ОПЕРАЦИОННАЯ СИСТЕМА АЛЬТ РАБОЧАЯ СТАНЦИЯ 10.4

Описание функциональных характеристик

Содержание

1 ОБЩИЕ СВЕДЕНИЯ ОБ ОС АЛЬТ РАБОЧАЯ СТАНЦИЯ 10.4

1.1 Краткое описание возможностей

Операционная система «Альт Рабочая станция» (далее – ОС «Альт Рабочая станция»), представляет собой совокупность интегрированных программ, созданных на основе ОС «Linux», и обеспечивает обработку, хранение и передачу информации в круглосуточном режиме эксплуатации.

ОС «Альт Рабочая станция» обладает следующими функциональными характеристиками:

- обеспечивает возможность обработки, хранения и передачи информации;
- 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 поддержку виртуальной памяти;
- обеспечивает поддержку запуска виртуальных машин;
- обеспечивает сетевую обработку данных, в том числе разграничение доступа к сетевым пакетам.

ОС «Альт Рабочая станция» – это комплекс необходимых программ для эффективного выполнения типовых задач: электронная почта, работа с документами и презентациями, прослушивание аудиофайлов и просмотр видео, работа в сети Интернет и многое другое.

Основные преимущества ОС «Альт Рабочая станция»:

- русскоязычный пользовательский интерфейс;
- графическая рабочая среда MATE;
- выбор разворачиваемых решений (например, виртуализация, мультимедиа приложения) на этапе установки;
- возможность как развернуть, так и использовать только определённые службы без Alterator;
- широкий выбор различных программ для профессиональной и домашней работы в сети Интернет, с документами, со сложной графикой и анимацией, для обработки звука и видео, разработки программного обеспечения и образования;
- подробная иллюстрированная документация.

1.2 Структура программных средств

ОС «Альт Рабочая станция» состоит из набора компонентов, предназначенных для реализации функциональных задач, необходимых пользователям (должностным лицам для выполнения

определённых должностных инструкций, повседневных действий), и поставляется в виде дистрибутива и комплекта эксплуатационной документации.

В структуре ОС «Альт Рабочая станция» можно выделить следующие функциональные элементы:

- ядро ОС;
- системные библиотеки;
- утилиты и драйверы;
- средства обеспечения информационной безопасности;
- системные приложения;
- средства обеспечения облачных и распределенных вычислений, средства виртуализации и системы хранения данных;
- системы мониторинга и управления;
- средства подготовки исполнимого кода;
- средства версионного контроля исходного кода;
- библиотеки подпрограмм (SDK);
- среды разработки, тестирования и отладки;
- интерактивные рабочие среды;
- графическая оболочка MATE;
- командные интерпретаторы;
- прочие системные приложения;
- прикладное программное обеспечение общего назначения;
- офисные приложения.

Ядро ОС «Альт Рабочая станция» 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.

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

2 ЗАГРУЗКА ОПЕРАЦИОННОЙ СИСТЕМЫ

2.1 Настройка загрузки

Вызов ОС «Альт Рабочая станция», установленной на жесткий диск, происходит автоматически и выполняется после запуска ПЭВМ и отработки набора программ BIOS. ОС «Альт Рабочая станция» вызывает специальный загрузчик.

Загрузчик настраивается автоматически и включает в свое меню все системы, установку которых на ПЭВМ он определил. Поэтому загрузчик также может использоваться для вызова других ОС, если они установлены на компьютере.

Примечание. При наличии на компьютере нескольких ОС (или при наличии нескольких вариантов загрузки), оператор будет иметь возможность выбрать необходимую ОС (вариант загрузки). В случае если пользователем ни один вариант не был выбран, то по истечении заданного времени будет загружена ОС (вариант загрузки), заданные по умолчанию.

При стандартной установке ОС «Альт Рабочая станция» в начальном меню загрузчика доступны несколько вариантов загрузки (Рис. 1): обычная загрузка, загрузка с дополнительными параметрами (например, «recovery mode» – загрузка с минимальным количеством драйверов), загрузка в программу проверки оперативной памяти (memtest).

Варианты загрузки

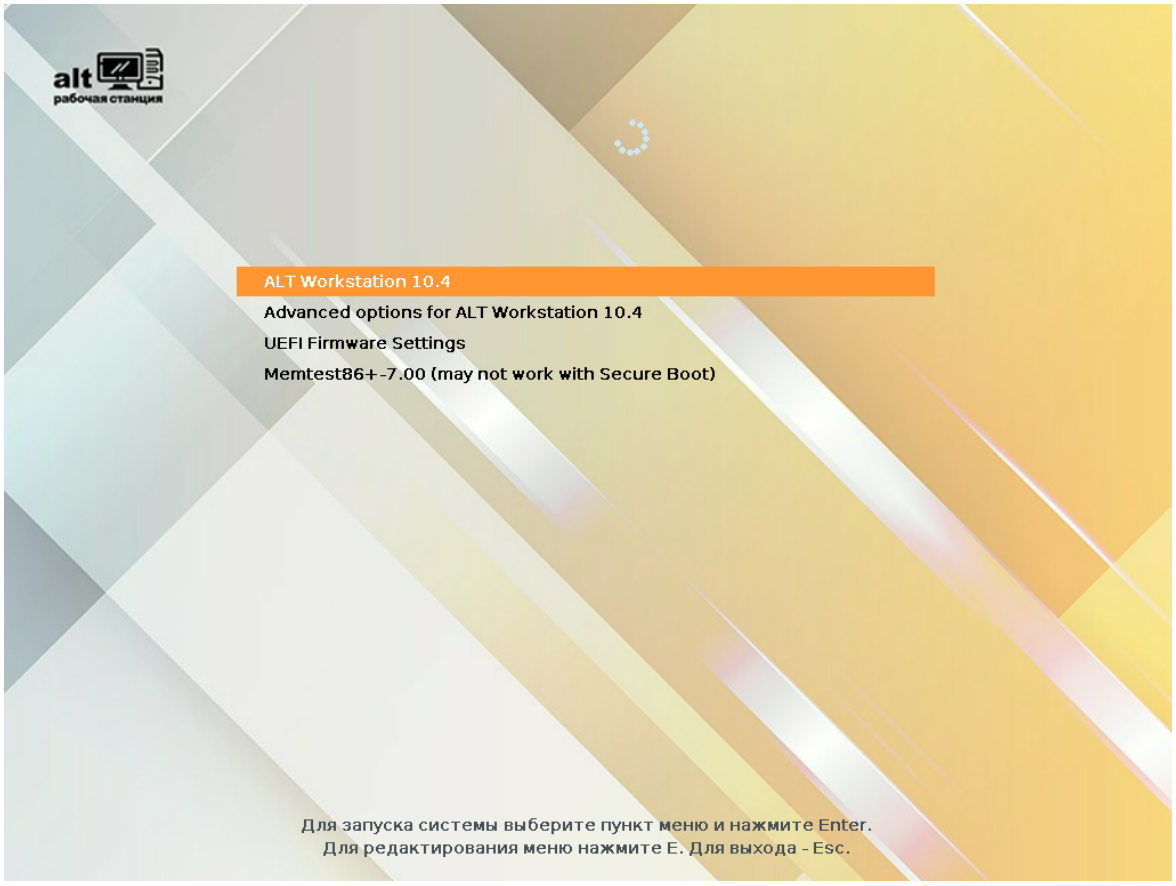

Рис. 1

По умолчанию, если не были нажаты управляющие клавиши на клавиатуре, загрузка ОС «Альт Рабочая станция» продолжится автоматически после небольшого времени ожидания (обычно несколько секунд). Нажав клавишу <Enter>, можно начать загрузку немедленно.

Для выбора дополнительных параметров загрузки нужно выбрать пункт «Дополнительные параметры для ALT Workstation 10.4» («Advanced options for ALT Workstation 10.4»).

Для выполнения тестирования оперативной памяти нужно выбрать пункт «Memtest86+-7.00».

Нажатием клавиши <E> можно вызвать редактор параметров загрузчика GRUB и указать параметры, которые будут переданы ядру ОС при загрузке.

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

Загрузка операционной системы может занять некоторое время, в зависимости от производительности компьютера. Основные этапы загрузки операционной системы – загрузка ядра, подключение (монтирование) файловых систем, запуск системных служб – периодически могут дополняться проверкой файловых систем на наличие ошибок. В этом случае время ожидания может занять больше времени, чем обычно. Подробную информацию о шагах загрузки можно получить, нажав клавишу <Esc>.

2.2 Получение доступа к зашифрованным разделам

В случае если был создан шифрованный раздел, потребуется вводить пароль при обращении к этому разделу (Рис. 2).

Например, если был зашифрован домашний раздел `/home`, то для того, чтобы войти в систему, потребуется ввести пароль этого раздела и затем нажать <Enter>.

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>.

2.3 Вход и работа в системе в консольном режиме

При загрузке в консольном режиме работа загрузчика ОС «Альт Рабочая станция» завершается запросом на ввод логина и пароля учетной записи (Рис. 3). В случае необходимости на другую консоль можно перейти, нажав <Ctrl>+<Alt>+<F2>.

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

Получение доступа к зашифрованным разделам

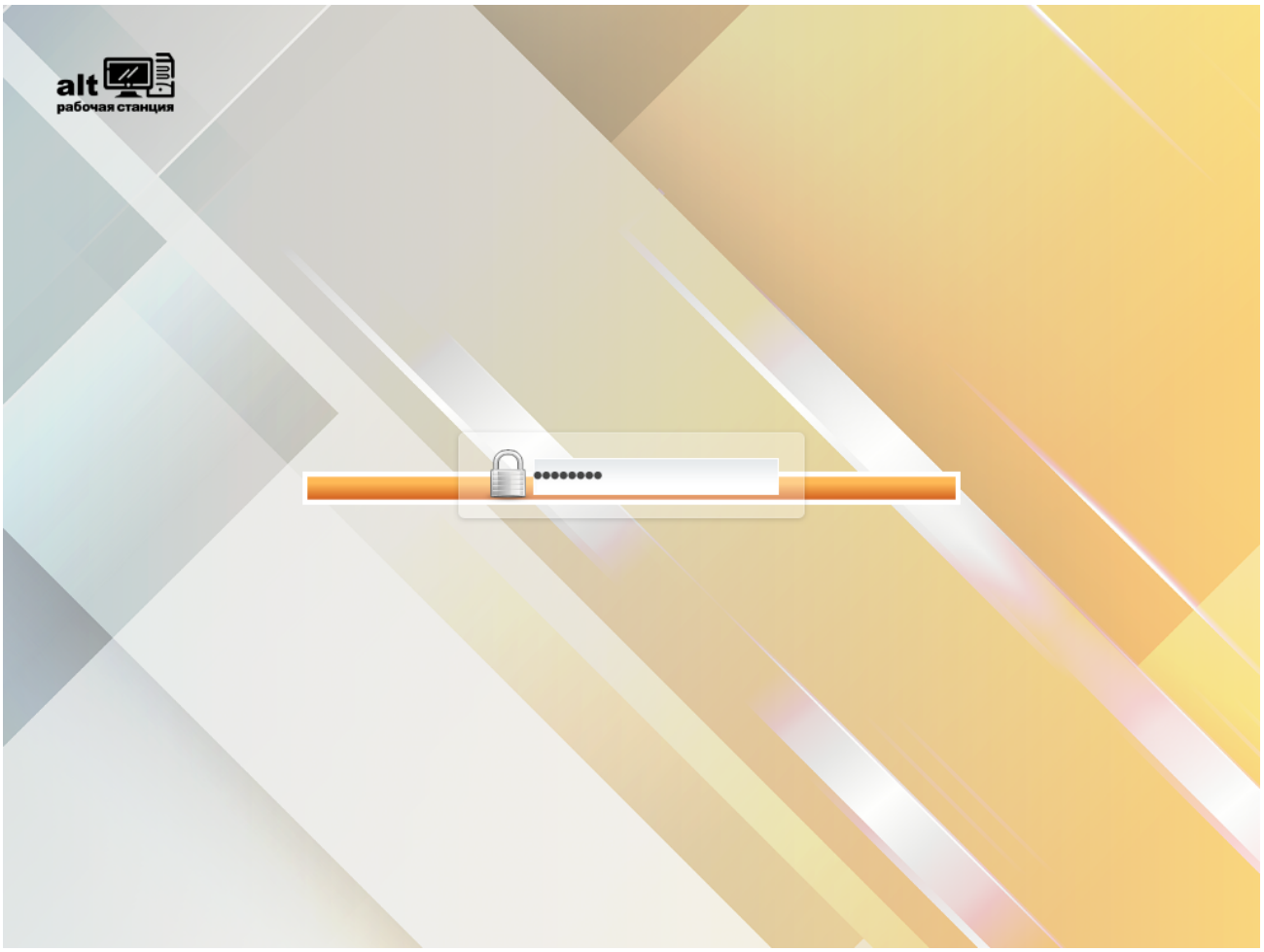

Рис. 2

В случае успешного прохождения процедуры аутентификации и идентификации будет выполнен вход в систему. ОС «Альт Рабочая станция» перейдет к штатному режиму работы и предоставит дальнейший доступ к консоли (Рис. 4).

Запрос на ввод логина

Рис. 3

Приглашение для ввода команд

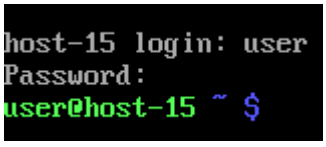

Рис. 4

2.4 Виртуальная консоль

В процессе работы ОС «Альт Рабочая станция» активно несколько виртуальных консолей. Каждая виртуальная консоль доступна по одновременному нажатию клавиш <Ctrl>, <Alt> и функциональной клавиши с номером этой консоли от <F2> до <F6>.

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

Двенадцатая виртуальная консоль (<Ctrl>+<Alt>+<F12>) выполняет функцию системной консоли – на нее выводятся сообщения о происходящих в системе событиях.

2.5 Вход и работа в системе в графическом режиме

Стандартная установка ОС «Альт Рабочая станция» включает графическую оболочку MATE. Графическая оболочка состоит из набора различных программ и технологий, используемых для управления ОС и предоставляющих пользователю удобный графический интерфейс для работы в виде графических оболочек и оконных менеджеров.

При загрузке в графическом режиме работа загрузчика ОС заканчивается переходом к окну входа в систему (Рис. 5), в котором необходимо выбрать логин учетной записи пользователя из выпадающего списка и ввести пароль, соответствующий этой учетной записи, затем нажать <Enter> или нажать кнопку «Войти».

В результате успешного прохождения процедуры аутентификации и идентификации будет выполнен вход в систему. ОС «Альт Рабочая станция» перейдет к штатному режиму работы и предоставит дальнейший доступ к графическому интерфейсу.

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

2.6 Рабочий стол MATE

На Рис. 6 показан графический стол MATE.

На рабочем столе MATE есть две особые области:

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

Окно входа в систему

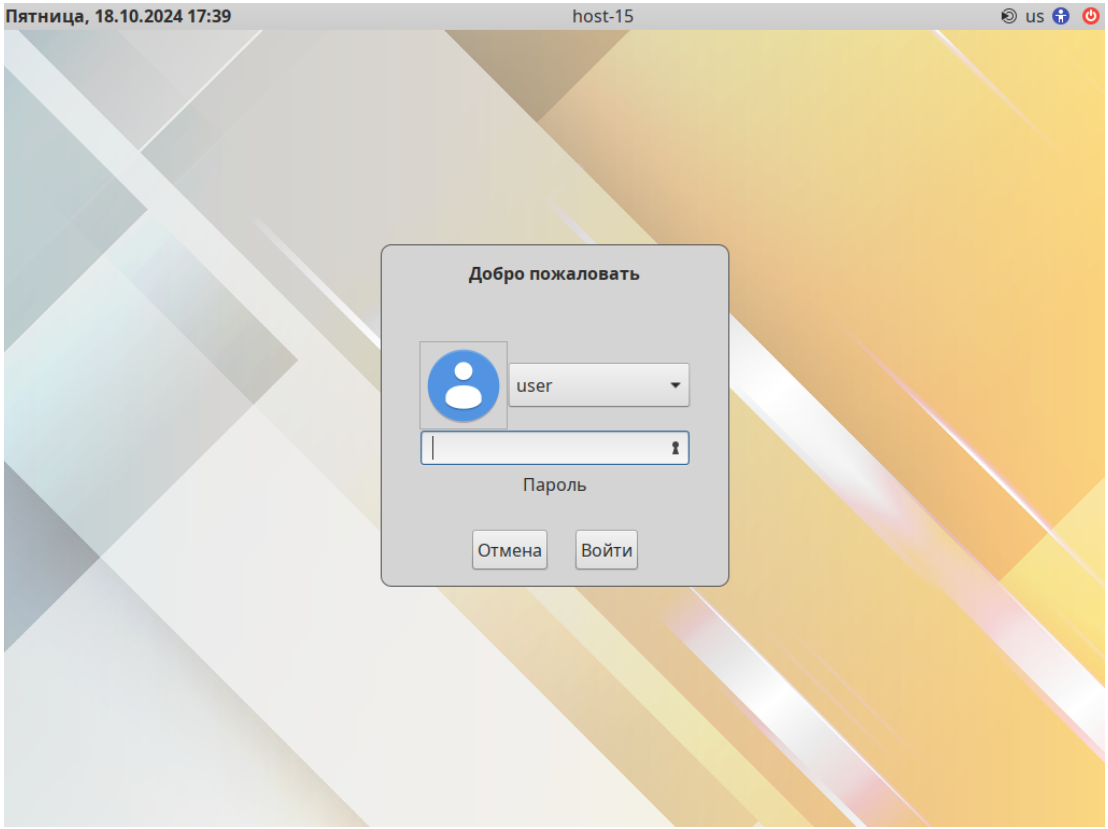

Рис. 5

Рабочий стол MATE

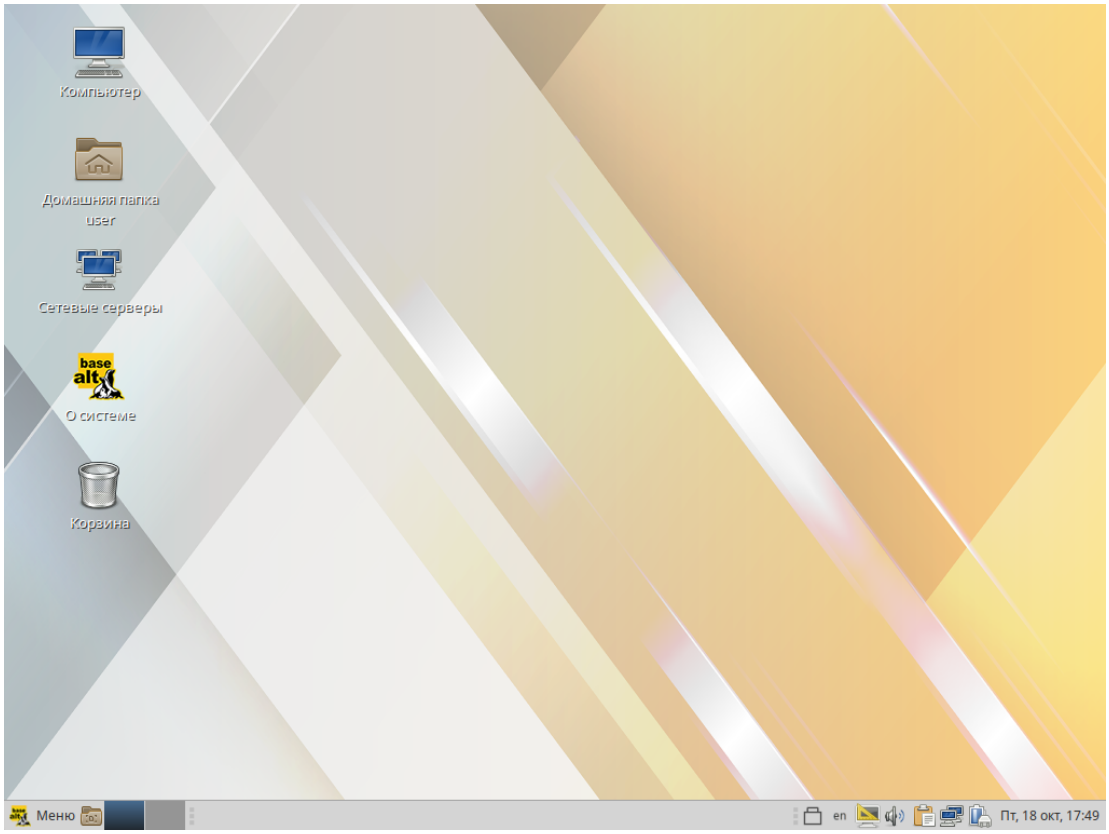

Рис. 6

Область рабочего стола включает в себя значки:

- «Компьютер» – предоставляет доступ к устройствам хранения данных;
- «Домашняя папка пользователя» – предоставляет доступ к домашнему каталогу пользователя `/home/<имя пользователя>`. В этой папке по умолчанию хранятся пользовательские файлы (например, аудиозаписи, видеозаписи, документы). У каждого пользователя своя «Домашняя» папка. Каждый пользователь имеет доступ только в свою «Домашнюю» папку;
- «Сетевые серверы» – позволяет просматривать сетевые подключения компьютера;
- «О системе» – предоставляет доступ к документации;
- «Корзина» – доступ к «удаленным файлам». Обычно удаляемый файл не удаляется из системы. Вместо этого он помещается в «Корзину». С помощью этого значка можно просмотреть или восстановить «удаленные файлы». Чтобы удалить файл из системы, нужно очистить «Корзину». Чтобы очистить «Корзину», необходимо щелкнуть правой кнопкой мыши по значку «Корзина» и выбрать в контекстном меню пункт «Очистить корзину». Можно сразу удалить файл из системы, минуя корзину. Для этого необходимо одновременно с удалением файла зажать клавишу <Shift>.

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

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

Панель MATE (Рис. 7) расположена в нижней части экрана. Панель MATE универсальна: она может содержать значки загрузчика, панели задач, переключатель окон или любое другое сочетание; и её можно удобно настроить. Для того чтобы увидеть возможные варианты настройки, необходимо щелчком правой кнопки мыши вызвать контекстное меню и переместить, удалить или изменить содержание панели по форме и существу.

Панель MATE со списком окон

Рис. 7

На левой части панели расположены:

- основное меню – «Меню MATE», обеспечивающее доступ ко всем графическим приложениями и изменениям настроек;
- кнопка «Свернуть все окна» – кнопка позволяет свернуть (развернуть) все открытые окна на текущем рабочем месте;

- «Переключатель рабочих мест» – это группа квадратов в правом нижнем углу экрана. Они позволяют переключать рабочие места. Каждое рабочее место предоставляет отдельный рабочий стол, на котором можно расположить приложения. По умолчанию активно два рабочих места. Можно изменить это число, нажав правой кнопкой мыши на «переключателе рабочих мест» и выбрав в контекстном меню пункт «Параметры». Для переключения между рабочими столами необходимо использовать комбинацию клавиш <Ctrl>+<Alt>+<←> или <Ctrl>+<Alt>+<→>.

Любые открытые приложения отображаются как кнопки в средней части окна. Тут отображаются все окна с области рабочего стола вне зависимости от того, видно окно или нет. Кнопка скрытого окна будет отображаться с белым фоном. Кнопка приложения, которое выбрано в данный момент, будет с серым фоном. Чтобы переключиться на другое приложение, можно кликнуть по нему левой кнопкой мыши. Для переключения между открытыми окнами также можно использовать комбинацию клавиш<Alt>+<Tab>.

На правой части панели находятся:

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

В левой части панели MATE находится «Меню MATE». Через «Меню MATE» (Рис. 8) осуществляется запуск всех приложений, установленных на компьютер.

Меню MATE

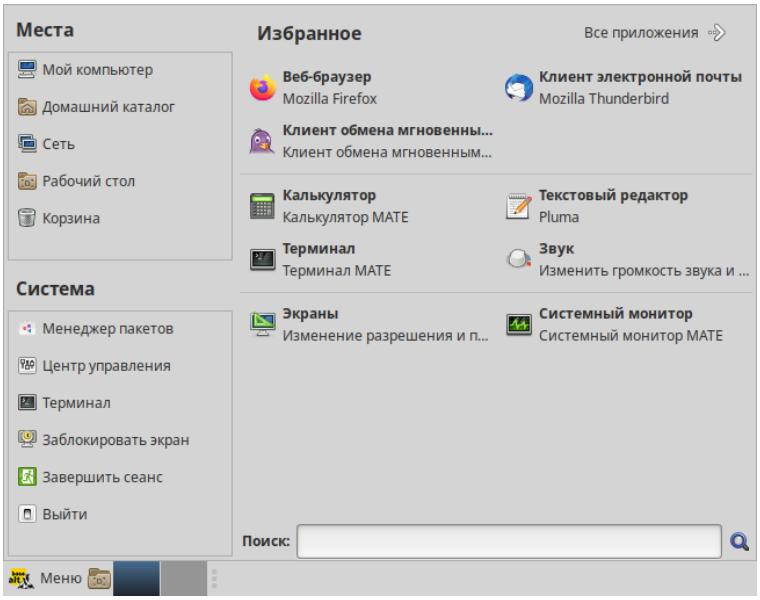

Рис. 8

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

Раздел «Места» содержит пять кнопок, обеспечивающих быстрый доступ к наиболее важным местам ОС:

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

Щелчок по любому пункту в подменю «Места» открывает файловый менеджер Caja.

Руководство Caja можно вызвать, выбрав меню «Справка» →«Содержание».

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

- «Менеджер пакетов» – запускает программу для централизованного управления программным обеспечением;
- «Центр управления» – запускает приложение, позволяющее настроить все аспекты рабочего окружения MATE;
- «Терминал» – запускает приложение «Терминал», которое позволяет вводить команды непосредственно с клавиатуры;
- «Заблокировать экран» – блокирует сеанс доступа пользователя;
- «Завершить сеанс» – запускает диалог, который позволяет завершить сеанс или переключить пользователя;
- «Выйти» – выводит диалоговое окно, которое позволяет перезагрузить или выключить компьютер.

Установленные приложения доступны в следующих пунктах раздела «Приложения»:

- «Все» – показывает полный список установленных приложений;
- «Аудио и видео»;
- «Графика»;
- «Интернет»;
- «Образовательные»;
- «Офис»;
- «Системные»;

- «Стандартные»;
- «Администрирование» – содержит инструменты, позволяющие администрировать систему;
- «Параметры» – содержит инструменты, позволяющие конфигурировать систему.

Этот список обновляется при установке или удалении программ.

Примечание. Если компьютер запрашивает пароль администратора (root), то это значит, что будут производиться важные системные настройки. Следует быть предельно внимательным к выводимым сообщениям.

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

Раздел «Избранное» позволяет получить быстрый доступ к выбранным приложениям. Для добавления приложения в раздел «Избранное» нужно в контекстном меню нужного приложения выбрать пункт «Отображать в избранном». Можно также перетащить иконку приложения на кнопку «Избранное», находящуюся в верхнем правом углу меню. Нажатие правой клавиши мыши позволяет как добавить, так и удалить элементы раздела «Избранное» (в том числе отступы и разделители).

2.7 Блокирование сеанса доступа

2.7.1 Блокирование сеанса доступа после установленного времени бездействия пользователя или по его запросу

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

Если пользователь оставляет свой компьютер на короткое время, он должен заблокировать свой экран, чтобы другие пользователи не могли получить доступ к его файлам или работающим приложениям.

Заблокировать сеанс доступа можно по запросу пользователя, выбрав пункт «Меню MATE» → «Система» → «Заблокировать экран» (Рис. 9).

Для разблокировки требуется ввести пароль пользователя и нажать кнопку «Разблокировать» (Рис. 10).

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

Блокирование сеанса доступа

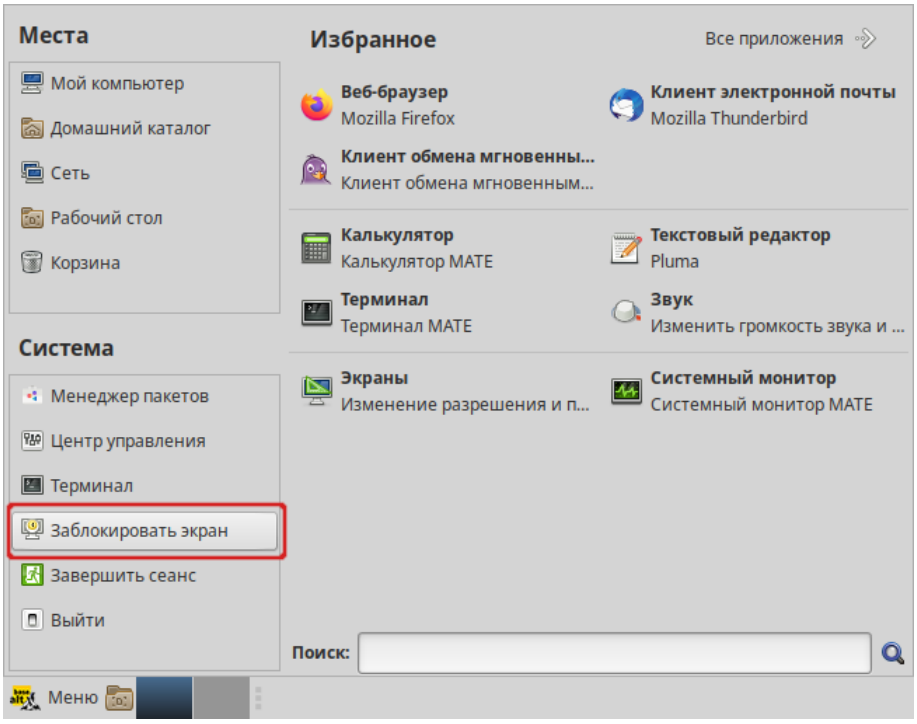

Рис. 9

Разблокирование сеанса доступа

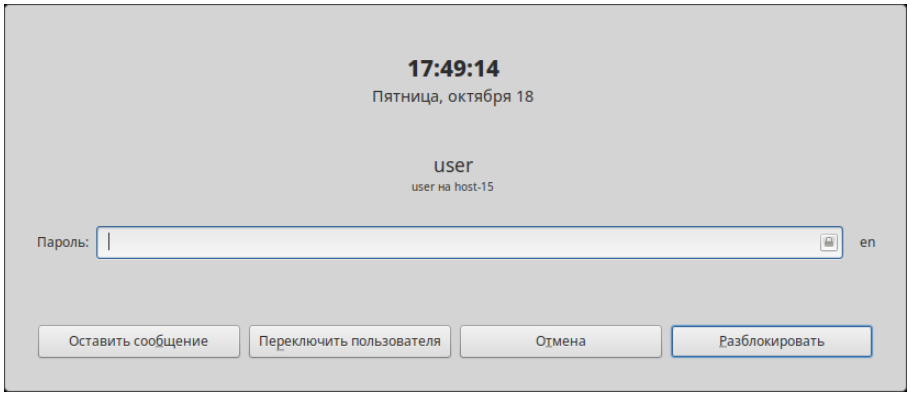

Рис. 10

При работе в графическом режиме блокирование сеанса доступа также происходит после установленного времени бездействия (по умолчанию 5 минут) посредством срабатывания программы – хранителя экрана (screensaver).

Время бездействия системы устанавливается в диалоговом окне «Параметры хранителя экрана», вызываемом из меню «Меню MATE»→ «Приложения»→ «Параметры»→ «Хранитель экрана».

2.7.2 Блокировка виртуальных текстовых консолей

Программа `vlock` позволяет заблокировать сеанс при работе в консоли.

Примечание. Должен быть установлен пакет `vlock`:

```
# apt-get install vlock
```

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:
```

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

2.8 Завершение сеанса пользователя

2.8.1 Графический режим

Для завершения сеанса пользователя в графическом режиме следует в «Меню MATE» в разделе «Система» выбрать пункт «Завершить сеанс» (Рис. 11).

Завершение сеанса пользователя

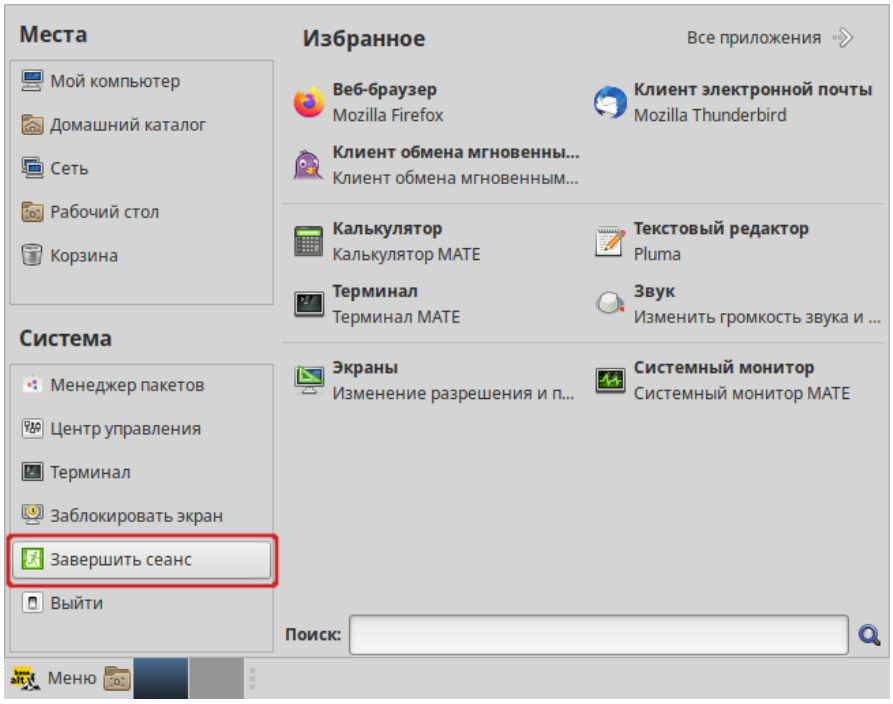

Рис. 11

Далее откроется окно, в котором предоставляется выбор дальнейших действий (Рис. 12):

- «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.

Окно выхода из системы

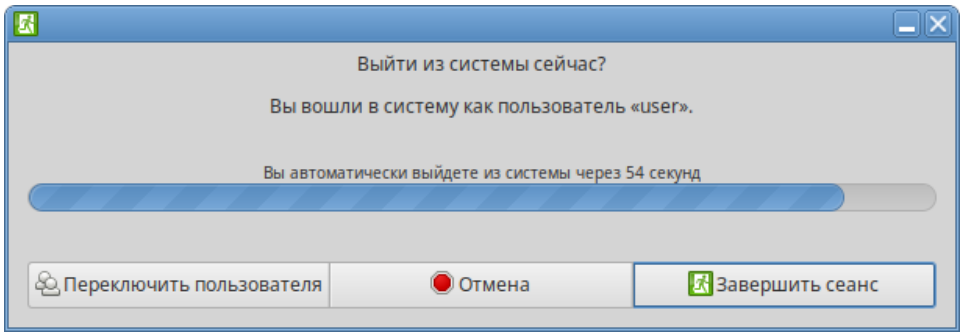

Рис. 12

2.8.2 Консольный режим

Завершить сеанс пользователя в консольном режиме можно, выполнив команду exit:

```
$ exit
host-15 login:
```

2.8.3 Настройки завершения сеанса пользователя в консоли

Для каждого пользователя можно настроить автоматическое завершение сеанса после установленного времени бездействия (неактивности) пользователя. Для этого необходимо в конец файла `/home/<имя пользователя>/.bash_profile` добавить строку:

```
TMOUT=300
```

где 300 – время в секундах от момента последнего действия до завершения сеанса пользователя.

2.9 Выключение/перезагрузка компьютера

2.9.1 Графический режим

Выбор пункта «Выйти» (Рис. 13) в «Меню MATE» позволяет выключить (или перезагрузить) систему.

При выборе этого пункта откроется окно, в котором предоставляется выбор дальнейших действий (Рис. 14):

- «Ждущий режим» – компьютер переводится в режим экономии энергии;
- «Спящий режим» – компьютер переводится в режим энергосбережения, позволяющий отключить питание компьютера, сохранив при этом текущее состояние операционной системы;
- «Перезагрузить» – выполняется перезапуск ОС;

- «Выключить» – выполняется выключение компьютера.

Выключение компьютера

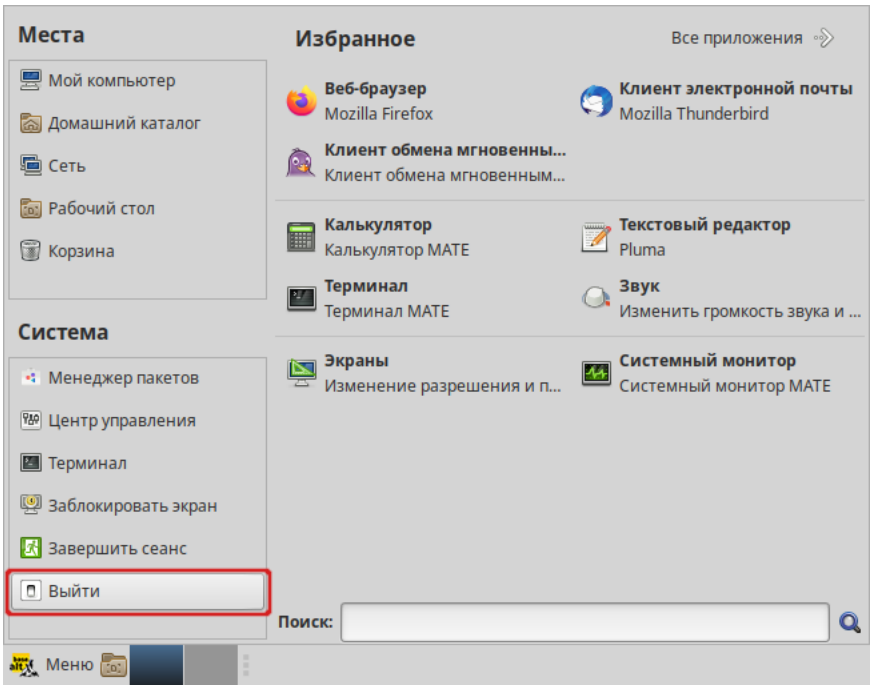

Рис. 13

Окно выключения компьютера

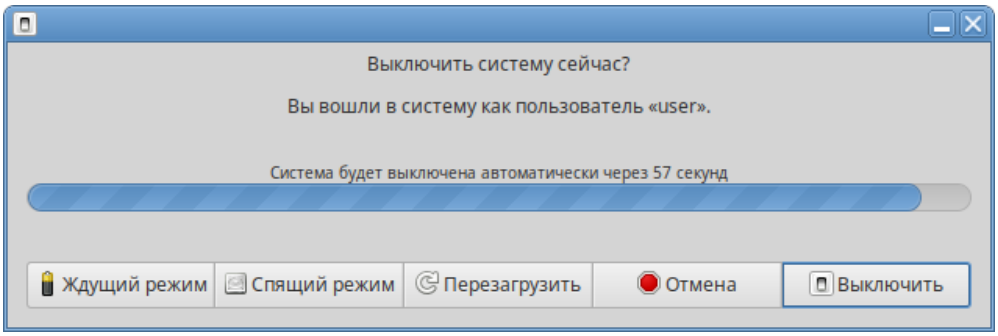

Рис. 14

Примечание. Если при разбивке жёсткого диска не создавался раздел подкачки (swap), то пункт «Спящий режим» в окне выключения компьютера будет отсутствовать.

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

2.9.2 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
```

3 ОБЗОР ПРИЛОЖЕНИЙ ДЛЯ РАБОЧЕЙ СТАНЦИИ

ОС «Альт Рабочая станция» содержит огромное число приложений (программ) для выполнения всех повседневных задач. При этом важно понимать, что для выполнения одного и того же действия могут быть использованы разные приложения. Например, для написания простых текстов доступен целый ряд текстовых редакторов с разным набором возможностей.

Набор программ с диска покрывает обычные потребности. Если же определённая программа отсутствует в системе, то её можно установить с диска или из огромного банка программного обеспечения ОС «Альт Рабочая станция».

3.1 Веб-навигация

Веб-браузеры – комплексные программы для обработки и отображения HTML-страниц по протоколу HTTP и HTTPS (открытие страниц сайтов, блогов и т.д.). Основное назначение веб-браузера – предоставление интерфейса между веб-сайтом и его посетителем. В базовые функции современных веб-браузеров входят:

- навигация и просмотр веб-ресурсов;
- показ оглавлений FTP-серверов и скачивание файлов;
- поддержка скриптовых языков.

Основные принципы работы с веб-браузером неизменны. Программа предоставляет пользователю адресную строку, в которую вносится адрес необходимого сайта. Эта же строка может использоваться для ввода поискового запроса. Для более быстрого доступа адреса часто посещаемых сайтов добавляются в закладки. Для перехода к предыдущей/следующей просмотренной веб-странице, как правило, предусмотрены специальные кнопки на панели инструментов.

3.1.1 Mozilla Firefox

Программа Mozilla Firefox – веб-браузер, поддерживающий большинство современных веб-технологий и интернет-протоколов. Браузер Mozilla Firefox предлагает пользователю логичный интерфейс и возможность полностью контролировать свою работу в Интернете (Рис. 15).

Веб-браузер Mozilla Firefox предоставляет широкие возможности настройки: пользователь может устанавливать дополнительные темы, изменяющие внешний вид программы, и расширения, добавляющие новую функциональность.

Для того чтобы открыть интернет-страницу, необходимо ввести её адрес в адресную строку браузера и нажать кнопку <Enter>. Если нужно открыть ссылку на следующую страницу в новой вкладке, то необходимо нажать на ней средней кнопкой (колесом) мыши. Есть возможность настроить одновременный просмотр нескольких страниц в разных вкладках одного окна.

Mozilla Firefox

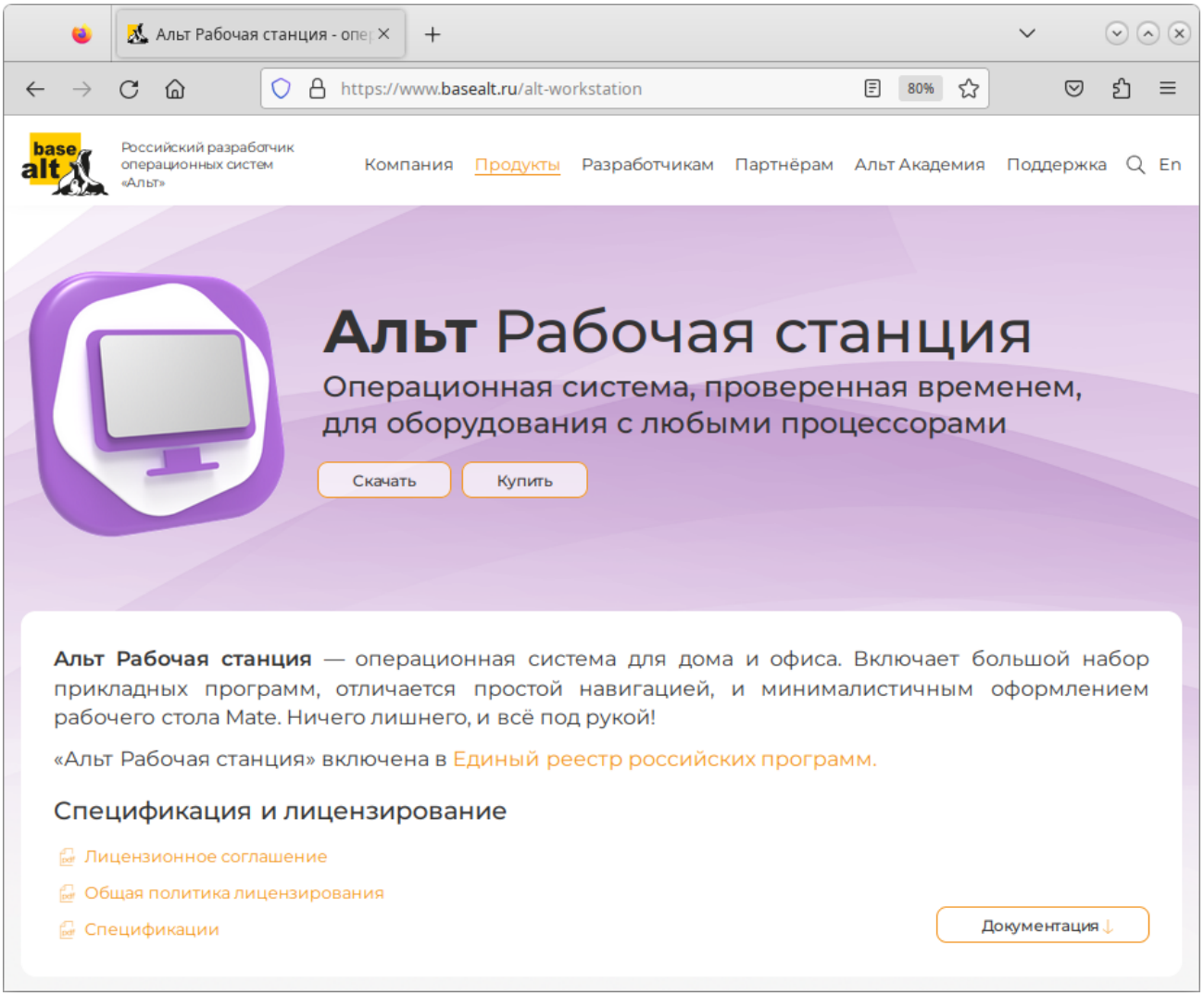

Рис. 15

Для быстрого доступа к часто посещаемым веб-страницам можно создать ссылки на «Панели закладок». Управление закладками и их редактирование осуществляется в рамках диалогового окна «Библиотека».

Панель навигации помогает пользователю искать:

- интеллектуальная строка ввода адреса предоставляет окно-подсказку с историей посещений, закладок и открытых вкладок, а также топа сайтов;
- строка поиска предлагает пользователю функцию поиска по мере набора текста.

Веб-браузер Mozilla Firefox работает как полнофункциональный FTP-клиент. Процесс загрузки найденных в Интернете файлов на жёсткий диск компьютера отображается в диалоговом окне менеджера загрузок. В настройках веб-браузера можно указать папку для сохранения файлов или выбрать возможность назначать папку при сохранении файлов.

Mozilla Firefox включает в себя встроенное средство для просмотра PDF, которое позволяет просматривать почти все PDF-файлы, найденные в Интернете, без использования внешнего приложения.

3.2 Электронная почта

Для работы с электронной почтой применяются специализированные программы – почтовые клиенты, предоставляющие пользователю гибкие и эффективные возможности работы с электронной корреспонденцией: различные средства сортировки сообщений, выбор шаблонов из готового набора, проверку орфографии по мере набора текста и другие полезные функции.

Современные пользователи предпочитают работать с электронной почтой через веб-интерфейс, используя браузер. Подручных средств, предоставляемых популярными почтовыми сервисами, для повседневных почтовых нужд пользователя практически достаточно, но использование специально предназначенных программ даёт некоторые преимущества:

- возможность одновременной работы с несколькими учётными записями;
- гибкие правила сортировки почты;
- обеспечение ограниченного доступа к отдельным папкам или учётным записям;
- наличие антиспам-систем и систем фильтрации рекламы;
- экономия входящего трафика.

Для Linux создано большое количество почтовых клиентов. Все они обладают своими особенностями и, как правило, имеют всё необходимое для успешной работы с электронной почтой: сортировку и фильтрацию сообщений, поддержку различных кодировок сообщений, возможность работы со списками рассылки и т.п.

Выбор почтового клиента зависит от личных предпочтений пользователя. Для первоначальной настройки любого почтового клиента потребуются следующие данные:

- адрес электронной почты;
- пароль для доступа к ящику электронной почты;
- имена серверов входящей и исходящей почты;
- тип сервера входящей почты (IMAP или POP3).

Адрес и порт для доступа к SMTP и POP3 серверам необходимо выяснить у провайдера электронной почты или у администратора сети предприятия.

3.2.1 Thunderbird

Mozilla Thunderbird – мощный почтовый клиент, позволяющий максимально эффективно работать с электронной почтой (Рис. 16). Mozilla Thunderbird позволяет работать с электронной корреспонденцией через протоколы POP, SMTP и IMAP, участвовать в конференциях Usenet, а также осуществлять подписку на новостные ленты RSS.

Функции Thunderbird:

- настройка интерфейса (изменение расположения окон, наличие и отсутствие кнопок на панели инструментов, изменение их размера и т.д.);
- отображение любого форматирования HTML, обеспечивающее кроссплатформенную совместимость;
- выбор режимов показа и компоновки учётных записей и почтовых папок;
- поддержка смены тем и установки расширений.

Почтовый клиент Mozilla Thunderbird

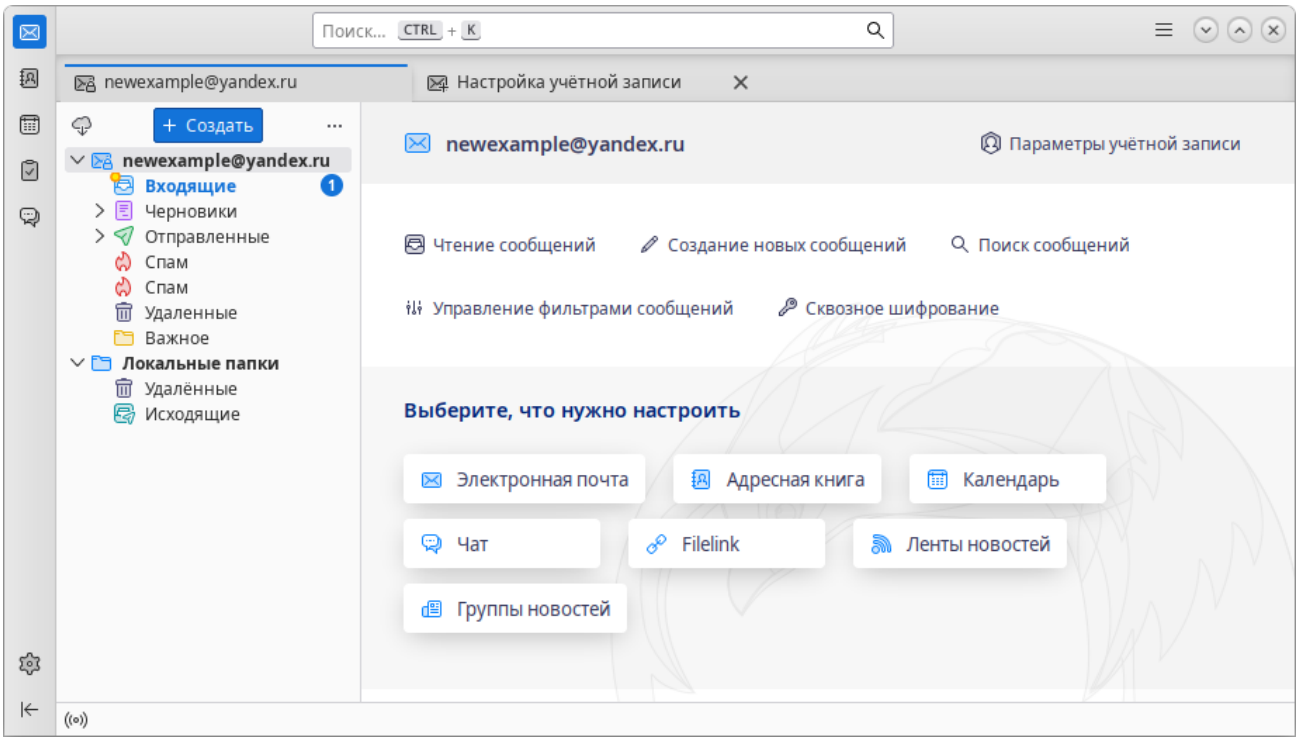

Рис. 16

При первом запуске почтового клиента Thunderbird будет автоматически запущен мастер «Настройка учётной записи почты».

Мастер создания учётной записи запросит (Рис. 17):

- имя пользователя;
- адрес электронной почты;
- пароль.

Далее, на основании введённой информации, мастер определяет протокол доступа (IMAP или POP3) и адреса серверов входящих и исходящих сообщений. Можно принять предложенные настройки, если они верны, нажав на кнопку «Готово», или указать правильные настройки, воспользовавшись кнопкой «Настроить вручную...». Добавить дополнительную учётную запись можно выбрав в левой части окна программы одну из существующих учётных записей, и затем нажав кнопку «Электронная почта».

Если почтовый ящик пользователя расположен на сервисе Gmail или Яндекс.Почта, то вся настройка происходит автоматически – необходимо ввести только имя учётной записи и пароль.

Если у пользователя есть несколько учётных записей можно выбирать метод их компоновки на панели почтовых папок.

Почтовый клиент Mozilla Thunderbird. Настройка учётной записи почты

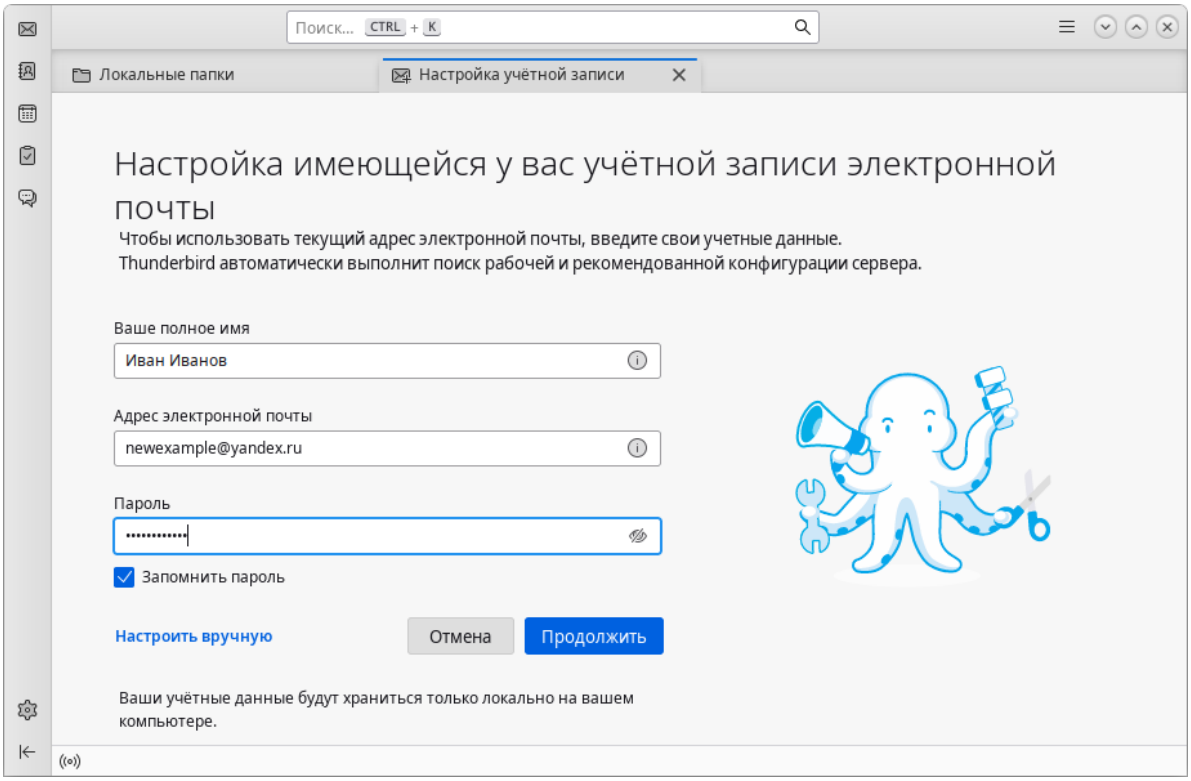

Рис. 17

Для составления письма необходимо нажать кнопку «Создать», в открывшемся окне «Создание сообщения» ввести адрес получателя, тему и текст письма (Рис. 18). Для проверки ошибок в тексте необходимо нажать кнопку «Орфография».

Использование почтового клиента

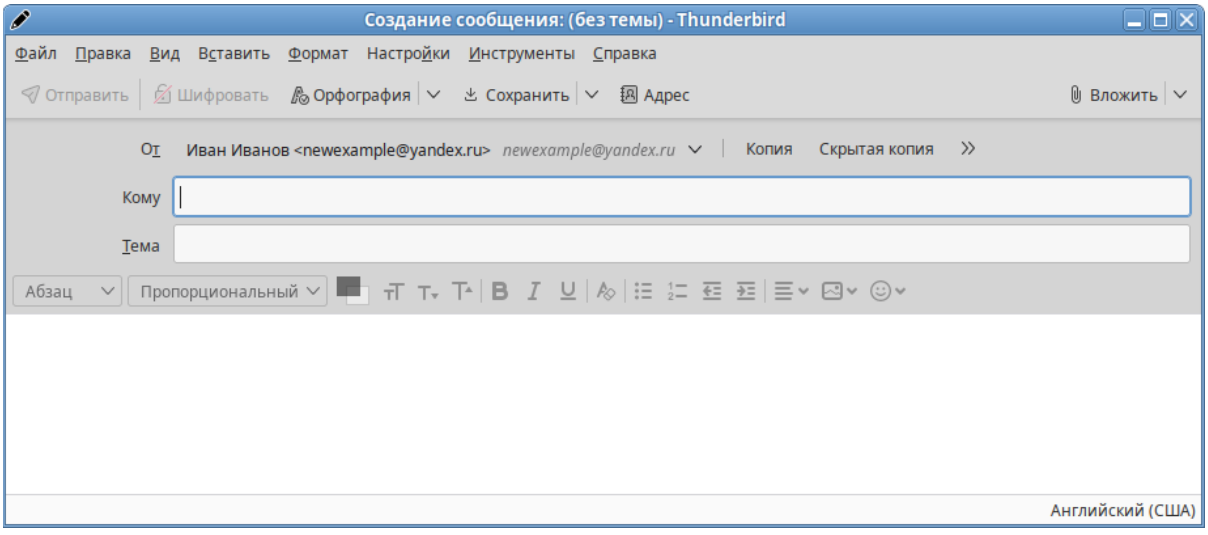

Рис. 18

В виде вложения к письму можно пересылать электронные документы, изображения, архивы и другие вложения. Для того чтобы добавить вложение, необходимо нажать кнопку «Вложить» и выбрать нужный файл в открывшемся окне. Закончив составление письма, необходимо нажать кнопку «Отправить».

3.3 Обмен мгновенными сообщениями

Для обмена сообщениями в режиме реального времени через Интернет необходима специализированная клиентская программа, передающая текстовые сообщения, а также файлы различных типов. Система мгновенного обмена сообщениями является одним из самых доступных и востребованных средств общения в Интернете. Преимущества инструментов мгновенного обмена информацией:

- скорость — мгновенные сообщения позволяют собеседникам общаться со скоростью нажатия на кнопку, без необходимости открывать письма и ждать ответа;
- удобство — программы обмена мгновенными сообщениями включают широкий набор коммуникативных и производственных функций.

Большинство современных программ мгновенного обмена сообщениями позволяют видеть, подключены ли в данный момент абоненты, занесённые в список контактов. Сообщения появляются на мониторе собеседника только после окончания редактирования и отправки. В список основных функций служб мгновенных сообщений входят:

- чат (видеочат, текстовый и голосовой);
- VoIP сервисы: звонки на компьютер, звонки на телефоны;
- возможность отправки SMS;
- передача файлов;
- инструменты для совместной работы в режиме реального времени;
- возможность общаться в чате непосредственно на веб-странице;
- напоминания и оповещения;
- хранение истории общения по каждому контакту;
- индикация о сетевом статусе занесённых в список контактов пользователей.

Существуют клиентские программы, позволяющие подключаться одновременно к нескольким сетям. Они поддерживают наиболее популярные протоколы, что избавляет пользователя от необходимости устанавливать отдельный IM-клиент для каждой сети.

3.3.1 Pidgin

Pidgin – мультипротокольная программа-клиент для мгновенного обмена сообщениями, позволяющая одновременно подключиться к нескольким сетям (Рис. 19). Поддерживает наиболее популярные протоколы: Bonjour, Gadu-Gadu, Google Talk, GroupWise, IRC, SIMPLE, Sametime, XMPP (Jabber) и Zephyr.

Окно списка собеседников Pidgin

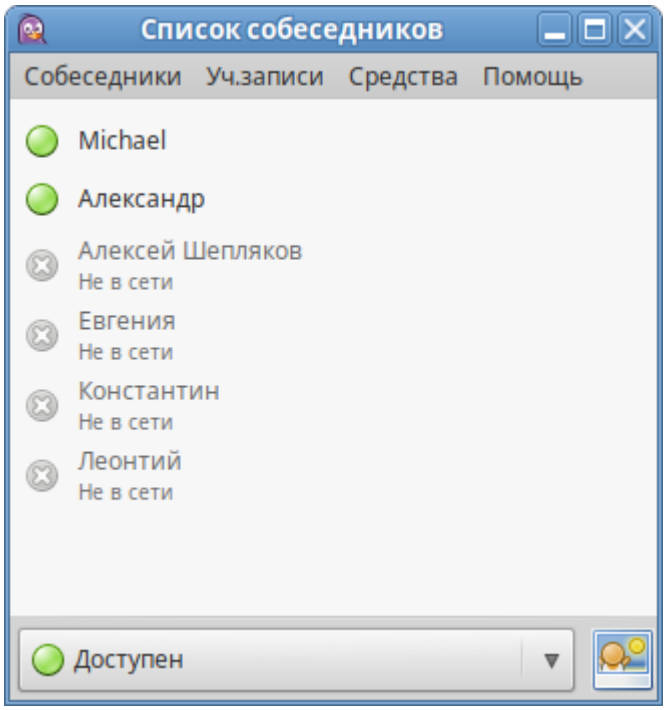

Рис. 19

Возможности Pidgin:

- поддержка особенностей различных сетей (статус сообщения, значки друзей, уведомление о наборе текста…);
- шифрованный чат;
- объединение контактов в один метаконтакт;
- запись протокола событий;
- поддержка вкладок в окне разговора;
- одновременное подключение к нескольким аккаунтам;
- слежение за пользователями;
- обмен файлами;
- многоязычный интерфейс.

Функционал Pidgin значительно расширяется за счёт использования плагинов.

После запуска Pidgin необходимо произвести его первоначальную настройку. При первом запуске Pidgin из меню «Уч.записи» → «Управление учётными записями» необходимо запустить диалоговое окно мастера создания учётной записи и создать учётную запись пользователя (Рис. 20).

Диалоговое окно мастера создания учётной записи

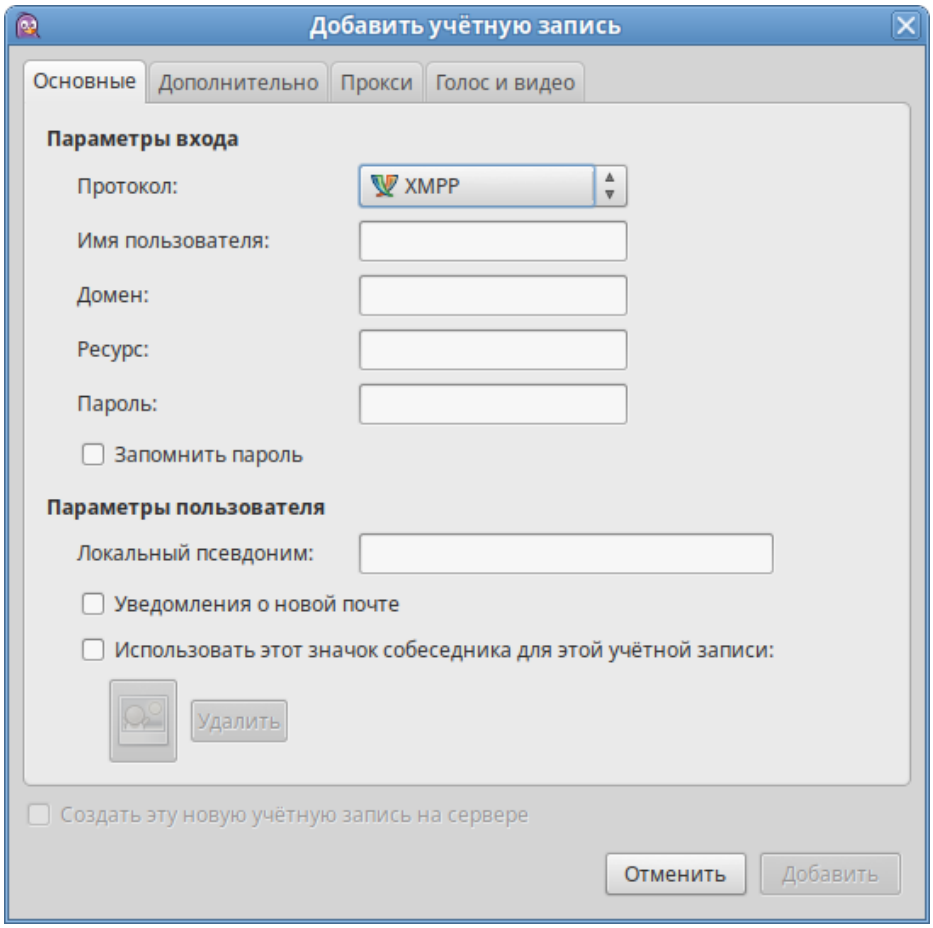

Рис. 20

Из списка поддерживаемых служб необходимо выбрать ту, которая будет использоваться (можно выбрать службу, основанную на открытых стандартах, например, jabber).

После настройки учётной записи следует добавить в список контактов собеседников (кнопка «Добавить собеседника…») и, при условии, что нужный собеседник подключен к службе мгновенных сообщений, можно начинать общение.

За дополнительной информацией по использованию Pidgin можно обратиться к справке, вызываемой из меню «Помощь» → «Помощь в сети».

3.4 Офисные приложения

Офисными приложениями традиционно называют пакет программ для работы с текстами, таблицами и презентациями.

3.4.1 LibreOffice

LibreOffice – пакет программ для работы с офисными документами. Кроме стандартных для LibreOffice форматов хранения данных, можно успешно открывать и сохранять документы, созданные в других популярных офисных пакетах (Рис. 21).

Пакет программ LibreOffice

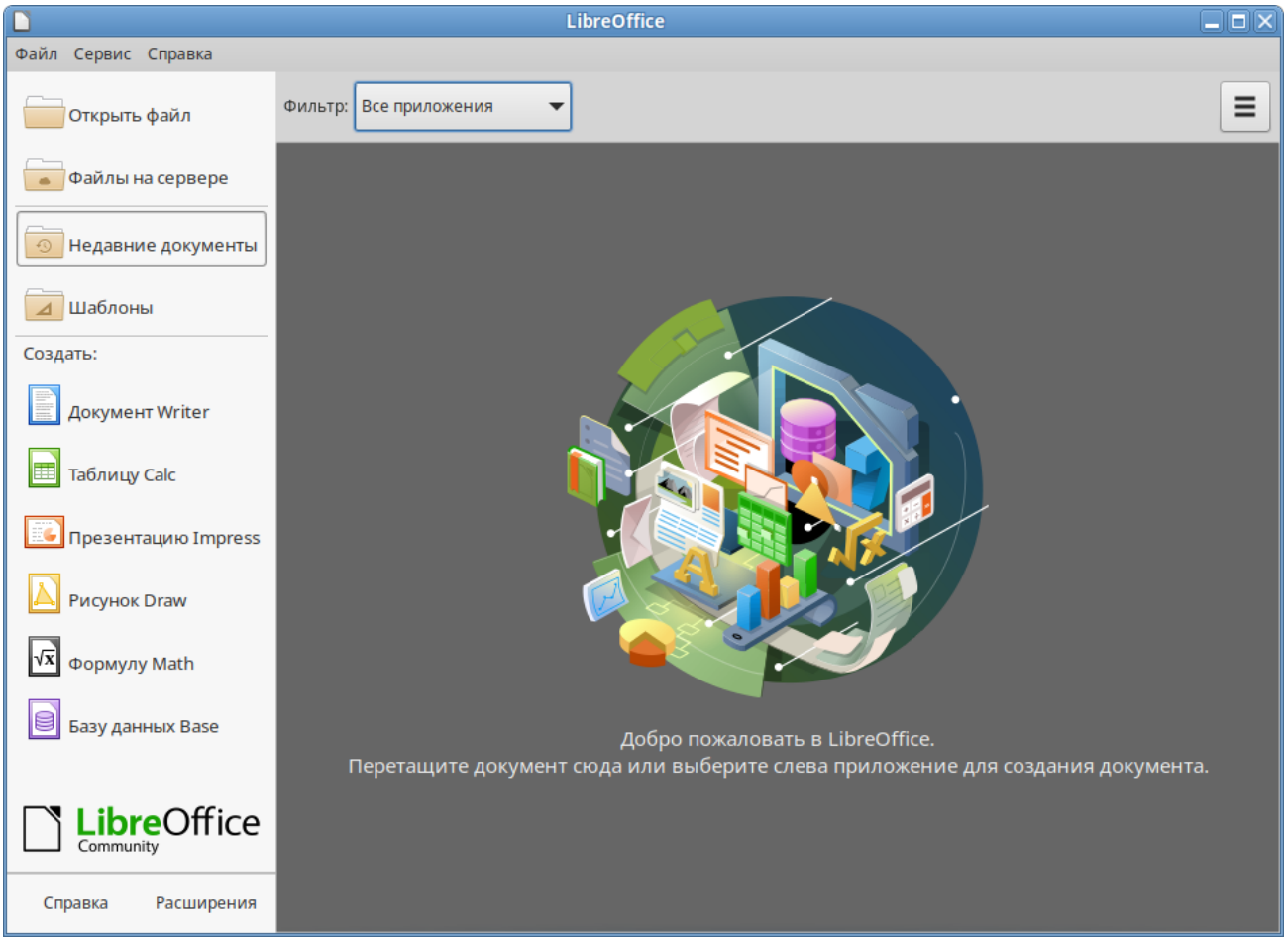

Рис. 21

Текстовый процессор (LibreOffice Writer) позволяет проектировать и создавать текстовые документы, содержащие изображения, таблицы или графики. В LibreOffice Writer можно сохранять документы в различных форматах, включая стандартизированный формат OpenDocument format (ODF), формат Microsoft Word (DOC, DOCX) или HTML. Кроме того, LibreOffice Writer позволяет экспортировать документ в формате переносимого документа (PDF). Текстовый процессор поддерживает и другие форматы.

Электронная таблица (LibreOffice Calc) предназначена для работы с электронными таблицами. Инструментарий электронных таблиц включает мощные математические функции, позволяющие вести сложные статистические, финансовые и прочие расчёты.

Презентация (LibreOffice Impress) позволяет создавать профессиональные слайд-шоу, которые могут включать диаграммы, рисованные объекты, текст, мультимедиа и множество других элементов. При необходимости можно также импортировать и изменять презентации Microsoft PowerPoint. Для того чтобы сделать экранные презентации более эффектными, можно использовать такие средства, как анимация, мультимедиа и переходы между слайдами.

Редактор формул (LibreOffice Math) позволяет создавать и редактировать математические и химические формулы. Math предоставляет различные операторы, функции и средства форматирования, облегчающие создание формул. Math может быть запущен автономно или вызван из других модулей LibreOffice (Writer, Calc, Impress, Draw).

Редактор рисунков (LibreOffice Draw) позволяет создавать рисунки различной сложности и экспортировать их с использованием нескольких общепринятых форматов изображений. Кроме того, можно вставлять в рисунки таблицы, диаграммы, формулы и другие элементы, созданные в программах LibreOffice.

Базы данных (LibreOffice Base) поддерживает некоторые обычные файловые форматы баз данных, например, BASE. Кроме того, можно использовать LibreOffice Base для подключения к внешним реляционным базам данных, например, к базам данных MySQL или Oracle. В базе LibreOffice Base невозможно изменить структуру базы данных или редактировать, вставлять и удалять записи для ниже перечисленных типов баз данных (они доступны только для чтения):

- файлы электронной таблицы;
- текстовые файлы;
- данные адресной книги.

3.5 Файловые менеджеры

Файловые менеджеры предоставляют интерфейс пользователя для работы с файловой системой и файлами. Файловые менеджеры позволяют выполнять наиболее частые операции над файлами – создание, открытие/проигрывание/просмотр, редактирование, перемещение, переименование, копирование, удаление, изменение атрибутов и свойств, поиск файлов и назначение прав. Помимо основных функций, многие файловые менеджеры включают ряд дополнительных возможностей, например, таких как работа с сетью (через FTP, NFS и т.п.), резервное копирование, управление принтерами и прочее.

3.5.1 Обзор файлового менеджера Caja

Caja – это современный файловый менеджер для рабочей среды MATE (Рис. 22). Файловый менеджер Caja является точкой доступа, как к файлам, так и к приложениям. Используя файловый менеджер, можно:

- создавать папки и документы;
- просматривать файлы и папки;
- управлять файлами и папками;
- настраивать и выполнять особые действия;
- получать доступ к съёмным носителям.

Файловый менеджер Caja

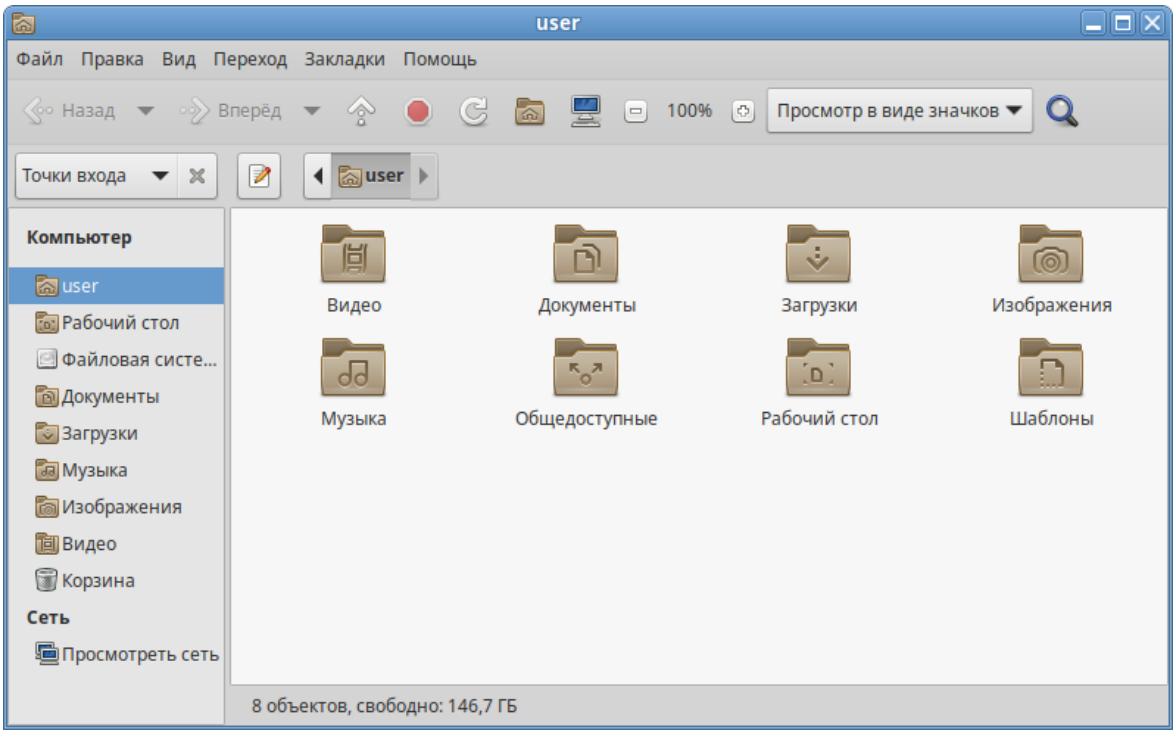

Рис. 22

Окно файлового менеджера состоит из боковой панели слева, основной области справа и панели адреса, расположенной над основной областью. На боковой панели размещены закладки на различные папки системы. Основная область отображает содержимое текущей папки. Панель адреса всегда показывает путь к текущей папке.

Двойной щелчок на папках открывает их, а щелчок правой кнопкой мыши на объектах открывает контекстное меню, предлагающее на выбор некоторые действия с ними.

Примечание. Контекстное меню файла, папки и свободного пространства могут сильно отличаться друг от друга.

Чтобы просмотреть свойства файла (папки), необходимо выделить файл (папку) и выполнить одно из следующих действий:

- в меню выбрать «Файл» → «Свойства»;
- в контекстном меню файла (папки) выбрать пункт «Свойства»;
- нажать <Alt>+<Enter>.

Окно «Свойства» объекта показывает подробную информацию о любом файле, папке или другом объекте в файловом менеджере (какие именно сведения будут доступны, определяется типом объекта).

С помощью окна «Свойства объекта» можно выполнить следующие действия:

- изменить значок объекта;
- изменить файловые права на доступ к объекту;

- выбрать, с помощью какого приложения следует открывать данный объект и другие объекты того же типа.

3.5.1.1 Домашняя папка

Все файлы и папки пользователя хранятся в системе внутри домашней папки (каталог /home/имя_пользователя). Открыть её можно, щёлкнув на значке папки на рабочем столе. Откроется файловый менеджер Caja, позволяющий просматривать содержимое дерева каталогов, удалять, переименовывать и производить прочие операции над файлами и папками.

Примечание. Домашняя папка есть у каждого пользователя системы, и по умолчанию содержащиеся в ней файлы недоступны для других пользователей (даже для чтения).

В домашней папке по умолчанию находятся несколько стандартных папок:

- «Документы» – папка, предназначенная для хранения документов;
- «Загрузки» – в данную папку по умолчанию загружаются файлы из Интернета;
- «Рабочий стол» – содержит файлы, папки и значки, отображающиеся на рабочем столе.
- «Видео», «Изображения», «Музыка», «Шаблоны» – папки, предназначенные для хранения файлов различных типов;
- «Общедоступные» – папка, предназначенная для хранения файлов, к которым могут иметь доступ другие пользователи сети.

Кроме того, в домашней папке и её подпапках можно создавать другие папки, например, выбрав в контекстном меню пункт «Создать папку…» (Рис. 23).

Пункт «Создать папку» в контекстном меню Caja

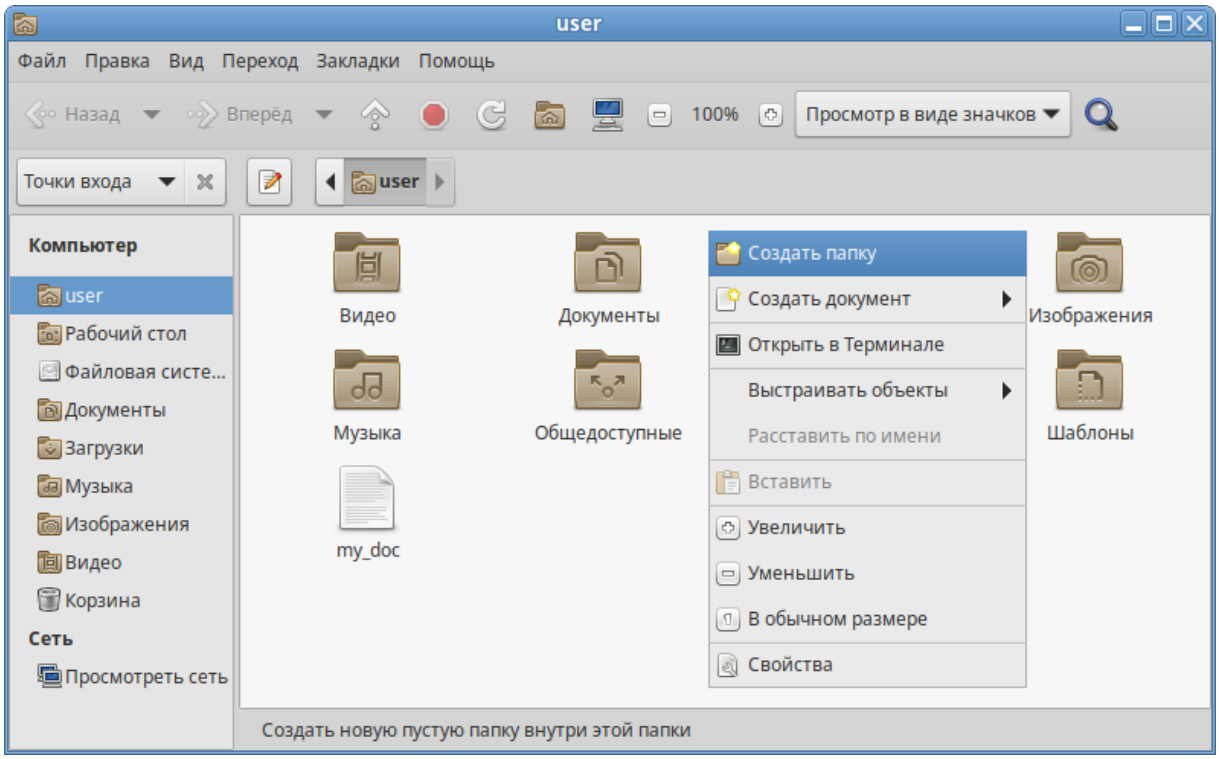

Рис. 23

Caja, как и прочие приложения ОС «Альт Рабочая станция», содержит руководство пользователя, вызываемое из раздела «Помощь» основного меню или нажатием <F1>. Ниже описаны лишь некоторые возможности файлового менеджера. За полным руководством обращайтесь к встроенному руководству пользователя Caja.

3.5.1.2 Строка адреса

Ориентироваться в сложно организованной системе вложенных папок и быстро перемещаться по ней поможет путь в адресной строке. Каждая папка в этом пути представлена в виде кнопки (Рис. 24). Нажав на кнопку, можно быстро открыть нужную папку.

Строка адреса может быть также представлена в виде редактируемой строки (Рис. 25). Чтобы переключить адресную строку из вида хлебных крошек к редактируемой версии можно нажать <Ctrl>+<L> или нажать кнопку  . Чтобы вернуться к показу кнопок, достаточно нажать клавишу <Esc> или повторно нажать кнопку  .

Адресная строка

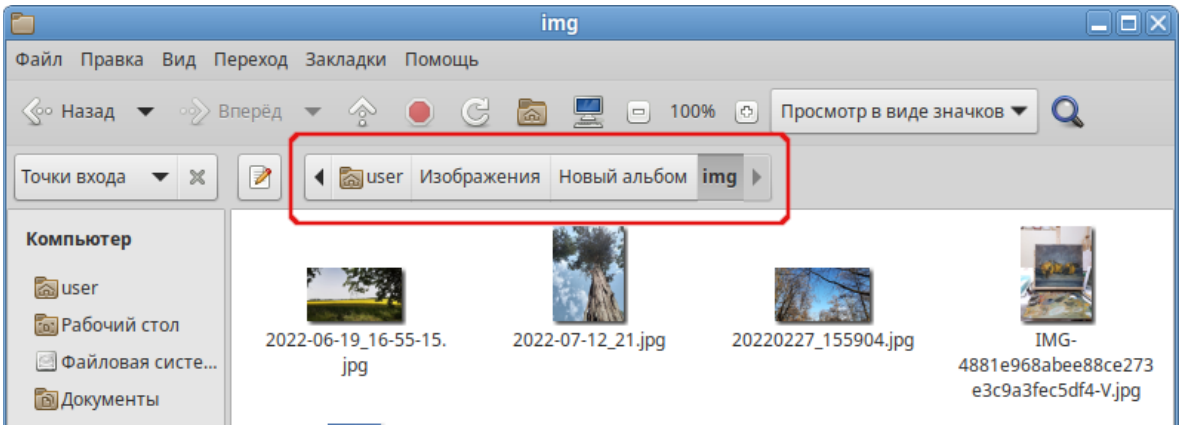

Рис. 24

Редактируемая строка адреса

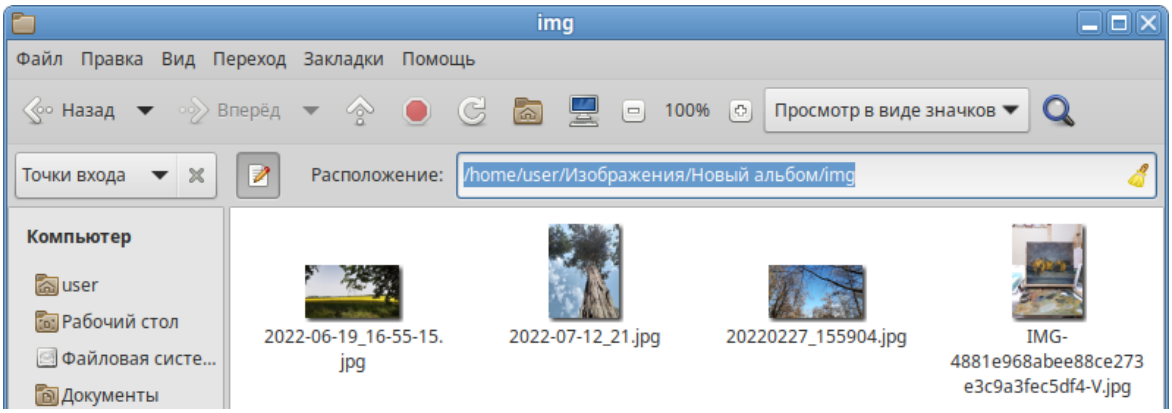

Рис. 25

3.5.1.3 Копирование и перемещение файлов

Скопировать или переместить файл или папку можно различными способами:

- «перетащить» папку или файл из одного открытого окна Caja в другое (где открыта целевая папка). Перетаскивание можно осуществлять и в двупанельном режиме (Рис. 26). В этом случае не потребуется запускать два экземпляра Caja – можно перемещать и копировать файлы и папки, перетаскивая их между панелями. Двупанельный режим можно активировать, нажав клавишу <F3>.
- копировать и перемещать папку или файл можно, используя основное стандартное меню «Правка» (либо контекстное меню):
  - необходимо выделить то, что нужно скопировать или переместить;
  - из основного меню «Правка» или из контекстного меню выбрать «Копировать» (для копирования) или «Вырезать» (для перемещения);
  - открыть папку, в которую нужно скопировать или переместить объект;
  - вызвать в этой папке из основного меню «Правка» (из контекстного меню) пункт «Вставить».

Копирование файлов в менеджере Caja

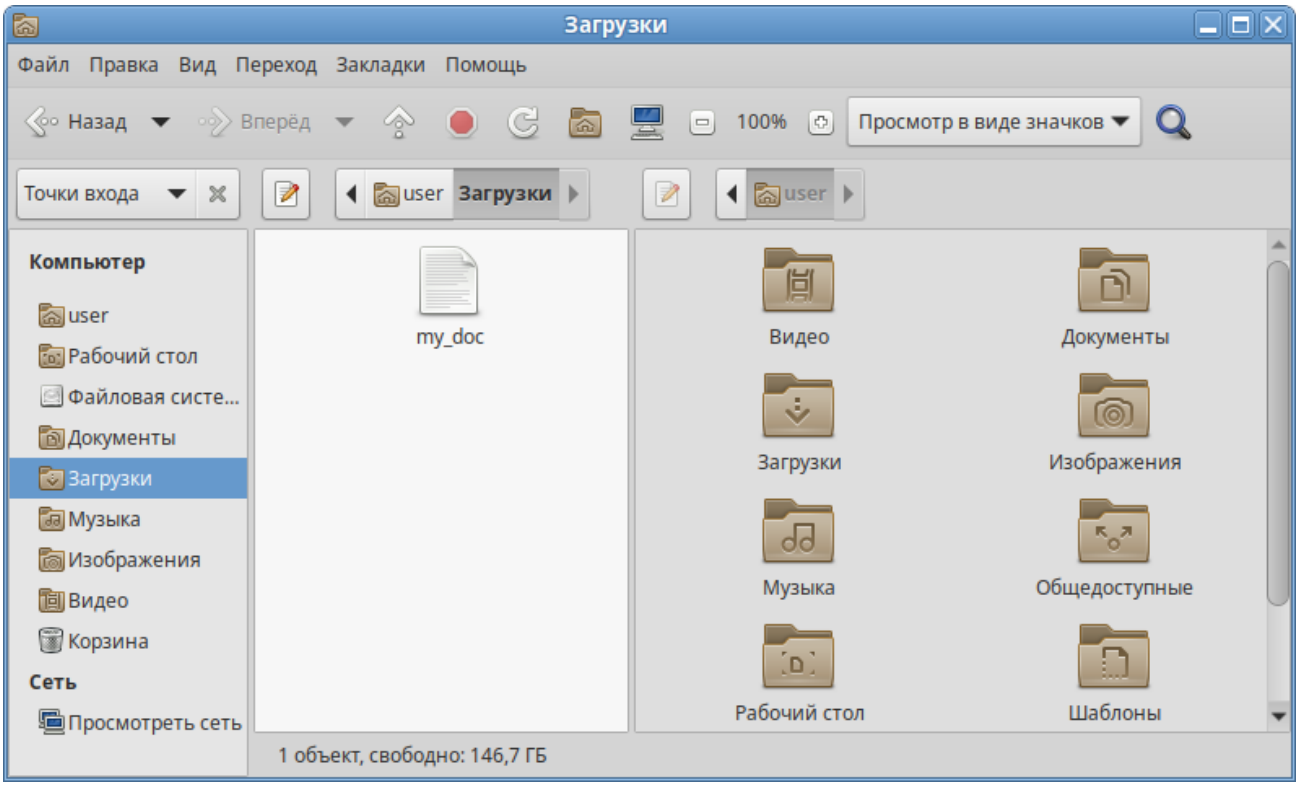

Рис. 26

Примечание. Для выбора сразу нескольких файлов или папок можно отметить их списком, удерживая при этом клавишу <Ctrl>.

3.5.1.4 Удаление файлов

Удалить выделенный объект можно из основного меню «Правка»→ «Удалить в корзину». Можно также использовать контекстное меню (Рис. 27) или удалять объекты клавишей <Del>. В этом случае файлы и папки удаляются в «Корзину». Это позволяет восстановить объект при его ошибочном удалении.

При ошибочном удалении можно восстановить объект из корзины. Для этого нужно открыть корзину, вызвать на удалённом файле или папке контекстное меню и в нём выбрать пункт «Восстановить». Выбор в контекстном меню пункта «Удалить окончательно» навсегда удалит ненужный файл или папку без возможности восстановления.

Для того чтобы безвозвратно удалить все содержимое корзины, необходимо выбрать в контекстном меню корзины пункт «Очистить корзину».

Для того чтобы не засорять жёсткий диск компьютера ненужными файлами и сразу удалять их, минуя корзину, можно воспользоваться пунктом меню «Правка»→«Удалить» (<Shift>+<Del>).

Caja. Удаление файла

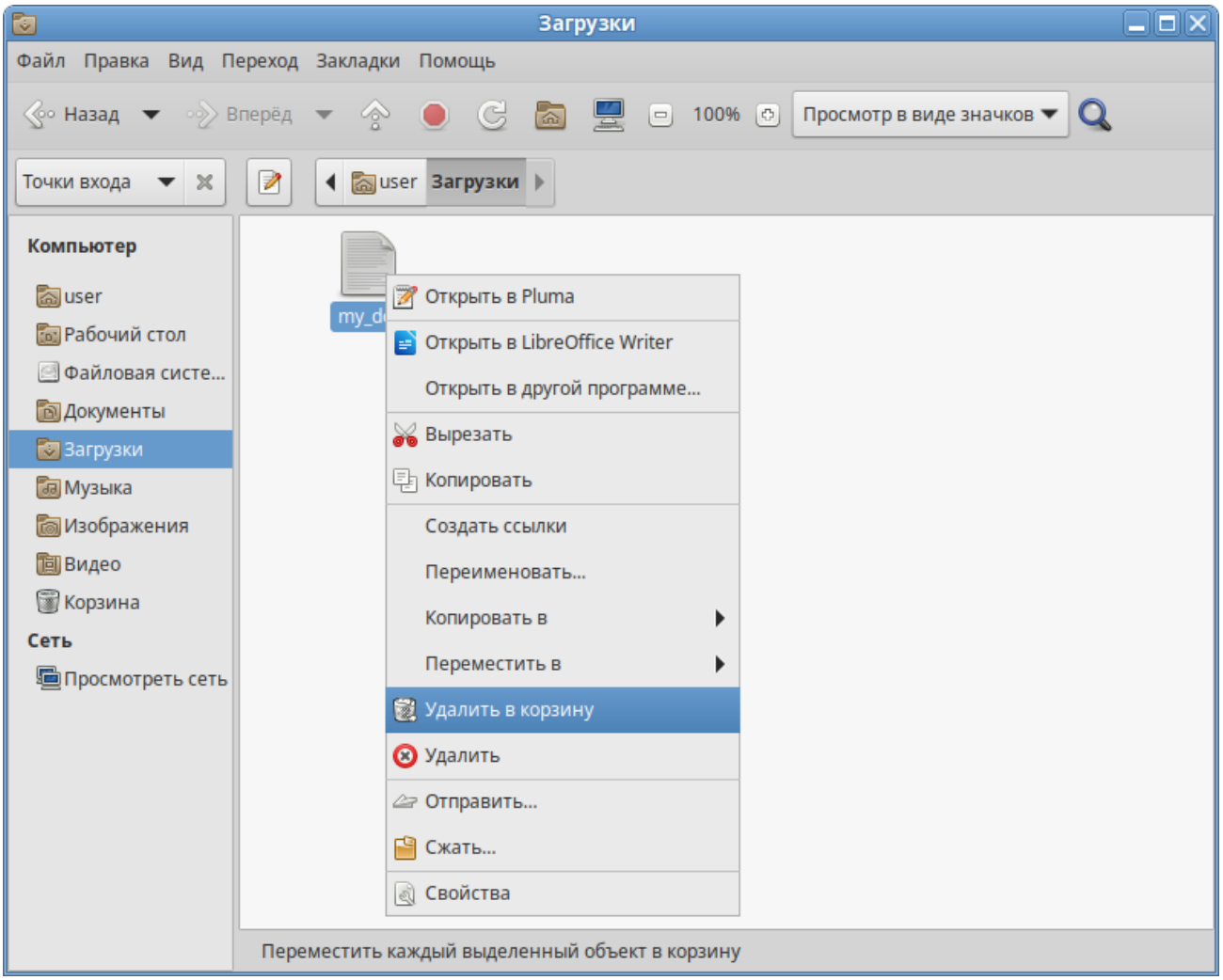

Рис. 27

3.5.1.5 Открытие файлов

Открыть файл из Caja – значит запустить приложение, ассоциированное с этим типом файлов, в нём и откроется файл.

Примечание. Для указания, какие приложения должны по умолчанию запускаться, используется инструмент «Предпочтительные приложения» («Меню MATE» → «Параметры» → «Предпочтительные приложения»). Для каждой категории предпочтительных приложений (Рис. 28) предусмотрено раскрывающееся меню со списком доступных для выбора приложений.

При щелчке на файл, являющийся изображением (например, .jpg файл) откроется программа просмотра изображений «Глаз MATE». Таким образом, можно открывать файлы простым щелчком прямо из файлового менеджера Caja.

Если на компьютере установлено несколько программ для работы с изображениями, то можно запустить нужную, выбрав её из контекстного меню (Рис. 29) (щелчок правой кнопкой мыши по файлу, далее «Открыть с помощью»). Можно выбрать программу из предлагаемого списка или попробовать открыть файл в произвольном приложении («Открыть с помощью» → «Другое приложение…»).

Предпочтительные приложения

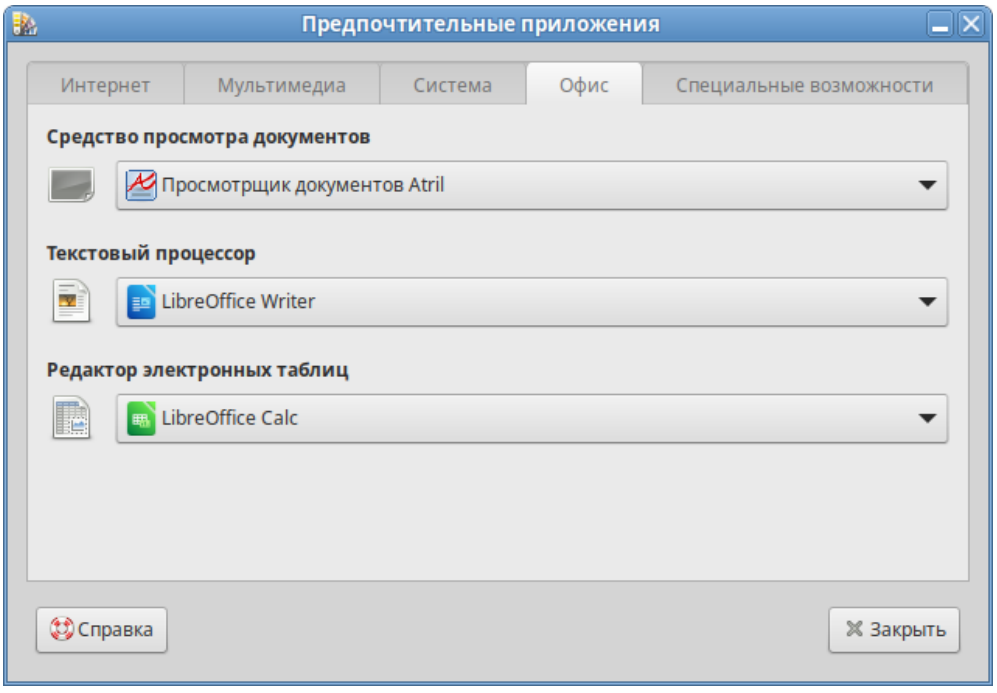

Рис. 28

Caja. Выбор приложения

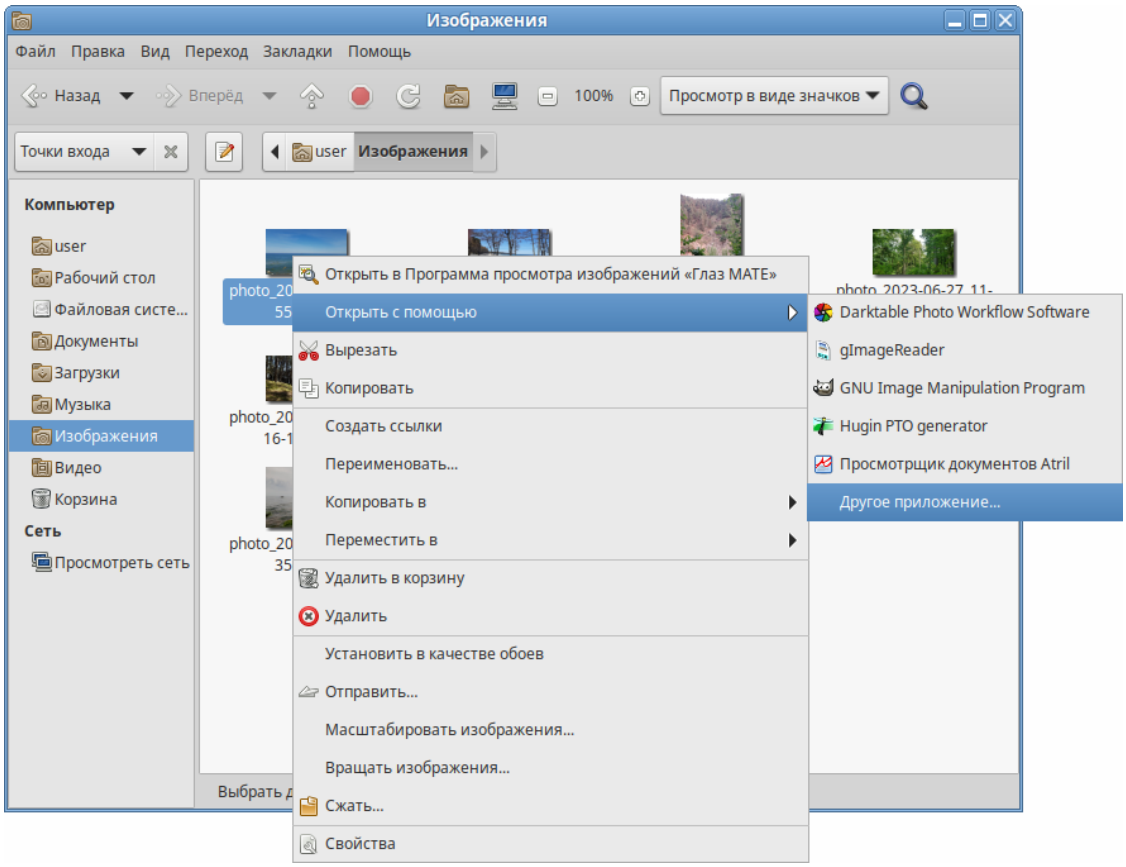

Рис. 29

3.5.1.6 Поиск файлов

В Caja можно выполнить поиск файлов по имени.

Панель поиска вызывается щелчком по значку лупы (<Ctrl>+<F>) (Рис. 30).

Caja. Вызов панели поиска

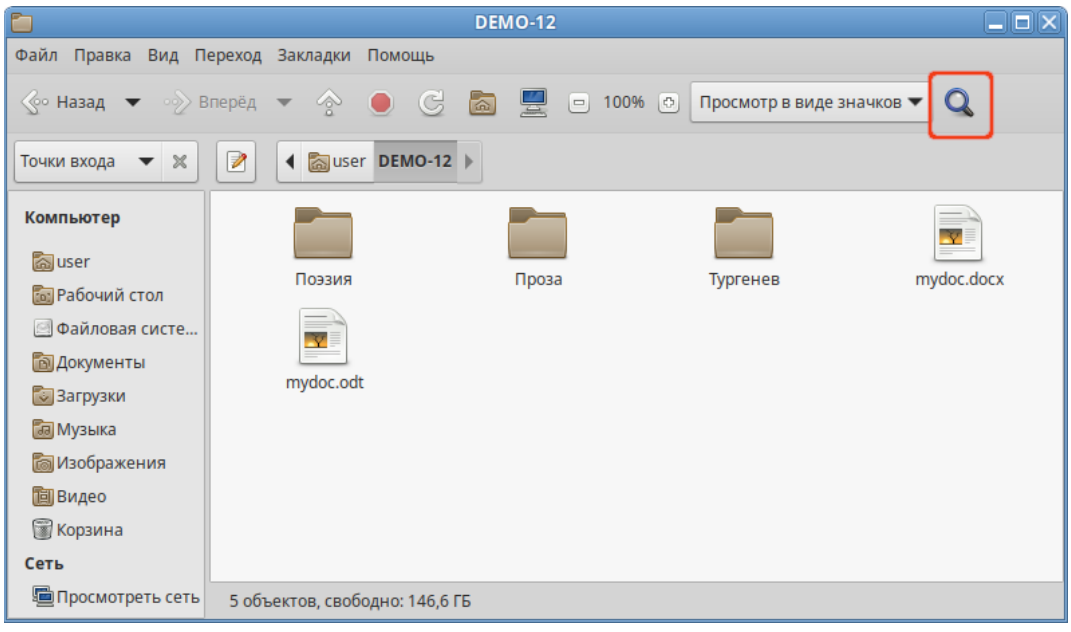

Рис. 30

Открывшаяся панель поиска по умолчанию настроена на поиск файлов в текущем каталоге и всех подкаталогах.

Для поиска следует ввести имя файла (часть имени) и щелкнуть по значку лупы (Рис. 31).

Caja. Панель поиска

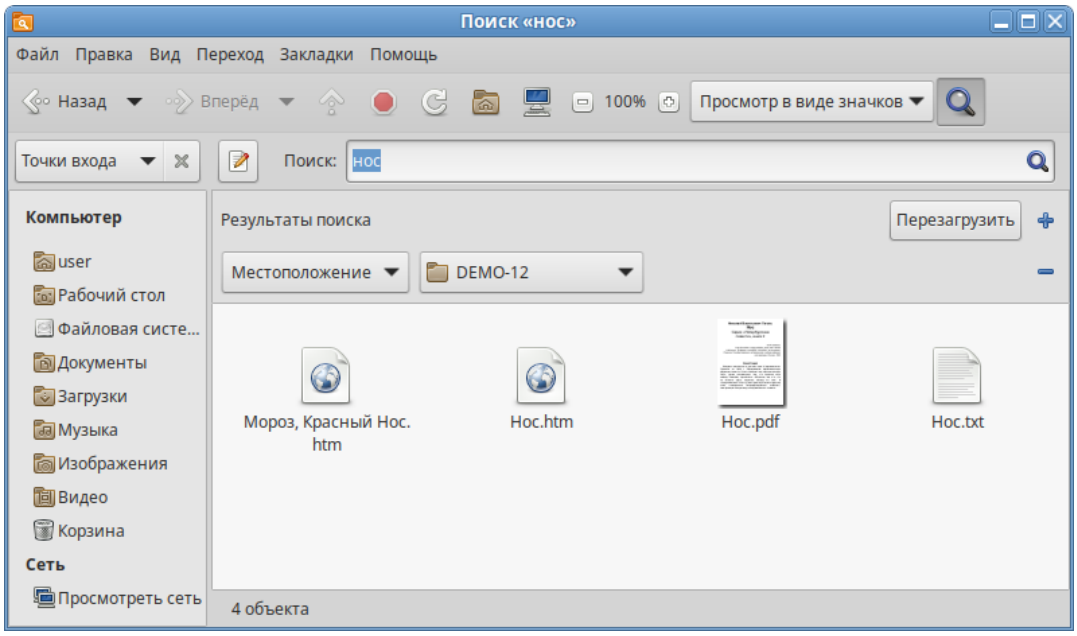

Рис. 31

Для сокращения результатов поиска дополнительно можно указать тип файлов (Рис. 32).

Caja. Параметры поиска

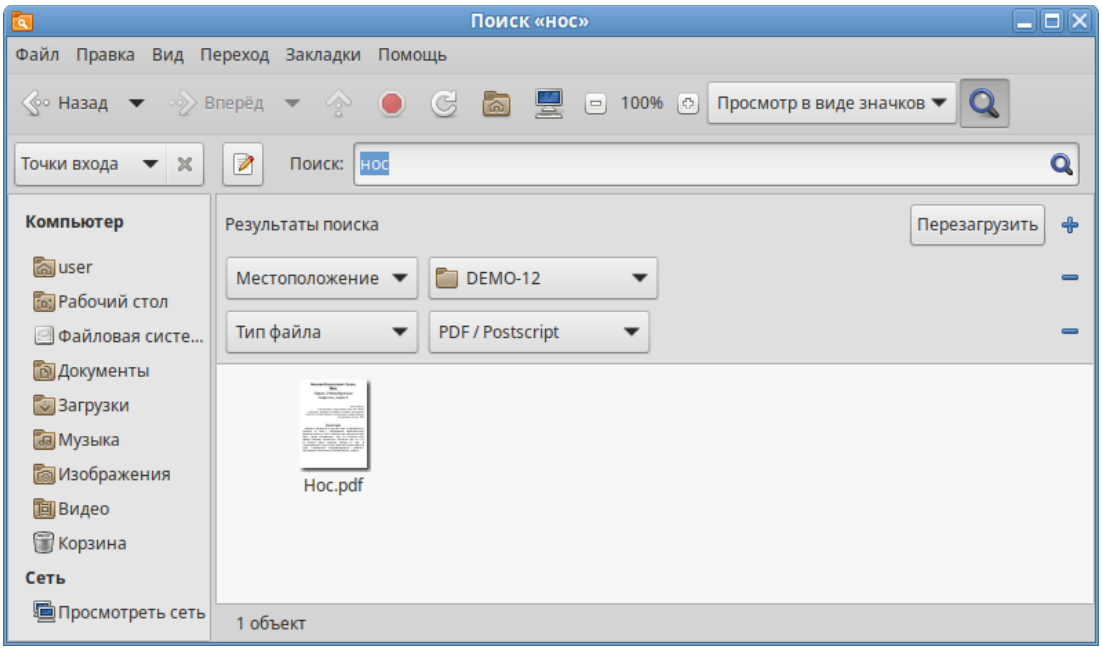

Рис. 32

Поиск нечувствителен к регистру. При поиске не используются подстановочные знаки или регулярные выражения.

Примечание. Полнотекстовый поиск по файлам с различными форматами можно осуществить в программе Recoll (см. Recoll – полнотекстовый поиск).

3.5.1.7 Использование сменных носителей

Файловый менеджер может совершать различные действия при появлении в системе съёмных носителей. Например, их подключение, открытие окна файлового менеджера для отображения их содержимого или запуск подходящего приложения для обработки (например, музыкального проигрывателя для аудио CD).

Подключить носитель – значит сделать его файловую систему доступной. При подключении носителя его файловая система присоединяется к вашей файловой системе в виде подкаталога.

В ОС «Альт Рабочая станция» настроено автоматическое подключение обнаруженных носителей, поэтому для подключения носителя, достаточно вставить его в подходящее устройство. Значок в виде носителя появится на рабочем столе. В окне файлового менеджера появится содержимое носителя (Рис. 33).

Содержимое USB-накопителя в окне Caja

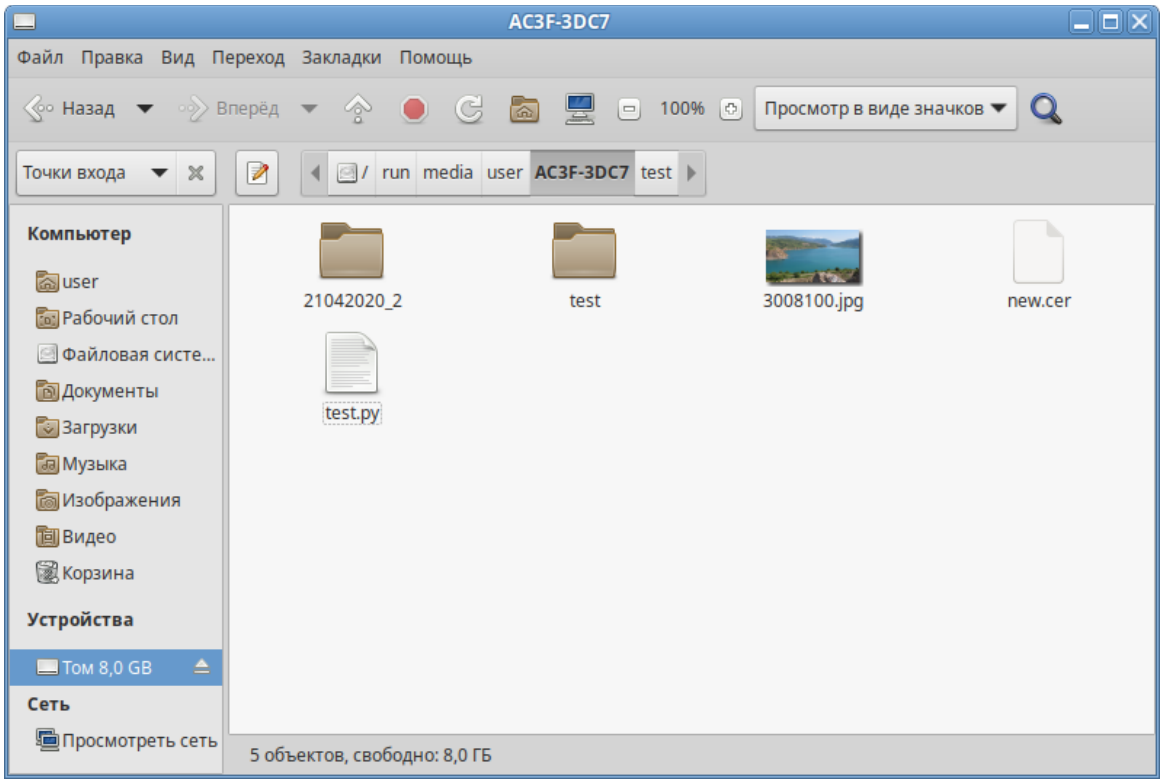

Рис. 33

Примечание. По умолчанию USB-накопители подключаются индивидуально для каждого пользователя (точка монтирования /run/media/<имя_пользователя>/).

Примечание. Если автоматического монтирования не произошло, следует убедиться, что на USB-накопитель не установлено ПО для защиты конфиденциальных данных, например, SecureDrive.

Для извлечения носителя необходимо сначала отключить его. Например, для извлечения USB-накопителя нужно выполнить следующие шаги:

1. Закрыть все окна диспетчера файлов, окна терминала и любые другие окна, осуществляющие доступ к USB-накопителю.
2. В контекстном меню носителя выбрать пункт «Извлечь» (Рис. 34).
3. Подождать, пока не исчезнет значок носителя (в окне файлового менеджера/с рабочего стола), затем извлечь носитель.

Извлечь носитель

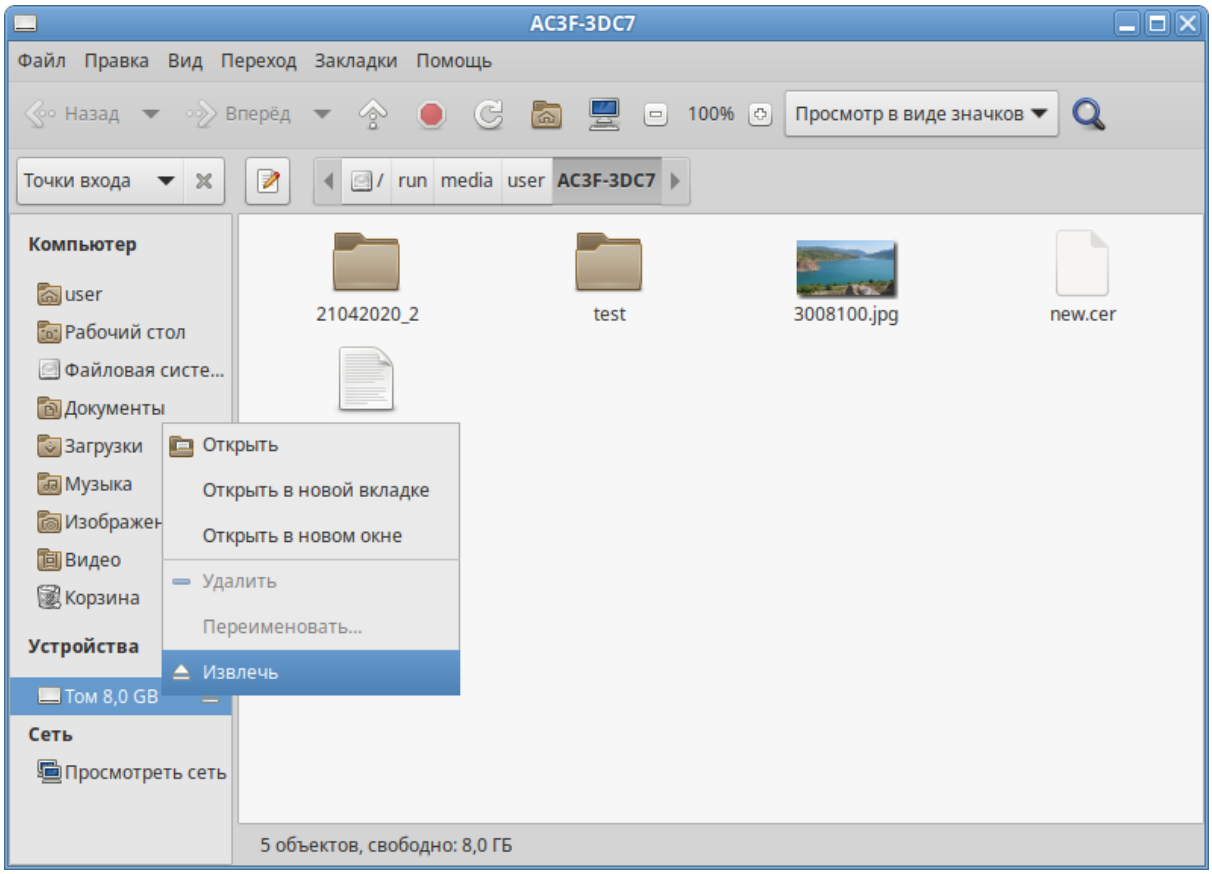

Рис. 34

3.5.1.8 Создание ресурсов общего доступа

Пользователи могут добавлять, изменять и удалять собственные ресурсы общего доступа. Эта возможность называется usershares и предоставляется службой Samba.

Примечание. Samba использует отдельную от системной базу данных пользователей. Для возможности доступа пользователя к папке (если запрещен гостевой доступ) необходимо внести его в базу данных Samba и установить пароль для доступа к общим ресурсам (он может совпа-

дать с основным паролем пользователя). Следует учитывать, что в базу данных Samba можно добавлять только тех пользователей, которые уже есть в системе.

Добавить пользователя в базу данных Samba можно, выполнив команду:

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

Можно создать отдельного пользователя, которому разрешить только доступ к Samba-ресурсам и запретить полноценный вход в систему:

```
# useradd user_samba -d /dev/null -s /sbin/nologin
# smbpasswd -a user_samba
```

Чтобы предоставить общий доступ к папке, нужно в контекстном меню папки выбрать пункт «Опции публикации», затем в открывшемся окне отметить пункт «Опубликовать эту папку», настроить параметры публикации (Рис. 35) и нажать кнопку «Создать публикацию».

Разрешить общий доступ к папке

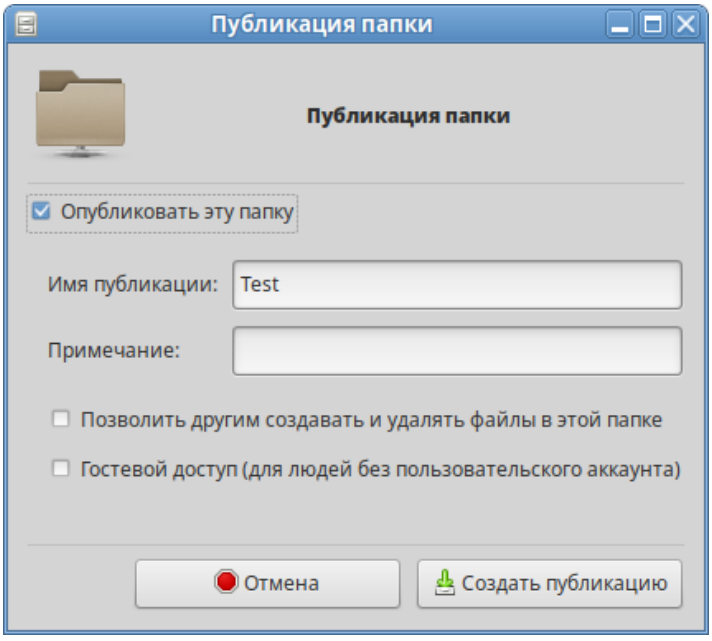

Рис. 35

Общие папки будут отображаться в разделе «Просмотреть сеть» файлового менеджера (Рис. 36). Для подключения к общей папке можно указать в адресной строке файлового менеджера протокол и адрес компьютера (smb://<имя_сервера> или smb://<IP_сервера>) и нажать клавишу <Enter>.

Примечание. Домашняя папка пользователя по умолчанию не отображается в списке доступных общих ресурсов в сетевом окружении. Обращение к домашней папке выполняется по имени пользователя. Например, для получения доступа к домашней папке пользователя user на компьютере с IP-адресом 192.168.0.192, необходимо указать в адресной строке smb://192.168.0.192/user (Рис. 37). Для возможности получения доступа к домашней папке по сети, необходимо добавить каждого локального пользователя в список пользователей Samba.

Ресурсы с общим доступом

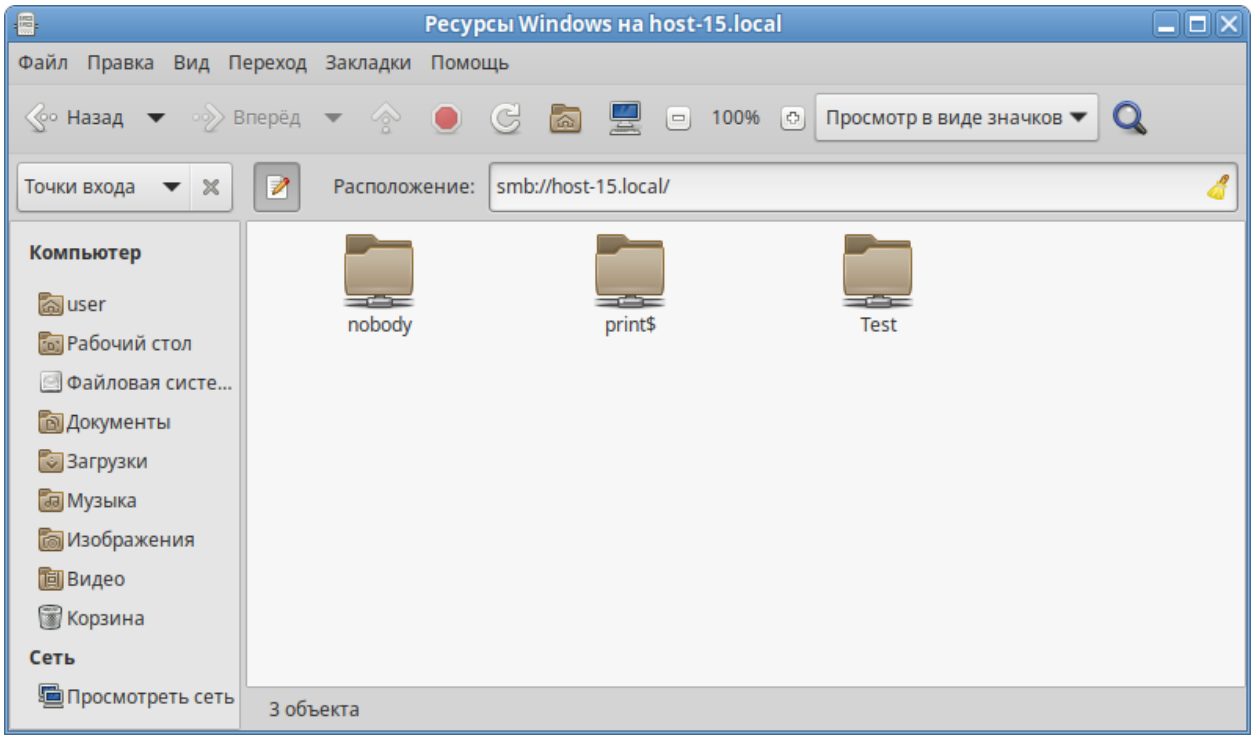

Рис. 36

Обращение к домашней папке пользователя user по сети

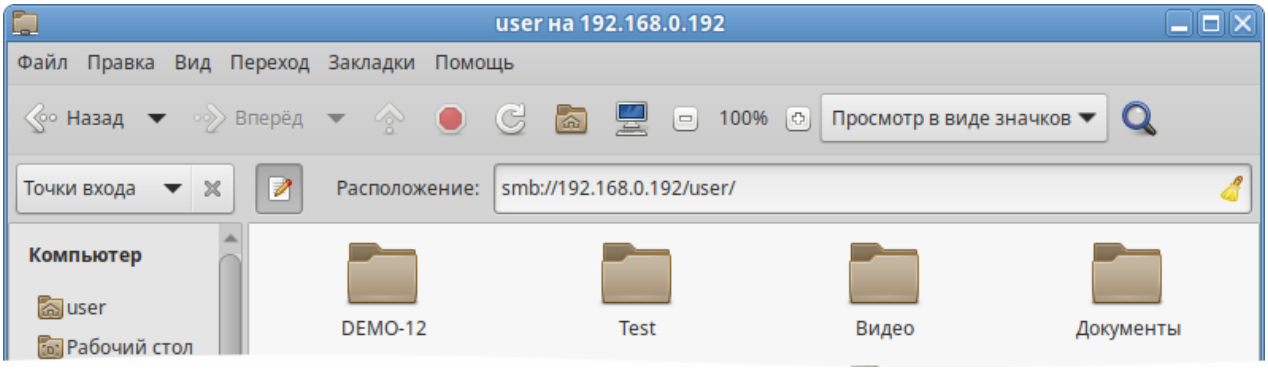

Рис. 37

Для доступа к папке, к которой запрещен гостевой доступ, необходимо указать имя и пароль пользователя Samba, и нажать кнопку «Подключиться» (Рис. 38).

После подключения к общей папке, и она появится на боковой панели в разделе «Сеть». Для добавления постоянной ссылки на сетевую папку следует выделить подключенную папку в разделе «Сеть» и в меню выбрать пункт «Закладки» → «Добавить закладку» (Рис. 39). В результате на боковой панели в разделе «Закладки» появится постоянная ссылка на сетевую папку.

Параметры подключения к общей папке

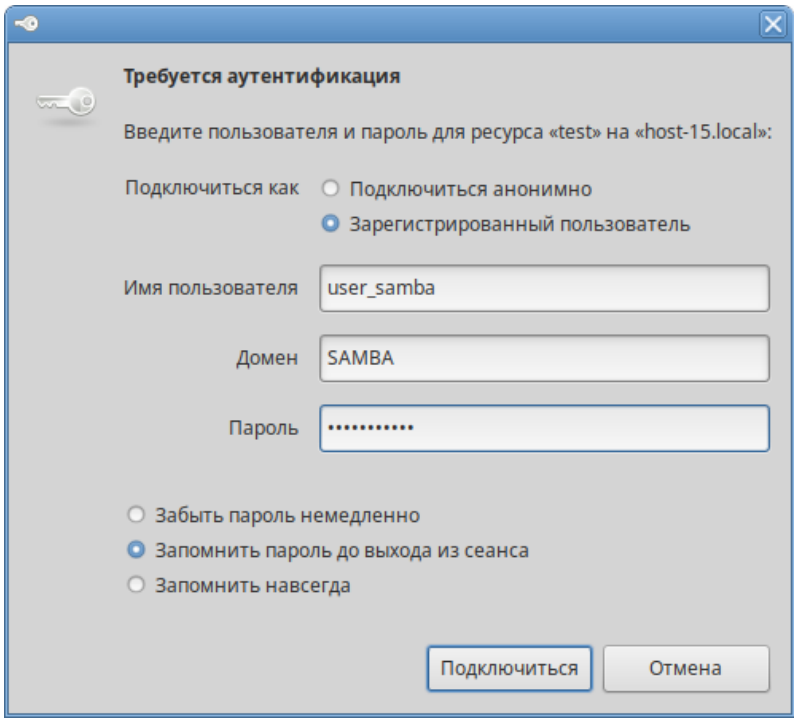

Рис. 38

Добавление закладки на сетевую папку

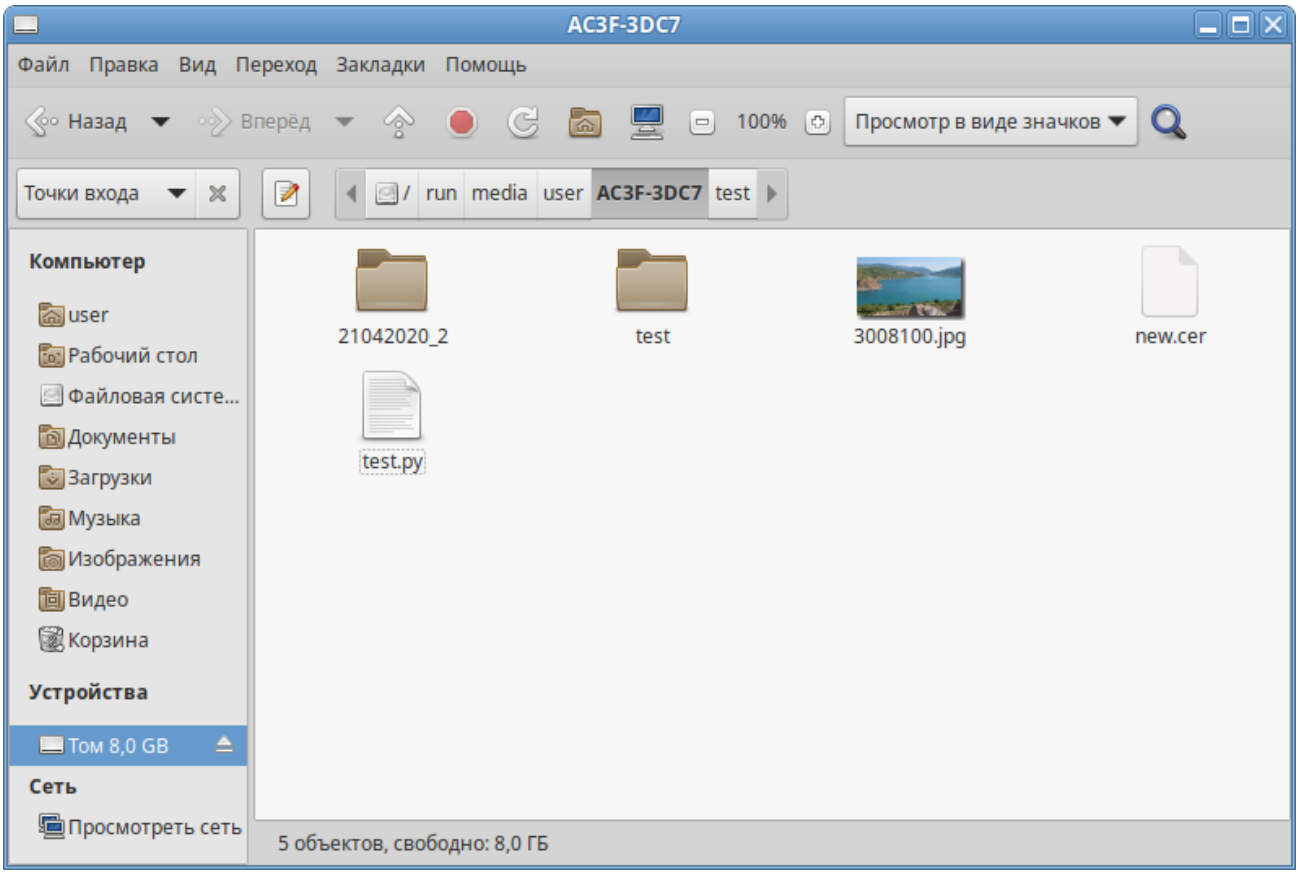

Рис. 39

3.6 Графика

ОС «Альт Рабочая станция» предлагает приложения для работы с растровой и векторной графикой. Выбор пользователя зависит как от личных предпочтений, так и от задач, которые он собирается решать, будь то простой просмотр графических файлов или, например, создание профессиональных макетов.

3.6.1 Графический редактор GIMP

GIMP (GNU Image Manipulation Program) – графический редактор, предназначенный для работы с растровой графикой. Одной из сильных сторон GIMP является его доступность для многих операционных систем.

GIMP пригоден для решения множества задач по изменению изображений. Типичные задачи, которые можно решать при помощи GIMP, включают в себя создание графики и логотипов, масштабирование и кадрирование фотографий, раскраску изображений, комбинирование изображений с использованием слоёв, ретуширование и преобразование изображений в различные форматы.

Главное окно GIMP (Рис. 40) содержит меню основных функций, панель инструментов и области, в которых отображаются текущие значения основного и фонового цветов, формы кисти, текущего градиента. Окна изображения соответствуют отдельным открытым графическим файлам (или слоям в них).

GIMP

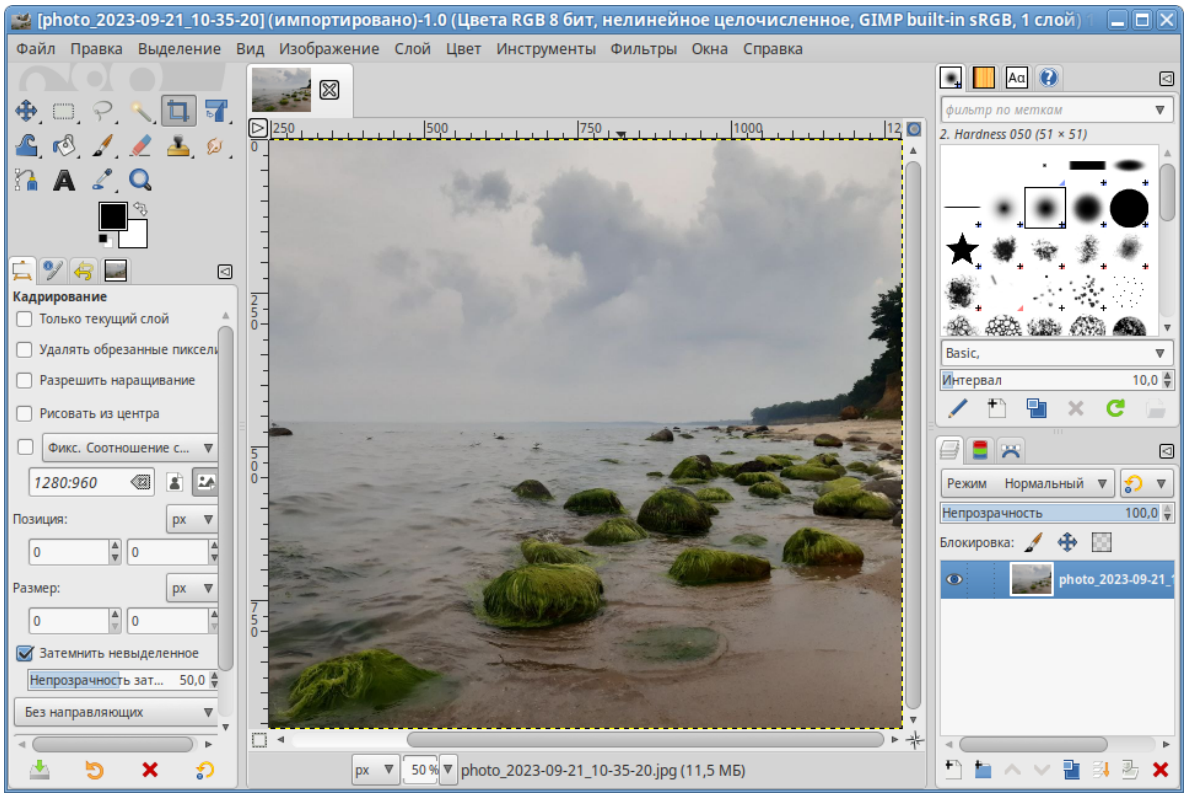

Рис. 40

Основная функциональность, доступная через «Инструменты» в главном окне, достаточно традиционна для программ этого класса. Она включает:

- выделение области изображения (прямоугольной, эллиптической или произвольной формы). Последовательно выделяемые области могут образовывать пересечения, объединения или вычитания;
- выделение смежных областей с заданием параметров выделения;
- перемещение, заливку выделенных областей;
- кадрирование (обрезку) изображения;
- изменение масштаба отображения на экране;
- вращение, масштабирование, искривление и зеркальное отображение изображения;
- ввод текста;
- выбор текущего цвета («Пипетка»);
- заливку области сплошным цветом или градиентом;
- рисование – «Карандаш» или «Кисть» произвольной формы;
- очистку («Ластик»).

В базовую функциональность GIMP входит также возможность захвата изображения со сканера и с экрана.

3.6.2 Векторный редактор Inkscape

Inkscape – мощный и удобный инструмент для создания художественных и технических иллюстраций в формате векторной графики (Рис. 41), полностью совместимый со стандартами XML, SVG и CSS. Редактор отличается широким набором инструментов для работы с цветами и стилями (выбор цвета, копирование цвета, копирование/вставка стиля, редактор градиента, маркеры контура).

В Inkscape поддерживаются все основные возможности SVG: контуры, текст, маркеры, клоны, альфа-канал, трансформации, градиенты, текстуры и группировка. Inkscape также поддерживает метаданные Creative Commons, правку узлов, слои, сложные операции с контурами, векторизацию растровой графики, редактирование текста прямо на изображении, заверстанный в фигуру текст.

Inkscape

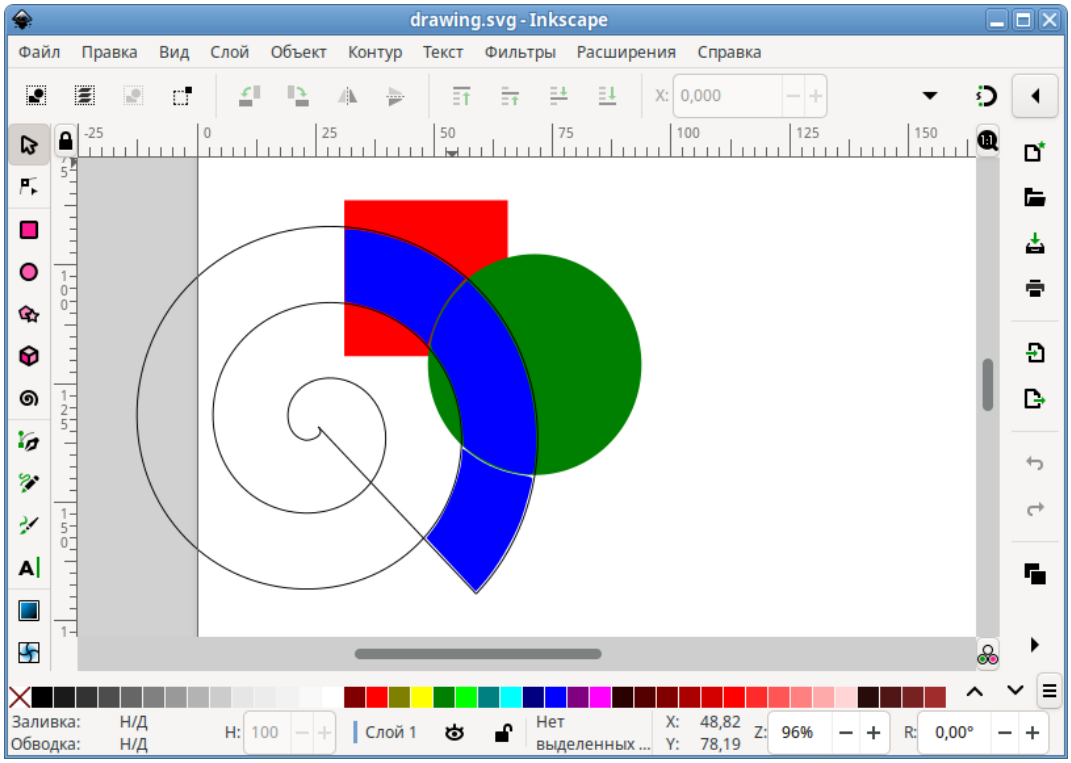

Рис. 41

3.6.3 Программа для распознавания текста gImageReader

gImageReader программа для распознавания текста (GUI Tesseract).

Особенности gImageReader:

- поддерживаемые форматы изображений: jpeg, png, tiff, gif, pnm, pcx, bmp;
- поддержка формата электронных документов PDF. Возможность выбрать отдельные страницы и диапазон страниц для распознавания;
- автоматическое обнаружение расположения страницы;
- выделение области с текстом для распознавания;
- получение изображения напрямую со сканера. Настройка разрешения, сохранение в формат png;
- проверка орфографии.

gImageReader можно применять без подключённого сканера и распознавать текст из имеющегося снимка (Рис. 42). gImageReader поддерживает автоматическое определение макета страницы, при этом пользователь может вручную определить и настроить регионы распознавания. Приложение позволяет импортировать изображения с диска, сканирующих устройств, буфера обмена и скриншотов. gImageReader также поддерживает многостраничные документы PDF.

Окно программы gImageReader

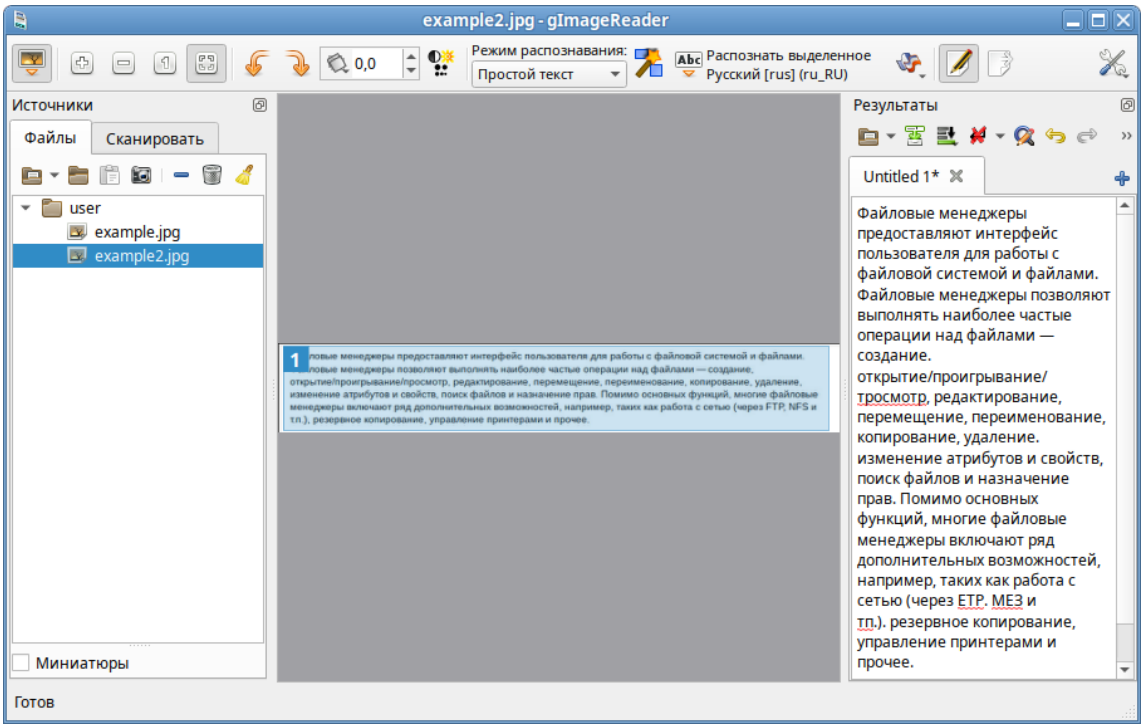

Рис. 42

Распознанный текст отображается непосредственно рядом с изображением. Базовое редактирование текста включает поиск/замену и удаление сломанных строк, если это возможно. Поддерживается проверка орфографии для выводимого текста, если установлены соответствующие словари.

gImageReader имеет возможности прямого получения изображения со сканера, но при этом отсутствует операция предварительного сканирования.

Для работы со сканером следует перейти на вкладку «Сканировать» («Acquire») в боковой панели, выбрать сканер из списка подключенных устройств, указать имя и расположение файла получаемого изображения, выбрать цветовой режим и разрешение (для наилучших результатов разрешение при сканировании должно быть не меньше 300 DPI).

После нажатия на кнопку «Отсканировать» («Scan») начнется процесс сканирования изображения, и при его завершении новое изображение появится в области просмотра (Рис. 43).

3.6.4 Xsane

Программа Xsane является удобным средством, как для сканирования отдельных изображений, так и для организации пакетного (многостраничного) сканирования.

При запуске программы сканирования изображений производится автоматический опрос доступных сканеров (устройств захвата изображений) и предлагается выбрать устройство для работы. Если к компьютеру не подключено ни одного сканера, то будет выдана соответствующая ошибка, затем программа будет закрыта.

Сканирование в окне программы gImageReader

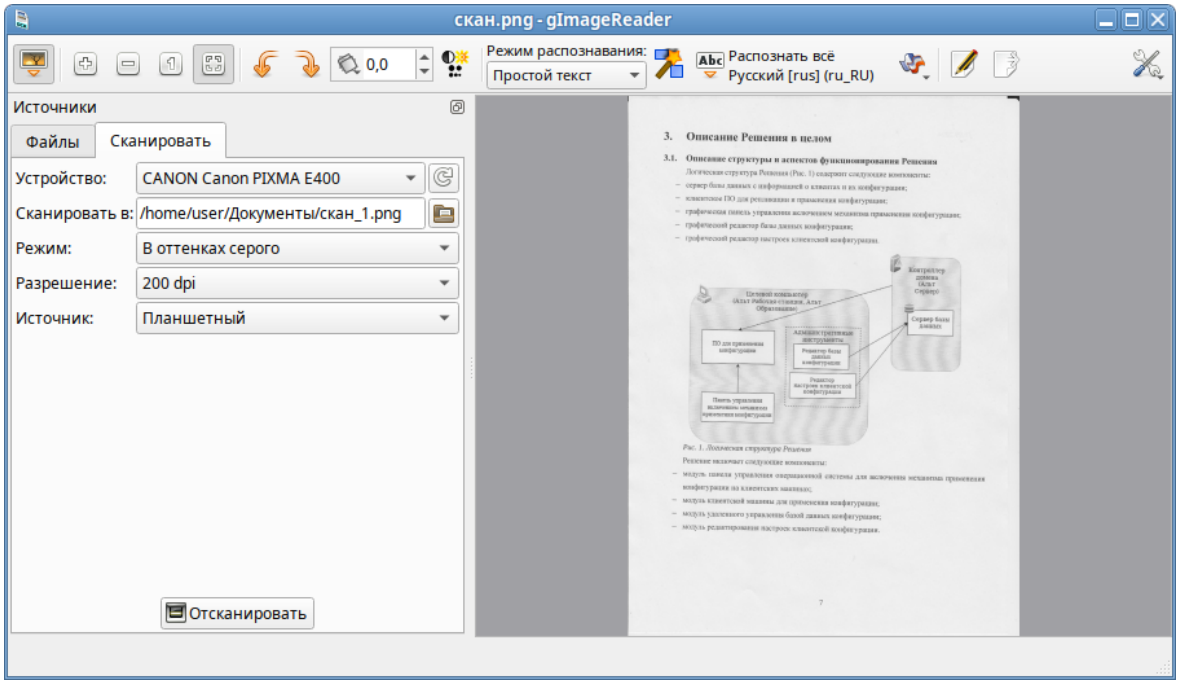

Рис. 43

Если программа нашла подключенный к системе сканер, будет открыт основной интерфейс приложения Xsane (Рис. 44).

Интерфейс приложения Xsane

Рис. 44

Предварительное сканирование выполняется в окне предварительного просмотра путём нажатия кнопки «Предварительное сканирование».

Пунктирная линия в окне предварительного сканирования показывает на выбранную по умолчанию область сканирования. Определить область сканирования можно, выделив её при помощи мыши.

При сканировании в итоговое изображение попадёт лишь область, ограниченная настройками предварительного сканирования.

Для сканирования отдельного изображения в программе Xsane необходимо:

- выбрать в основном окне имя и формат файла (если в поле «Назначение» выбрано значение «Сохранение»), режим сканирования и разрешение, а также выставить при необходимости гамму, яркость и контрастность;
- в окне предварительного просмотра нажать кнопку «Предварительное сканирование»;
- после завершения процесса предварительного сканирования, выделить мышью область для сканирования;
- в основном окне программы нажать кнопку «Сканировать»;
- после завершения процесса сканирования (если в поле «Назначение» было выбрано значение «Средство просмотра»), в окне просмотра (Рис. 45) можно воспользоваться инструментами преобразования изображений (поворот, отражение, масштабирование и т.п.) и затем сохранить скорректированную сканкопию.

Результат сканирования в окне просмотра

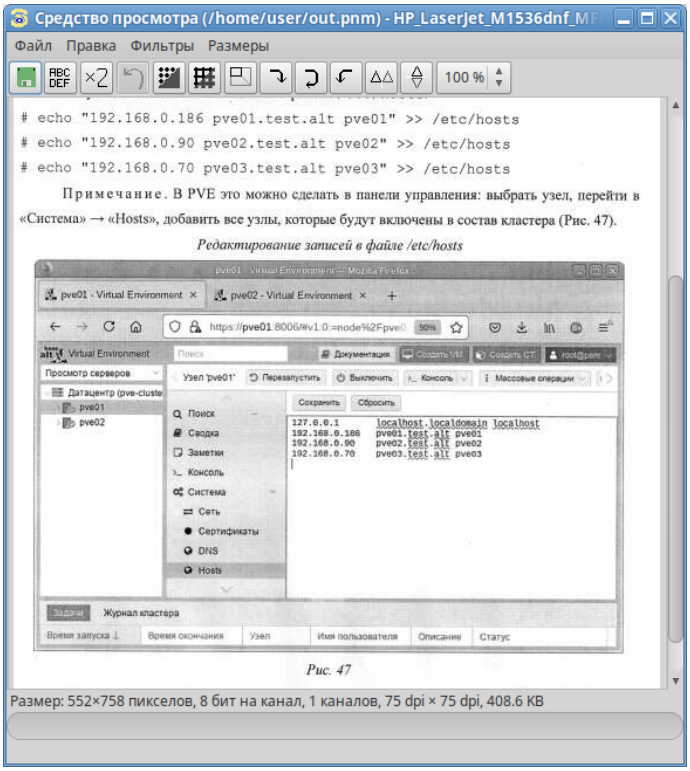

Рис. 45

Xsane предоставляет возможность создать многостраничный документ, минуя промежуточный этап сохранения страниц в виде отдельных графических файлов и использования вспомогательных утилит. Возможно создание документа в формате pdf, tiff или PostScript.

Для сканирования в Xsane с созданием многостраничного документа необходимо:

- в основном окне Xsane выбрать назначение сканирования «Многостраничный» (Рис. 46);
- в открывшемся окне «Многостраничный проект», ввести имя создаваемого многостраничного файла и нажать кнопку «Создать проект» (Рис. 47);
- перейти в окно «Предварительный просмотр» и отметить область сканирования (если это необходимо);
- в основном окне программы, нажать кнопку «Сканировать» (рекомендуется в поле «Число страниц для сканирования» оставить 1 и каждый раз нажимать «Сканировать» для сканирования следующей страницы);
- после завершения сканирования всех страниц перейти в окно «Многостраничный проект». В нем отражаются имена файлов, соответствующих отдельным страницам документа. Каждый из этих файлов можно просмотреть, отредактировать, переместить по отношению к другим страницам, или удалить (Рис. 48);
- выбрать тип многостраничного документа (pdf, tiff или PostScript) в соответствующем выпадающем списке и нажать кнопку «Сохранить многостраничный файл».

Xsane. Настройки сканирования

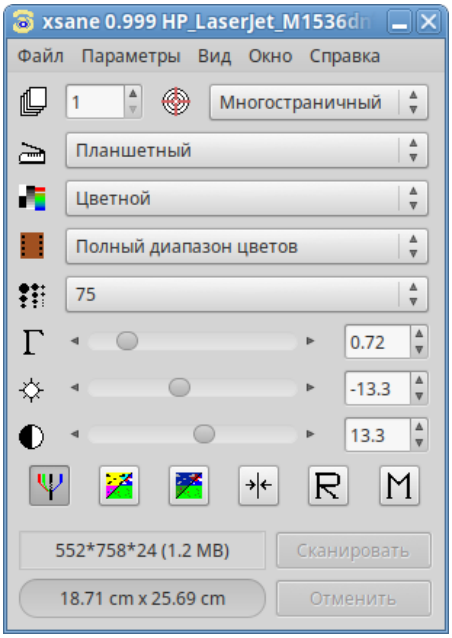

Рис. 46

Xsane. Создание многостраничного документа

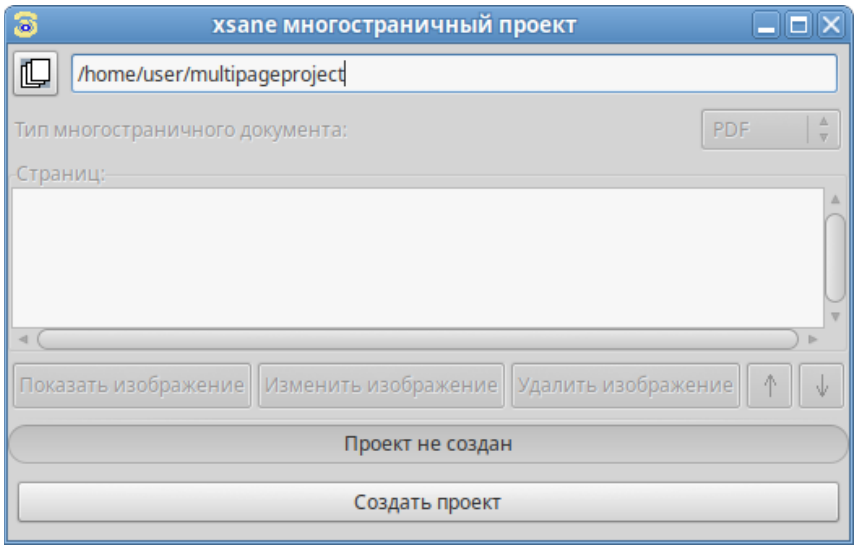

Рис. 47

Xsane. Многостраничный проект

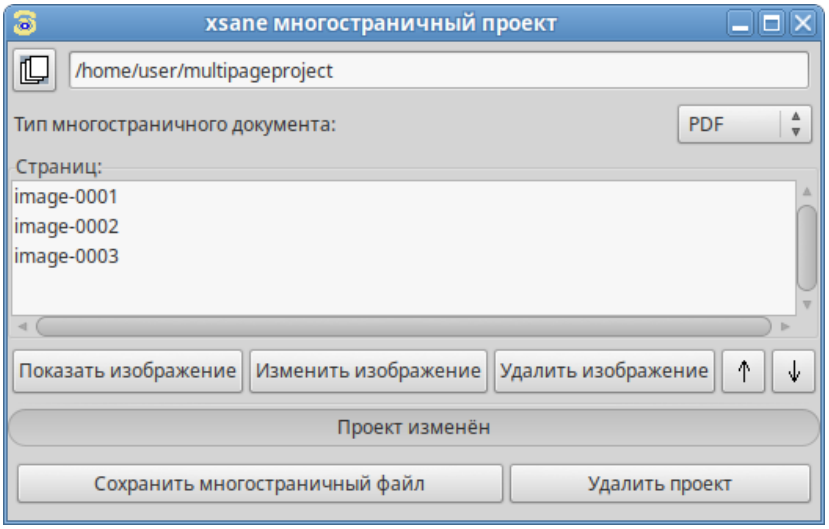

Рис. 48

3.6.5 Глаз MATE

Глаз MATE является простым приложением для просмотра изображений. После загрузки изображения (Рис. 49) можно увеличивать его масштаб, вращать изображение, а также просматривать другие изображения из каталога, в котором находится открытое изображение.

3.7 Менеджер архивов Engrampa

Менеджер архивов можно использовать для создания, просмотра, изменения и распаковки архивов. Архив – это файл, служащий контейнером для других файлов. Архив может содержать множество файлов, папок и подпапок обычно в сжатом виде.

Окно программы Глаз MATE

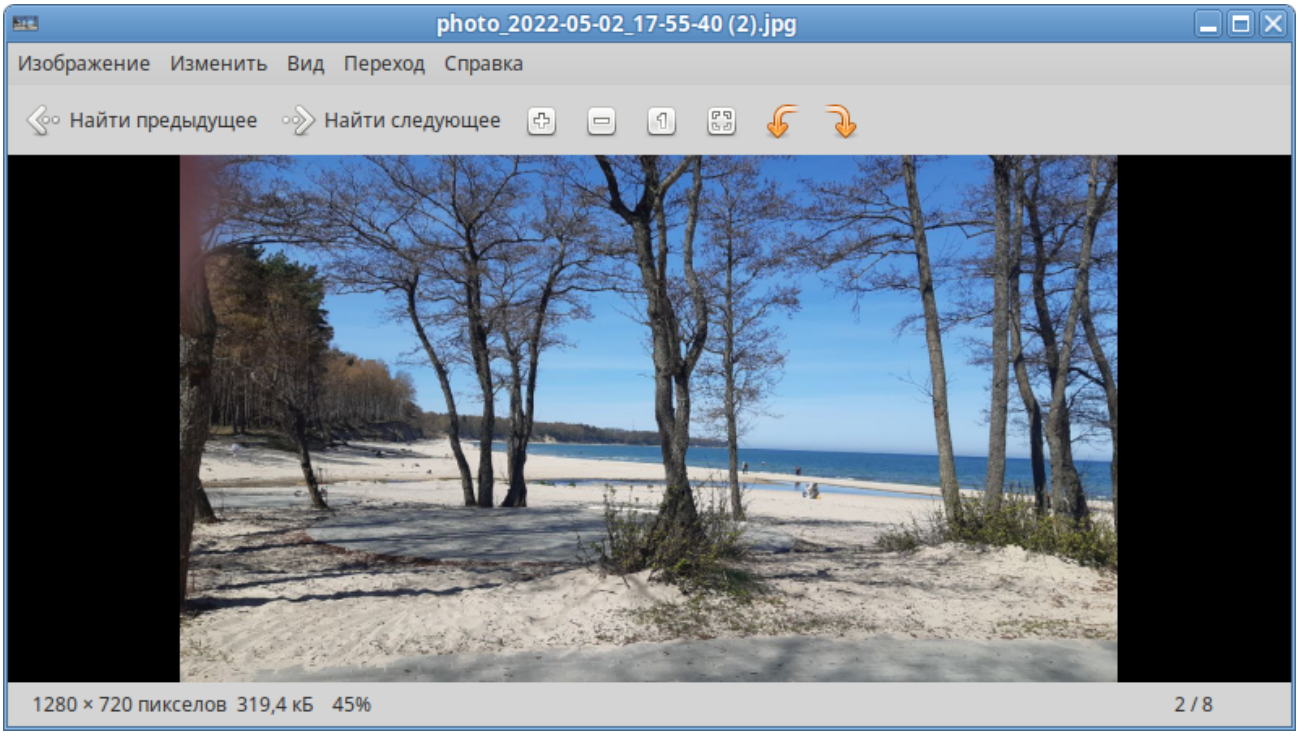

Рис. 49

Менеджер архивов поддерживает, в числе прочих, следующие форматы архивов (должны быть установлены соответствующие инструменты командной строки):

- архив 7-zip – .7z;
- образ компакт-диска – .iso (только чтение);
- архив RAR (Roshal ARchive) – .rar (только чтение);
- архив Tar – .tar;
- архив Tar, сжатый bzip – tar.bz или .tbz;
- архив Tar, сжатый bzip2 – tar.bz2 или .tbz2;
- архив Tar, сжатый gzip – tar.gz или .tgz;
- архив Tar, сжатый xz – tar.xz;
- архив Zip – .zip.

Менеджер архивов автоматически определяет тип архива и отображает (Рис. 50):

- имя архива в заголовке окна;
- содержимое архива в области отображения;
- число файлов и папок (объектов) в текущем местоположении и их размер (в распакованном виде) в строке состояния.

Менеджер архивов Engrampa

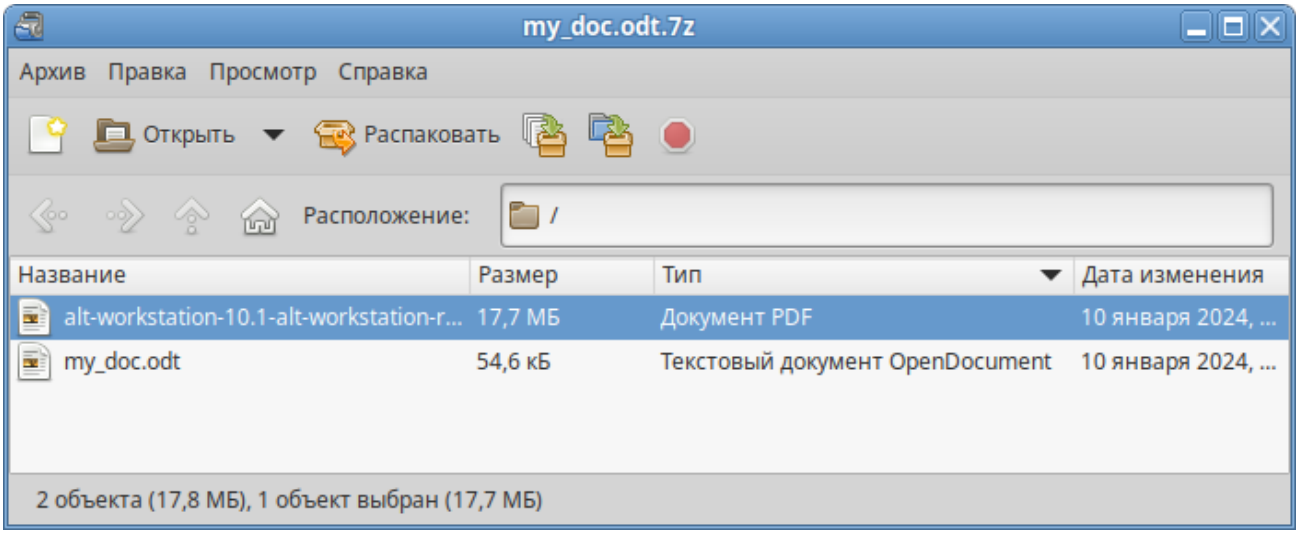

Рис. 50

3.7.1 Использование файлового менеджера для работы с архивом

Файловый менеджер можно использовать для добавления файлов в архив или для извлечения файлов из архива.

Для добавления файла/каталога в архив необходимо:

- в контекстном меню файла/каталога, выбрать пункт «Сжать» (Рис. 51);
- в открывшемся окне необходимо ввести имя архива, выбрать из выпадающего списка тип архива, выбрать место для хранения архива и нажать кнопку «Создать» (Рис. 52).

Добавление файлов в архив

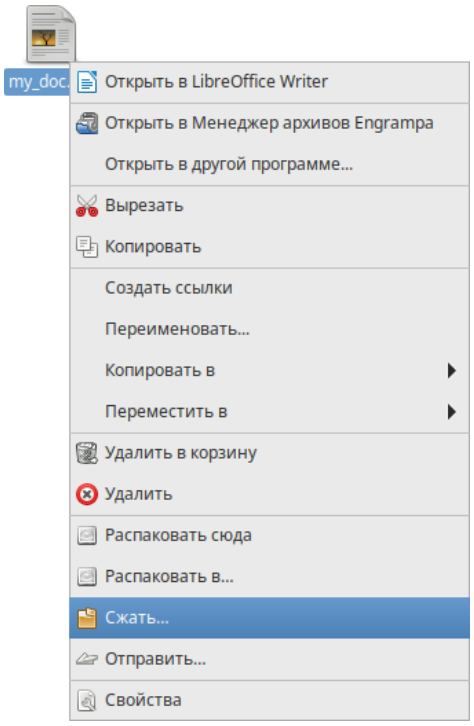

Рис. 51

Создание архива

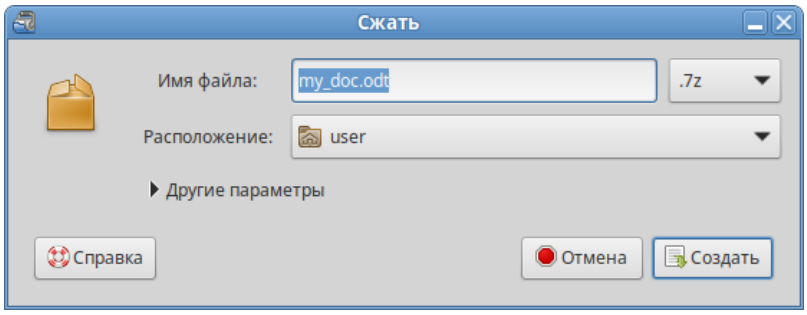

Рис. 52

При создании нового архива можно указать дополнительные параметры, раскрыв пункт «Другие параметры» в окне создания архива. Можно указать следующие дополнительные параметры (Рис. 53):

- «Пароль» – пароль, который будет использоваться для шифрования (не все типы архивов поддерживают шифрование). Если пароль не указан, архив не будет зашифрован;
- «Шифровать также список файлов» – пароль будет запрашиваться даже для просмотра списка файлов, содержащихся в архиве, в противном случае он будет использоваться только для извлечения файлов из архива;
- «Разделить на тома размером» – позволяет разбить архив на несколько файлов указанного размера. Только 7-Zip архивы поддерживают эту функцию.

Дополнительные параметры

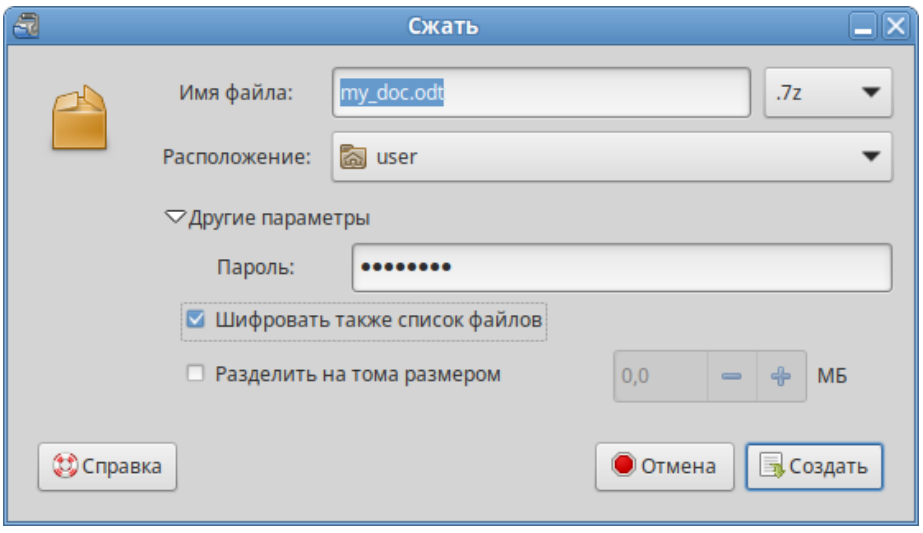

Рис. 53

Для того чтобы извлечь файлы из архива, следует в контекстном меню архива выбрать пункт «Распаковать сюда» (Рис. 54) – файлы будут распакованы в текущий каталог, или «Распаковать в...» – можно указать каталог, куда будут извлечены файлы.

Извлечение файлов из архива

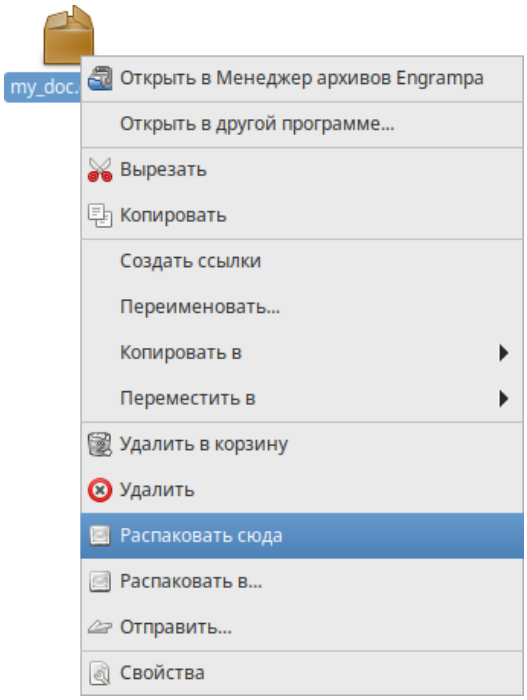

Рис. 54

3.8 Системный монитор

Приложение «Системный монитор» отображает список всех запущенных приложений, а также, сколько каждое из них занимает процессорного времени и оперативной памяти.

Для запуска «Системного монитора» следует выбрать пункт «Меню MATE» → «Приложения» → «Системные» → «Системный монитор MATE».

Вся информация распределена по четырем вкладкам:

- во вкладке «Система» выводится базовая информация о системе;
- вкладка «Процессы» позволяет просматривать и управлять запущенными процессами. Каждый процесс можно приостановить, остановить, изменить приоритет и выполнить некоторые другие действия;
- во вкладке «Ресурсы» (Рис. 55) в реальном времени выводится информация о ресурсах (в виде графиков) – использование процессора (CPU), использование оперативной памяти (RAM) и файла подкачки (SWAP), а также использование сети;
- во вкладке «Файловые системы» можно просматривать информацию о файловых системах.

При щелчке правой кнопкой мыши по любому запущенному процессу открывается контекстное меню (Рис. 56), с помощью которого можно завершить «зависшее» приложение, остановить, перезапустить и даже изменить его приоритет времени, что позволит регулировать допустимый объем требований к системным ресурсам.

Системный монитор

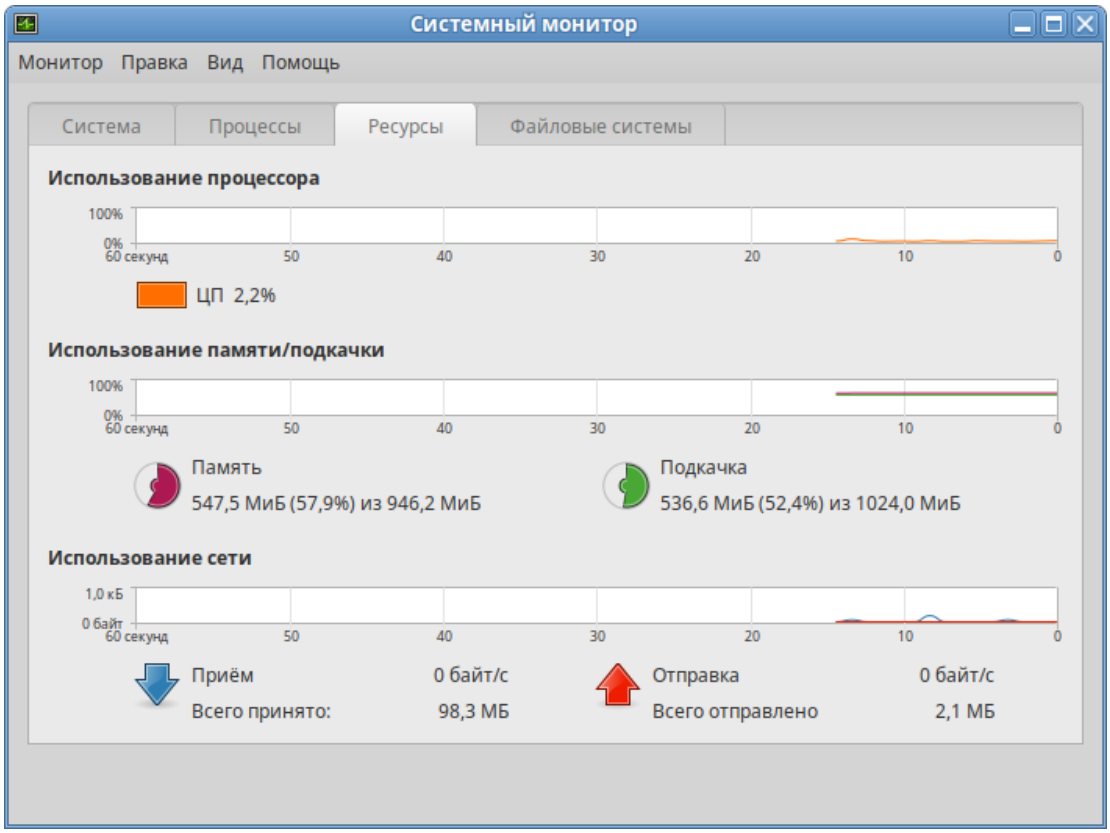

Рис. 55

Контекстное меню процесса

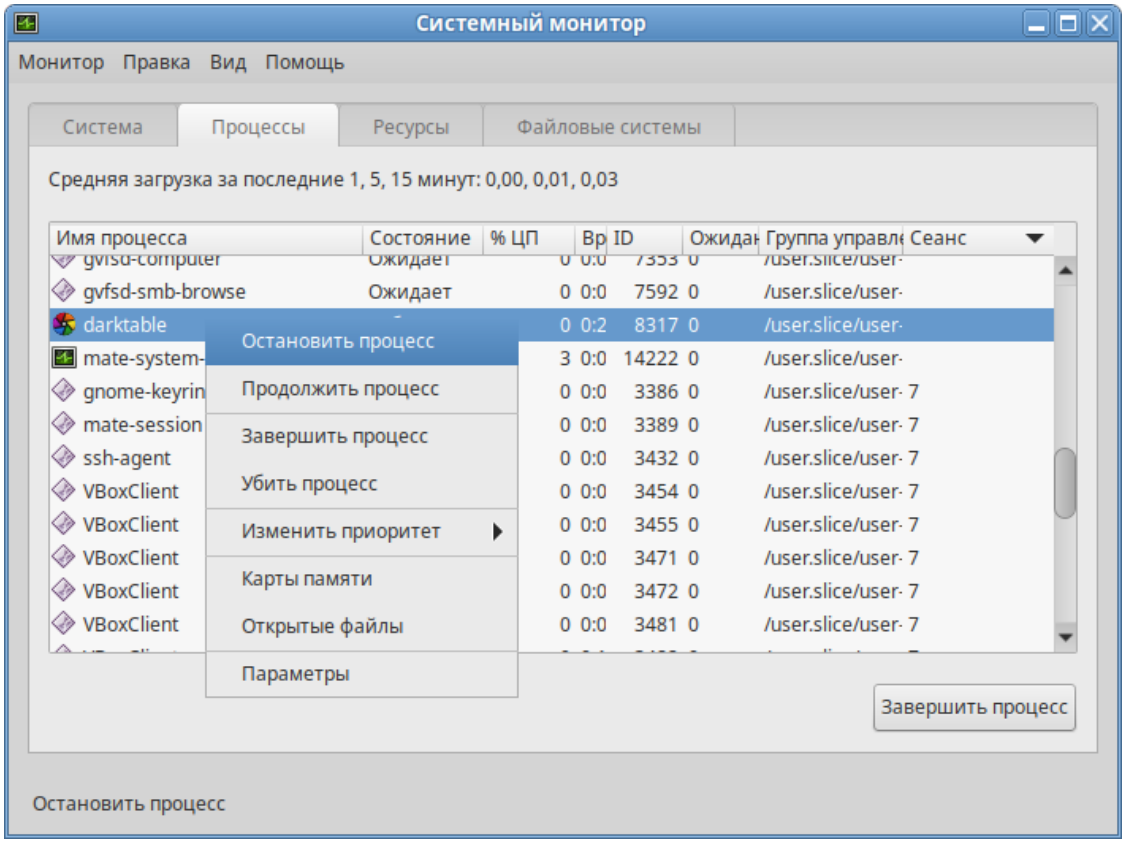

Рис. 56

Для изменения приоритета процесса необходимо:

- выбрать вкладку «Процессы», чтобы отобразить список процессов;
- выбрать процесс, приоритет которого следует изменить;
- в контекстном меню процесса выбрать пункт «Изменить приоритет» (Рис. 57);
- если выбрать пункт «Вручную», откроется диалоговое окно «Изменить приоритет процесса...» (Рис. 58), здесь можно использовать ползунок, чтобы установить уровень приоритета. Приоритет процесса задается уровнем nice. Меньшее значение nice соответствует более высокому приоритету;
- нажать кнопку «Изменить приоритет».

Изменение приоритета процесса

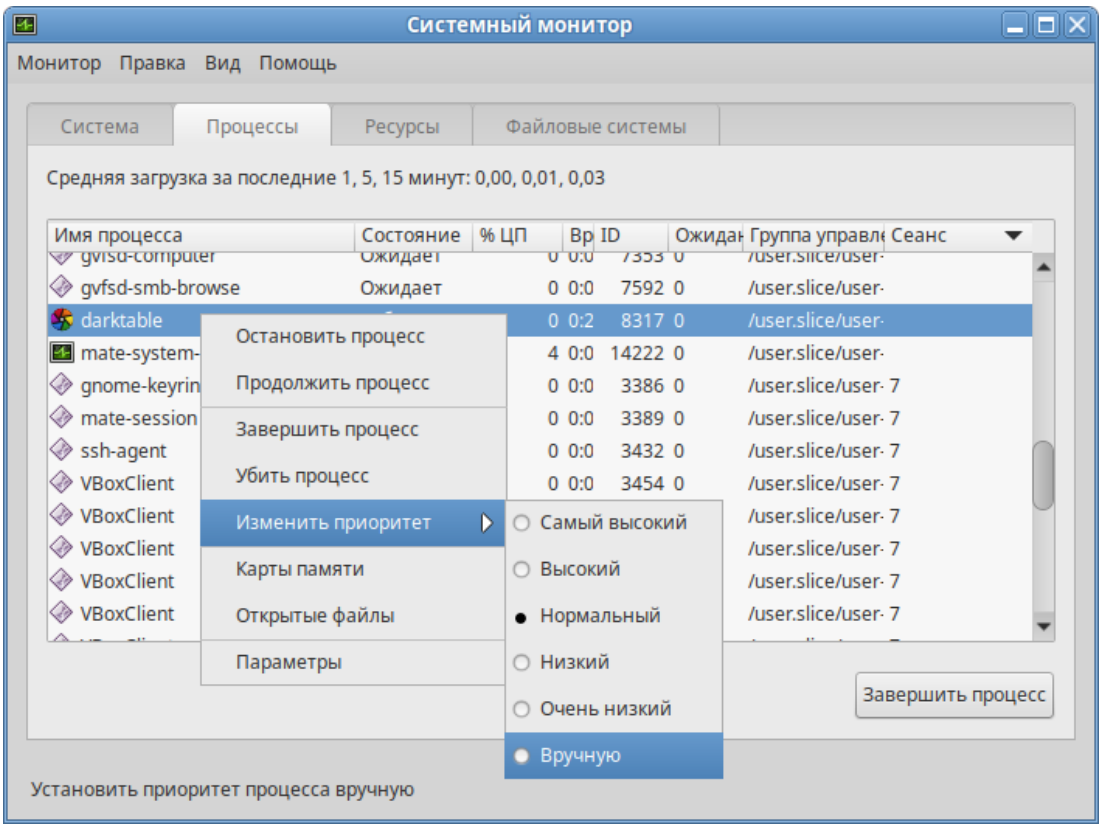

Рис. 57

Диалоговое окно «Изменить приоритет процесса...»

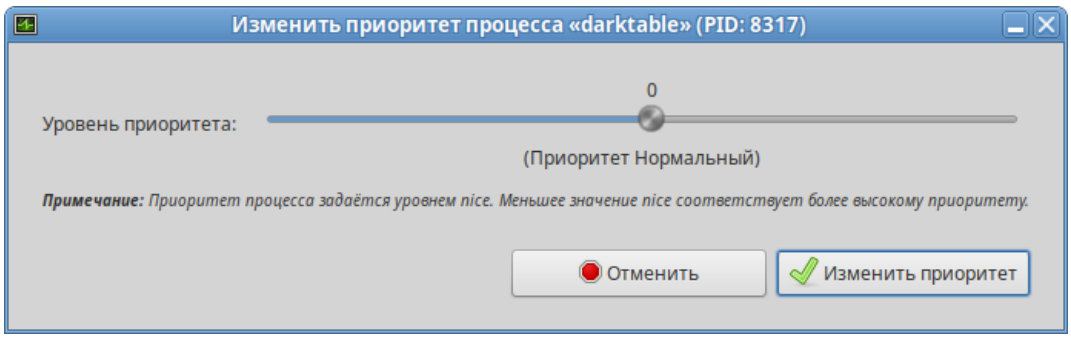

Рис. 58

Примечание. Для установки более высокого приоритета, чем тот, который уже установлен у процесса, потребуется ввести пароль пользователя root.

3.9 Центр приложений

Центр приложений позволяет легко устанавливать и удалять программы из репозиториев Альт, совместимых с вашим дистрибутивом, и сторонних приложений в формате Flatpak. Центр приложений позволяет выполнять поиск по названиям и описаниям среди доступных приложений.

Примечание. Flatpak – система для создания, распространения и запуска изолированных настольных приложений в Linux. Приложения flatpak устанавливаются из репозитория flathub.

Примечание. Для возможности установки приложений из репозитория flathub пользователям, не входящим в группу wheel, следует разрешить для всех доступ к инструментам монтирования файловых систем fuse:

```
# control fusermount public
```

Для запуска «Центра приложений» следует выбрать пункт «Меню MATE» → «Приложения» → «Системные» → «Центр приложений».

Вся информация распределена по двум вкладкам (Рис. 59):

- на вкладке «Обзор» показаны доступные приложения;
- вкладка «Установлено» позволяет просматривать и удалять установленные приложения (Рис. 60).

Центр приложений

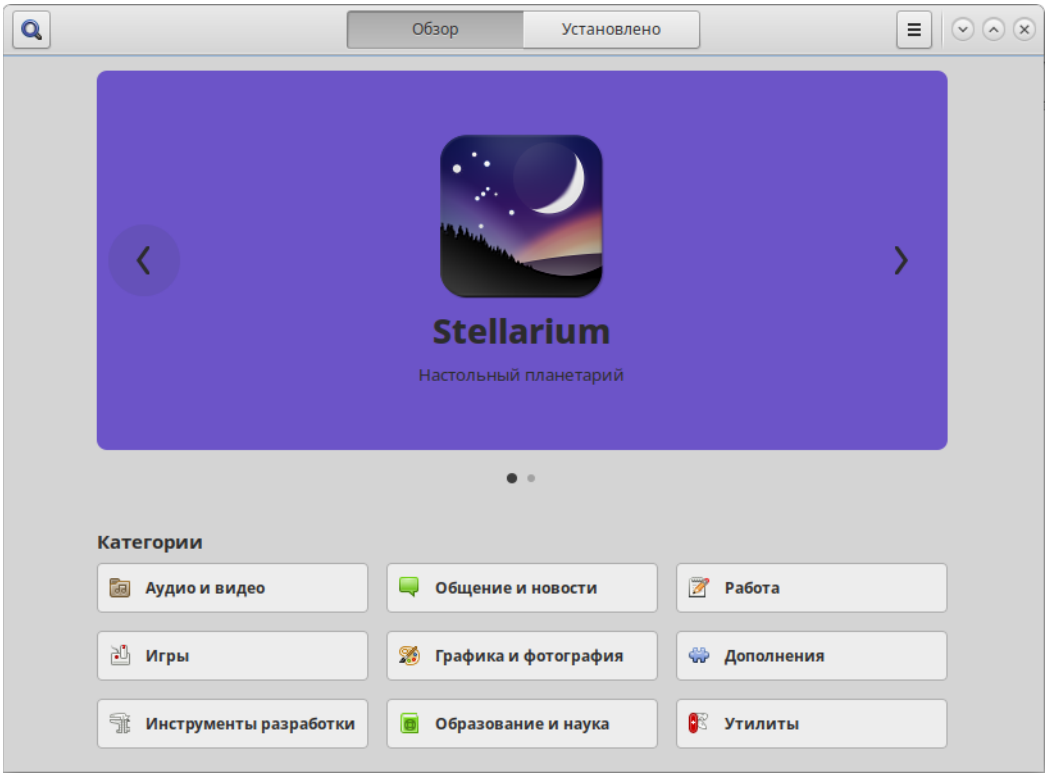

Рис. 59

Центр приложений. Вкладка «Установлено»

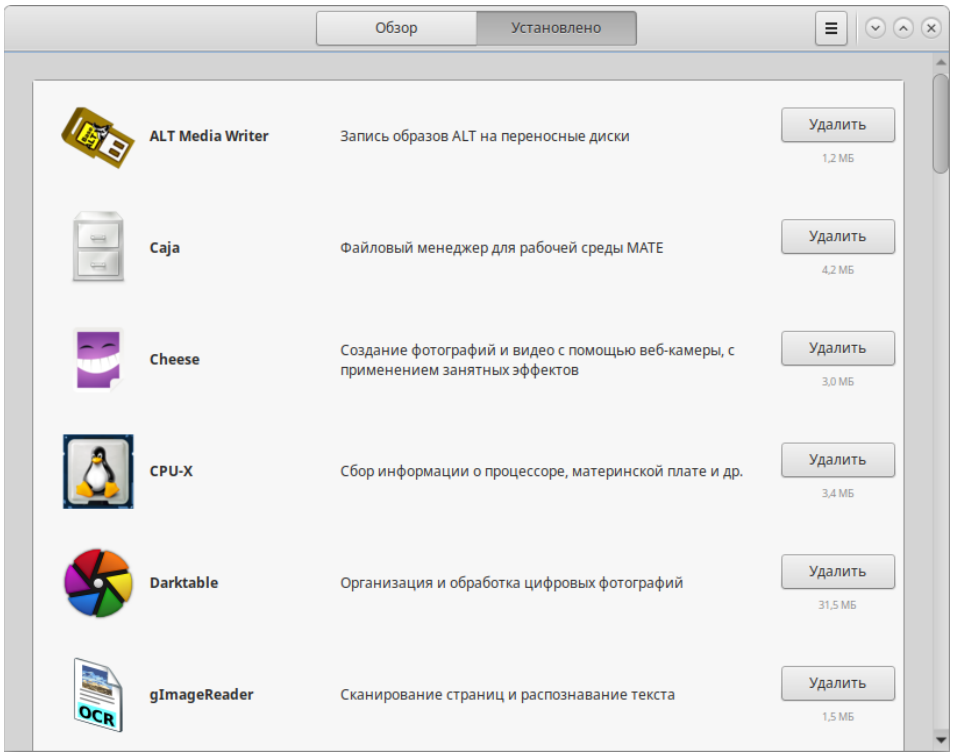

Рис. 60

На вкладке «Обзор» доступные приложения разбиты на категории. Чтобы найти приложение, следует выбрать категорию приложения. Внутри группы, в выпадающем списке «Показывать», можно дополнительно выбрать подкатегорию, тем самым сократив область поиска (Рис. 61).

Центр приложений. Категория «Графика и фотография»

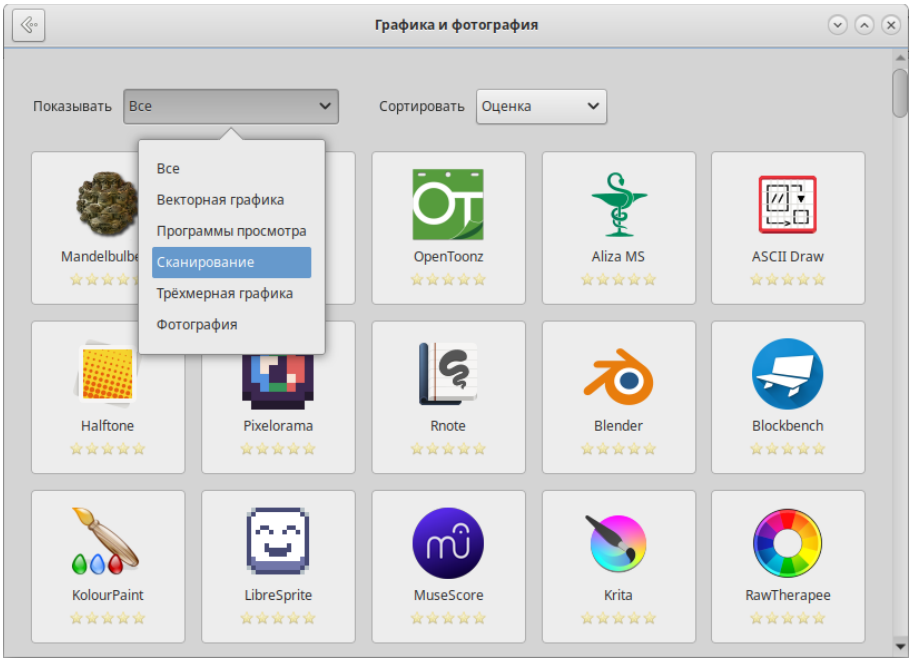

Рис. 61

Быстро найти необходимое приложение можно используя поиск. Строка поиска открывается, при нажатии на кнопку в виде лупы, расположенную в левом верхнем углу «Центра приложений». В строке поиска нужно ввести название приложения.

При выборе приложения, в детальном просмотре, доступны кнопки «Установить»/«Запустить»/«Удалить» (в зависимости от того установлено данное приложение или нет), выводятся снимки экрана, полное описание, а также пользовательские комментарии (Рис. 62). Чтобы установить какое-либо приложение сначала нужно его найти, затем выбрать из списка и нажать на кнопку «Установить».

Центр приложений. Детальный просмотр приложения «Krita»

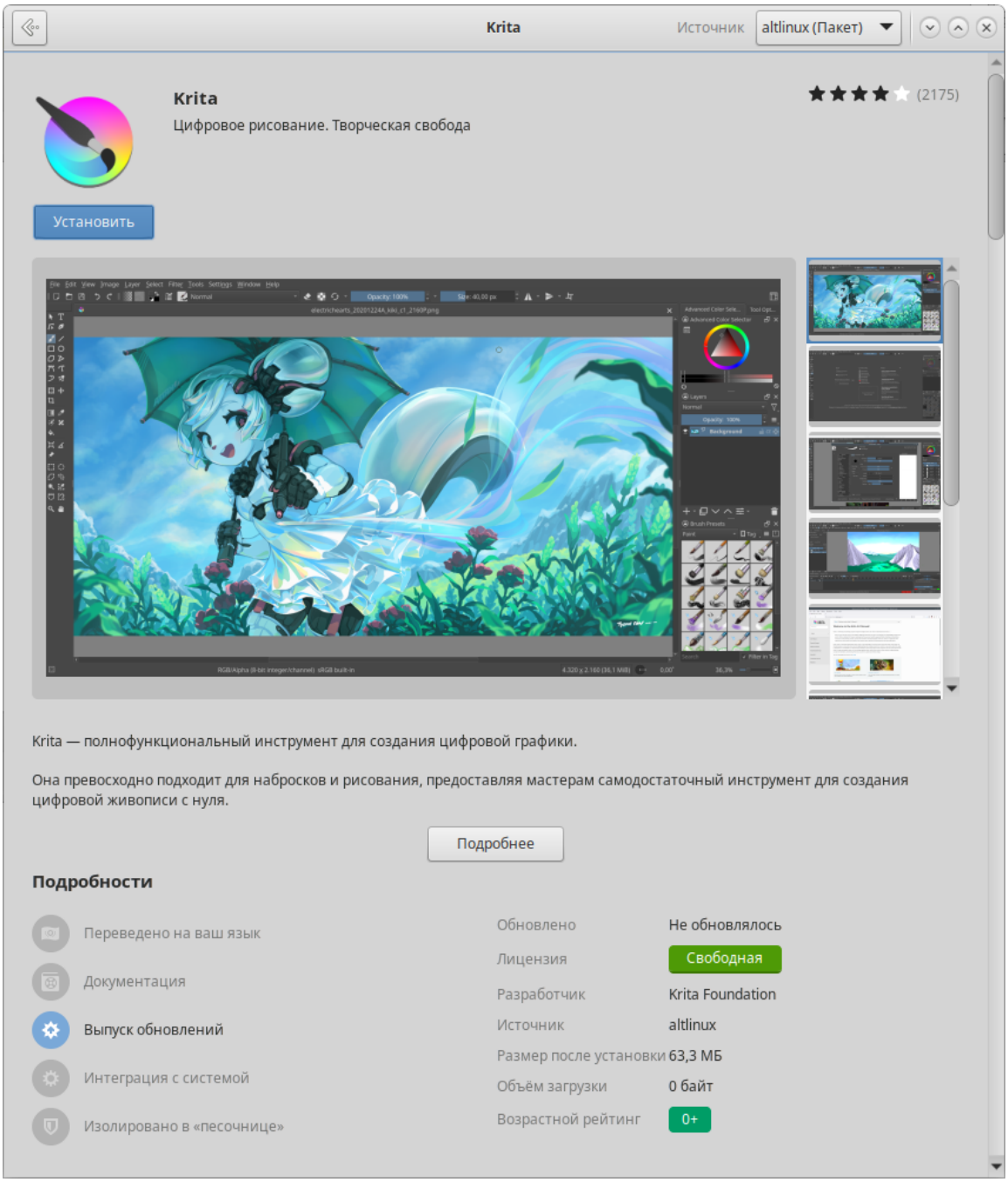

Рис. 62

В этом же окне, если приложение можно установить из разных источников, можно выбрать источник установки (Рис. 63).

Чтобы установить приложение нужно нажать на кнопку «Установить».

Центр приложений. Выбор источника установки

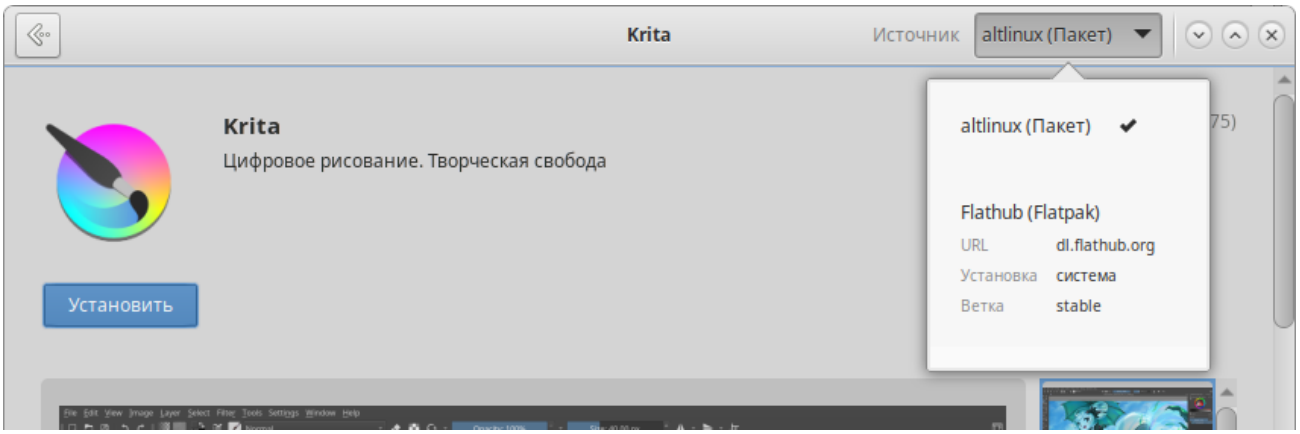

Рис. 63

Примечание. При удалении программ потребуется ввести пароль пользователя root.

Список подключенных репозиториев можно просмотреть, нажав на кнопку дополнительных сведений (Рис. 64) и выбрав пункт «Репозитории ПО».

Центр приложений. Кнопка дополнительных сведений

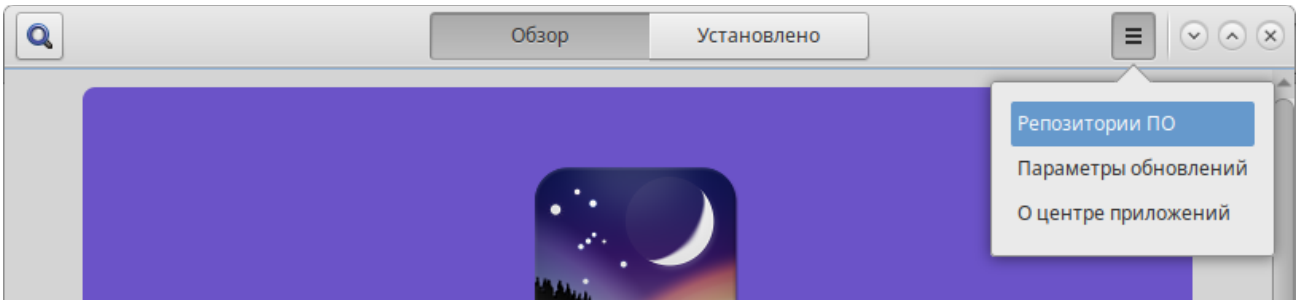

Рис. 64

3.10 Установка сторонних приложений с официальных сайтов

Программа appinstall позволяет установить популярные приложения (например, Google Chrome, Zoom, Skype) с официальных сайтов.

Примечание. appinstall является графическим интерфейсом к `epm play` (см. раздел «Единая команда управления пакетами (epm)»).

Для запуска appinstall следует выбрать пункт «Меню запуска приложений» → «Системные» → «App Install».

При запуске необходимо ввести пароль администратора системы (root).

Для установки приложения достаточно выбрать его в списке приложений и нажать кнопку «Установка» (Рис. 65).

Графический интерфейс к epm play

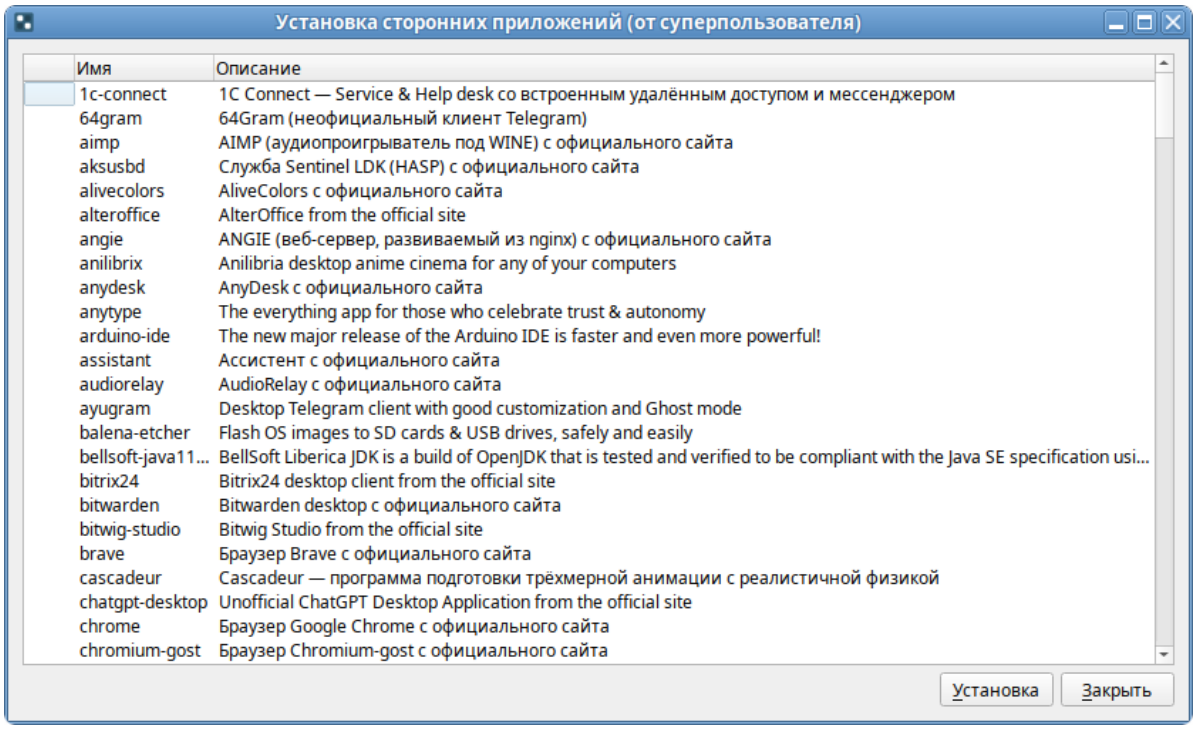

Рис. 65

3.11 Recoll – полнотекстовый поиск

Recoll – программа для полнотекстового поиска по файлам с различными форматами. Помимо обычного поиска, Recoll позволяет использовать некоторые дополнительные функции: поиск по автору, размеру и формату файла, а также поддерживаются такие операторы, как «AND» или «OR».

Для запуска Recoll необходимо в «Меню MATE» выбрать пункт «Приложения» → «Стандартные» → «Recoll».

3.11.1 Индексация файлов

Для поиска требуется предварительная индексация библиотекой Xapian заданных каталогов. Переиндексация может запускаться в фоновом режиме или по запросу.

Индексация – это процесс, с помощью которого анализируется набор документов и данные вводятся в базу данных. Повторное индексирование обычно является инкрементным: документы будут обрабатываться только в том случае, если они были изменены с момента последней индексации.

Произвести настройку индексирования (выбрать каталоги для поиска) можно при первом запуске программы (Рис. 66).

Настройка первого индексирования

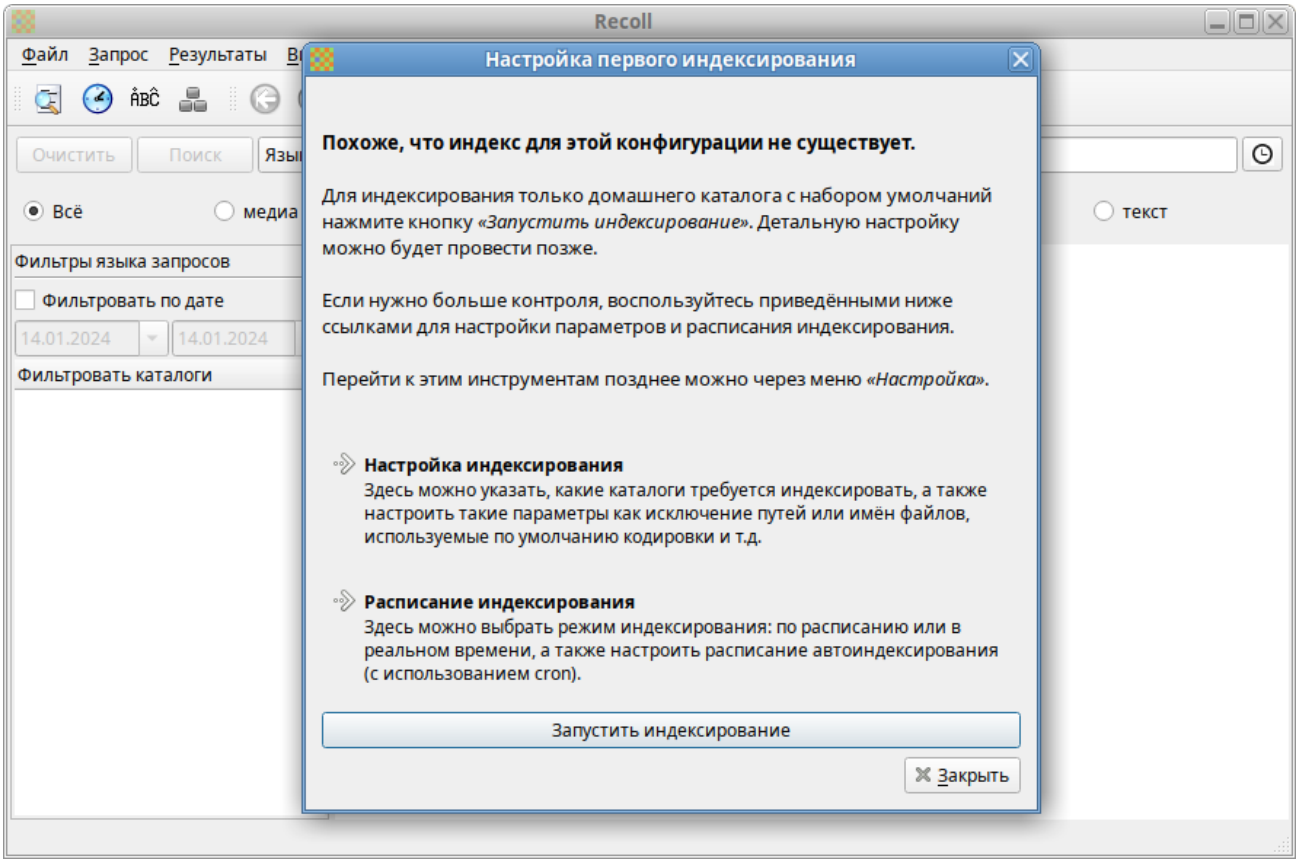

Рис. 66

Для индексирования только домашнего каталога с настройками по умолчанию, необходимо нажать кнопку «Запустить индексирование». Для указания каталогов, а также настройки параметров индексирования можно нажать ссылку «Настройка индексирования». Для задания расписания индексирования следует нажать ссылку «Расписание индексирования».

Настроить параметры индексации можно, выбрав в главном меню Recoll пункт «Настройки» → «Настройка индекса». Окно настройки индексации разделено на четыре вкладки: «Общие параметры», «Локальные параметры», «История в веб» и «Параметры поиска».

На вкладке «Общие параметры» (Рис. 67) можно установить каталог верхнего уровня, от которого рекурсивно начнётся индексация (по умолчанию это домашний каталог пользователя); указать пути, которые следует пропустить при индексации файлов.

Настройка параметров индексирования. Общие параметры

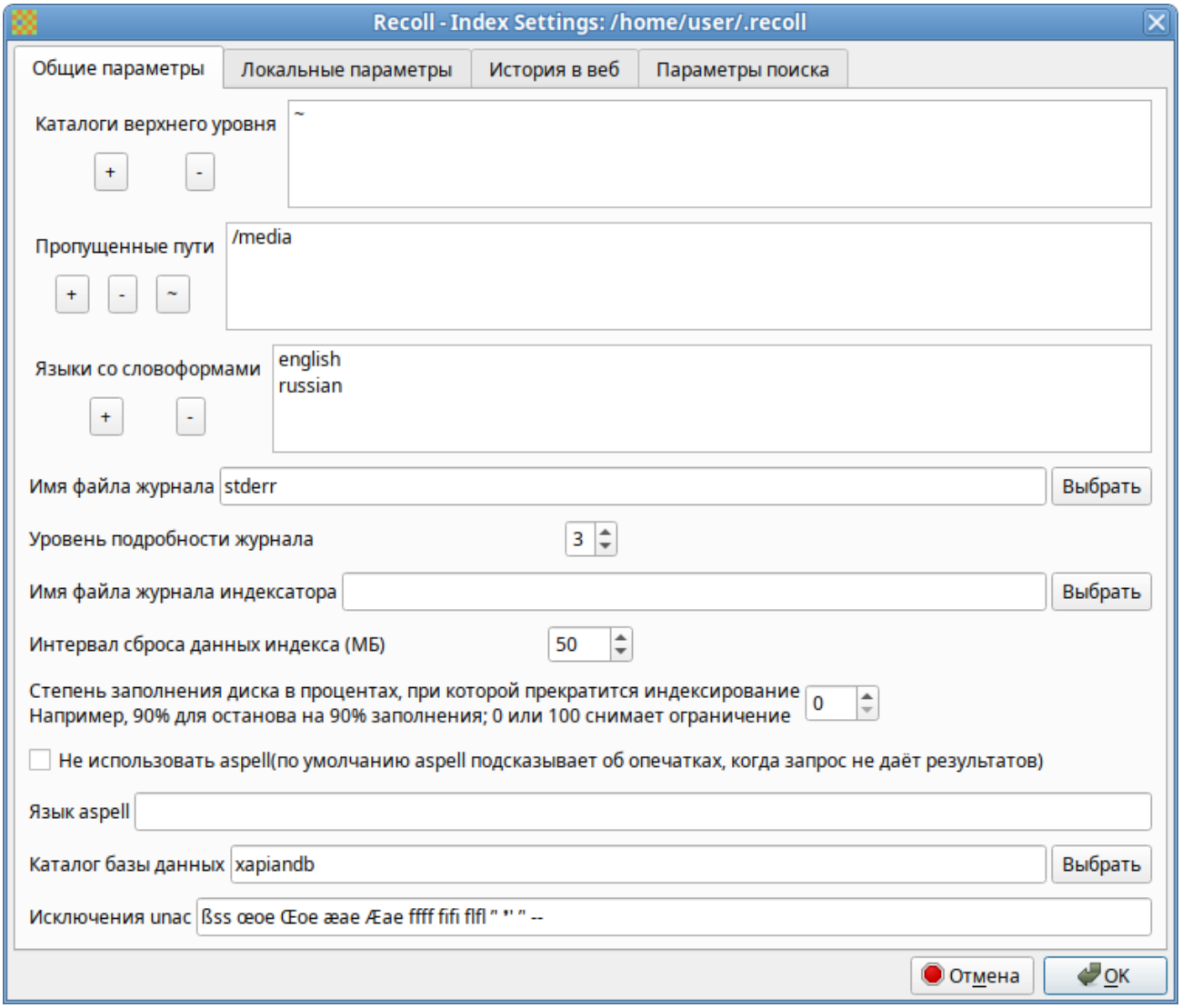

Рис. 67

На вкладке «Локальные параметры» (Рис. 68) можно переопределить переменные для подкаталогов. Переменные устанавливаются для текущего выбранного каталога (или для верхнего уровня, если в списке ничего не выбрано или выбрана пустая строка). Например, можно переопределить кодировку файлов, добавив в поле «Пользовательские подкаталоги» каталог, в котором находятся файлы с кодировкой отличной от Unicode, и в выпадающем списке «Кодировка по умолчанию» выбрать нужную кодировку.

Настройка параметров индексирования. Частные параметры

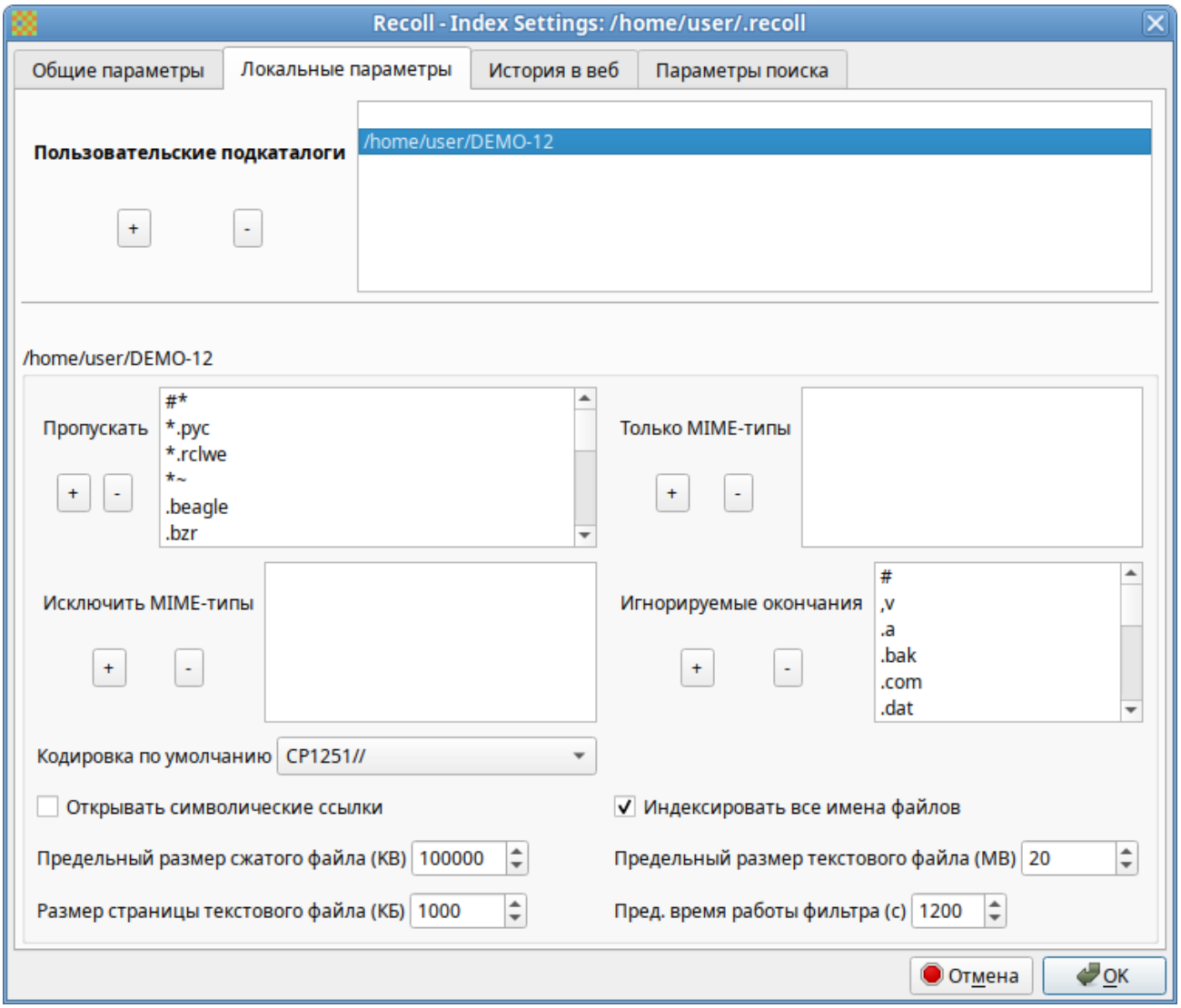

Рис. 68

Запустить индексацию можно выбрав в меню «Файл» → «Обновить индекс».

Индексирование Recoll может выполняться в двух основных режимах:

- периодическая индексация – выполняется в определённое время (например, по ночам, когда компьютер простаивает);
- индексация в реальном времени (фоновое индексирование) – recollindex постоянно работает как сервис и использует монитор изменений файловой системы для обнаружения изменений файлов. Новые или обновленные файлы индексируются сразу.

Выбрать и настроить режим индексирования можно, выбрав в главном меню Recoll «Настройки» → «Расписание индексирования» (Рис. 69).

Настройка расписания индексирования

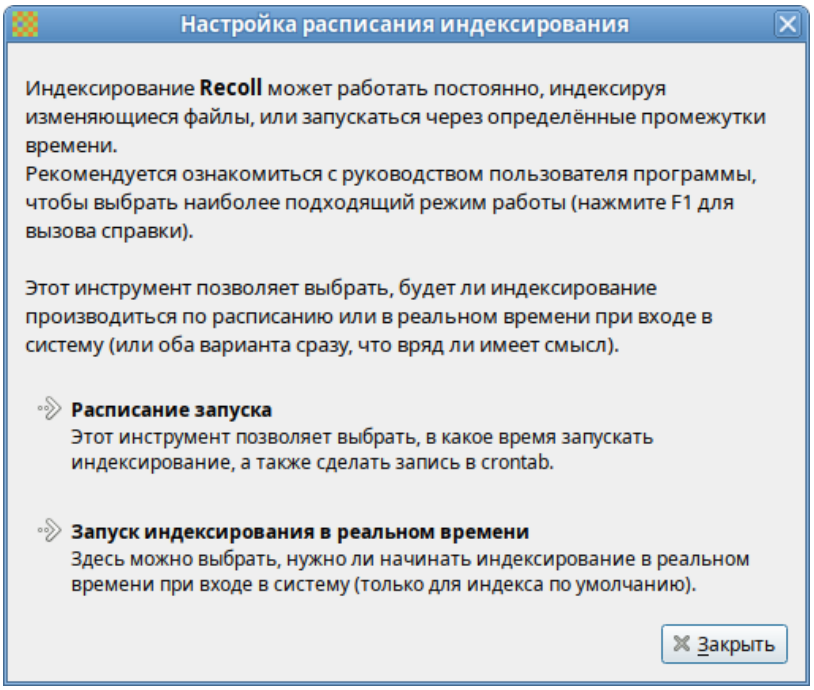

Рис. 69

3.11.2 Поиск файлов

Recoll имеет два интерфейса поиска:

- простой поиск – одно поле ввода (по умолчанию на главном экране), в которое можно ввести несколько слов (Рис. 70);
- расширенный поиск – панель, доступ к которой осуществляется через меню («Инструменты» → «Сложный поиск») или значок панели инструментов. Расширенный поиск имеет несколько полей ввода (Рис. 71), которые можно использовать для создания логического условия, с дополнительной фильтрацией по типу файла, местоположению в файловой системе, дате изменения и размеру.

Простой поиск

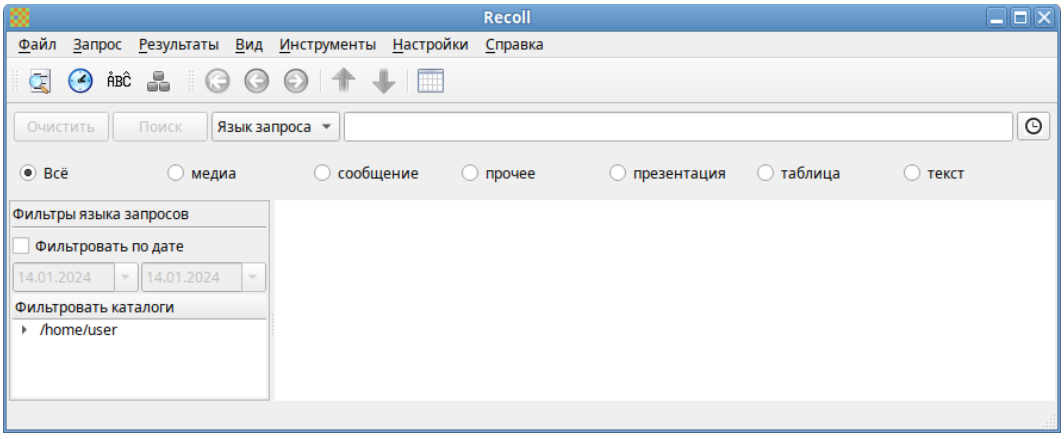

Рис. 70

Сложный поиск

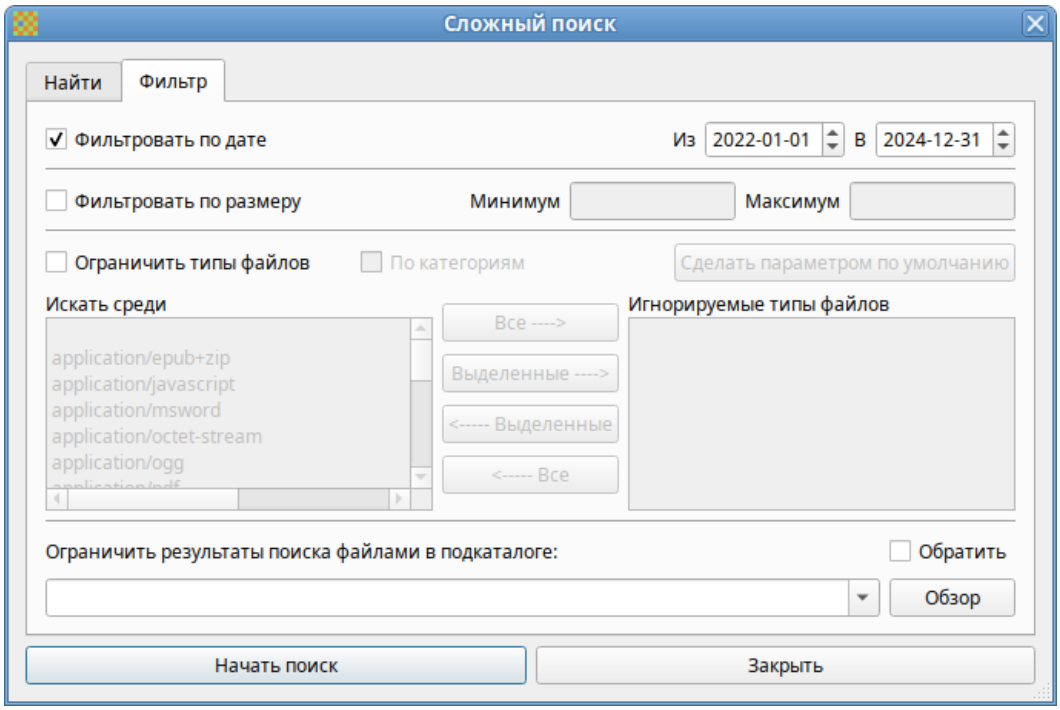

Рис. 71

Для выполнения поиска следует выбрать поисковый режим («Любое слово», «Все слова», «Имя файла» или «Язык запроса»), ввести поисковые слова и нажать кнопку «Поиск» или <Enter> (Рис. 72).

Поиск файлов

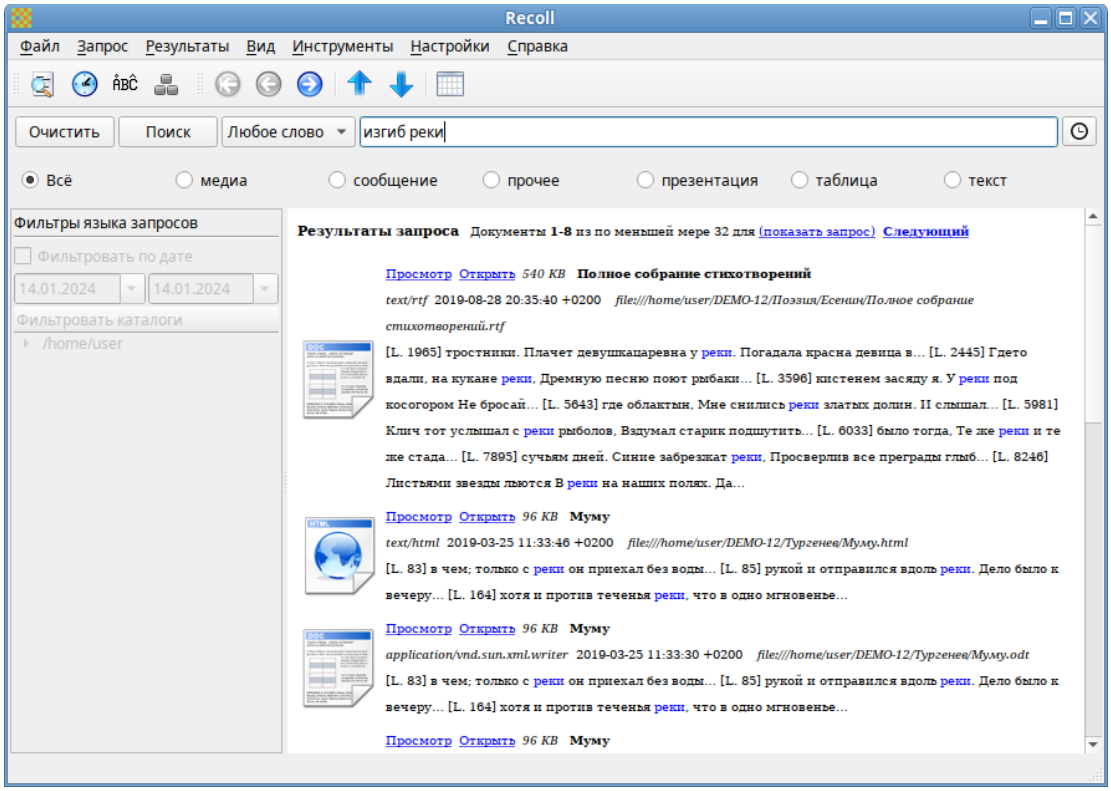

Рис. 72

Режим поиска по умолчанию – «Язык запроса». В этом режиме будет выполнен поиск документов, содержащих все условия поиска, как и в режиме «Все слова». В режиме «Любое слово» будут найдены документы, содержащие любое из введенных вами поисковых слов. В режиме «Имя файла» выполняется сопоставление поискового запроса только имени файла, но не содержимого.

Recoll предоставляет большие возможности по поиску. Разделителем в перечне искомых строк в Recoll служит пробел; поэтому запросы, содержащие пробел должны заключаться в кавычки. В запросах допускаются символы-маски *, ? и [ ].

3.11.3 Список результатов поиска

После запуска поиска список результатов мгновенно отобразится в главном окне.

По умолчанию список документов представлен в порядке релевантности (насколько хорошо система оценивает соответствие документа запросу). Можно отсортировать результат по дате по возрастанию или по убыванию, используя вертикальные стрелки на панели инструментов.

Каждый результат поиска сопровождается небольшим фрагментом файла (Рис. 72).

При нажатии ссылки «Просмотр» откроется внутреннее окно предварительного просмотра документа. При нажатии ссылки «Открыть» запускается внешнее средство просмотра документа. В контекстном меню каждой записи списка результатов есть пункт «Открыть с помощью», для выбора приложения из списка тех, которые зарегистрированы в системе для данного типа MIME-документа (Рис. 73).

Контекстное меню результата запроса

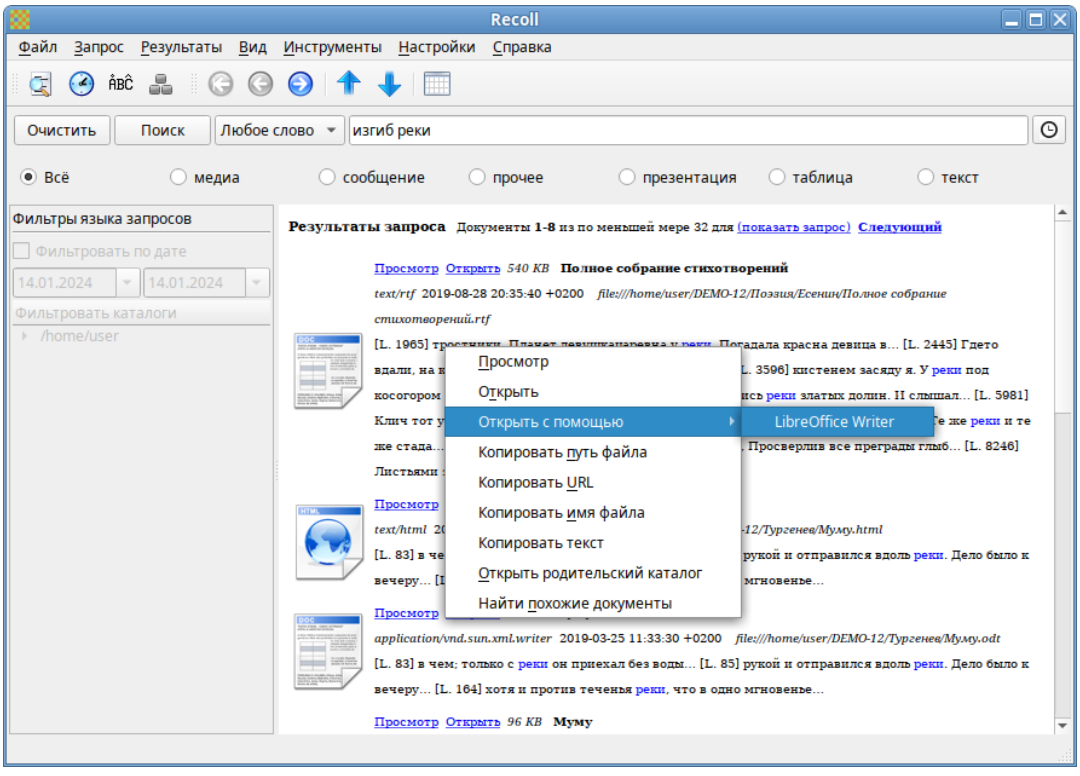

Рис. 73

Результаты поиска можно представить в виде таблицы. Щелчок по заголовку столбца позволит выполнить сортировку по значениям в столбце (Рис. 74).

Результаты поиска в виде таблицы

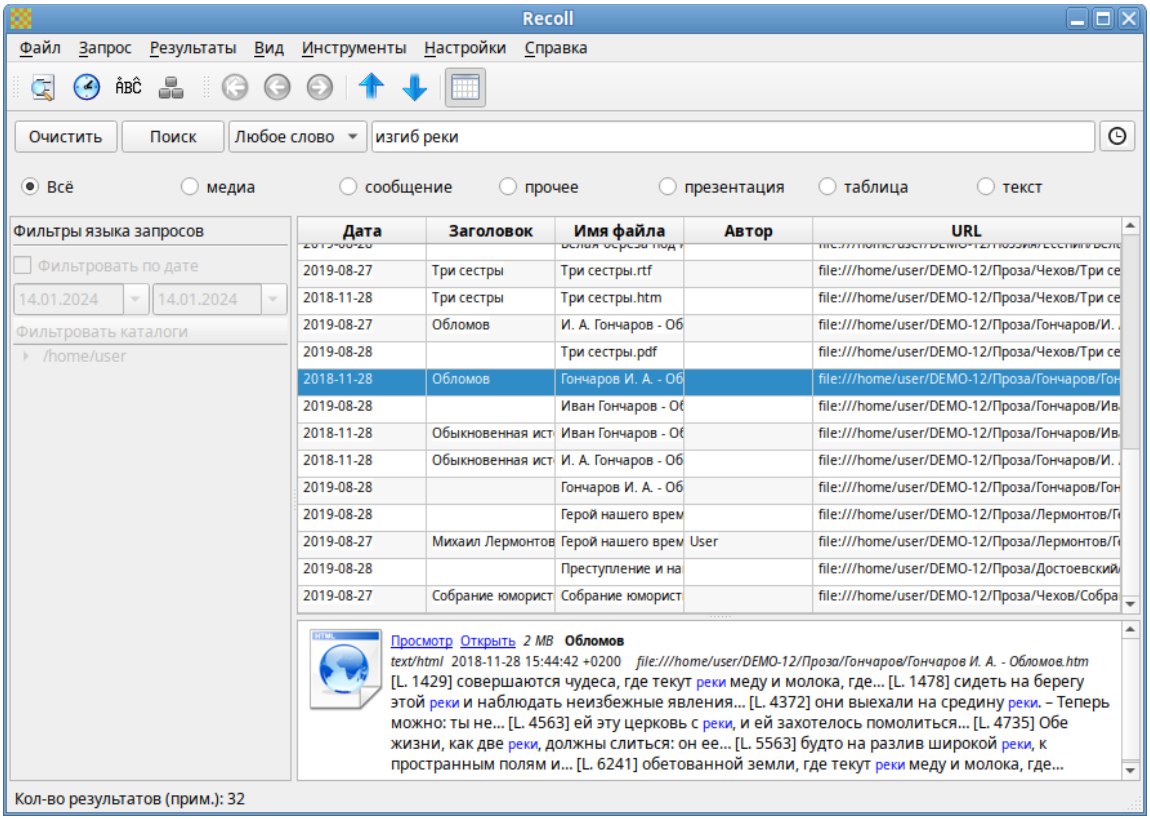

Рис. 74

По умолчанию Recoll позволяет рабочему окружению выбирать, какое приложение следует использовать для открытия документа данного типа. Настроить это действие можно с помощью меню «Настройки» → «Настройка интерфейса» → «Интерфейс пользователя» (Рис. 75).

При нажатии кнопки «Выбор приложений-редакторов» откроется диалоговое окно, где можно выбрать приложение, которое будет использоваться для открытия каждого MIME-типа (Рис. 76).

Пользовательская настройка

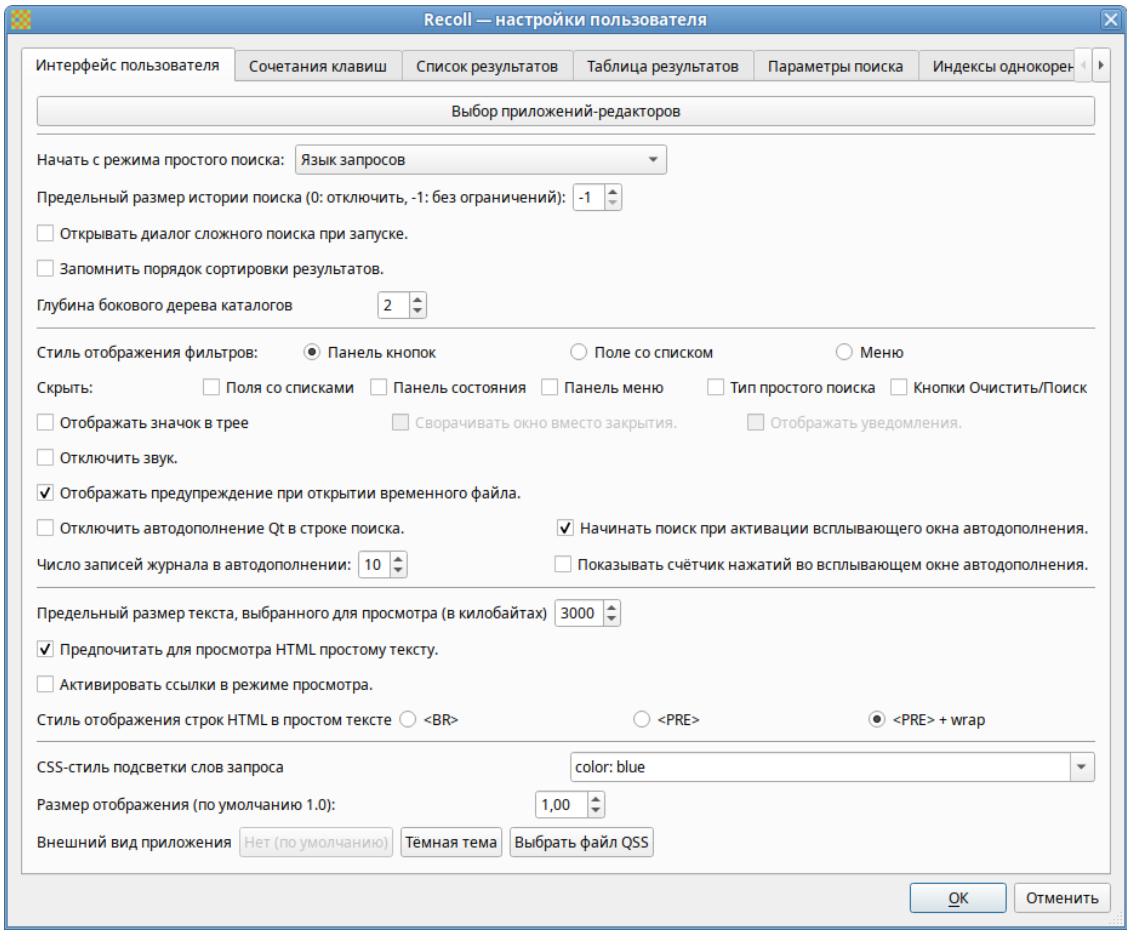

Рис. 75

Пользовательская настройка

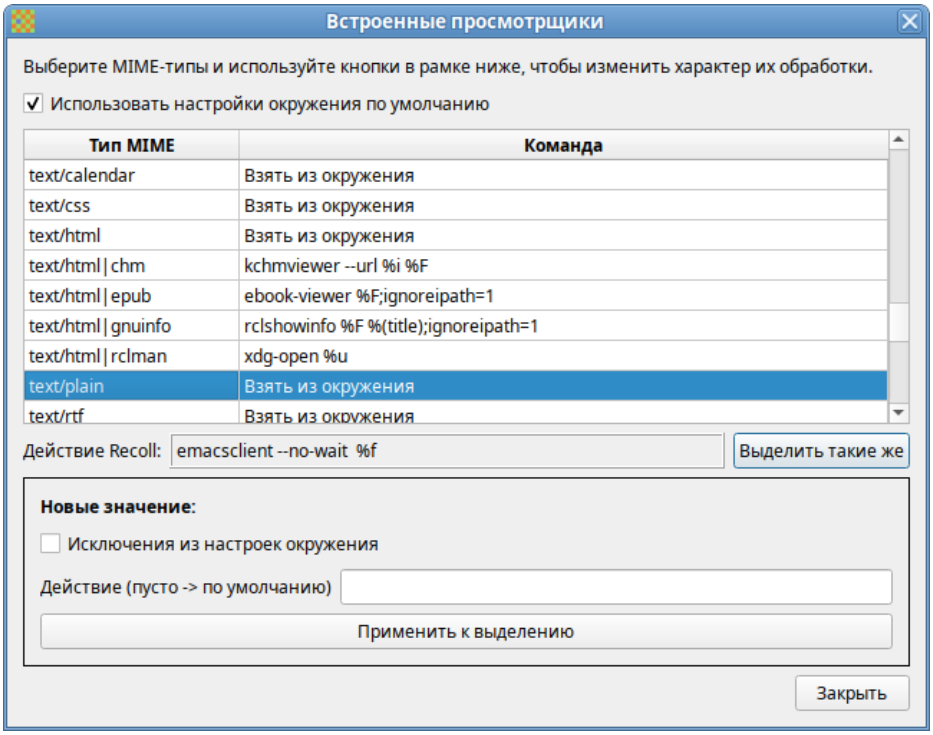

Рис. 76

4 НАСТРОЙКА СИСТЕМЫ

4.1 Центр управления системой

Для управления настройками установленной системы можно использовать Центр управления системой. Центр управления системой (ЦУС) представляет собой удобный интерфейс для выполнения наиболее востребованных административных задач: добавление и удаление пользователей, настройка сетевых подключений, просмотр информации о состоянии системы и другие административные задачи.

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

ЦУС состоит из нескольких независимых диалогов-модулей. Каждый модуль отвечает за настройку определённой функции или свойства системы. Модули центра управления системой имеют справочную информацию.

4.1.1 Применение ЦУС

ЦУС можно использовать для разных целей, например:

- настройки даты и времени;
- управления системными службами;
- просмотра системных журналов;
- управления выключением удаленного компьютера (доступно только в веб-интерфейсе);
- настройки ограничений выделяемых ресурсов памяти пользователям (квоты);
- настройки ограничений на использование внешних носителей (доступно только в веб-интерфейсе);
- управления политиками control (системные ограничения);
- конфигурирования сетевых интерфейсов;
- настройки межсетевого экрана;
- изменения пароля администратора системы (root);
- создания, удаления и редактирования учётных записей пользователей.

4.1.2 Запуск ЦУС в графической среде

ЦУС можно запустить следующими способами:

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

При запуске необходимо ввести пароль администратора системы (root) (Рис. 77).

Запуск Центра управления системой

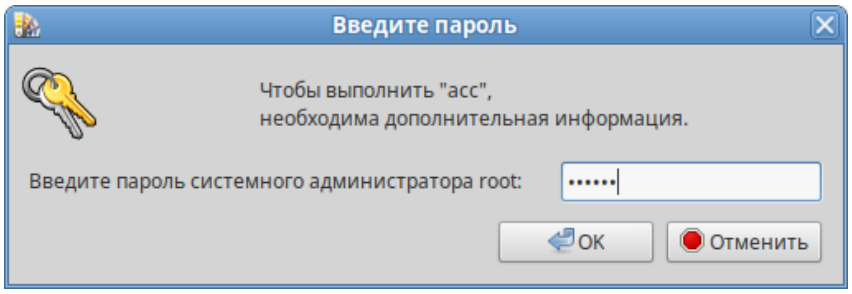

Рис. 77

После успешного входа можно приступать к настройке системы (Рис. 78).

Центр управления системой

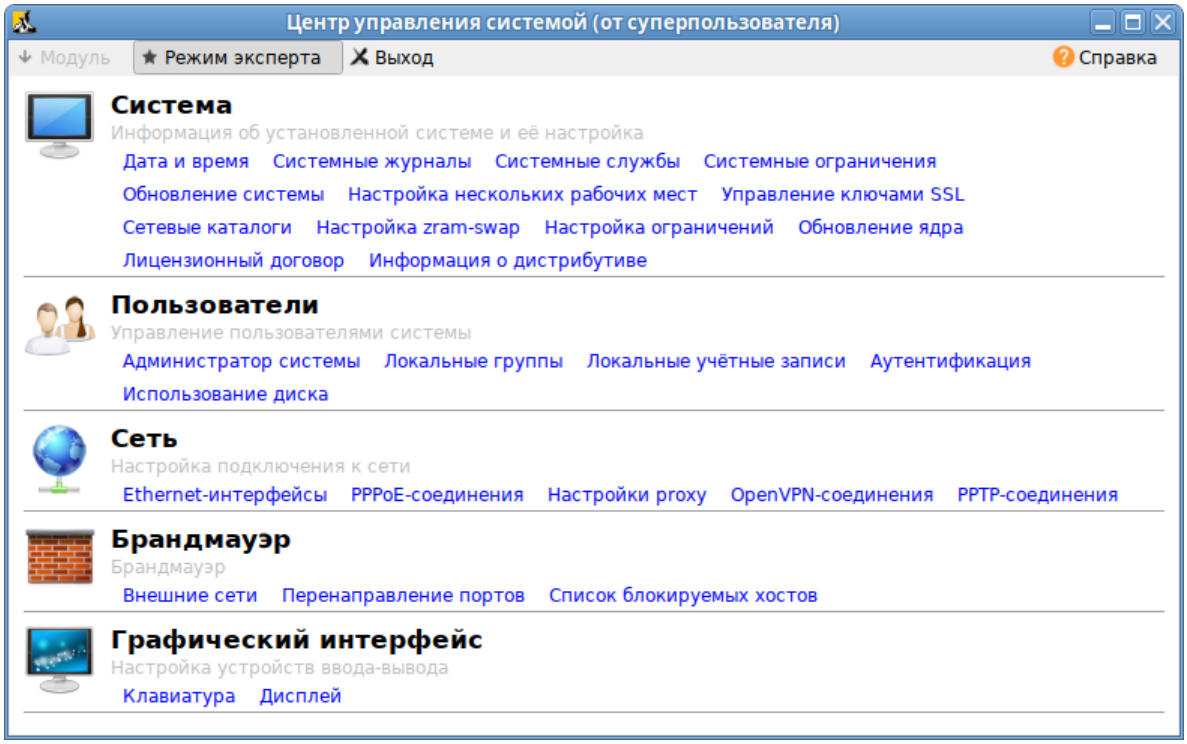

Рис. 78

4.1.3 Использование веб-ориентированного ЦУС

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

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

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

И запущен сервис ahttpd:

```
# systemctl enable --now ahttpd
```

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

Например, если IP-адрес компьютера под управлением ОС «Альт Рабочая станция» 192.168.0.196, то интерфейс управления будет доступен по адресу: https://192.168.0.196:8080/

При запуске ЦУС необходимо ввести в соответствующие поля имя пользователя (root) и пароль пользователя (Рис. 79).

Запрос пароля администратора для запуска веб-интерфейса ЦУС

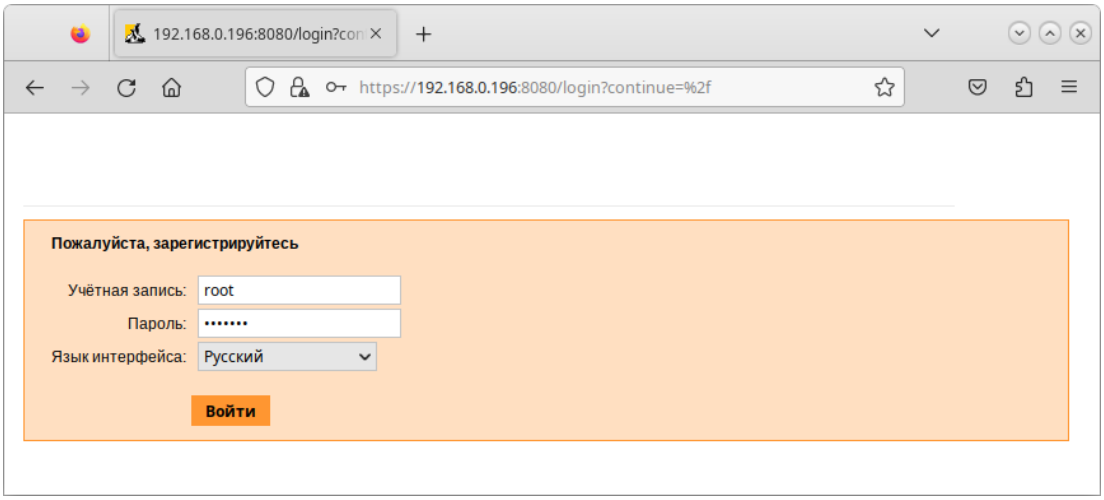

Рис. 79

После этого будут доступны все возможности ЦУС на той машине, к которой было произведено подключение через веб-интерфейс (Рис. 80).

Окно веб-интерфейса ЦУС

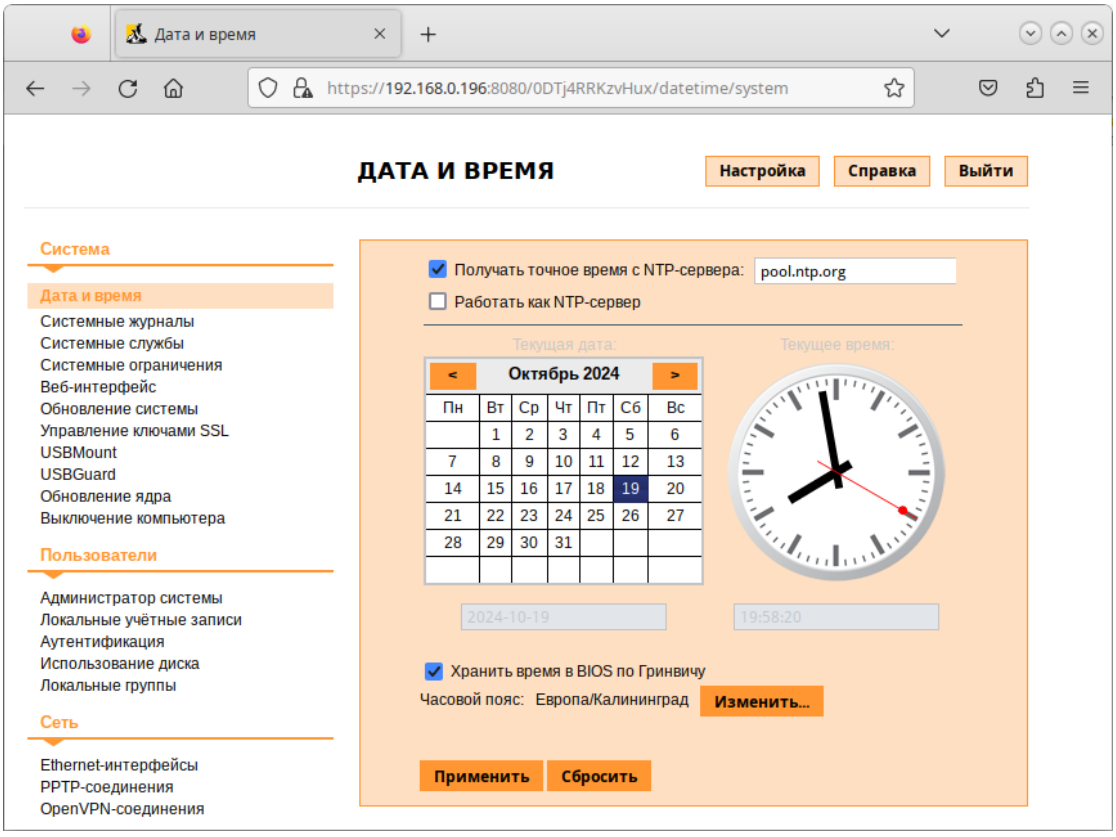

Рис. 80

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

- основной режим;
- режим эксперта.

ЦУС содержит справочную информацию по включённым в него модулям. Об использовании самого интерфейса системы управления можно прочитать (Рис. 81), нажав на кнопку «Справка» на начальной странице ЦУС.

Веб-интерфейс ЦУС. Справка

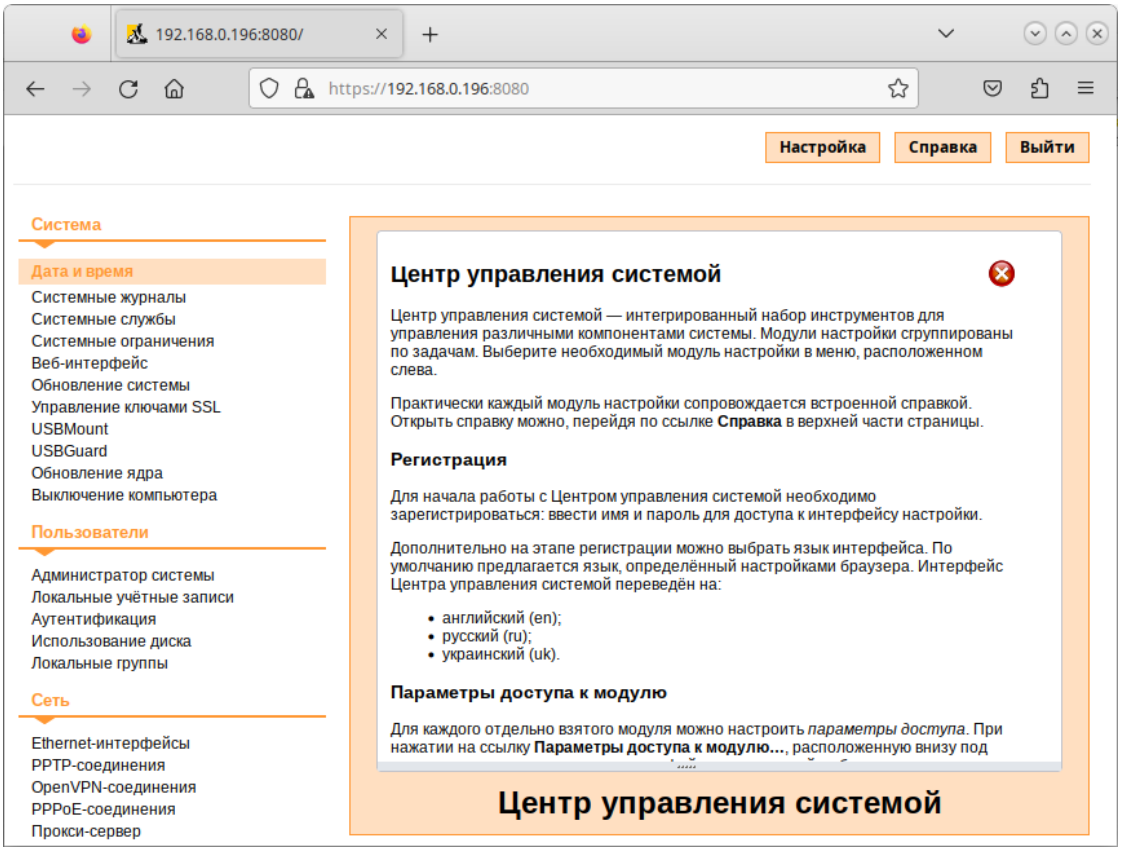

Рис. 81

После работы с ЦУС, в целях безопасности, не следует оставлять открытым браузер. Необходимо обязательно выйти из сеанса работы с ЦУС, нажав на кнопку «Выйти».

Подробнее об использовании ЦУС можно узнать в главе «Средства удаленного администрирования».

4.2 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. Запустить инструмент настройки «Сессии», можно выбрав пункт «Меню MATE» → «Приложения» → «Параметры» → «Запускаемые приложения».

4.2.1 Вкладка автоматического запуска программ

Список автоматически запускаемых программ представлен на вкладке «Автоматически запускаемые программы» (Рис. 82). Этот список содержит краткое описание каждой программы и отметку, указывающую запускать программу или нет.

Автоматически запускаемые программы

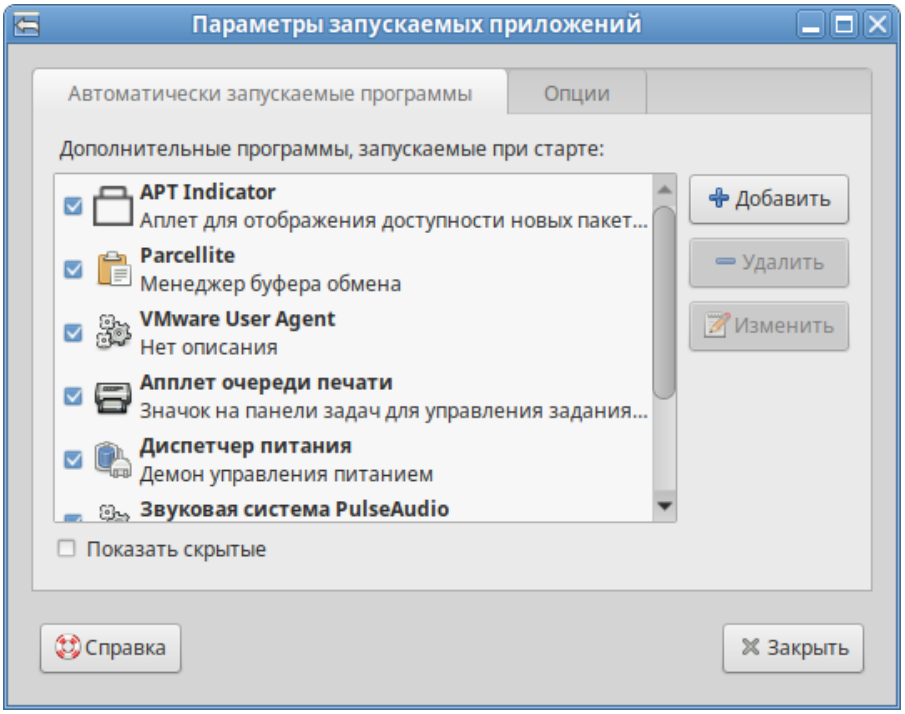

Рис. 82

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

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

- нажать кнопку «Добавить». Откроется окно «Новая автоматически запускаемая программа»;
- указать имя программы и команду, которая запустит приложение (Рис. 83);
- нажать кнопку «Добавить».

Добавление автоматически запускаемой программы

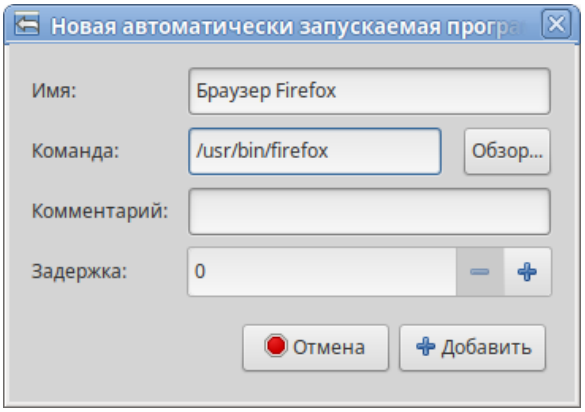

Рис. 83

4.2.2 Вкладка настроек сессии

Менеджер сеанса может запомнить приложения, которые 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. 84).

Запоминать запущенные приложения при выходе из сеанса

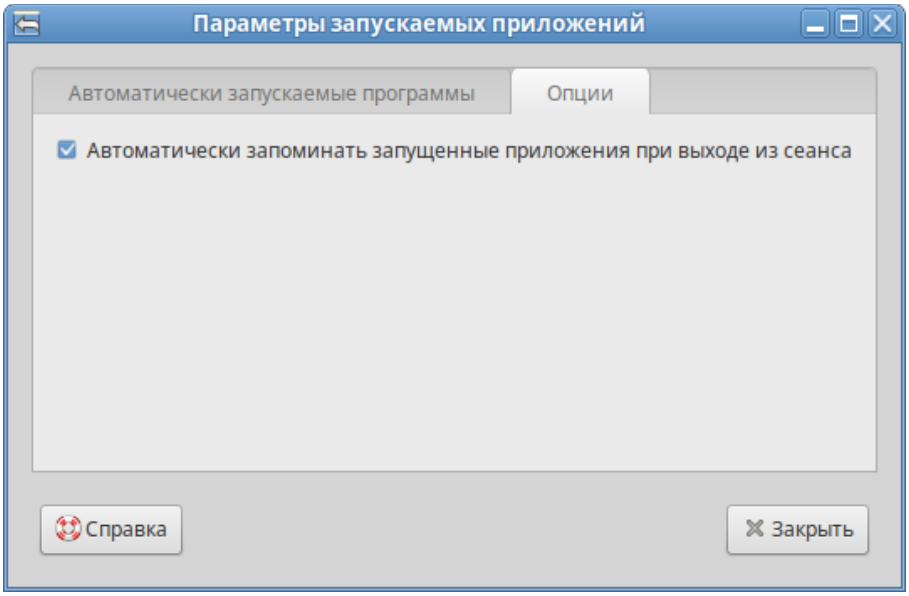

Рис. 84

4.3 Настройка сети

4.3.1 NetworkManager

Для управления настройками сети в ОС «Альт Рабочая станция» используется программа NetworkManager. NetworkManager позволяет подключаться к различным типам сетей: проводные, беспроводные, мобильные, VPN и DSL, а также сохранять эти подключения для быстрого доступа к сети.

NetworkManager доступен как апплет, находящийся в системном лотке.

При нажатии левой кнопкой мыши на значок NetworkManager, появляется меню, в котором можно выбрать одну из доступных сетей и подключиться к ней. Из этого меню так же можно отключить активное Wi-Fi соединение или установить VPN соединение (Рис. 85).

NetworkManager

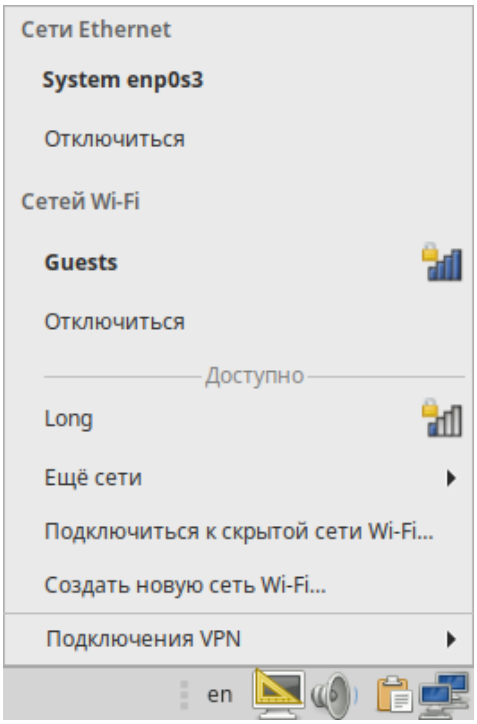

Рис. 85

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

При нажатии правой кнопкой мыши на значок NetworkManager, появляется контекстное меню, из которого можно получить доступ к изменению некоторых настроек (Рис. 86). Здесь можно посмотреть версию программы, получить сведения о подключении, изменить соединения (например, удалить Wi-Fi сеть, чтобы не подключаться к ней автоматически).

Контекстное меню NetworkManager

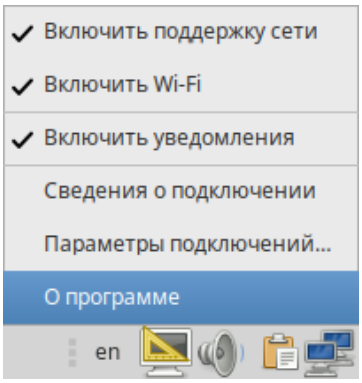

Рис. 86

Для того чтобы просмотреть информацию о сетевом подключении, следует в меню NetworkManager, вызываемом нажатием правой кнопкой мыши, выбрать пункт «Сведения о подключении». Сведения об активных соединениях будут отображены в диалоговом окне «Сведения о подключении», каждое в отдельной вкладке (Рис. 87).

Информация о сетевом соединении

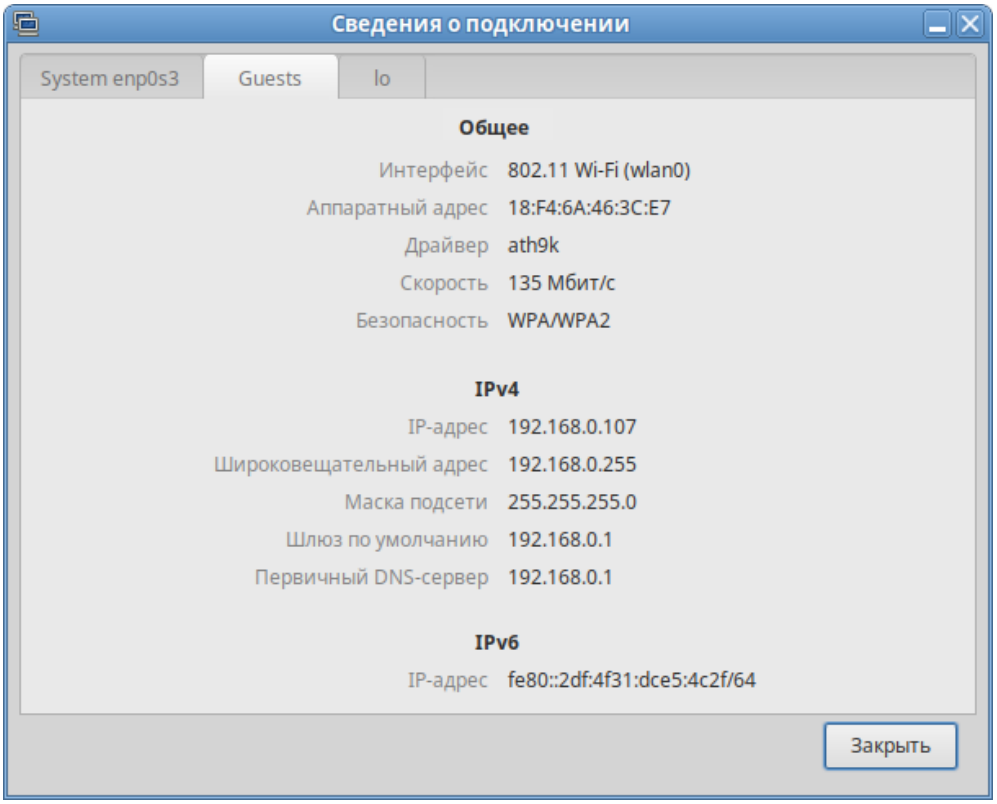

Рис. 87

Для настройки соединений, следует в меню NetworkManager, вызываемом нажатием правой кнопкой мыши, выбрать пункт «Параметры подключений...». В открывшемся окне будет показан сгруппированный по типам список соединений. Необходимо выбрать нужную сеть и нажать кнопку «Редактировать выбранное подключение» (Рис. 88).

Изменение настроек сетевых соединений

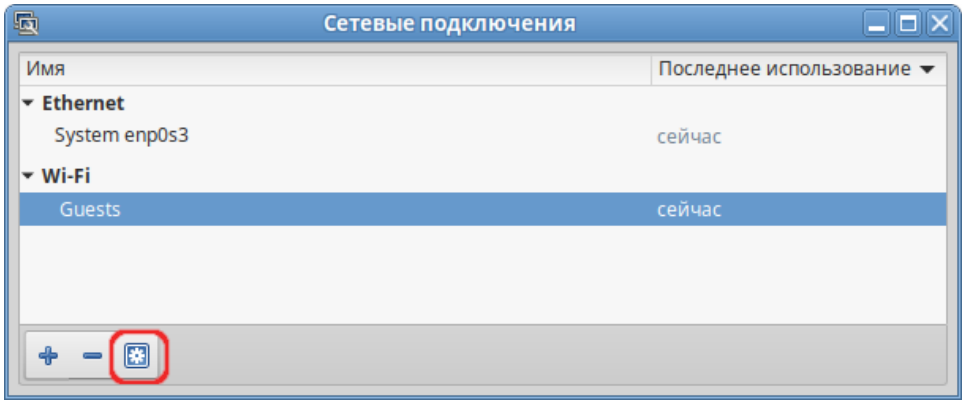

Рис. 88

В открывшемся окне можно изменить настройки сетевого интерфейса (Рис. 89).

Окно изменения настроек сетевого интерфейса

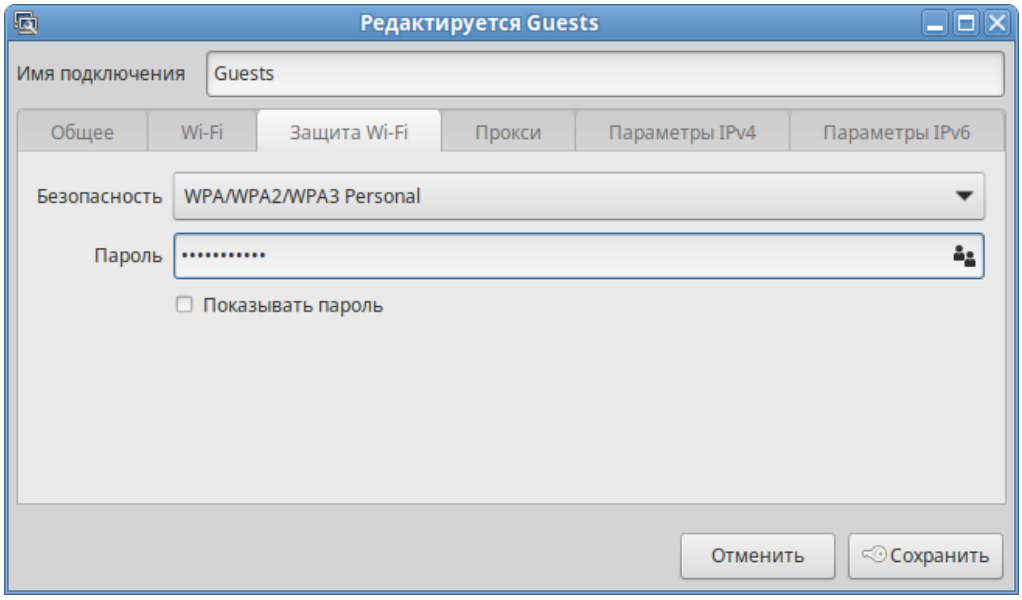

Рис. 89

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

4.3.2 Настройка в ЦУС

Настройку сети можно выполнить в ЦУС в разделе «Сеть» → «Ethernet интерфейсы». Здесь можно задать как глобальные параметры сети (адрес сервера DNS, имя компьютера), так и настройки конкретного сетевого интерфейса.

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

4.4 Установка принтера

Перед началом установки необходимо убедиться в том, что в случае локального подключения принтер присоединён к соответствующему порту компьютера и включён, а в случае сетевого подключения принтер корректно сконфигурирован для работы в сети.

Настройки принтера можно запустить следующими способами:

- в графической среде MATE: «Меню MATE» → «Приложения» → «Администрирование» → «Параметры печати».
- из командной строки, выполнив команду:

```
$ system-config-printer
```

Примечание. Если возникает ошибка «Служба печати недоступна» (Рис. 90), следует нажать кнопку «Запустить службу». Потребуется ввести пароль пользователя root.

Можно также в терминале от имени системного администратора root выполнить команду:

```
# systemctl restart cups
```

После выполнения команды необходимо вернуться к окну «Настройки принтера» и нажать кнопку «Обновить».

Ошибка «Служба печати недоступна»

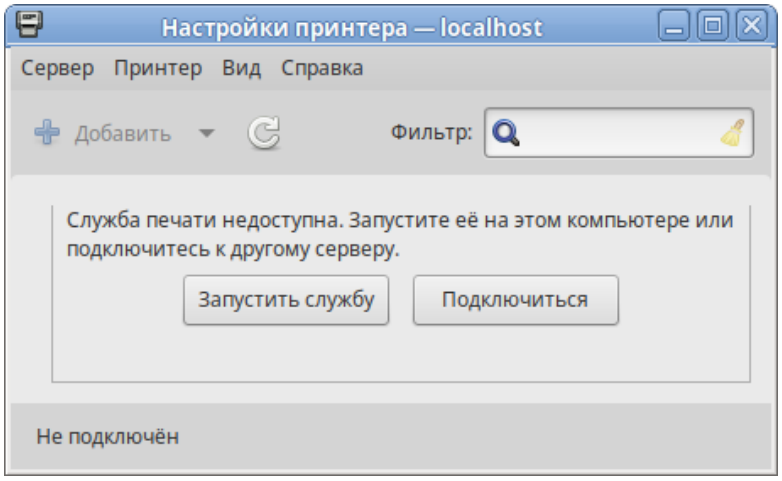

Рис. 90

Для добавления принтера необходимо нажать кнопку «Добавить» (Рис. 91).

Настройка печати

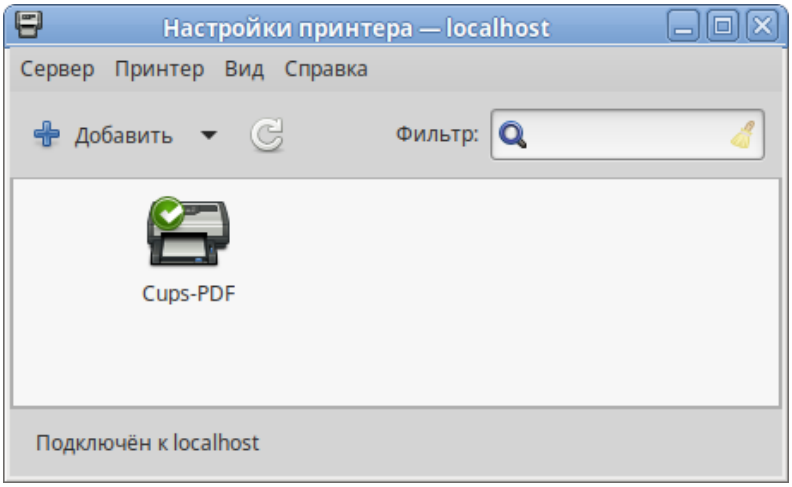

Рис. 91

В открывшемся окне необходимо определить устройство из предложенных в списке «Устройства» (Рис. 92) и удостовериться, что тип соединения указан корректно. Переход к следующему шагу осуществляется нажатием кнопки «Вперёд».

Настройка печати

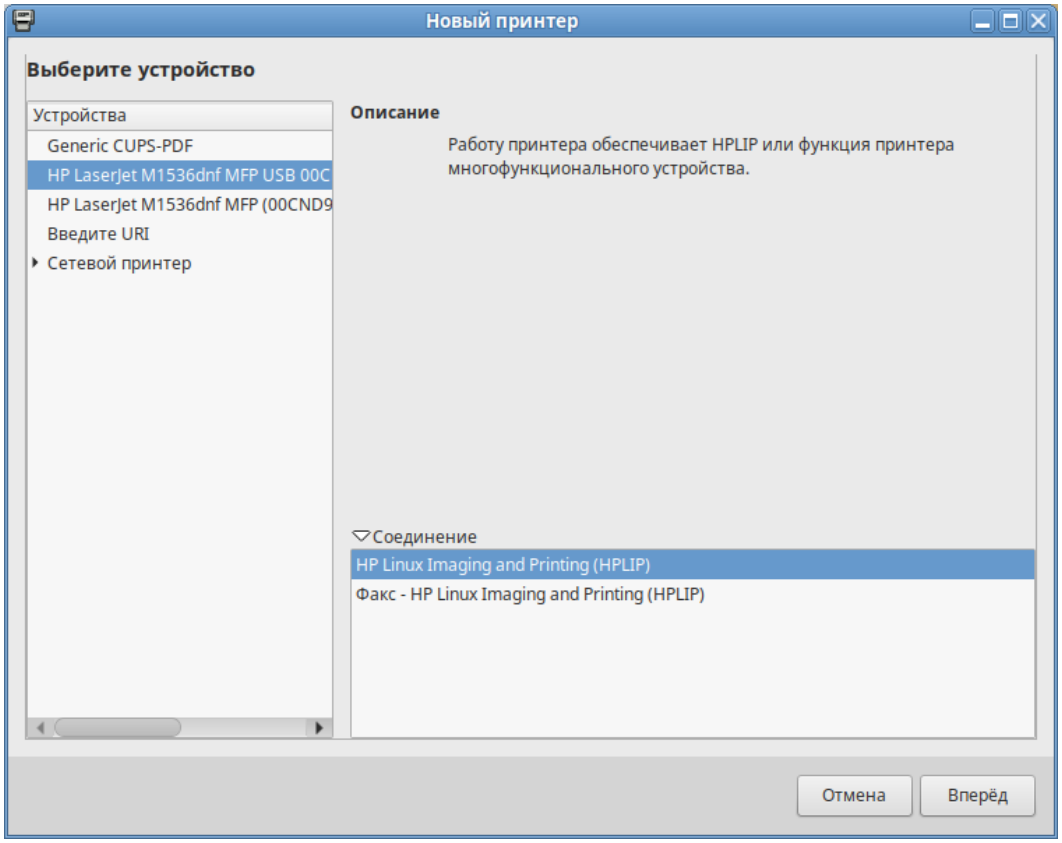

Рис. 92

В окне «Опишите принтер», в строке «Имя принтера» можно изменить имя принтера и добавить описание (Рис. 93).

Настройка печати

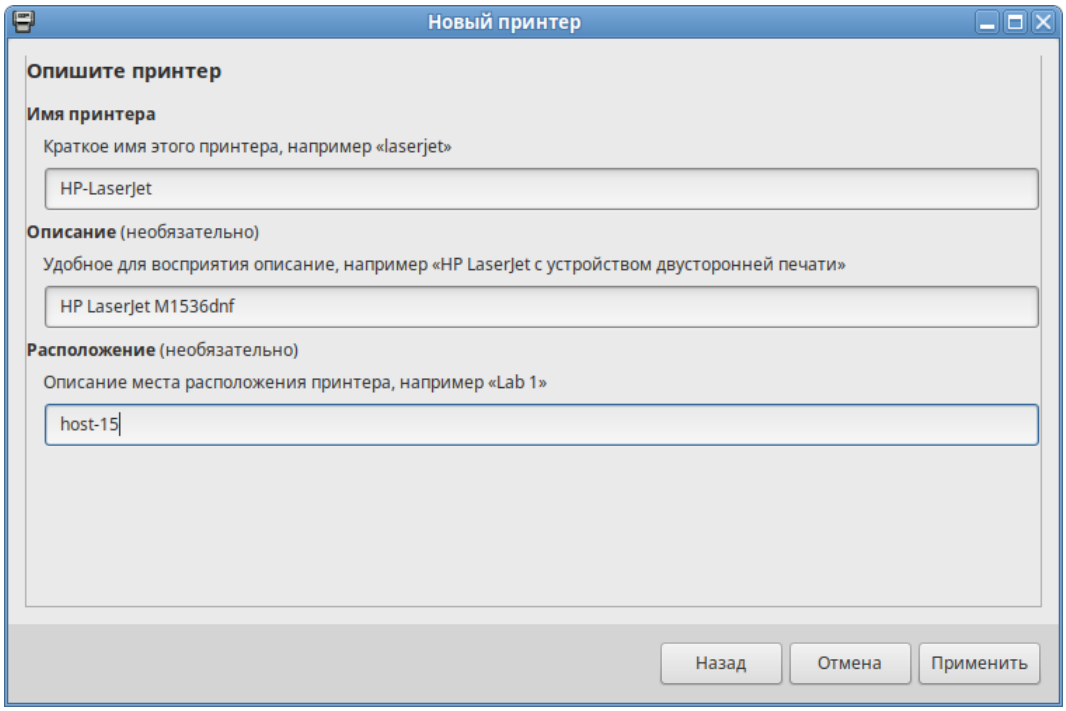

Рис. 93

После нажатия кнопки «Применить» установка принтера завершена, принтер станет доступным для печати (Рис. 94).

Настройка печати

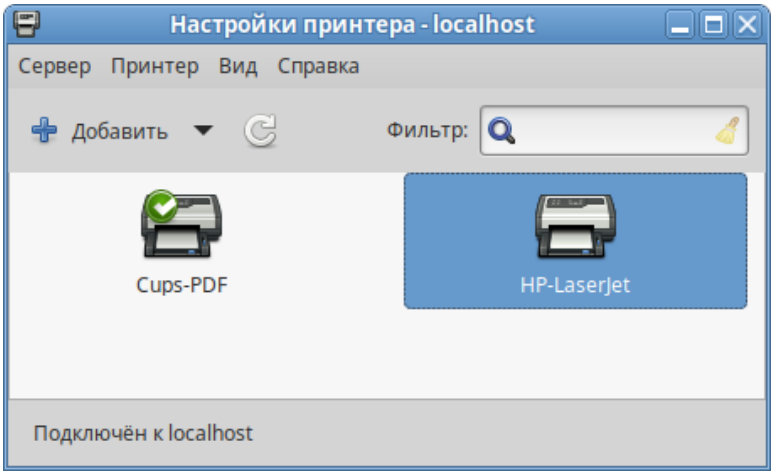

Рис. 94

Далее будет предложена проверка печати. После проверки откроется диалог, в котором, при желании, можно настроить дополнительные параметры принтера: разрешение, размер используемой по умолчанию бумаги, а также задать принтер по умолчанию.

Изменить настройки добавленного принтера можно в любой момент, выбрав в программе нужный принтер, затем в меню «Принтер» → «Свойства».

4.5 Настройка сканера подключенного к USB-порту

В ОС «Альт Рабочая станция» доступ к сканерам обеспечивается программой SANE (Scanner Access Now Easy). Система SANE состоит из двух частей: аппаратной поддержки (backend, libsane) и программной поддержки (frontend). Первая часть обеспечивает собственно доступ к сканеру, вторая – графический интерфейс для сканирования (xsane).

4.5.1 Конфигурация SANE

Подключите сканер к компьютеру и проверьте доступность сканера:

```
$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 004: ID 03f0:012a HP, Inc HP LaserJet M1536dnf MFP
Bus 002 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching Hub
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 2.0 root hub
```

В примере сканер определен на шине USB 002 как устройство 004.

При помощи команды `sane-find-scanner` можно проверить поддержку сканера системой SANE:

```
$ sane-find-scanner -q
```

```
could not open USB device 0x1d6b/0x0002 at 001:001: Access denied
(insufficient permissions)
found USB scanner (vendor=0x03f0 [Hewlett-Packard], product=0x012a [HP
LaserJet M1536dnf MFP]) at libusb:002:004
could not open USB device 0x80ee/0x0021 at 002:002: Access denied
(insufficient permissions)
could not open USB device 0x1d6b/0x0001 at 002:001: Access denied
(insufficient permissions)
```

В выводе должны присутствовать интерфейс сканера и имя используемого устройства. В данном случае сканер был распознан на шине 002 как устройство 004.

Примечание. Если бы доступ к сканеру также был запрещен (как и доступ к другим USB-устройствам), необходимо рассмотреть разрешения на шину USB:

```
# ls -l /dev/bus/usb/002/
итого 0
crw-rw-r--  1 root root 189, 128 окт 28 12:00 001
crw-rw-r--  1 root root 189, 129 окт 28 12:00 002
crw-rw-r--+ 1 root lp   189, 130 окт 28 12:42 003
```

И добавить пользователя в нужную группу (в данном случае в группу lp):

```
# gpasswd -a user lp
```

Далее необходимо ОБЯЗАТЕЛЬНО перезапустить сеанс пользователя.

Теперь необходимо убедиться, что сканер опознан программой графического интерфейса. В состав системы SANE входит утилита `scanimage`, позволяющая работать со сканером из командной строки (опция `-L` используется для показа информации о сканере):

```
$ scanimage -L
device `hpaio:/usb/HP_LaserJet_M1536dnf_MFP?serial=00CND9D8YC9C' is a
Hewlett-Packard HP_LaserJet_M1536dnf_MFP all-in-one
```

В контексте локального USB-устройства, доступ к которому имеет обычный пользователь, положительный ответ указывает, что SANE поддерживает этот сканер.

Проверка работы сканера:

```
$ scanimage -T -d 'hpaio:/usb/HP_LaserJet_M1536dnf_MFP?
serial=00CND9D8YC9C'
scanimage: scanning image of size 637x876 pixels at 1 bits/pixel
scanimage: acquiring gray frame, 1 bits/sample
scanimage: reading one scanline, 80 bytes...    PASS
scanimage: reading one byte...          PASS
```

```
scanimage: stepped read, 2 bytes...     PASS
scanimage: stepped read, 4 bytes...     PASS
scanimage: stepped read, 8 bytes...     PASS
scanimage: stepped read, 16 bytes...    PASS
scanimage: stepped read, 32 bytes...    PASS
scanimage: stepped read, 64 bytes...    PASS
scanimage: stepped read, 128 bytes...   PASS
scanimage: stepped read, 127 bytes...   PASS
scanimage: stepped read, 63 bytes...    PASS
scanimage: stepped read, 31 bytes...    PASS
scanimage: stepped read, 15 bytes...    PASS
scanimage: stepped read, 7 bytes...     PASS
scanimage: stepped read, 3 bytes...     PASS
```

где 'hpaio:/usb/HP_LaserJet_M1536dnf_MFP?serial=00CND9D8YC9C' – актуальное имя подключенного устройства, которое можно взять из вывода предыдущей команды.

Для проверки работы сканера можно выполнить сканирование с сохранением результата в файл, например:

```
$ scanimage --format=png -d 'hpaio:/usb/HP_LaserJet_M1536dnf_MFP?serial=00CND9D8YC9C'
> ~/scan.png
```

Примечание. Для некоторых устройств Hewlett-Packard требуется установить актуальный плагин с сервера HP. Для установки плагина необходимо выполнить команду (должен быть установлен пакет `hplip`, при установке плагина потребуется ввести пароль суперпользователя):

```
$ hp-plugin -i
…
Enter option (d=download*, p=specify path, q=quit) ? d
…
Do you accept the license terms for the plug-in (y=yes*, n=no, q=quit)
? y
Please enter the root/superuser password:
```

Примечание. Для работы со сканерами Epson необходимо установить пакеты `epson-scan2`, `imagescan-sane`, `iscan-free`, `iscan-data` и `firmware-iscan` из репозитория:

```
# apt-get install epsonscan2 imagescan-sane iscan-free iscan-data
firmware-iscan
```

Для работы со сканерами Epson также может потребоваться скачать и установить пакет `epsonscan2-non-free-plugin` с официального сайта Epson.

4.5.2 Интерфейсы для сканирования (frontend)

Интерфейс – это программа, которая взаимодействует с SANE для получения отсканированного вывода в желаемом формате. SANE был разработан для взаимодействия с любым SANE-совместимым интерфейсом, командной строкой или на основе графического интерфейса пользователя:

- scanimage – интерфейс командной строки для управления сканированием;
- xsane – графический интерфейс для получения изображения со сканера. Может быть вызван через GIMP;
- сканер документов (simple-scan) – приложение с минимальным графическим интерфейсом.

4.6 Настройка загрузчика GRUB2

Grub Customizer – приложение для настройки загрузчика Grub в графическом интерфейсе. Grub Customizer позволяет редактировать (переименовать, удалить, скрыть) пункты меню загрузчика, цвета пунктов меню, изменять фоновое изображение загрузчика Grub.

П р и м е ч а н и е . Любая ошибка при редактировании настроек загрузчика может привести к неспособности системы загрузиться.

Чтобы запустить Grub Customizer следует выбрать «Меню MATE» → «Приложения» → «Администрирование» → «Grub Customizer».

Для запуска модуля потребуется ввести пароль пользователя root (Рис. 95).

Запуск Grub Customizer

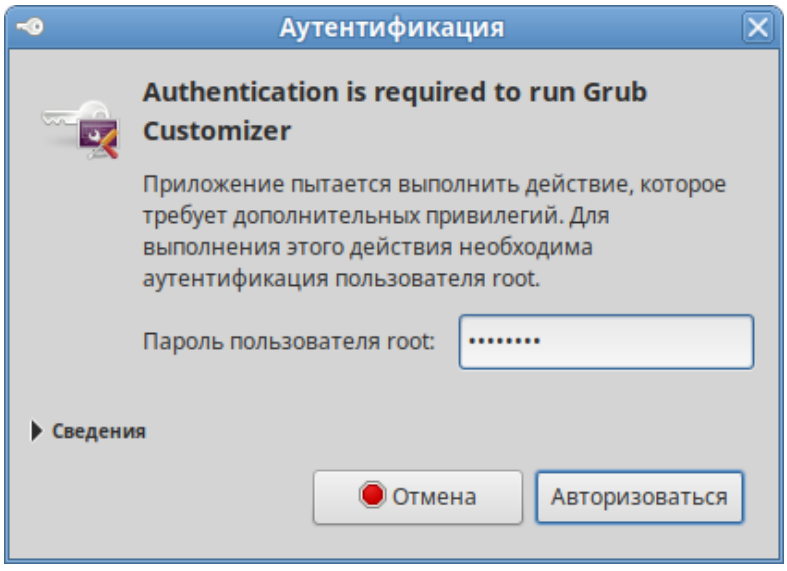

Рис. 95

На вкладке «Просмотреть настройки» показан список возможных вариантов загрузки операционных систем (Рис. 96).

Здесь можно изменить, создать и удалить пункт меню (выбрав соответствующий пункт в контекстном меню, либо на панели инструментов).

Вкладка «Просмотреть настройки»

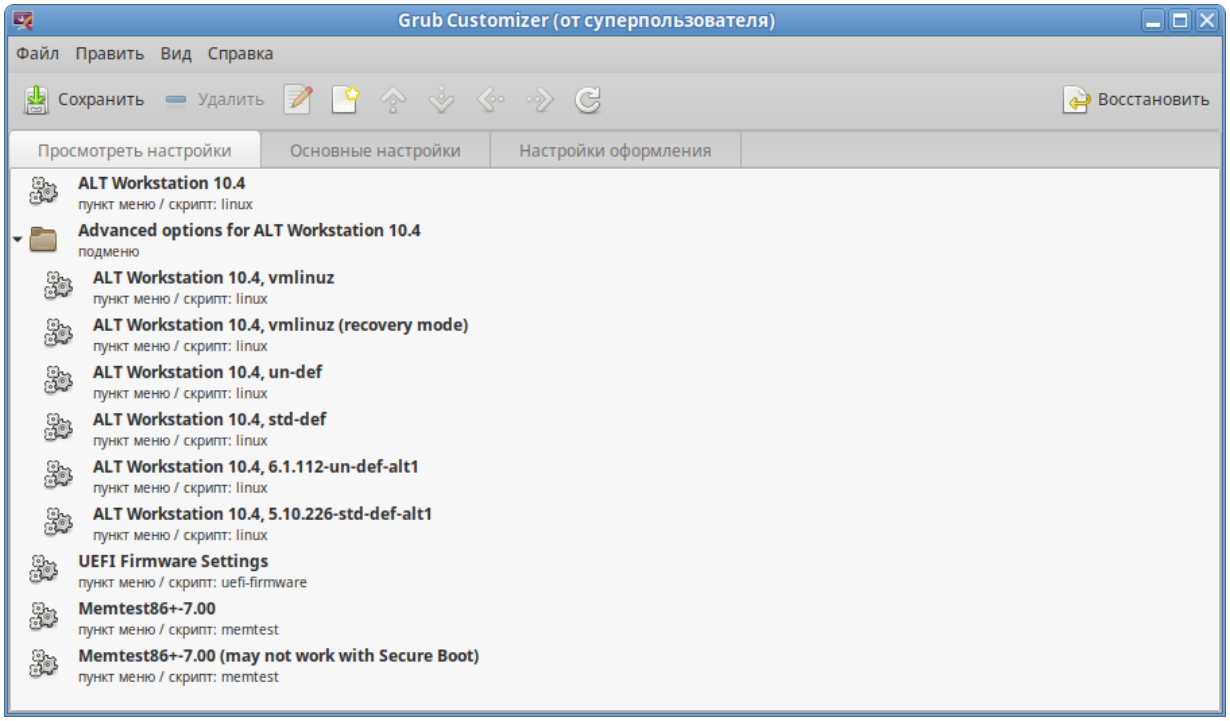

Рис. 96

На вкладке «Основные настройки» можно выбрать стандартно загружаемую ОС (по умолчанию, загружается первая по списку), настроить время ожидания загрузки после показа меню, указать параметры ядра (Рис. 97).

Вкладка «Основные настройки»

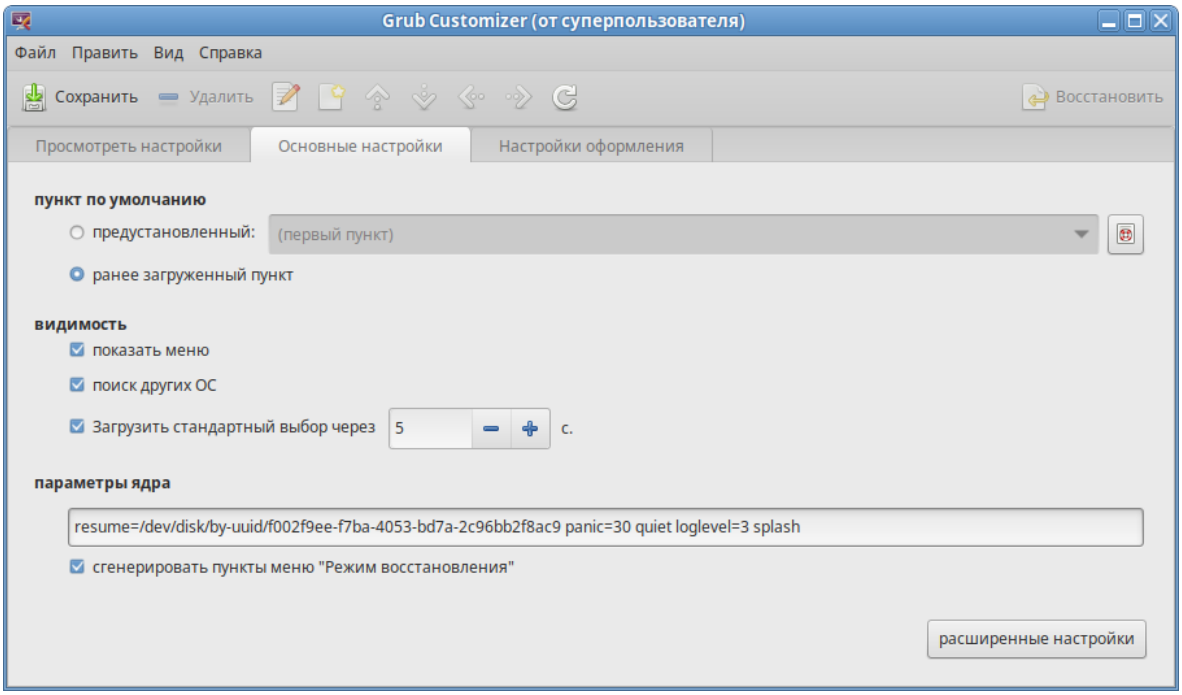

Рис. 97

На вкладке «Настройки оформления» можно менять способы отображения GRUB и внешний вид меню (Рис. 98).

Вкладка «Настройки оформления»

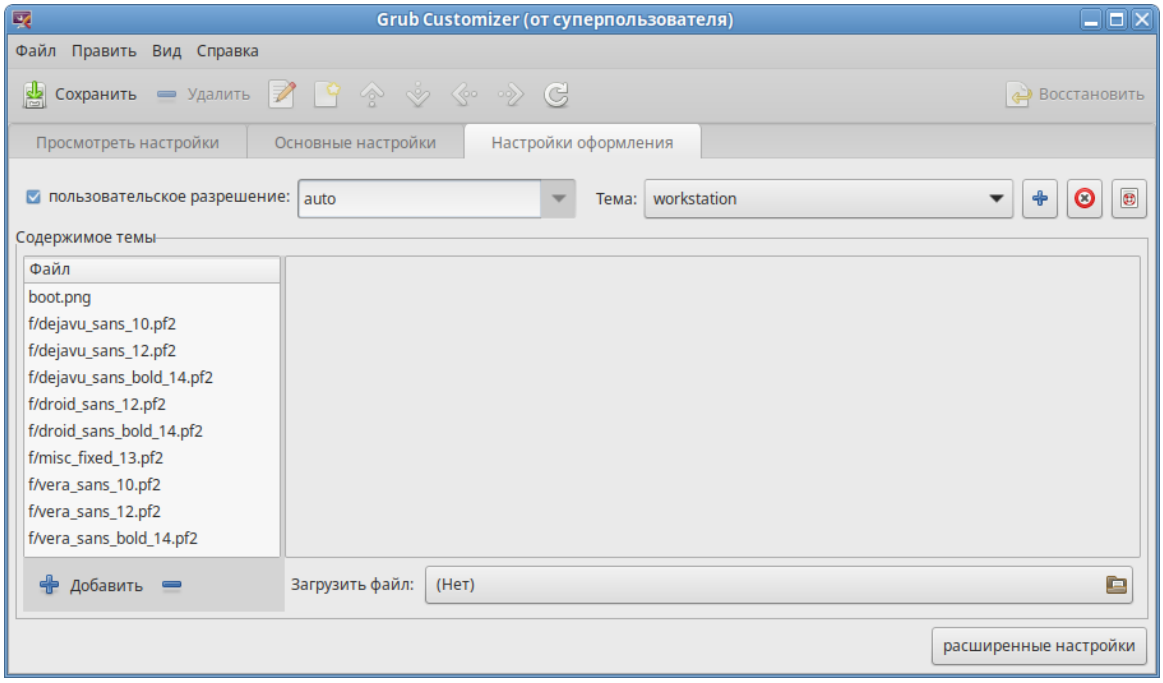

Рис. 98

Примечание. При выборе фонового изображения следует обратить внимание на параметры изображения, чтобы меню было контрастным, выделялось на фоне изображения и было легко читаемым.

4.7 Изменение пароля пользователя

Пароли пользователей в ОС «Альт Рабочая станция» первоначально определяет администратор системы при создании учетных записей пользователей. Однако пользователи имеют возможность в любое время изменить свой пароль.

Для запуска утилиты для смены своего пароля, следует выбрать «Меню MATE» → «Приложения» → «Параметры» → «UserPasswd».

Откроется окно, в котором необходимо ввести свой текущий (старый) пароль (Рис. 99).

Запрос старого пароля пользователя

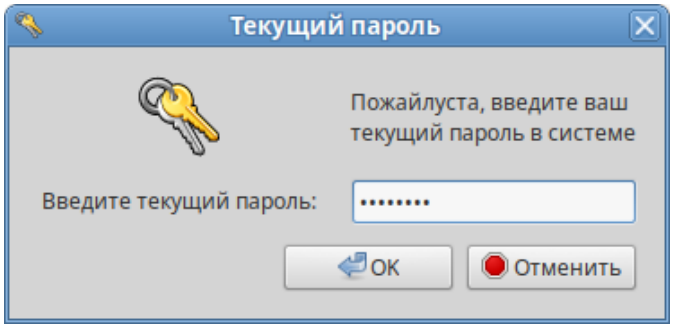

Рис. 99

Затем следует ввести новый пароль (Рис. 100) и повторить его (Рис. 101).

Новый пароль пользователя

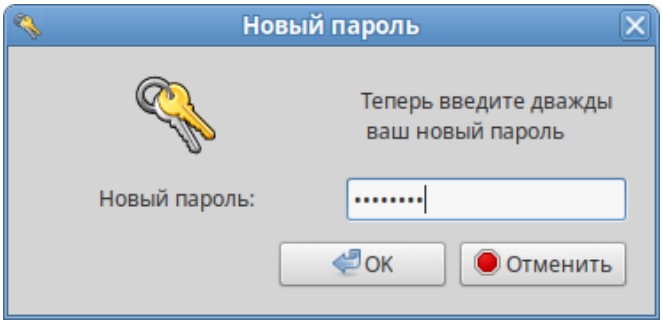

Рис. 100

Повторный ввод нового пароля пользователя

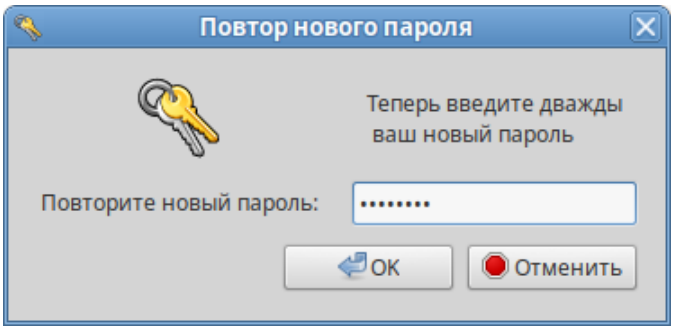

Рис. 101

Примечание. Новый пароль должен соответствовать техническим требованиям к паролям, заданным администратором системы.

4.8 Ввод рабочей станции в домен Active Directory

Ниже приведена инструкция по вводу рабочей станции под управлением ОС «Альт Рабочая станция» в домен Active Directory (работающий под Windows или под Samba AD в режиме DC). Параметры домена:

- TEST.ALT – имя домена;
- TEST – рабочая группа;
- HOST-15 – имя компьютера в Netbios;
- Administrator – имя пользователя-администратора;
- Pa$$word – пароль администратора.

4.8.1 Подготовка

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

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

Синхронизация времени с контроллером домена производится автоматически.

Для ввода компьютера в домен, на нём должен быть доступен сервер DNS, имеющий записи про контроллер домена Active Directory. Ниже приведен пример настройки сетевого интерфей-

са со статическим IP-адресом. При получении IP-адреса по DHCP данные о сервере DNS также должны быть получены от сервера DHCP.

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

- в ЦУС в разделе «Сеть» → «Ethernet интерфейсы» задать имя компьютера, указать в поле «DNS-серверы» DNS-сервер домена и в поле «Домены поиска» – домен для поиска (Рис. 102);
- в консоли:
  - задать имя компьютера:
    ```
    # hostnamectl set-hostname host-15.test.alt
    ```
  - в качестве первичного DNS должен быть указан DNS-сервер домена. Для этого необходимо создать файл /etc/net/ifaces/enp0s3/resolv.conf со следующим содержимым:
    ```
    nameserver 192.168.0.122
    ```
    где 192.168.0.122 – IP-адрес DNS-сервера домена.
  - указать службе resolvconf, использовать DNS контроллера домена и домен для поиска. Для этого в файле /etc/resolvconf.conf добавить/отредактировать следующие параметры:
    ```
    interface_order='lo lo[0-9]* lo.* enp0s3'
    search_domains= test.alt
    ```
    где enp0s3 – интерфейс, на котором доступен сервер, `test.alt` – домен.
  - обновить DNS адреса:
    ```
    # resolvconf –u
    ```

В результате выполненных действий 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 необходимо перезагрузить систему.

Настройка на использование DNS-сервера домена

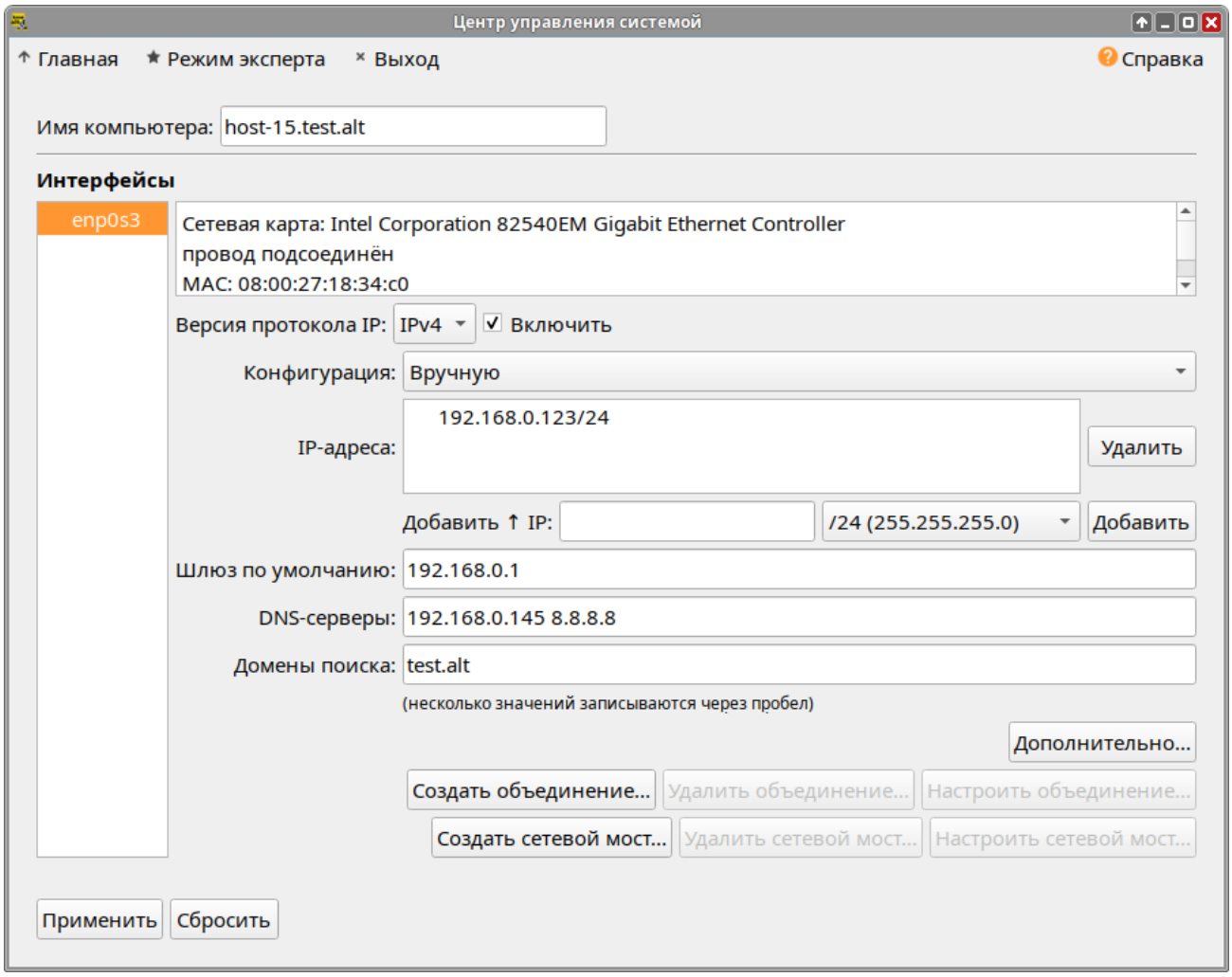

Рис. 102

4.8.2 Ввод в домен

4.8.2.1 Ввод в домен в ЦУС

Для ввода рабочей станции в домен необходимо запустить ЦУС («Меню MATE» → «Приложения» → «Администрирование» → «Центр управления системой»). В ЦУС следует перейти в раздел «Пользователи» → «Аутентификация». Здесь необходимо выбрать пункт «Домен Active Directory» (Рис. 103) и заполнить поля, после чего нажать кнопку «Применить».

В открывшемся окне (Рис. 104) необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку «ОК».

При успешном подключении к домену, отобразится соответствующая информация (Рис. 105).

Далее необходимо перезагрузить рабочую станцию для применения всех настроек.

Ввод в домен в «Центре управления системой»

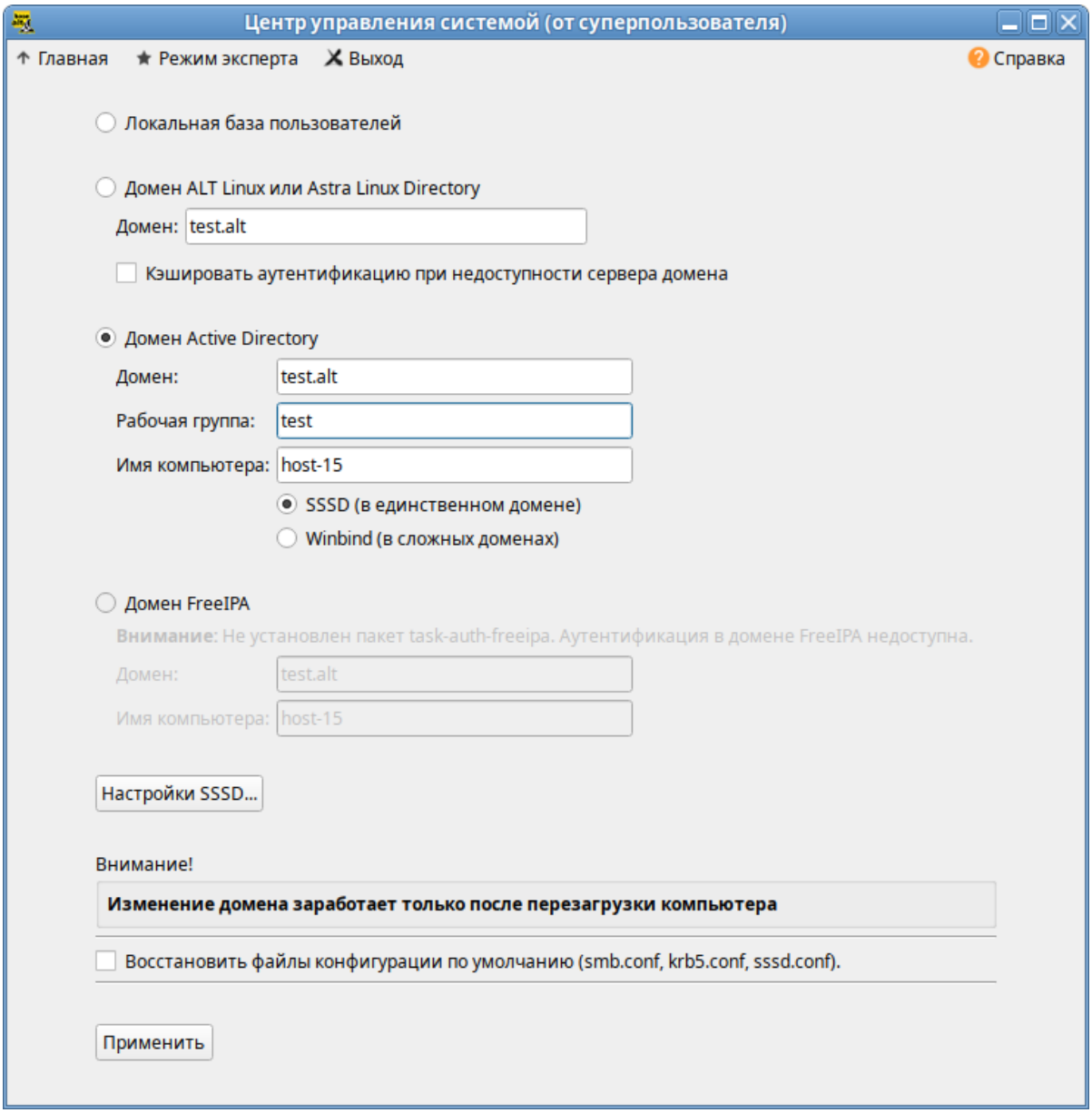

Рис. 103

Параметры учетной записи с правами подключения к домену

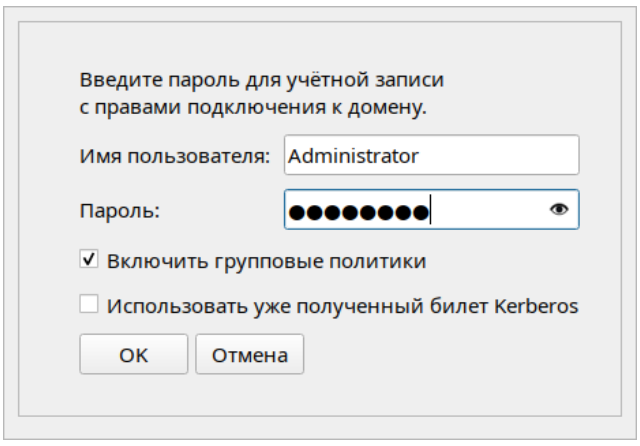

Рис. 104

Успешное подключение к домену

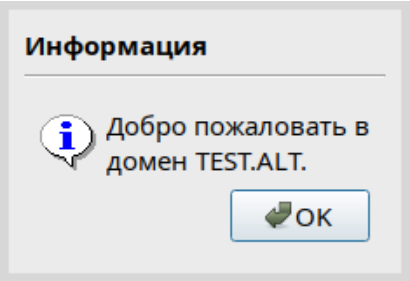

Рис. 105

4.8.2.2 Ввод в домен в командной строке

Для ввода рабочей станции в домен можно воспользоваться следующей командой:

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

4.8.2.3 Проверка работы

Проверить подключение к домену:

```
$ getent passwd ivanov
ivanov:*:417001106:417000513: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, 21 окт 2024 08:46:50 EET
KDC server: 192.168.0.122
Server time offset: 0
Last machine account password change: Пн, 21 окт 2024 08:47:43 EET


# net ads testjoin
Join is OK
```

Примечание. Список пользователей на сервере можно посмотреть, выполнив команду:

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

4.8.3 Вход пользователя

В окне входа в систему необходимо ввести логин учетной записи пользователя домена и нажать кнопку «Войти» (Рис. 106), в открывшемся окне ввести пароль, соответствующий этой учетной записи и нажать кнопку «Войти» (Рис. 107).

Вход пользователя

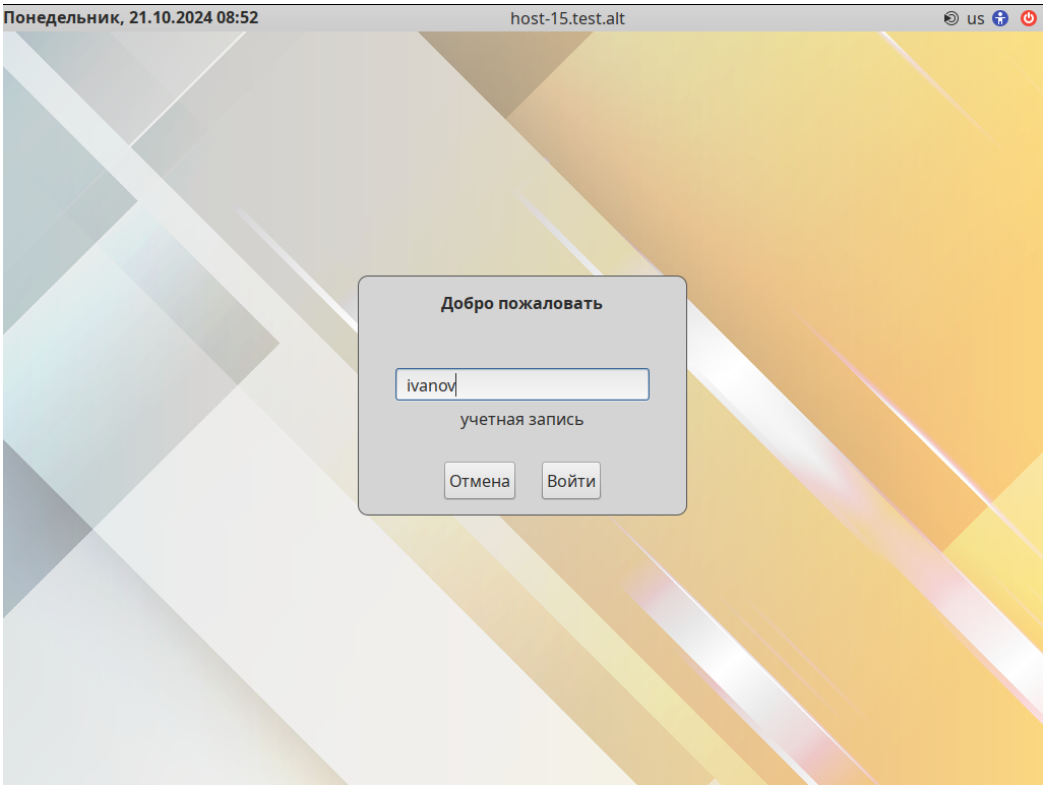

Рис. 106

Примечание. Чтобы настроить автоматическое заполнение поля «Имя пользователя» именем последнего пользователя, входившего в систему, в файле `/etc/lightdm/lightdm-gtk-greeter.conf` (группа [greeter]) необходимо указать:

```
enter-username = true
```

Примечание. В случае использования в окне логина символов верхнего регистра (например, Irina.Soboleva вместо irina.soboleva) или лишних символов (не использующихся для стандартного имяобразования в Linux) может наблюдаться некорректное поведение системы (например, не выставляются переменные окружения XDG_RUNTIME_DIR и DBUS_SESSION_BUS_ADDRESS). Для возможности использовать для входа привычные способы написания (с доменным суффиксом, точками, символами верхнего регистра) необходимо выполнить команду:

```
# control pam_canonicalize_user enabled
```

или в файле `/etc/pam.d/system-auth-common` расскомментировать строку:

```
auth  required  pam_canonicalize_user.so
```

Запрос пароля

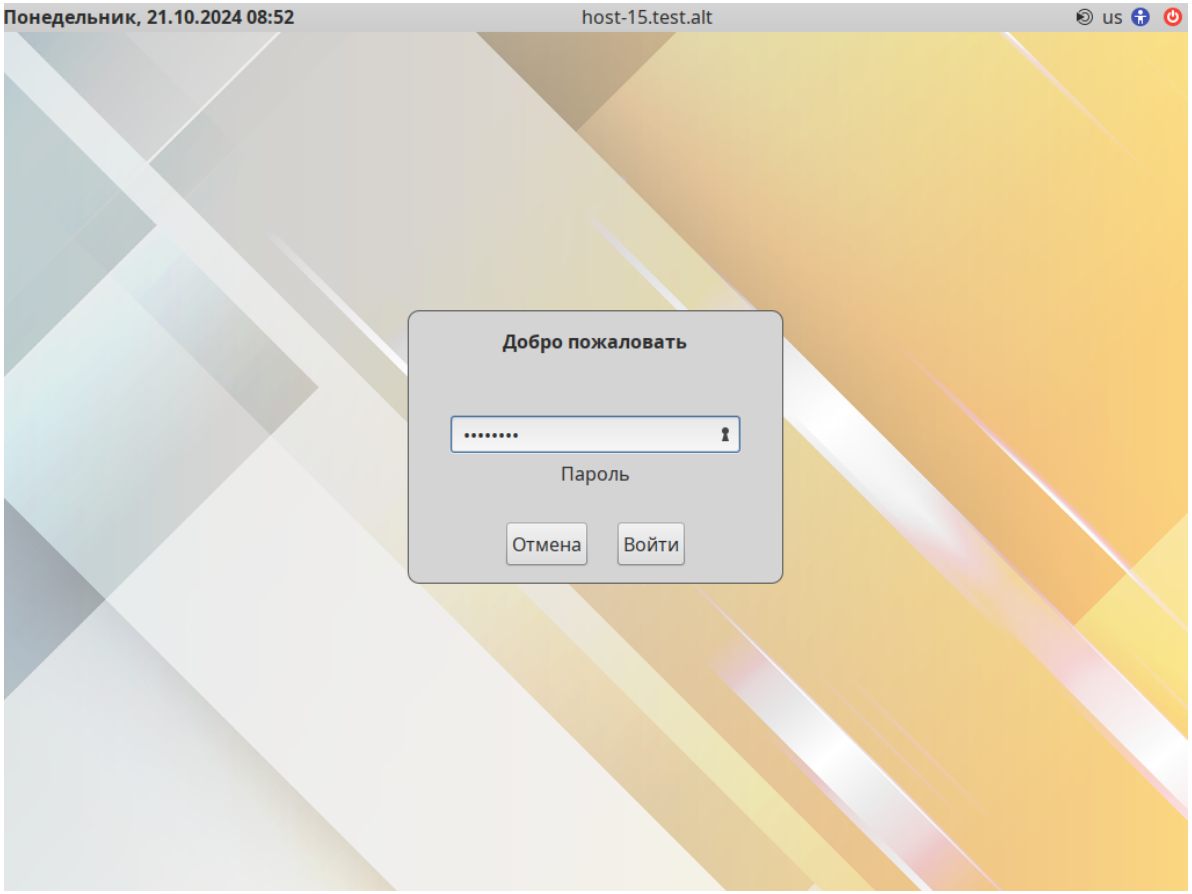

Рис. 107

4.8.4 Отображение глобальных групп на локальные роли

При вводе машины в домен создаются следующие локальные роли:

- роль пользователей (users);
- роль пользователей с расширенными правами (powerusers);
- роль локальных администраторов (localadmins).

Локальные роли users и localadmins назначаются для глобальных групп в домене.

Список назначенных ролей и привилегий:

```
# rolelst
domain users:users
domain admins:localadmins
localadmins:wheel,vboxadd,vboxusers
powerusers:remote,vboxadd,vboxusers
users:cdwriter,cdrom,audio,video,proc,radio,camera,floppy,xgrp,scan-
ner,uucp,vboxusers,fuse,vboxadd
vboxadd:vboxsf
# id ivanov
```

```
uid=906201103(ivanov) gid=906200513(domain users) группы=906200513(do-
main users),906201107(sales),
906201114(office),100(users),80(cdwriter),22(cdrom),81(audio),475(vide
o),19(proc),
83(radio),444(camera),71(floppy),498(xgrp),499(scanner),14(uucp),462(v
boxusers),464(fuse),488(vboxadd),487(vboxsf)
```

Если необходимо выдать права администраторов пользователям, которые не являются администраторами домена (Domain Admins), то нужно на контроллере домена завести новую группу в AD (например, PC Admins):

```
# samba-tool group add 'PC Admins'
Added group PC Admins
```

Добавить туда необходимых пользователей (например, пользователя ivanov):

```
# samba-tool group addmembers 'PC Admins' ivanov
Added members to group PC Admins
```

Затем на машине, введённой в домен, добавить роль для данной группы:

```
# roleadd 'PC Admins' localadmins
# rolelst
domain users:users
domain admins:localadmins
pc admins:localadmins
localadmins:wheel,vboxadd,vboxusers
powerusers:remote,vboxadd,vboxusers
users:cdwriter,cdrom,audio,video,proc,radio,camera,floppy,xgrp,scan-
ner,uucp,vboxusers,fuse,vboxadd
vboxadd:vboxsf
```

После этого пользователь, входящий в группу PC Admins, сможет получать права администратора.

4.8.5 Подключение файловых ресурсов

Рассматриваемые способы позволяют подключать файловые ресурсы (file shares) для доменного пользователя без повторного ввода пароля (SSO, Single Sign-On).

4.8.5.1 Подключение с использованием gvfs

Недостаток такого способа – необходимо открыть ресурс в файловом менеджере (Caja, Pcmanfm). Однако можно открывать любые ресурсы на любых серверах, входящие в домен Active Directory.

1. Установить необходимые пакеты:

```
# apt-get install fuse-gvfs gvfs-backend-smb gvfs-utils
```

2. Включить пользователя в группу `fuse`:

```
# gpasswd -a <пользователь> fuse
```

3. Войти под доменным пользователем.

4. Открыть ресурс в файловом менеджере (например, по адресу `smb://server/sysvol`). Ресурс смонтирован по пути `/run/<uid_пользователя>/gvfs`.

Другой вариант (полезно для скриптов в автозапуске):

```
gvfs-mount smb://server/sysvol/
```

Примечание. Если необходимо открывать что-то с ресурса в WINE, в winecfg необходимо добавить диск с путём `/run/<uid_пользователя>/gvfs`.

4.8.5.2 Подключение с использованием pam_mount

В этом случае заданный ресурс подключается с заданного сервера автоматически при каждом входе доменным пользователем.

1. 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
```

2. 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
```

3. 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=krb5,cruid=%
(USERUID),nounix,uid=%(USERUID),gid=%
(USERGID),file_mode=0664,dir_mode=0775" />
```

где

- uid="10000-2000200000" – диапазон присваиваемых uid для доменных пользователей (подходит для Winbind и для SSSD);
- server="dc1.test.alt" – имя сервера с ресурсом;
- path="sysvol" – имя файлового ресурса на сервере;

- mountpoint="~/share" – путь монтирования в домашнем каталоге пользователя.

Опционально можно добавить:

- sgrp="group_name" — имя группы, при членстве пользователя в которой, папка будет примонтирована.

Примечание. По умолчанию для монтирования используется smb версии 1.0, если у вас он отключен, то укажите в параметрах версию 2 или 3:

```
<volume uid="10000-2000200000" fstype="cifs" server="dc1.test.alt "
path="sysvol" mountpoint="~/share" options="sec=krb5,vers=2.0,cruid=%
(USERUID),nounix,uid=%(USERUID),gid=%
(USERGID),file_mode=0664,dir_mode=0775" />
```

4.9 Групповые политики

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

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

Инструменты управления групповыми политиками будут установлены в систему, если при установке дистрибутива отметить пункт «Групповые политики» → «Инструменты администрирования».

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

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

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

Политики подразделяются на политики для компьютеров (Machine) и политики для пользователей (User). Политики для компьютеров применяются на хосте в момент загрузки, а также в мо-

мент явного или регулярного запроса планировщиком (раз в час). Пользовательские политики применяются в момент входа в систему.

Групповые политики можно использовать для разных целей, например:

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

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

4.9.1 Развертывание групповых политик

Процесс развёртываня групповых политик:

1. Развернуть сервер Samba AD DC (например, на машине с установленной ОС «Альт Сервер»).
2. На сервере Samba AD DC установить административные шаблоны:

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

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

- скачать и установить ADMX-файлы от Microsoft, выполнив команду:

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

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

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

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

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

3. Ввести клиентскую рабочую станцию в домен Active Directory по инструкции (см. «Ввод рабочей станции в домен Active Directory»).

Примечание. На рабочей станции должен быть установлен пакет `alterator-gpupdate`:

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

Для автоматического включения групповых политик, при вводе в домен, в окне ввода имени и пароля пользователя, имеющего право вводить машины в домен, отметить пункт «Включить групповые политики» (Рис. 104).

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

Примечание. Если клиентская рабочая станция уже находится в домене, можно вручную включить групповые политики с помощью модуля alterator-gpupdate. Для этого в ЦУС в разделе «Система» → «Групповые политики» следует выбрать шаблон локальной политики («Сервер», «Рабочая станция» или «Контроллер домена») и установить отметку в пункте «Управление групповыми политиками» (Рис. 108).

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

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

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

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

Модуль ЦУС «Групповые политики»

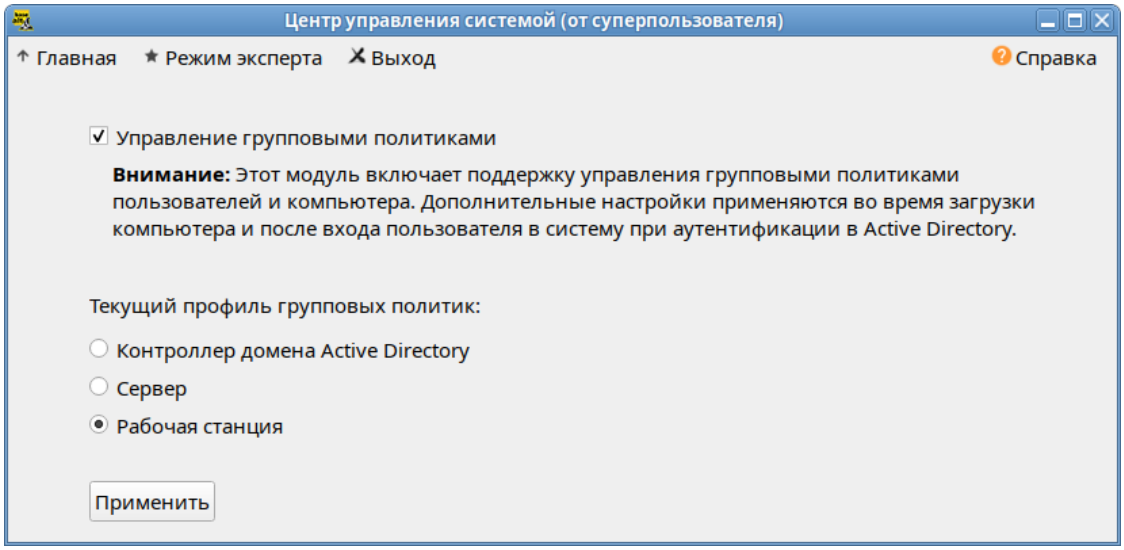

Рис. 108

5. Настроить, если это необходимо, RSAT на машине с ОС Windows (управление сервером Samba с помощью RSAT поддерживается из среды до Windows 2012R2 включительно):

- ввести машину с ОС Windows в домен (управление сервером Samba с помощью RSAT поддерживается из среды до Windows 2012R2 включительно);
- включить компоненты удаленного администрирования (этот шаг можно пропустить, если административные шаблоны были установлены на контроллере домена). Для задания конфигурации с помощью RSAT необходимо скачать файлы административных шаблонов (файлы ADMX) и зависящие от языка файлы ADML из репозитория http://git.altlinux.org/gears/a/admx-basealt.git (https://github.com/altlinux/admx-basealt) и разместить их в каталоге \\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\PolicyDefinitions.
- корректно установленные административные шаблоны будут отображены в оснастке «Редактор управления групповыми политиками» в разделе «Конфигурация компьютера»/ «Конфигурация пользователя» → «Политики» → «Административные шаблоны» (Рис. 109).

Административные шаблоны в консоли gpme.msc

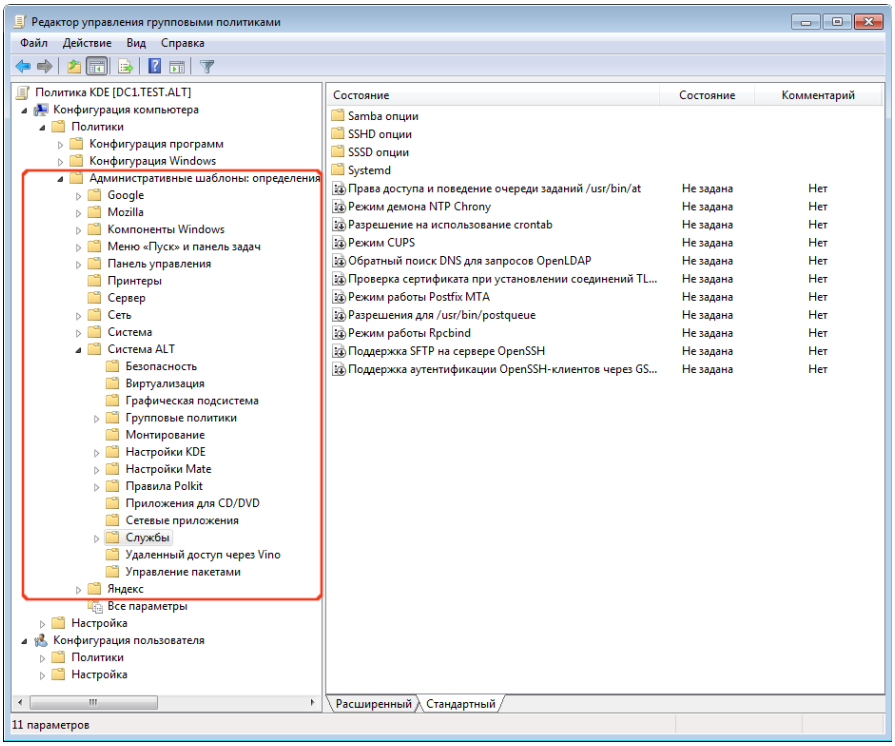

Рис. 109

4.9.2 Пример создания групповой политики

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

- добавить доменные устройства (компьютеры/пользователи) в подразделение (OU) (инструмент ADMC или оснастка Active Directory «Пользователи и компьютеры»);
- создать политику и назначить её на OU (ADMC или оснастка «Управление групповой политикой»);
- отредактировать параметры политики (GPUI или оснастка «Редактор управления групповыми политиками»).

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

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

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

Далее запустить ADMC из меню («Меню MATE» → «Системные» → «ADMC») или командой `admc`:

```
$ admc
```

Интерфейс ADMC показан на Рис. 110.

Интерфейс ADMC

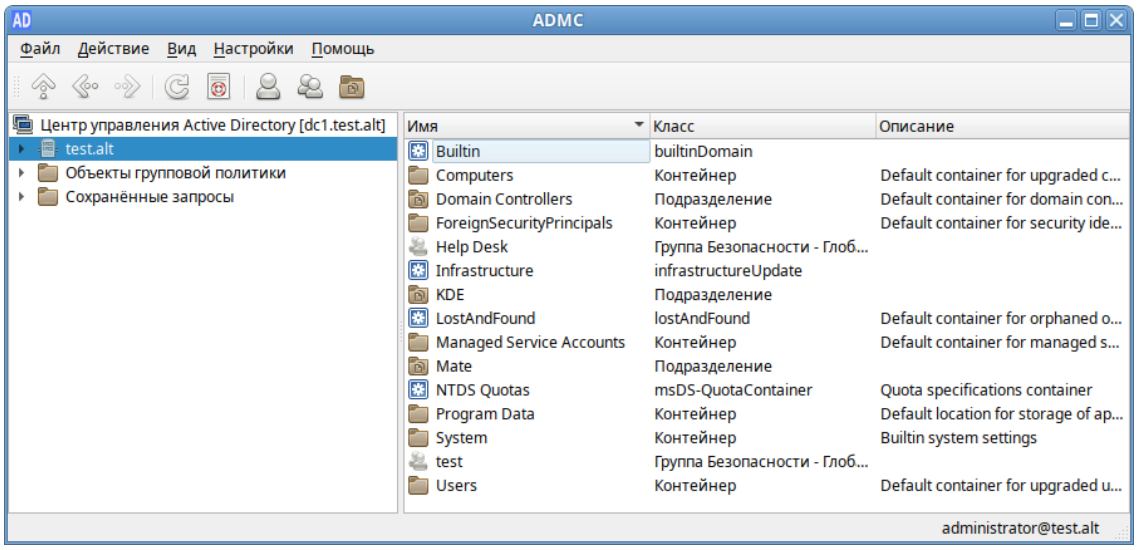

Рис. 110

Для создания подразделения следует:

- в контекстном меню домена выбрать пункт «Создать» → «Подразделение» (Рис. 111);
- в открывшемся окне ввести название подразделения (например, OU) и нажать кнопку «ОК» (Рис. 112).

ADMC. Создание нового подразделения

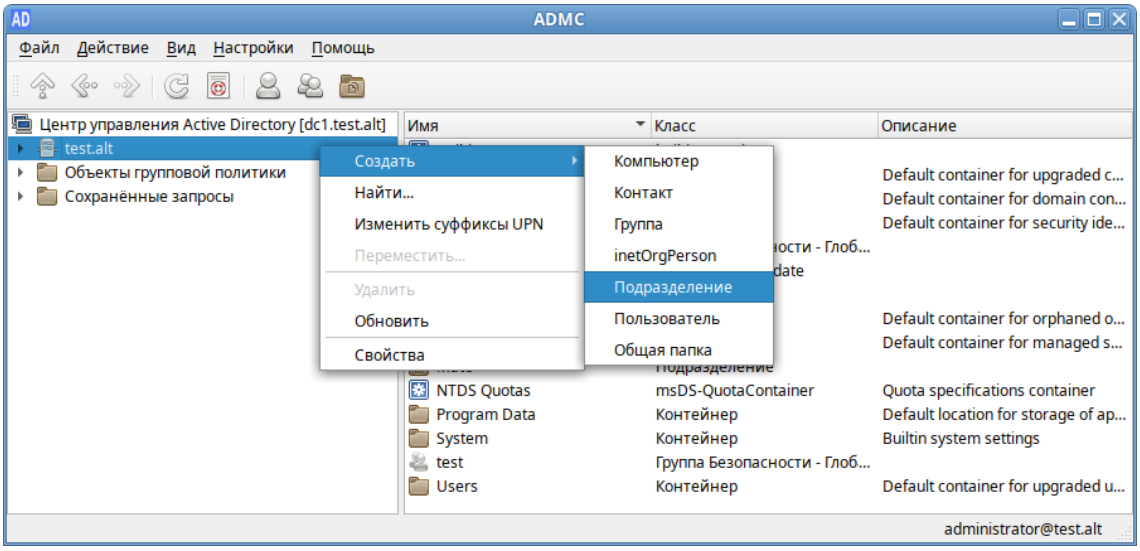

Рис. 111

ADMC. Новое подразделение

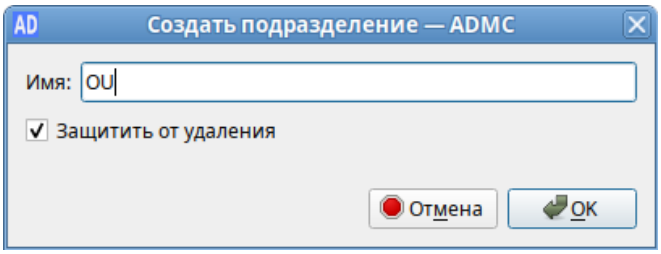

Рис. 112

Далее необходимо переместить компьютеры и пользователей домена в подразделение OU (Рис. 113):

- в контекстном меню пользователя/компьютера выбрать пункт «Переместить…»;
- в открывшемся диалоговом окне «Выбор контейнера – ADMC» выбрать контейнер, в который следует переместить учетную запись пользователя.

Для создания политики для подразделения:

- в контекстном меню подразделения (в папке «Объекты групповой политики») выбрать пункт «Создать политику и связать с этим подразделением» (Рис. 114);
- в открывшемся окне ввести название политики и нажать кнопку «ОК» (Рис. 115).

Компьютеры и пользователи в подразделении OU

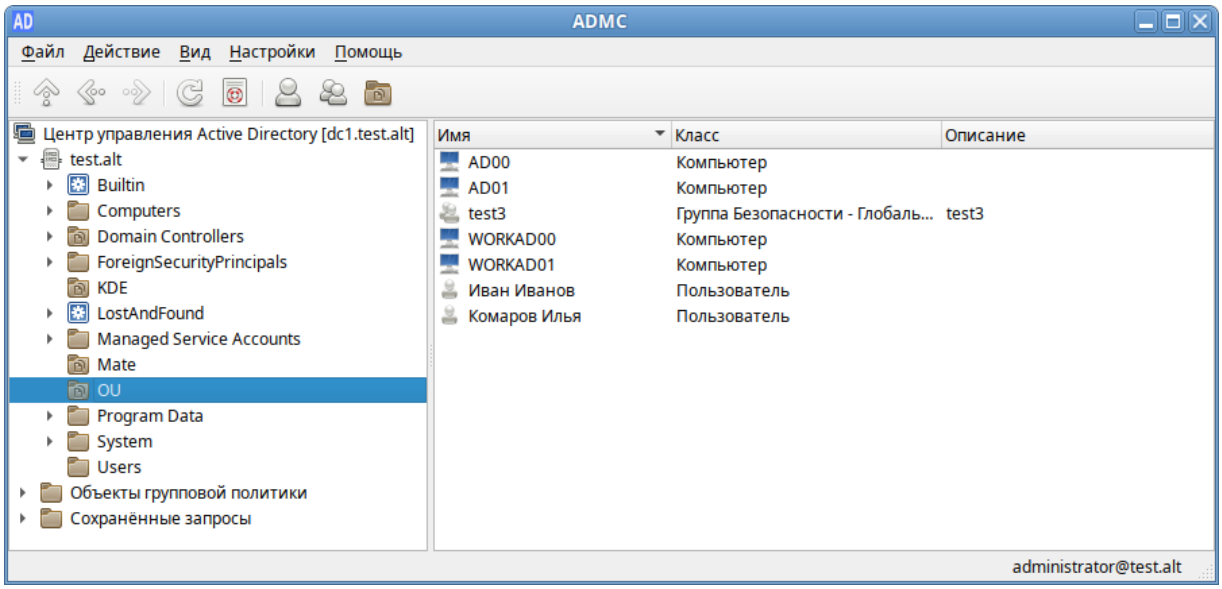

Рис. 113

ADMC. Контекстное меню подразделения в объектах групповых политик

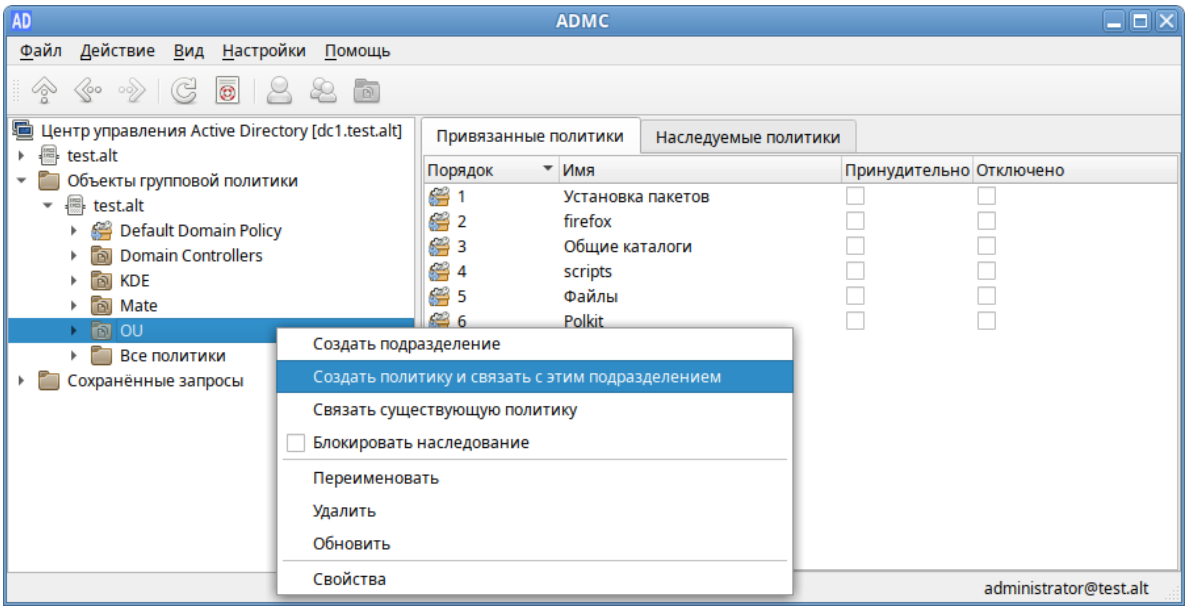

Рис. 114

ADMC. Создание объекта групповой политики

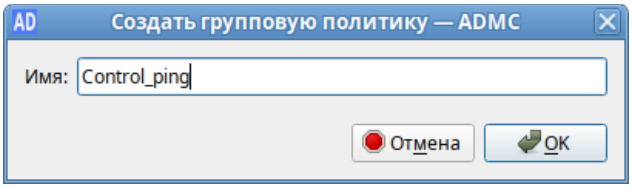

Рис. 115

Редактирование настроек групповой политики:

- в контекстном меню политики выбрать пункт «Изменить…» (Рис. 116);
- откроется окно редактирования групповых политик (GPUI) (Рис. 117);
- перейти в «Компьютер» → «Административные шаблоны» → «Система ALT». Здесь есть несколько разделов, соответствующих категориям control. Выбрать раздел «Сетевые приложения», в правом окне редактора отобразится список политик (Рис. 118);
- щелкнуть левой кнопкой мыши на политике «Разрешения для /usr/bin/ping». Откроется диалоговое окно настройки политики. Выбрать параметр «Включено», в выпадающем списке «Кому разрешено выполнять» выбрать пункт «Только root» и нажать кнопку «ОК» (Рис. 119);
- после обновления политики на клиенте, выполнять команду ping сможет только администратор:

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

```
# control ping
restricted
```

ADMC. Контекстное меню объекта групповой политики

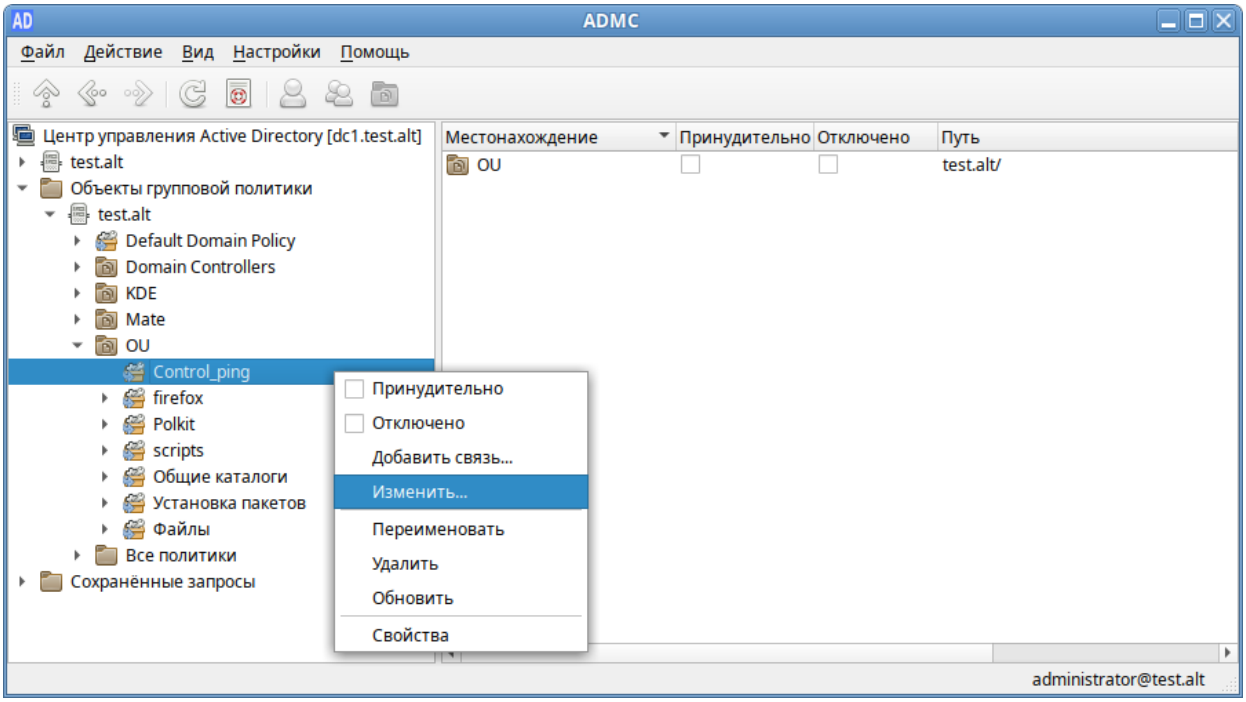

Рис. 116

Модуль редактирования настроек клиентской конфигурации (GPUI)

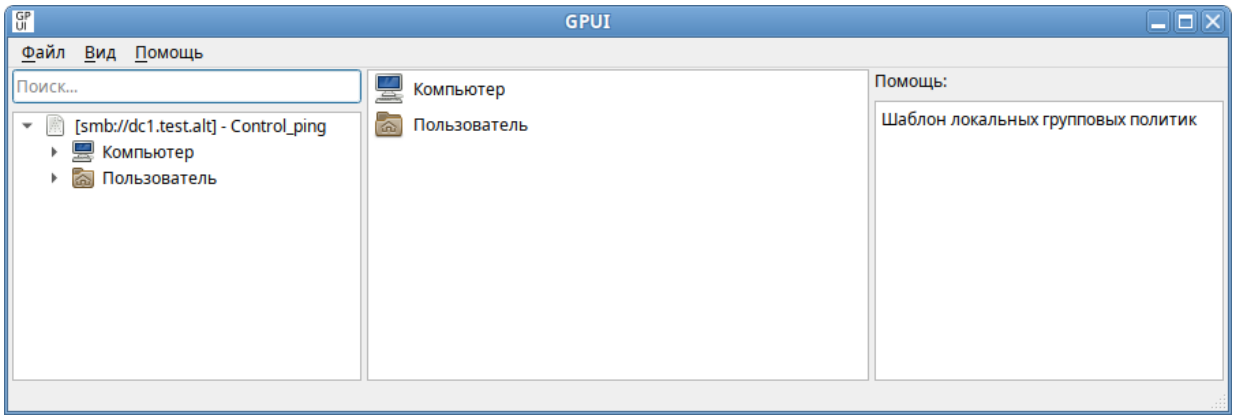

Рис. 117

Модуль редактирования настроек клиентской конфигурации (GPUI)

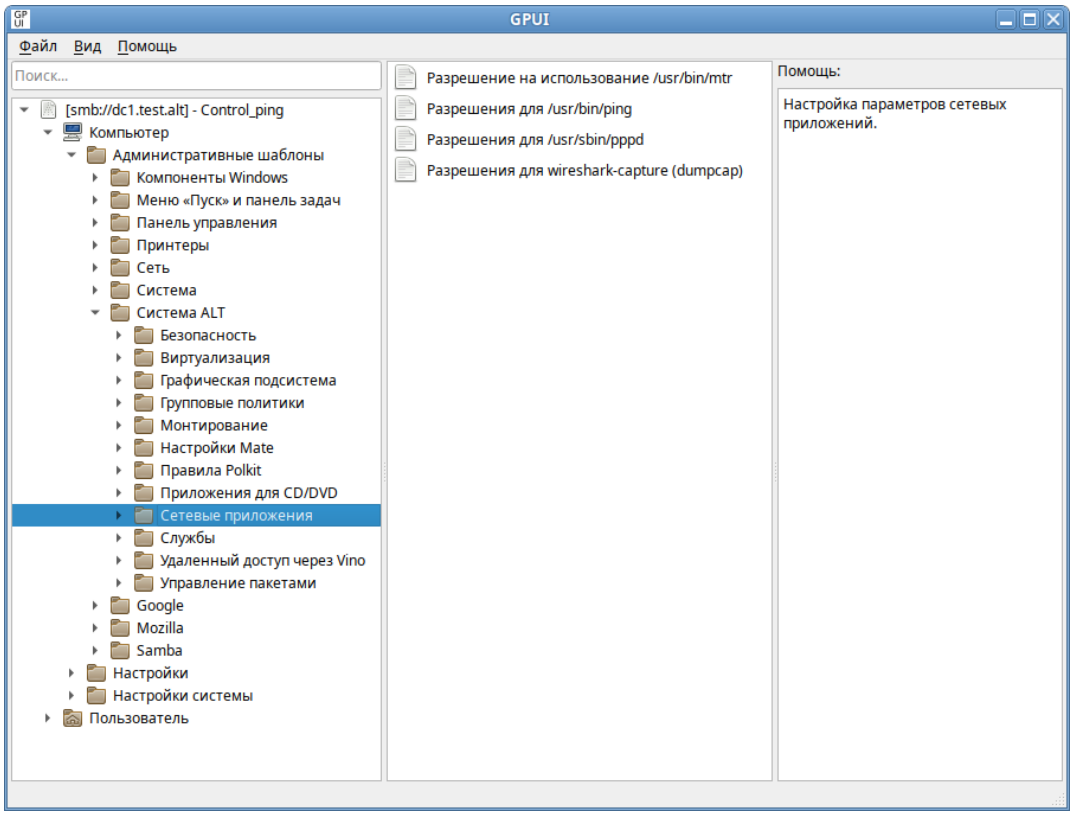

Рис. 118

GPUI. Диалоговое окно настройки политики

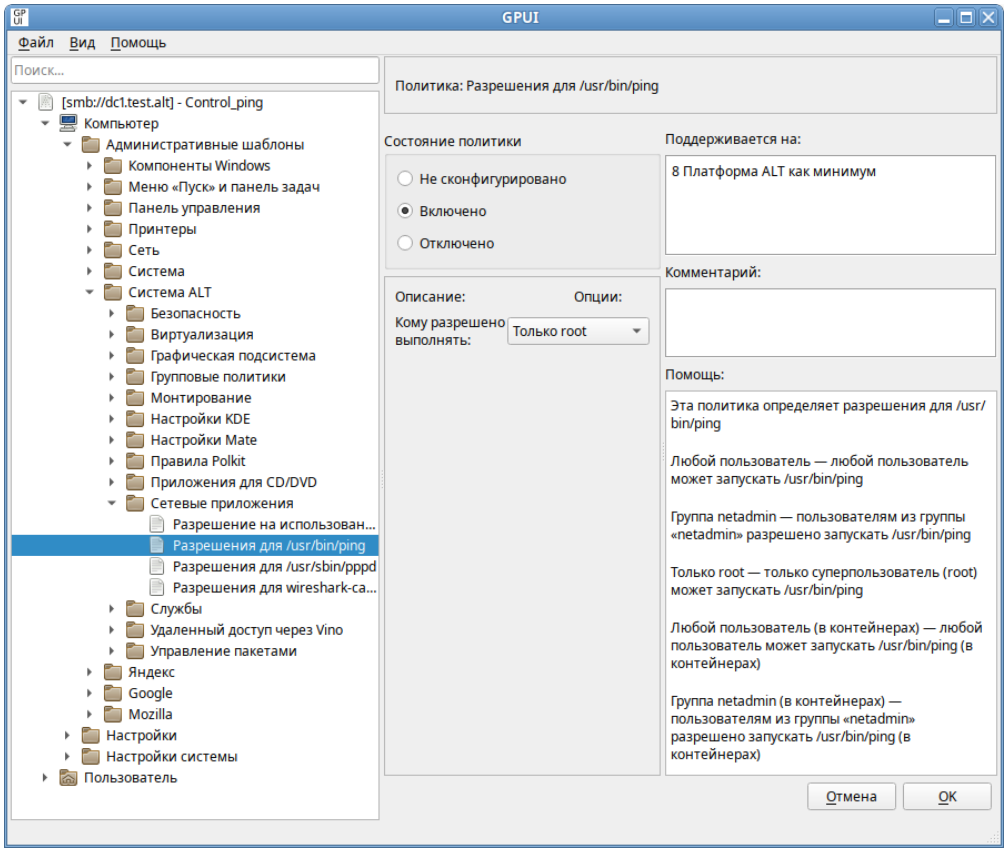

Рис. 119

Пример создания групповой политики на машине с ОС Windows:

- на машине, с установленным RSAT, открыть оснастку «Управление групповыми политиками» (gpmc.msc);
- создать новый объект групповой политики (GPO) и связать его с подразделением (OU), в который входят машины или учетные записи пользователей;
- в контекстном меню GPO, выбрать пункт «Изменить…». Откроется редактор GPO;
- перейти в раздел «Конфигурация компьютера» → «Политики» → «Административные шаблоны» → «Система ALT». Здесь есть несколько подразделов, соответствующих категориям control. Выбрать раздел «Сетевые приложения», в правом окне редактора отобразится список политик (Рис. 120);
- дважды щелкнуть левой кнопкой мыши на политике «Разрешения для /usr/bin/ping». Откроется диалоговое окно настройки политики (Рис. 121). Выбрать параметр «Включить», в выпадающем списке «Кому разрешено выполнять» выбрать пункт «Только root» и нажать кнопку «Применить».

Раздел «Сетевые приложения»

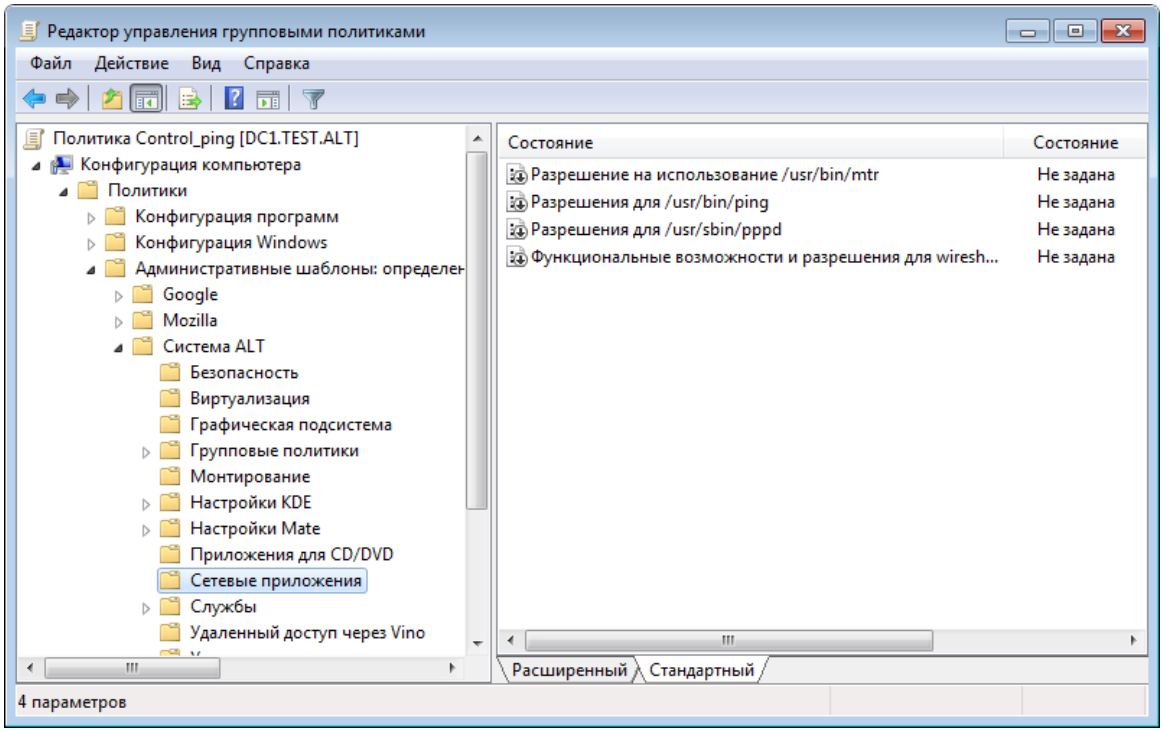

Рис. 120

Политика «Разрешения для /usr/bin/ping»

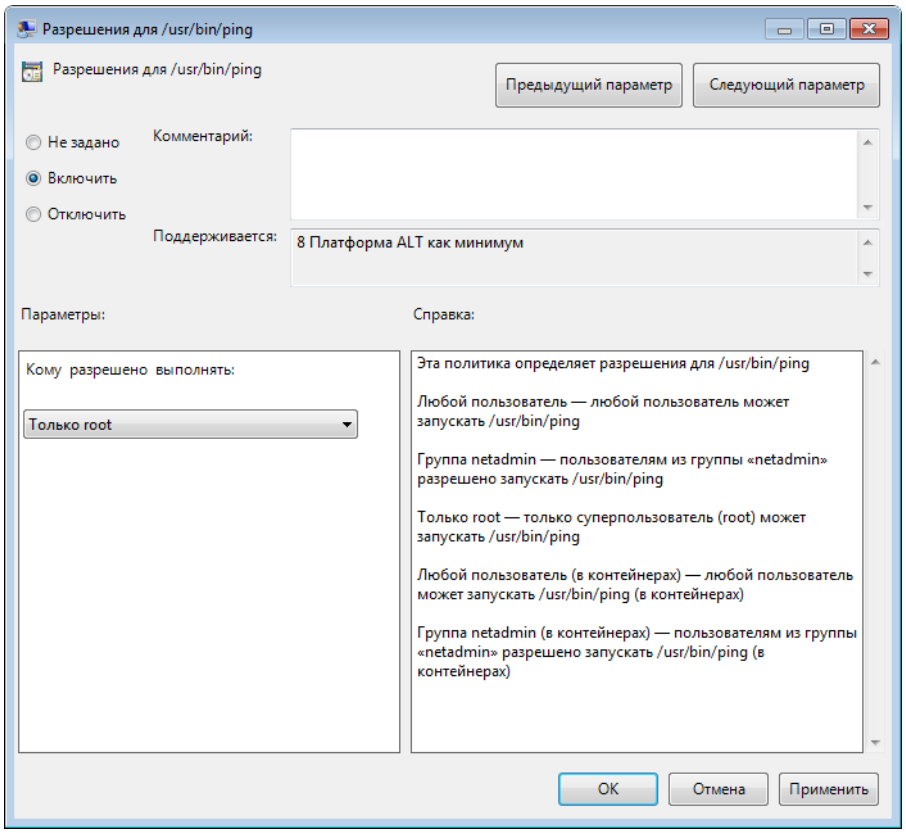

Рис. 121

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

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

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

4.10 Ввод рабочей станции в домен FreeIPA

Ниже приведена инструкция по вводу рабочей станции под управлением ОС «Альт Рабочая станция» в домен FreeIPA.

4.10.1 Установка FreeIPA клиента

Установить необходимые пакеты:

```
# apt-get install freeipa-client libsss_sudo krb5-kinit bind-utils libbind zip task-auth-freeipa
```

Примечание. Очистить конфигурацию freeipa-client невозможно. В случае если это необходимо (например, для удаления, переустановки freeipa-client) следует переустановить систему.

4.10.2 Настройка сети

Клиентские компьютеры должны быть настроены на использование DNS-сервера, который был сконфигурирован на сервере FreeIPA во время его установки. При получении IP-адреса по DHCP данные о сервере DNS также должны быть получены от сервера DHCP. Ниже приведен пример настройки сетевого интерфейса со статическим IP-адресом.

В сетевых настройках необходимо указать использовать сервер FreeIPA для разрешения имен. Эти настройки можно выполнить как в графическом интерфейсе, так и в консоли:

- в ЦУС в разделе «Сеть» → «Ethernet интерфейсы» задать имя компьютера, указать в поле «DNS-серверы» IP-адрес FreeIPA сервера и в поле «Домены поиска» – домен для поиска (Рис. 122);
- в консоли:
  - задать имя компьютера:
    ```
    # hostnamectl set-hostname comp02.example.test
    ```
  - добавить DNS сервер, для этого необходимо 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 eth0 – интерфейс, на котором доступен FreeIPA сервер, example.test – домен.
  - обновить DNS адреса:
    ```
    # resolvconf -u
    ```

Настройка на использование DNS-сервера FreeIPA

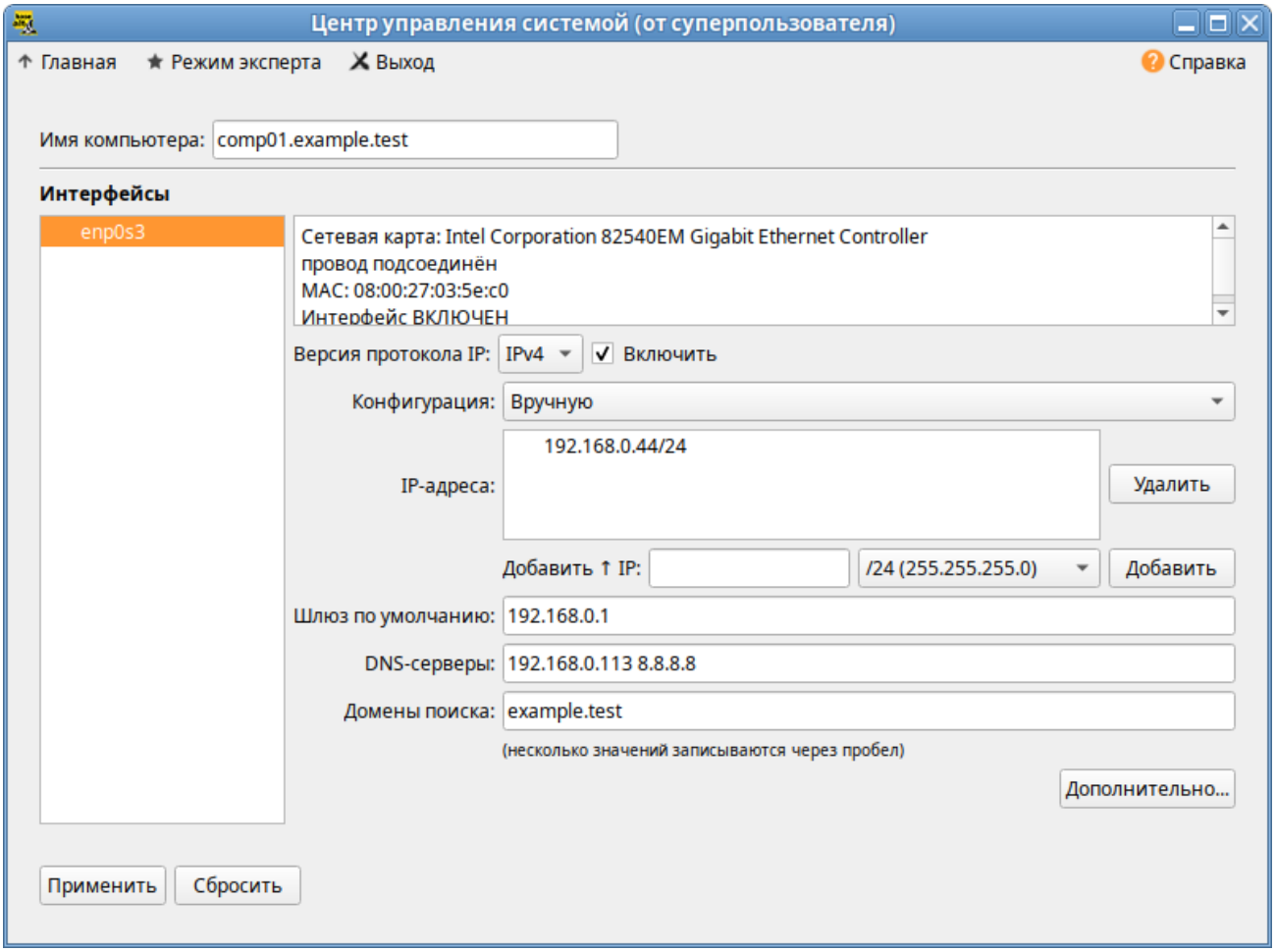

Рис. 122

В результате выполненных действий в файле `/etc/resolvconf.conf` должны появиться строки:

```
search example.test
nameserver 192.168.0.113
```

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

4.10.3 Подключение к серверу в ЦУС

Для ввода рабочей станции в домен FreeIPA, необходимо в ЦУС перейти в раздел «Пользователи» → «Аутентификация».

В открывшемся окне следует выбрать пункт «Домен FreeIPA», заполнить поля «Домен» и «Имя компьютера» (Рис. 123), затем нажать кнопку «Применить».

Ввод в домен FreeIPA в Центре управления системой

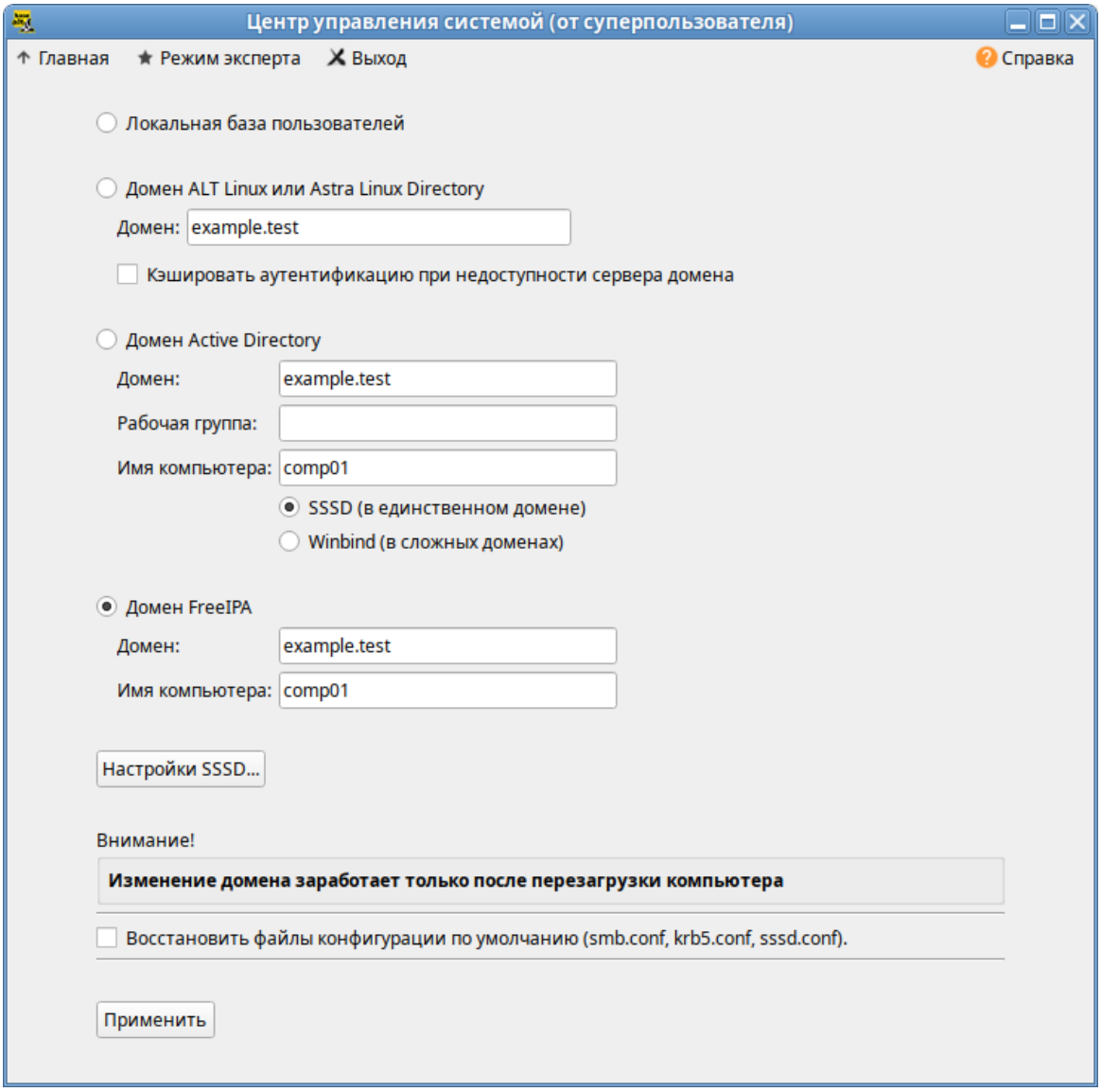

Рис. 123

В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль (Рис. 124) и нажать кнопку «ОК».

Параметры учетной записи с правами подключения к домену

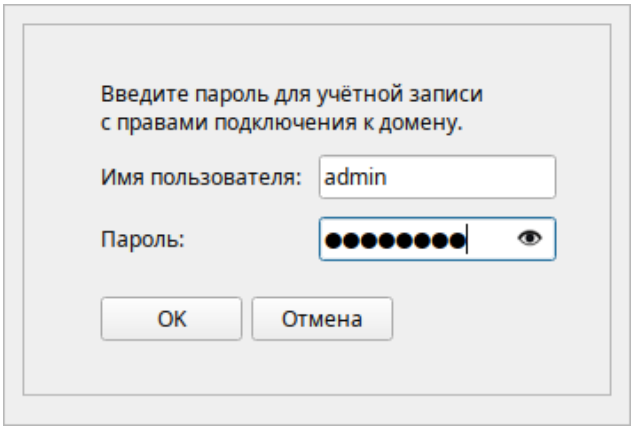

Рис. 124

В случае успешного подключения, будет выведено соответствующее сообщение (Рис. 125).

Подключение к серверу FreeIPA

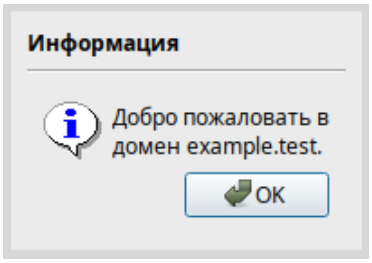

Рис. 125

Далее следует перезагрузить рабочую станцию.

4.10.4 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: comp02.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]:
```

Необходимо ответить «yes», ввести имя пользователя, имеющего право вводить машины в домен, и его пароль.

Примечание. Если при входе в домен возникает такая ошибка:

```
Hostname (comp02.example.test) does not have A/AAAA record.
Failed to update DNS records.
```

Необходимо проверить IP-адрес доменного DNS сервера в файле `/etc/resolv.conf`.

В случае возникновения ошибки, необходимо перед повторной установкой запустить процедуру удаления:

```
# ipa-client-install -U --uninstall
```

Для работы sudo-политик для доменных пользователей на клиентской машине необходимо разрешить доступ к sudo:

```
# control sudo public
```

4.10.5 Вход пользователя

В окне входа в систему (Рис. 126) необходимо ввести логин учетной записи пользователя FreeIPA и нажать кнопку «Войти», в открывшемся окне ввести пароль, соответствующий этой учетной записи и нажать кнопку «Войти».

Вход пользователя

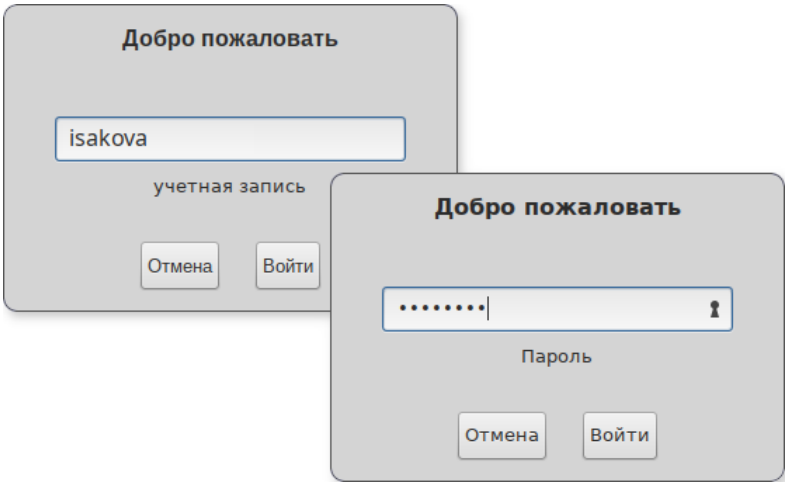

Рис. 126

При первом входе пользователя будет запрошен текущий (установленный администратором) пароль и затем у пользователя запрашивается новый пароль и его подтверждение (Рис. 127).

Примечание. Чтобы настроить автоматическое заполнение поля «Имя пользователя» именем последнего пользователя, входившего в систему, в файле `/etc/lightdm/lightdm-gtk-greeter.conf` (группа [greeter]) необходимо указать:

```
enter-username = true
```

Запрос текущего пароля и нового пароля при первом подключении к серверу FreeIPA

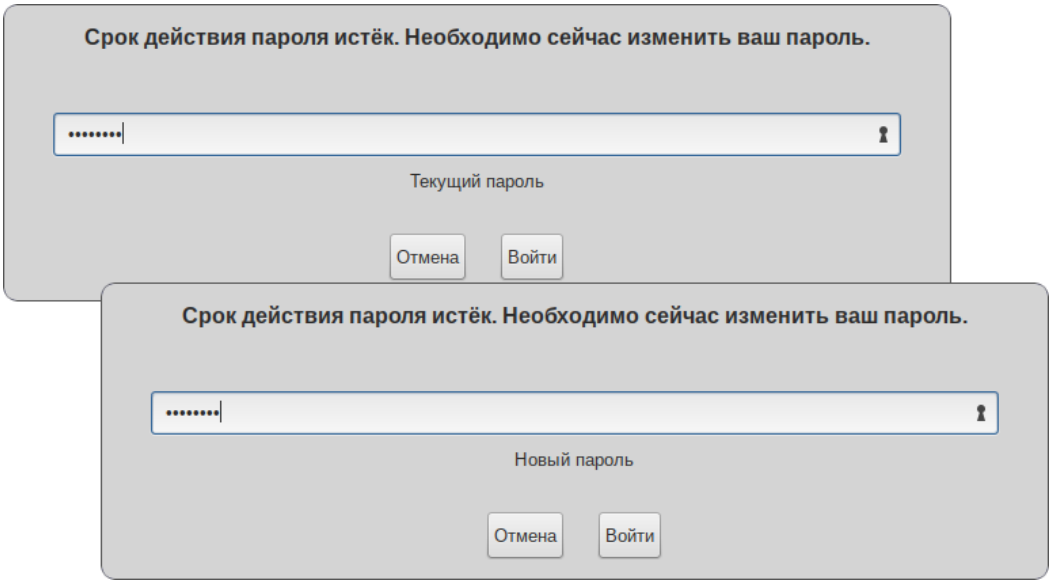

Рис. 127

5 СРЕДСТВА УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ

Дальнейшие разделы описывают некоторые возможности использования ОС «Альт Рабочая станция», настраиваемые в ЦУС.

5.1 Вход в систему

Начать работу по настройке системы можно сразу после её установки, используя для настройки «Центр управления системой» – веб-ориентированный интерфейс, позволяющий управлять системой с любого компьютера сети (см. раздел «Использование веб-ориентированного ЦУС»).

5.2 Конфигурирование сетевых интерфейсов

ОС «Альт Рабочая станция» поддерживает самые разные способы подключения к сети Интернет:

- Ethernet;
- PPTP;
- PPPoE;
- и т.д.

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

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

Конфигурирование сетевых интерфейсов осуществляется в модуле ЦУС «Ethernet-интерфейсы» (пакет `alterator-net-eth`) из раздела раздел «Сеть» (Рис. 128).

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;

Настройка модуля «Ethernet-интерфейсы»

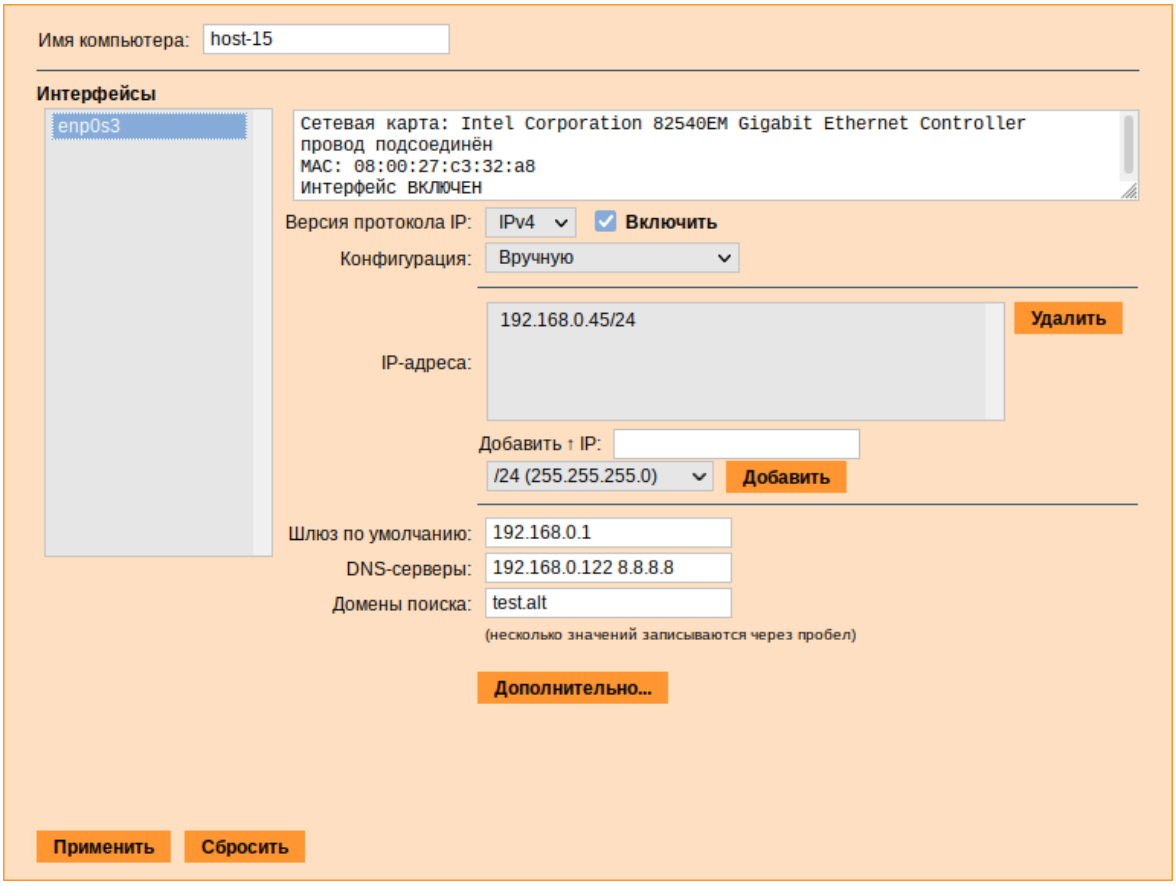

Рис. 128

- «Конфигурация» – выбрать способ назначения IP-адресов (службы DHCP, Zeroconf, вручную);
- «IP-адреса» – пул назначенных IP-адресов из поля «Добавить ↑ IP», выбранные адреса можно удалить нажатием кнопки «Удалить»;
- «Добавить ↑ IP» – ввести IP-адрес вручную и выбрать в выпадающем поле предпочтительную маску сети, затем нажать кнопку «Добавить» для переноса адреса в пул поля «IP-адреса»;
- «Шлюз по умолчанию» – в поле для ввода необходимо ввести адрес шлюза, который будет использоваться сетью по умолчанию;
- «DNS-серверы» – в поле для ввода необходимо ввести список предпочтительных DNS-серверов, которые будут получать информацию о доменах, выполнять маршрутизацию почты и управлять обслуживающими узлами для протоколов в домене;
- «Домены поиска» – в поле для ввода необходимо ввести список предпочтительных доменов, по которым будет выполняться поиск.

«IP-адрес» и «Маска сети» – обязательные параметры каждого узла IP-сети. Первый параметр – уникальный идентификатор машины, от второго напрямую зависит, к каким машинам

локальной сети данная машина будет иметь доступ. Если требуется выход во внешнюю сеть, то необходимо указать параметр «Шлюз по умолчанию».

В случае наличия DHCP-сервера можно все вышеперечисленные параметры получить автоматически – выбрав в списке «Конфигурация» пункт «Использовать DHCP» (Рис. 129).

Автоматическое получение настроек от DHCP сервера

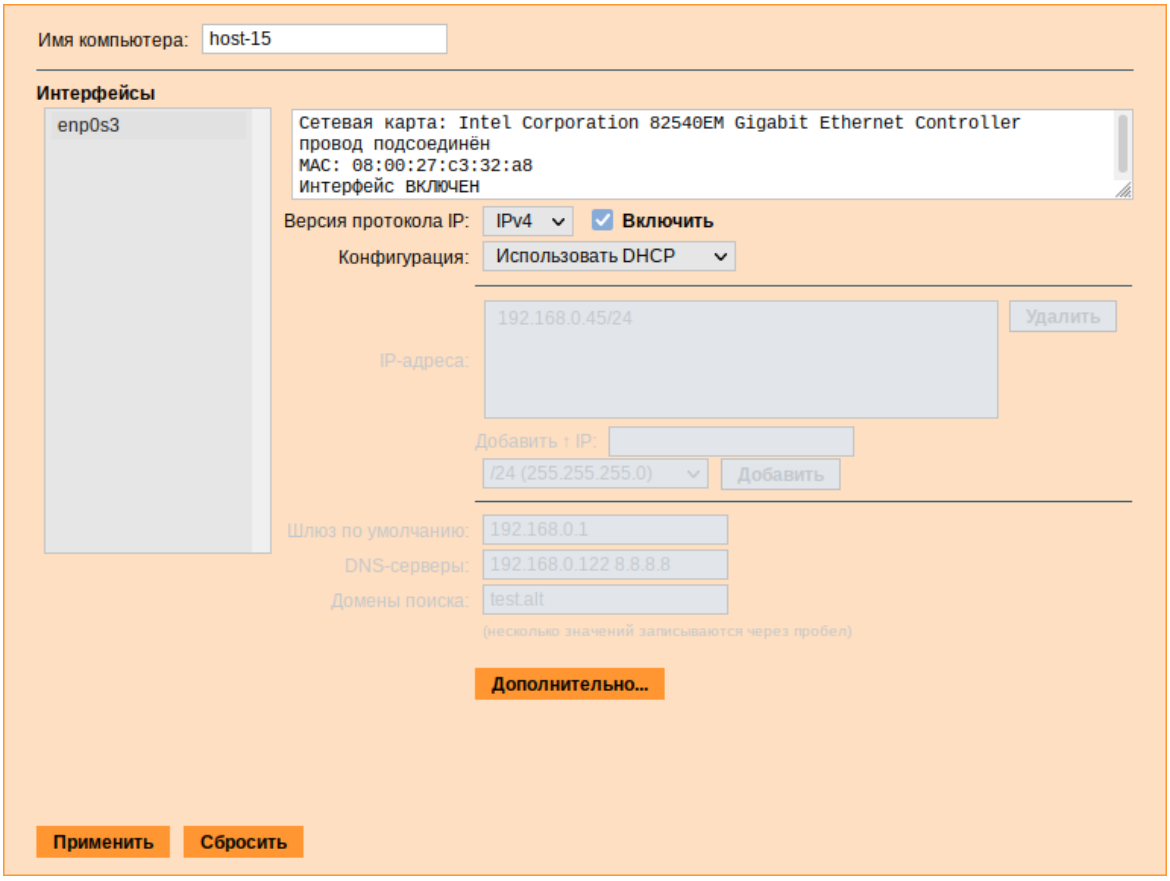

Рис. 129

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.

Дополнительно для каждого интерфейса можно настроить сетевую подсистему (NetworkManager, Etcnet), а также указать должен ли запускаться данный интерфейс при загрузке системы (Рис. 130).

Выбор сетевой подсистемы

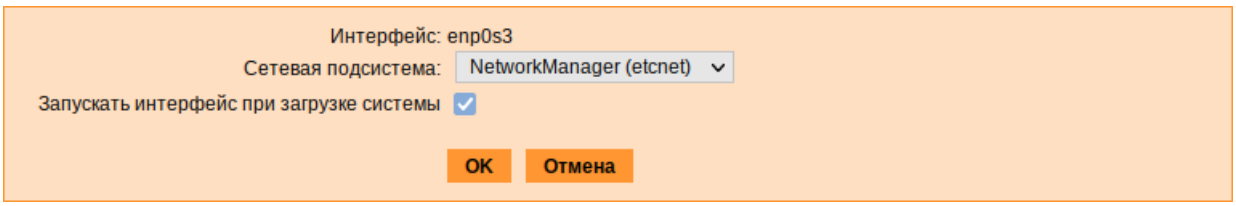

Рис. 130

В списке «Сетевая подсистема» можно выбрать следующие режимы:

- «Etcnet» – в этом режиме настройки берутся исключительно из файлов находящихся в каталоге настраиваемого интерфейса `/etc/net/ifaces/<интерфейс>`. Настройки сети могут изменяться либо в ЦУС в данном модуле, либо напрямую через редактирование файлов `/etc/net/ifaces/<интерфейс>`;
- «NetworkManager (etcnet)» – в этом режиме NetworkManager сам инициирует сеть, используя в качестве параметров – настройки из файлов Etcnet. Настройки сети могут изменяться либо в ЦУС в данном модуле, либо напрямую через редактирование файлов `/etc/net/ifaces/<интерфейс>`. В этом режиме можно просмотреть настройки сети, например, полученный по DHCP IP-адрес, через графический интерфейс NetworkManager;
- «NetworkManager (native)» – в данном режиме управление настройками интерфейса передаётся NetworkManager и не зависит от файлов Etcnet. Управлять настройками можно через графический интерфейс NetworkManager. Файлы с настройками находятся в каталоге `/etc/NetworkManager/system-connections`. Этот режим особенно актуален для задач настройки сети на клиенте, когда IP-адрес необходимо получать динамически с помощью DHCP, а DNS-сервер указать явно. Через ЦУС так настроить невозможно, так как при включении DHCP отключаются настройки, которые можно задавать вручную;
- «Не контролируется» – в этом режиме интерфейс находится в состоянии DOWN (выключен).

5.2.1 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. Различные производители материнских плат дают разные названия данной возможности, например: «Boot Option ROM» или «Boot From From Onboard LAN».

Последовательность установки при установке с DVD-диска и при сетевой установке не отличаются друг от друга.

5.3 Соединение удалённых офисов (OpenVPN-сервер)

ОС «Альт Рабочая станция» предоставляет возможность безопасного соединения удалённых офисов, используя технологию VPN (англ. Virtual Private Network – виртуальная частная сеть), которая позволяет организовать безопасные шифрованные соединения через публичные сети (например, Интернет) между удалёнными офисами или локальной сетью и удалёнными пользователями. Таким образом, можно связать два офиса организации, что делает

работу с документами, расположенными в сети удалённого офиса, более удобной. Помимо соединения целых офисов, также существует возможность организовать доступ в офисную сеть для работы в ней извне. Это означает, например, что сотрудник может работать в своём привычном окружении, даже находясь в командировке или просто из дома.

5.3.1 Настройка OpenVPN-сервера

OpenVPN-сервер может быть развернут, например, на базе ОС «Альт Сервер» или ОС «Альт Рабочая станция. Модуль «OpenVPN-сервер» (пакет `alterator-openvpn-server`) из раздела «Серверы» позволяет задать параметры OpenVPN-сервера (Рис. 131).

Модуль «OpenVPN-сервер»

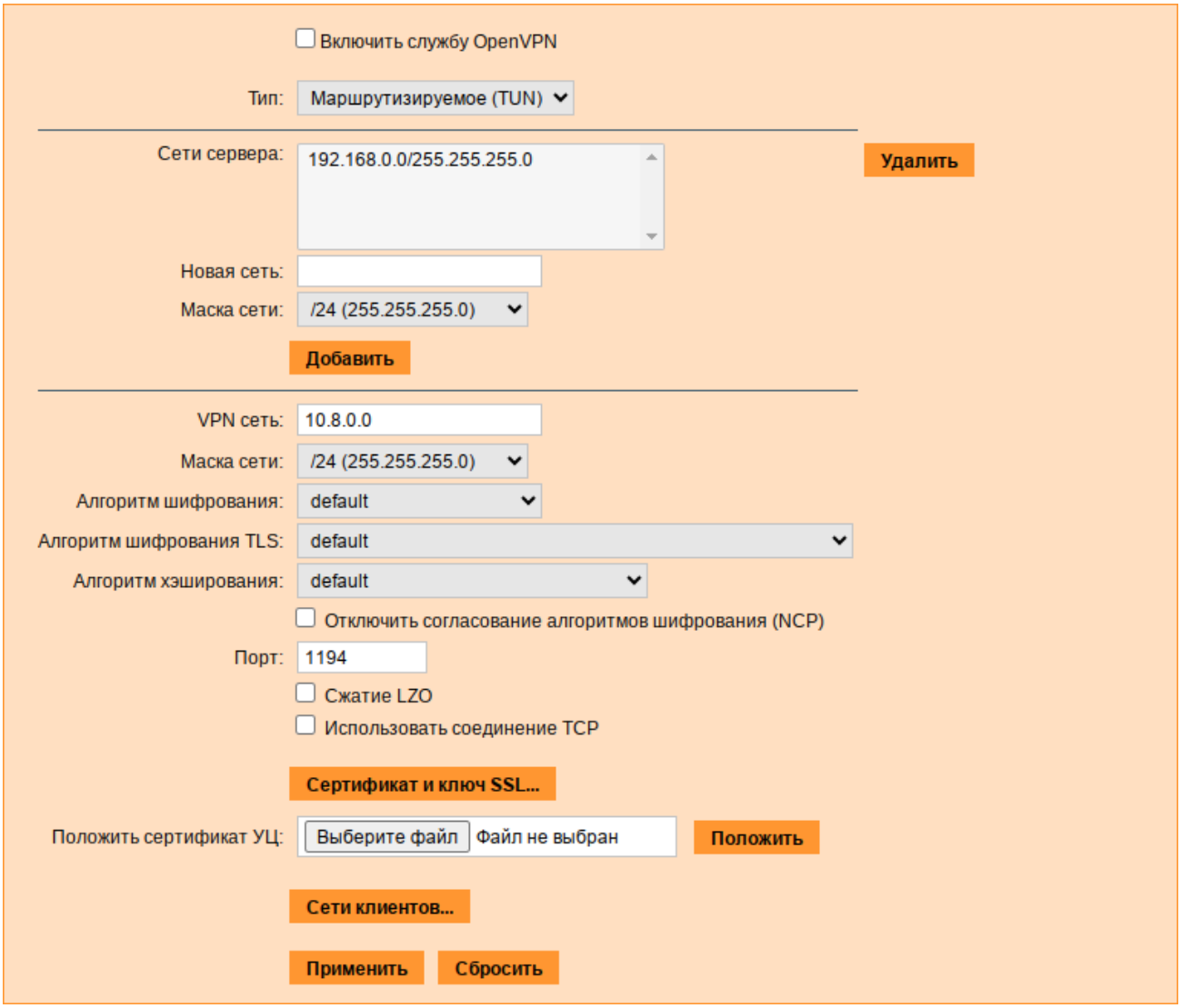

Рис. 131

Используя модуль «OpenVPN-сервер» можно:

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

- настроить сети клиентов.

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

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

Для настройки сертификата и ключа ssl необходимо нажать на кнопку «Сертификат и ключ ssl..». Откроется окно модуля «Управление ключами SSL» (пакет `alterator-sslkey`) (Рис. 132).

Модуль «Управление ключами SSL»

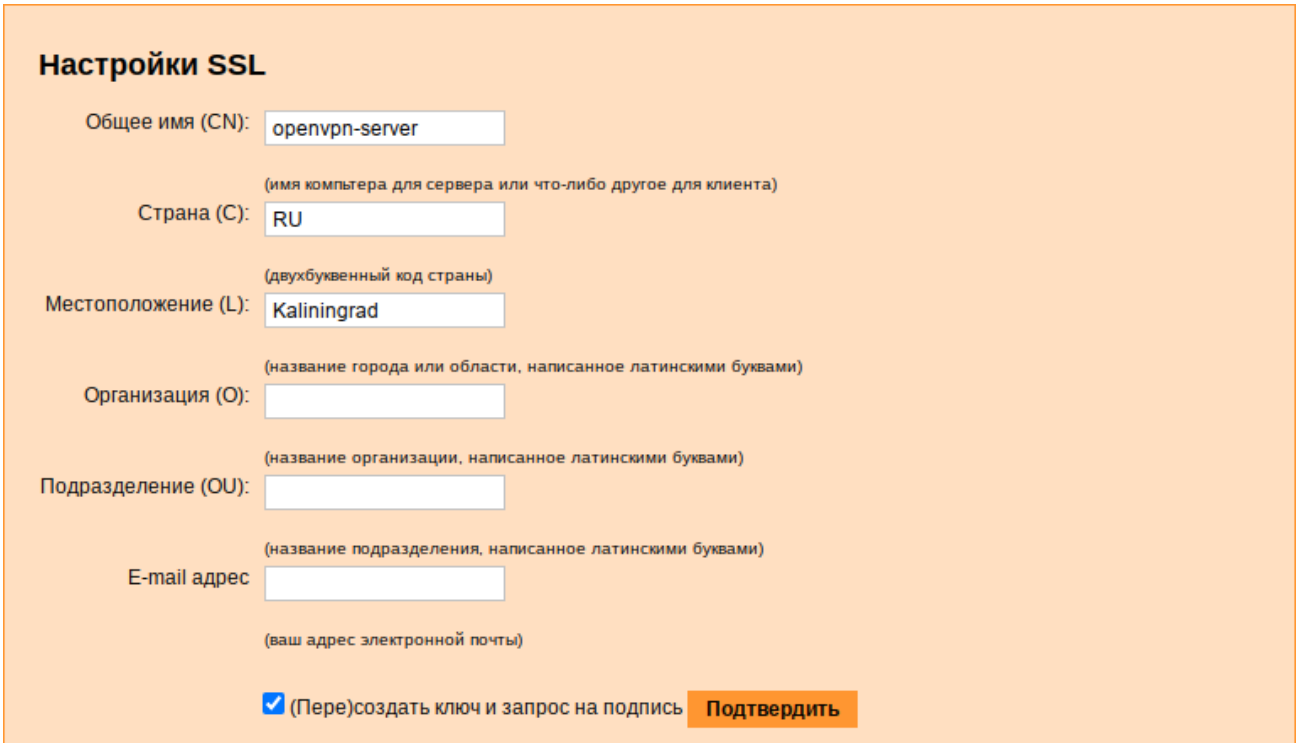

Рис. 132

Здесь нужно заполнить поле «Общее имя (CN)» и поле «Страна (C)» (прописными буквами), отметить пункт «(Пере)создать ключ и запрос на подпись» и нажать кнопку «Подтвердить». После чего станет активной кнопка «Забрать запрос на подпись» (Рис. 133).

Забрать запрос на подпись

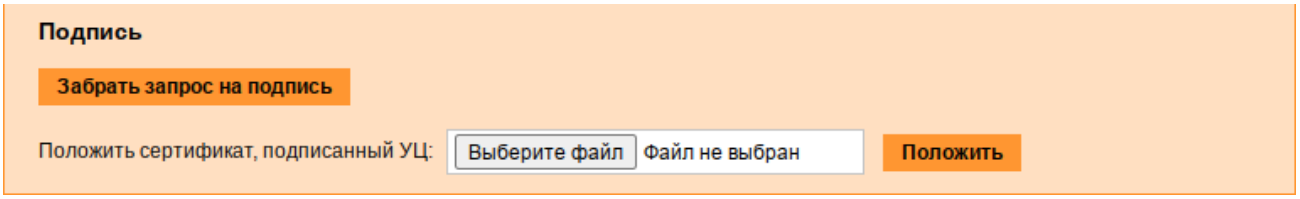

Рис. 133

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

В модуле «Управление ключами SSL» появился новый ключ: «openvpn-server (Нет сертификата)» (Рис. 134).

Ключ openvpn-server

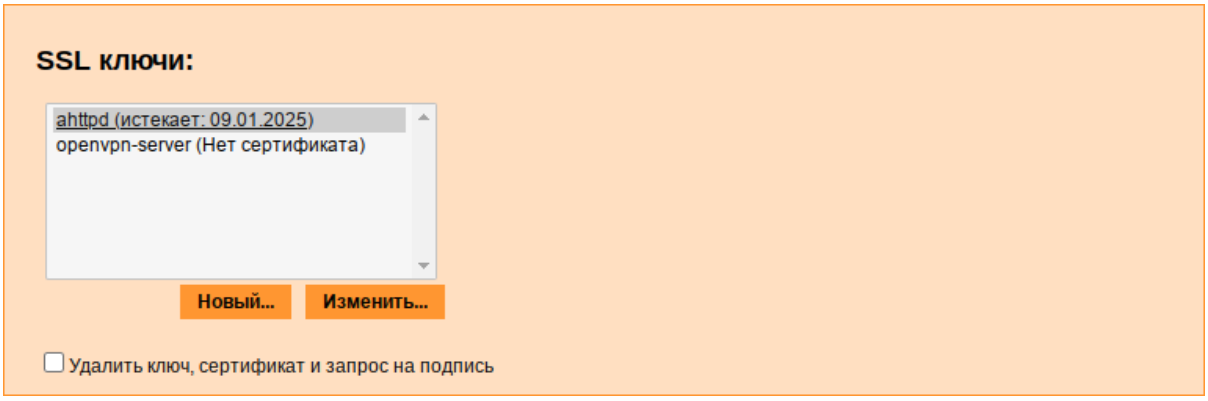

Рис. 134

Подписать сертификат можно в модуле «Удостоверяющий Центр» (пакет `alterator-ca`) на сервере.

Примечание. Можно подписать сертификат в консоли, с помощью openssl. Для этого необходимо выполнить следующие действия:

1. Для возможности подписывать любые сертификаты, необходимо открыть файл `/var/lib/ssl/openssl.cnf` и изменить значение параметра policy на следующее:

   ```
   policy = policy_anything
   ```

2. Создать каталоги:

   ```
   # mkdir -p /root/CA/demoCA
   # cd /root/CA
   # mkdir -p ./demoCA/newcerts
   ```

   Создать файл базы с действующими и отозванными сертификатами:

   ```
   # touch ./demoCA/index.txt
   ```

   Создать файл индекса для базы ключей и сертификатов:

   ```
   # echo '01' > ./demoCA/serial
   ```

   Создать файл индекса для базы отозванных сертификатов:

   ```
   # echo '01' > ./demoCA/crlnumber
   ```

3. Создать «самоподписанный» сертификат `ca-root.pem` и закрытый ключ `ca-root.key`, которыми будут заверяться/подписываться ключи и сертификаты клиентов:

   ```
   # openssl req -new -x509 -keyout ca-root.key -out ca-root.pem
   ```

Ввести пароль для закрытого ключа и ответить на запросы о владельце ключа.

4. Подписать запрос на сертификат своим «самоподписанным» `ca-root.pem` сертификатом и ключом `ca-root.key` с помощью следующей команды (необходимо) :

```
# openssl ca -cert ca-root.crt -keyfile ca-root.pem -days 3650 -in /home/user/openvpn-server.csr -out /home/user/output.pem
```

где:

/home/user/openvpn-server.csr – путь, до полученного в модуле «Управление ключами SSL», файла `openvpn-server.csr;`

/home/user/output.pem – файл, в который будет записан подписанный сертификат.

Примечание. Можно также установить пакет `alterator-ca` на Рабочей станции (`alterator-ca` не входит в состав ISO-образа дистрибутива, его можно установить из репозитория p10). Чтобы подписать сертификат необходимо перейти в модуль «Удостоверяющий Центр» →«Управление сертификатами», нажать кнопку «Выберите файл», указать путь до файла `openvpn-server.csr` и нажать кнопку «Загрузить запрос» (Рис. 135). В результате на экране появится две группы цифр и кнопка «Подписать» (Рис. 136). Необходимо нажать на кнопку «Подписать» и сохранить файл `output.pem` (подписанный сертификат).

Запрос на подпись сертификата

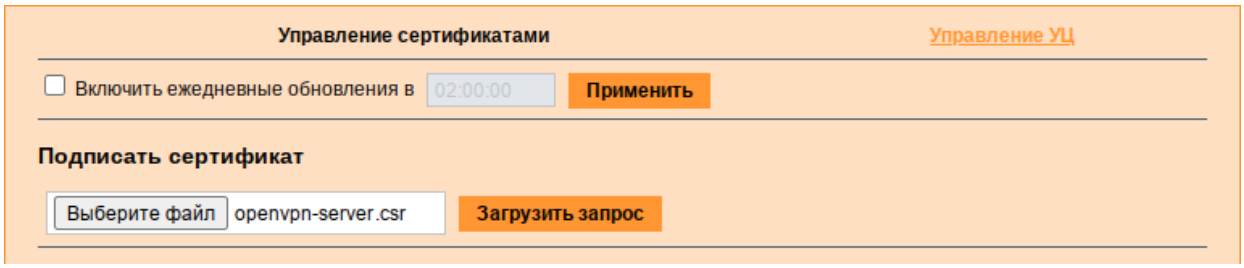

Рис. 135

Подписанный сертификат следует положить к его ключу. Для этого в разделе «Управление ключами SSL» необходимо выделить ключ «openvpn-server (Нет сертификата)» и нажать кнопку «Изменить». В появившемся окне, в пункте «Положить сертификат, подписанный УЦ» нужно нажать кнопку «Выберите файл», указать путь до файла `output.pem` и нажать кнопку «Положить» (Рис. 137).

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

Запрос на подпись сертификата

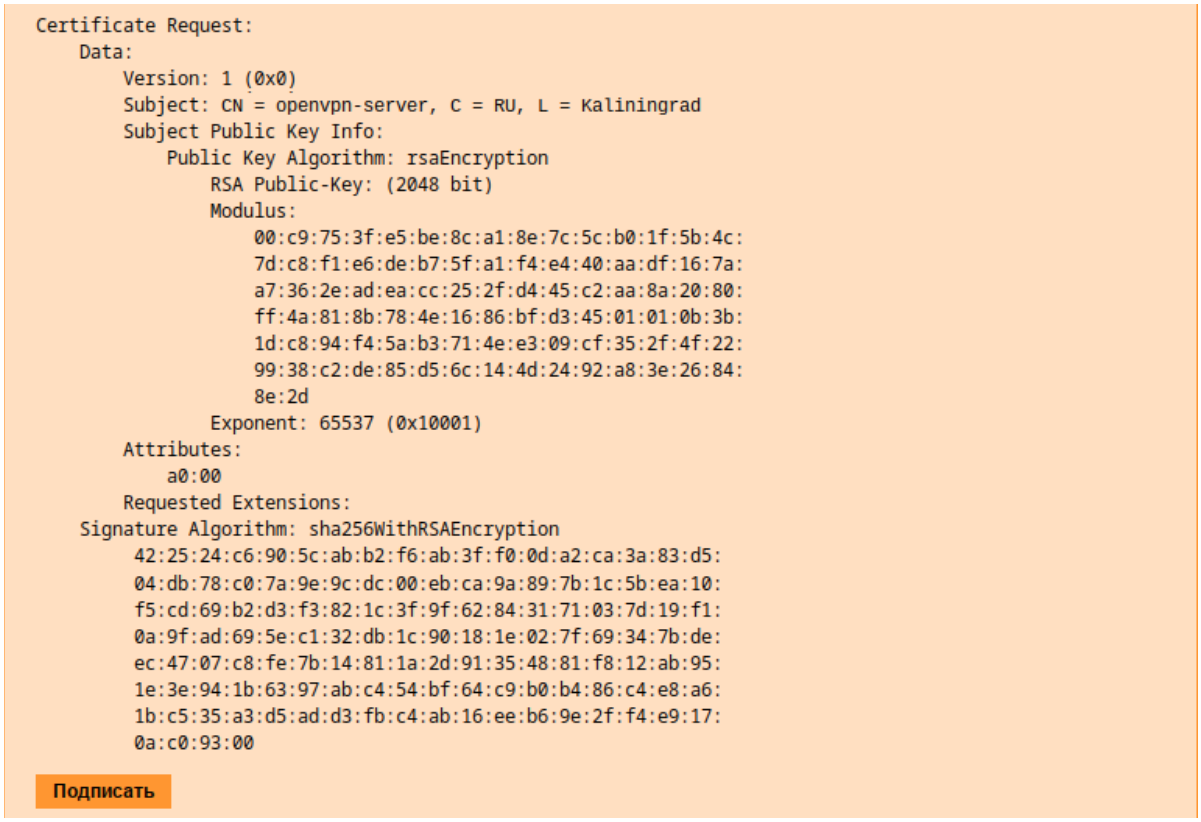

Рис. 136

Сертификат, подписанный УЦ

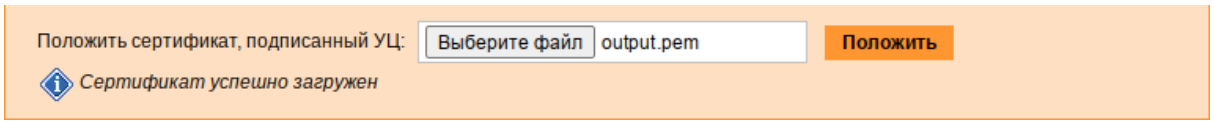

Рис. 137

В модуле «OpenVPN-сервер» необходимо положить сертификат УЦ. Для этого в графе «Положить сертификат УЦ» следует нажать кнопку «Выберите файл», указать путь к файлу сертификата УЦ и нажать кнопку «Положить» (Рис. 138). Появится сообщение: «Сертификат УЦ успешно загружен».

Выбор сертификата УЦ в модуле «OpenVPN-сервер»

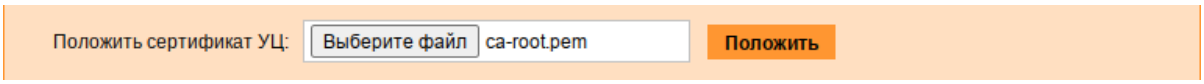

Рис. 138

Примечание. Если использовался модуль «Удостоверяющий Центр», то для получения сертификата УЦ необходимо перейти в модуле «Удостоверяющий Центр» на вкладку «Управление УЦ» и нажать на ссылку «Сертификат: ca-root.pem» (Рис. 139).

Сертификат УЦ

Рис. 139

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

5.3.2 Настройка клиентов

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

Для создания нового соединения необходимо отметить пункт «Сетевой туннель (TUN)» или «Виртуальное Ethernet устройство (TAP)» и нажать кнопку «Создать соединение» (Рис. 140). Должен быть выбран тот же тип, что и на стороне сервера.

Создание нового OpenVPN- соединения

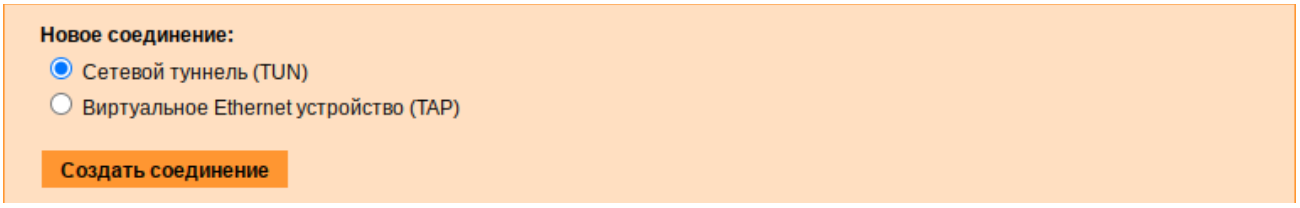

Рис. 140

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

Помимо этого нужно создать ключ (например, openvpn) в модуле «Управление ключами SSL» и подписать его в модуле «Удостоверяющий Центр» (пакет `alterator-ca`) на сервере.

В результате станут доступны настройки соединения (Рис. 141).

На клиенте в модуле «OpenVPN-соединение» необходимо указать:

- состояние – «запустить»;
- сервер – IP адрес сервера или домен;
- порт – 1194;
- ключ – выбрать подписанный на сервере ключ.

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

Модуль «OpenVPN- соединения»

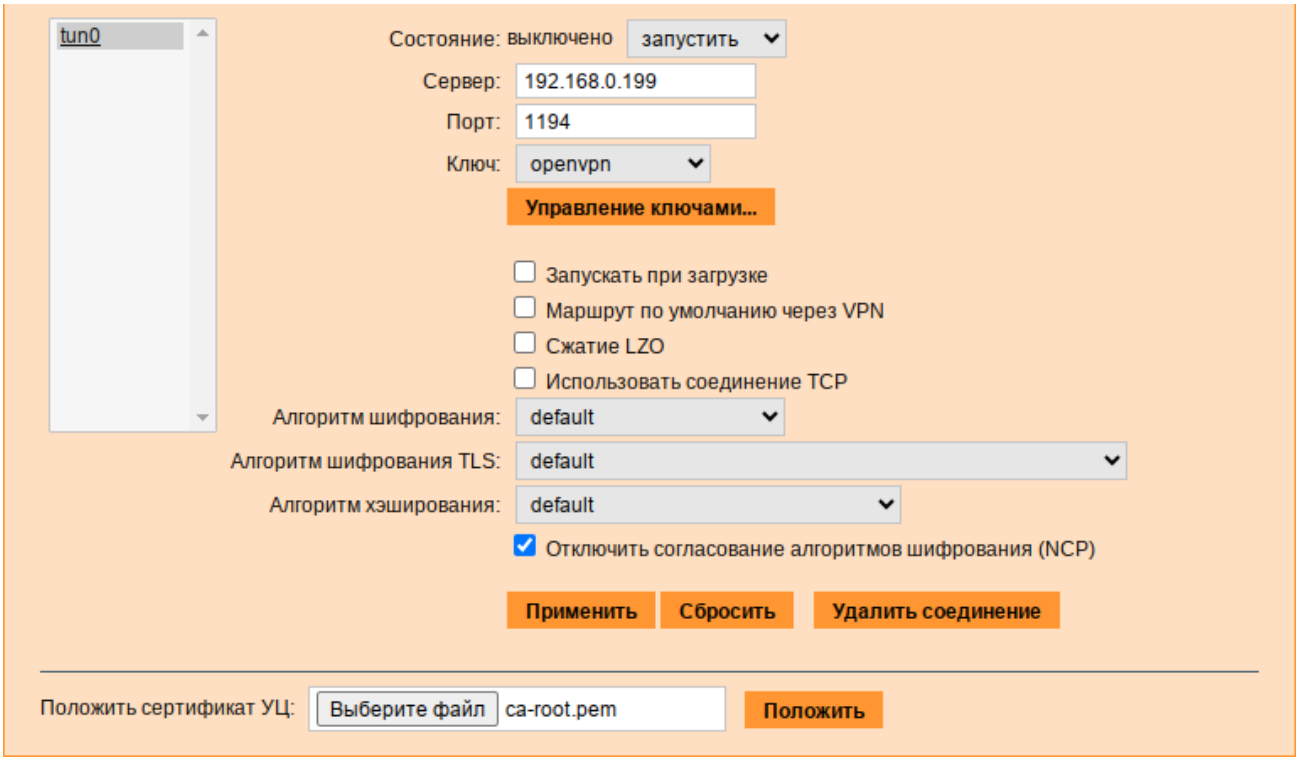

Рис. 141

Проверить, появилось ли соединение с сервером можно командой:

```
$ ip addr
```

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

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

5.4 Доступ к службам из сети Интернет

5.4.1 Внешние сети

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

Для разрешения внешних и внутренних входящих соединений предусмотрен раздел ЦУС «Брандмауэр». В списке «Разрешить входящие соединения на внешних интерфейсах» модуля «Внешние сети» (пакет `alterator-net-iptables`) перечислены наиболее часто используемые службы, отметив которые, можно сделать их доступными для соединений на

внешних сетевых интерфейсах (Рис. 142). Если необходимо предоставить доступ к службе, отсутствующей в списке, то нужно задать используемые этой службой порты в соответствующих полях.

Модуль «Внешние сети»

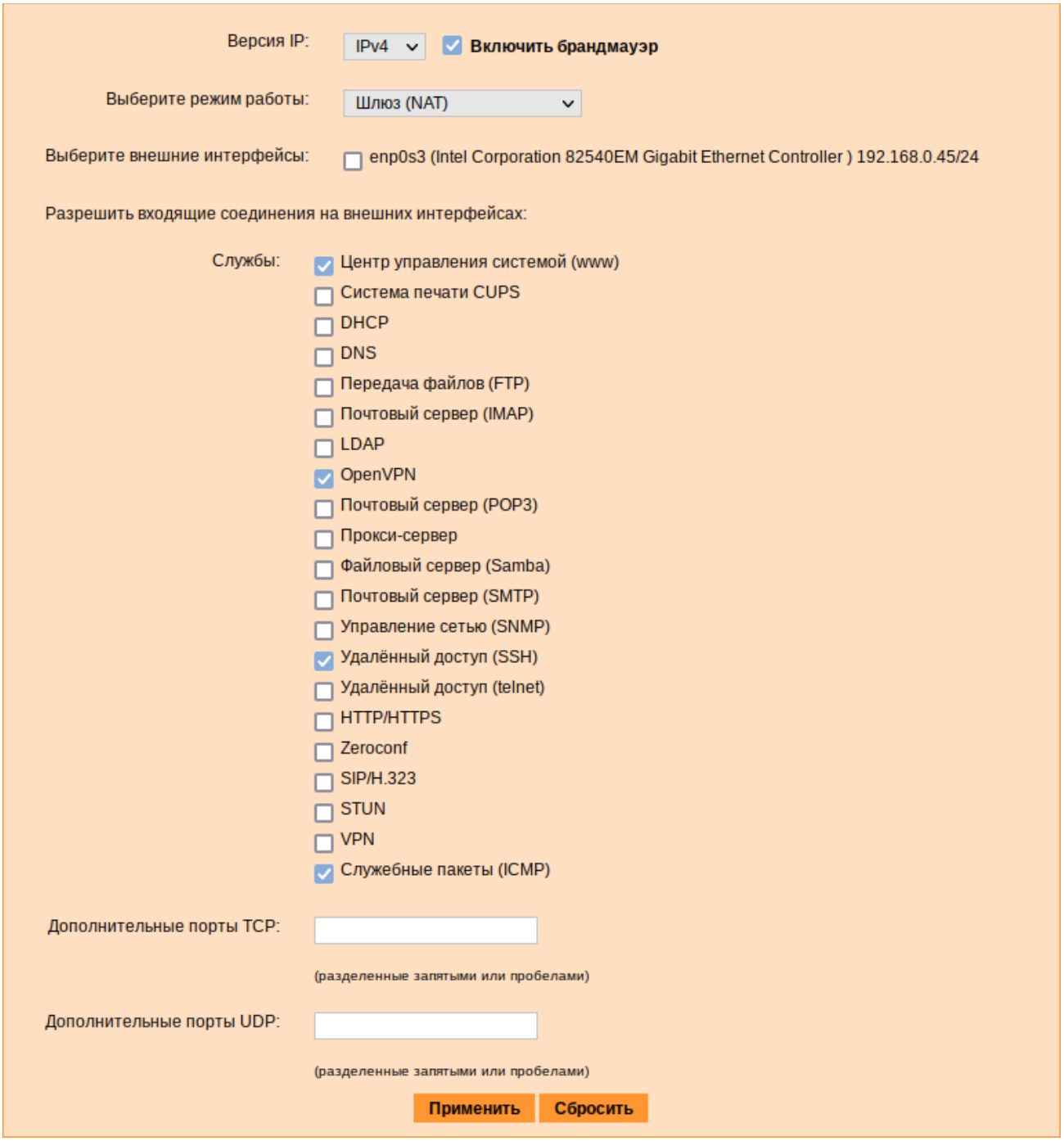

Рис. 142

Можно выбрать один из трех 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;
- Хост (Рабочая станция) – в этом режиме можно для всех интерфейсов открыть или закрыть порт. Внешними автоматически выбираются все интерфейсы, кроме lo и специальных исключений (virbr*, docker*).

В любом режиме включено только перенаправление пакетов с внутренних интерфейсов. Перенаправление пакетов с внешних интерфейсов всегда выключено. Все внутренние интерфейсы открыты для любых входящих соединений.

5.4.2 Список блокируемых хостов

Модуль «Список блокируемых хостов» (пакет `alterator-net-iptables`) 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 флажка «Использовать чёрный список» (Рис. 143).

Модуль «Список блокируемых хостов»

Рис. 143

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

Для удаления узла необходимо выбрать его из списка и нажать кнопку «Удалить».

5.5 Обслуживание рабочей станции

Регулярный мониторинг состояния системы, своевременное резервное копирование, обновление установленного ПО, являются важной частью комплекса работ по обслуживанию рабочей станции.

5.5.1 Мониторинг состояния системы

Для обеспечения бесперебойной работы рабочей станции крайне важно производить постоянный мониторинг ее состояния. Все события, происходящие с рабочей станцией, записываются в журналы, анализ которых помогает избежать сбоев в работе 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. 144).

Модуль «Системные журналы»

Рис. 144

Доступны следующие виды журналов:

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

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

5.5.2 Системные службы

Для изменения состояния служб можно использовать модуль ЦУС «Системные службы» (пакет `alterator-services`) из раздела «Система». Интерфейс позволяет изменять текущее состояние службы и, если необходимо, применить опцию запуска службы при загрузке системы (Рис. 145).

Модуль «Системные службы»

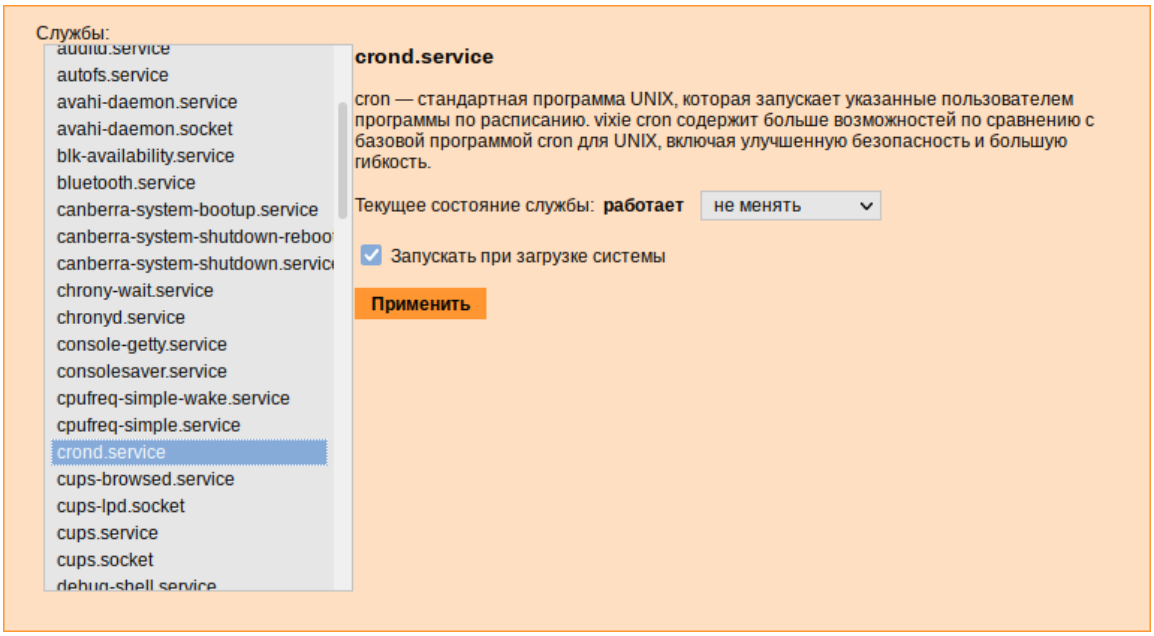

Рис. 145

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

5.5.3 Системные ограничения

Средствами модуля «Системные ограничения» (пакет `alterator-control`) из раздела «Система» определяются несколько заранее заданных режимов доступа к тому или иному файлу. Администратор системы может установить один из этих режимов – он будет гарантированно сохранён при обновлении системы.

Модуль также может использоваться как простой конфигуратор, позволяющий переключать многие системные службы между заранее определёнными состояниями.

На Рис. 146 показаны политики для команды `fusermount`.

Для переключения состояния следует выбрать политику и нажать кнопку «Сохранить».

Модуль «Системные ограничения»

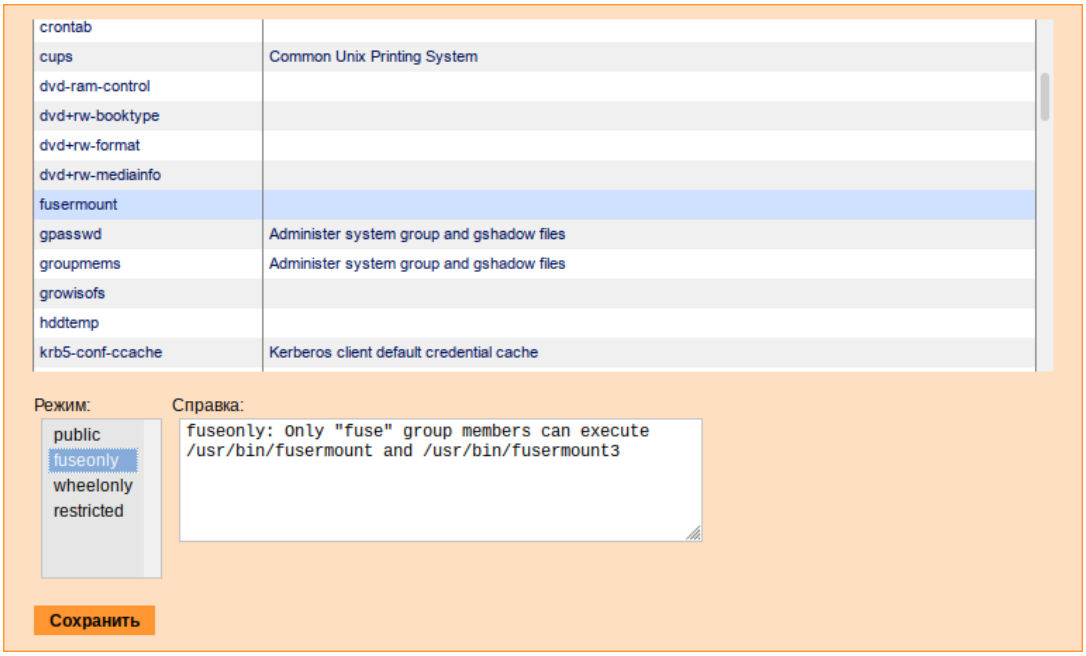

Рис. 146

5.5.4 Обновление системы

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

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. 147).

Модуль «Обновление системы»

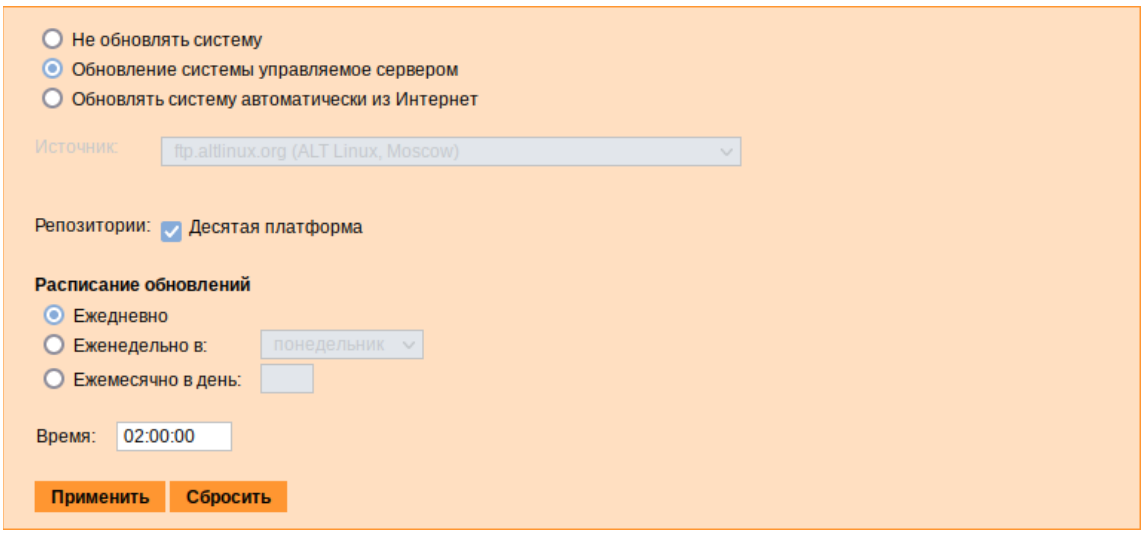

Рис. 147

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

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

Необходимо также указать репозитории. Следует обратить внимание на то, что разные репозитории бывают разной степени стабильности и чем стабильнее репозиторий, тем реже там появляются новые версии приложений.

Процесс обновления системы будет запускаться автоматически согласно заданному расписанию.

Примечание. Чтобы указать в качестве сервера обновлений локально настроенный источник, необходимо выбрать режим «Обновлять систему автоматически из Интернет», выбрать в списке «Другой адрес» и указать адрес локального сервера обновлений, например, http://<ip сервера>/mirror (Рис. 148).

Указание источника обновлений

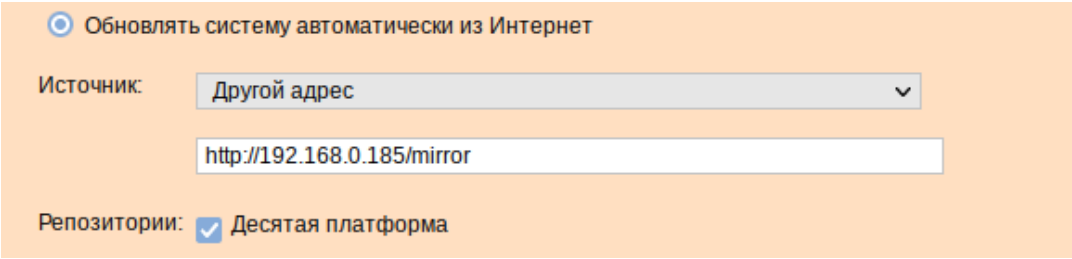

Рис. 148

5.5.5 Обновление систем, не имеющих выхода в Интернет

Для систем, не имеющих прямого выхода в Интернет, рекомендуется установка отдельного сервера обновлений (например, на базе ОС «Альт Сервер» или ОС «Альт Рабочая станция»), находящегося вне защищенного контура и организация ограниченного доступа к этому серверу.

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

На странице модуля можно выбрать, как часто выполнять закачку пакетов, можно выставить время, когда начинать зеркалирование (Рис. 149).

Здесь также можно выбрать репозитории, локальные срезы которых необходимы. При нажатии на название репозитория, появляются настройки этого репозитория (Рис. 150).

Необходимо выбрать источник, архитектуру процессора (если их несколько, то стоит выбрать соответствующие).

Модуль «Сервер обновлений»

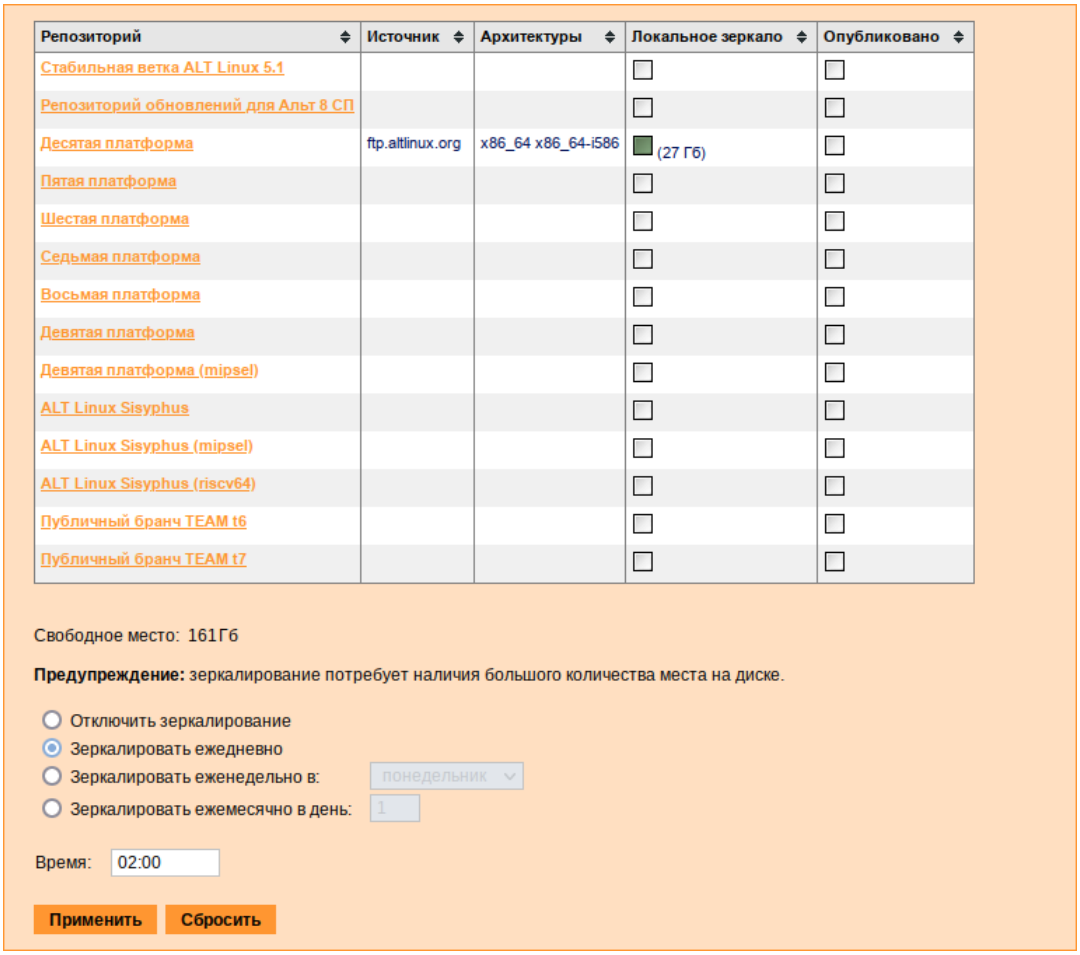

Рис. 149

Настройки репозитория

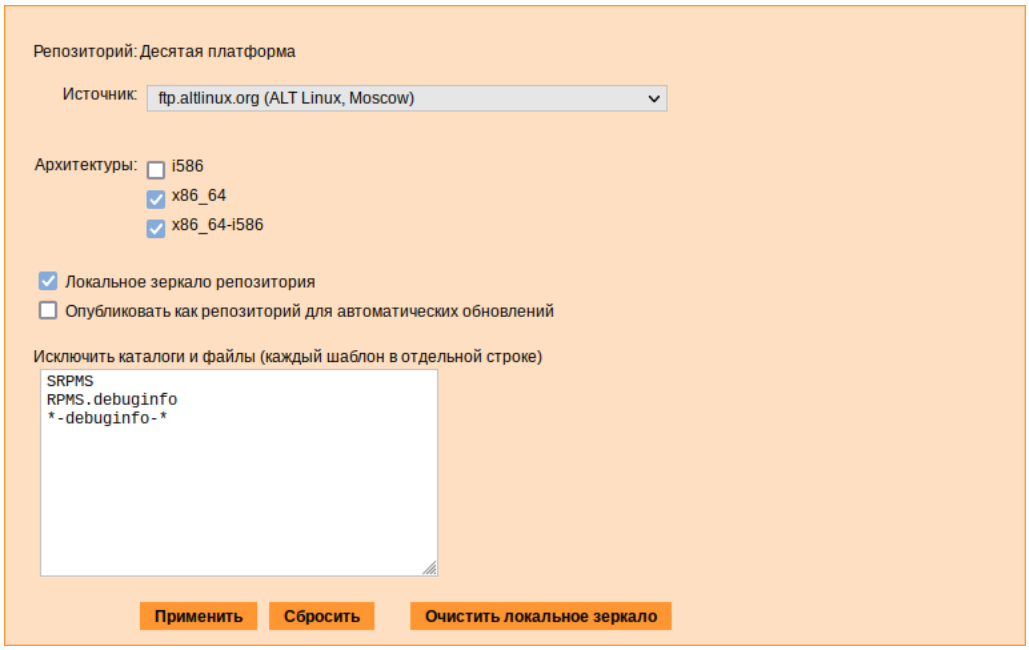

Рис. 150

Примечание. При выборе любой архитектуры также будет добавлен источник с noarch.

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

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

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

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

  Шаблоны указываются по одному в отдельной строке. Символ «*» используется для подстановки любого количества символов.
- Публикация репозитория – в этом случае публикуется или URL внешнего сервера, содержащего репозиторий или, если включено локальное зеркало репозитория, адрес этого сервера. Такая публикация позволяет клиентским машинам автоматически настроить свои менеджеры пакетов на использование внешнего или локального репозитория. Со стороны клиентских машин, в этом случае, необходимо настроить модуль «Обновление системы», отметив в нём пункт «Обновление системы управляемое сервером».

  Настройка локального репозитория заканчивается нажатием на кнопку «Применить».

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

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

где `/media/disk/localrepo` – папка-хранилище локального репозитория.

5.5.5.1 Настройка веб-сервера

Установить веб-сервер nginx:

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

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

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

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

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

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

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

Запустить nginx и добавить его в автозагрузку:

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

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

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

Проверить правильность настройки репозиториев:

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

5.5.5.2 Настройка FTP-сервера

Установить, настроить и запустить сервер FTP (см. Настройка сервера FTP).

Создать каталог `/var/ftp/mirror`:

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

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

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

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

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

На клиентских машинах необходимо настроить репозитории:

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

5.5.6 Локальные учётные записи

Модуль «Локальные учётные записи» (пакет `alterator-users`) из раздела «Пользователи» предназначен для администрирования системных пользователей (Рис. 151).

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

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

В модуле ЦУС «Локальные учетные записи» (только GUI) можно задать профиль киоска для пользователя (Рис. 152). Режим «киоск» служит для ограничения прав пользователей в системе.

Веб-интерфейс модуля alterator-users

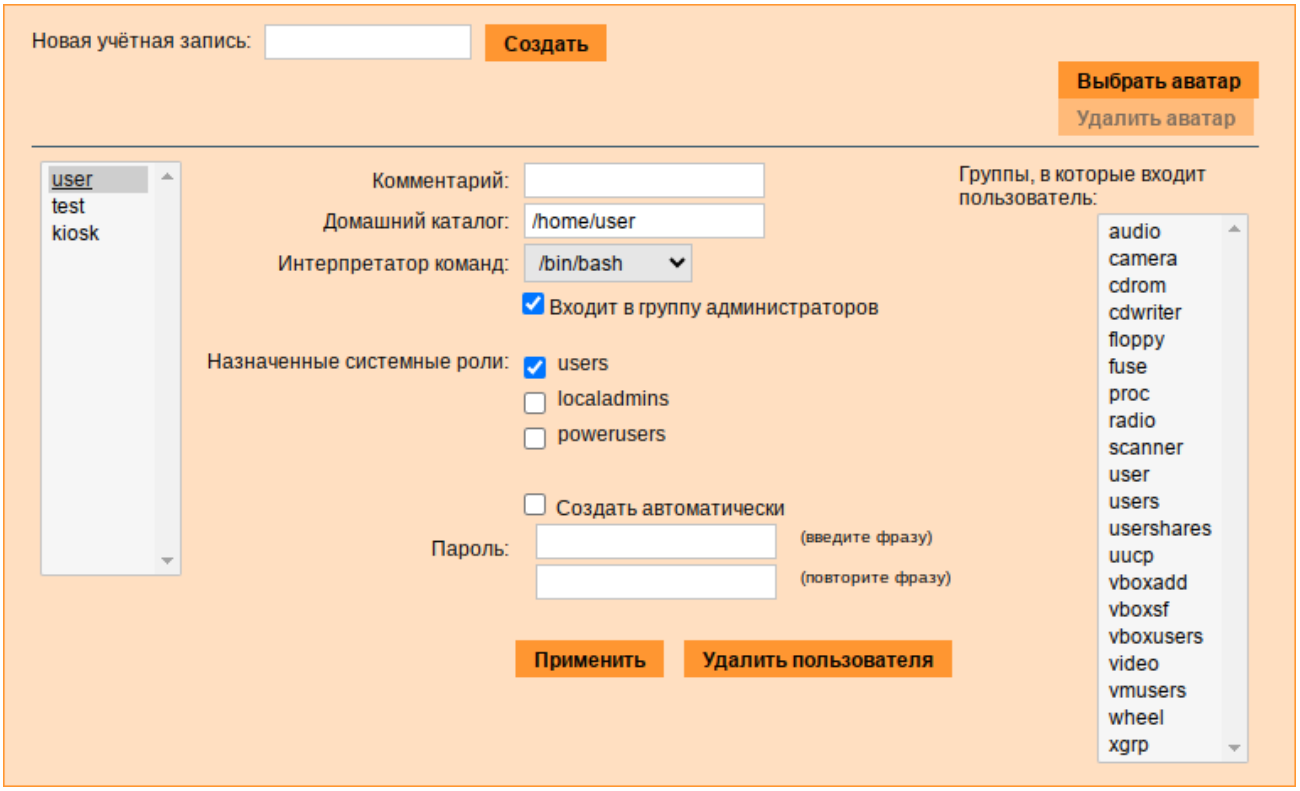

Рис. 151

Настройка режима «киоск» для пользователя kiosk

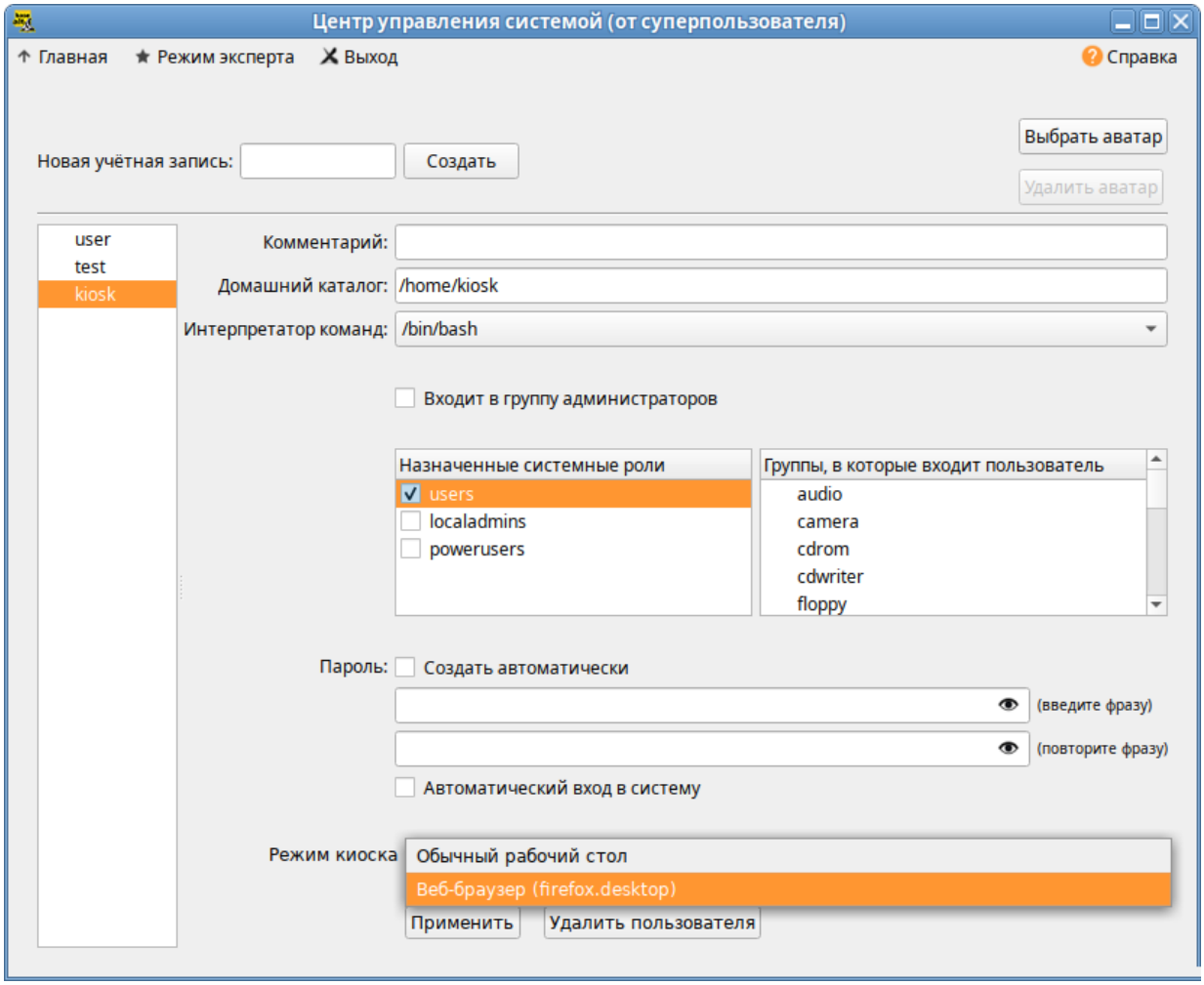

Рис. 152

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»:

1. Создать каталог `/etc/kiosk` (если он еще не создан);
2. Создать файл `/etc/kiosk/firefox.desktop` со следующим содержимым:

```
#!/usr/bin/env xdg-open
[Desktop Entry]
Version=1.0
Type=Application
Terminal=false
Exec=/usr/local/bin/webkiosk
```

```
Name=Веб-браузер
Icon=start
```

3. Создать файл `/usr/local/bin/webkiosk` со следующим содержимым:

```
#!/bin/bash
marco --replace &
firefox --kiosk --incognito https://ya.ru
```

4. Сделать файл `/usr/local/bin/webkiosk` исполняемым:

```
# chmod +x /usr/local/bin/webkiosk
```

5. В модуле «Локальные учётные записи», выбрать учетную запись пользователя, затем в выпадающем списке «Режим киоска» выбрать пункт «Веб-браузер (firefox.desktop)» и нажать кнопку «Применить».
6. Завершить сеанс текущего пользователя и войти в систему, используя учетную запись пользователя, для которого настроен режим «киоск».

Пользователю будет доступен только веб-браузер firefox, по умолчанию будет загружена страница, адрес которой указан в файле `/usr/local/bin/webkiosk`.

5.5.7 Администратор системы

В модуле «Администратор системы» (пакет `alterator-root`) из раздела «Пользователи» можно изменить пароль суперпользователя (root), заданный при начальной настройке системы (Рис. 153).

Модуль «Администратор системы»

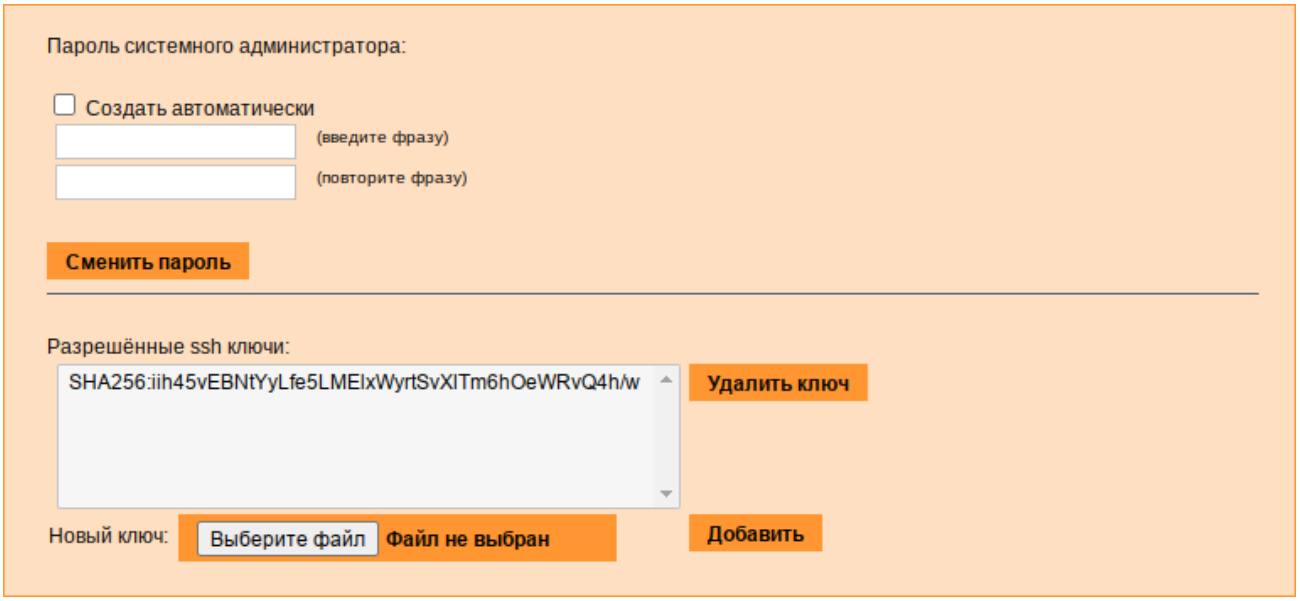

Рис. 153

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

5.5.8 Дата и время

В модуле «Дата и время» (пакет `alterator-datetime`) из раздела «Система» можно изменить дату и время в системе, сменить часовой пояс, а также настроить автоматическую синхронизацию часов по протоколу NTP и предоставление точного времени по этому протоколу для рабочих станций локальной сети (Рис. 154).

Модуль «Дата и время»

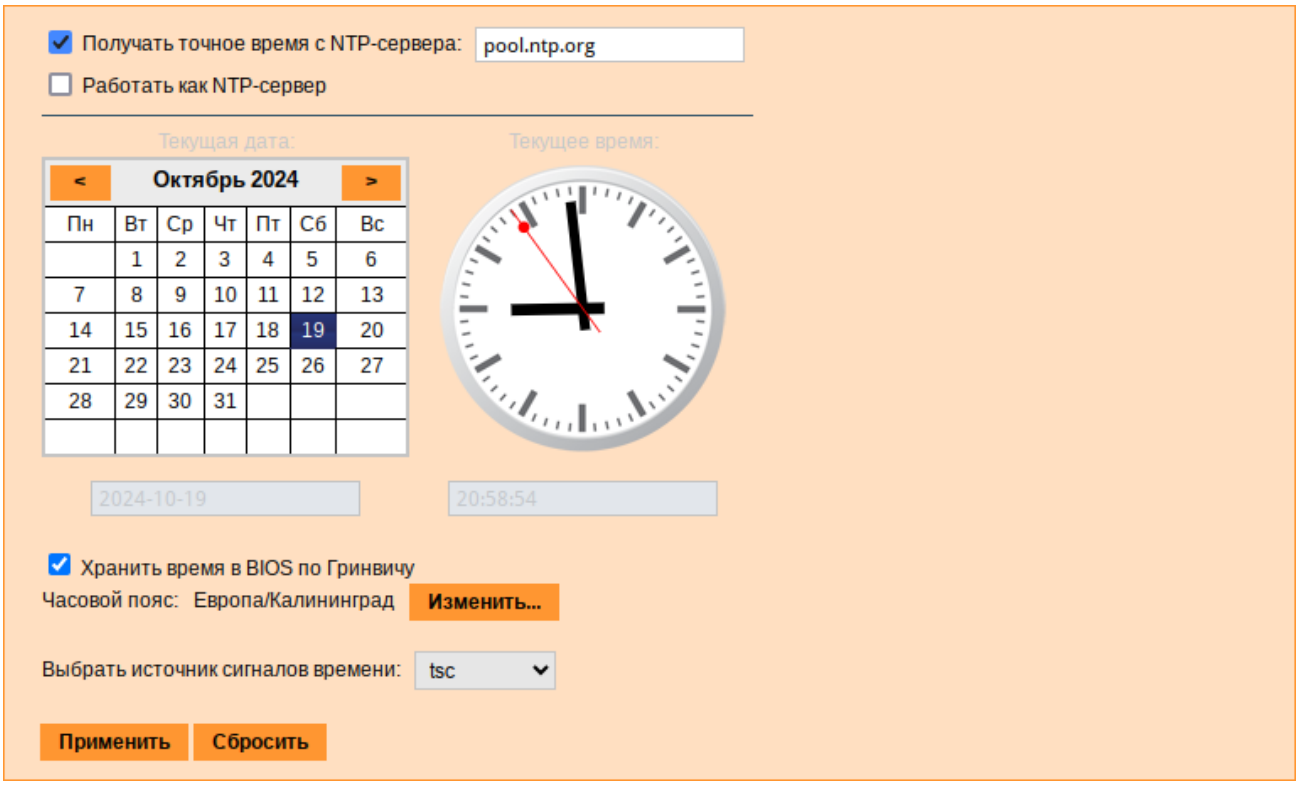

Рис. 154

Системное время зависит от следующих факторов:

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

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

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

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

5.5.9 Настройка прокси-сервера

Модуль «Прокси-сервер» (пакет `alterator-sysconfig`) из раздела «Система» позволяет настроить параметры прокси-сервера, используемого для выхода в Интернет (Рис. 154).

*Модуль «*Прокси-сервер*»*

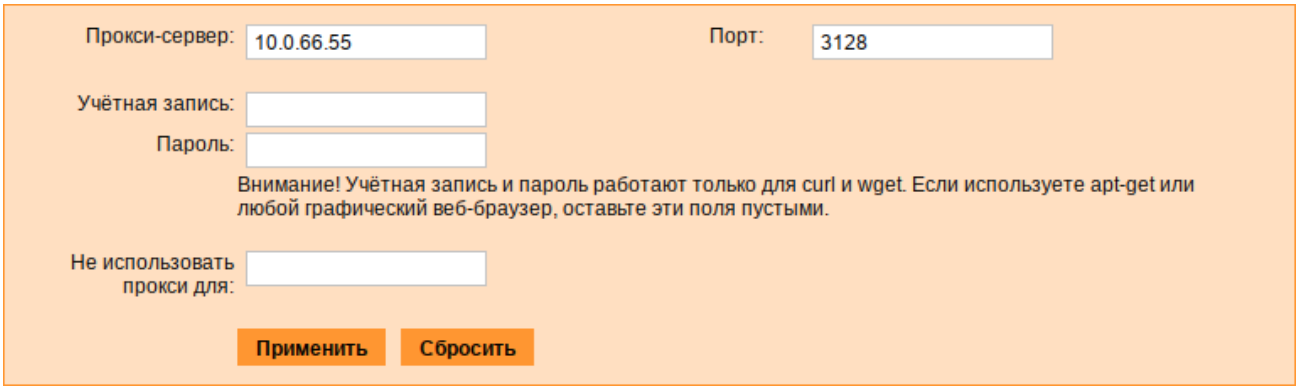

Рис. 155

Данный модуль позволяет настроить:

- IP-адрес и порт используемого прокси-сервера;
- логин и пароль для доступа, если прокси-сервер требует аутентификацию.

После нажатия кнопки «Применить» все параметры запишутся в файл `/etc/sysconfig/network` в следующем виде:

```
HTTP_PROXY=http://username:password@address:port
HTTPS_PROXY=http://username:password@address:port
FTP_PROXY=http://username:password@address:port
NO_PROXY=""
```

Указанный прокси-сервер будет использоваться ПО для доступа в сеть Интернет.

Примечание. Для применения настроек прокси-сервера необходимо перезагрузить систему.

5.5.10 Ограничение использования диска

Модуль «Использование диска» (пакет `alterator-quota`) в разделе «Пользователи» позволяет ограничить использование дискового пространства пользователями, заведёнными в системе в модуле «Пользователи».

Модуль позволяет задать ограничения (квоты) для пользователя при использовании определённого раздела диска. Ограничить можно как суммарное количество килобайт, занятых файлами пользователя, так и количество этих файлов (Рис. 156).

Модуль «Использование диска»

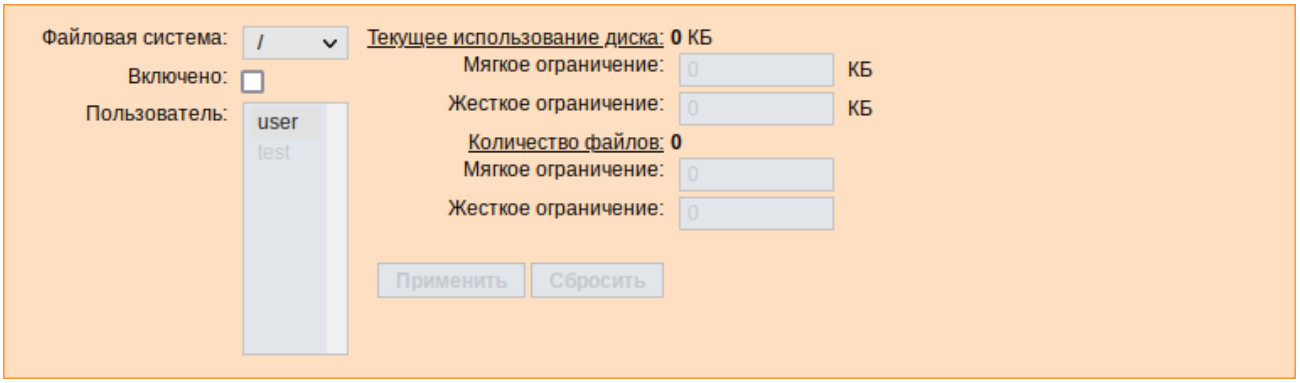

Рис. 156

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. 157).

Модуль «Использование диска»

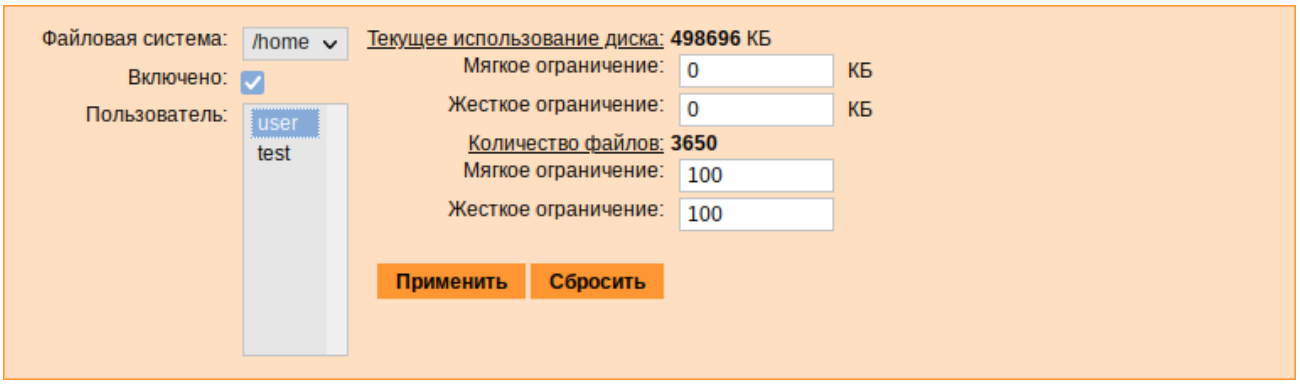

Рис. 157

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

При задании ограничений различают жёсткие и мягкие ограничения:

- мягкое ограничение: нижняя граница ограничения, которая может быть временно превышена. Временное ограничение – одна неделя;
- жёсткое ограничение: использование диска, которое не может быть превышено ни при каких условиях.

Значение 0 при задании ограничений означает отсутствие ограничений.

5.5.11 Выключение и перезагрузка компьютера

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

Модуль ЦУС «Выключение компьютера» позволяет:

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

Возможна настройка ежедневного применения данных действий в заданное время.

Так как выключение и перезагрузка – критичные для функционирования компьютера операции, то по умолчанию настройка выставлена в значение «Продолжить работу» (Рис. 158). Для выключения, перезагрузки или перехода в энергосберегающие режимы нужно отметить соответствующий пункт и нажать «Применить».

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

Модуль «Выключение компьютера»

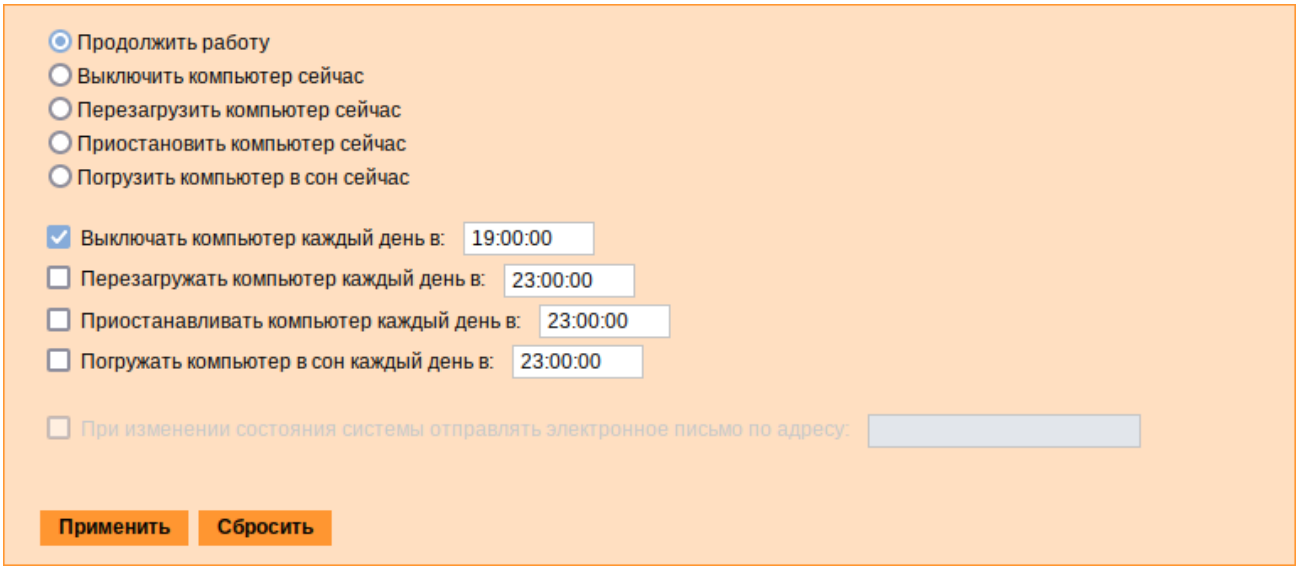

Рис. 158

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

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

Для настройки оповещений необходимо отметить пункт «При изменении состояния системы отправлять электронное письмо по адресу», ввести e-mail адрес и нажать кнопку «Применить» (Рис. 159).

Модуль «Выключение компьютера». Настройка оповещений

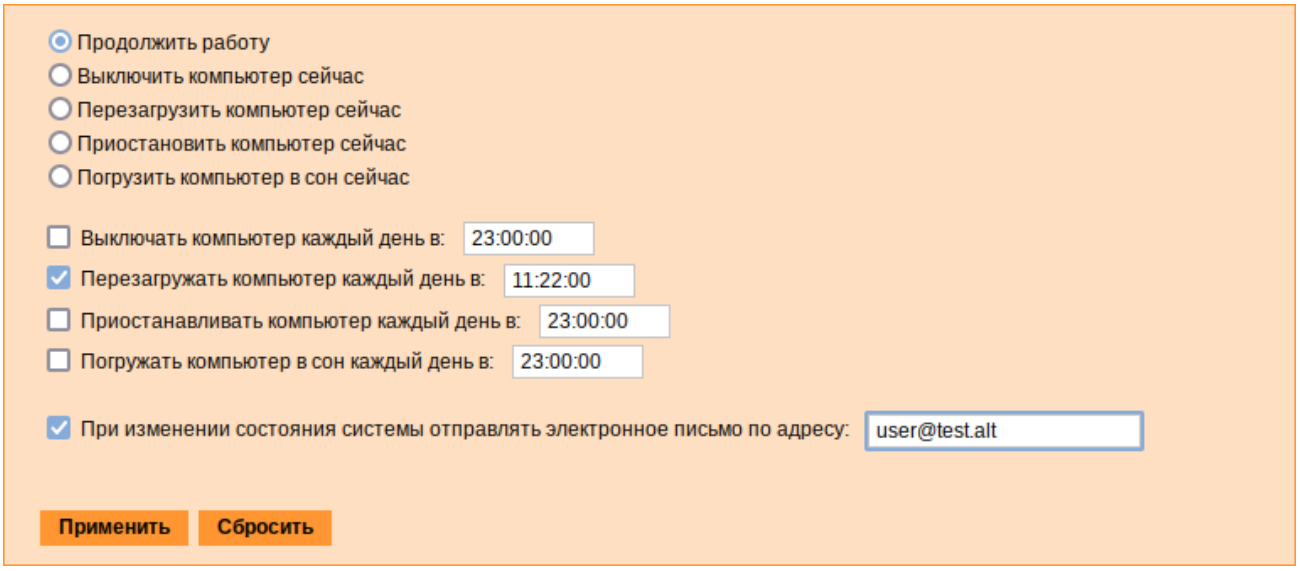

Рис. 159

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

```
Thu Sep 14 11:46:59 EET 2023: The host-15.test.alt is about to start.
```

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

5.5.12 Настройка ограничений на использование USB-устройств

Модуль ЦУС «USBGuard» (пакет alterator-usbguard) из раздела «Система» предназначен для настройки ограничений на использование USB-устройств. Модуль работает на основе функционала USBGuard, позволяет вести чёрный и белый списки ограничений и предоставляет два типа действий – allow/block.

Модуль предоставляет следующие возможности:

- сканирование подключенных устройств;
- выбор и добавление устройств в набор правил из списка подключенных устройств;
- создание предустановленных правил для распространённых сценариев;
- создание правил по дескрипторам интерфейса: CC:SS:PP;
- создание правил по свойствам USB-устройства: PID, VID;
- создание правил по хешу устройства по PID+VID+SN;
- создание сложных правил с дополнительными условиями;
- загрузка правил из csv-файла;
- редактирование значений в созданных правилах;
- просмотр журнала событий подключения/отключения USB-устройств.

5.5.12.1 Информационное поле

В информационном поле (Рис. 160) отображается текущее состояние службы usbguard, список пользователей и групп, которые могут редактировать правила, сообщения об ошибках и предупреждения.

Модуль «USBGuard». Информационное поле

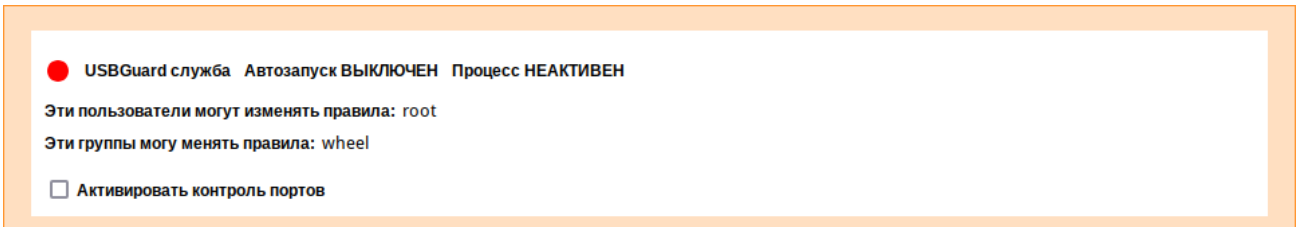

Рис. 160

Примечание. Добавить/удалить пользователя/группу, которые могут редактировать правила, можно в командной строке, например:

- дать пользователю user полный доступ к разделам «devices» и «exceptions», пользователь user также будет иметь возможность просматривать и изменять текущую политику:

```
# usbguard add-user -u user --devices ALL --policy modify,list --
exceptions ALL
```

- удалить права у пользователя user:

```
# usbguard remove-user -u user
```

Для включения контроля за USB-устройствами необходимо установить отметку в пункте «Активировать контроль портов», нажать кнопку «Проверить», а затем кнопку «Применить». Служба usbguard будет запущена и добавлена в автозагрузку (Рис. 161).

Контроль портов активирован

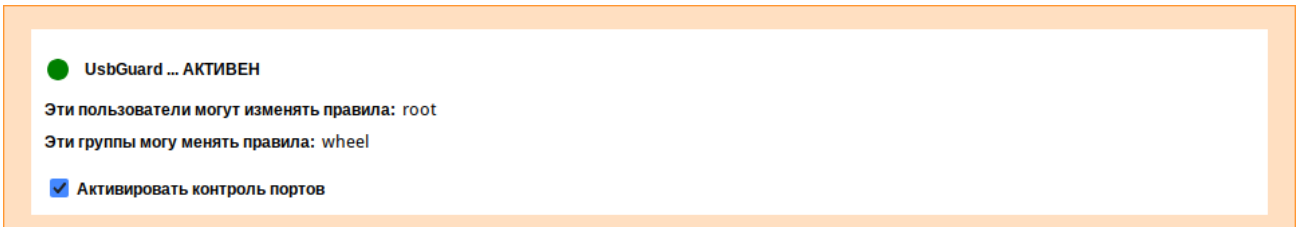

Рис. 161

Примечание. По умолчанию будет установлен режим «Белый список»: «Заблокировать все, кроме подключенных устройств», поэтому все подключенные устройства будут добавлены в список разрешённых, а все новые USB-устройства будут блокироваться. Изменить поведение по умолчанию можно, установив нужный режим перед запуском службы usbguard (см. «Предустановки»).

Для отключения контроля за USB-устройствами необходимо снять отметку с поля «Активировать контроль портов», нажать кнопку «Проверить», а затем кнопку «Применить» и перезагрузить систему.

5.5.12.2 Список USB-устройств

Если служба usbguard запущена, в веб-интерфейсе будет отображён список текущих подключённых устройств (Рис. 162).

USBGuard. Список USB-устройств

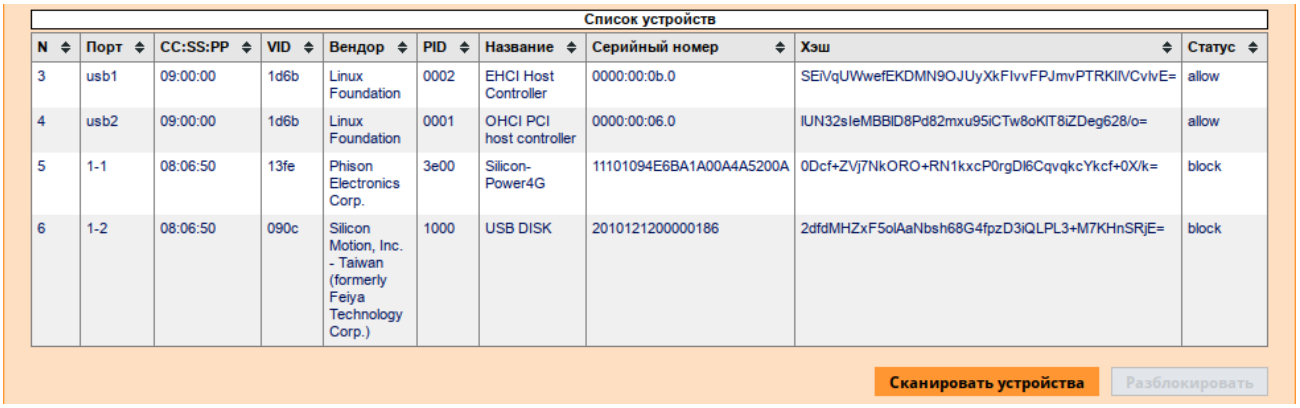

Рис. 162

В столбце «Статус» отображается текущее состояние USB-устройства («allow» – разрешённое устройство, «block» – заблокированное устройство).

Для редактирования состояния USB-устройства, необходимо выделить строку с нужным USB-устройством и нажать кнопку «Разблокировать»/«Заблокировать». При этом будет добавлено соответствующее правило в таблицу «Хэш».

Примечание. Если активен «Белый список», то для устройства со статусом «block» будет активна кнопка «Разблокировать», если активен «Чёрный список», то для устройства со статусом «allow» будет активна кнопка «Заблокировать».

Кнопка «Сканировать устройства» позволяет обновить список подключённых USB-устройств.

5.5.12.3 Предустановки

Правила могут работать в режиме белого или чёрного списка (Рис. 163). После установки режима «Чёрный список», будут заблокированы только перечисленные в данном списке USB-устройства. После установки режима «Белый список», будут заблокированы все USB-устройства, кроме перечисленных в данном списке.

Модуль «USBGuard». Предустановки

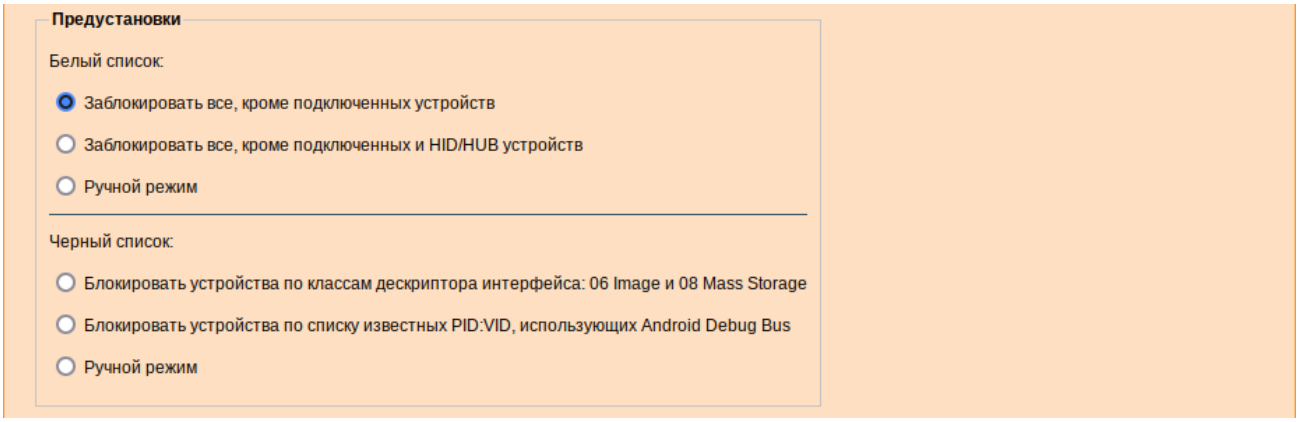

Рис. 163

Кроме ручного режима добавления правил в списки существует возможность предварительной настройки списков. Для предварительной настройки правил необходимо:

1) выбрать соответствующий пункт:

- «Белый список»:

- «Заблокировать все, кроме подключенных устройств» – в правила (таблица «Хэш») с действием «allow» будут добавлены все подключенные устройства. Все новые USB-устройства будут заблокированы (будут отображаться в таблице «Список устройств» со статусом «block»);
- «Заблокировать все, кроме подключенных и HID/HUB устройств» – в правила с действием «allow» будут добавлены все подключенные устройства (таблица «Хэш») и все устройства с интерфейсами 03:*:* и 09:*:* (таблица «Маски CC:SS:PP»). Все новые USB-устройства кроме HID/HUB-устройств (клавиатуры, мыши, джойстики, USB-концентраторы) будут заблокированы (будут отображаться в таблице «Список устройств» со статусом «block»);
- «Ручной режим» – позволяет установить свои правила.

- «Чёрный список»:

- «Блокировать устройства по классам дескриптора интерфейса: 06 Image и 08 Mass Storage» – в правила (таблица «Маски CC:SS:PP») с действием «block» будут добавлены все устройства с интерфейсами 08:*:* и 06:*:*. Все USB-устройства Mass Storage Device (USB-накопитель, карта памяти, кардридер, цифровая фотокамера) и Image (веб-камера, сканер) будут заблокированы (будут отображаться в таблице «Список устройств» со статусом «block»);
- «Блокировать устройства по списку известных PID:VID, использующих Android Debug Bus» – в правила (таблица «Маски VID:PID») с действием «block» будут добавлены известные Android-устройства. Все Android-устройства будут забло-

кированы (будут отображаться в таблице «Список устройств» со статусом «block»);

- «Ручной режим» – позволяет установить свои правила.

2) нажать кнопку «Проверить». Будут показаны планируемые изменения (Рис. 164);
3) если изменения корректные, нажать кнопку «Применить».
4) для отмены изменений (до нажатия кнопки «Применить») следует выбрать пункт «Ручной режим», нажать кнопку «Проверить», а затем «Применить».

Планируемые изменения

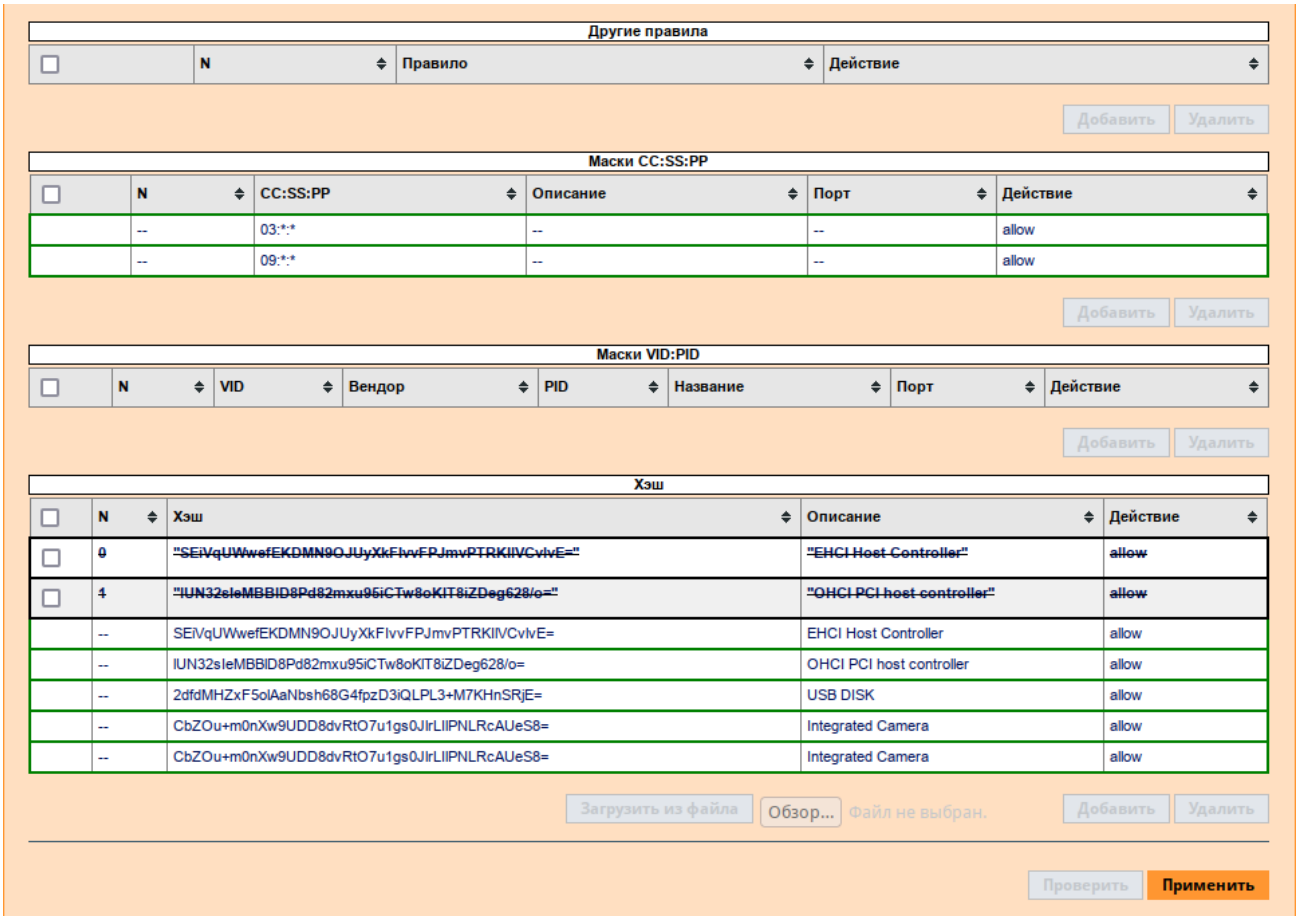

Рис. 164

5.5.12.4 Добавление правил

Для добавления нового правила должен быть выбран пункт «Ручной режим» в белом или чёрном списках. Если «Ручной режим» выбран в белом списке, правило будет добавлено с действием «allow», если в чёрном – с действием «block».

5.5.12.4.1 Правила по классу интерфейса

Назначение USB-устройств может определяться кодами классов, которые сообщаются USB-узлу для загрузки необходимых драйверов. Коды классов позволяют унифицировать работу с однотипными устройствами разных производителей. Устройство может поддерживать один или несколько классов, максимальное количество которых определяется количеством доступных

endpoints. Например, широко известны устройства класса Human Interface Device, HID (мыши, клавиатуры, игровые манипуляторы и т.д.) или устройства Mass Storage (USB-накопители, карты памяти и т.д.).

Примечание. Класс интерфейса указывается как три 8-битных числа в шестнадцатеричном формате, разделенных двоеточием (CC:SS:PP). Числа обозначают класс интерфейса (CC), подкласс (SS) и протокол (PP). Вместо номера подкласса и протокола можно использовать символ *, чтобы соответствовать всем подклассам или протоколам. Сопоставление определенного класса и определенного протокола не допускается, то есть если в качестве номера подкласса используется *, то для протокола также необходимо использовать *.

Добавление правила по маске:

1) под таблицей «Маски CC:SS:PP» нажать кнопку «Добавить»;
2) в поле «CC:SS:PP» вписать маску, например, правило для всех устройств с интерфейсами 09:*:* (Рис. 165);
3) нажать кнопку «Проверить». Корректное правило будет выделено зелёным цветом (Рис. 166), некорректное – красным;
4) исправить или удалить некорректное правило и повторно нажать кнопку «Проверить»;
5) нажать кнопку «Применить» для активации правила. Правило для всех устройств с интерфейсами 09:*:* будет добавлено.

Добавление правила для всех устройств с интерфейсами 09::**

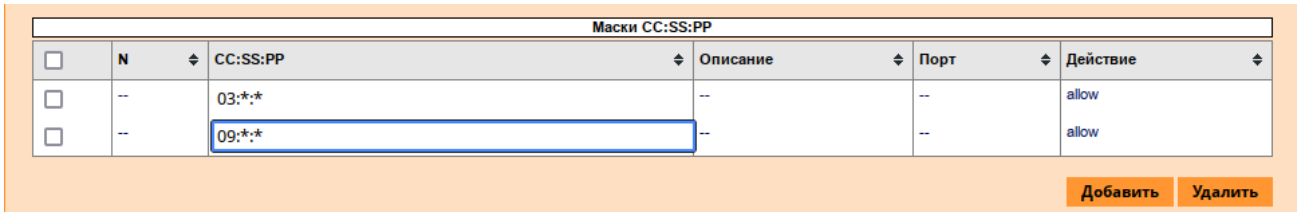

Рис. 165

Проверка правила

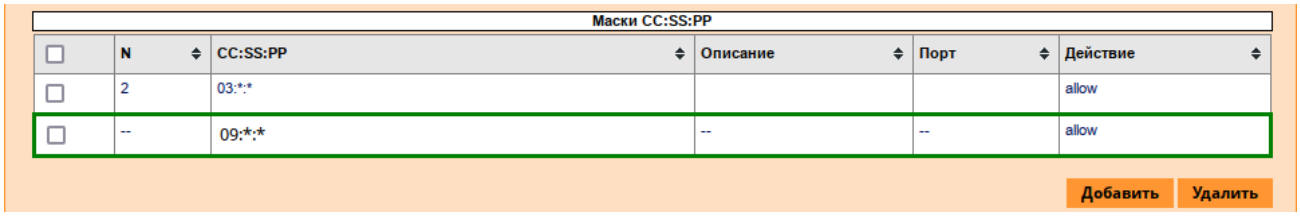

Рис. 166

5.5.12.4.2 Правила по VID&PID

Каждое USB-устройство содержит атрибуты, куда входит идентификатор разработчика устройства (VID) и идентификатор изделия (PID). На основании этих идентификаторов узел (компьютер) ищет методы работы с этим устройством (обычно это выражается в требовании установить драйверы, поставляемые разработчиком устройства).

Примечание. И VID и PID – это 16-битные числа в шестнадцатеричной системе счисления. В правиле можно также использовать символ *:

- для соответствия любому идентификатору устройства *:*
- для соответствия любому идентификатору продукта от конкретного поставщика, например, 090c:*

Добавление правила по VID&PID:

1) под таблицей «Маски ID:PID» нажать кнопку «Добавить»;
2) в поле «VID» вписать идентификатор разработчика устройства (VID), а в поле «PID» идентификатор изделия (PID) (Рис. 167);
3) нажать кнопку «Проверить». Корректное правило будет выделено зелёным цветом, некорректное – красным;
4) исправить или удалить некорректное правило и повторно нажать кнопку «Проверить»;
5) нажать кнопку «Применить» для активации правила.

Добавление правила по VID& PID

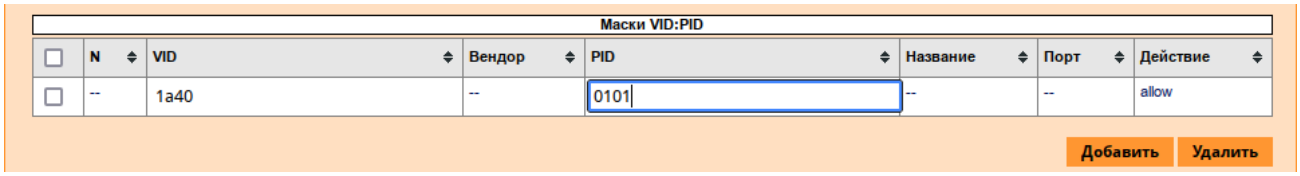

Рис. 167

5.5.12.4.3 Правила по хешу

Для каждого USB-устройства USBGuard вычисляет хеш на основе значений атрибутов устройства и данных дескриптора USB (PID+VID+SN).

Добавление правила по хешу:

1) под таблицей «Хэш» нажать кнопку «Добавить»;
2) в поле «Хэш» вписать хеш устройства (Рис. 168);
3) нажать кнопку «Проверить». Корректное правило будет выделено зелёным цветом, некорректное – красным;
4) исправить или удалить некорректное правило и повторно нажать кнопку «Проверить»;
5) нажать кнопку «Применить» для активации правила.

Добавление правила по хешу

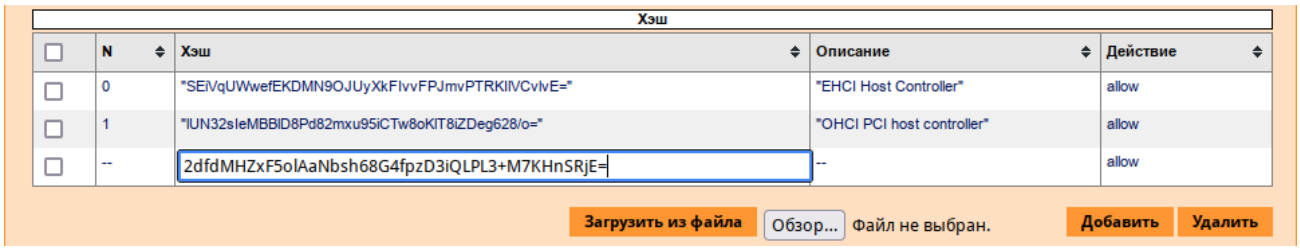

Рис. 168

5.5.12.4.4 Другие правила

Модуль позволяет создавать сложные правила с дополнительными условиями.

Добавление сложного правила:

1) под таблицей «Другие правила» нажать кнопку «Добавить»;
2) в поле «Правило» вписать правило (Рис. 169). Например, правило, разрешающее подключение принтера только через определённый порт:

```
allow id 04a9:177a name "Canon E400" serial "F572EC" via-port "1-2"
hash "eql9yA8m+5VVMmhXOvbUzwNPDGCAPq+fxIQHvbptlsY="
```

3) нажать кнопку «Проверить». Корректное правило будет выделено зелёным цветом, некорректное – красным;
4) исправить или удалить некорректное правило и повторно нажать кнопку «Проверить»;
5) нажать кнопку «Применить» для активации правила.

Добавление сложного правила

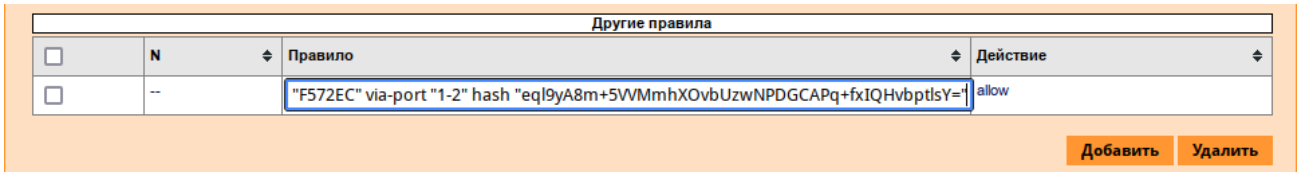

Рис. 169

5.5.12.4.5 Загрузка правил из файла

Правила должны быть добавлены в csv-файл, по одному правилу в каждой строке. Строка должна иметь вид:

```
allow/block,Interface,PID:VID,Hash
```

Например:

```
allow,,090c:1000,"2dfdMHZxF5olAaNbsh68G4fpzD3iQLPL3+M7KHnSRjE="
allow,00:00:*,,
allow,,1000:*,
allow,,,"eql9yA8m+5VVMmhXOvbUzwNPDGCAPq+fxIQHvbptlsY="
```

Примечание. Файл не должен содержать конфликтные правила – должны быть либо все allow, либо все block.

Загрузка правил из файла:

1) нажать кнопку «Обзор» (под таблицей «Хэш») и выбрать файл с правилами;
2) нажать кнопку «Загрузить из файла»;
3) нажать кнопку «Проверить». Корректное правило будет выделено зелёным цветом, некорректное – красным;
4) исправить или удалить некорректное правило и повторно нажать кнопку «Проверить»;
5) нажать кнопку «Применить» для активации правила.

Примечание. При загрузке правил из файла политика тоже будет выбрана из файла. Если в файле указана политика противоположная текущей, все существующие правила будут удалены.

5.5.12.5 Удаление правил

Пример удаления правила по маске:

1) в таблице «Маски CC:SS:PP» установить отметку в поле с соответствующим правилом;
2) нажать кнопку «Удалить». Правило будет готово к удалению (Рис. 170);
3) нажать кнопку «Проверить»;
4) нажать кнопку «Применить» для удаления правила.

Удаление правила

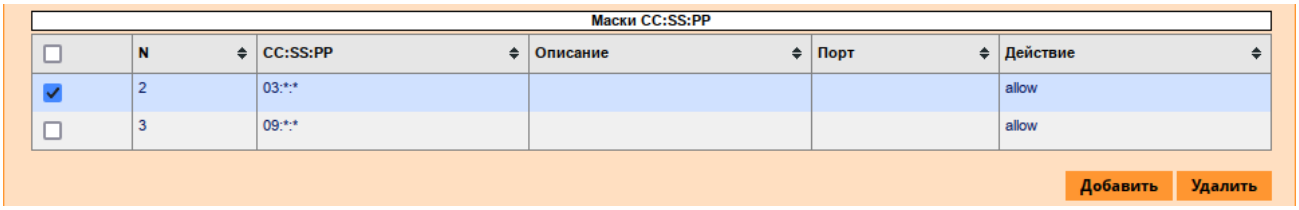

Рис. 170

Правила из других таблиц удаляются аналогичным способом.

5.5.12.6 Просмотр журнала аудита

Для просмотра журнала событий подключения/отключения USB-устройств (журнала аудита) необходимо нажать кнопку «Журнал», расположенную в левом нижнем углу модуля. По нажатию на эту кнопку раскрывается журнал аудита (Рис. 171).

Журнал аудита USBGuard

Рис. 171

Примечание. Фильтрация по логу USBGuard – строгая, регистрозависимая.

5.5.13 Настройка ограничения доступа к файловой системе USB-устройства

Модуль ЦУС «USBMount» (пакет alterator-usbmount) из раздела «Система» позволяет ограничить доступ к файловой системе USB-устройства по UID/GID. В модуле также предусмотрена возможность просмотра журнала событий подключения/отключения USB-устройств.

Особенности работы модуля:

- если для устройства не создано правило, то служба не вмешивается в логику монтирования USB-устройства;
- если для устройства создано правило, то служба монтирует блочные устройства на назначенном USB-устройстве в каталог /media/alt-usb-mount/$user_$group или /media/alt-usb-mount/root_$group, если пользователь не указан;
- служба назначает ACL для указанного пользователя и группы на каталог, в котором будет создана точка монтирования блочного устройства;
- в правилах можно указать только существующего локального пользователя и пользовательскую группу;
- доступ к USB-устройству назначенному пользователю и группе предоставляется полностью (rw);
- любой пользователь может отмонтировать устройство через стандартные средства ОС;
- служба не вмешивается в права самих файловых систем блочных устройств;
- рекомендуемая файловая система для переносных носителей exFAT.

П р и м е ч а н и е . Особенности работы модуля с файловыми системами:

- EXT2/3/4, XFS, BTRFS поддерживают права. Доступ к файловой системе будет также определяться назначенными правами самой файловой системы;
- FAT16/FAT32/exFAT не поддерживают права. Доступ будет полностью определяться через точку монтирования, назначенную в USBMount;
- ISO9660/UDF поддерживает только readonly. Доступ будет предоставлен только на чтение;
- NTFS поддерживает права. Не рекомендуется использовать. В случае если ранее NTFS носитель был извлечён небезопасно, то носитель будет смонтирован только для чтения.

5.5.13.1 Запуск/останов службы

В модуле отображается текущее состояние службы USBMount (Рис. 172).

Для включения контроля над устройствами необходимо передвинуть переключатель «Служба USBMount остановлена» и нажать кнопку «Сохранить». Служба USBMount будет запущена и добавлена в автозагрузку.

Для отключения контроля над устройствами необходимо передвинуть переключатель «Служба USBMount активна» и нажать кнопку «Сохранить».

Служба USBMount остановлена

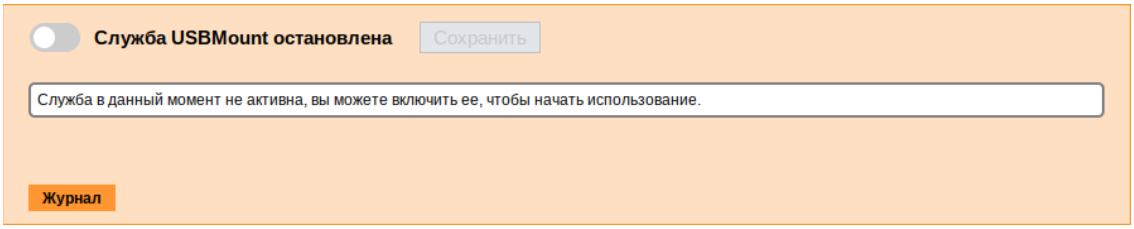

Рис. 172

5.5.13.2 Список устройств

Если служба USBMount запущена, в веб-интерфейсе будет отображён список текущих подключённых устройств (Рис. 173).

Служба USBMount запущена

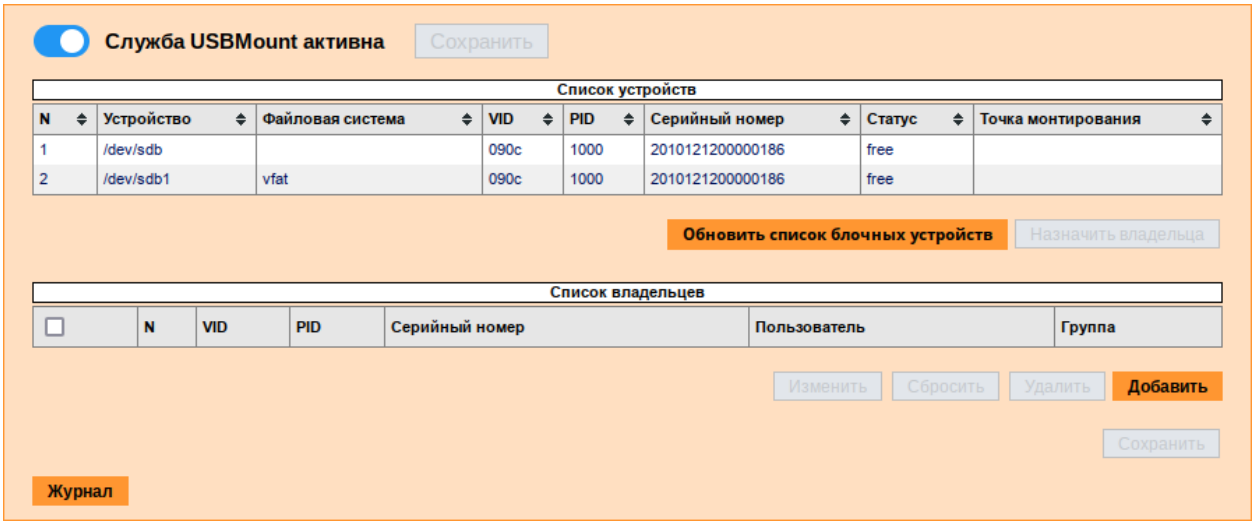

Рис. 173

В столбце «Статус» отображается текущее состояние устройства («free» – владелец для устройства не назначен, «owned» – устройству назначен владелец).

Если устройству назначен владелец и устройство примонтировано, то текущая точка монтирования отображается в столбце «Точка монтирования».

Кнопка «Обновить список блочных устройств» позволяет обновить список подключённых устройств.

5.5.13.3 Добавление/удаление правил

Для того чтобы назначить права для подключенного блочного устройства, необходимо выполнить следующие действия:

1) выделить строку с нужным устройством в таблице «Список устройств» (Рис. 174) и нажать кнопку «Назначить владельца» (или дважды щелкнуть мышью по строке с устройством):
2) правило будет добавлено в таблицу «Список владельцев» (Рис. 175);
3) в столбце «Пользователь» выбрать пользователя, в столбце «Группа» – группу владельца блочного устройства (Рис. 176);

4) нажать кнопку «Сохранить». Статус устройства в таблице «Список устройств» изменится на «owned» (Рис. 177).

Назначение владельца для подключенного устройства

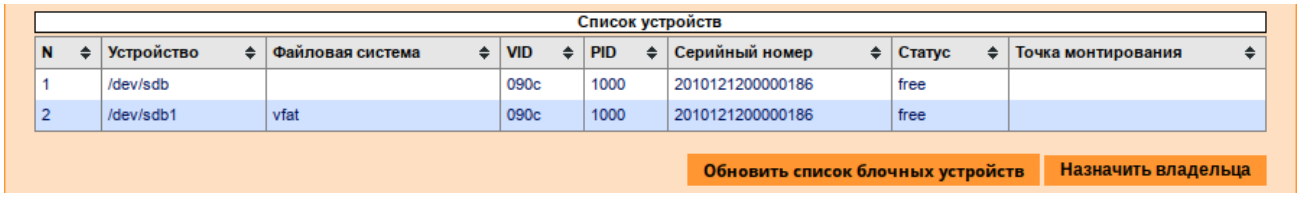

Рис. 174

Правило добавлено в таблицу «Список владельцев»

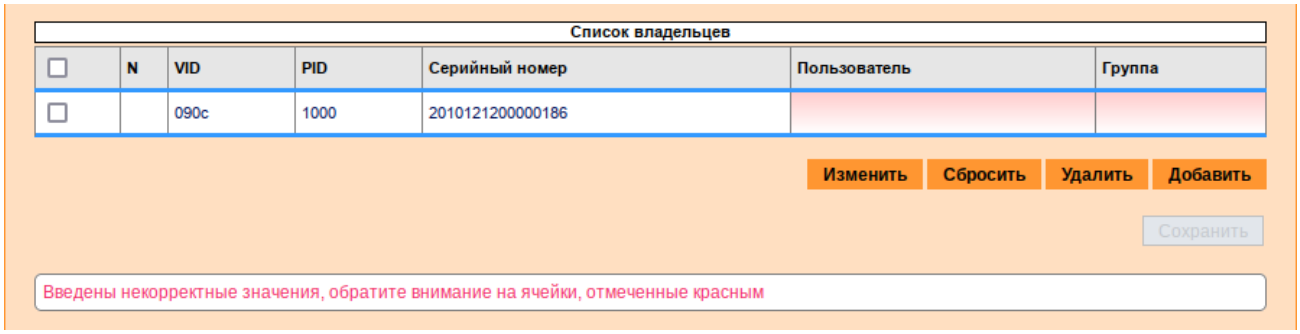

Рис. 175

Указание пользователя и группы для блочного устройства

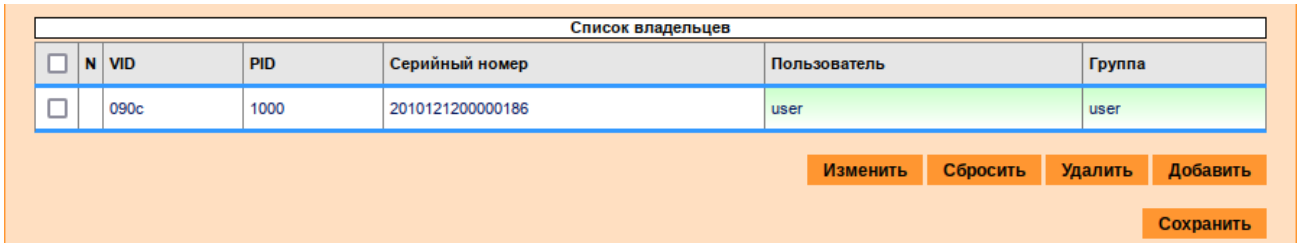

Рис. 176

Статус «owned» для устройства в таблице «Список устройств»

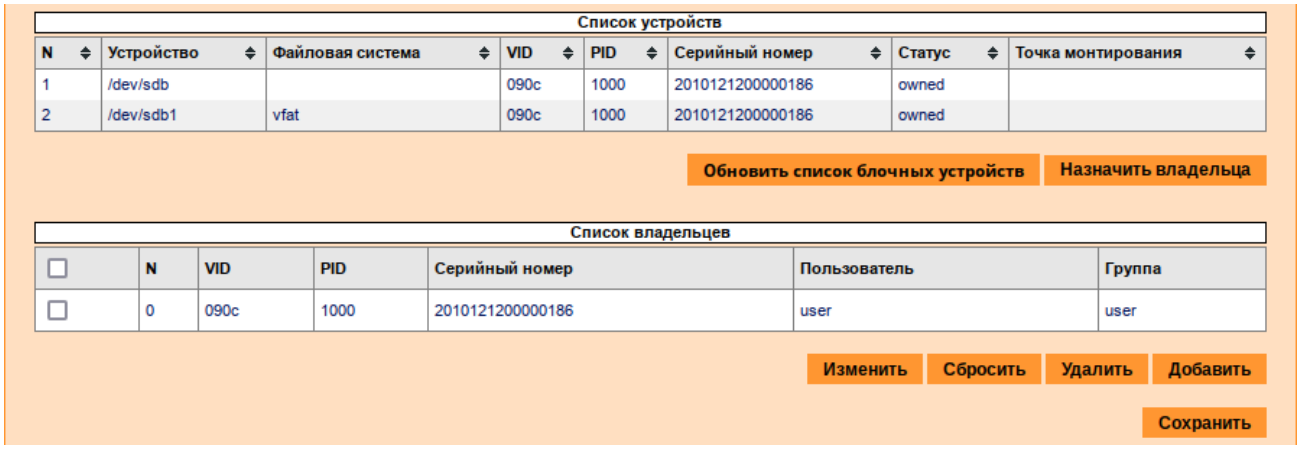

Рис. 177

Примечание. При создании/редактировании правила, некорректные значения будут выделены красным цветом, корректные – зелёным.

Чтобы назначить права для произвольного блочного устройства, необходимо:

1) нажать кнопку «Добавить», расположенную под таблицей «Список владельцев». В таблицу будет добавлена пустая строка (Рис. 178);
2) в соответствующих столбцах указать «VID, PID» и «Серийный номер устройства» (Рис. 179);
3) в столбце «Пользователь» выбрать пользователя, в столбце «Группа» – группу владельца блочного устройства (Рис. 180);
4) нажать кнопку «Сохранить».

USBMount. Создание нового правила

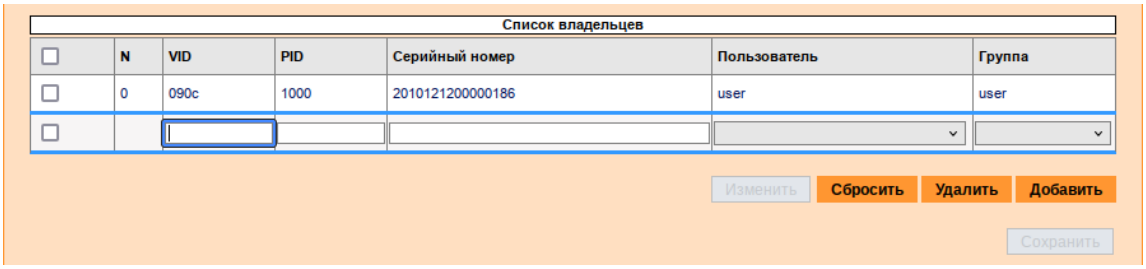

Рис. 178

USBMount. Параметры устройства

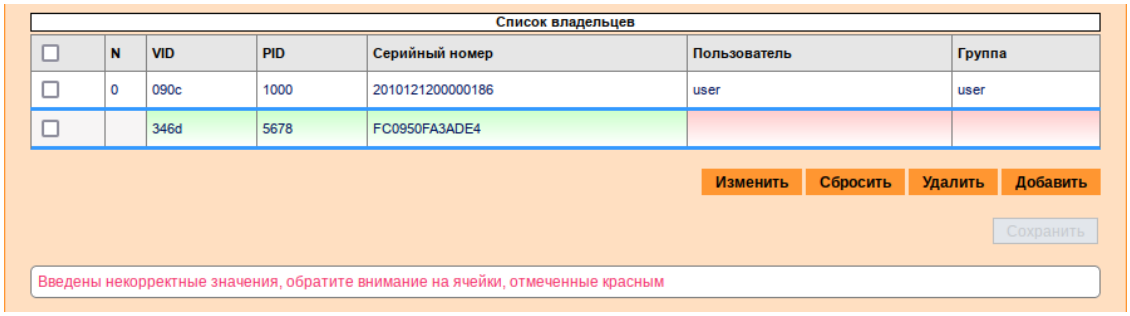

Рис. 179

USBMount. Указание группы для блочного устройства

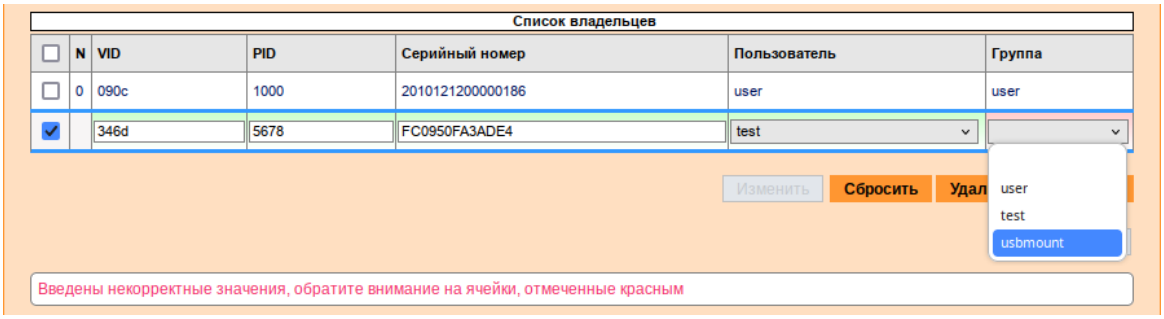

Рис. 180

Примечание. Если необходимо назначить права для определённой группы пользователей, в столбце «Пользователь» следует выбрать прочерк.

Редактирование правила:

1) дважды щелкнуть мышью по строке с правилом в таблице «Список владельцев» (или выделить строку в таблице «Список владельцев» и нажать кнопку «Изменить»);
2) внести изменения;
3) нажать кнопку «Сохранить».

Удаление правила:

1) выделить строку(и) с правилом в таблице «Список владельцев»;
2) нажать кнопку «Удалить» (Рис. 181);
3) нажать кнопку «Сохранить».

USBMount. Удаление правила

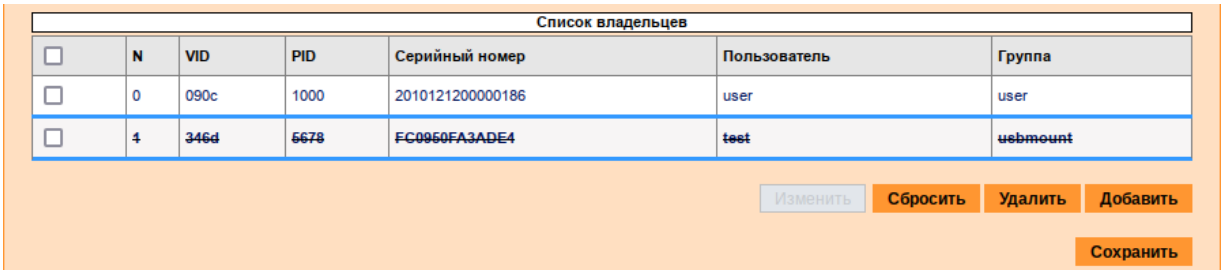

Рис. 181

Примечание. Для отмены внесённых изменений (до нажатия кнопки «Сохранить») следует нажать кнопку «Сбросить».

5.5.13.4 Просмотр журнала аудита

Для просмотра журнала событий подключения/отключения USB-устройств необходимо нажать кнопку «Журнал», расположенную в левом нижнем углу модуля. По нажатию на эту кнопку раскрывается журнал аудита (Рис. 182).

Журнал аудита USBMount

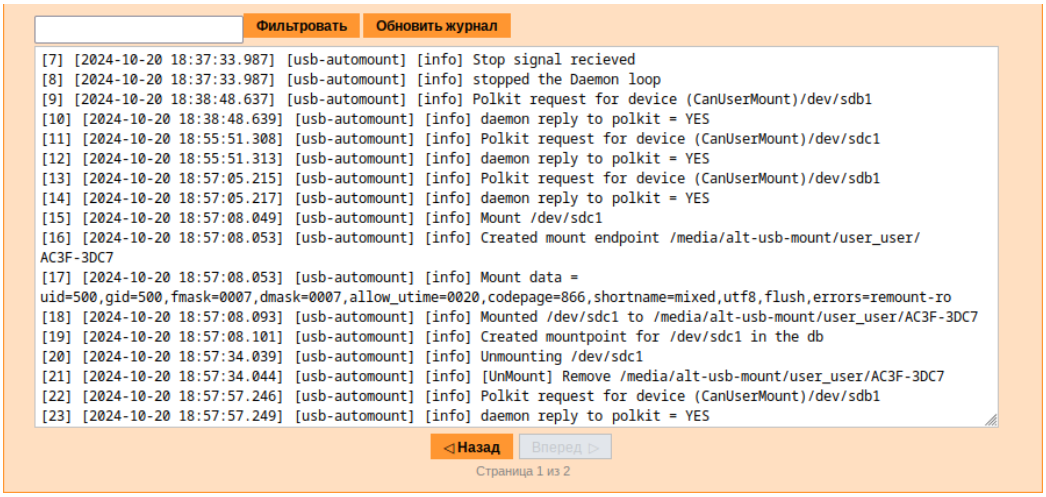

Рис. 182

5.6 Прочие возможности ЦУС

Возможности ЦУС ОС «Альт Рабочая станция» не ограничиваются только теми, что были описаны выше.

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
```

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

```
# systemctl restart ahttpd
```

5.7 Права доступа к модулям ЦУС

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

Для разрешения доступа пользователю к конкретному модулю, администратору в веб-интерфейсе ЦУС необходимо выбрать нужный модуль и нажать ссылку «Параметры доступа к модулю», расположенную в нижней части окна модуля (Рис. 183).

Ссылка «Параметры доступа к модулю»

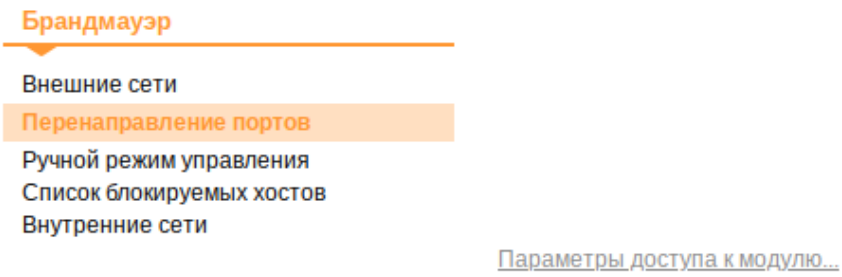

Рис. 183

В открывшемся окне, в списке «Новый пользователь», необходимо выбрать пользователя, который получит доступ к данному модулю, и нажать кнопку «Добавить» (Рис. 184). Для сохранения настроек необходимо перезапустить HTTP-сервер, для этого достаточно нажать кнопку «Перезапустить HTTP-сервер».

Параметры доступа к модулю

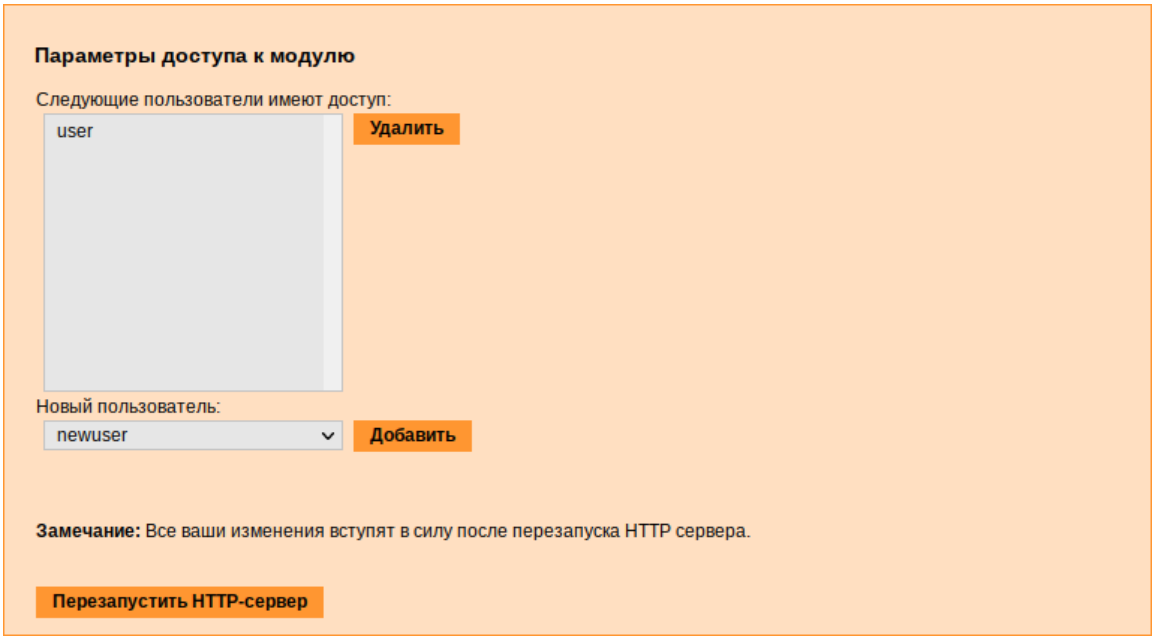

Рис. 184

Для удаления доступа пользователя к определенному модулю, администратору, в окне этого модуля необходимо нажать ссылку «Параметры доступа к модулю», в открывшемся окне в списке пользователей которым разрешен доступ, выбрать пользователя, нажать кнопку «Удалить» (Рис. 184) и перезапустить HTTP-сервер.

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

6 ФУНКЦИОНАЛ ОПЕРАЦИОННОЙ СИСТЕМЫ

6.1 ГОСТ в OpenSSL

6.1.1 Поддержка шифрования по ГОСТ в OpenSSL

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

1. Установить пакет `openssl-gost-engine`:

   ```
   # 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
   ```

6.1.2 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:
            33:16:0f:9e:ab:c5:cb:2b:97:9a:57:c5:99:f9:88:b9:7e:68:23:86
        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: Jan 12 14:25:18 2024 GMT
            Not After : Jan 11 14:25:18 2025 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:E50615F7CE64842F60D12F757914FE6CE02924BD4C21800B4138670494A8EE8D
               Y:62F5C4BAC4170304CA06C3ADAC909709EB4B6888727AD11DC5D7E52E9827D2E0
            Parameter set: GOST R 34.10-2012 (256 bit) ParamSet A
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                A2:78:10:51:27:1A:2E:BE:64:F9:71:50:B7:4F:AD:87:43:A3:73:81
            X509v3 Authority Key Identifier:
                keyid:A2:78:10:51:27:1A:2E:BE:64:F9:71:50:B7:4F:AD:87:43:A3:73:81

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)
         17:72:f3:5f:01:5f:03:cb:a2:86:f3:3d:3b:ee:55:75:19:88:
         dc:3a:51:24:4b:0f:a6:1d:fe:26:7a:b4:eb:fb:10:31:1b:0f:
         27:76:8e:20:f3:b8:03:24:c5:a3:3e:71:34:e5:f5:78:02:4b:
         65:8b:37:c6:d2:e7:3f:cd:97:65
```

6.2 Задание хешей паролей в соответствии с ГОСТ Р 34.11-2012

6.2.1 Задание хешей паролей в соответствии с ГОСТ Р 34.11-2012 в ЦУС

Для измения типа хеша по умолчанию на ГОСТ Р 34.11-2012 необходимо в ЦУС перейти в раздел «Система» → «Настройки безопасности».

Примечание. Должен быть установлен пакет `alterator-secsetup`:

```
# apt-get install alterator-secsetup
```

В открывшемся окне следует отметить пункт «Включить хеширование паролей пользователей по алгоритму ГОСТ Р 34.11-2012» и нажать кнопку «Применить» (Рис. 185).

Задание хешей паролей в соответствии с ГОСТ Р 34.11-2012

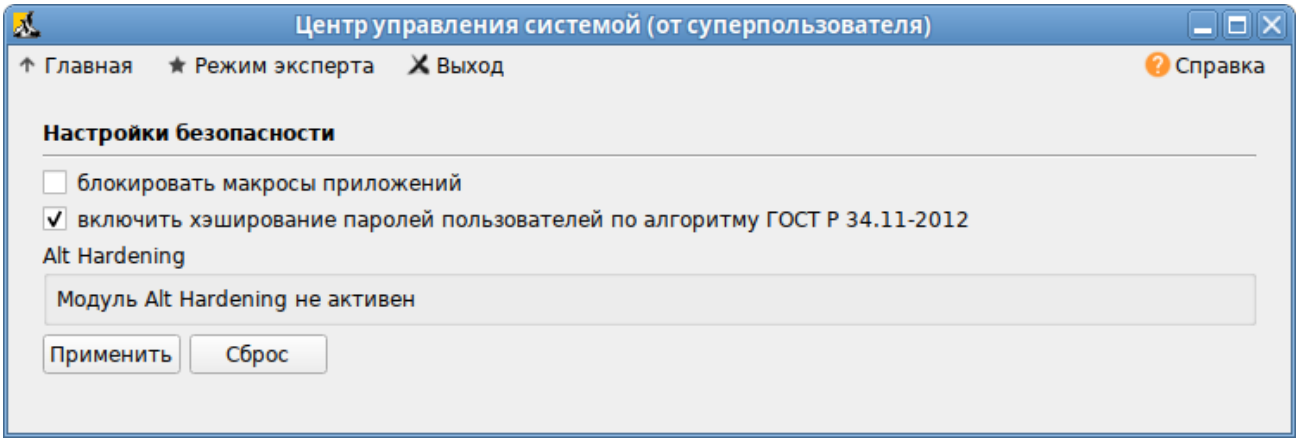

Рис. 185

Проверить настройку можно, установить пароль пользователю и выполнив команду:

```
# passwd user
```

```
# passwd -S user
Password set, gost-yescrypt encryption.
```

6.2.2 Задание хешей паролей в соответствии с ГОСТ Р 34.11-2012 в консоли

Просмотреть тип хеша пароля пользователя:

```
# passwd -S <имя>
```

Пример ожидаемого результата:

```
# passwd -S user
Password set, yescrypt encryption.
```

Изменить типа хеша по умолчанию на gost-yescrypt:

```
# control tcb-hash-prefix gost_yescrypt
```

Примечание. Должен быть установлен tcb-hash-prefix-control:

```
# apt-get install tcb-hash-prefix-control
```

Установить пароль пользователю:

```
# passwd user
```

Проверка:

```
# passwd -S user
Password set, gost-yescrypt encryption.
```

Список возможных хеш-функций можно вывести, выполнив команду:

```
# control tcb-hash-prefix help
bcrypt_2b: prefix=$2b$ count=8 (4 - 31 limit)
bcrypt_2y: prefix=$2y$ count=8 (4 - 31 limit)
bcrypt_2a: prefix=$2a$ count=8 (4 - 31 limit)
yescrypt: prefix=$y$ count=8 (0 - 11 limit)
scrypt: prefix=$7$ count=8 (0 - 11 limit)
gost_yescrypt: prefix=$gy$ count=8 (0 - 11 limit)
sha256: prefix=$5$ count=10000 (1000 - 100000 limit)
sha512: prefix=$6$ count=10000 (1000 - 100000 limit)
default: hash prefix managed by libcrypt
```

Текущее значение хеш-функции:

```
# control tcb-hash-prefix
gost_yescrypt
```

Изменить типа хеша на установленный по умолчанию:

```
# control tcb-hash-prefix default
```

6.3 Подпись и проверка ЭЦП ГОСТ

Для создания и проверки электронной подписи в ОС «Альт Рабочая станция» можно использовать программу ALT CSP КриптоПро (Подпись и проверка ЭЦП ГОСТ). Возможности ALT CSP КриптоПро:

- создание электронной подписи (отсоединенной и присоединенной);
- подпись группы файлов;
- создание электронной подписи в zip-контейнере;
- проверка электронной подписи;
- просмотр содержимого zip-контейнера с документом и электронной подписью.

Примечание. Необходимо установить пакет `alt-csp-cryptopro`, если он еще не установлен:

```
# apt-get install alt-csp-cryptopro
```

Примечание. Для работы ALT CSP КриптоПро должно быть установлено программное обеспечение КриптоПро, у пользователя должен существовать контейнер с сертификатом (в локальном считывателе или на токене).

Запустить ALT CSP КриптоПро можно:

- из меню рабочей среды: «Меню MATE» → «Стандартные» → «ALT CSP КриптоПро»;
- из контекстного меню файла в файловом менеджере Caja: «Caja-Actions actions» → «Подписать документ» (Рис. 186). Для возможности запуска из контекстного меню файла должен быть установлен пакет `mate-file-manager-actions`;
- из командной строки:

```
$ alt-csp-cryptopro
```

Контекстное меню файла в файловом менеджере Caja

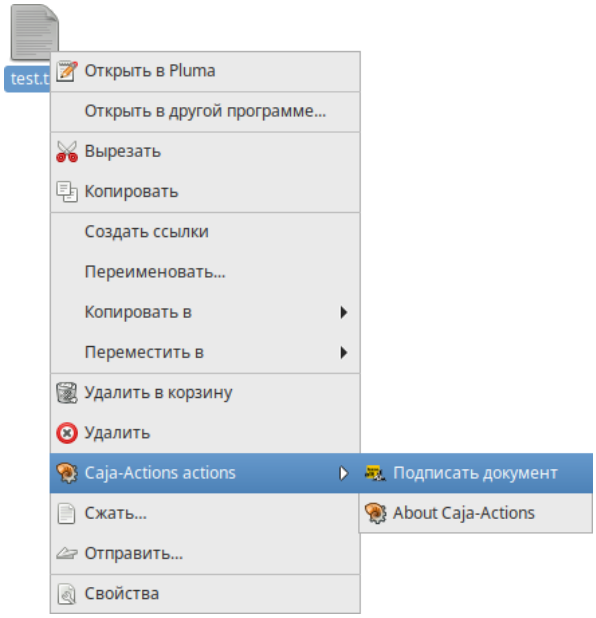

Рис. 186

6.3.1 Создание электронной подписи

Особенности отсоединенной электронной подписи:

- файл подписи создается отдельно от подписываемого файла (подписываемый документ остается неизменным);
- для проверки подписи нужно передавать два файла – исходный документ и файл подписи;
- нет ограничения по формату подписываемых документов.

Для создания отсоединенной подписи следует на вкладке «Подпись» (Рис. 187), в разделе «Документ» нажать кнопку «Выбрать» и выбрать электронный документ. Нажав кнопку «Просмотреть», можно просмотреть содержимое электронного документа.

Выбор документа для создания электронной подписи

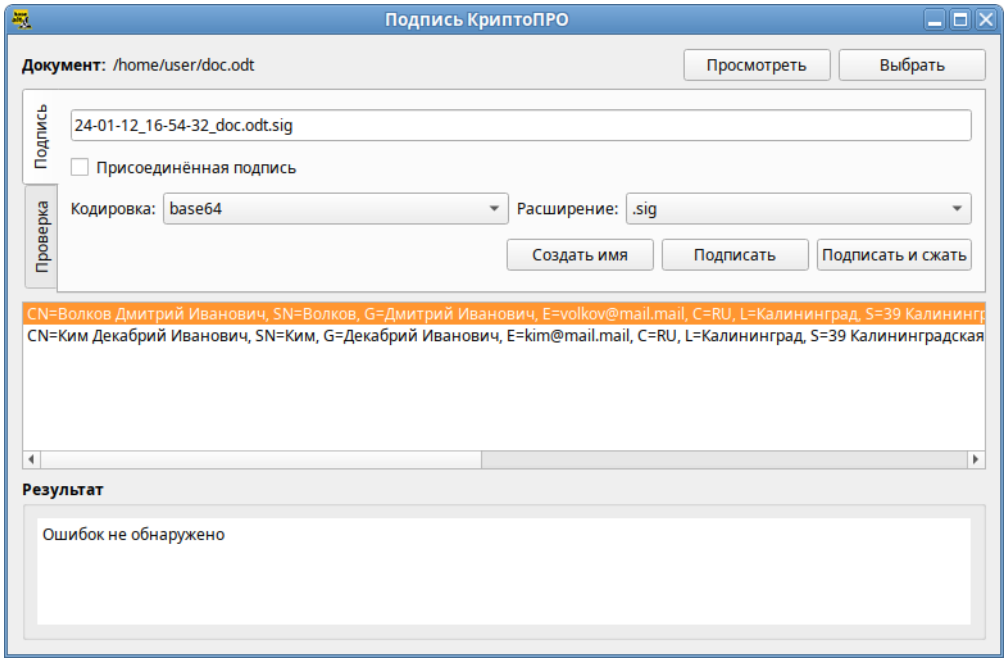

Рис. 187

Примечание. Документ будет выбран автоматически, если программа была запущена из контекстного меню файла.

Далее следует выбрать сертификат, которым будет подписан документ.

Примечание. Если окно выбора сертификатов пустое, то сертификатов для подписи у вас просто нет, и вам следует установить хотя бы один.

В выпадающем списке «Кодировка» можно выбрать кодировку подписи: base64 (по умолчанию) или DER. В выпадающем списке «Расширение» можно задать расширение файла цифровой подписи: .p7b, .p7s, .sig (по умолчанию) или .sign.

Название файла цифровой подписи по умолчанию будет сформировано путем добавления к имени файла информации о текущей дате и времени, например, `гг-мм-дд_чч-мм-сс_<ИМЯ_ФАЙЛА>.sig`. При необходимости это имя можно откорректировать вручную или вернуть к виду по умолчанию, нажав кнопку «Создать имя».

Для генерации электронной подписи следует нажать кнопку «Подписать».

В открывшемся окне необходимо ввести пароль на контейнер, если он был установлен, и нажать кнопку «ОК».

В результате успешного создания электронной подписи в поле «Результат» появится сообщение «Ошибок не обнаружено». Сформированный файл подписи по умолчанию будет сохранен в тот же каталог, в котором находится файл с исходными данными.

ALT CSP КриптоПро позволяет объединить электронный документ и соответствующую ему электронную подпись в zip-архив (<ИМЯ_ФАЙЛА>.signed.zip). Для создания zip-архива необходимо при создании электронной подписи нажать кнопку «Подписать и сжать». В результате со-

здания электронной подписи, будет сформирован zip-архив, в который будут перемещены файл электронного документа и файл электронной подписи.

Присоединенная подпись – разновидность электронной подписи, при создании которой формируется файл, содержащий как саму электронную подпись, так и исходный документ. Отправлять для проверки подписи нужно будет только этот файл. Для проверки и прочтения такого документа должно быть установлено ПО, поддерживающее работу с прикрепленной подписью.

Для создания присоединенной подписи необходимо при создании электронной подписи в разделе «Подпись» установить отметку в поле «Присоединенная подпись» (Рис. 188). В том же каталоге, в котором хранился исходный документ, появится файл, содержащий как саму электронную подпись, так и исходный документ.

Создание присоединенной подписи

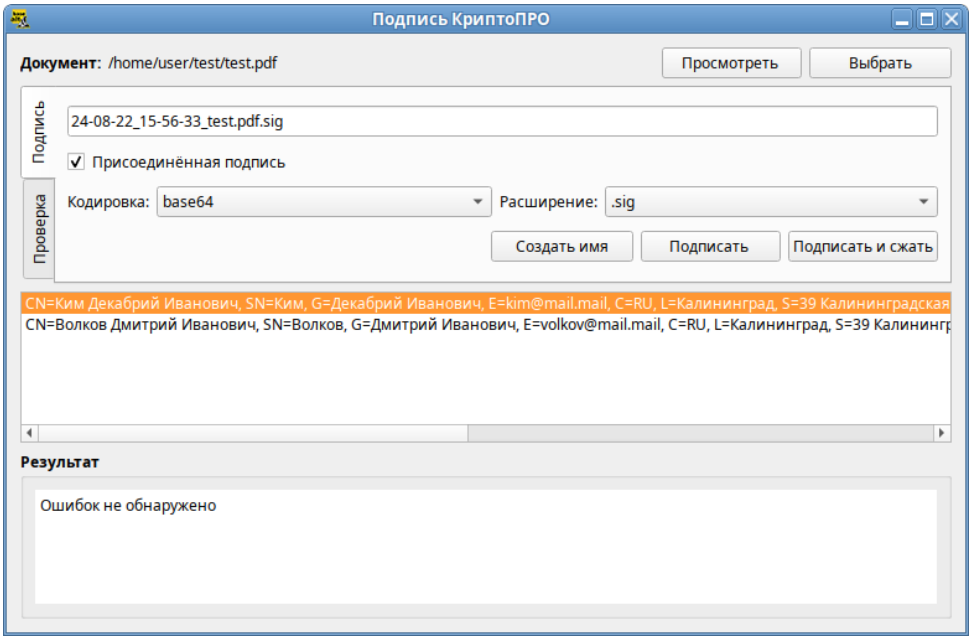

Рис. 188

Примечание. Пример извлечения файла с данными из файла электронной подписи:

```
$ cryptcp -verify 24-08-22_15-56-33_test.pdf.sig test_new.pdf
```

В файл test_new.pdf будут извлечены данные.

Для того чтобы подписать несколько файлов, можно выбрать их в файловом менеджере и запустить ALT CSP КриптоПро из контекстного меню или в ALT CSP КриптоПро в разделе «Документ» нажать кнопку «Выбрать» и выбрать нужные файлы. В поле «Документ» будет указано количество выбранных файлов, а в поле «Результат» будут перечислены выбранные файлы (Рис. 189). Далее следует выбрать сертификат, которым будет подписан документ, указать кодировку подписи, задать расширение файла цифровой подписи и нажать кнопку «Подписать». В каталоге с выбранными файлами будут созданы подписи файлов (например, <ИМЯ_ФАЙЛА>.sig, если было выбрано расширение sig).

Подпись группы файлов

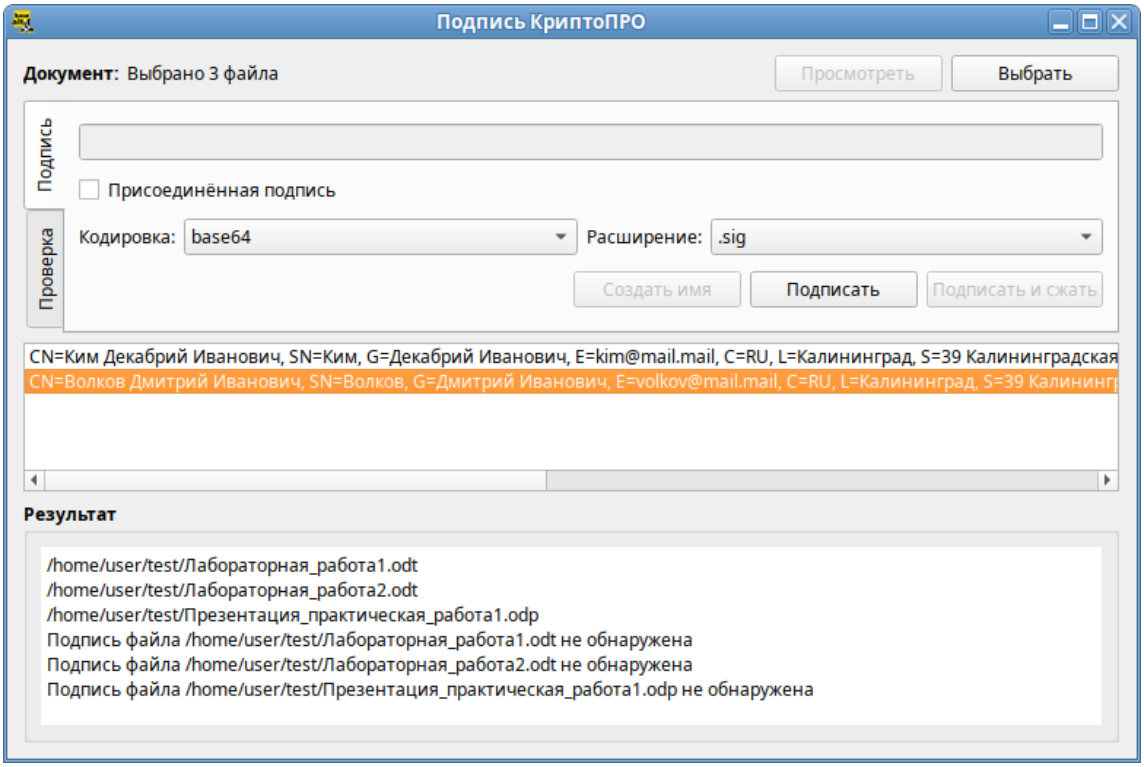

Рис. 189

6.3.2 Проверка электронной подписи

Проверка электронной подписи выполняется во вкладке «Проверка».

Для проверки отсоединенной подписи нужны оба файла, файл подписи и файл исходного документа. Для проверки подписи необходимо нажать кнопку «Выбрать» и выбрать электронный документ. Далее следует выбрать подпись, нажав кнопку «Выбрать» в секции «Подпись» и выбрать файл электронной подписи. После появления имени подписи в секции «Подпись» необходимо нажать кнопку «Проверить» (Рис. 190).

Проверка отсоединенной электронной подписи

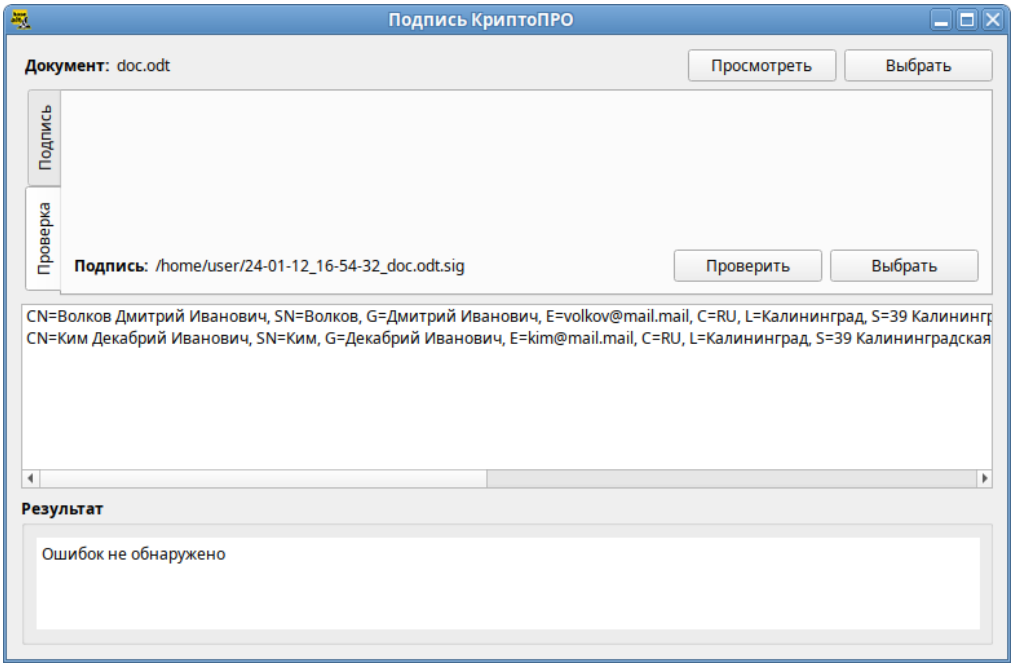

Рис. 190

Примечание. Если программа «Подпись и проверка ЭЦП ГОСТ» была запущена из контекстного меню файла, документ будет выбран автоматически. Если программа была запущена из контекстного меню файла электронной подписи, подпись и документ будут выбраны автоматически.

Для проверки электронной подписи в контейнере достаточно выбрать zip-архив (документ и подпись будут выбраны автоматически) и нажать кнопку «Проверить» (Рис. 191).

Проверка электронной подписи в zip-архиве

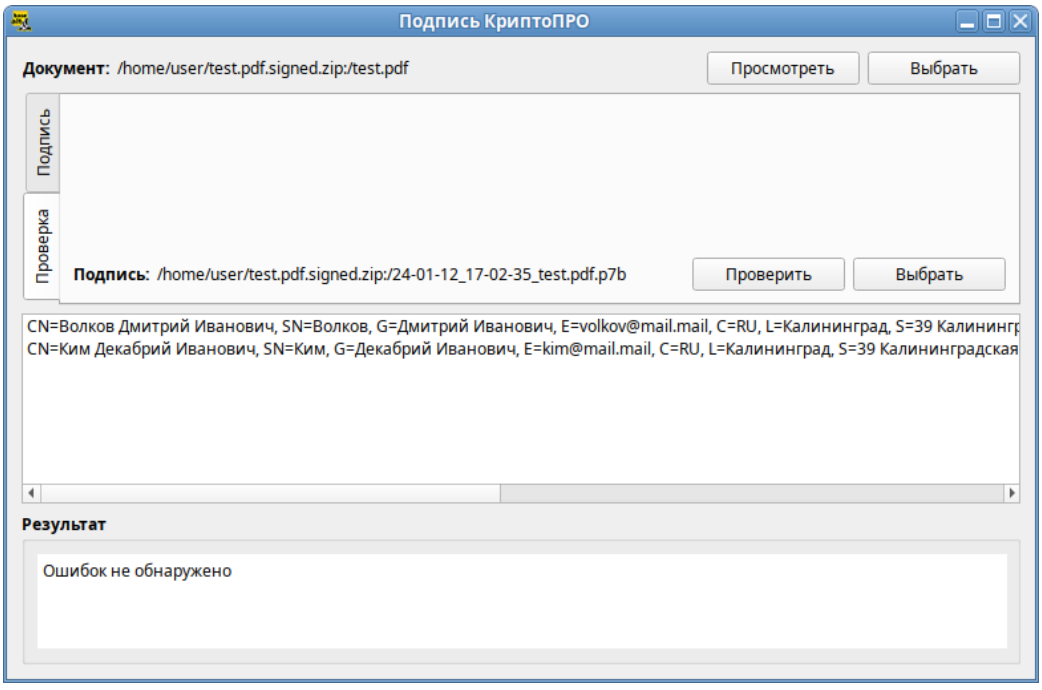

Рис. 191

Для проверки присоединённой электронной подписи необходимо выбрать подписанный электронный документ и нажать кнопку «Проверить» (Рис. 192).

Проверка присоединенной электронной подписи

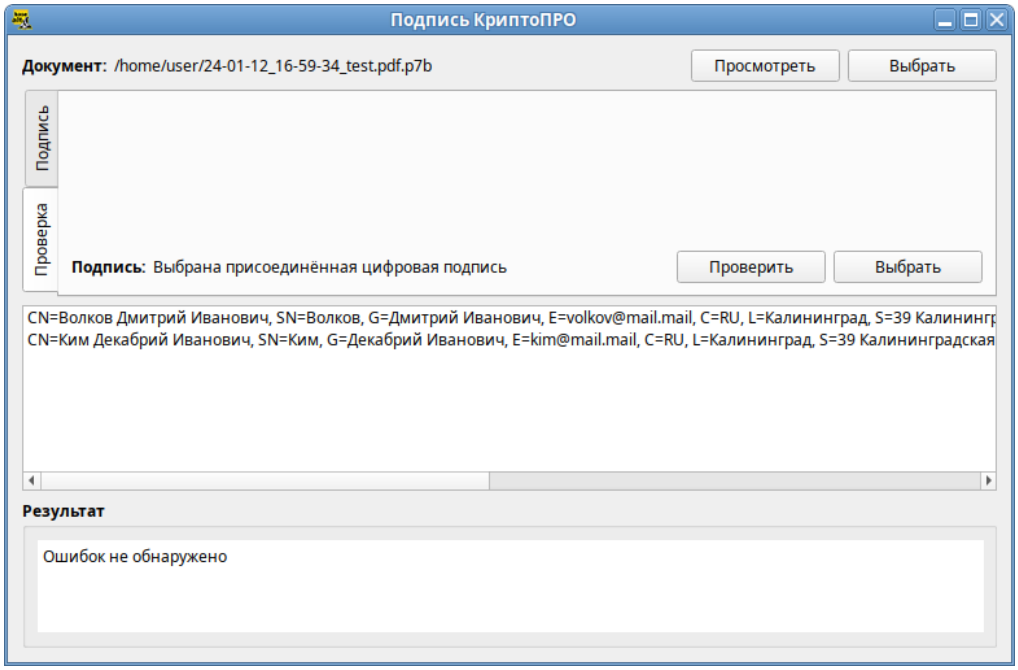

Рис. 192

6.4 Управление шифрованными разделами

Зашифрованный раздел может быть создан, например, при установке системы.

В LUKS для одного зашифрованного раздела используются восемь слотов, в каждом из которых может храниться отдельный пароль (ключ). Любой из восьми ключей может быть использован для расшифровки раздела. Любой пароль может быть изменён или удалён необратимо.

Для управления шифрованными разделами можно воспользоваться командой `cryptsetup`. Ниже описаны лишь некоторые возможности утилиты `cryptsetup`. Для получения более подробной информации используйте команду `man cryptsetup`.

Просмотреть текущее состояние всех слотов:

```
# cryptsetup luksDump /dev/sdb1 | grep Slot
Key Slot 0: DISABLED
Key Slot 1: ENABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

где /dev/sdb1 – шифрованный раздел.

Примечание. Определить является ли устройство LUKS-разделом:

```
# cryptsetup isLuks -v /dev/sdb1
Команда выполнена успешно.
```

Определить какой раздел является шифруемым можно, выполнив команду:

```
# lsblk
NAME                                          MAJ:MIN RM  SIZE RO TYPE
MOUNTPOINT
sda                                             8:0    0   18G  0 disk
├─sda1                                          8:1    0 1023M  0 part
[SWAP]
└─sda2                                          8:2    0   17G  0 part
/
sdb                                             8:16   0   18G  0 disk
└─sdb1                                          8:17   0   18G  0 part
  └─luks-7853363d-e7e2-1a42-b5b9-0af119e19920 253:0    0   18G  0
crypt /home
sr0                                            11:0    1 1024M  0 rom
```

Добавить новый пароль на зашифрованный раздел (требуется предоставить уже имеющийся пароль интерактивно или посредством опции `--key-file`):

```
# cryptsetup luksAddKey /dev/sdb1
Введите любую существующую парольную фразу:
Введите новую парольную фразу для слота ключа:
Парольная фраза повторно:
```

Пароль будет назначен в первый свободный слот:

```
# cryptsetup luksDump /dev/sdb1 | grep Slot
Key Slot 0: ENABLED
Key Slot 1: ENABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

Можно указать номер определенного слота с помощью опции `--key-slot`, например:

```
# cryptsetup luksAddKey /dev/sdb1 --key-slot 5
```

Заменить один из паролей на другой (старый пароль нужно ввести интерактивно или задать опцией `--key-file`):

```
# cryptsetup luksChangeKey /dev/sdb1
Введите изменяемую парольную фразу:
Введите новую парольную фразу:
Парольная фраза повторно:
```

Если задан номер слота (опцией `--key-slot`), нужно ввести старый пароль именно для заданного слота, и замена пароля произойдёт тоже в этом слоте. Если номер слота не задан и есть свободный слот, то сначала новый пароль будет записан в свободный слот, а потом будет затёрт слот, содержащий старый пароль. Если свободных слотов не окажется, то новый пароль будет записан прямо в слот, ранее содержащий старый пароль.

Удалить заданный пароль (затирает слот):

```
# cryptsetup luksRemoveKey /dev/sdb1
Введите удаляемую парольную фразу:
```

Примечание. В пакетном режиме (`-q`) удаление даже последнего пароля будет выполнено без каких-либо предупреждений. Если ни одного пароля не останется (то есть все слоты ключей будут пусты), дешифровать LUKS-раздел станет невозможно.

Процедура сброса забытого пароля на зашифрованный раздел:

1. Получить зашифрованные пароли всех разделов:

```
# dmsetup table --showkey
luks-7853363d-e7e2-1a42-b5b9-0af119e19920: 0 37730304 crypt aes-cbc-
essiv:sha256
b15c22e8d60a37bcd27fb438637a8221fbec66c83be46d33a8331a4002cf3144 0
8:17 4096
```

Часть поля после «aes-cbc-essiv:sha256» является зашифрованным паролем.

Сохранить зашифрованный пароль в текстовый файл:

```
# echo
"b15c22e8d60a37bcd27fb438637a8221fbec66c83be46d33a8331a4002cf3144" >
lukskey.txt
```

2. Преобразовать существующий пароль из текстового файла в двоичный файл:

```
# xxd -r -p lukskey.txt lukskey.bin
luks-7853363d-e7e2-1a42-b5b9-0af119e19920: 0 37730304 crypt aes-cbc-
essiv:sha256
```

```
b15c22e8d60a37bcd27fb438637a8221fbec66c83be46d33a8331a4002cf3144 0
8:17 4096
```

3. Добавить новый пароль, используя существующий пароль, извлеченный в бинарный файл:

```
# cryptsetup luksAddKey /dev/sdb1 --master-key-file <(cat lukskey.bin)
Введите новую парольную фразу для слота ключа:
Парольная фраза повторно:
```

Примечание. Сбросить пароль на зашифрованный раздел можно, только если данный раздел уже примонтирован.

6.5 Timeshift

Timeshift – программа для автоматического периодического создания копий системы (снимков/snapshots).

Timeshift предназначен, прежде всего, для создания снимков 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 меню MATE: «Приложения» → «Системные» → «Программа для восстановления системы» или из командной строки:

```
$ timeshift-launcher
```

Запуск Timeshift требует прав администратора, поэтому необходимо ввести пароль администратора (Рис. 193).

Запрос пароля для запуска Timeshift

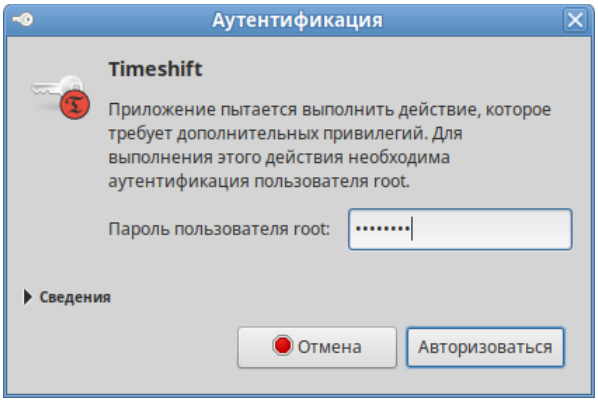

Рис. 193

При первом запуске 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. 194).

Окно программы Timeshift

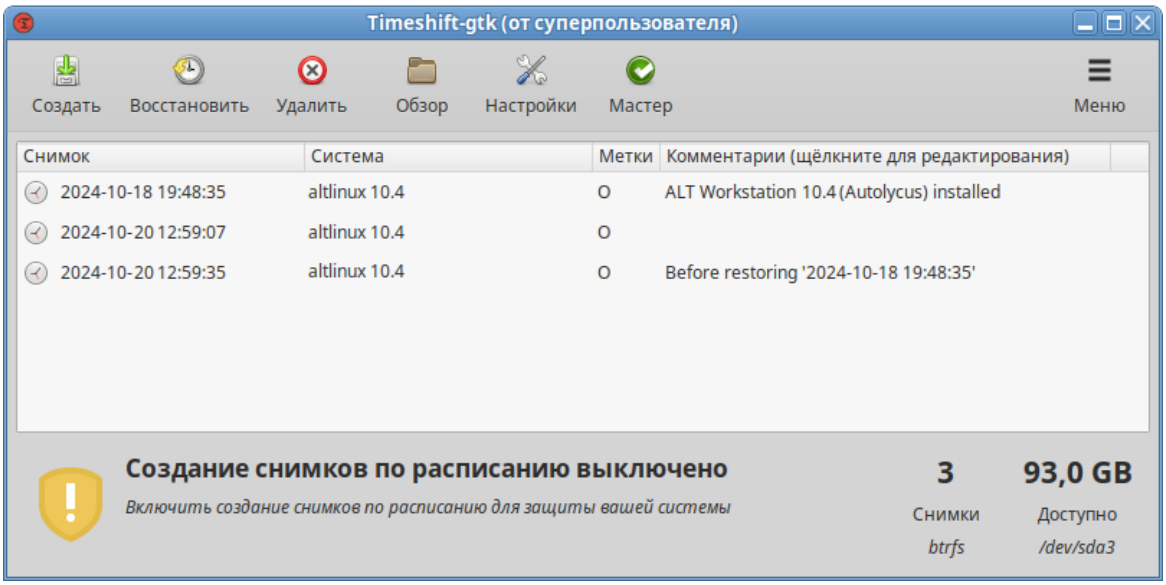

Рис. 194

6.5.1 Настройка резервного копирования

6.5.1.1 Режим RSYNC

Особенности режима RSYNC:

- снимки создаются путем копирования системных файлов при помощи rsync и создания жёстких 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 необходимо перезагрузить после восстановления снимка.

Тип снимков «RSYNC» можно выбрать на вкладке «Тип» окна настроек Timeshift (Рис. 195) или на первом шаге работы мастера установки.

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`.

Выбрать место, где будут храниться снимки, можно на вкладке «Место» (Рис. 196).

Выбор режима RSYNC

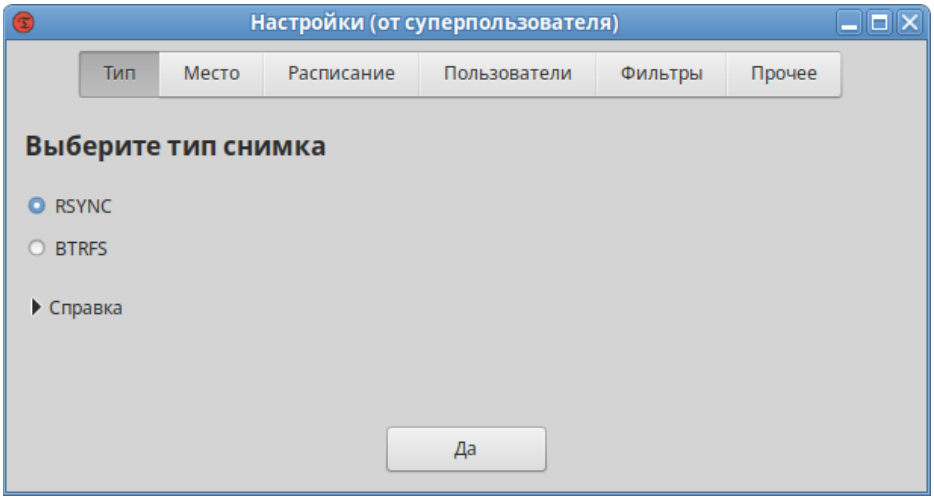

Рис. 195

Выбор места хранения снимков RSYNC

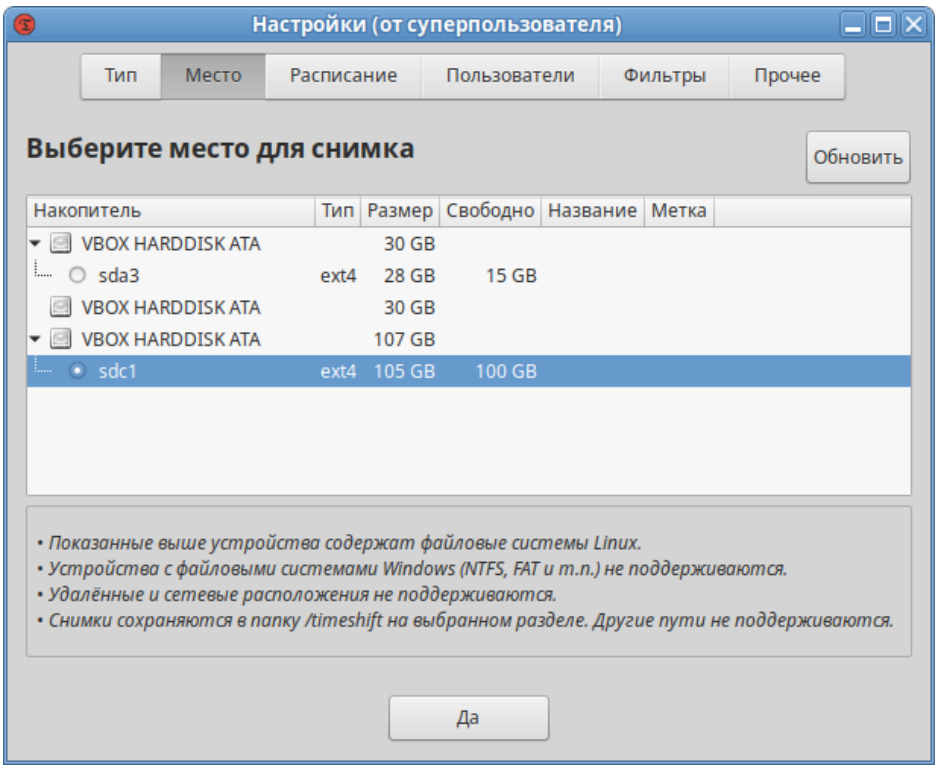

Рис. 196

На вкладке «Расписание» (Рис. 197) следует выбрать уровни создания снимков (ежемесячно, еженедельно, ежедневно, ежечасно, при загрузке) и указать количество сохраняемых снимков для каждого уровня.

Примечание. Снимки уровня «Загрузка» создаются при каждом запуске системы (с задержкой в 10 минут). Они выполняются в фоне и не влияют на скорость загрузки системы.

По умолчанию домашние каталоги пользователей не включаются в резервную копию. На вкладке «Пользователи» можно изменить это поведение. Например, если выбрать опцию

«Включить только скрытые файлы» (Рис. 198), будет выполнено резервное копирование и восстановление скрытых файлов и каталогов в домашнем каталоге пользователя (эти каталоги содержат пользовательские файлы конфигурации).

Расписание для снимков RSYNC

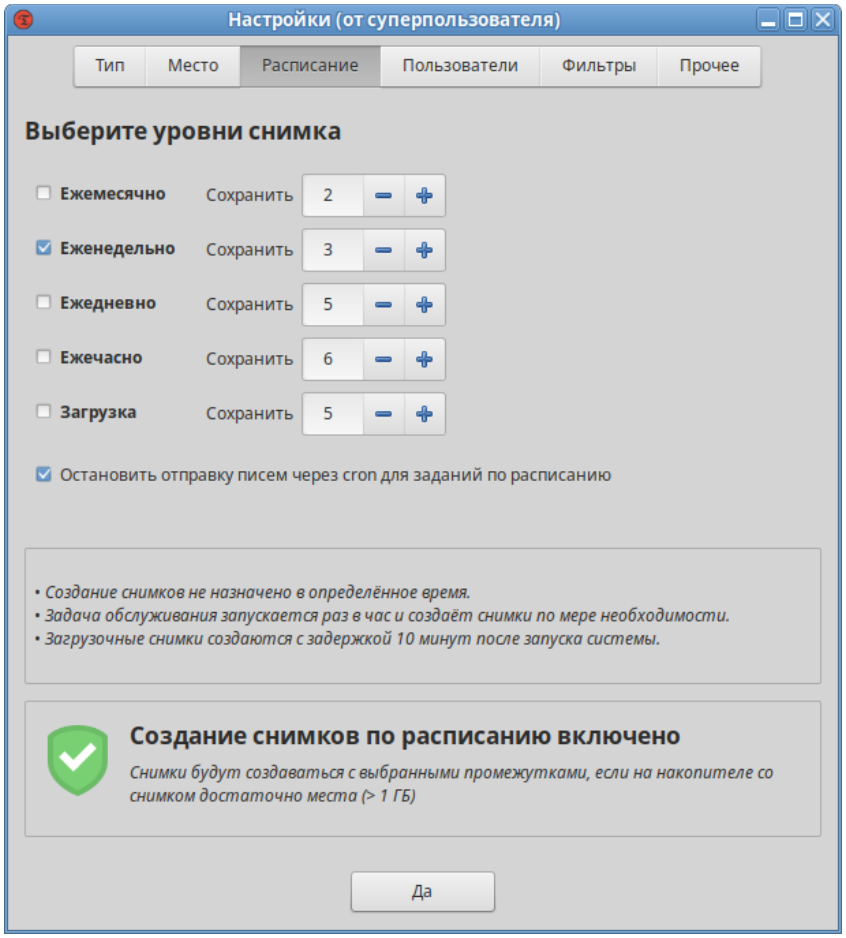

Рис. 197

Timeshift. Вкладка «Пользователи»

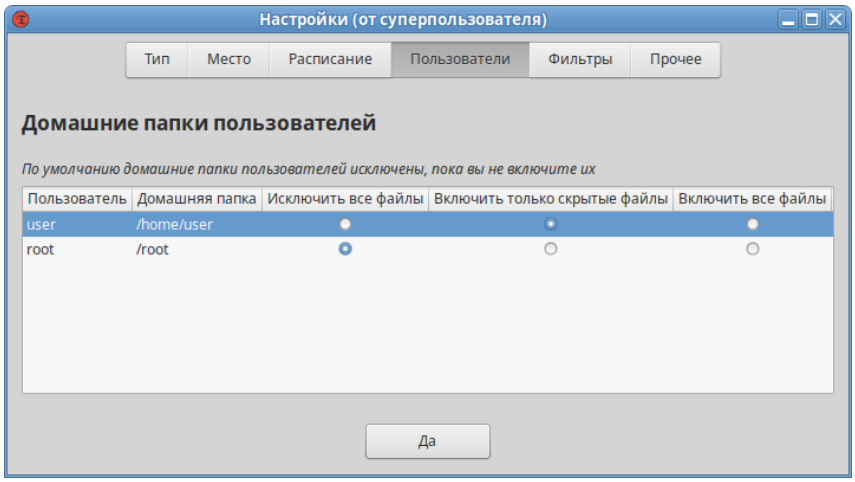

Рис. 198

На вкладке «Фильтры» (Рис. 199) можно указать, какие файлы/каталоги включать/исключать из резервного копирования (динамические каталоги исключаются по умолчанию: `/dev`, `/proc`, …).

В данном примере из резервной копии будут исключены все файлы mp3, все системные журналы, кроме журналов аудита. Просмотреть итоговый список исключений (Рис. 200) можно, нажав кнопку «Итог». Отредактировать шаблон можно, дважды щелкнув левой кнопкой мыши по строке шаблона.

Timeshift. Вкладка «Фильтры»

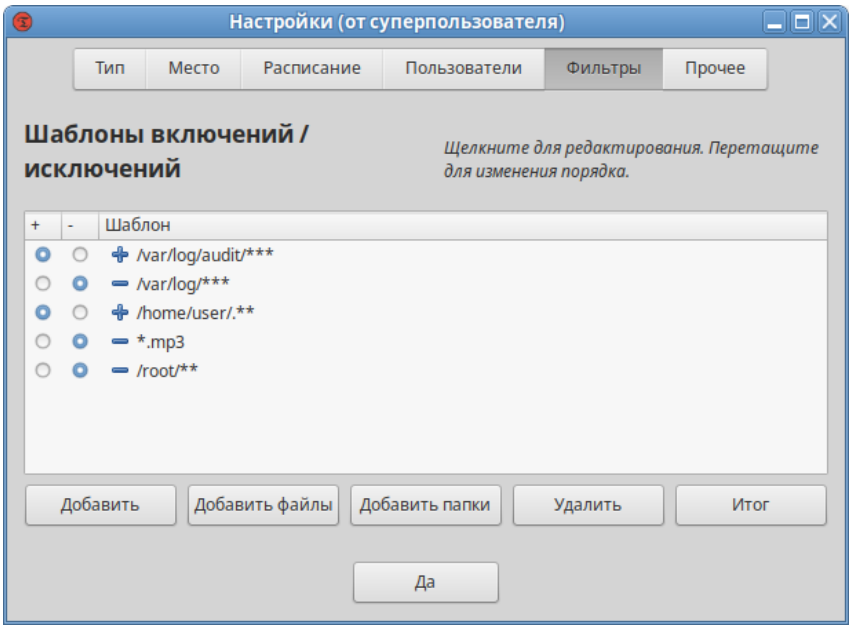

Рис. 199

Список исключений

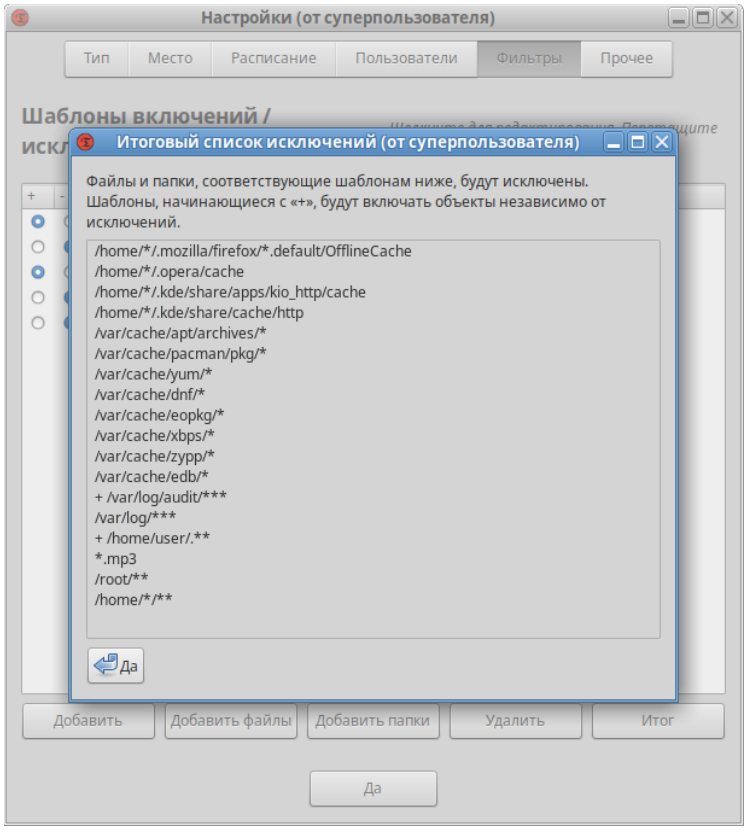

Рис. 200

На вкладке «Прочее» (Рис. 220) можно выбрать формат даты.

Timeshift. Вкладка «Прочее»

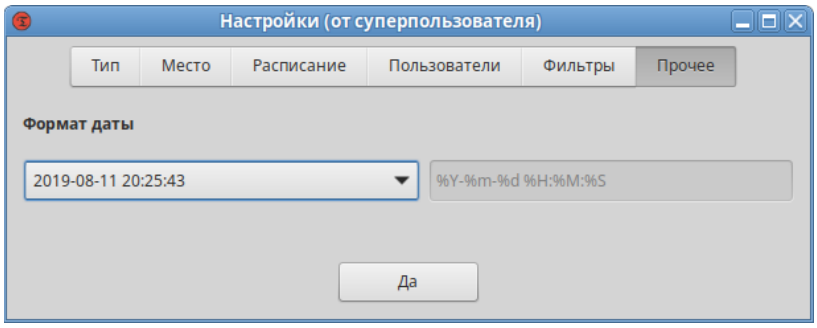

Рис. 201

6.5.1.2 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 нём, 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. 202):

- подтом @ с точкой монтирования в /;
- подтом @home с точкой монтирования в /home.

Тип снимков BTRFS можно выбрать на вкладке «Тип» окна настроек Timeshift (Рис. 203) или на первом шаге работы мастера установки.

Корень системы с файловой системой BtrFS

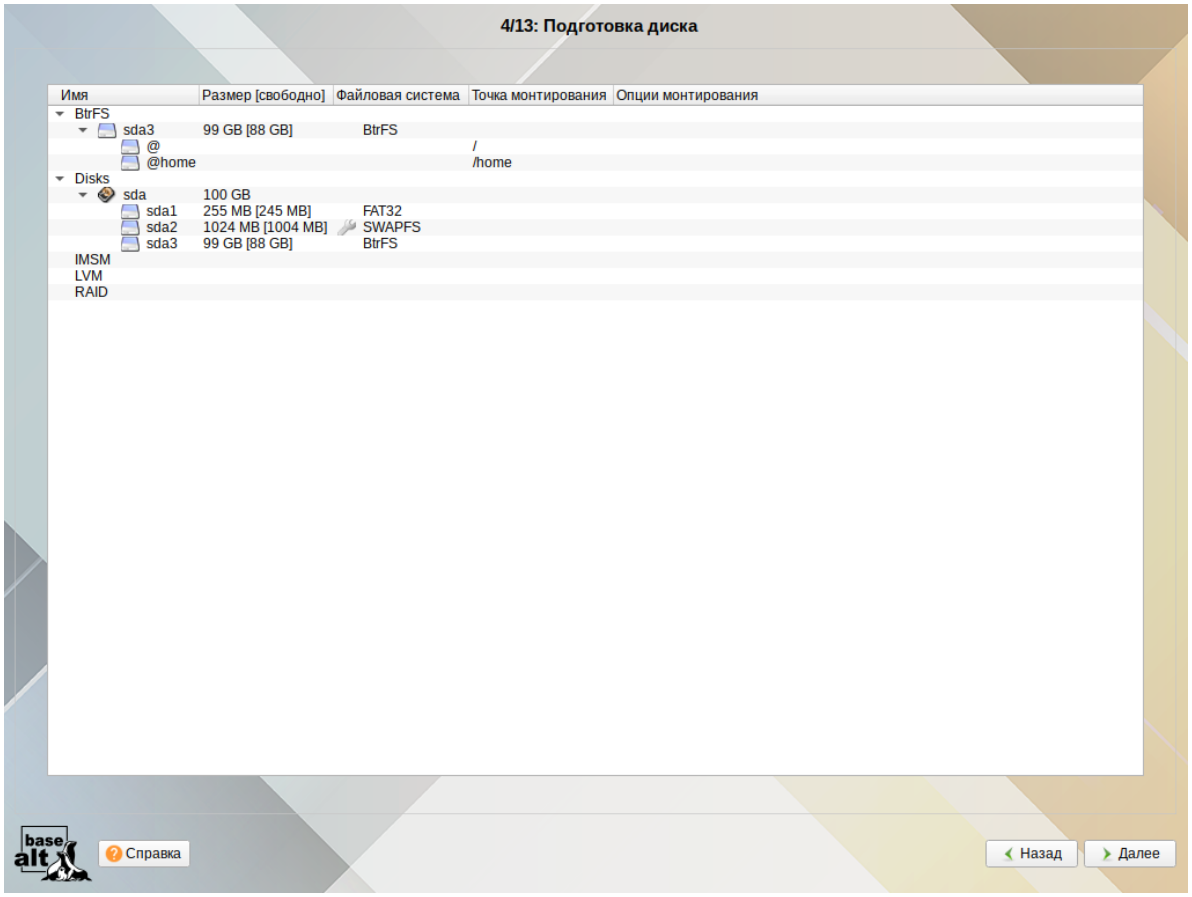

Рис. 202

Выбор режима BTRFS

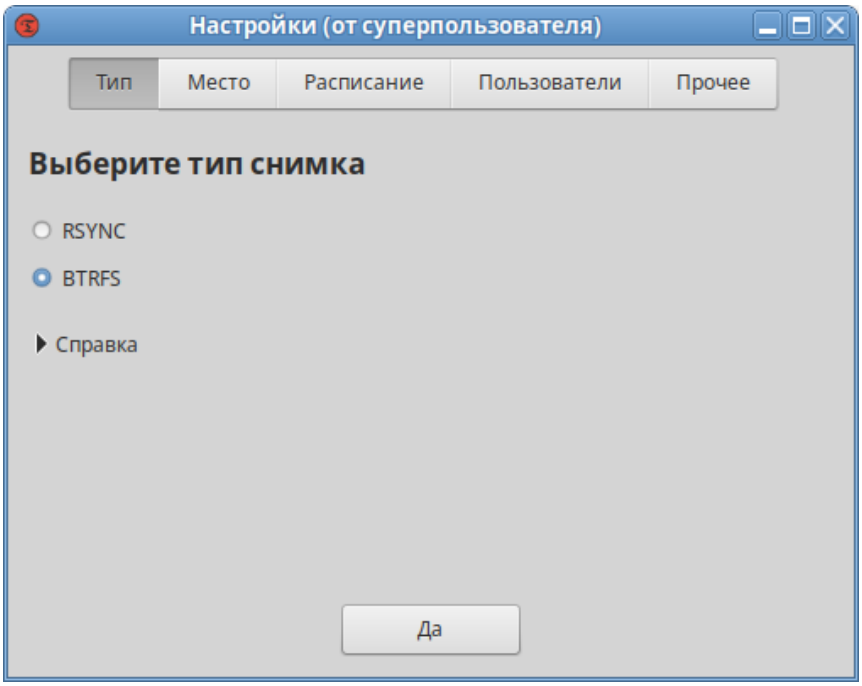

Рис. 203

Снимки BTRFS сохраняются в системном разделе, другие разделы не поддерживается (Рис. 204).

Выбор места хранения снимков BTRFS

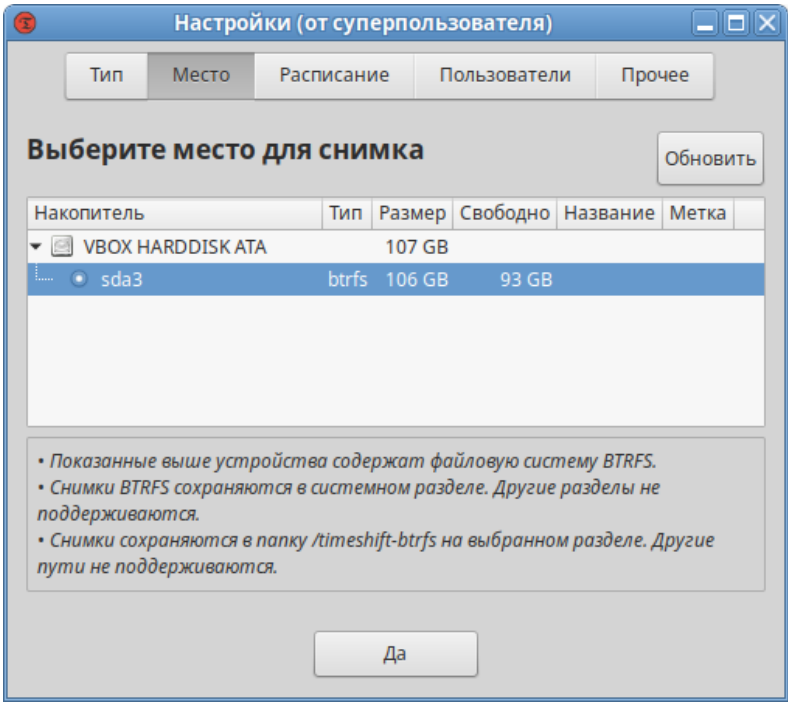

Рис. 204

На вкладке «Расписание» следует выбрать уровни создания снимков (ежемесячно, еженедельно, ежедневно, ежечасно, при загрузке) и указать количество сохраняемых снимков для каждого уровня (Рис. 205).

Расписание для снимков BTRFS

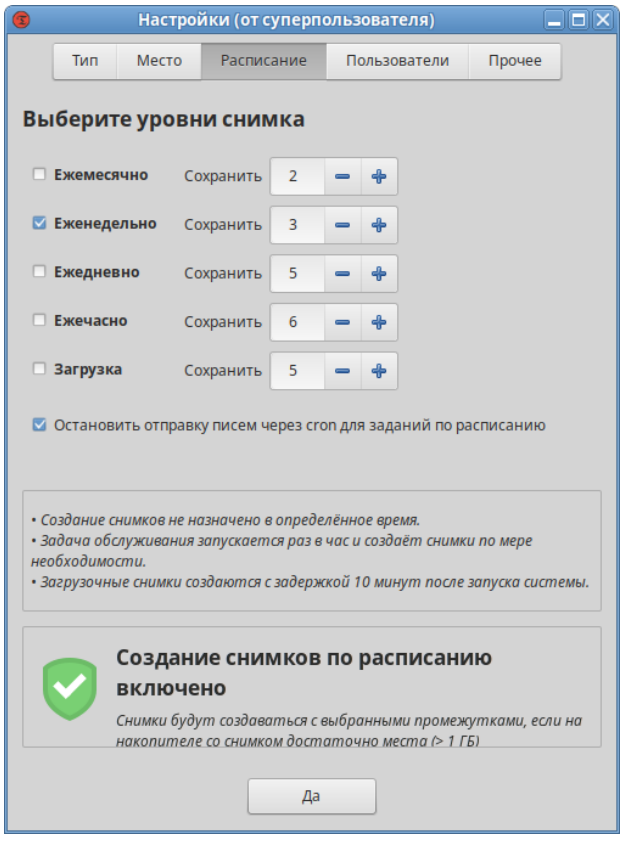

Рис. 205

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. 206).

Включить подраздел @home в создаваемые снимки

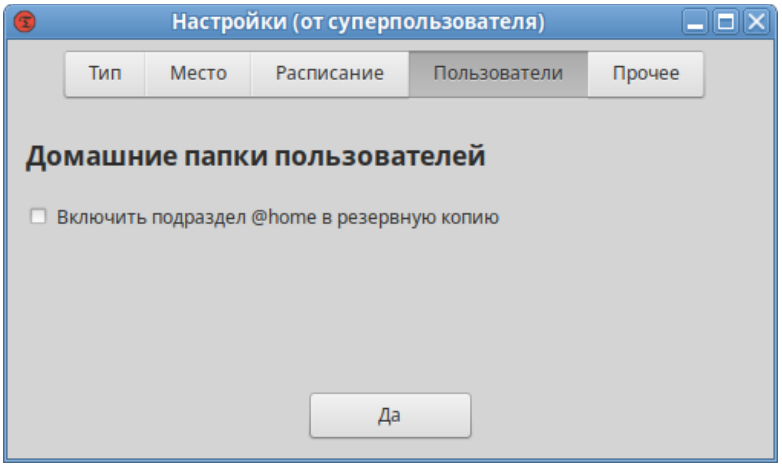

Рис. 206

На вкладке «Прочее» (Рис. 207) можно выбрать формат даты.

Timeshift. Вкладка «Прочее»

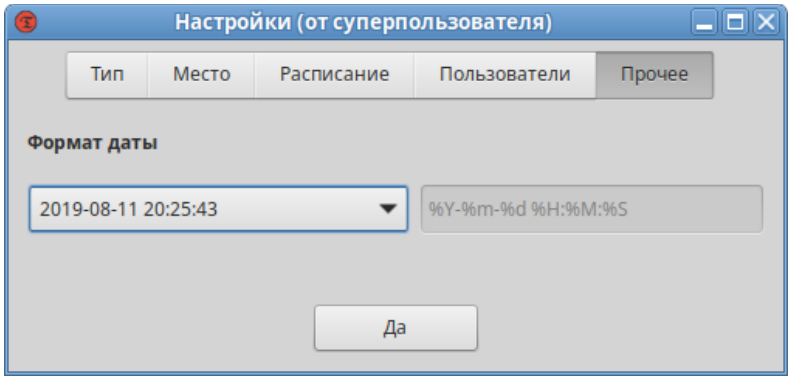

Рис. 207

6.5.2 Создание снимков

Снимки будут создаваться автоматически согласно настроенному расписанию.

Для создания снимка в ручном режиме следует нажать кнопку «Создать» на панели инструментов (Рис. 208). Резервная копия будет создана на устройстве хранения, который был указан в настройках.

Создание снимка в режиме RSYNC

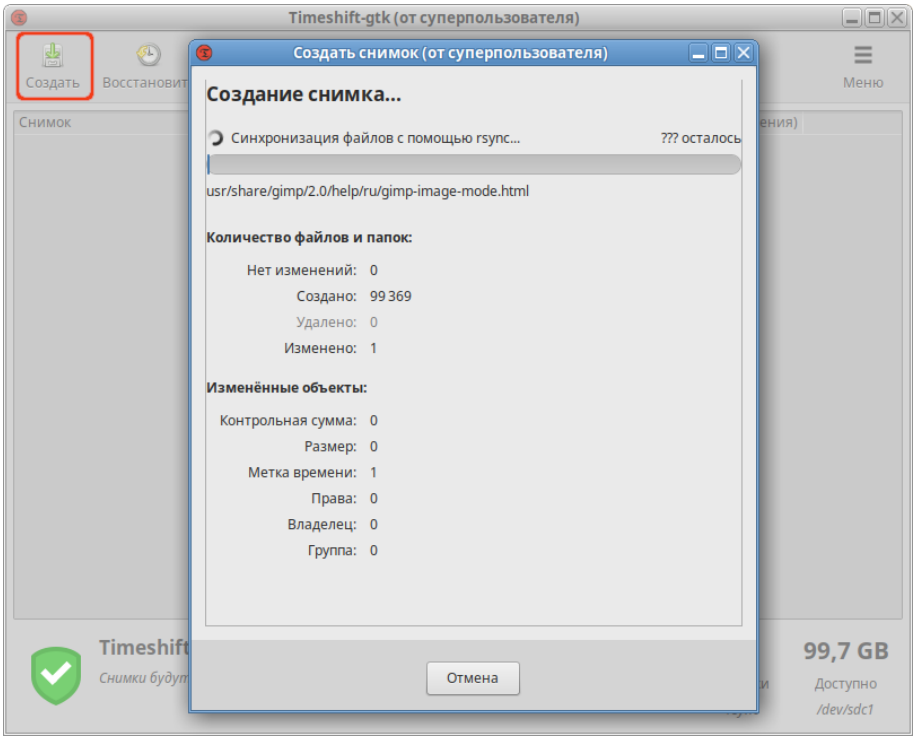

Рис. 208

6.5.3 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».

При восстановлении снимка в режиме RSYNC после нажатия кнопки «Восстановить» можно выбрать устройство, куда будут восстановлены файлы (***Рис. 209***), указать нужно ли переустанавливать GRUB (кнопка «Настройки загрузчика (дополнительные)»).

На следующем шаге (Рис. 210) будут показаны файлы, которые будут созданы/восстановлены/удалены в процессе восстановления снимка (только в режиме RSYNC).

Примечание. Если основная система не загружается, можно загрузиться с установочного диска в режиме LiveCD, запустить Timeshift, на вкладке «Место» указать расположение снимков и восстановить снимок в основной системе (Рис. 211) или загрузиться в режиме восстановления и развернуть снимок в командной строке (см. ниже).

Выбор целевого устройства

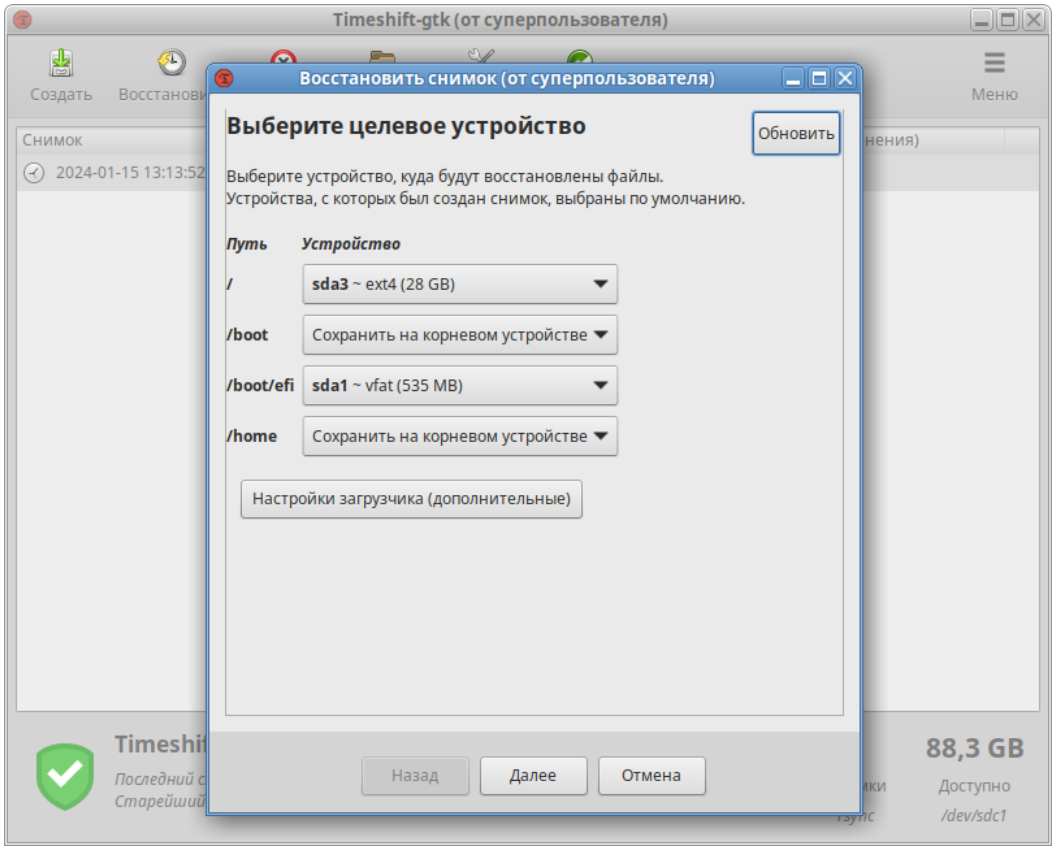

Рис. 209

Восстановление снимка в режиме RSYNC

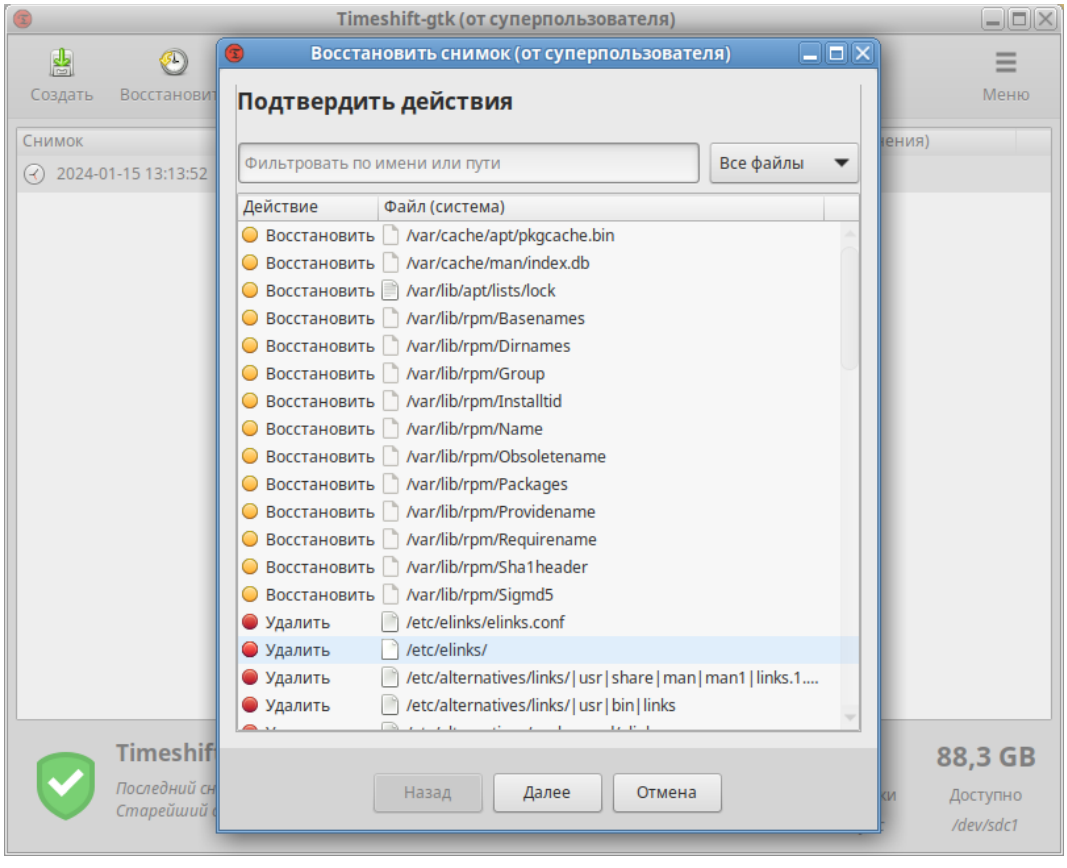

Рис. 210

Восстановление снимка в LiveCD

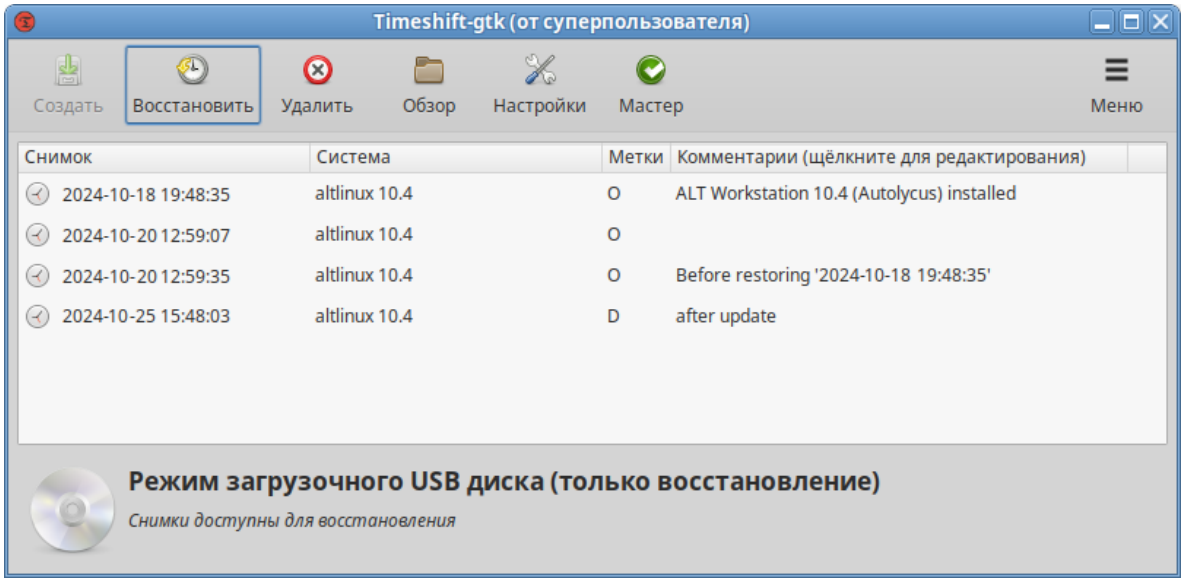

Рис. 211

6.5.4 Работа с Timeshift в командной строке

Примечание. Одновременно может работать только один экземпляр Timeshift, поэтому для работы с Timeshift из командной строки необходимо закрыть окно программы Timeshift.

Вывод справки о команде:

```
$ timeshift
```

Просмотр списка снимков:

```
# timeshift --list
Mounted '/dev/sda3' at '/run/timeshift/4020/backup'
btrfs: Quotas are not enabled
Device : /dev/sda3
UUID   : 545f72ee-6001-4476-85df-31b257000301
Path   : /run/timeshift/4020/backup
Mode   : BTRFS
Status : OK
3 snapshots, 93.0 GB free

Num     Name                 Tags  Description
------------------------------------------------------------------------------
0    >  2024-10-18_19-48-35  O     ALT Workstation 10.4 (Autolycus) installed
1    >  2024-10-20_12-59-07  O
2    >  2024-10-20_12-59-35  O     Before restoring '2024-10-18 19:48:35'
```

Пример создания снимка (в режиме RSYNC):

```
# timeshift --create --comments "after update" --tags D
Mounted '/dev/sdc1' at '/run/timeshift/4907/backup'
```

```
-------------------------------------------------------------------------
Estimating system size...
Creating new snapshot...(RSYNC)
Saving to device: /dev/sdc1, mounted at path: /run/timeshift/4907/backup
Linking from snapshot: 2024-10-20_13-13-52
Syncing files with rsync...
Created control file: /run/timeshift/4907/backup/timeshift/snapshots/2024-10-
20_15-53-25/info.json
RSYNC Snapshot saved successfully (26s)
Tagged snapshot '2024-10-20_15-53-25': ondemand
-------------------------------------------------------------------------
```

Пример создания (в режиме BTRFS):

```
# timeshift --create --comments "after update" --tags D
Using system disk as snapshot device for creating snapshots in BTRFS mode
Mounted '/dev/sda3' at '/run/timeshift/4060/backup'
btrfs: Quotas are not enabled
Creating new backup...(BTRFS)
Saving to device: /dev/sda3, mounted at path: /run/timeshift/4060/backup
Created directory: /run/timeshift/4060/backup/timeshift-btrfs/snapshots/2024-
10-20_15-48-03
Created subvolume snapshot:
/run/timeshift/4060/backup/timeshift-btrfs/snapshots/2024-10-20_15-48-03/@
Created control file:
/run/timeshift/4060/backup/timeshift-btrfs/snapshots/2024-10-20_15-48-03/
info.json
BTRFS Snapshot saved successfully (0s)
Tagged snapshot '2024-01-15_15-48-03': 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 '2024-10-20_15-48-03'
```

Восстановить определенный снимок в необходимый раздел:

```
# timeshift --restore --snapshot 1 --target /dev/sda2
```

Удалить снимок:

```
# timeshift --delete --snapshot '2024-10-20_15-48-03'
```

Если основная система не загружается, то необходимо 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 1 --target
/dev/sda2 --grub-device /dev/sda
```

4) перезагрузить систему.

6.6 Создание SSH-туннелей, использующих контроль целостности заголовков IP-пакетов в соответствии с ГОСТ Р 34.12-2015

6.6.1 Установка пакетов

Пакеты необходимо установить как на сервере, так и на клиенте.

Примечание. Должна быть включена Поддержка шифрования по ГОСТ в OpenSSL.

Примечание. Для установки пакетов gostcrypto, в список репозиториев должен быть добавлен репозиторий gostcrypto. Сделать это можно в программе управления пакетами Synaptic, дописав для дистрибутива «p10/branch/x86_64» в поле «Раздел(ы)» значение gostcrypto (Рис. 212). После изменения списка репозиториев, необходимо получить сведения о находящихся в них пакетах.

Добавление репозитория gostcrypto в Synaptic

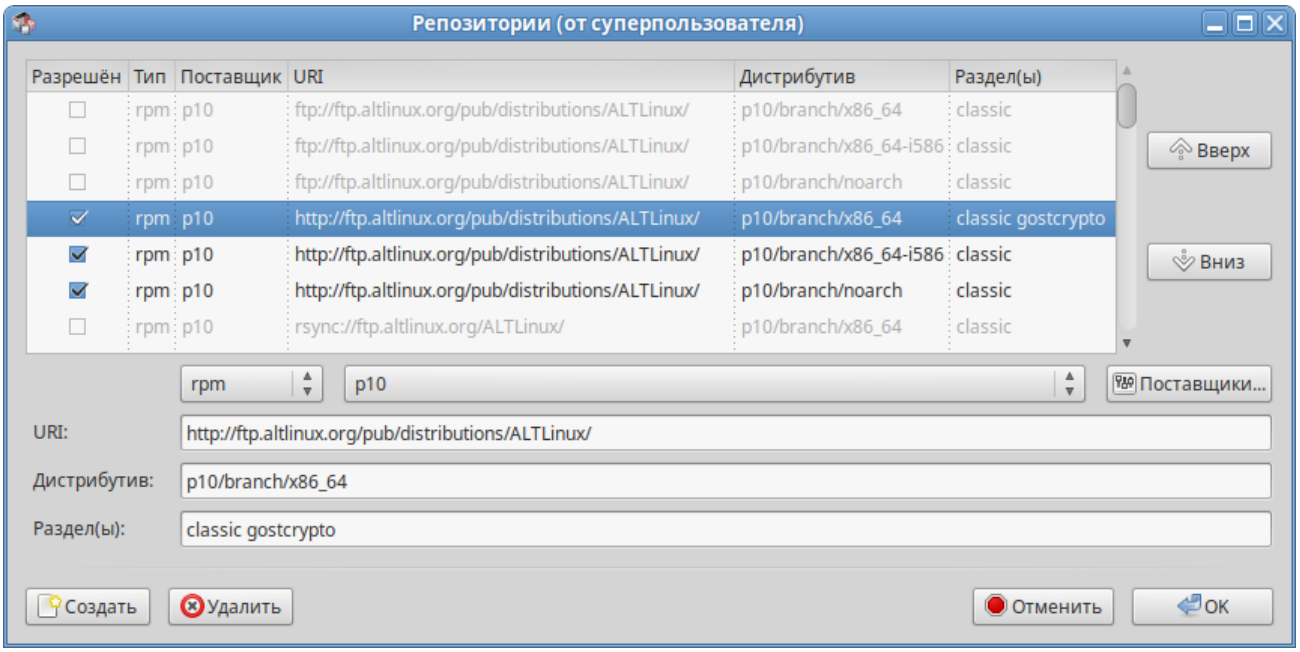

Рис. 212

Установить пакеты openssh-gostcrypto, openssh-clients-gostcrypto, openssh-server-gostcrypto, openssh-server-control-gostcrypto, openssh-common-gostcrypto, openssh-askpass-common-gostcrypto:

```
# apt-get install openssh-gostcrypto openssh-clients-gostcrypto
openssh-server-gostcrypto openssh-server-control-gostcrypto openssh-
common-gostcrypto openssh-askpass-common-gostcrypto
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие дополнительные пакеты будут установлены:
  openssl-gost-engine
Следующие пакеты будут УДАЛЕНЫ:
     openssh openssh-askpass-common openssh-clients openssh-common
openssh-server
  openssh-server-control
Следующие НОВЫЕ пакеты будут установлены:
  openssh-askpass-common-gostcrypto openssh-clients-gostcrypto
  openssh-common-gostcrypto openssh-gostcrypto
  openssh-server-control-gostcrypto openssh-server-gostcrypto
  openssl-gost-engine
ВНИМАНИЕ: Будут удалены важные для работы системы пакеты
Обычно этого делать не следует. Вы должны точно понимать возможные
последствия!
  openssh-server openssh-server-control (по причине openssh-server)
0 будет обновлено, 7 новых установлено, 6 пакетов будет удалено и 34
не будет обновлено.
Необходимо получить 1409kB архивов.
После распаковки потребуется дополнительно 421kB дискового
пространства.
Вы делаете нечто потенциально опасное!
Введите фразу 'Yes, do as I say!' чтобы продолжить.
 Yes, do as I say!
```

Примечание. При выполнении этой команды будет выведено предупреждение «*Введите фразу 'Yes, do as I say!' чтобы продолжить»* вместо обычного «*Y/n»*. Это происходит, потому что к замене предлагаются критически важные с точки зрения APT пакеты. Если вы согласны с данной заменой, необходимо ввести фразу «*Yes, do as I say!*» и нажать <Enter>.

Список поддерживаемых алгоритмов шифрования трафика можно посмотреть с помощью

команды:

```
$ ssh -Q cipher
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
rijndael-cbc@lysator.liu.se
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
grasshopper-cbc@altlinux.org
grasshopper-ctr@altlinux.org
magma-cbc@altlinux.org
magma-ctr@altlinux.org
```

Список поддерживаемых MAC (коды аутентификации сообщений):

```
$ ssh -Q mac
hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-512
hmac-md5
hmac-md5-96
umac-64@openssh.com
umac-128@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com
grasshopper-mac@altlinux.org
```

```
hmac-gostr3411-2012-256@altlinux.org
hmac-streebog-256@altlinux.org
hmac-gostr3411-2012-512@altlinux.org
hmac-streebog-512@altlinux.org
hmac-gostr3411-2012-256-etm@altlinux.org
hmac-streebog-256-etm@altlinux.org
hmac-gostr3411-2012-512-etm@altlinux.org
hmac-streebog-512-etm@altlinux.org
```

6.6.2 Настройка сервера SSH

Настройки сервера SSH находятся в файле `/etc/openssh/sshd_config`.

Добавить в файл `/etc/openssh/sshd_config` строки:

```
Ciphers grasshopper-ctr@altlinux.org
MACs grasshopper-mac@altlinux.org,hmac-streebog-512@altlinux.org
```

Перезапустить службу sshd:

```
# systemctl restart sshd
```

6.6.3 Подключение к серверу SSH

Команда подключения к серверу с использованием алгоритмов ГОСТ Р 34.12-2015:

```
$ ssh <пользователь>@<сервер> -oCiphers=grasshopper-ctr@altlinux.org -
oMACs=grasshopper-mac@altlinux.org,hmac-streebog-512@altlinux.org
```

Пробросить порт с сервера на локальную машину (для демонстрации туннеля):

```
$ ssh <пользователь>@<сервер> -oCiphers=grasshopper-ctr@altlinux.org -
oMACs=grasshopper-mac@altlinux.org,hmac-streebog-512@altlinux.org    -L
127.0.0.1:222:127.0.0.1:22
```

Зайти на всё тот же сервер через туннель (в другом окне терминала):

```
$    ssh    <пользователь>@127.0.0.1    -p    222    -oCiphers=grasshopper-
ctr@altlinux.org     -oMACs=grasshopper-mac@altlinux.org,hmac-streebog-
512@altlinux.org
```

Для того чтобы не указывать алгоритм шифрования и коды аутентификации в команде подключения, можно указать эти параметры в конфигурации клиента SSH. Настройки клиентской части SSH делятся на глобальные и пользовательские. Глобальные клиентские настройки находятся в файле `/etc/openssh/ssh_config` и применяются ко всем пользователям. Пользовательские настройки находятся в файле `~/.ssh/config` (в домашнем каталоге пользователя) и применяются к одному пользователю.

Например, можно добавить в конец файла `/etc/openssh/ssh_config` строки:

```
Ciphers grasshopper-ctr@altlinux.org
MACs grasshopper-mac@altlinux.org,hmac-streebog-512@altlinux.org
```

Теперь подключиться к серверу, выполнив команду:

```
$ ssh <пользователь>@<сервер>
```

Примечание. Порядок применения пользовательских настроек SSH: высший приоритет имеют ключи командной строки, затем следуют настройки пользователя, а после них используются глобальные настройки клиентской части.

Если при выполнении подключения использовать опцию `-v` для вывода отладочной информации, то используемый для подключения метод защитного преобразования будет отображен в выводе:

```
$ ssh -v <пользователь>@<сервер>
...
debug1: kex: server->client cipher: grasshopper-ctr@altlinux.org MAC:
grasshopper-mac@altlinux.org compression: none
debug1: kex: client->server cipher: grasshopper-ctr@altlinux.org MAC:
grasshopper-mac@altlinux.org compression: none
...
```

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

Для возможности использования ГОСТ алгоритмов шифрования и хеширования должна быть включена «Поддержка шифрования по ГОСТ в OpenSSL».

Установить пакет `openvpn-gostcrypto`:

```
# apt-get install openvpn-gostcrypto
```

Примечание. Для установки пакетов gostcrypto, в список репозиториев должен быть добавлен репозиторий gostcrypto. Сделать это можно в программе управления пакетами Synaptic, дописав для дистрибутива «p10/branch/x86_64» в поле «Раздел(ы)» значение gostcrypto (Рис. 212). После изменения списка репозиториев, необходимо получить сведения о находящихся в них пакетах.

6.7.1 Настройка в ЦУС

Выполнить настройку сервера OpenVPN-сервера (см. «Соединение удалённых офисов (OpenVPN-сервер)»).

Выбрать алгоритмы шифрования и алгоритм хеширования. По умолчанию OpenVPN автоматически подбирает алгоритм шифрования, не учитывая алгоритм, заданный в поле «Алгоритм шифрования», поэтому необходимо отметить пункт «Отключить согласование алгоритмов шифрования (NCP)» (Рис. 213).

На стороне клиента, необходимо указать алгоритмы шифрования, такие же, как и на стороне сервера (Рис. 214).

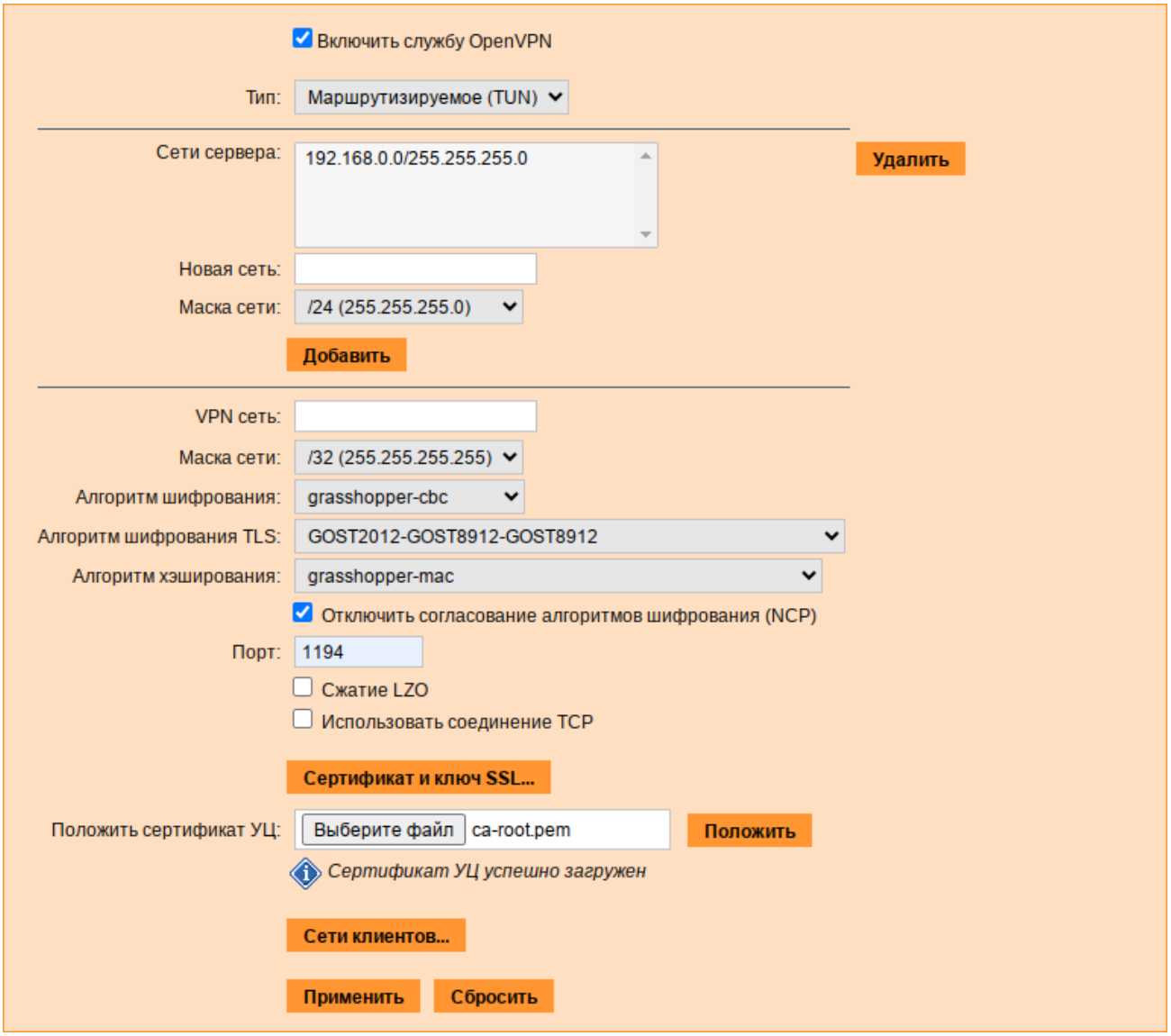

Рис. 213

Проверка подключения на стороне сервера:

```
# journalctl -f| grep openvpn
дек 07 20:57:08 dc1.test.alt openvpn[254812]: 192.168.0.145:55939 TLS: Initial packet from [AF_INET]192.168.0.45:55939, sid=d1366cce 4584a510
дек 07 20:57:08 dc1.test.alt openvpn[262676]: TLS: Initial packet from [AF_INET]192.168.0.145:1194, sid=393e755a d49a39a8
дек 07 20:57:08 dc1.test.alt openvpn[262676]: VERIFY OK: depth=1, C=RU, O=Test, OU=Test Certification Authority, CN=Test Root Certification Authority
```

```
...
дек 07 20:57:08 dc1.test.alt openvpn[254812]: 192.168.0.145:55939 Outgoing Data Chan-
nel: Using 128 bit message hash 'grasshopper-mac' for MAC authentication
дек 07 20:57:08 dc1.test.alt openvpn[254812]: 192.168.0.145:55939 Incoming Data Chan-
nel: Cipher 'grasshopper-cbc' initialized with 256 bit key
дек 07 20:57:08 dc1.test.alt openvpn[254812]: 192.168.0.145:55939 Incoming Data Chan-
nel: Using 128 bit message hash 'grasshopper-mac' for MAC authentication
```

Создание нового OpenVPN-соединения

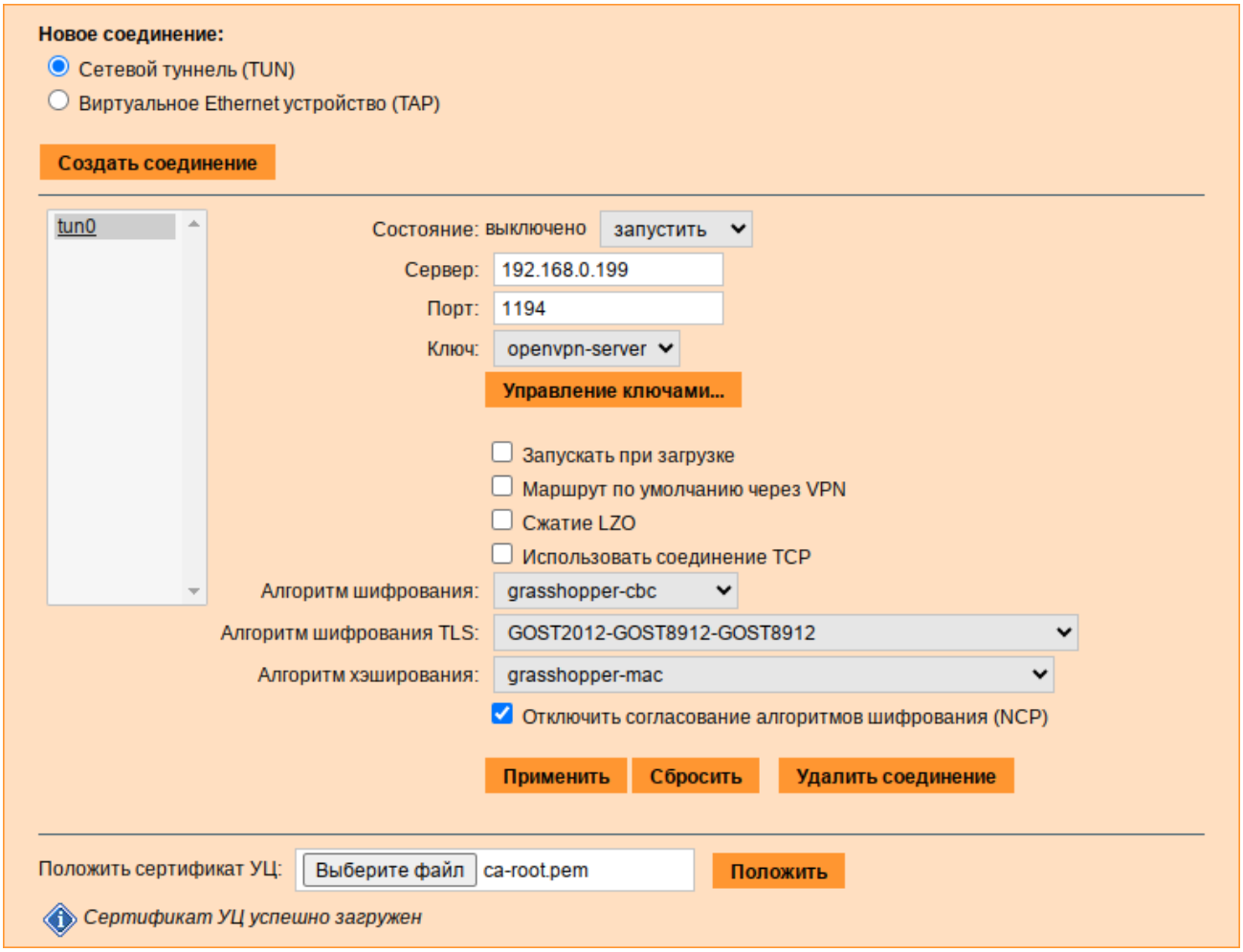

Рис. 214

6.7.2 Настройка в командной строке

6.7.2.1 Создание ключей для OpenVPN-туннеля средствами утилиты openssl

Для генерации всех необходимых ключей и сертификатов необходимо выполнить следующие действия:

1. Для возможности подписывать любые сертификаты, необходимо открыть файл `/var/lib/ssl/openssl.cnf` и изменить значение параметра policy на следующее:

   ```
   policy = policy_anything
   ```

2. Создать каталоги:

```
# mkdir -p /root/CA/demoCA
# cd /root/CA
# mkdir -p ./demoCA/newcerts
```

Создать файл базы с действующими и отозванными сертификатами:

```
# touch ./demoCA/index.txt
```

Создать файл индекса для базы ключей и сертификатов:

```
# echo '01' > ./demoCA/serial
```

Создать файл индекса для базы отозванных сертификатов:

```
# echo '01' > ./demoCA/crlnumber
```

3. 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
```

Ввести пароль для закрытого ключа и ответить на запросы о владельце ключа.

4. Создать пару «ключ-сертификат» для сервера и каждого клиента, желающего подключиться к серверу. Для этого, сгенерировать ключ и запрос на сертификат для сервера:

```
# openssl req -new -nodes -keyout server.pem -out server.crs
```

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
```

Сгенерировать запрос на сертификат для пользователя:

```
# openssl req -new -nodes -keyout client.pem -out client.crs
```

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 client.crs -out client.crt
```

5. Задать параметры Диффи-Хеллмана для сервера:

```
# openssl dhparam -out server.dh 2048
```

6. Разместить ключи и сертификаты в каталогах сервера и клиента следующим образом:

- 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.

7. Для новых клиентов создать новые ключи и отдать комплектом `my-ca.crt`, `новый_сертификат.crt`, `новый_ключ.pem`.

Для создания списка отзыва сертификатов необходимо выполнить следующие действия:

1. Выполнить следующую команду:
   ```
   # openssl ca -cert my-ca.crt -keyfile my-ca.pem -gencrl -out crl.pem
   ```
2. Отозвать сертификат `user_1.crt`:
   ```
   # openssl ca -cert my-ca.crt -keyfile my-ca.pem -revoke user_1.crt -out crl.pem
   ```
3. Обновить список (обязательно после каждого отзыва сертификата):
   ```
   # openssl ca -cert my-ca.crt -keyfile my-ca.pem -gencrl -out crl.pem
   ```
4. Просмотреть `crl.pem`:
   ```
   # openssl crl -noout -text -in crl.pem
   ```
5. Поместить файл `crl.pem` в каталог `/var/lib/openvpn`.

6.7.2.2 Настройка сервера OpenVPN

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/`.

Ранее созданные ключи и сертификаты необходимо перенести в каталог `/etc/openvpn/keys/`.

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/*
```

Каждый файл конфигурации по маске `/etc/openvpn/*.conf` является конфигурацией отдельного экземпляра демона openvpn.

Примечание. Для настройки OpenVPN-сервера можно использовать образец файла конфигурации OpenVPN, для этого следует скопировать файл `/usr/share/doc/openvpn-gostcrypto-2.4.9/server.conf` в каталог `/etc/openvpn/` (номер версии в названии каталога может быть другим).

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`;
- ncp-disable – для возможности использования шифра отличного от AES-256-GCM

Далее приводится пример конфигурации в файле `server.conf`:

```
# cat /etc/openvpn/server.conf
port 1194
proto udp
dev tun
ca   /etc/openvpn/keys/my-ca.crt
cert /etc/openvpn/keys/server.crt
key  /etc/openvpn/keys/server.pem
dh /etc/openvpn/keys/server.dh
comp-lzo
server 10.8.0.0 255.255.255.0
tls-server
cipher grasshopper-cbc
tls-cipher GOST2012-GOST8912-GOST8912
ncp-disable
verb 3
mute 10
keepalive 10 60
user openvpn
group openvpn
persist-key
persist-tun
status openvpn-status.log
ifconfig-pool-persist server_ipp.txt
verb 3
client-to-client
management localhost 1194
push "route 192.168.0.0 255.255.255.0"
push "dhcp-option DNS 192.168.0.122"
;client-config-dir /etc/openvpn/ccd
```

Ключи и сертификаты необходимо перенести в каталог `/etc/openvpn/keys/`.

Запустить сервер OpenVPN:

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

6.7.2.3 Настройка VPN-подключения по протоколу OpenVPN в Network Manager

Для настройки VPN-подключения по протоколу OpenVPN в Network Manager, следует выполнить следующие действия:

1. Нажать левой кнопкой мыши на значок NetworkManager, в меню выбрать «Подключения VPN» → «Добавить подключение VPN…» (*Рис. 215*).

Создание нового OpenVPN-соединения

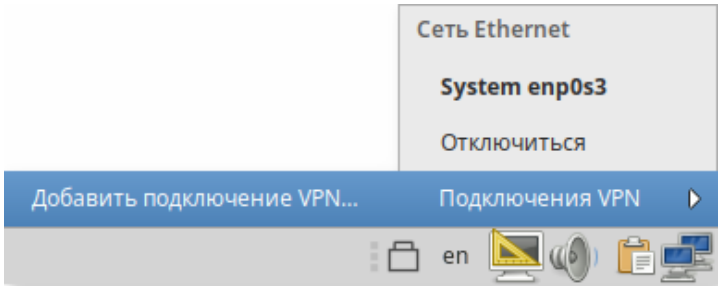

Рис. 215

2. В списке выбора типа подключения выбрать пункт «OpenVPN» (Рис. 216) и нажать кнопку «Создать».

Примечание. Если имеется файл конфигурации клиента, в списке выбора типа соединения можно выбрать пункт «Импортировать сохраненную конфигурацию VPN…» и указать этот файл, параметры соединения будут настроены согласно этому файлу.

Выбор типа VPN-соединения

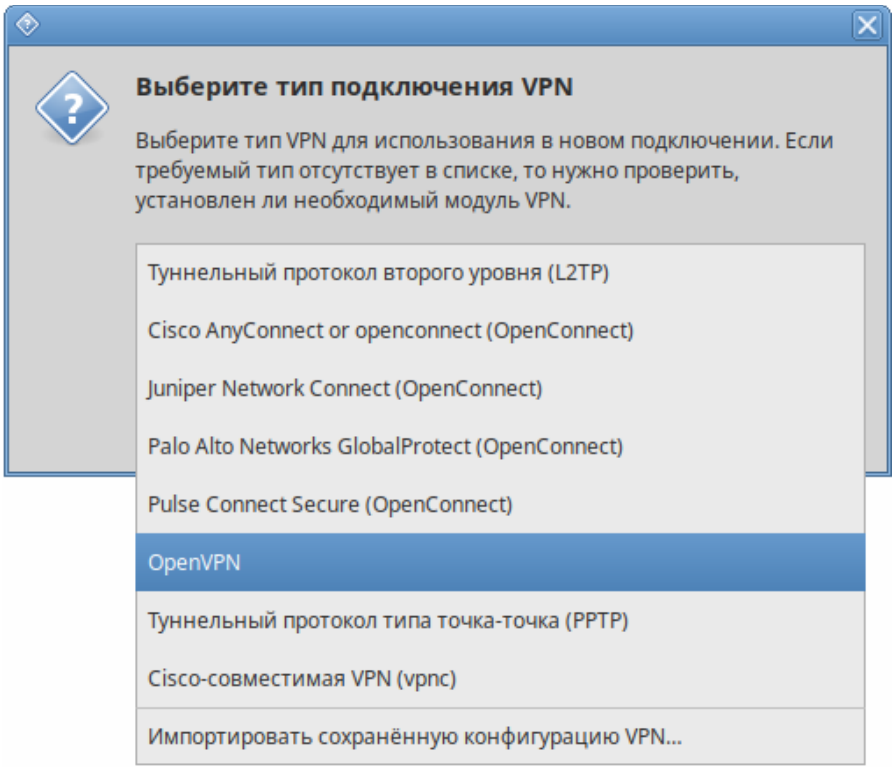

Рис. 216

3. В открывшемся окне указать IP-адрес OpenVPN-сервера, сертификат УЦ, приватный ключ и сертификат пользователя (*Рис. 217*).
4. Нажать кнопку «Дополнительно» чтобы указать параметры подключения. Настройки соединения находятся на разных вкладках, например, на вкладке «Защита» можно указать алгоритм шифрования (*Рис. 218*).

Параметры VPN-соединения

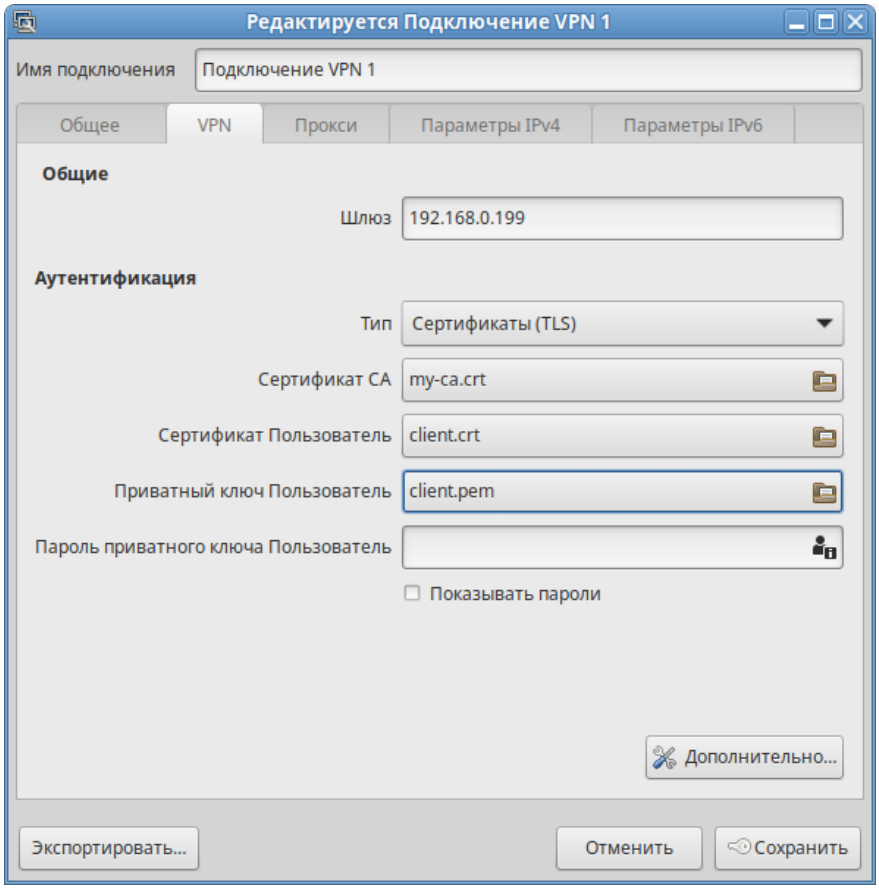

Рис. 217

Дополнительные параметры OpenVPN

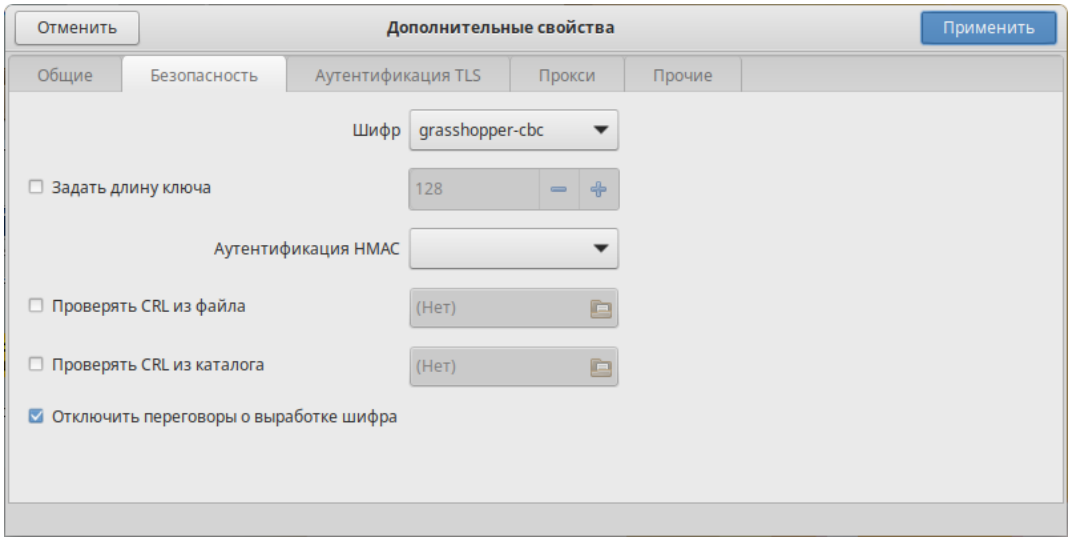

Рис. 218

5. Сохранить сделанные изменения, нажав кнопку «ОК» и затем «Сохранить».
6. Выполнить подключение (*Рис. 219*).

Создание VPN-соединения

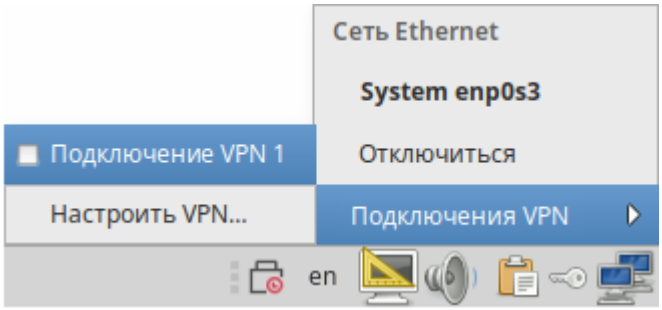

Рис. 219

Выполнить настройку OpenVPN-клиента можно также в командной строке. Для этого:

- скопировать файл `/usr/share/doc/openvpn-gostcrypto-2.4.9/client.conf` в каталог `/etc/openvpn/`;
- скопировать ранее сгенерированные ключи и сертификаты в каталог `/etc/openvpn/keys/` и укажите их в `/etc/openvpn/client.conf`;
- в файле `/etc/openvpn/client.conf` в поле `remote` указать IP-адрес OpenVPN-сервера, другие параметры привести в соответствие с настройками сервера, например:

```
remote 192.168.0.102 1194
ca   /etc/openvpn/keys/my-ca.crt
cert /etc/openvpn/keys/client.crt
key  /etc/openvpn/keys/client.pem
#remote-cert-tls server
cipher grasshopper-cbc
tls-cipher GOST2012-GOST8912-GOST8912
```

- запустить клиент OpenVPN:

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

6.8 Поддержка файловых систем

Файловая система представляет собой набор правил, определяющих то, как хранятся и извлекаются документы, хранящиеся на устройстве.

В ОС «Альт Рабочая станция» поддерживаются следующие файловые системы:

- ext2 – нежурналируемая файловая система; относительно проста в восстановлении, но нуждается в относительно долгой проверке целостности после сбоя питания или ядра. Может использоваться для /boot или readonly-разделов;
- ext3 – журналируемая и достаточно надёжная файловая система, имеет среднюю производительность;

- ext4 – журналируемая файловая система, логическое продолжение ext3, позволяет полностью отключить журналирование;
- btrfs – поддерживает снимки (копии файловой системы на определенный момент времени), сжатие и подтома;
- iso9660 – файловая система ISO 9660 для дисков с данными компакт-дисков.

Файловые системы FAT/FAT32/NTFS поддерживаются в установленной системе, но не для установки на них Linux.

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 каталог `/mnt/filesystem`, в который 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
     # 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 системы:

  ```
  # 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/
   ```

Примечание. Для просмотра файловых систем на физических дисках можно воспользоваться командой `df`:

```
$ df -Th | grep "^/dev"
```

или `lsblk`:

```
$ lsblk -f
```

Команда `fsck` позволяет узнать файловую систему раздела, который ещё не примонтирован:

```
# fsck -N /dev/sdc1
fsck из util-linux 2.39.2
[/sbin/fsck.xfs (1) -- /dev/sdc1] fsck.xfs /dev/sdc1
```

6.9 Поддержка сетевых протоколов

6.9.1 SMB

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

6.9.1.1 Настройка Samba

Samba настраивается с помощью конфигурационного файла `/etc/samba/smb.conf`.

Примечание. После редактирования файла `smb.conf`, следует запускать команду `testparm` для проверки файла на синтаксические ошибки.

6.9.1.1.1 Добавление пользователя

Создать пользователя samba в системе и указать пароль:

```
# useradd -m user_samba
# passwd user_samba
```

Добавить пользователя в файл `smbpasswd` с тем же паролем:

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

6.9.1.1.2 Создание ресурсов общего доступа

Создать папку `sharefolder`, для общих ресурсов:

```
# mkdir /mnt/sharefolder
```

Назначить нового владельца:

```
# chown -R user_samba:users /mnt/sharefolder
# chmod -R ugo+rwx /mnt/sharefolder
```

Добавить в конфигурационный файл сервера Samba `/etc/samba/smb.conf` строки:

```
[public]
        #путь к общей папке
        path=/mnt/sharefolder
        read only=No
        #открыть гостевой доступ
        guest ok=Yes
        comment = Public
```

Перезапустить службу:

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

6.9.1.1.3 Создание ресурсов общего доступа от имени обычного пользователя

Создание ресурсов общего доступа от имени обычного пользователя рассмотрено в разделе «Создание ресурсов общего доступа».

6.9.1.2 Настройка клиента

6.9.1.2.1 Подключение по протоколу SMB в графической среде

Для создания подключения по протоколу SMB в графической среде MATE можно, запустить файловый менеджер, указать в адресной строке протокол и адрес сервера (Рис. 220). Нажать клавишу <Enter>. Будут показаны ресурсы с общим доступом (Рис. 221). Для доступа к папке, необходимо указать имя пользователя, пароль и нажать кнопку «Подключиться» (Рис. 222).

Создание подключения по протоколу SMB

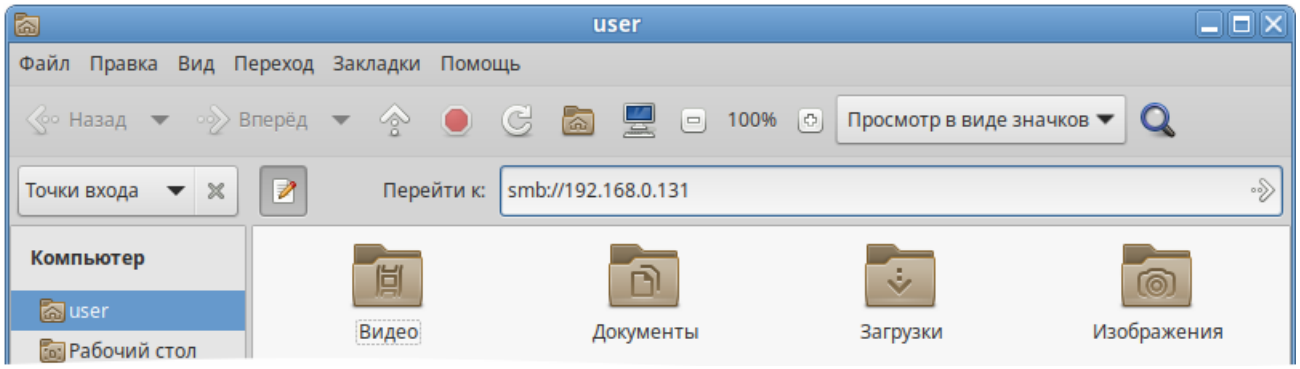

Рис. 220

Создание подключения по протоколу SMB

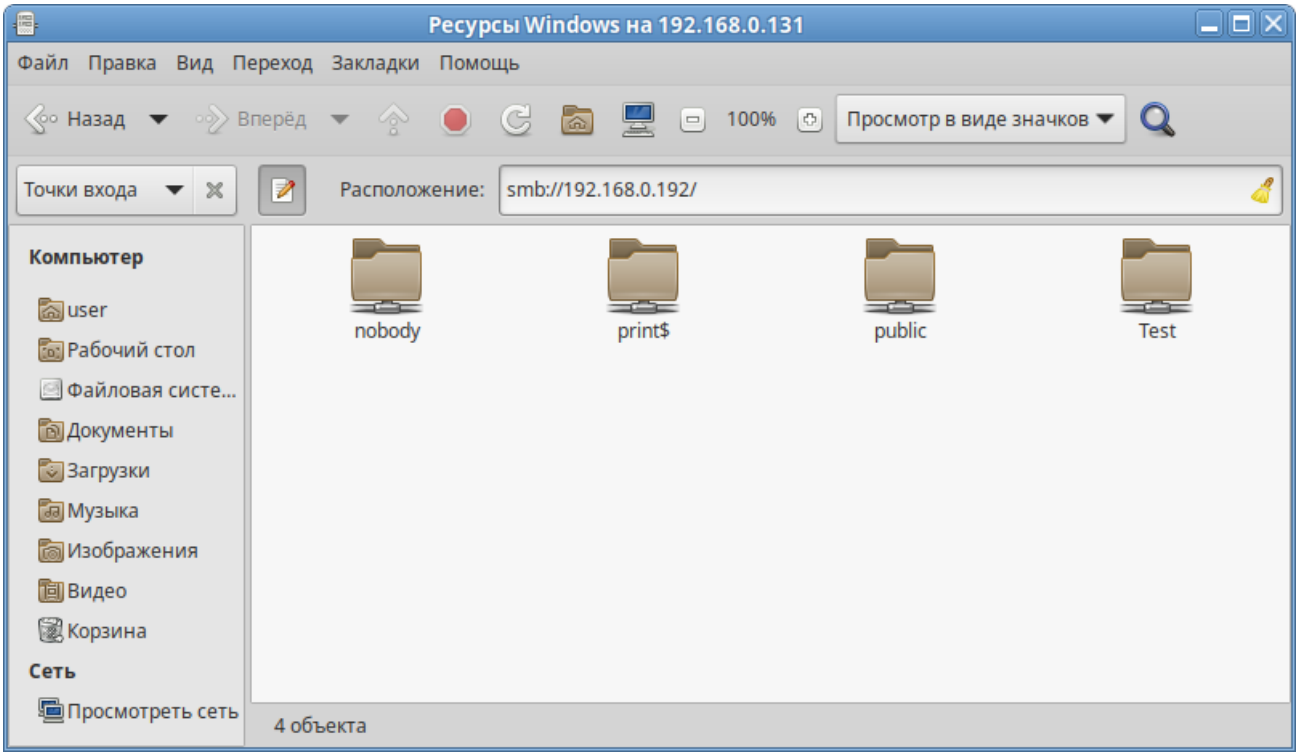

Рис. 221

Создание подключения по протоколу SMB

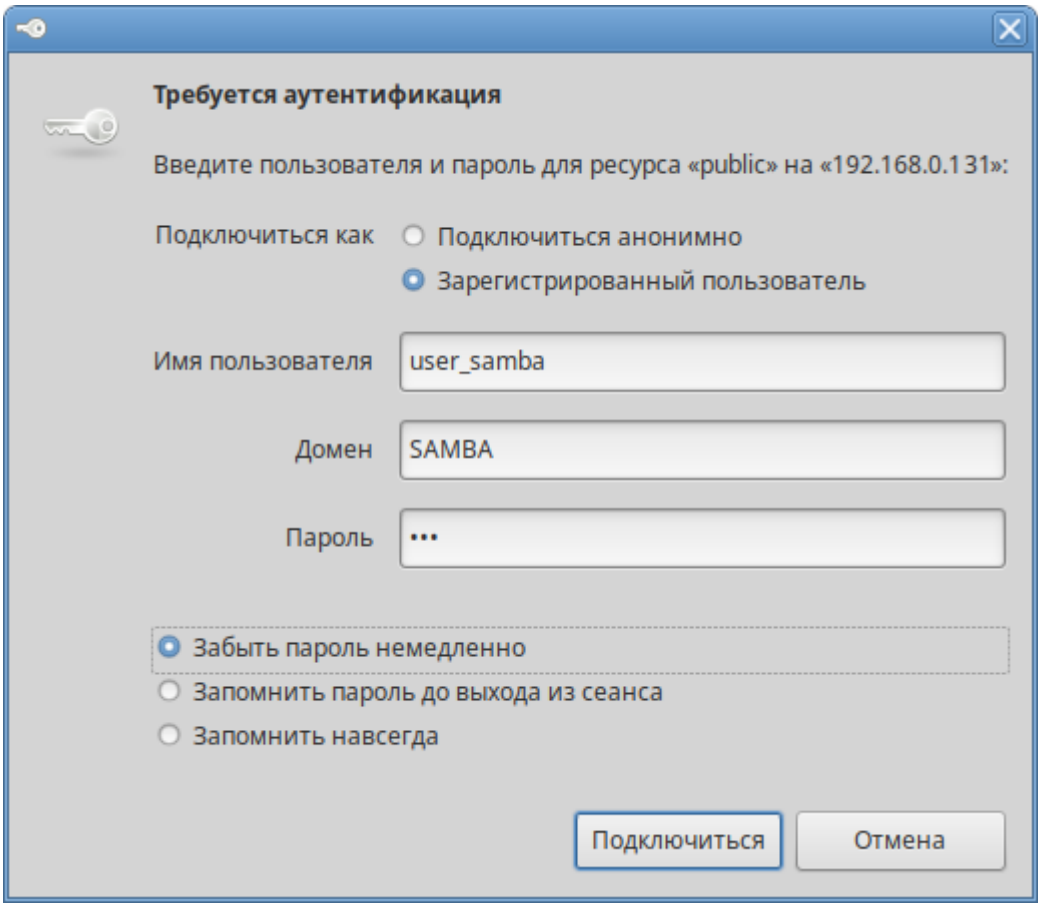

Рис. 222

6.9.1.2.2 Монтирование ресурса Samba через /etc/fstab

Просмотреть список общедоступных ресурсов на сервере:

```
$ smbclient -L 192.168.0.131 -U%
```

Просмотреть список ресурсов на сервере доступных пользователю user_samba:

```
$ smbclient -L 192.168.0.131 -Uuser_samba
Enter SAMBA\user_samba's password:

   Sharename       Type      Comment
   ---------       ----      -------
   print$          Disk      Printer Drivers
   public          Disk      Public
   IPC$            IPC       IPC Service (Samba 4.19.7-alt4)
   Test            Disk
   user_samba      Disk      Home Directories
SMB1 disabled -- no workgroup available
```

Создать файл `/etc/samba/sambacreds` (например, командой `mcedit /etc/samba/sambacreds`), с содержимым:

```
username=имя_пользователя
password=пароль
```

Для защиты информации, права на файл `/etc/samba/sambacreds`, надо установить так, чтобы файл был доступен на чтение и запись только пользователю-владелецу файла:

```
# chmod 600 /etc/samba/sambacreds
```

и принадлежать root:

```
# chown root: /etc/samba/sambacreds
```

Для монтирования ресурса Samba в `/etc/fstab` необходимо прописать, строку вида:

```
//СЕРВЕР/ИМЯ_РЕСУРСА            /mnt/точка_монтирования            cifs
credentials=/путь/к/полномочиям/sambacreds 0 0
```

Например:

```
//192.168.0.131/public   /mnt/server_public   cifs   users,_netdev,x-
systemd.automount,credentials=/etc/samba/sambacreds 0 0
```

6.9.2 NFS

6.9.2.1 Настройка сервера NFS

Примечание. Должен быть установлен пакет `nfs-server` (пакет `nfs-server` не входит в состав ISO-образа дистрибутива, его можно установить из репозитория p10):

```
# apt-get install nfs-server
```

Запустить NFS-сервер и включить его по умолчанию:

```
# systemctl enable --now nfs
```

В файле /etc/exports следует указать экспортируемые каталоги (каталоги, которые будет разрешено монтировать с других машин):

```
/mysharedir ipaddr1(rw)
```

Например, чтобы разрешить монтировать /home на сервере необходимо добавить в /etc/exports строку:

```
/home 192.168.0.0/24(no_subtree_check,rw)
```

где 192.168.0.0/24 – разрешение экспорта для подсети 192.168.0.X; rw – разрешены чтение и запись.

Подробную информацию о формате файла можно посмотреть командой:

```
man exports
```

После внесения изменений в файл /etc/exports необходимо выполнить команду:

```
# exportfs -r
```

Проверить список экспортируемых файловых систем можно, выполнив команду:

```
# exportfs
/home 192.168.0.0/24
```

6.9.2.2 Использование NFS

Подключение к NFS-серверу можно производить как вручную, так и настроив автоматическое подключение при загрузке.

Для ручного монтирования необходимо:

- создать точку монтирования:

```
# mkdir /mnt/nfs
```

- примонтировать файловую систему:

```
# mount -t nfs 192.168.0.131:/home /mnt/nfs
```

где 192.168.0.131 – IP адрес сервера NFS; /mnt/nfs – локальный каталог, куда монтируется удалённый каталог;

- проверить наличие файлов в каталоге /mnt/nfs:

```
# ls –al /mnt/nfs
```

Должен отобразиться список файлов каталога /home расположенного на сервере NFS.

Для автоматического монтирования к NFS-серверу при загрузке необходимо добавить следующую строку в файл /etc/fstab:

```
192.168.0.131:/home    /mnt/nfs      nfs      intr,soft,nolock,_netdev,x-systemd.automount    0 0
```

Примечание. Прежде чем изменять /etc/fstab, необходимо смонтировать каталог вручную, для того чтобы убедиться, что все работает.

6.9.3 FTP

6.9.3.1 Настройка сервера FTP

Установить пакеты `vsftpd`, `anonftp` (пакеты `vsftpd` и `anonftp` не входят в состав ISO-образа дистрибутива, их можно установить из репозитория p10):

```
# apt-get install vsftpd anonftp
```

Изменить настройку прав доступа в файле `/etc/vsftpd.conf`:

```
local_enable=YES
chroot_local_user=YES
local_root=/var/ftp/
```

Перезапустить vsftpd.socket:

```
# systemctl restart vsftpd.socket
```

Убедиться в нормальной работе FTP-сервера:

```
# netstat -ant | grep 21
tcp        0      0 :::21                   :::*                    LISTEN
```

FTP-сервер запущен и принимает соединения на 21 порту.

Создать файл в каталоге /var/ftp/:

```
# echo "vsftpd test file" > /var/ftp/test.txt
```

6.9.3.2 Подключение рабочей станции

Создать подключение по протоколу FTP в графической среде MATE можно в файловом менеджере. Для этого следует указать в адресной строке протокол и адрес сервера (Рис. 223) и нажать клавишу <Enter>. В появившемся окне указать имя пользователя, пароль и нажать кнопку «Подключиться» (Рис. 224).

Создание подключения по протоколу FTP

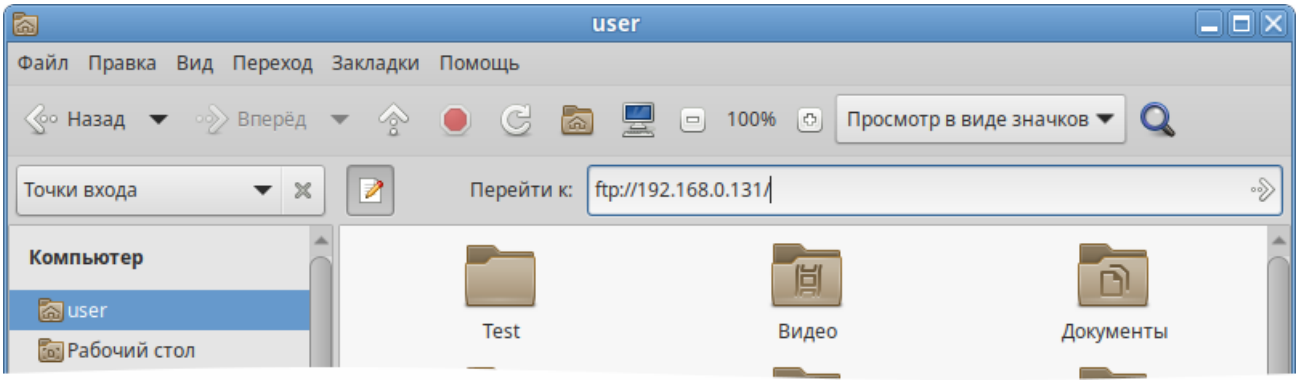

Рис. 223

Создание подключения по протоколу FTP

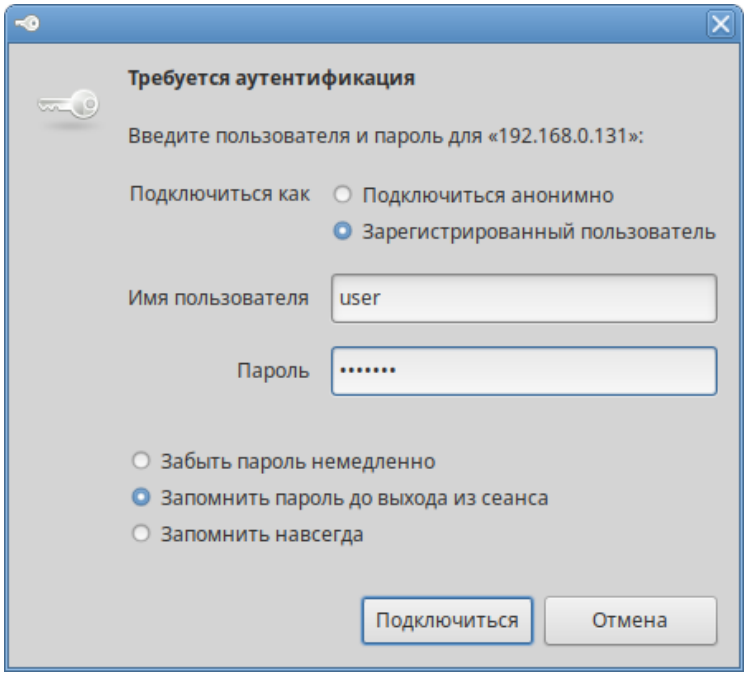

Рис. 224

Должен отобразиться список файлов каталога `/var/ftp/`, расположенного на сервере FTP (Рис. 225).

Файл на FTP сервере

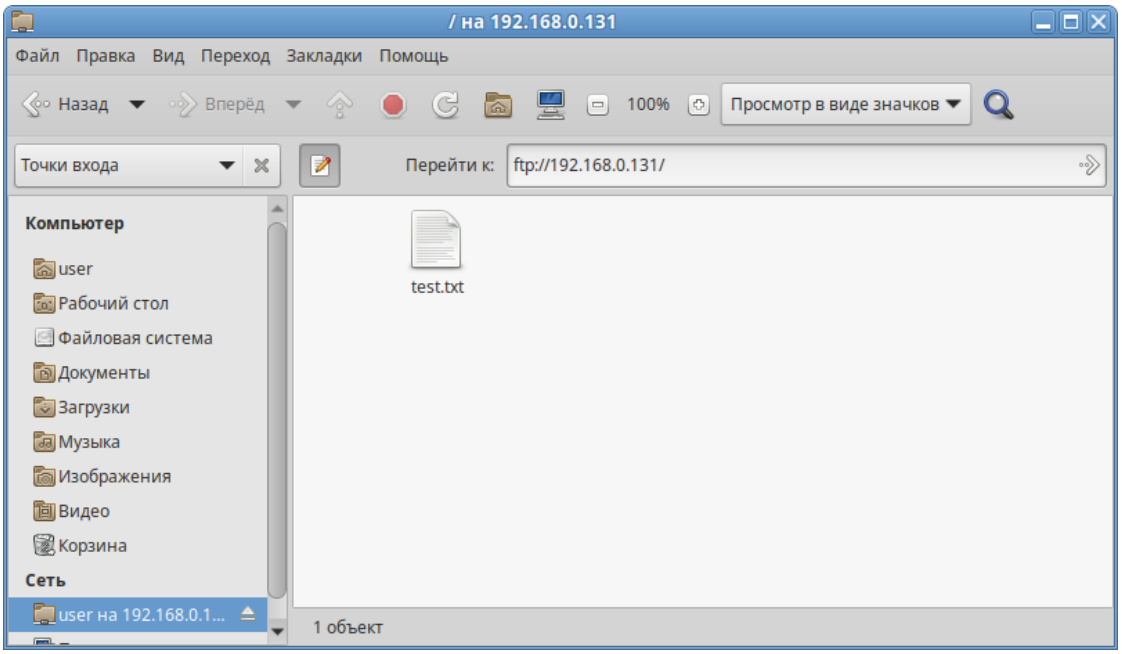

Рис. 225

6.9.4 NTP

6.9.4.1 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 и работу в качестве NTP-сервера и нажать кнопку «Применить» (Рис. 226).
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
   ```
3. Перезапустить сервис командой:

   ```
   # systemctl restart chronyd
   ```
4. Убедиться в нормальной работе NTP-сервера, выполнив команду:

   ```
   # systemctl status chronyd.service
   ```

Настройка модуля «Дата и время»

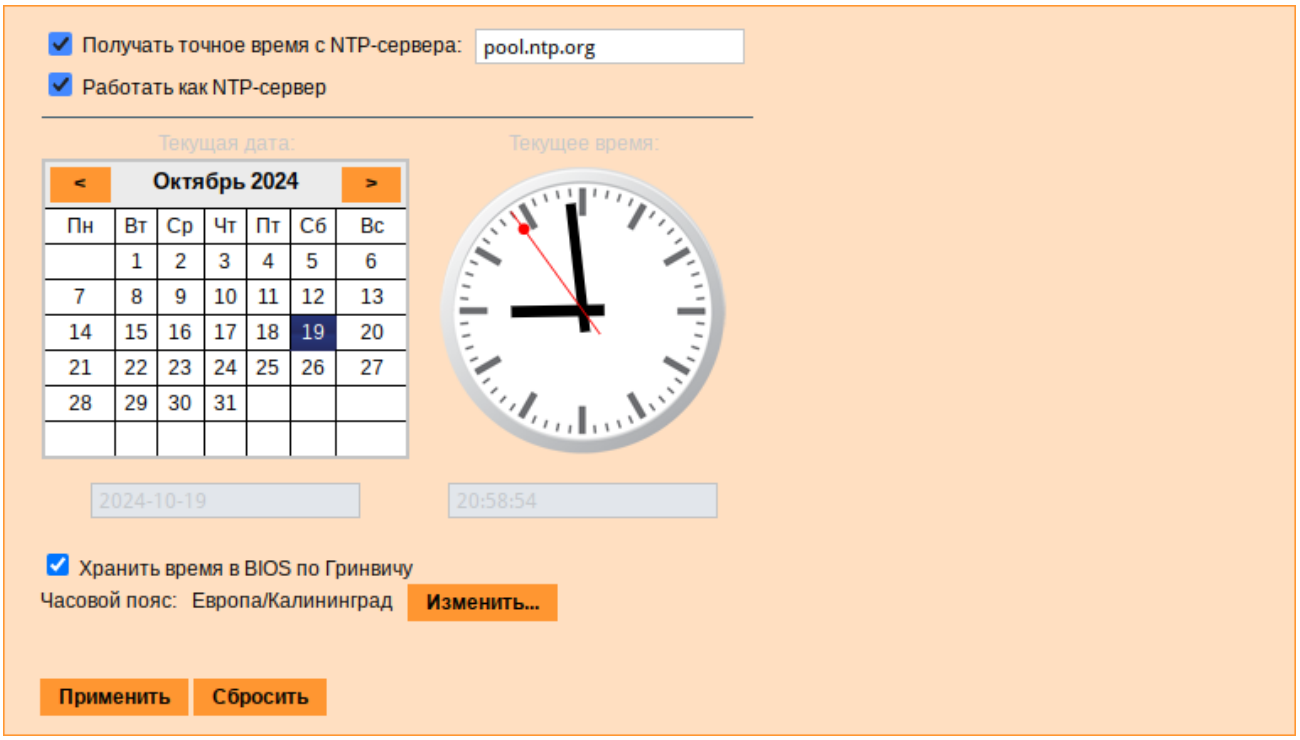

Рис. 226

6.9.4.2 Настройка рабочей станции

Настроить модуль «Дата и время» на получение точного времени с NTP-сервера (в качестве NTP-сервера указать IP-адрес сервера NTP) и нажать кнопку «Применить» (Рис. 227).

Настройка модуля «Дата и время» на рабочей станции

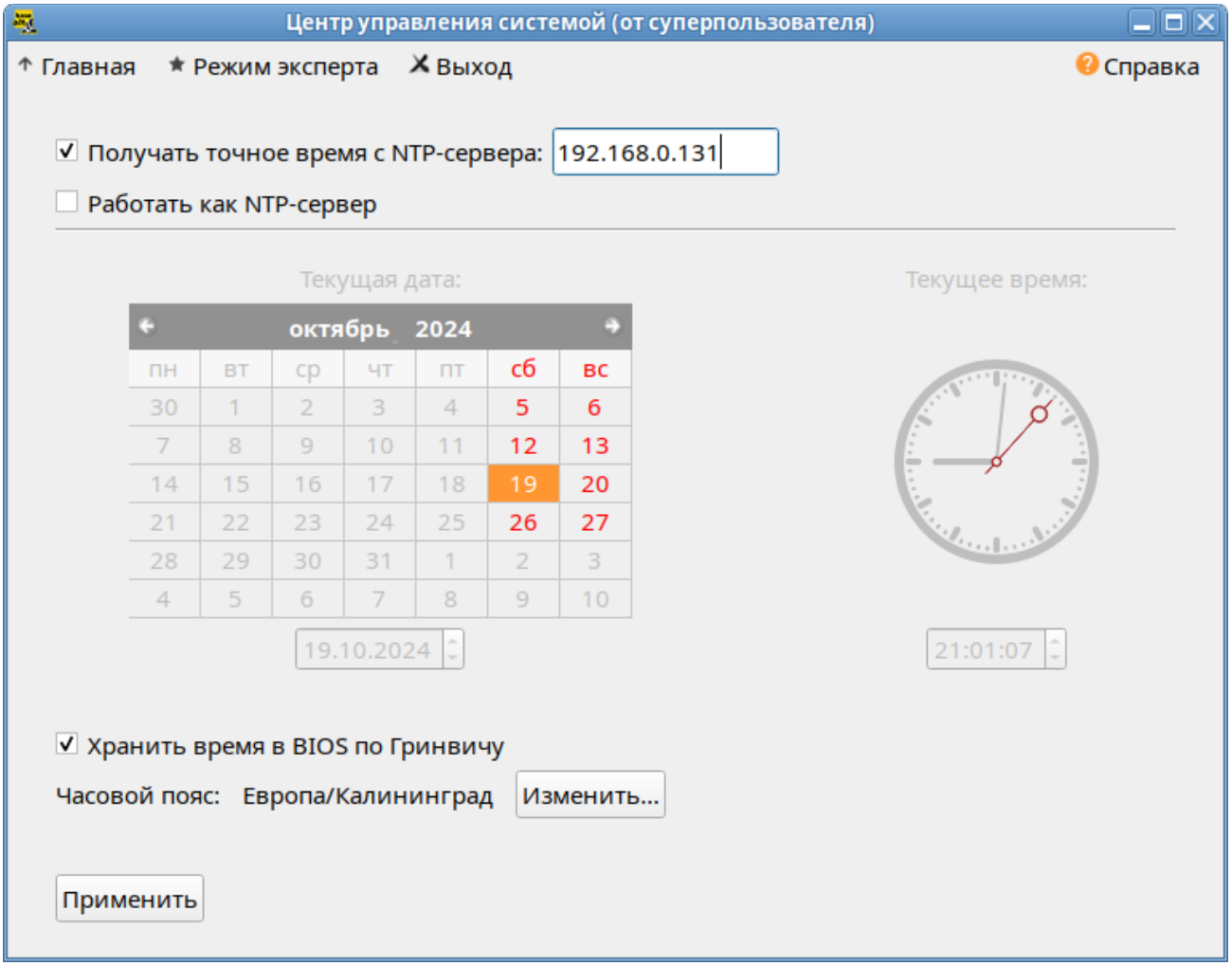

Рис. 227

Проверить текущие источники времени:

```
$ chronyc sources
MS Name/IP address   Stratum Poll Reach LastRx Last sample
===============================================================================
^? 192.168.0.131           0  10     0     -     +0ns[   +0ns] +/-    0n
```

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
```

6.9.5 HTTP(S)

6.9.5.1 Настройка сервера HTTP

Установить пакет `apache2-base` (пакет `apache2-base` не входит в состав ISO-образа дистрибутива, его можно установить из репозитория p10):

```
# 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
```

6.9.5.2 Настройка рабочей станции

Запустить браузер, перейти по адресу `http://<IP-адрес>` (Рис. 228).

Обращение к серверу и получение данных по протоколу http

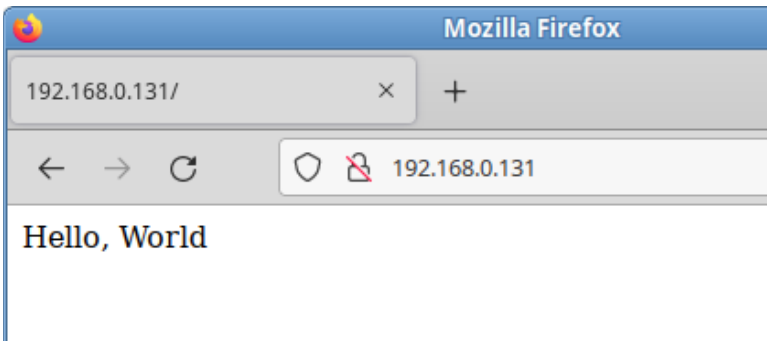

Рис. 228

Можно также выполнить команду:

```
$ curl http://192.168.0.131
Hello, World
```

Происходит обращение к серверу и получение данных по протоколу http.

6.10 Виртуальная (экранная) клавиатура

Onboard – гибкая в настройках виртуальная (экранная) клавиатура.

Виртуальная клавиатура полезна тогда, когда по каким либо причинам, нет возможности использовать обычную клавиатуру. Виртуальная клавиатура также может оказаться удобной пользователям сенсорных экранов (touchscreen).

Примечание. Должен быть установлен пакет `onboard`:

```
# apt-get install onboard
```

6.10.1 Клавиатура onboard при входе в систему

Для того чтобы появилась возможность использовать виртуальную клавиатуру при входе в систему, необходимо в файле `/etc/lightdm/lightdm-gtk-greeter.conf` выставить параметр `keyboard` в значение `onboard --xid`:

```
[greeter]
...
keyboard=onboard --xid
...
```

Чтобы запустить виртуальную клавиатуру на странице входа, следует нажать клавишу <F3> или щёлкнуть значок человека на верхней панели, а затем отметить пункт «Экранная клавиатура» (Рис. 229).

На экране появится виртуальная клавиатура (Рис. 230), её можно использовать для ввода имени пользователя и пароля.

Страница входа в систему

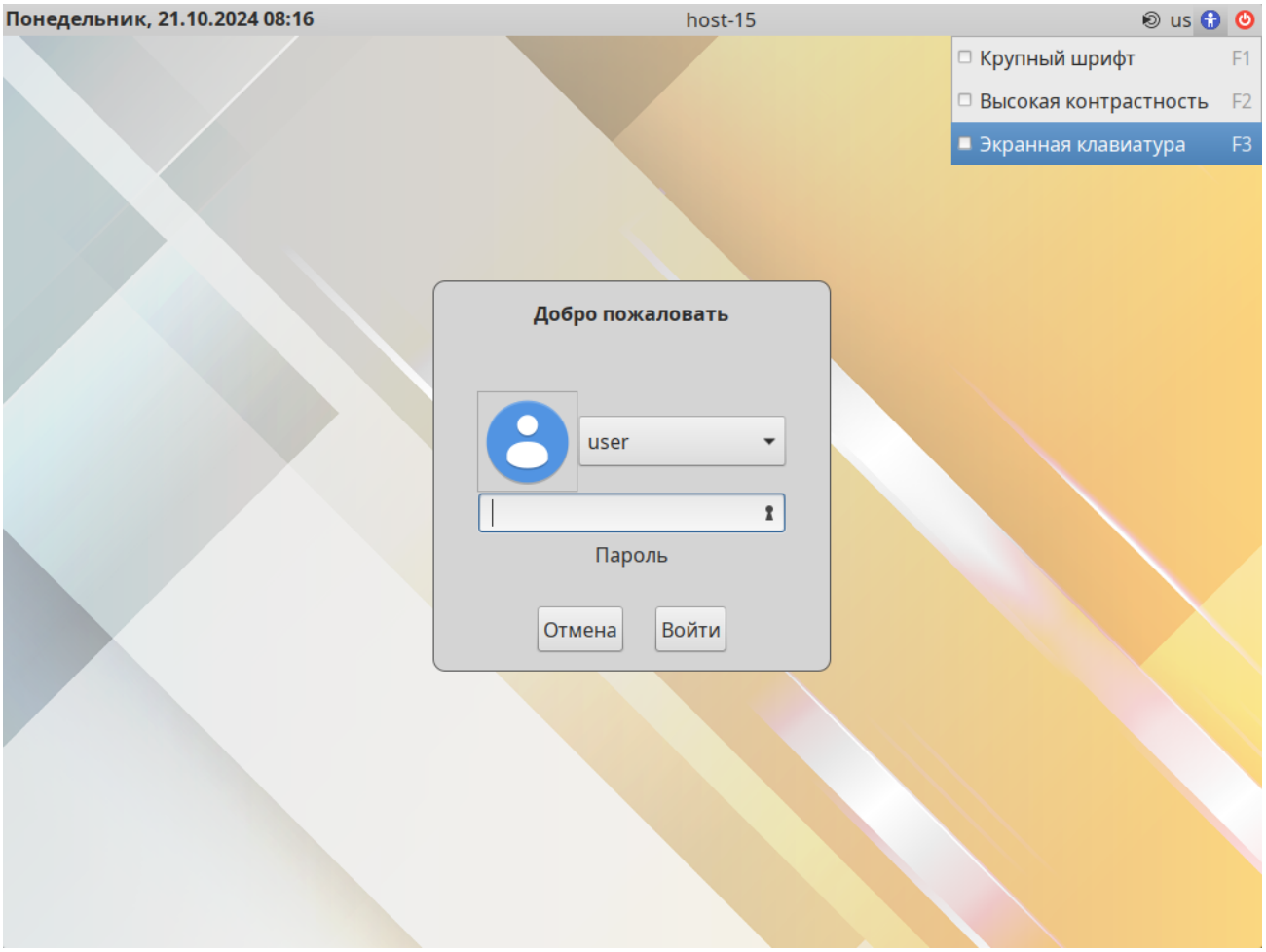

Рис. 229

6.10.2 Клавиатура onboard при разблокировке экрана

Для того чтобы появилась возможность использовать виртуальную клавиатуру при разблокировке экрана, достаточно из репозитория установить пакет `mate-screensaver-screenkeyboard`:

```
# apt-get install mate-screensaver-screenkeyboard
```

Виртуальная клавиатура при входе в систему

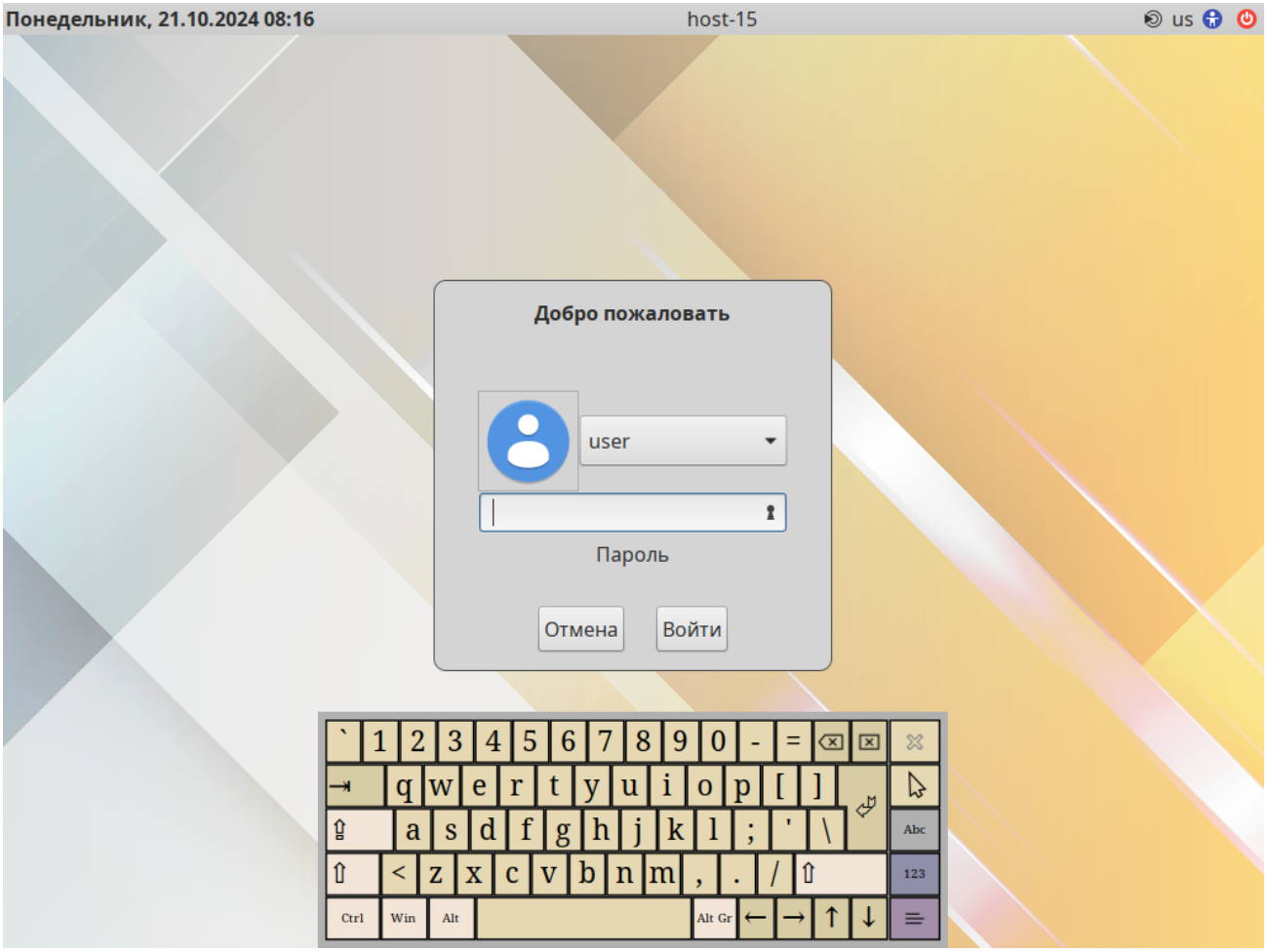

Рис. 230

В результате при разблокировке экрана появится виртуальная клавиатура (Рис. 231), её можно использовать для ввода пароля.

Виртуальная клавиатура при разблокировке экрана

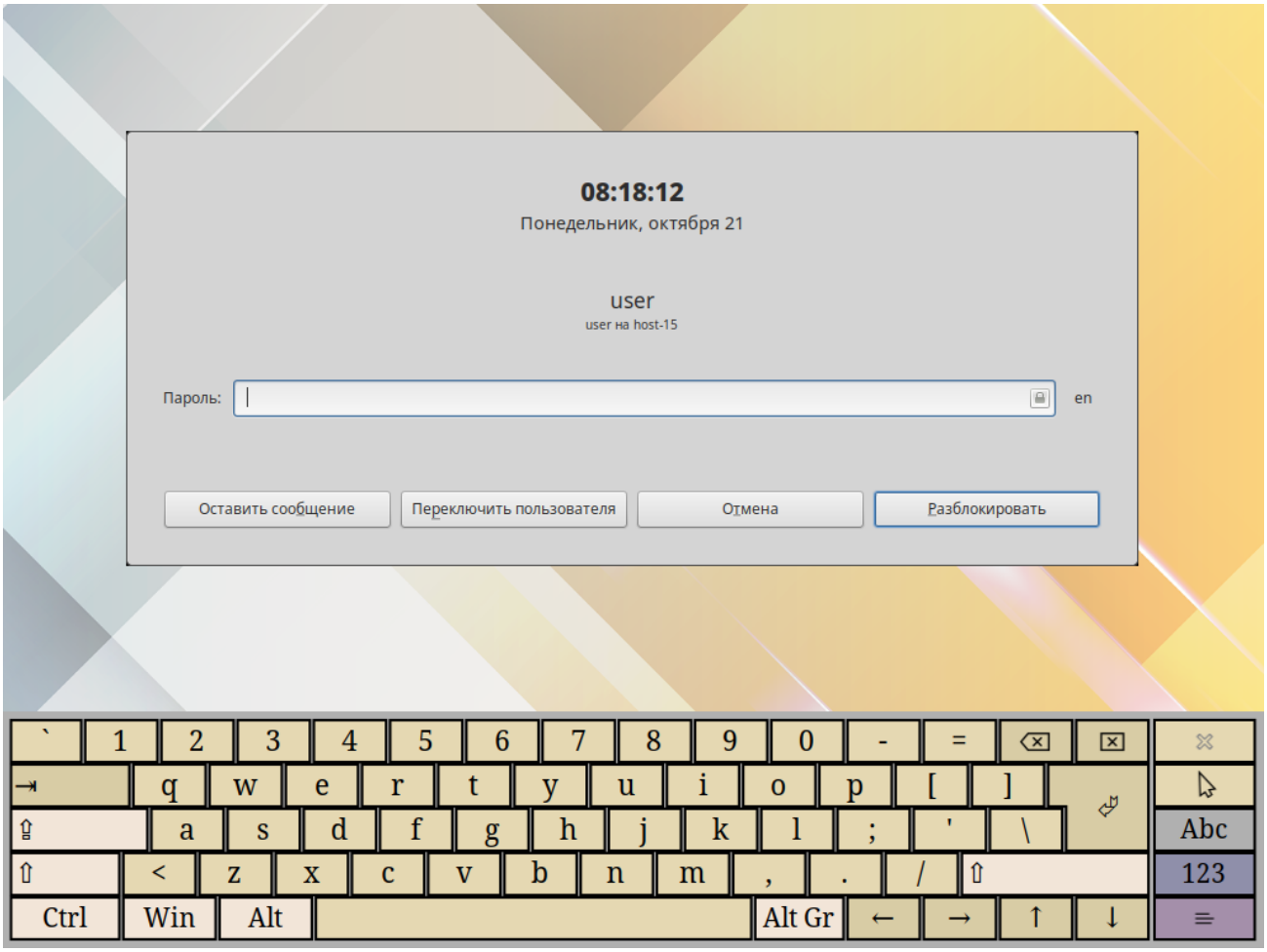

Рис. 231

6.11 Настройка многоместного режима

Модуль «Настройка нескольких рабочих мест» – графическое средство настройки мультитерминального режима, позволяющего обеспечить одновременную работу нескольких пользователей на одном компьютере.

Для настройки многоместного режима необходимо в ЦУС перейти в раздел «Система» → «Настройка нескольких рабочих мест».

Примечание. Необходимым условием для организации нескольких рабочих мест является наличие нескольких видеокарт, одна из которых может быть встроенной. Если вам нужно три места, потребуется 3 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.

По умолчанию в системе есть единственное рабочее место с именем seat0, к которому подключены все доступные устройства, они перечислены в списке «Устройства seat0» (Рис. 232). Это рабочее место нельзя удалить или изменить.

Интерфейс модуля «Настройка нескольких рабочих мест»

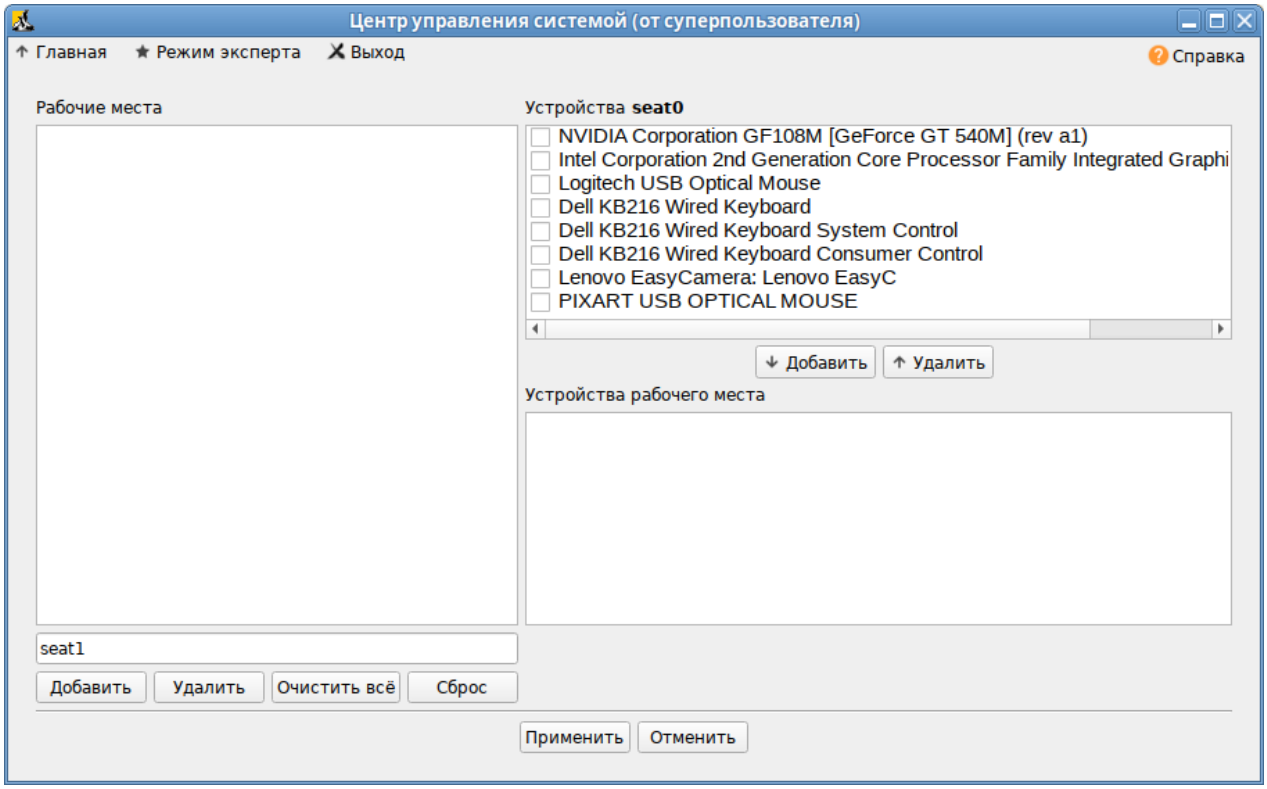

Рис. 232

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, необходимо выделить его в списке «Рабочие места», устройства будут показаны в списке «Устройства рабочего места».

Создание дополнительного рабочего места:

1. Ввести имя нового рабочего места в поле ввода, расположенное под списком рабочих мест, и нажать кнопку «Добавить». 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.

2. Выделить нужное рабочее место в списке «Рабочие места», а в списке «Устройства seat0» выбрать устройство, которое будет назначено выбранному рабочему месту. Нажать кнопку «Добавить». Устройство появится в списке устройств выбранного рабочего места. Выделить дополнительному рабочему месту видеокарту, клавиатуру и мышь (Рис. 233).

   Предупреждение. Основную видеокарту нельзя переключать на другие рабочие места.

3. Аналогичным образом настроить все рабочие места.

4. Для подключения назначенных устройств к дополнительным рабочим местам необходимо нажать кнопку «Применить». Чтобы настройки вступили в силу необходимо перезагрузить компьютер (Рис. 234).

Устройства рабочего места

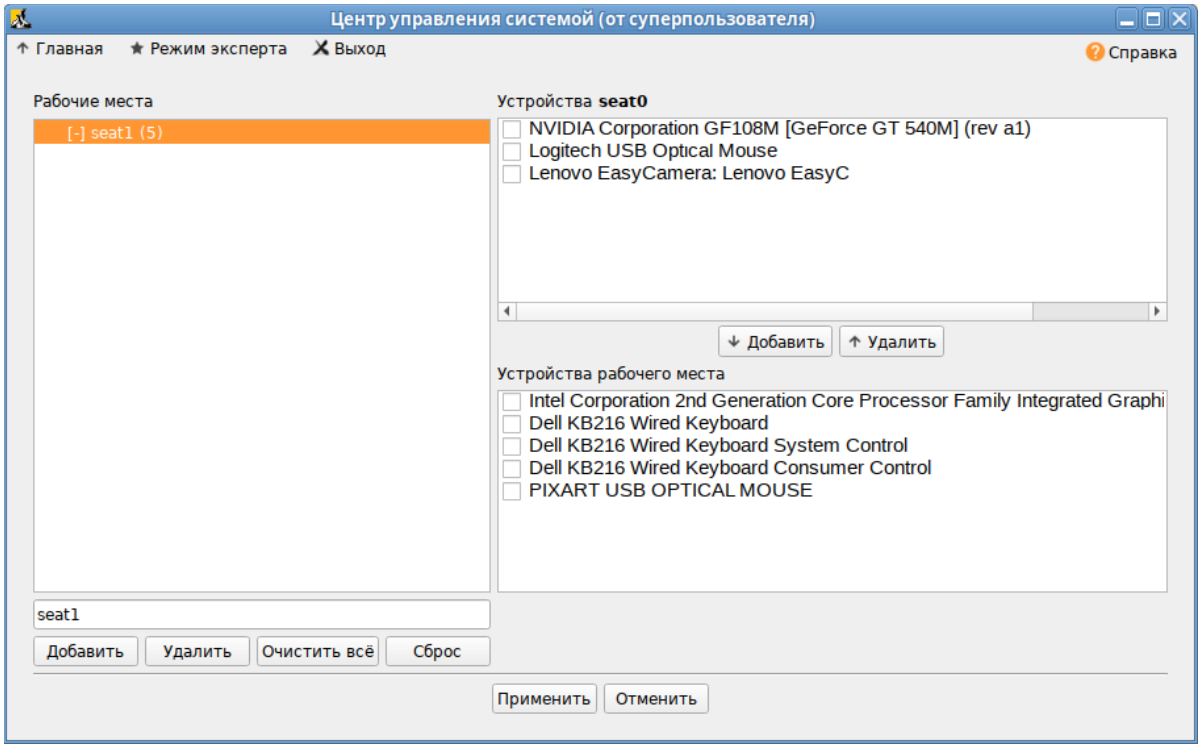

Рис. 233

Активация многоместного режима

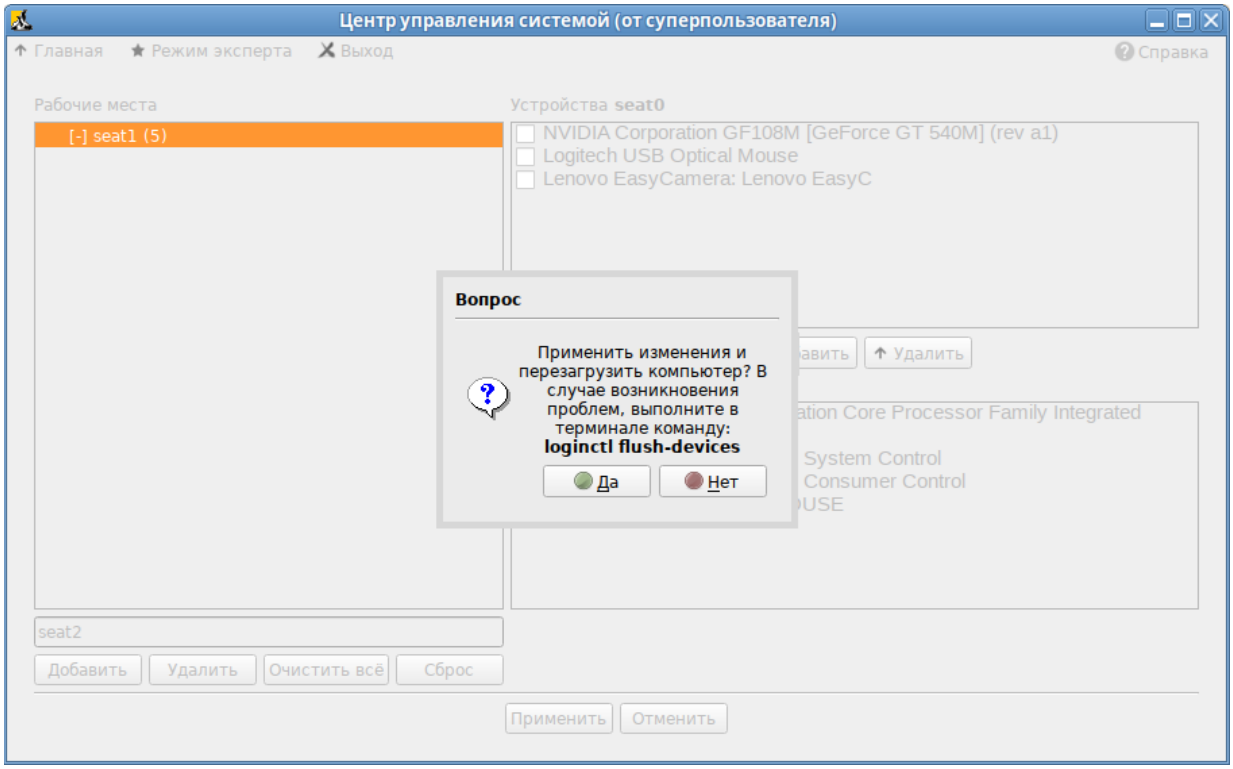

Рис. 234

Если после перезагрузки на мониторы не выводится никакая информация, это означает, что «закреплённая» за seat0 видеокарта была передана на другое рабочее место.

Чтобы исправить данную проблему необходимо сбросить настройки. Для этого следует залогиниться во второй текстовой консоли, удалить дополнительные рабочие места, выполнив команду (от root):

```
# loginctl flush-devices
```

И перезагрузить компьютер.

7 ОГРАНИЧЕНИЕ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ

7.1 Ограничение полномочий пользователей

7.1.1 Ограничение полномочий пользователей по использованию консолей

7.1.1.1 Отключение влияния бита SUID на привилегии порождаемого процесса в ЦУС

Для включения запрета бита исполнения необходимо в ЦУС перейти в раздел «Система» → «Блокировка терминала».

В списке пользователей следует выбрать пользователя, в окне «Список TTY» отметить консоли, которые должны быть заблокированы для данного пользователя, перенести их в окно «Заблокированные TTY» и нажать кнопку «Применить» (Рис. 235).

Ограничение полномочий пользователей по использованию консолей

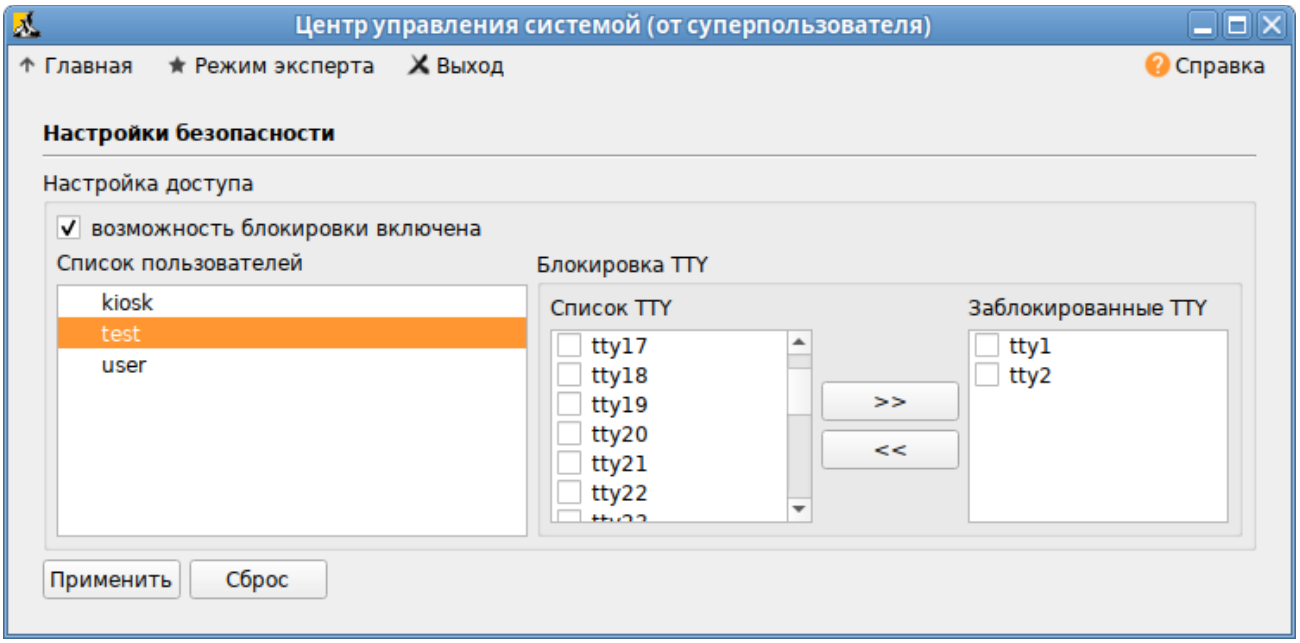

Рис. 235

7.1.1.2 Настройка ограничения в консоли

Чтобы ограничить консольный доступ для пользователей/групп с помощью модуля `pam_access.so` необходимо внести изменения в файл `/etc/security/access.conf`.

Примечание. Формат файла `/etc/security/access.conf`:

`permission:users:origins`

где

- permission — знак «+» (плюс) для предоставления доступа, или знак «-» (минус) — отказ в доступе;
- users — список пользователей или групп пользователей или ключевое слово ALL;
- origins — список TTY (для локального доступа), имен хостов, доменных имен, IP-адресов, ключевое слово ALL или LOCAL.

Чтобы ограничить доступ для всех пользователей, кроме пользователя root, следует внести следующие изменения:

```
# vim /etc/security/access.conf
-:ALL EXCEPT root: tty2 tty3 tty4 tty5 tty6
```

Доступ может быть ограничен для конкретного пользователя:

```
# vim /etc/security/access.conf
-:user: tty2 tty3 tty4 tty5 tty6
```

Доступ может быть ограничен для группы, содержащей несколько пользователей:

```
# vim /etc/security/access.conf
-:group:LOCAL
```

Далее необходимо сконфигурировать стек PAM для использования модуля pam_access.so для ограничения доступа на основе ограничений, определенных в файле `/etc/security/access.conf`. Для этого дописать в файл `/etc/pam.d/system-auth-local-only` строку `account required pam_access.so` после строки `account required pam_tcb.so`:

```
auth            required        pam_tcb.so shadow fork nullok
account         required        pam_tcb.so shadow fork
account         required        pam_access.so
password        required        pam_passwdqc.so config=/etc/passwdqc.-
conf
password        required        pam_tcb.so use_authtok shadow fork
nullok write_to=tcb
session         required        pam_tcb.so
```

7.1.2 Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы

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

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

Первое поле (domain) может содержать:

- имя пользователя;
- имя группы (перед именем группы нужно указать символ «@»);
- символ «*» (данное ограничение будет ограничением по умолчанию);
- символ «%»– используется только с ограничением maxlogins. Группа, указанная после %, ограничивает число параллельных сеансов всех пользователей, которые являются членами группы. Если символ «%» используется отдельно, он идентичен использованию «*» с ограничением maxsyslogins;

- диапазон uid, заданный как <min_uid>:<max_uid>;
- диапазон gid, заданный как @<min_gid>:<max_gid>;
- gid, заданный как %:<gid> – используется только с ограничением maxlogins.

Второе поле – это тип ограничения: мягкое (soft) или жесткое (hard). Мягкое ограничение определяет число системных ресурсов, которое пользователь все еще может превысить, жесткое ограничение превысить невозможно. При попытке сделать это, пользователь получит сообщение об ошибке. Символ «-» используется для одновременной установки как мягкого, так и жесткого ограничения.

Элементом ограничения (item) может быть:

- core – ограничение размера файла core (Кбайт);
- data – максимальный размер данных (Кбайт);
- fsize – максимальный размер файла (Кбайт);
- memlock – максимальное заблокированное адресное пространство (Кбайт);
- nofile – максимальное число открытых файлов;
- stack – максимальный размер стека (Кбайт);
- cpu – максимальное время процессора (минуты);
- nproc – максимальное число процессов;
- as – ограничение адресного пространства;
- maxlogins – максимальное число одновременных регистраций в системе;
- maxsyslogins – максимальное количество учётных записей;
- priority – приоритет запуска пользовательских процессов;
- locks – максимальное число файлов блокировки;
- sigpending — максимальное количество сигналов, которые можно передать процессу;
- msgqueue – максимальный размер памяти для очереди POSIX сообщений (байт);
- nice – максимальный приоритет, который можно выставить: [-20, 19];
- rtprio – максимальный приоритет времени выполнения.

Чтобы установить максимальное число процессов для пользователя user в файл `limits.conf` нужно добавить записи:

```
user soft nproc 50
user hard nproc 60
```

Первая строка определяет мягкое ограничение (равное 50), а вторая – жесткое.

Следующие строки обеспечат одновременную работу не более 15 пользователей из каждой группы пользователей (group1 и group2):

```
%group1 - maxlogins 14
%group2 - maxlogins 14
```

В первом и втором случае из каждой группы пользователей одновременно работать смогут не более 15. При шестнадцатой регистрации пользователь из группы увидит сообщение:

```
There were too many logins for 'user'.
```

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

```
* - maxlogins 5
```

Примечание. Ограничения также можно настраивать в ЦУС в разделе «Система» → «Настройки ограничений» (Рис. 236). Для этого необходимо установить пакет `alterator-limits` (из репозитория p10):

```
# apt-get install alterator-limits
```

Установка ограничений ресурсов, доступных пользователю

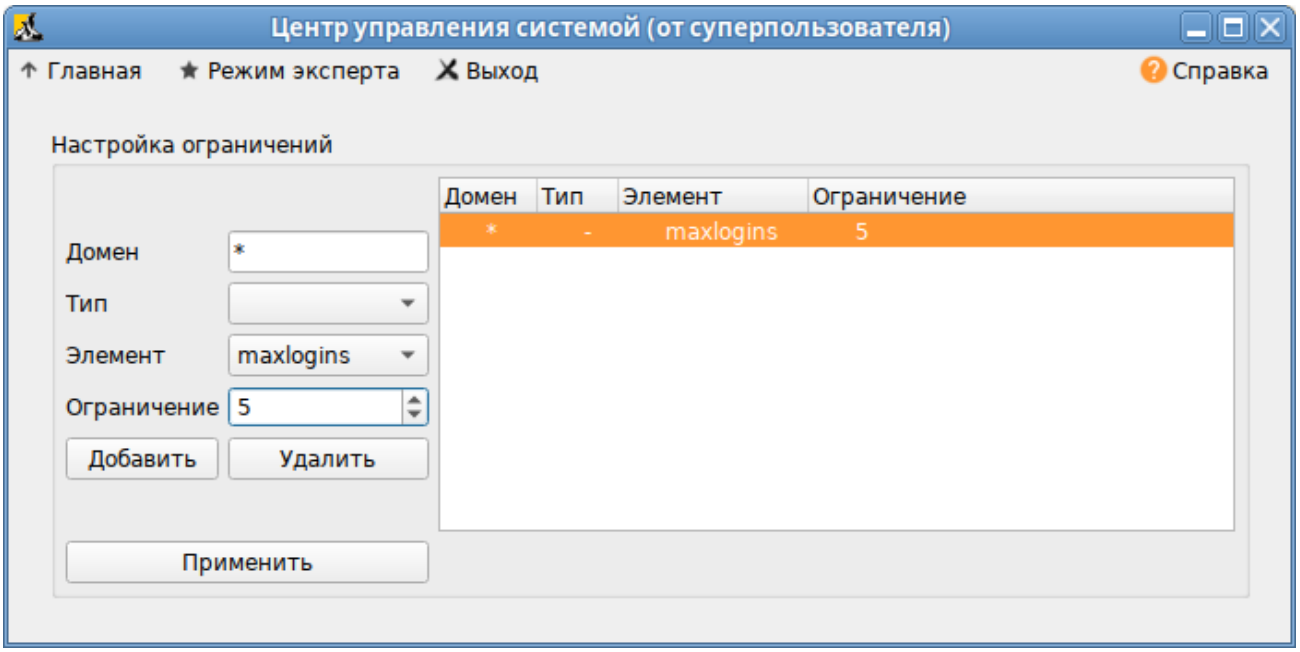

Рис. 236

7.2 Блокировка макросов в приложениях

Для того чтобы включить блокировку макросов в приложениях, необходимо в ЦУС перейти в раздел «Система» → «Настройки безопасности».

Примечание. Должен быть установлен пакет `alterator-secsetup`:

```
# apt-get install alterator-secsetup
```

В открывшемся окне следует отметить пункт «Блокировать макросы приложений» и нажать кнопку «Применить» (Рис. 237).

Блокировка макросов в приложениях

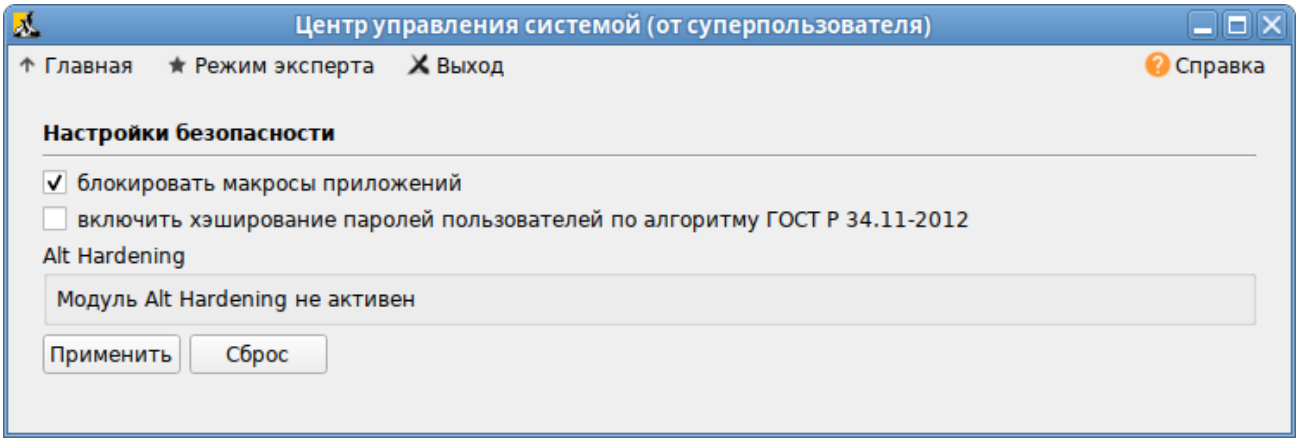

Рис. 237

Макросы будут заблокированы.

7.3 Модуль AltHa

AltHa – это модуль безопасности Linux, который 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 необходимо 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.

Включить AltHa можно также в модуле «Настройка загрузчика GRUB2».

7.3.1 Запрет бита исполнения (SUID)

При включенном подмодуле `altha.nosuid`, биты SUID во всех двоичных файлах, кроме явно перечисленных, игнорируются в масштабе всей системы.

7.3.1.1 Отключение влияния бита SUID на привилегии порождаемого процесса в ЦУС

Для включения запрета бита исполнения необходимо в ЦУС перейти в раздел «Система» → «Настройки безопасности».

Примечание. Должен быть установлен пакет `alterator-secsetup`:

```
# apt-get install alterator-secsetup
```

В открывшемся окне следует отметить пункт «Отключить влияние suid бита на привилегии порождаемого процесса» и нажать кнопку «Применить» (Рис. 238).

Отключение влияния бита SUID на привилегии порождаемого процесса

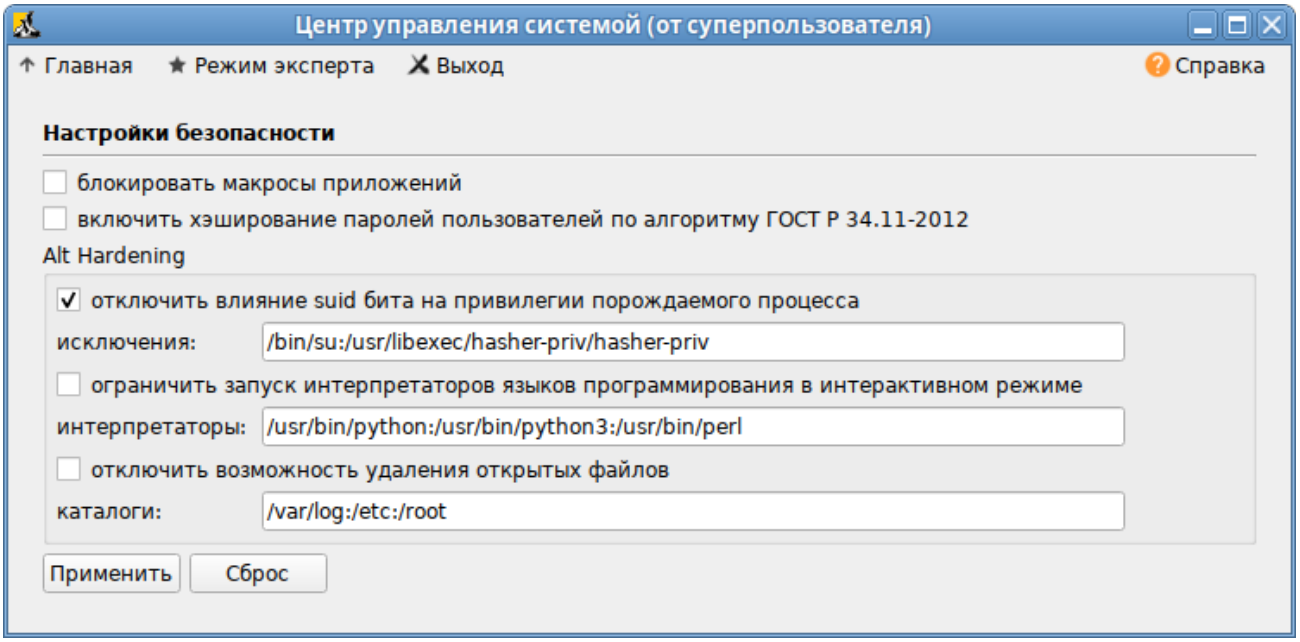

Рис. 238

Исключения это список включенных двоичных файлов SUID, разделённых двоеточиями.

7.3.1.2 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 необходимо, 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.

7.3.2 Блокировка интерпретаторов (запрет запуска скриптов)

При включении блокировки интерпретаторов блокируется несанкционированное использование интерпретатора для выполнения кода напрямую из командной строки.

7.3.2.1 Блокировка интерпретаторов (запрет запуска скриптов) в ЦУС

Для включения режима блокировки интерпретаторов необходимо в ЦУС перейти в раздел «Система» → «Настройки безопасности».

В открывшемся окне следует отметить пункт «Ограничить запуск интерпретаторов языков программирования в интерактивном режиме» и нажать кнопку «Применить». Поле «Интерпретаторы» должно содержать разделённый запятыми список ограниченных интерпретаторов (Рис. 239).

Блокировка интерпретаторов (запрет запуска скриптов)

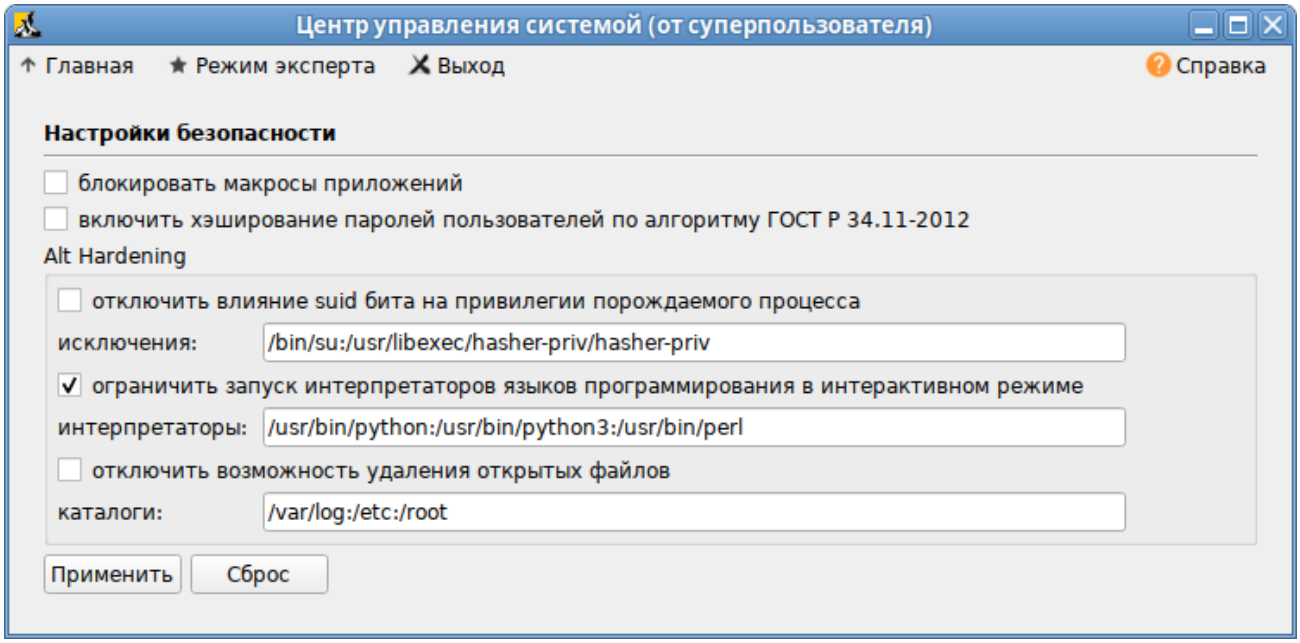

Рис. 239

7.3.2.2 Блокировка интерпретаторов (запрет запуска скриптов) 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.

Список заблокированных интерпретаторов:

```
# sysctl -n kernel.altha.rstrscript.interpreters
/usr/bin/python:/usr/bin/python3:/usr/bin/perl:/usr/bin/tclsh
```

8 УСТАНОВКА/ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

После установки ОС «Альт Рабочая станция», при первом запуске, доступен тот или иной набор программного обеспечения. Количество предустановленных программ зависит от выбора, сделанного при установке системы. Имеется возможность доустановить программы, которых не хватает в системе, из разных источников.

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

Примечание. В установочный комплект ОС «Альт Рабочая станция» включено наиболее употребительное программное обеспечение. В то же время вы можете использовать репозиторий продукта (p10) для установки дополнительных программных пакетов.

Для установки дополнительного ПО можно использовать программу управления пакетами Synaptic.

8.1 Установка/обновление программного обеспечения в графической среде

8.1.1 Программа управления пакетами Synaptic

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

При запуске необходимо ввести пароль администратора системы (Рис. 240).

Synaptic. Запрос пароля администратора

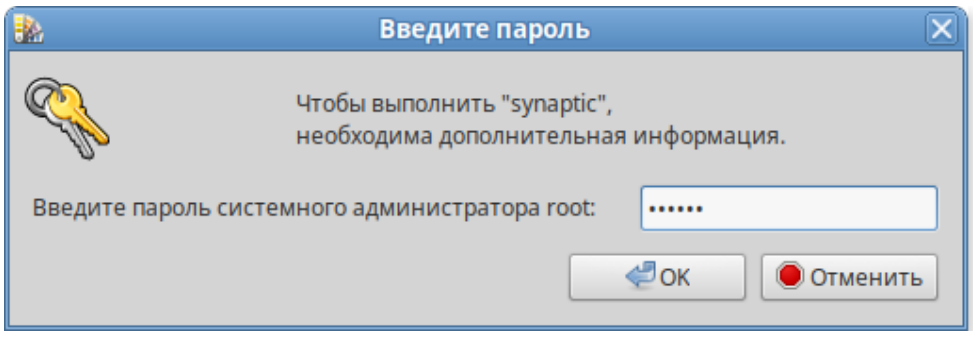

Рис. 240

Для облегчения поиска доступные для установки программы разделены на группы, выводимые в левой части окна программы (Рис. 241).

Программа управления пакетами Synaptic

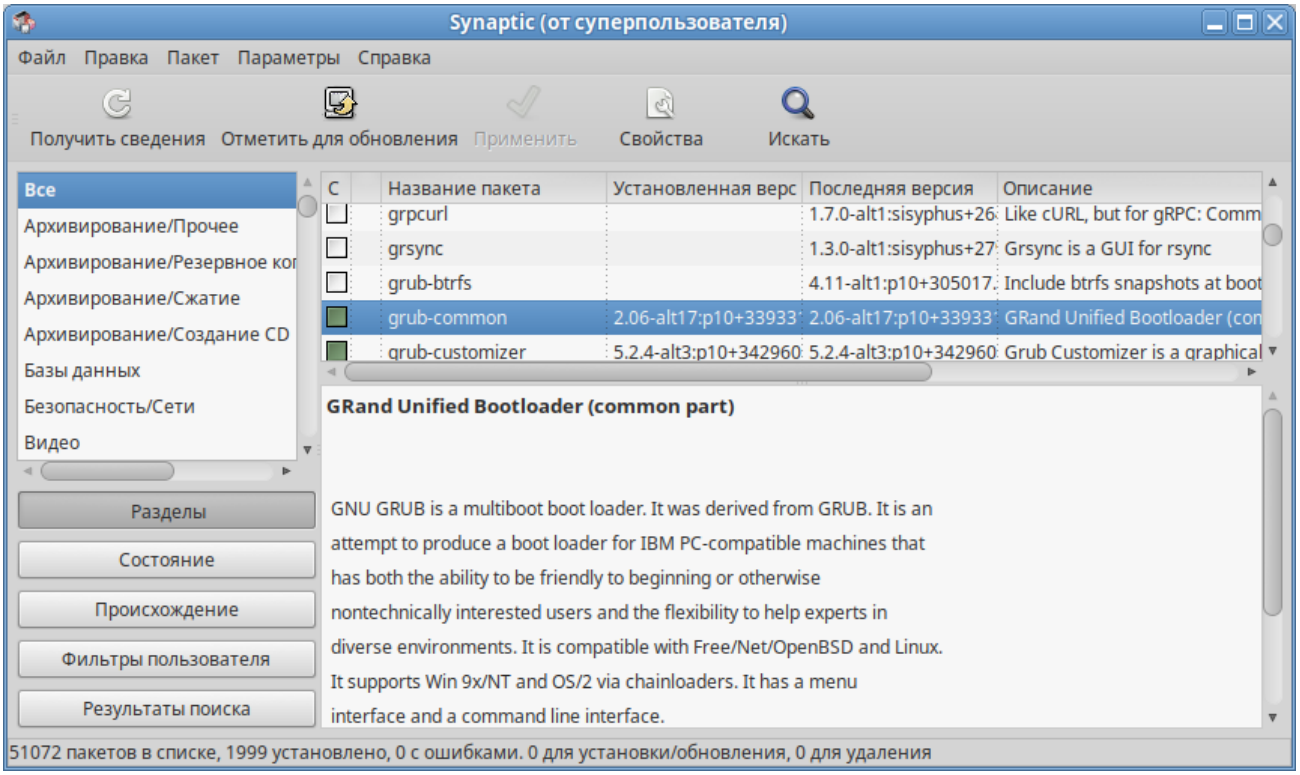

Рис. 241

Справа расположен список самих программ с указанием их текущего состояния:

- зелёная метка – пакет уже установлен;
- белая метка – пакет не установлен;
- зелёная метка со звёздочкой – для установленного пакета имеется обновление.

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

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

Для начала установки необходимо двойным щелчком мыши отметить неустановленный пакет в правой половине окна и нажать кнопку «Применить». При необходимости менеджер пакетов попросит вставить установочный диск.

8.1.2 Добавление репозиториев в Synaptic

Программа Synaptic может использоваться для выбора репозитория, совместимого с дистрибутивом. Для указания конкретного репозитория в меню «Параметры» → «Репозитории» необходимо отметить один из предлагаемых вариантов и нажать кнопку «OK» (Рис. 242). К предложенному списку можно добавить любые репозитории, нажав на кнопку «Создать» и введя необходимые данные.

Добавление репозиториев в Synaptic

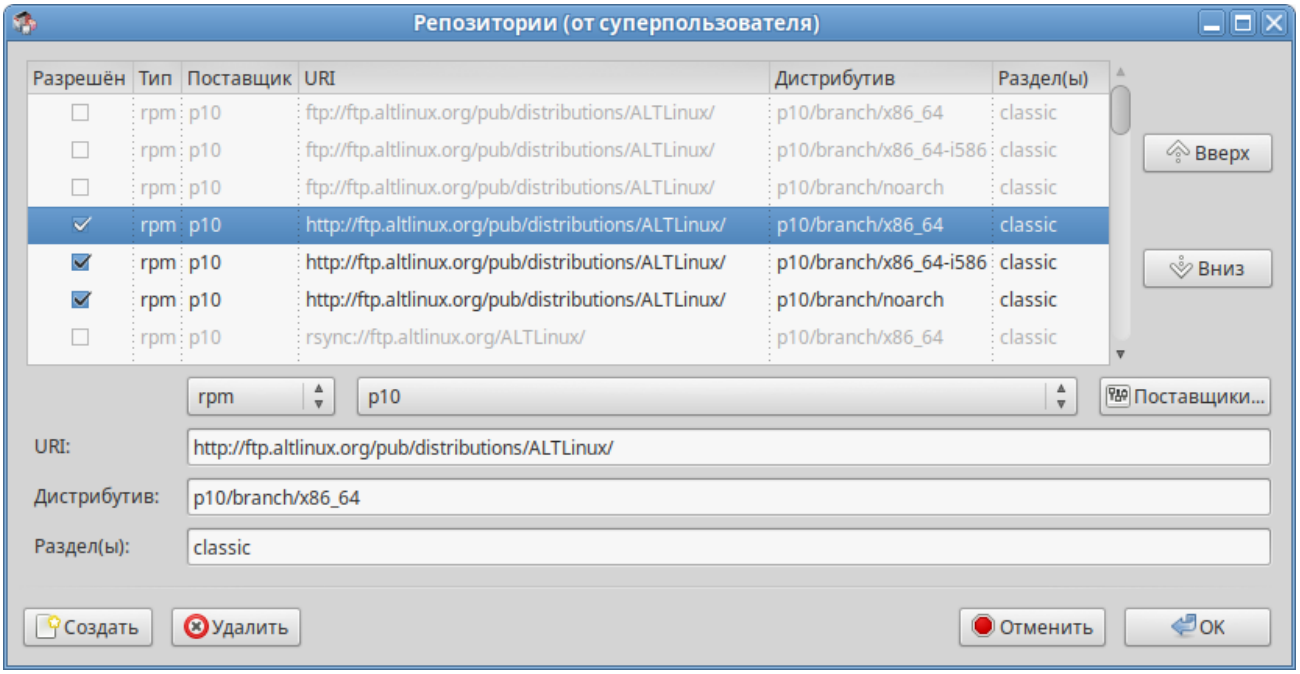

Рис. 242

После выбора и добавления репозиториев необходимо получить сведения о находящихся в них пакетах (кнопка «Получить сведения» см. Рис. 241). В противном случае, список доступных для установки программ будет не актуален.

8.2 Обновление системы

8.2.1 Обновление всех установленных пакетов

Обновить все установленные пакеты можно в программе Synaptic.

Synaptic поддерживает два варианта обновления системы:

- интеллектуальное обновление (рекомендуется) – попытается разрешить конфликты пакетов перед обновлением системы. Действие интеллектуального обновления аналогично действию команды `apt-get dist-upgrade`;
- стандартное обновление – обновление обновит только те пакеты, которые не требуют установки дополнительных зависимостей.

По умолчанию Synaptic использует интеллектуальное обновление. Для того чтобы изменить метод обновления системы, необходимо открыть диалоговое окно «Параметры» («Параметры» → «Параметры») и на вкладке «Основное» в списке «Обновить систему» выбрать требуемый способ.

Для обновления системы необходимо (Рис. 243):

1. Нажать кнопку «Получить сведения» (<Ctrl+<R>), для того чтобы скачать список самых последних версий ПО.

2. Нажать кнопку «Отметить для обновления» (<Ctrl>+<G>), для того чтобы Synaptic отметил доступные для обновления пакеты. При этом программа может вывести окно со списком вносимых изменений.
3. Нажать кнопку «Применить». Будет показан список изменений, который произойдет при обновлении пакетов. Тут следует обратить внимание на объём данных, который будет скачан из сети. После подтверждения Synaptic начнёт загружать файлы, затем начнётся непосредственно установка.

Обновление всех установленных пакетов в Synaptic

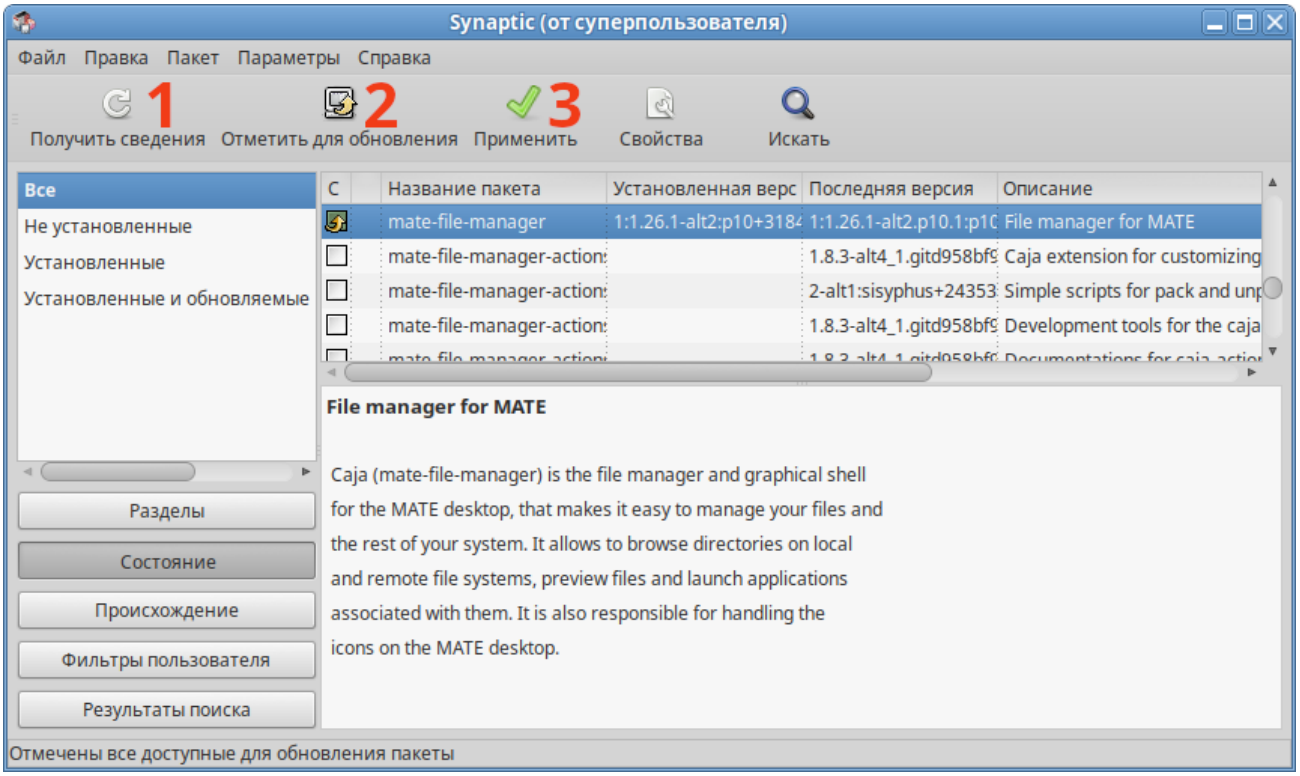

Рис. 243

8.2.2 Обновление ядра ОС

Модуль ЦУС «Обновление ядра» реализует функционал утилиты `update-kernel`. Для обновления ядра ОС необходимо в ЦУС перейти в раздел «Система» → «Обновление ядра».

В главном окне модуля отображается ядро, загруженное по умолчанию, и список установленных модулей ядра (Рис. 244).

Для того чтобы обновить ядро, следует нажать кнопку «Обновить ядро…».

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

Интерфейс модуля «Обновление ядра»

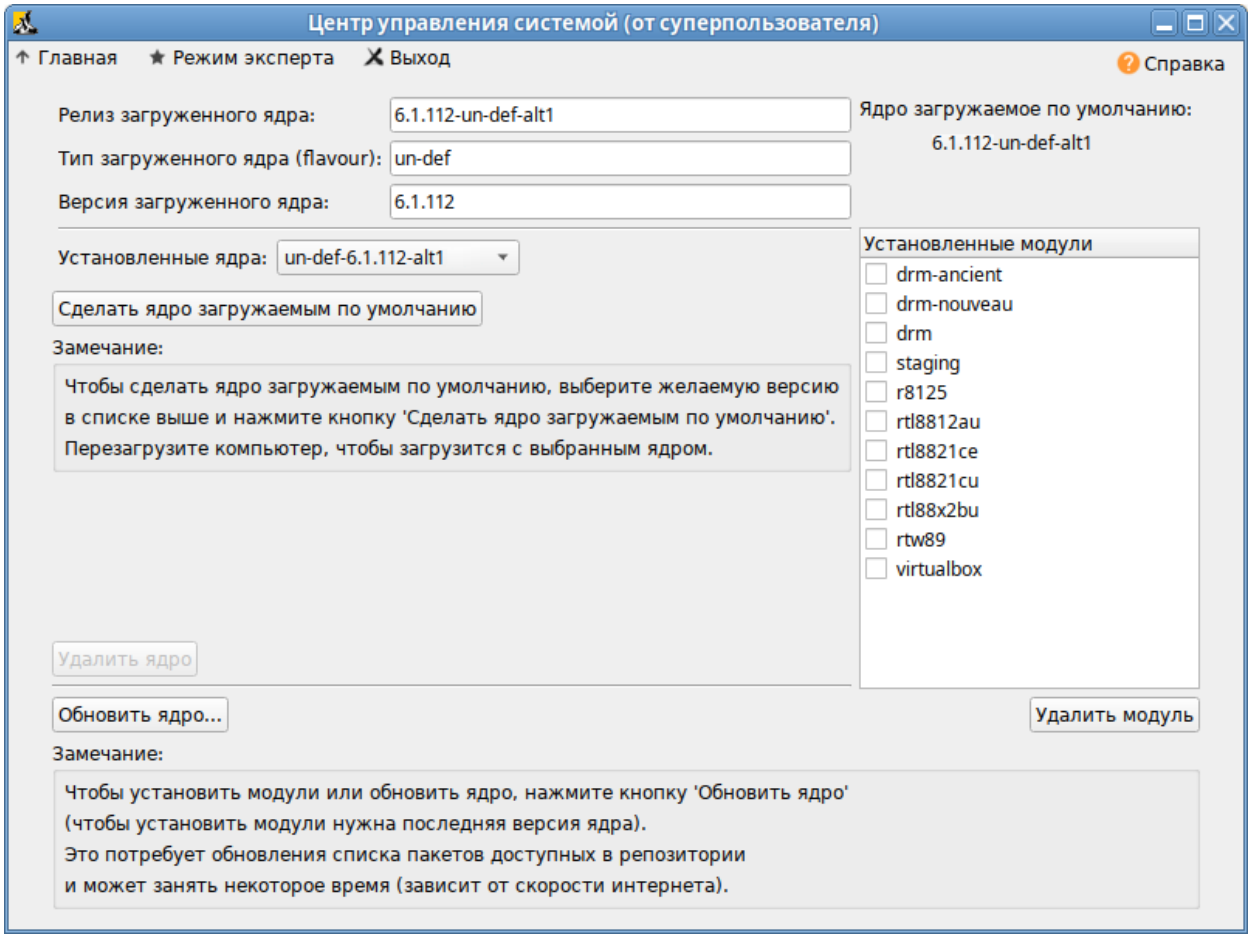

Рис. 244

Если в системе уже установлено последнее ядро, сообщение об этом появится в открывшемся окне (Рис. 245), иначе в этом окне будет показано доступное к установке ядро.

Доступное к установке ядро

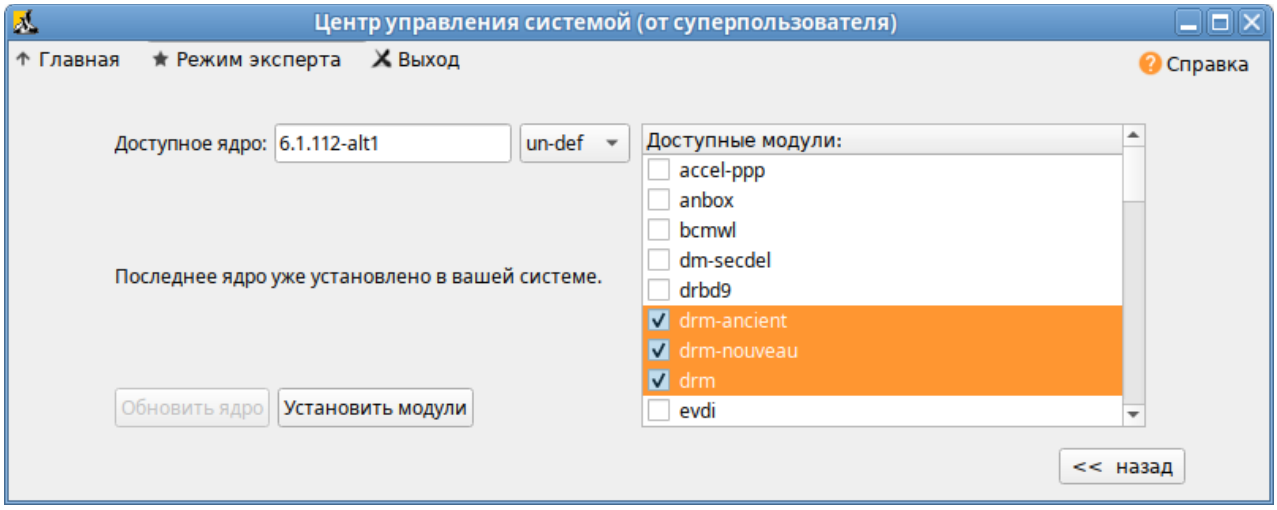

Рис. 245

Чтобы обновить ядро, необходимо нажать кнопку «Обновить ядро». Далее следует подтвердить желание обновить ядро нажатием кнопки «Да». Установленное ядро станет загружаемым по умолчанию.

Примечание. Новое ядро загрузится только после перезагрузки системы.

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

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

8.3 Установка/обновление программного обеспечения в консоли

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).

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.

8.3.1 Источники программ (репозитории)

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.

Примечание. Для одновременного подключения нескольких репозиториев необходимо отслеживать их совместимость друг с другом, т.е. их пакетная база должна отражать один определённый этап разработки. Совместное использование репозиториев, относящихся к разным дистрибутивам, или смешивание стабильного репозитория с нестабильной веткой разработки (Sisyphus) может привести к различным неожиданностям и трудностям при обновлении пакетов.

APT 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 необходимо поместить в файл `/etc/apt/sources.list`, либо в любой файл `.list` (например, `mysources.list`) в каталоге `/etc/apt/sources.list.d/`. Описания репозиториев заносятся в эти файлы в следующем виде:

```
rpm [подпись] метод: путь база название
rpm-src [подпись] метод: путь база название
```

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/vendor.list`;
- метод – способ доступа к репозиторию: ftp, http, file, cdrom, copy;
- путь – путь к репозиторию в терминах выбранного метода;
- база – относительный путь к базе данных репозитория;
- название – название репозитория.

При выборе пакетов для установки APT руководствуется всеми доступными репозиториями вне зависимости от способа доступа к ним. Таким образом, если в репозитории, доступном по сети Интернет, обнаружена более новая версия программы, чем на CD (DVD)-носителе информации, APT начнет загружать данный пакет по сети.

8.3.1.1 Добавление репозиториев

Непосредственно после установки дистрибутива «Альт Рабочая станция» в `/etc/apt/sources.list`, а также в файлах `/etc/apt/sources.list.d/*.list` обычно указывается несколько репозиториев:

- репозиторий с установочного диска дистрибутива;

- интернет-репозиторий, совместимый с установленным дистрибутивом.

8.3.1.1.1 Утилита apt-repo для работы с репозиториями

Для добавления репозиториев можно воспользоваться утилитой `apt-repo`.

Примечание. Для выполнения большинства команд необходимы права администратора.

Просмотреть список активных репозиториев можно, выполнив команду:

```
$ apt-repo list
```

Команда добавления репозитория в список активных репозиториев:

```
apt-repo add <репозиторий>
```

Команда удаления или выключения репозитория:

```
apt-repo rm <репозиторий>
```

Команда удаления всех репозиториев:

```
apt-repo clean
```

Обновление информации о репозиториях:

```
apt-repo update
```

Вывод справки:

```
man apt-repo
```

или

```
apt-repo –help
```

Типичный пример использования: удалить все источники и добавить стандартный репозиторий p10 (архитектура выбирается автоматически):

```
# apt-repo rm all
# apt-repo add p10
```

Или то же самое одной командой:

```
# apt-repo set p10
```

8.3.1.1.2 Добавление репозитория на сменном диске

Для добавления в `sources.list` репозитория на сменном диске в APT предусмотрена специальная утилита – `apt-cdrom`.

Чтобы добавить запись о репозитории на сменном диске необходимо:

- создать каталог для монтирования. Точка монтирования указывается в параметре `Acquire::CDROM::mount` в файле конфигурации APT (`/etc/apt/apt.conf`), по умолчанию это `/media/ALTLinux`:

```
# mkdir /media/ALTLinux
```

- примонтировать носитель в указанную точку:

```
# mount /dev/sdXN /media/ALTLinux
```

где /dev/sdXN – соответствующее блочное устройство (например, /dev/dvd – для CD/DVD-диска).

- добавить носитель, выполнив команду:

```
# apt-cdrom -m add
```

После этого в sources.list появится запись о подключённом диске.

Примечание. Команду mount /dev/носитель /media/ALTLinux необходимо выполнять перед каждой командой apt-get install имя_пакета.

8.3.1.1.3 Добавление репозиториев вручную

Для редактирования списка репозиториев можно отредактировать в любом текстовом редакторе файлы из папки /etc/apt/sources.list.d/. Для изменения этих файлов необходимы права администратора. В файле alt.list может содержаться такая информация:

```
rpm [alt] http://ftp.altlinux.org/pub/distributions/ALTLinux
p10/x86_64 classic
rpm [alt] http://ftp.altlinux.org/pub/distributions/ALTLinux
p10/x86_64-i586 classic
rpm [alt] http://ftp.altlinux.org/pub/distributions/ALTLinux
p10/noarch classic
```

По сути, каждая строчка соответствует некому репозиторию. Для выключения репозитория достаточно закомментировать соответствующую строку (дописать символ решётки перед строкой). Для добавления нового репозитория необходимо дописать его вниз этого или любого другого файла.

8.3.1.2 Обновление информации о репозиториях

В случае если в sources.list присутствует репозиторий, содержимое которого может изменяться, как происходит с любым постоянно разрабатываемым репозиторием, в частности, обновлений по безопасности (updates), то прежде чем работать с APT, необходимо синхронизировать локальную базу данных с удаленным сервером.

Обновление данных осуществляется командой:

```
# apt-get update
```

После выполнения этой команды, apt обновит свой кэш новой информацией.

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.

Практически любое действие с системой apt начинается с обновления данных от активиро-

ванных источников. Список источников необходимо обновлять при поиске новой версии пакета, установке пакетов или обновлении установленных пакетов новыми версиями.

8.3.2 Поиск пакетов

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
gimp-help-en - English help files for the GIMP
gimp-help-ru - Russian help files for the GIMP
gimp-script-ISONoiseReduction - Gimp script for reducing sensor noise
at high ISO values
gimp-plugin-gutenprint - GIMP plug-in for gutenprint [...]
```

Символ «^» в поисковом выражении, указывает на то, что необходимо 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.ru>
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.
```

При поиске с помощью `apt-cache` можно использовать русскую подстроку. В этом случае будут найдены пакеты, имеющие описание на русском языке.

8.3.3 Установка или обновление пакета

Установка пакета с помощью APT выполняется командой:

```
# apt-get install <имя_пакета>
```

Примечание. Перед установкой и обновлением пакетов необходимо 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 пакеты, требующие для работы другие, пока еще не установленные. В этом случае он определяет, какие пакеты необходимо установить, и устанавливает их, пользуясь всеми доступными репозиториями.

Установка пакета gimp командой `apt-get install gimp` приведет к следующему диалогу с APT (если пакет еще не установлен):

```
# 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.
Необходимо 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.

Например, если пакет gimp установлен и в репозитории нет обновлённой версии этого пакета, то вывод команды `apt-get install gimp` будет таким:

```
# apt-get install gimp
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Последняя версия gimp уже установлена.
0 будет обновлено, 0 новых установлено, 0 пакетов будет удалено и 2262 не будет обновлено.
```

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 Рабочая станция», и `apt-get` в таком случае откажется выполнять операции установки, удаления или обновления.

Для восстановления целостности ОС «Альт Рабочая станция» необходимо 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
```

8.3.4 Удаление установленного пакета

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 необходимо 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.
Необходимо 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, необходимо 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
```

8.3.5 Обновление всех установленных пакетов

Полное обновление всех установленных в системе пакетов производится при помощи команд:

```
# apt-get update && apt-get dist-upgrade
```

Первая команда (`apt-get update`) обновит индексы пакетов. Вторая команда (`apt-get dist-upgrade`) позволяет обновить только те установленные пакеты, для которых в репозиториях, перечисленных в `/etc/apt/sources.list`, имеются новые версии.

В случае обновления всего дистрибутива APT проведёт 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.

Примечание. Команда `apt-get dist-upgrade` обновит систему, но ядро ОС не будет обновлено.

8.3.6 Обновление ядра

Для обновления ядра ОС необходимо выполнить команду:

```
# update-kernel
```

Примечание. Если индексы пакетов сегодня еще не обновлялись перед выполнением команды `update-kernel` необходимо выполнить команду `apt-get update`.

Команда `update-kernel` обновляет и модули ядра, если в репозитории обновилось что-то из модулей без обновления ядра.

Новое ядро загрузится только после перезагрузки системы.

8.4 Единая команда управления пакетами (epm)

Основное назначение единой команды управления пакетами – унифицировать управление пакетами в дистрибутивах с разными пакетными менеджерами. Утилита `epm` упрощает процедуру управления пакетами, может использоваться в скриптах и установщиках, сервисных программах, в повседневном администрировании различных систем. В `epm` добавлены типовые операции, которые в случае использования apt потребовали бы ввода более одной команды.

Единая команда управления пакетами включает в себя следующую функциональность:

- управление пакетами (установка/удаление/поиск);
- управление репозиториями (добавление/удаление/обновление/список);
- управление системными сервисами (включение/выключение/список).

Список поддерживаемых форматов пакетов: rpm, deb, tgz, tbz, tbz2, apk, pkg.gz.

Примечание. Установка утилиты `epm`, если она еще не установлена, выполняется ко-

мандой:

```
# apt-get install eepm
```

Подробную информацию об утилите epm и её опциях можно получить, выполнив команду:

```
$ epm --help
```

Ниже описаны лишь некоторые возможности утилиты `epm`.

Установка пакета из репозитория или из локального файла в систему:

```
# epm install <имя_пакета>
```

Примечание. Если пакет создан сторонним поставщиком, то при его установке командой `epm install` не будут выполнены установочные скрипты из пакета. Это предохраняет систему от повреждения, но может привести к тому, что пакет не заработает. Вернуть стандартное поведение можно добавлением `--scripts`:

```
# epm install --scripts <имя_пакета>
```

Установить сторонние программы безопасным и простым способом:

```
# epm play <имя_программы>
```

Список программ, которые можно установить данной командой, можно просмотреть, выполнив команду:

```
$ epm play
Available applications (for current arch x86_64):
  64gram               - 64Gram (unofficial Telegram Desktop)
   aimp                     - AIMP (Wine based audio player) from the
official site
  aksusbd               - Sentinel LDK daemon (HASP) from the official
site
  …
  zerotier-one          - ZeroTier - A Smart Ethernet Switch for Earth
from the official site
  zoom                 - Zoom client from the official site
```

Команда `epm play` требует наличия доступа в сеть Интернет.

Примечание. Для некоторых сторонних rpm-пакетов написаны дополнительные правила для перепаковки (при перепаковке пакета создаётся пакет, учитывающий, что нужно для работы исходного пакета). Установить такие пакеты можно, выполнив команду:

```
# epm install --repack <имя_пакета>
```

Для deb-пакетов ключ `--repack` применяется автоматически.

Удаление пакета из системы:

```
# epm remove <имя_пакета>
```

Поиск пакета в репозитории:

```
# epm search <текст>
```

Получить список установленных пакетов:

```
$ epm list
```

Удалить пакеты, от которых не зависят какие-либо другие пакеты, установленные в системе:

```
# epm autoremove
```

Обновить все установленные пакеты и ядро ОС:

```
# epm full-upgrade
```

9 ОБЩИЕ ПРИНЦИПЫ РАБОТЫ ОС

Работа с операционной средой заключается в вводе определенных команд (запросов) к операционной среде и получению на них ответов в виде текстового отображения.

Основой операционной среды является операционная система.

Операционная система (ОС) – совокупность программных средств, организующих согласованную работу операционной среды с аппаратными устройствами компьютера (процессор, память, устройства ввода-вывода и т. д.).

Диалог с ОС осуществляется посредством командных интерпретаторов и системных библиотек.

Каждая системная библиотека представляет собой набор программ, динамически вызываемых операционной системой.

Командные интерпретаторы – особый род специализированных программ, позволяющих осуществлять диалог с ОС посредством команд.

Для удобства пользователей при работе с командными интерпретаторами используются интерактивные рабочие среды (далее – ИРС), предоставляющие пользователю удобный интерфейс для работы с ОС.

В самом центре ОС изделия находится управляющая программа, называемая ядром. В ОС изделия используется новейшая модификация «устойчивого» ядра Linux – версия 5.10.

Ядро взаимодействует с компьютером и периферией (дисками, принтерами и т. д.), распределяет ресурсы и выполняет фоновое планирование заданий.

Другими словами, ядро ОС изолирует пользователя от сложностей аппаратуры компьютера, командный интерпретатор от ядра, а ИРС от командного интерпретатора.

9.1 Процессы и файлы

ОС «Альт Рабочая станция» 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, который представляет собой, как было сказано выше, 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.

9.1.1 Процессы функционирования ОС

Все программы, которые выполняются в текущий момент времени, называются процессами. Процессы можно разделить на два основных класса: системные процессы и пользовательские процессы. Системные процессы – программы, решающие внутренние задачи ОС, например, организацию виртуальной памяти на диске или предоставляющие пользователям те или иные сервисы (процессы-службы).

Пользовательские процессы – процессы, запускаемые пользователем из командного интерпретатора для решения задач пользователя или управления системными процессами. Linux изначально разрабатывался как многозадачная система. Он использует технологии, опробованные и отработанные другими реализациями UNIX, которые существовали ранее.

Фоновый режим работы процесса – режим, когда программа может работать без взаимодействия с пользователем. В случае необходимости интерактивной работы с пользователем (в общем случае) процесс будет «остановлен» ядром, и работа его продолжится только после переведения его в «нормальный» режим работы.

9.1.2 Файловая система ОС

В ОС использована файловая система Linux, которая в отличие от файловых систем DOS и Windows(™) является единым деревом. Корень этого дерева – каталог, называемый root (рут), и обозначаемый «/». Части дерева файловой системы могут физически располагаться в разных разделах разных дисков или вообще на других компьютерах, – для пользователя это прозрачно. Процесс присоединения файловой системы раздела к дереву называется монтированием, удаление – размонтированием. Например, файловая система CD-ROM в изделии монтируется по умолчанию в каталог /media/cdrom (путь в изделии обозначается с использованием «/», а не «\», как в DOS/ Windows). Текущий каталог обозначается «./».

Файловая система изделия содержит каталоги первого уровня:

- /bin (командные оболочки (shell), основные утилиты);
- /boot (содержит ядро системы);
- /dev (псевдофайлы устройств, позволяющие работать с ними напрямую);
- /etc (файлы конфигурации);
- /home (личные каталоги пользователей);
- /lib (системные библиотеки, модули ядра);
- /lib64 (64-битные системные библиотеки);
- /media (каталоги для монтирования файловых систем сменных устройств);
- /mnt (каталоги для монтирования файловых систем сменных устройств и внешних файловых систем);

- /proc (файловая система на виртуальном устройстве, ее файлы содержат информацию о текущем состоянии системы);
- /root (личный каталог администратора системы);
- /sbin (системные утилиты);
- /sys (файловая система, содержащая информацию о текущем состоянии системы);
- /usr (программы и библиотеки, доступные пользователю);
- /var (рабочие файлы программ, очереди, журналы);
- /tmp (временные файлы).

9.1.3 Организация файловой структуры

Система домашних каталогов пользователей помогает организовывать безопасную работу пользователей в многопользовательской системе. Вне своего домашнего каталога пользователь обладает минимальными правами (обычно чтение и выполнение файлов) и не может нанести ущерб системе, например, удалив или изменив файл.

Кроме файлов, созданных пользователем, в его домашнем каталоге обычно содержатся персональные конфигурационные файлы некоторых программ.

Маршрут (путь) – это последовательность имён каталогов, представляющий собой путь в файловой системе к данному файлу, где каждое следующее имя отделяется от предыдущего наклонной чертой (слэшем). Если название маршрута начинается со слэша, 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 символам:

- строчные и ПРОПИСНЫЕ буквы. Следует обратить внимание на то, что регистр всегда имеет значение;
- цифры;
- символ подчеркивания (_);
- точка (.).

Для удобства работы можно использовать точку (.)для отделения имени файла от расширения файла. Данная возможность может быть необходима пользователям или некоторым программам, но не имеет значение для shell.

9.1.4 Иерархическая организация файловой системы

Каталог /:

/boot – место, где хранятся файлы необходимые для загрузки ядра системы;

/lib – здесь располагаются файлы динамических библиотек, необходимых для работы большей части приложений и подгружаемые модули ядра;

/lib64 – здесь располагаются файлы 64-битных динамических библиотек, необходимых для работы большей части приложений;

/bin – минимальный набор программ необходимых для работы в системе;

/sbin – набор программ для административной работы с системой (программы необходимые только суперпользователю);

/home – здесь располагаются домашние каталоги пользователей;

/etc – в данном каталоге обычно хранятся 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 системы инициализации SysVinit;

/etc/passwd – база данных пользователей, в которой содержится информация об имени пользователя, его настоящем имени, личном каталоге, закодированный пароль и другие данные;

/etc/shadow – теневая база данных пользователей. При этом информация из файла /etc/passwd перемещается в /etc/shadow, который недоступен по чтению 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`;

/dev – в этом каталоге находятся файлы устройств. Файлы в `/dev` создаются сервисом `udev`;

/usr – обычно файловая система `/usr` достаточно большая по объему, так как все программы установлены именно здесь. Вся информация в каталоге `/usr` помещается туда во время установки системы. Отдельно устанавливаемые пакеты программ и другие файлы размещаются в каталоге `/usr/local`. Некоторые подкаталоги системы `/usr` рассмотрены ниже;

/usr/bin – практически все команды, хотя некоторые находятся в `/bin` или в `/usr/local/bin`;

/usr/sbin – команды, используемые при администрировании системы и не предназначенные для размещения в файловой системе `root`;

/usr/local – здесь рекомендуется размещать файлы, установленные без использования пакетных менеджеров, внутренняя организация каталогов практически такая же, как и корневого каталога;

/usr/man – каталог, где хранятся файлы справочного руководства `man`;

/usr/share – каталог для размещения общедоступных файлов большей части приложений.

Каталог `/var`:

/var/log – место, где хранятся файлы аудита работы системы и приложений;

/var/spool – каталог для хранения файлов находящих в очереди на обработку для того или иного процесса (очередь на печать, отправку почты и т. д.);

/tmp – временный каталог необходимый некоторым приложениям;

/proc – файловая система `/proc` является виртуальной и в действительности она не существует на диске. Ядро создает её в памяти компьютера. Система `/proc` предоставляет информацию о системе.

9.1.5 Имена дисков и разделов

Все физические устройства компьютера отображаются в каталог `/dev` файловой системы изделия (об этом – ниже). Диски (в том числе IDE/SATA/SCSI жёсткие 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 порядке обнаружения системой.

Раздел диска обозначается числом после его имени. Например, /dev/sdb4 – четвертый раздел второго диска.

9.1.6 Разделы, необходимые для работы ОС

Для работы ОС необходимо создать на жестком диске (дисках) 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 свободного места на диске много, то можно создать отдельные разделы для каталогов `/usr`, `/home`, `/var`.

9.1.7 Команды

Далее приведены основные команды, использующиеся в ОС «Альт Рабочая станция»:

- ar – создание и работа с библиотечными архивами;
- at – формирование или удаление отложенного задания;
- awk – язык обработки строковых шаблонов;
- batch – планирование команд в очереди загрузки;
- bc – строковый калькулятор;
- chfn – управление информацией учетной записи (имя, описание);
- chsh – управление выбором командного интерпретатора (по умолчанию – для учётной 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;
- gettext – получение строки интернационализации из каталогов перевода;
- grep – вывод строки, содержащей шаблон поиска;
- 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;
- killall – удаление процессов по имени;
- lpr – система печати;
- ls – вывод содержимого каталога;
- lsb_release – вывод информации о дистрибутиве;
- m4 – запуск макропроцессора;
- md5sum – генерация и проверка MD5-сообщения;
- mknod – создание файла специального типа;
- mktemp – генерация уникального имени файла;
- more – постраничный вывод содержимого файла;
- mount – монтирование ФС;
- msgfmt – создание объектного файла сообщений из файла сообщений;
- newgrp – смена идентификатора группы;
- nice – изменение приоритета процесса перед его запуском;

- nohup – работа процесса после выхода из системы;
- od – вывод содержимого файла в восьмеричном и других видах;
- passwd – смена пароля учетной записи;
- patch – применение файла описания изменений к оригинальному файлу;
- pidof – вывод идентификатора процесса по его имени;
- ps – вывод информации о процессах;
- renice – изменение уровня приоритета процесса;
- sed – строковый редактор;
- sendmail – транспорт системы электронных сообщений;
- sh – командный интерпретатор;
- shutdown – команда останова системы;
- su – изменение идентификатора запускаемого процесса;
- sync – сброс системных буферов на носители;
- tar – файловый архиватор;
- umount – размонтирование ФС;
- useradd – создание новой учетной записи или обновление существующей;
- userdel – удаление учетной записи и соответствующих файлов окружения;
- usermod – модификация информации об учетной записи;
- w – список пользователей, кто в настоящий момент работает в системе и с какими файлами;
- who – вывод списка пользователей системы.

Узнать об опциях команд можно с помощью команды `man`.

10 РАБОТА С НАИБОЛЕЕ ЧАСТО ИСПОЛЬЗУЕМЫМИ КОМПОНЕНТАМИ

10.1 Командные оболочки (интерпретаторы)

Для управления ОС используется командные интерпретаторы (shell).

Зайдя в систему, можно увидеть приглашение – строку, содержащую символ «$» (далее, этот символ будет обозначать командную строку). Программа ожидает ввода команд. Роль командного интерпретатора – передавать команды пользователя операционной системе. При помощи командных интерпретаторов можно писать небольшие программы – сценарии (скрипты). В Linux доступны следующие командные оболочки:

bash – самая распространённая оболочка под linux. Она ведет историю команд и предоставляет возможность их редактирования.

pdksh – клон korn shell, хорошо известной оболочки в UNIX(™) системах.

Оболочкой по умолчанию является «Bash» (Bourne Again Shell) Проверить, какая оболочка используется можно, выполнив команду:

```
$ echo $SHELL
```

У каждой оболочки свой синтаксис. Все примеры в дальнейшем построены с использованием оболочки Bash.

10.1.1 Командная оболочка Bash

В Bash имеется несколько приемов для работы со строкой команд. Например, используя клавиатуру, можно:

<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 <↑> и <↓>. Чтобы найти конкретную команду в списке набранных, не пролистывая всю историю, необходимо набрать <Ctrl> + <R> и начать вводить символы ранее введенной команды.

Для просмотра истории команд можно воспользоваться командой history. Команды, присутствующие в истории, отображаются в списке пронумерованными. Чтобы запустить конкретную команду необходимо набрать:

```
!номер команды
```

Если ввести:

```
!!
```

запустится последняя, из набранных команд.

В Bash имеется возможность самостоятельного завершения имен команд из общего списка команд, что облегчает работу при вводе команд, в случае, если имена программ и команд слишком длинны. При нажатии клавиши <Tab> Bash завершает имя команды, программы или каталога, если не существует нескольких альтернативных вариантов. Например, чтобы использовать программу декомпрессии `gunzip`, можно набрать следующую команду:

```
$ gu
```

Затем нажать <Tab>. Так как в данном случае существует несколько возможных вариантов завершения команды, то необходимо повторно нажать клавишу <Tab>, чтобы получить список имен, начинающихся с gu.

В предложенном примере можно получить следующий список:

```
$ gu
guile gunzip gupnp-binding-tool
```

Если набрать: n (`gunzip` – это единственное имя, третьей буквой которого является «n»), а затем нажать клавишу <Tab>, то оболочка самостоятельно дополнит имя. Чтобы запустить команду нужно нажать <Enter>.

Программы, вызываемые из командной строки, Bash ищет в каталогах, определяемых в системной переменной PATH. По умолчанию в этот перечень каталогов не входит текущий каталог, обозначаемый ./ (точка слеш) (если только не выбран один из двух самых слабых уровней защиты). Поэтому, для запуска программы из текущего каталога, необходимо использовать команду (в примере запускается команда prog):

```
./prog
```

10.1.2 Базовые команды оболочки Bash

Все команды, приведенные ниже, могут быть запущены в режиме консоли. Для получения более подробной информации следует использовать команду `man`. Пример:

```
$ man ls
```

10.1.2.1 Учетные записи пользователей

Команда su

Команда `su` позволяет изменить «владельца» текущего сеанса (сессии) без необходимости завершать сеанс и открывать новый.

Синтаксис:

```
su [ОПЦИИ...] [ПОЛЬЗОВАТЕЛЬ]
```

Команду можно применять для замены текущего пользователя на любого другого, но чаще всего она используется для получения пользователем прав суперпользователя (root).

При вводе команды `su -` будет запрошен пароль суперпользователя (root), и, в случае ввода корректного пароля, пользователь получит привилегии суперпользователя. Чтобы вернуться к правам пользователя, необходимо ввести команду:

```
exit
```

Команда id

Команда `id` выводит информацию о пользователе и группах, в которых он состоит, для заданного пользователя или о текущем пользователе (если ничего не указано).

Синтаксис:

```
id [параметры] [ПОЛЬЗОВАТЕЛЬ]
```

Команда passwd

Команда `passwd` меняет (или устанавливает) пароль, связанный с входным_именем пользователя.

Обычный пользователь может менять только пароль, связанный с его собственным входным_именем.

Команда запрашивает у обычных пользователей старый пароль (если он был), а затем дважды запрашивает новый. Новый пароль должен соответствовать техническим требованиям к паролям, заданным администратором системы.

10.1.2.2 Основные операции с файлами и каталогами

Команда ls

Команда `ls` (list) выдает список файлов каталога.

Синтаксис:

```
ls [опции...] [файл...]
```

Основные опции:

`-a` – просмотр всех файлов, включая скрытые;

`-l` – отображение более подробной информации;

`-R` – выводить рекурсивно информацию о подкаталогах.

Команда cd

Команда `cd` предназначена для смены каталога. Команда работает как с абсолютными, так и с относительными путями. Если каталог не указан, используется значение переменной окружения `$HOME` (домашний каталог пользователя). Если каталог задан полным маршрутным именем, он становится текущим. По отношению к новому каталогу нужно иметь право на выполнение, которое в данном случае трактуется как разрешение на поиск.

Синтаксис:

```
cd [-L|-P] [каталог]
```

Если в качестве аргумента задано «-», то это эквивалентно `$OLDPWD`. Если переход был осуществлен по переменной окружения `$CDPATH` или в качестве аргумента был задан «-» и смена

каталога была успешной, то абсолютный путь нового рабочего каталога будет выведен на стандартный вывод.

Примеры:

- находясь в домашнем каталоге перейти в его подкаталог `docs/` (относительный путь):

```
$ cd docs/
```

- сделать текущим каталог `/usr/bin` (абсолютный путь):

```
$ cd /usr/bin/
```

- сделать текущим родительский каталог:

```
$ cd ..
```

- вернуться в предыдущий каталог:

```
$ cd -
```

- сделать текущим домашний каталог:

```
$ cd
```

Команда pwd

Команда `pwd` выводит абсолютный путь текущего (рабочего) каталога.

Синтаксис:

```
pwd [-L|-P]
```

Опции:

`-P` – не выводить символические ссылки;

`-L` – выводить символические ссылки.

Команда rm

Команда `rm` служит для удаления записей о файлах. Если заданное имя было последней ссылкой на файл, то файл уничтожается.

Синтаксис:

```
rm [опции...] имя_файла
```

Основные опции:

`-f` – не запрашивать подтверждения;

`-i` – запрашивать подтверждение;

`-r`, `-R` – рекурсивно удалять содержимое указанных каталогов.

Пример. Удалить все файлы `html` в каталоге `~/html`:

```
$ rm -i ~/html/*.html
```

Команда mkdir

Команда `mkdir` позволяет создать каталог.

Синтаксис:

```
mkdir [-p] [-m права] [каталог...]
```

Команда rmdir

Команда `rmdir` удаляет записи, соответствующие указанным пустым каталогам.

Синтаксис:

`rmdir [-p] [`*`каталог...`*`]`

Основные опции:

`-p` – удалить каталог и его потомки.

Команда `rmdir` часто заменяется командой `rm -rf`, которая позволяет удалять каталоги, даже если они не пусты.

Команда cp

Команда `cp` предназначена для копирования файлов из одного в другие каталоги.

Синтаксис:

`cp [-fip] [`*`исх_файл`*`] [`*`цел_файл`*`]`

`cp [-fip] [`*`исх_файл...`*`] [`*`каталог`*`]`

`cp [-R] [[-H] | [-L] | [-P]] [-fip] [`*`исх_файл...`*`] [`*`каталог`*`]`

Основные опции:

`-p` – сохранять по возможности времена изменения и доступа к файлу, владельца и группу, права доступа;

`-i` – запрашивать подтверждение перед копированием в существующие файлы;

`-r`, `-R` – рекурсивно копировать содержимое каталогов.

Команда mv

Команда `mv` предназначена для перемещения файлов.

Синтаксис:

`mv [-fi] [`*`исх_файл...`*`] [`*`цел_файл`*`]`

`mv [-fi] [`*`исх_файл...`*`] [`*`каталог`*`]`

В первой синтаксической форме, характеризующейся тем, что последний операнд не является ни каталогом, ни символической ссылкой на каталог, `mv` перемещает исх_файл в цел_файл (происходит переименование файла).

Во второй синтаксической форме `mv` перемещает исходные файлы в указанный каталог под именами, совпадающими с краткими именами исходных файлов.

Основные опции:

`-f` – не запрашивать подтверждения перезаписи существующих файлов;

`-i` – запрашивать подтверждение перезаписи существующих файлов.

Команда cat

Команда `cat` последовательно выводит содержимое файлов.

Синтаксис:

`cat [опции...] [файл...]`

Основные опции:

`-n`, `--number` – нумеровать все строки при выводе;

`-E`, `--show-ends` – показывать $ в конце каждой строки.

Если файл не указан, читается стандартный ввод. Если в списке файлов присутствует имя «-», вместо этого файла читается стандартный ввод.

Команда head

Команда `head` выводит первые 10 строк каждого файла на стандартный вывод.

Синтаксис:

```
head [опции...] [файл...]
```

Основные опции:

`-n`, `--lines=[-]K` – вывести первые К строк каждого файла, а не первые 10;

`-q`, `--quiet` – не печатать заголовки с именами файлов.

Команда less

Команда `less` позволяет постранично просматривать текст (для выхода необходимо нажать <q>).

Синтаксис:

```
less имя_файла
```

Команда grep

Команда `grep` имеет много опций и предоставляет возможности поиска символьной строки в файле.

Синтаксис:

```
grep шаблон_поиска файл
```

10.1.2.3 Поиск файлов

Команда find

Команда `find` предназначена для поиска всех файлов, начиная с корневого каталога. Поиск может осуществляться по имени, типу или владельцу файла.

Синтаксис:

```
find [-H] [-L] [-P] [-Оуровень] [-D help|tree|search|stat|rates|opt|
exec] [путь…] [выражение]
```

Ключи для поиска:

`-name` – поиск по имени файла;

`-type` – поиск по типу f=файл, d=каталог, l=ссылка(lnk);

`-user` – поиск по владельцу (имя или UID).

Когда выполняется команда `find`, можно выполнять различные действия над найденными файлами. Основные действия:

-exec команда \; – выполнить команду. Запись команды должна заканчиваться экранированной точкой с запятой. Строка «{}» заменяется текущим маршрутным именем файла;

-execdir команда \; – то же самое что и exec, но команда вызывается из подкаталога, содержащего текущий файл;

-ok команда – эквивалентно -exec за исключением того, что перед выполнением команды запрашивается подтверждение (в виде сгенерированной командной строки со знаком вопроса в конце) и она выполняется только при ответе: y;

-print – вывод имени файла на экран.

Путем по умолчанию является текущий подкаталог. Выражение по умолчанию -print.

Примеры:

- найти в текущем каталоге обычные файлы (не каталоги), имя которых начинается с символа «~»:

```
$ find . -type f -name "~*" -print
```

- найти в текущем каталоге файлы, измененные позже, чем файл file.bak:

```
$ find . -newer file.bak -type f -print
```

- удалить все файлы с именами a.out или *.o, доступ к которым не производился в течение недели:

```
$ find / \( -name a.out -o -name '*.o' \) \ -atime +7 -exec rm {} \;
```

- удалить из текущего каталога и его подкаталогов все файлы нулевого размера, запрашивая подтверждение:

```
$ find . -size 0c -ok rm {} \;
```

Команда whereis

Команда whereis сообщает путь к исполняемому файлу программы, ее исходным файлам (если есть) и соответствующим страницам справочного руководства.

Синтаксис:

```
whereis [опции...] имя_файла
```

Опции:

-b – вывод информации только об исполняемых файлах;

-m – вывод информации только о страницах справочного руководства;

-s – вывод информации только об исходных файлах.

10.1.2.4 Мониторинг и управление процессами

Команда ps

Команда ps отображает список текущих процессов.

Синтаксис:

```
ps [-aA] [-defl] [-G список] [-o формат...] [-p список] [-t список] [-U список] [-g список] [-n список] [-u список]
```

По умолчанию выводится информация о процессах с теми же действующим UID и управляющим терминалом, что и у подающего команду пользователя.

Основные опции:

`-a` – вывести информацию о процессах, ассоциированных с терминалами;

`-f` – вывести «полный» список;

`-l` – вывести «длинный» список;

`-p список` – вывести информацию о процессах с перечисленными в списке PID;

`-u список` – вывести информацию о процессах с перечисленными идентификаторами или именами пользователей.

Команда kill

Команда `kill` позволяет прекратить исполнение процесса или передать ему сигнал.

Синтаксис:

```
kill [-s] [сигнал] [идентификатор] [...]
kill [-l] [статус_завершения]
kill [-номер_сигнала] [идентификатор] [...]
```

Идентификатор – PID ведущего процесса задания или номер задания, предварённый знаком «%».

Основные опции:

`-l` – вывести список поддерживаемых сигналов;

`-s сигнал`, `-сигнал` – послать сигнал с указанным именем.

Если обычная команда `kill` не дает желательного эффекта, необходимо использовать команду `kill` с параметром `-9`:

```
$ kill -9 PID_номер
```

Команда df

Команда `df` показывает количество доступного дискового пространства в файловой системе, в которой содержится файл, переданный как аргумент. Если ни один файл не указан, показывается доступное место на всех смонтированных файловых системах. Размеры по умолчанию указаны в блоках по 1КБ по умолчанию.

Синтаксис:

```
df [опция...] [файл...]
```

Основные опции:

`-total` – подсчитать общий объем в конце;

`-h`, `--human-readable` – печатать размеры в удобочитаемом формате (например, 1K, 234M, 2G).

Команда du

Команда `du` подсчитывает использование диска каждым файлом, для каталогов подсчет происходит рекурсивно.

Синтаксис:

```
du [опции][файл...]
```

Основные опции:

`-a`, `--all` – выводить общую сумму для каждого заданного файла, а не только для каталогов;

`-c`, `--total` – подсчитать общий объем в конце. Может быть использовано для выяснения суммарного использования дискового пространства для всего списка заданных файлов;

`-d`, `--max-depth=N` – выводить объем для каталога (или файлов, если указано `--all`) только если она на N или менее уровней ниже аргументов командной строки;

`-S`, `--separate-dirs` – выдавать отдельно размер каждого каталога, не включая размеры подкаталогов;

`-s`, `--summarize` – отобразить только сумму для каждого аргумента.

Команда which

Команда `which` отображает полный путь к указанным командам или сценариям.

Синтаксис:

```
which [опции] [--] имя_программы [...]
```

Основные опции:

`-a`, `--all` – выводит все совпавшие исполняемые файлы по содержимому в переменной окружения `$PATH`, а не только первый из них;

`-c`, `--total` – подсчитать общий объем в конце. Может быть использовано для выяснения суммарного использования дискового пространства для всего списка заданных файлов;

`-d`, `--max-depth=N` – выводить объем для каталога (или файлов, если указано `--all`) только если она на N или менее уровней ниже аргументов командной строки;

`-S`, `--separate-dirs` – выдавать отдельно размер каждого каталога, не включая размеры подкаталогов;

`--skip-dot` – пропускает все каталоги из переменной окружения `$PATH`, которые начинаются с точки.

10.1.2.5 Использование многозадачности

ОС «Альт Рабочая станция» – многозадачная система.

Для того чтобы запустить программу в фоновом режиме, необходимо набрать «&» после имени программы. После этого оболочка дает возможность запускать другие приложения.

Так как некоторые программы интерактивны – их запуск в фоновом режиме бессмысленен. Подобные программы просто остановятся, если их запустить в фоновом режиме.

Можно также запускать нескольких независимых сеансов. Для этого в консоли необходимо набрать <Alt> и одну из клавиш, находящихся в интервале от <F1> до <F6>. На экране появится новое приглашение системы, и можно открыть новый сеанс.

Команда bg

Команда `bg` используется для того, чтобы перевести задание на задний план.

Синтаксис:

```
bg [идентификатор ...]
```

Идентификатор – PID ведущего процесса задания или номер задания, предварённый знаком «%».

Команда fg

Команда `fg` позволяет перевести задание на передний план.

Синтаксис:

```
fg [идентификатор ...]
```

Идентификатор – PID ведущего процесса задания или номер задания, предварённый знаком «%».

10.1.2.6 Сжатие и упаковка файлов

Команда tar

Сжатие и упаковка файлов выполняется с помощью команды `tar`, которая преобразует файл или группу файлов в архив без сжатия (tarfile).

Упаковка файлов в архив чаще всего выполняется следующей командой:

```
$ tar -cf [имя создаваемого файла архива] [упаковываемые файлы и/или каталоги]
```

Пример использования команды упаковки архива:

```
$ tar -cf moi_dokumenti.tar Docs project.tex
```

Распаковка содержимого архива в текущий каталог выполняется командой:

```
$ tar -xf [имя файла архива]
```

Для сжатия файлов используются специальные программы сжатия: `gzip`, `bzip2` и `7z`.

10.2 Стыкование команд в системе

10.2.1 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>. Сокращённое название сигнала конца текста – EOT (end of text).

10.2.2 Перенаправление ввода и вывода

При необходимости можно перенаправить стандартный вывод, используя символ > и стандартный ввод, используя символ <.

Фильтр (filter) – программа, которая читает данные из стандартного ввода, некоторым образом их обрабатывает и результат направляет на стандартный вывод. Когда применяется перенаправление, в качестве стандартного ввода и вывода могут выступать файлы. Как указывалось выше, по умолчанию, `stdin` и `stdout` относятся к клавиатуре и к экрану соответственно. 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.

10.2.3 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
```

Пример стыкования нескольких команд. Команда head – является фильтром следующего свойства: она выводит первые строки из входного потока (в примере на вход будет подан выход от нескольких состыкованных команд). Если необходимо вывести на экран последнее по алфавиту имя файла в текущем каталоге, можно использовать следующую команду:

```
$ ls | sort -r | head -1 notes
```

где команда `head -1` выводит на экран первую строку получаемого ей входного потока строк (в примере поток состоит из данных от команды `ls`), отсортированных в обратном алфавитном порядке.

10.2.4 Не деструктивное перенаправление вывода

Эффект от использования символа > для перенаправления вывода файла является деструктивным; то есть, 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.

10.3 Средства управления дискреционными правами доступа

10.3.1 Команда chmod

Команда `chmod` предназначена для изменения прав доступа файлов и каталогов.

Синтаксис:

```
chmod [ОПЦИЯ]... РЕЖИМ[,РЕЖИМ]... [Файл...]
chmod [ОПЦИЯ]... --reference=ИФАЙЛ ФАЙЛ...
```

Основные опции:

`-R` – рекурсивно изменять режим доступа к файлам, расположенным в указанных каталогах;

`--reference=ИФАЙЛ` – использовать режим файла ИФАЙЛ.

Команда `chmod` изменяет права доступа каждого указанного файла в соответствии с правами доступа, указанными в параметре режим, который может быть представлен как в символьном виде, так и в виде восьмеричного, представляющего битовую маску новых прав доступа.

Формат символьного режима следующий:

```
[ugoa...][[+-=][разрешения...]...]
```

Здесь разрешения – это ноль или более букв из набора «rwxXst» или одна из букв из набора «ugo».

Каждый аргумент – это список символьных команд изменения прав доступа, разделеных запятыми. Каждая такая команда начинается с нуля или более букв «ugoa», комбинация которых указывает, чьи права доступа к файлу будут изменены: пользователя, владеющего файлом (u), пользователей, входящих в группу, к которой принадлежит файл (g), остальных пользователей (o) или всех пользователей (a). Если не задана ни одна буква, то автоматически будет использована буква «a», но биты, установленные в umask, не будут затронуты.

Оператор «+» добавляет выбранные права доступа к уже имеющимся у каждого файла, «-» удаляет эти права, «=» присваивает только эти права каждому указанному файлу.

Буквы «rwxXst» задают биты доступа для пользователей: «r» – чтение, «w» – запись, «x» – выполнение (или поиск для каталогов), «X» – выполнение/поиск, только если это каталог или же файл с уже установленным битом выполнения, «s» – задать ID пользователя и группы при выполнении, «t» – запрет удаления.

Числовой режим состоит из не более четырех восьмеричных цифр (от нуля до семи), которые складываются из битовых масок с разрядами «4», «2» и «1». Любые пропущенные разряды дополняются лидирующими нулями:

- первый разряд выбирает установку идентификатора пользователя (setuid) (4) или идентификатора группы (setgid) (2) или sticky-бита (1);
- второй разряд выбирает права доступа для пользователя, владеющего данным файлом: чтение (4), запись (2) и исполнение (1);
- третий разряд выбирает права доступа для пользователей, входящих в данную группу, с тем же смыслом, что и у второго разряда;
- четвертый разряд выбирает права доступа для остальных пользователей (не входящих в данную группу), опять с тем же смыслом.

Примеры:

- установить права, позволяющие владельцу читать и писать в файл `f1`, а членам группы и прочим пользователям только читать. Команду можно записать двумя способами:

```
$ chmod 644 f1
```

```
$ chmod u=rw,go=r f1
```

- позволить всем выполнять файл `f2`:

```
$ chmod +x f2
```

- запретить удаление файла `f3`:

```
$ chmod+t f3
```

- дать всем права на чтение запись и выполнение, а также на переустановку идентификатора группы при выполнении файла `f4`:

```
$ chmod =rwx,g+s f4
$ chmod 2777 f4
```

10.3.2 Команда chown

Команда `chown` изменяет владельца и/или группу для каждого заданного файла.

Синтаксис:

```
chown [КЛЮЧ]…[ВЛАДЕЛЕЦ][:[ГРУППА]] ФАЙЛ
```

Изменить владельца может только владелец файла или суперпользователь. Владелец не изменяется, если он не задан в аргументе. Группа также не изменяется, если не задана, но если после символьного ВЛАДЕЛЬЦА стоит символ «:», подразумевается изменение группы на основную группу текущего пользователя. Поля ВЛАДЕЛЕЦ и ГРУППА могут быть как числовыми, так и символьными.

Примеры:

- поменять владельца `/u` на пользователя `test`:

```
$ chown test /u
```

- поменять владельца и группу `/u`:

```
$ chown test:staff /u
```

- поменять владельца `/u` и вложенных файлов на `test`:

```
$ chown -hR test /u
```

10.3.3 Команда chgrp

Команда `chgrp` изменяет группу для каждого заданного файла.

Синтаксис:

```
chgrp [ОПЦИИ] ГРУППА ФАЙЛ
```

Основные опции:

`-R` – рекурсивно изменять файлы и каталоги;

`--reference=ИФАЙЛ` – использовать группу файла ИФАЙЛ.

10.3.4 Команда umask

Команда `umask` задает маску режима создания файла в текущей среде командного интерпретатора равной значению, задаваемому операндом режим. Эта маска влияет на начальное значение битов прав доступа всех создаваемых далее файлов.

Синтаксис:

```
umask [-p] [-S] [режим]
```

Пользовательской маске режима создания файлов присваивается указанное восьмеричное значение. Три восьмеричные цифры соответствуют правам на чтение/запись/выполнение для владельца, членов группы и прочих пользователей соответственно. Значение каждой заданной в маске цифры вычитается из соответствующей «цифры», определенной системой при создании файла. Например, umask 022 удаляет права на запись для членов группы и прочих пользователей (у файлов, создававшихся с режимом 777, он оказывается равным 755; а режим 666 преобразуется в 644).

Если маска не указана, выдается ее текущее значение:

```
$ umask
0022
```

или то же самое в символьном режиме:

```
$ umask -S
u=rwx,g=rx,o=rx
```

Команда `umask` распознается и выполняется командным интерпретатором bash.

10.3.5 Команда chattr

Команда `chattr` изменяет атрибуты файлов на файловых системах ext3, ext4.

Синтаксис:

```
chattr [ -RVf ] [+-=aAcCdDeFijmPsStTux] [ -v версия ] <ФАЙЛЫ> …
```

Основные опции:

`-R` – рекурсивно изменять атрибуты каталогов и их содержимого. Символические ссылки игнорируются;

`-V` – выводит расширенную информацию и версию программы;

`-f` – подавлять сообщения об ошибках;

`-v версия` – установить номер версии/генерации файла.

Формат символьного режима:

```
+-=aAcCdDeFijmPsStTux
```

Оператор «+» означает добавление выбранных атрибутов к существующим атрибутам; «-» означает их снятие; «=» означает определение только этих указанных атрибутов для файлов.

Символы «aAcCdDeFijmPsStTux» указывают на новые атрибуты файлов:

- a – только добавление к файлу;
- A – не обновлять время последнего доступа (atime) к файлу;
- c – сжатый файл;
- C – отключение режима «Copy-on-write» для указанного файла;
- d – не архивировать (отключает создание архивной копии файла командой `dump`);
- D – синхронное обновление каталогов;
- e – включает использование extent при выделении места на устройстве (атрибут не может быть отключён с помощью `chattr`);
- F – регистронезависимый поиск в каталогах;
- i – неизменяемый файл (файл защищен от изменений: не может быть удалён или переименован, к этому файлу не могут быть созданы ссылки, и никакие данные не могут быть записаны в этот файл);
- j – ведение журнала данных (данные файла перед записью будут записаны в журнал ext3/ ext4);
- m – не сжимать;
- P – каталог с вложенными файлами является иерархической структурой проекта;
- s – безопасное удаление (перед удалением все содержимое файла полностью затирается «00»);
- S – синхронное обновление (аналогичен опции монтирования «sync» файловой системы);
- t – отключает метод tail-merging для файлов;
- T – вершина иерархии каталогов;
- u – неудаляемый (при удалении файла его содержимое сохраняется, это позволяет пользователю восстановить файл);

  x – прямой доступ к файлам (атрибут не может быть установлен с помощью `chattr`).

10.3.6 Команда lsattr

Команда `lsattr` выводит атрибуты файла расширенной файловой системы.

Синтаксис:

```
lsattr [ -RVadlpv ] <ФАЙЛЫ> …
```

Опции:

`-R` – рекурсивно изменять атрибуты каталогов и их содержимого. Символические ссылки игнорируются;

`-V` – выводит расширенную информацию и версию программы;

`-a` – просматривает все файлы в каталоге, включая скрытые файлы (имена которых начинаются с «.»);

`-d` – отображает каталоги так же, как и файлы вместо того, чтобы просматривать их содержимое;

`-l` – отображает параметры, используя длинные имена вместо одного символа;

`-p` – выводит номер проекта файла;

`-v` – выводит номер версии/генерации файла.

10.3.7 Команда getfacl

Команда `getfacl` выводит атрибуты файла расширенной файловой системы.

Синтаксис:

```
getfacl [ --aceEsRLPtpndvh ] <ФАЙЛ> …
```

Опции:

`-a` – вывести только ACL файла;

`-d` – вывести только ACL по умолчанию;

`-c` – не показывать заголовок (имя файла);

`-e` – показывать все эффективные права;

`-E` – не показывать эффективные права;

`-s` – пропускать файлы, имеющие только основные записи;

`-R` – для подкаталогов рекурсивно;

`-L` – следовать по символическим ссылкам, даже если они не указаны в командной строке;

`-P` – не следовать по символическим ссылкам, даже если они указаны в командной строке;

`-t` – использовать табулированный формат вывода;

`-p` – не удалять ведущие «/» из пути файла;

`-n` – показывать числовые значения пользователя/группы.

Формат вывода:

```
1: # file: somedir/
2: # owner: lisa
3: # group: staff
4: # flags: -s-
5: user::rwx
6: user:joe:rwx               #effective:r-x
7: group::rwx           #effective:r-x
8: group:cool:r-x
9: mask:r-x
10: other:r-x
11: default:user::rwx
```

```
12: default:user:joe:rwx #effective:r-x
13: default:group::r-x
14: default:mask:r-x
15: default:oter:---
```

Строки 1 – 3 указывают имя файла, владельца и группу владельцев.

В строке 4 указаны биты setuid (s), setgid (s) и sticky (t): либо буква, обозначающая бит, либо тире (-). Эта строка включается, если какой-либо из этих битов установлен, и опускается в противном случае, поэтому она не будет отображаться для большинства файлов.

Строки 5, 7 и 10 относятся к традиционным битам прав доступа к файлу, соответственно, для владельца, группы-владельца и всех остальных. Эти три элемента являются базовыми. Строки 6 и 8 являются элементами для отдельных пользователя и группы. Строка 9 – маска эффективных прав. Этот элемент ограничивает эффективные права, предоставляемые всем группам и отдельным пользователям. Маска не влияет на права для владельца файла и всех других. Строки 11 – 15 показывают ACL по умолчанию, ассоциированный с данным каталогом.

10.3.8 Команда setfacl

Команда `setfacl` изменяет ACL к файлам или каталогам. В командной строке за последовательностью команд идет последовательность файлов (за которой, в свою очередь, также может идти последовательность команд и так далее).

Синтаксис:

```
setfacl [-bkndRLPvh] [{-m|-x} acl_spec] [{-M|-X} acl_file] <ФАЙЛ> …
setfacl --restore=file
```

Опции:

`-b` – удалить все разрешенные записи ACL;

`-k` – удалить ACL по умолчанию;

`-n` – не пересчитывать маску эффективных прав, обычно `setfacl` пересчитывает маску (кроме случая явного задания маски) для того, чтобы включить ее в максимальный набор прав доступа элементов, на которые воздействует маска (для всех групп и отдельных пользователей);

`-d` – применить ACL по умолчанию;

`-R` – для подкаталогов рекурсивно;

`-L` – переходить по символическим ссылкам на каталоги (имеет смысл только в сочетании с опцией `-R`);

`-P` – не переходить по символическим ссылкам на каталоги (имеет смысл только в сочетании с опцией `-R`);

`-L` – следовать по символическим ссылкам, даже если они не указаны в командной строке;

`-P` – не следовать по символическим ссылкам, даже если они указаны в командной строке;

`--mask` – пересчитать маску эффективных прав;

`-m` – изменить текущий ACL для файла;

`-M` – прочитать записи ACL для модификации из файла;

`-x` – удалить записи из ACL файла;

`-X` – прочитать записи ACL для удаления из файла;

`--restore=file` – восстановить резервную копию прав доступа, созданную командой `getfacl -R` или ей подобной. Все права доступа дерева каталогов восстанавливаются, используя этот механизм. В случае если вводимые данные содержат элементы для владельца или группы-владельца, и команда `setfacl` выполняется пользователем с именем root, то владелец и группа-владелец всех файлов также восстанавливаются. Эта опция не может использоваться совместно с другими опциями за исключением опции `--test`;

`--set=acl` – установить ACL для файла, заменив текущий ACL;

`--set-file=file` – прочитать записи ACL для установления из файла;

`--test` – режим тестирования (ACL не изменяются).

При использовании опций `--set`, `-m` и `-x` должны быть перечислены записи ACL в командной строке. Элементы ACL разделяются одинарными кавычками.

При чтении ACL из файла при помощи опций `-set-file`, `-M` и `-X` команда `setfacl` принимает множество элементов в формате вывода команды `getfacl`. В строке обычно содержится не больше одного элемента ACL.

Команда `setfacl` использует следующие форматы элементов ACL:

- права доступа отдельного пользователя (если не задан UID, то права доступа владельца файла):

```
[d[efault]:] [u[ser]:]uid [:perms]
```

- права доступа отдельной группы (если не задан GID, то права доступа группы-владельца):

```
[d[efault]:] g[roup]:gid [:perms]
```

- маска эффективных прав:

```
[d[efault]:] m[ask][:] [:perms]
```

- права доступа всех остальных:

```
[d[efault]:] o[ther][:] [:perms]
```

Элемент ACL является абсолютным, если он содержит поле `perms` и является относительным, если он включает один из модификаторов: «+» или «^». Абсолютные элементы могут использоваться в операциях установки или модификации ACL. Относительные элементы могут использоваться только в операции модификации ACL. Права доступа для отдельных пользователей,

группы, не содержащие никаких полей после значений UID, GID (поле `perms` при этом отсутствует), используются только для удаления элементов.

Значения UID и GID задаются именем или числом. Поле `perms` может быть представлено комбинацией символов «r», «w», «x», «-» или цифр (0 – 7).

Изначально файлы и каталоги содержат только три базовых элемента ACL: для владельца, группы-владельца и всех остальных пользователей. Существует ряд правил, которые следует учитывать при установке прав доступа:

- не могут быть удалены сразу три базовых элемента, должен присутствовать хотя бы один;
- если ACL содержит права доступа для отдельного пользователя или группы, то ACL также должен содержать маску эффективных прав;
- если ACL содержит какие-либо элементы ACL по умолчанию, то в последнем должны также присутствовать три базовых элемента (т. е. права доступа по умолчанию для владельца, группы-владельца и всех остальных);
- если ACL по умолчанию содержит права доступа для всех отдельных пользователей или групп, то в ACL также должна присутствовать маска эффективных прав.

Для того чтобы помочь пользователю выполнять эти правила, команда setfacl создает права доступа, используя уже существующие, согласно следующим условиям:

- если права доступа для отдельного пользователя или группы добавлены в ACL, а маски прав не существует, то создается маска с правами доступа группы-владельца;
- если создан элемент ACL по умолчанию, а трех базовых элементов не было, тогда делается их копия и они добавляются в ACL по умолчанию;
- если ACL по умолчанию содержит какие-либо права доступа для конкретных пользователя или группы и не содержит маску прав доступа по умолчанию, то при создании эта маска будет иметь те же права, что и группа по умолчанию.

Пример. Изменить разрешения для файла `test.txt`, принадлежащего пользователю liza и группе docs, так, чтобы:

- пользователь ivan имел права на чтение и запись в этот файл;
- пользователь misha не имел никаких прав на этот файл.

Исходные данные:

```
$ ls -l test.txt
-rw-r--r-- 1 liza docs 8 янв 22 15:54 test.txt
$ getfacl test.txt
# file: test.txt
# owner: liza
# group: docs
```

```
user::rw-
group::r--
other::r--
```

Установить разрешения (от пользователя liza):

```
$ setfacl -m u:ivan:rw- test.txt
$ setfacl -m u:misha:--- test.txt
```

Просмотреть разрешения (от пользователя liza):

```
$ getfacl test.txt
# file: test.txt
# owner: liza
# group: docs
user::rw-
user:ivan:rw-
user:misha:---
group::r--
mask::rw-
other::r--
```

Примечание. Символ «+» (плюс) после прав доступа в выводе команды ls -l указывает на использование ACL:

```
$ ls -l test.txt
-rw-rw-r--+ 1 liza docs 8 янв 22 15:54 test.txt
```

10.4 Управление пользователями

10.4.1 Общая информация

Пользователи и группы внутри системы обозначаются цифровыми идентификаторами – UID и GID, соответственно.

Пользователь может входить в одну или несколько групп. По умолчанию он входит в группу, совпадающую с его именем. Чтобы узнать, в какие еще группы входит пользователь, можно использовать команду `id`, вывод её может быть примерно следующим:

```
uid=500(test) gid=500(test) группы=500(test),16(rpm)
```

Такая запись означает, что пользователь test (цифровой идентификатор 500) входит в группы test и rpm. Разные группы могут иметь разный уровень доступа к тем или иным каталогам; чем в большее количество групп входит пользователь, тем больше прав он имеет в системе.

Примечание. В связи с тем, что большинство привилегированных системных утилит в дистрибутивах «Альт» имеют не SUID-, а SGID-бит, необходимо быть предельно внимательным и осторожным в переназначении групповых прав на системные каталоги.

10.4.2 Команда useradd

Команда `useradd` регистрирует нового пользователя или изменяет информацию по умолчанию о новых пользователях.

Синтаксис:

```
useradd [ОПЦИИ...] <ИМЯ ПОЛЬЗОВАТЕЛЯ>
useradd -D [ОПЦИИ...
```

Возможные опции:

`-b каталог` – базовый каталог для домашнего каталога новой учётной записи;

`-c комментарий` – текстовая строка (обычно используется для указания фамилии и мени);

`-d каталог` – домашний каталог новой учётной записи;

`-D` – показать или изменить настройки по умолчанию для useradd;

`-e дата` – дата устаревания новой учётной записи;

`-g группа` – имя или ID первичной группы новой учётной записи;

`-G группы` – список дополнительных групп (через запятую) новой учётной записи;

`-m` – создать домашний каталог пользователя;

`-M` – не создавать домашний каталог пользователя;

`-p пароль` – зашифрованный пароль новой учётной записи (не рекомендуется);

`-s оболочка` – регистрационная оболочка новой учётной записи (по умолчанию /bin/bash);

`-u UID` – пользовательский ID новой учётной записи.

Команда `useradd` имеет множество параметров, которые позволяют менять её поведение по умолчанию. Например, можно принудительно указать, какой будет UID или какой группе будет принадлежать пользователь:

```
# useradd -u 1500 -G usershares new_user
```

10.4.3 Команда passwd

Команда passwd поддерживает традиционные опции `passwd` и утилит `shadow`.

Синтаксис:

```
passwd [ОПЦИИ...] [ИМЯ ПОЛЬЗОВАТЕЛЯ]
```

Возможные опции:

`-d`, `--delete` – удалить пароль для указанной записи;

`-f`, `--force` – форсировать операцию;

`-k`, `--keep-tokens` – сохранить не устаревшие пароли;

`-l`, `--lock` – блокировать указанную запись;

`--stdin` – прочитать новые пароли из стандартного ввода;

`-S`, `--status` – дать отчет о статусе пароля в указанной записи;

`-u`, `--unlock` – разблокировать указанную запись;

`-?`, `--help` – показать справку и выйти;

`--usage` – дать короткую справку по использованию;

`-V`, `--version` – показать версию программы и выйти.

Код выхода: при успешном завершении `passwd` заканчивает работу с кодом выхода 0. Код выхода 1 означает, что произошла ошибка. Текстовое описание ошибки выводится на стандартный поток ошибок.

Пользователь может в любой момент поменять свой пароль. Единственное, что требуется для смены пароля – знать текущий пароль.

Только суперпользователь может обновить пароль другого пользователя.

10.4.4 Добавление нового пользователя

Для добавления нового пользователя используйте команды `useradd` и `passwd`:

```
# useradd test1

# passwd test1
passwd: updating all authentication tokens for user test1.

You can now choose the new password or passphrase.

A valid password should be a mix of upper and lower case letters, digits, and
other characters.  You can use a password containing at least 7 characters
from all of these classes, or a password containing at least 8 characters
from just 3 of these 4 classes.
An upper case letter that begins the password and a digit that ends it do not
count towards the number of character classes used.

A passphrase should be of at least 3 words, 11 to 72 characters long, and
contain enough different characters.

Alternatively, if no one else can see your terminal now, you can pick this as
your password: "Burst*texas$Flow".
```

```
Enter new password:
Weak password: too short.
Re-type new password:
passwd: all authentication tokens updated successfully.
```

В результате описанных действий в системе появился пользователь test1 с некоторым паролем. Если пароль оказался слишком слабым с точки зрения системы, она об этом предупредит (как в примере выше). Пользователь в дальнейшем может поменять свой пароль при помощи команды `passwd` – но если он попытается поставить слабый пароль, система откажет ему (в отличие от *root*) в изменении.

В ОС «Альт Сервер» для проверки паролей на слабость используется модуль PAM `passwdqc`.

10.4.5 Настройка парольных ограничений

Настройка парольных ограничений производится в файле `/etc/passwdqc.conf`.

Файл `passwdqc.conf` состоит из 0 или более строк следующего формата:

`опция=значение`

Пустые строки и строки, начинающиеся со знака решетка («#»), игнорируются. Символы пробела между опцией и значением не допускаются.

Опции, которые могут быть переданы в модуль (в скобках указаны значения по умолчанию): min=N0,N1,N2,N3,N4 (min=disabled,24,11,8,7) – минимально допустимая длина пароля.

Используемые типы паролей по классам символов (алфавит, число, спецсимвол, верхний и нижний регистр) определяются следующим образом:

- тип N0 используется для паролей, состоящих из символов только одного класса;
- тип N1 используется для паролей, состоящих из символов двух классов;
- тип N2 используется для парольных фраз, кроме этого требования длины, парольная фраза должна также состоять из достаточного количества слов;
- типы N3 и N4 используются для паролей, состоящих из символов трех и четырех классов, соответственно.

Ключевое слово disabled используется для запрета паролей выбранного типа N0 – N4 независимо от их длины.

Примечание. Каждое следующее число в настройке «min» должно быть не больше, чем предыдущее.

При расчете количества классов символов, заглавные буквы, используемые в качестве первого символа и цифр, используемых в качестве последнего символа пароля, не учитываются.

max=N (max=40) – максимально допустимая длина пароля. Эта опция может быть использована для того, чтобы запретить пользователям устанавливать пароли, которые могут быть слишком длинными для некоторых системных служб. Значение 8 обрабатывается особым образом: пароли длиннее 8 символов, не отклоняются, а обрезаются до 8 символов для проверки надежности (пользователь при этом предупреждается).

passphrase=N (passphrase=3) – число слов, необходимых для ключевой фразы (значение 0 отключает поддержку парольных фраз).

match=N (match=4) – длина общей подстроки, необходимой для вывода, что пароль хотя бы частично основан на информации, найденной в символьной строке (значение 0 отключает поиск подстроки). Если найдена слабая подстрока пароль не будет отклонен; вместо этого он будет подвергаться обычным требованиям к прочности при удалении слабой подстроки. Поиск подстроки нечувствителен к регистру и может обнаружить и удалить общую подстроку, написанную в обратном направлении.

similar=permit|deny (similar=deny) – параметр similar=permit разрешает задать новый пароль, если он похож на старый (параметр similar=deny – запрещает). Пароли считаются похожими, если есть достаточно длинная общая подстрока, и при этом новый пароль с частично удаленной подстрокой будет слабым.

random=N[,only] (random=42) – размер случайно сгенерированных парольных фраз в битах (от 26 до 81) или 0, чтобы отключить эту функцию. Любая парольная фраза, которая содержит предложенную случайно сгенерированную строку, будет разрешена вне зависимости от других возможных ограничений. Значение only используется для запрета выбранных пользователем паролей.

enforce=none|users|everyone (enforce=users) – параметр enforce=users задает ограничение задания паролей в passwd на пользователей без полномочий root. Параметр enforce=everyone задает ограничение задания паролей в passwd и на пользователей, и на суперпользователя root. При значении none модуль PAM будет только предупреждать о слабых паролях.

retry=N (retry=3) – количество запросов нового пароля, если пользователь с первого раза не сможет ввести достаточно надежный пароль и повторить его ввод.

Далее приводится пример задания следующих значений в файле /etc/passwdqc.conf:

```
min=8,7,4,4,4
enforce=everyone
```

В указанном примере пользователям, включая суперпользователя root, будет невозможно задать пароли:

- типа N0 (символы одного класса) – длиной меньше восьми символов;
- типа N1 (символы двух классов) – длиной меньше семи символов;
- типа N2 (парольные фразы), типа N3 (символы трех классов) и N4 (символы четырех классов) – длиной меньше четырех символов.

10.4.6 Управление сроком действия пароля

Для управления сроком действия паролей используется команда `chage`.

Примечание. Должен быть установлен пакет `shadow-change`:

```
# apt-get install shadow-change
```

`chage` изменяет количество дней между сменой пароля и датой последнего изменения пароля.

Синтаксис команды:

```
chage [опции] логин
```

Основные опции:

`-d, --lastday LAST_DAY` – установить последний день смены пароля в LAST_DAY (число дней с 1 января 1970). Дата также может быть указана в формате ГГГГ-ММ-ДД;

`-E, --expiredate EXPIRE_DAYS` – установить дату окончания действия учётной записи в EXPIRE_DAYS (число дней с 1 января 1970). Дата также может быть указана в формате ГГГГ-ММ-ДД. Значение `-1` удаляет дату окончания действия учётной записи;

`-I, --inactive INACTIVE` – используется для задания количества дней «неактивности», то есть дней, когда пользователь вообще не входил в систему, после которых его учетная запись будет заблокирована. Пользователь, чья учетная запись заблокирована, должен обратиться к системному администратору, прежде чем снова сможет использовать систему. Значение `-1` отключает этот режим;

`-l,--list` – просмотр информации о «возрасте» учётной записи пользователя;

`-m, --mindays MIN_DAYS` – установить минимальное число дней перед сменой пароля. Значение 0 в этом поле обозначает, что пользователь может изменять свой пароль, когда угодно;

`-M, --maxdays MAX_DAYS` – установить максимальное число дней перед сменой пароля. Когда сумма MAX_DAYS и LAST_DAY меньше, чем текущий день, у пользователя будет запрошен новый пароль до начала работы в системе. Эта операция может предваряться предупреждением (параметр `-W`). При установке значения `-1,` проверка действительности пароля не будет выполняться;

`-W, --warndays WARN_DAYS` – установить число дней до истечения срока действия пароля, начиная с которых пользователю будет выдаваться предупреждение о необходимости смены пароля.

Пример настройки времени действия пароля для пользователя test:

```
# chage -M 5 test
```

Получить информацию о «возрасте» учётной записи пользователя test:

```
# chage -l test
Последний раз пароль был изменён                    : дек 27, 2023
Срок действия пароля истекает                       : янв 01, 2024
Пароль будет деактивирован через                    : янв 11, 2024
Срок действия учётной записи истекает                     : никогда
Минимальное количество дней между сменой пароля           : -1
Максимальное количество дней между сменой пароля          : 5
Количество дней с предупреждением перед деактивацией пароля     : -1
```

Примечание. Задать время действия пароля для вновь создаваемых пользователей можно, изменив параметр PASS_MAX_DAYS в файле /etc/login.defs.

10.4.7 Настройка неповторяемости пароля

Для настройки неповторяемости паролей используется модуль pam_pwhistory, который сохраняет последние пароли каждого пользователя и не позволяет пользователю при смене пароля чередовать один и тот же пароль слишком часто.

Примечание. В данном случае системный каталог станет доступным для записи пользователям группы `pw_users` (следует создать эту группу и включить в неё пользователей).

Примечание. База используемых паролей ведется в файле `/etc/security/opasswd`, в который пользователи должны иметь доступ на чтение и запись. При этом они могут читать хеши паролей остальных пользователей. Не рекомендуется использовать на многопользовательских системах.

Создайте файл `/etc/security/opasswd` и дайте права на запись пользователям:

```
# install -Dm0660 -gpw_users /dev/null /etc/security/opasswd
# chgrp pw_users /etc/security
# chmod g+w /etc/security
```

Для настройки этого ограничения необходимо изменить файл `/etc/pam.d/system-auth-local-only` таким образом, чтобы он включал модуль `pam_pwhistory` после первого появления строки с паролем:

```
password        required        pam_passwdqc.so config=/etc/passwdqc.-
conf
password        required        pam_pwhistory.so debug use_authtok re-
member=10 retry=3
```

После добавления этой строки в файле `/etc/security/opasswd` будут храниться последние 10 паролей пользователя (содержит хеши паролей всех учетных записей пользователей) и при попытке использования пароля из этого списка будет выведена ошибка:

```
Password has been already used. Choose another.
```

В случае если необходимо, чтобы проверка выполнялась и для суперпользователя root, в настройки нужно добавить параметр enforce_for_root:

```
password        required        pam_pwhistory.so
use_authtok enforce_for_root remember=10 retry=3
```

10.4.8 Модификация пользовательских записей

Для модификации пользовательских записей применяется утилита `usermod`:

```
# usermod -G audio,rpm,test1 test1
```

Такая команда изменит список групп, в которые входит пользователь test1 – теперь это audio, rpm, test1.

```
# usermod -l test2 test1
```

Будет произведена смена имени пользователя с test1 на test2.

Команды `usermod -L test2` и `usermod -U test2` соответственно временно блокируют возможность входа в систему пользователю test2 и возвращают всё на свои места.

Изменения вступят в силу только при следующем входе пользователя в систему.

При неинтерактивной смене или задании паролей для целой группы пользователей используется команда `chpasswd`. На стандартный вход ей следует подавать список, каждая строка которого будет выглядеть как `имя:пароль`.

10.4.9 Удаление пользователей

Для удаления пользователей используется команда `userdel`.

Команда `userdel test2` удалит пользователя test2 из системы. Если будет дополнительно задан параметр `-r`, то будет уничтожен и домашний каталог пользователя. Нельзя удалить пользователя, если в данный момент он еще работает в системе.

10.5 Режим суперпользователя

10.5.1 Какие бывают пользователи?

Linux – система многопользовательская, а потому пользователь – ключевое понятие для организации всей системы доступа в Linux. Файлы всех пользователей в Linux хранятся раздельно, у каждого пользователя есть собственный домашний каталог, в котором он может хранить свои данные. Доступ других пользователей к домашнему каталогу пользователя может быть ограничен.

Суперпользователь в Linux – это выделенный пользователь системы, на которого не распространяются ограничения прав доступа. Именно суперпользователь имеет возможность произ-

вольно изменять владельца и группу файла. Ему открыт доступ на чтение и запись к любому файлу или каталогу системы.

Среди учётных записей Linux всегда есть учётная запись суперпользователя – root. Поэтому вместо «суперпользователь» часто говорят «root». Множество системных файлов принадлежат root, множество файлов только ему доступны для чтения или записи. Пароль этой учётной записи – одна из самых больших драгоценностей системы. Именно с её помощью системные администраторы выполняют самую ответственную работу.

10.5.2 Для чего может понадобиться режим суперпользователя?

Системные утилиты, например, такие, как ЦУС или «Программа управления пакетами Synaptic» требуют для своей работы привилегий суперпользователя, потому что они вносят изменения в системные файлы. При их запуске выводится диалоговое окно с запросом пароля системного администратора.

10.5.3 Как получить права суперпользователя?

Для опытных пользователей, умеющих работать с командной строкой, существует два различных способа получить права суперпользователя.

Первый – это зарегистрироваться в системе под именем root.

Второй способ – воспользоваться специальной утилитой `su` (shell of user), которая позволяет выполнить одну или несколько команд от лица другого пользователя. По умолчанию эта утилита выполняет команду sh от пользователя root, то есть запускает командный интерпретатор. Отличие от предыдущего способа в том, что всегда известно, кто именно запускал `su`, а значит, ясно, кто выполнил определённое административное действие.

В некоторых случаях удобнее использовать не `su`, а утилиту `sudo`, которая позволяет выполнять только заранее заданные команды.

Примечание. Для того чтобы воспользоваться командами `su` и `sudo`, необходимо быть членом группы `wheel`. Пользователь, созданный при установке системы, по умолчанию уже включён в эту группу.

В дистрибутивах «Альт» для управления доступом к важным службам используется подсистема `control`. `control` – механизм переключения между неким набором фиксированных состояний для задач, допускающих такой набор.

Команда `control` доступна только для суперпользователя (root). Для того чтобы посмотреть, что означает та или иная политика `control` (разрешения выполнения конкретной команды, управляемой `control`), надо запустить команду с ключом `help`:

```
# control su help
```

Запустив `control` без параметров, можно увидеть полный список команд, управляемых командой (facilities) вместе с их текущим состоянием и набором допустимых состояний.

10.5.4 Как перейти в режим суперпользователя?

Для перехода в режим суперпользователя наберите в терминале команду (**минус важен!**):

```
su -
```

Если воспользоваться командой `su` без ключа, то происходит вызов командного интерпретатора с правами root. При этом значение переменных окружения, в частности $PATH, остаётся таким же, как у пользователя: в переменной $PATH не окажется каталогов `/sbin`, `/usr/sbin`, без указания полного имени будут недоступны команды `route`, `shutdown`, `mkswap` и другие. Более того, переменная $HOME будет указывать на каталог пользователя, все программы, запущенные в режиме суперпользователя, сохранят свои настройки с правами root в каталоге пользователя, что в дальнейшем может вызвать проблемы.

Чтобы избежать этого, следует использовать `su -`. В этом режиме `su` запустит командный интерпретатор в качестве login shell, и он будет вести себя в точности так, как если бы в системе зарегистрировался root.

11 ОБЩИЕ ПРАВИЛА ЭКСПЛУАТАЦИИ

11.1 Включение компьютера

Для включения компьютера необходимо:

- включить стабилизатор напряжения, если компьютер подключен через стабилизатор напряжения;
- включить принтер, если он нужен;
- включить монитор компьютера, если он не подключен к системному блоку кабелем питания;
- включить компьютер (переключателем на корпусе компьютера либо клавишей с клавиатуры).

После этого на экране компьютера появятся сообщения о ходе работы программ проверки и начальной загрузки компьютера.

11.2 Выключение компьютера

Для выключения компьютера надо:

- закончить работающие программы;
- выбрать функцию завершения работы и выключения компьютера, после чего ОС самостоятельно выключит компьютер, имеющий системный блок формата ATX;
- выключить компьютер (переключателем на корпусе AT системного блока);
- выключить принтер;
- выключить монитор компьютера (если питание монитора не от системного блока);
- выключить стабилизатор, если компьютер подключен через стабилизатор напряжения.