, `/home`, `/var`.

20.1.2. Командные оболочки (интерпретаторы)

Для управления ОС используются командные интерпретаторы (shell).

После входа в систему, 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 распространенная оболочка под Linux, которая ведет историю команд и предоставляет возможность их редактирования.

20.1.3. Командная оболочка Bash

В Bash имеется несколько приемов для работы со строкой команд. Например, можно использовать следующие сочетания клавиш:

- <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 нужно 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 нужно 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, нужно использовать команду (в примере запускается команда `prog`):

```
./prog
```

20.1.4. Стыкование команд в системе Linux

20.1.4.1. 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, программа `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, программа `cat` немедленно возвращает на экран. При вводе информации со стандартного ввода конец текста сигнализируется вводом специальной комбинации клавиш, как правило, <Ctrl>+<D>. Сокращенное название сигнала конца текста – EOT (end of text).

20.1.4.2. Перенаправление ввода и вывода

При нужности 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. Программа `sort` является простым фильтром – она сортирует входные данные и посылает результат на стандартный вывод. Совсем простым фильтром является программа `cat` – она ничего не делает с входными данными, а просто пересылает их на выход.

20.1.4.3. 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 нужно 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.

20.1.4.4. 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.

20.2. Режим суперпользователя

20.2.1. Пользователи ОС

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 учетных записей Linux всегда есть учетная 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 учетной записи – одна из самых больших драгоценностей системы. Именно с ее помощью системные администраторы выполняют самую ответственную работу.

20.2.2. Назначение режима суперпользователя

Системные утилиты, например, такие, как ЦУС или программа управления пакетами Synaptic, настройки КСЗ ОС требуют для своей работы привилегий суперпользователя, потому что они вносят изменения в системные файлы. При их запуске выводится запрос/диалоговое окно с запросом пароля системного администратора.

20.2.3. Получение прав суперпользователя

Существует два различных способа получить права суперпользователя.

Первый – это зарегистрироваться в системе под именем root в командной строке.

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 определенное административное действие.

В некоторых случаях удобнее использовать не `su`, а утилиту `sudo`, которая позволяет выполнять только заранее заданные команды.

Примечание. Для того чтобы воспользоваться командами `su` и `sudo`, нужно быть членом группы wheel. Пользователь, созданный при установке системы, по умолчанию уже включен в эту группу.

В дистрибутивах ОС Альт СП 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.

20.2.4. Переход в режим суперпользователя

Для перехода в режим суперпользователя наберите в терминале команду `su -`.

Синтаксис:

```
su [-] [name [arg…]]
```

Чтобы вернуться к правам пользователя, нужно ввести следующую команду:

```
exit
```

Если воспользоваться командой `su` без ключа, то происходит вызов командного интерпретатора с правами root. При этом значение переменных окружения, в частности `$PATH`, остается таким же, как у пользователя: в переменной `$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.

20.3. Управление пользователями

Подробнее о средствах управления учетными записями пользователей смотрите в документе «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03».

20.4. Система инициализации systemd и sysvinit

20.4.1. Запуск операционной системы

20.4.1.1. Запуск системы

Алгоритм запуска компьютера:

1) BIOS (БСВВ) компьютера;
2) загрузчик системы (например, LILO, GRUB или другой). В загрузчике можно задать параметры запуска системы (см. п. 6.1);
3) загрузка ядра Linux;
4) запускается на выполнение первый процесс в системе – init.

Ядром запускается самая первая программа в системе init. Ее задачей является запуск новых процессов и повторный запуск завершившихся. Можно просмотреть, где расположился init в иерархии процессов системы, введите команду: `pstree`.

От конфигурации init зависит, какая система инициализации будет использована.

20.4.1.2. 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 ОС Альт СП используется sysvinit (от System V init).

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.

20.4.2. Примеры команд управления службами, журнал в systemd

Обратите внимание, что команды `service` и `chkconfig` продолжат работать в systemd практически без изменений. Тем не менее, в таблице 72 показано как выполнить те же действия с помощью встроенных утилит systemctl.

Т а б л и ц а 72 – 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`	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.

Окончание таблицы 72

Команды sysvinit	Команды systemd	Примечания
`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 создается новая служба или модифицируется любая конфигурация.

20.4.3. 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.

Можно запускать `journalctl` с разными ключами (таблица 73).

Для ознакомления с прочими возможностями, читайте руководство по journalctl. Для этого используйте команду `man journalctl`.

Т а б л и ц а 73 – Примеры запуска journalctl

Команда	Описание
`journalctl -b`	Покажет сообщения только с текущей загрузки.
`journalctl -f`	Покажет только последние сообщения.
`journalctl --since "2015-07-20 17:15:00"`	Просмотреть все сообщения начиная с 20 июля 2015 года 17:15.
`journalctl –k`	Просмотр сообщений ядра.
`journalctl /usr/lib/systemd/system`	Все сообщение конкретной утилиты systemd.
`journalctl _PID=1`	Просмотр сообщения определенного процесса, покажет сообщения первого процесса (init).
`journalctl -u netcfg`	Все сообщения конкретного приложения или службы.
`journalctl _UID=33`	Все сообщения процессов, запущенных от имени конкретного пользователя.

21. СООБЩЕНИЯ АДМИНИСТРАТОРУ

При возникновении проблем в процессе функционирования ОС Альт СП появляются диагностические сообщения трех типов: информационные, предупреждающие и сообщения об ошибках.

Администратор должен проанализировать диагностические сообщения и принять меры по устранению появившихся проблем.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД – база данных;

БСВВ – базовая система ввода-вывода;

ЕПП – единое пользовательское пространство;

КСЗ – комплекс средств защиты;

НЖМД – накопитель на жестких магнитных дисках;

ОС – операционная система;

ПИ – программное изделие;

ПО – программное обеспечение;

ПЭВМ – персональная электронная вычислительная машина;

СВТ – средство вычислительной техники;

СУБД – система управления базами данных;

УЦ – удостоверяющий центр;

ФС – файловая система;

ЦУС – центр управления системой;

AD – Active Directory;

DC – Domain Controller;

PDC – Primary Domain Controller.

Лист регистрации изменений									
Номера листов (страниц)					*Всего листов (страниц) в докум.*	*№ докумен-та*	*Входящий № сопро-водитель-ного докум. и дата*	*Подп.*	*Да-та*
Изм.	*изменен-ных*	*заменен-ных*	*новых*	*аннули-рован-ных*					