

Акционерное общество «Иридиум»

Операционная система «Иридиум»

Руководство администратора

Листов 235

МОСКВА, 2023

СОДЕРЖАНИЕ

1	Общие сведения об ОС Иридиум 10.1.....	4
1.1	Краткое описание возможностей.....	4
1.2	Структура программных средств.....	5
2	Загрузка операционной системы.....	7
2.1	Настройка загрузки.....	7
2.2	Получение доступа к зашифрованным разделам.....	8
2.3	Вход и работа в системе в консольном режиме.....	8
2.4	Виртуальная консоль.....	9
2.5	Вход и работа в системе в графическом режиме.....	10
2.6	Рабочий стол МАТЕ.....	11
2.7	Блокирование сеанса доступа.....	15
2.8	Завершение сеанса пользователя.....	17
2.9	Выключение/перезагрузка компьютера.....	19
3	Обзор приложений для рабочей станции.....	21
3.1	Веб-навигация.....	21
3.2	Электронная почта.....	22
3.3	Обмен мгновенными сообщениями.....	26
3.4	Офисные приложения.....	29
3.5	Файловые менеджеры.....	30
3.6	Графика.....	46
3.7	Менеджер архивов Engrampa.....	53
3.8	Системный монитор.....	55
3.9	Центр приложений.....	59
3.10	Установка сторонних приложений с официальных сайтов.....	64
3.11	Recoll – полнотекстовый поиск.....	65

4	Настройка системы	75
4.1	Центр управления системой	75
4.2	Выбор программ, запускаемых автоматически при входе в систему	78
4.3	Настройка сети.....	81
4.4	Установка принтера	84
4.5	Настройка сканера подключенного к USB-порту	87
4.6	Настройка загрузчика GRUB2	89
4.7	Изменение пароля пользователя	91
4.8	Ввод рабочей станции в домен Active Directory.....	93
4.9	Групповые политики.....	101
4.10	Ввод рабочей станции в домен FreeIPA.....	112
5	Средства удаленного администрирования	118
5.1	Вход в систему.....	118
5.2	Конфигурирование сетевых интерфейсов	118
5.3	Сетевая установка операционной системы на рабочие места	122
5.4	Соединение удалённых офисов (OpenVPN-сервер).....	124
5.5	Доступ к службам из сети Интернет	131
5.6	Обслуживание рабочей станции	133
5.7	Прочие возможности ЦУС	148
5.8	Права доступа к модулям ЦУС.....	148
6	Функционал операционной системы.....	150
6.1	ГОСТ в OpenSSL	150
6.2	Задание хешей паролей в соответствии с ГОСТ Р 34.11-2012.....	151
6.3	Подпись и проверка ЭЦП ГОСТ	152
6.4	Управление шифрованными разделами.....	158
6.5	Создание ssh-туннелей, использующих контроль целостности заголовков IP-пакетов в соответствии с ГОСТ Р 34.12-2015	160
6.6	Создание защищенных VPN-туннелей, использующих контроль заголовков IP-пакетов в соответствии с ГОСТ Р 34.12-2015	164

6.7	Поддержка файловых систем.....	172
6.8	Поддержка сетевых протоколов	173
6.9	Виртуальная (экранная) клавиатура	183
6.10	Настройка многоместного режима	187
7	Ограничение действий пользователя.....	190
7.1	Ограничение полномочий пользователей	190
7.2	Блокировка макросов в приложениях	193
7.3	Модуль AltНа.....	194
8	Установка/обновление программного обеспечения	198
8.1	Установка/обновление программного обеспечения в графической среде	198
8.2	Обновление системы.....	200
8.3	Установка/обновление программного обеспечения в консоли.....	203
8.4	Единая команда управления пакетами (rpm)	211
9	Общие принципы работы ОС.....	214
9.1	Процессы и файлы.....	214
10	Работа с наиболее часто используемыми компонентами	221
10.1	Командные оболочки (интерпретаторы).....	221
10.2	Стыкование команд в системе	231
11	Общие правила эксплуатации	234
11.1	Включение компьютера.....	234
11.2	Выключение компьютера	234

1 ОБЩИЕ СВЕДЕНИЯ ОБ ОС «ИРИДИУМ»

1.1 Краткое описание возможностей

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

ОС «Иридиум» 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 «Иридиум» – 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 «Иридиум»:

- 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 «Иридиум» состоит из набора компонентов предназначенных для реализации функциональных задач необходимых пользователям (должностным лицам для выполнения определённых должностными инструкциями, повседневных действий) и поставляется в виде дистрибутива и комплекта эксплуатационной документации.

В структуре ОС «Иридиум» 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 «Иридиум» 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 «Иридиум», установленной на жесткий диск, происходит автоматически и выполняется после запуска ПЭВМ и отработки набора программ BIOS. ОС «Иридиум» 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.

П р и м е ч а н и е . 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 «Иридиум» 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

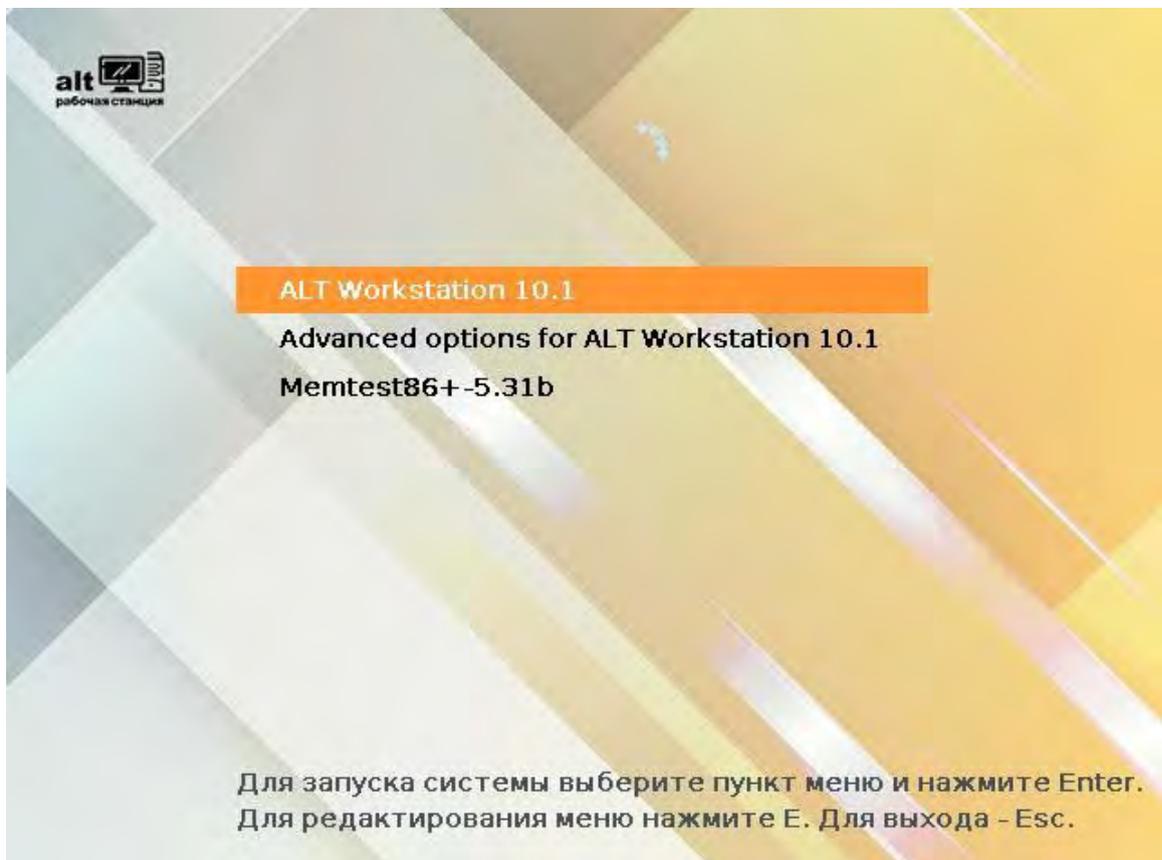


Рис. 1

По умолчанию, если не были нажаты управляющие клавиши на клавиатуре, загрузка ОС «Иридиум» 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» («Advanced options for ALT Workstation»).

Для выполнения тестирования оперативной памяти нужно выбрать пункт «Memtest86+5.31b».

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 зашифрованный раздел, потребуется вводить пароль при обращении к этому разделу (Рис. 2).

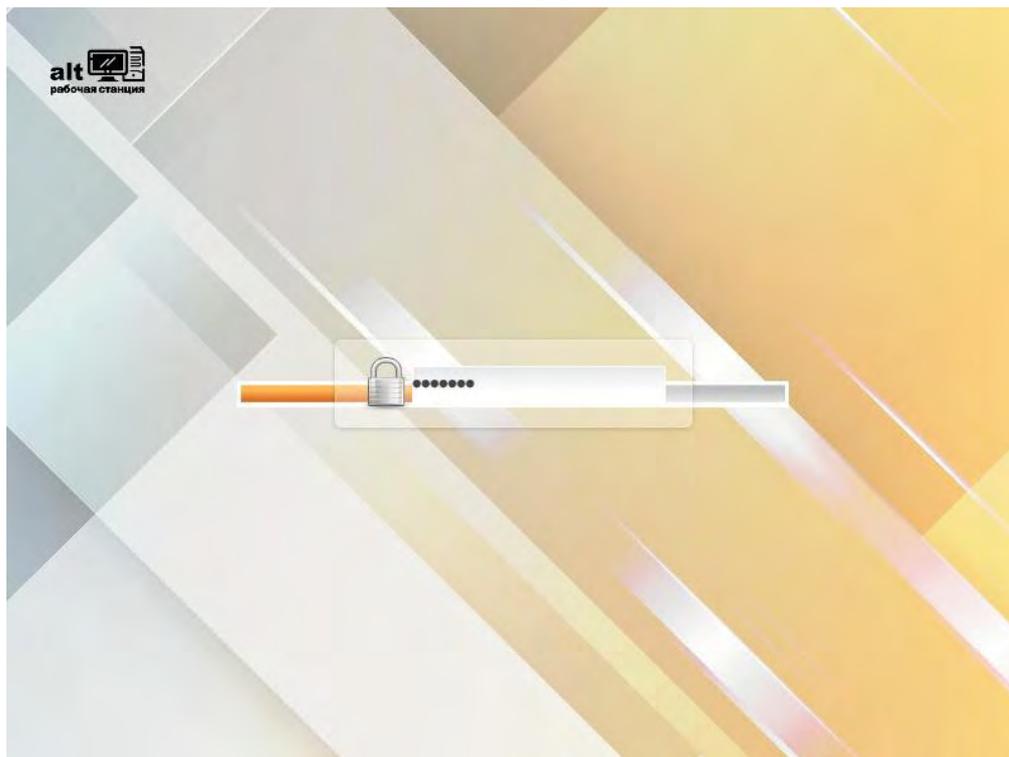
Например, если был зашифрован домашний раздел /home, то для того, чтобы войти в систему, потребуется ввести пароль этого раздела и затем нажать <Enter>.

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 «Иридиум» 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 «Иридиум» перейдет к штатному режиму работы и предоставит дальнейший доступ к консоли (Рис. 4).

Запрос на ввод логина

```
host-15 login:
```

Рис. 3

Приглашение для ввода команд

```
host-15 login: user  
Password:  
user@host-15 ~ $
```

Рис. 4

2.4 Виртуальная консоль

В процессе работы ОС «Иридиум» 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 «Иридиум» 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».

Окно входа в систему

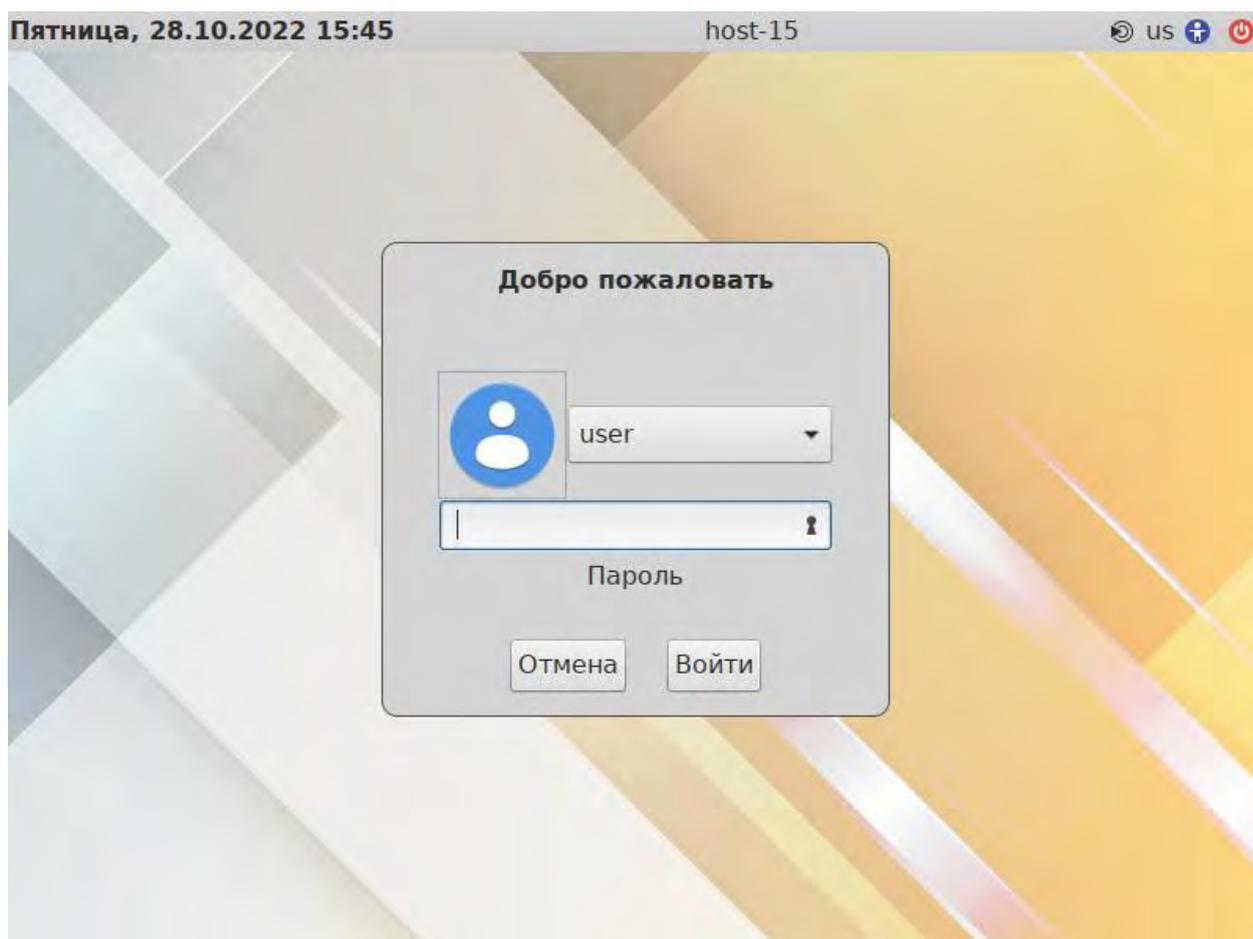


Рис. 5

В результате успешного прохождения процедуры аутентификации и идентификации будет выполнен вход в систему. ОС «Иридиум» 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.

Рабочий стол MATE

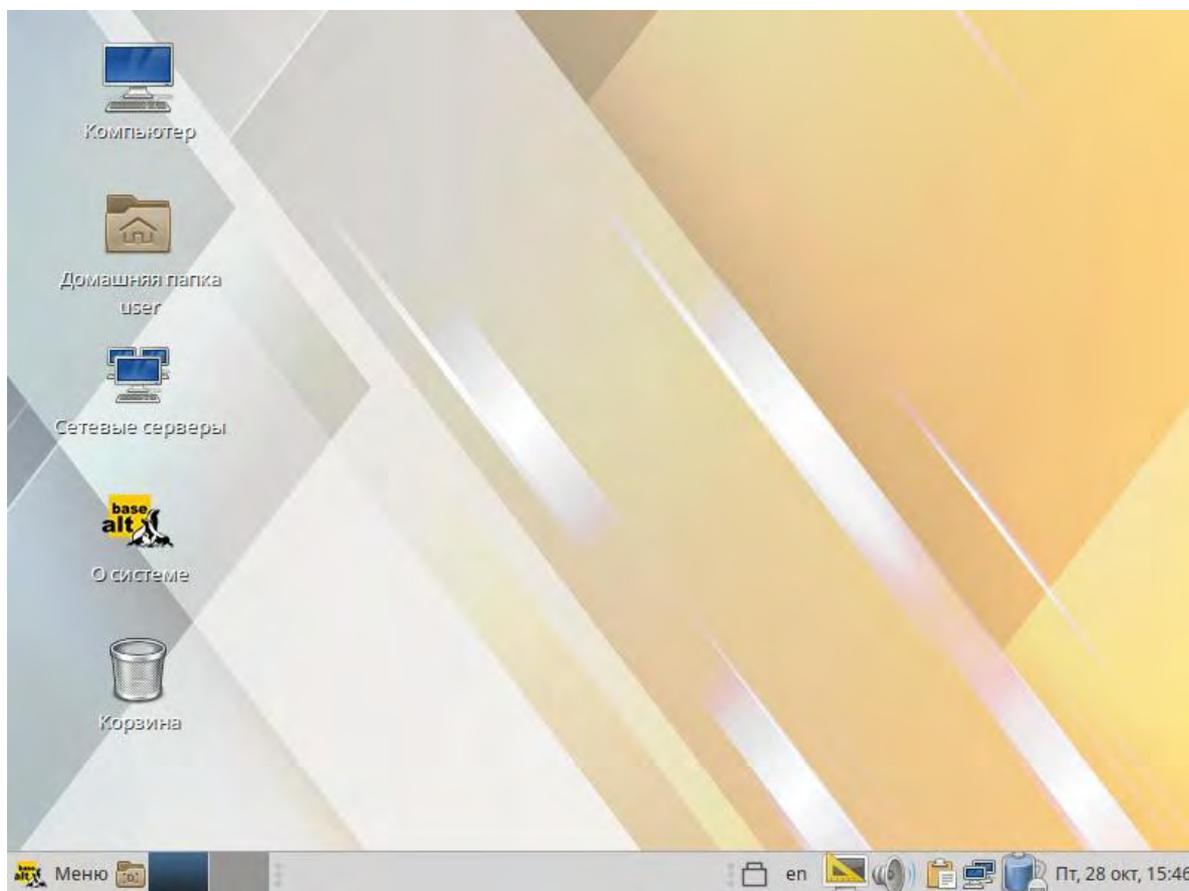


Рис. 6

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).

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 пользователь-

- ские 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, при удалении файла, он 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 МАТЕ (Рис. 7) расположена в нижней части экрана. Панель МАТЕ 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 МАТЕ со списком окон



Рис. 7

На левой части панели расположены:

- основное меню – «Меню МАТЕ», обеспечивающее доступ ко всем графическим приложениям 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 «Настройка». 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 МАТЕ находится «Меню МАТЕ». Через «Меню МАТЕ» (Рис. 8) осуществляется запуск всех приложений, установленных на компьютер.

Меню МАТЕ

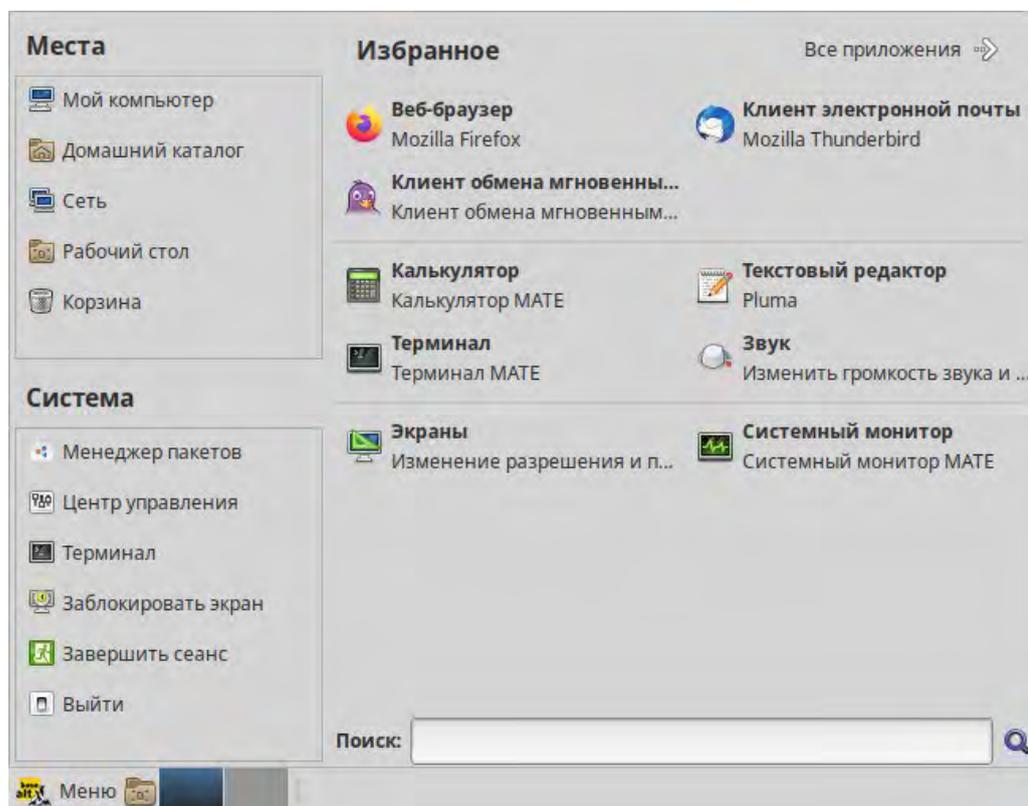


Рис. 8

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 «удалённым файлам».

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

Руководство Саја 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 МАТЕ;
- «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, который 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.

П р и м е ч а н и е . 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 символов, в меню остаются видны только те приложения, которые соответствуют запросу. Если объект поиска отсутствует в меню, функция «Поиск» «предложит» другие возможные действия, например поиск в файлах ОС или поисковой системе.

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». Также можно 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

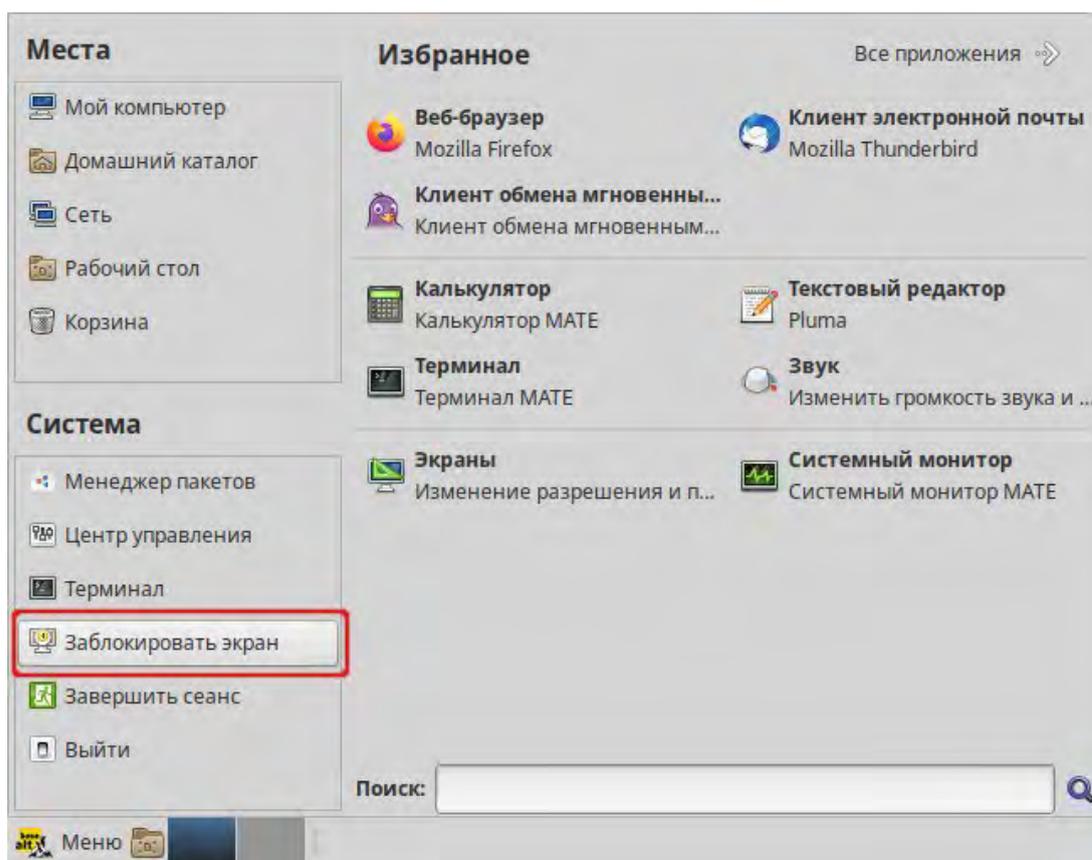


Рис. 9

Разблокирование сеанса доступа

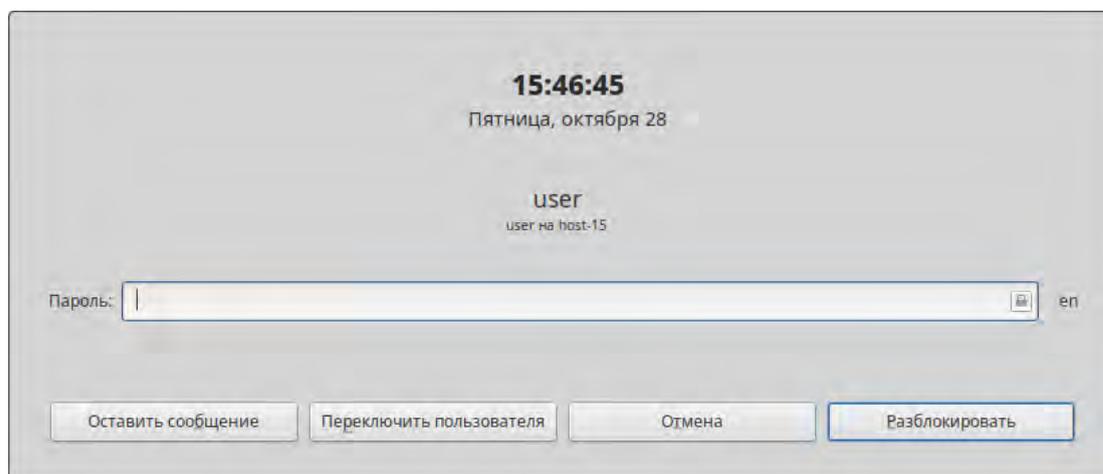


Рис. 10

Также при работе в графическом режиме блокирование сеанса доступа 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 МАТЕ»→ «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 «-а» 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 МАТЕ» в разделе «Система» выбрать пункт «Завершить сеанс» (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.

Завершение сеанса пользователя

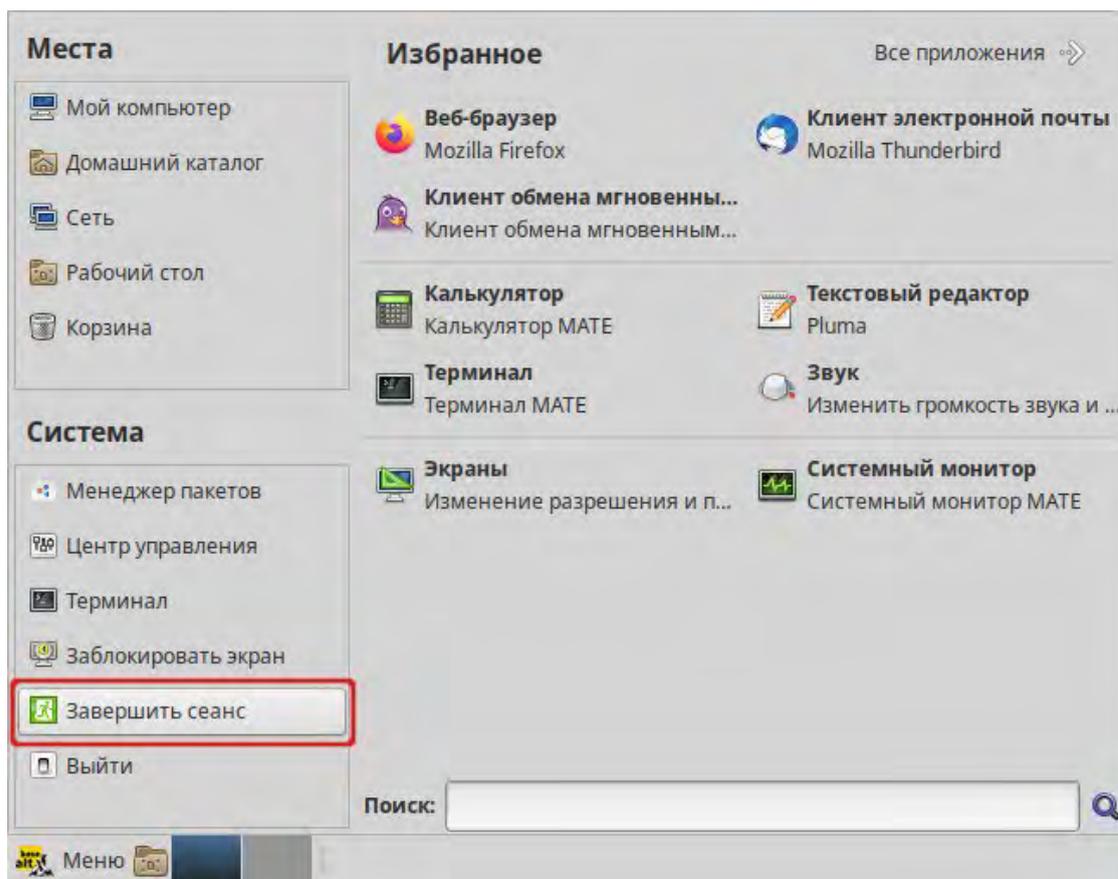


Рис. 11

Окно выхода из системы

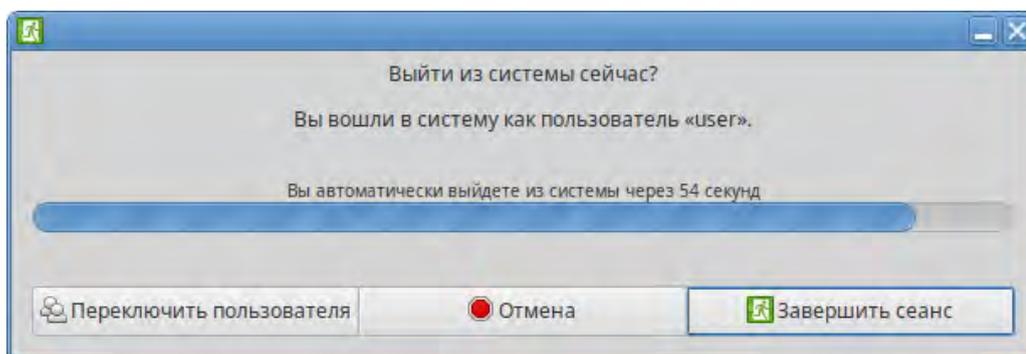


Рис. 12

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:

TMOUТ=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 МАТЕ» позволяет выключить (или перезагрузить) систему.

Выключение компьютера

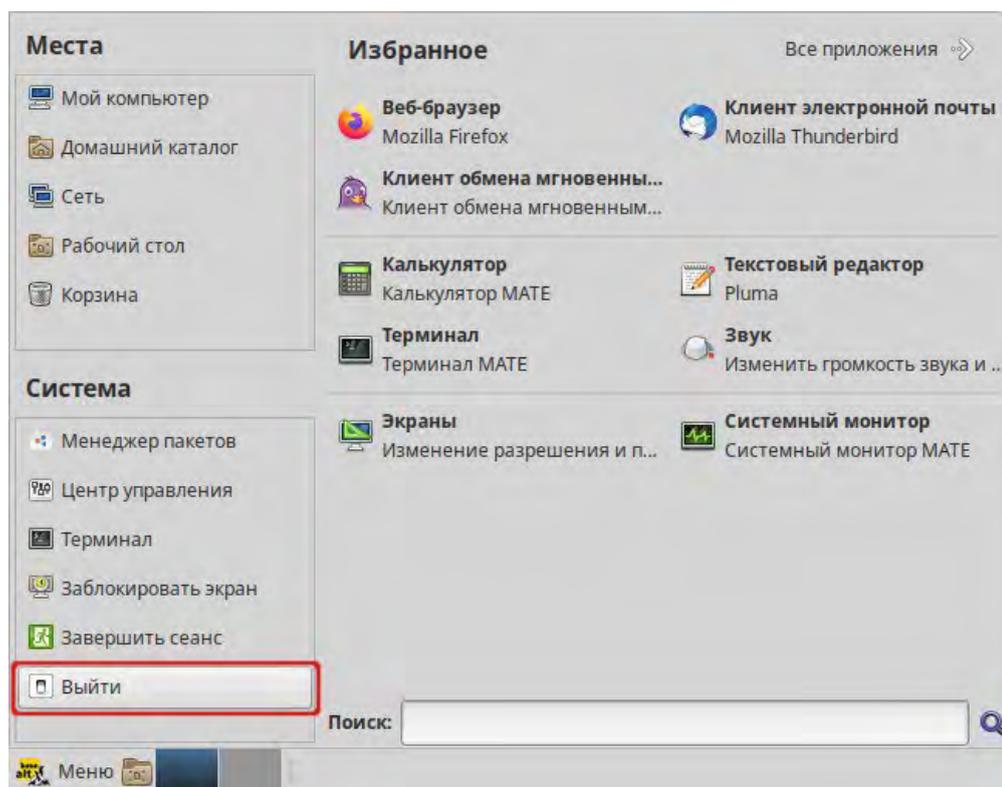
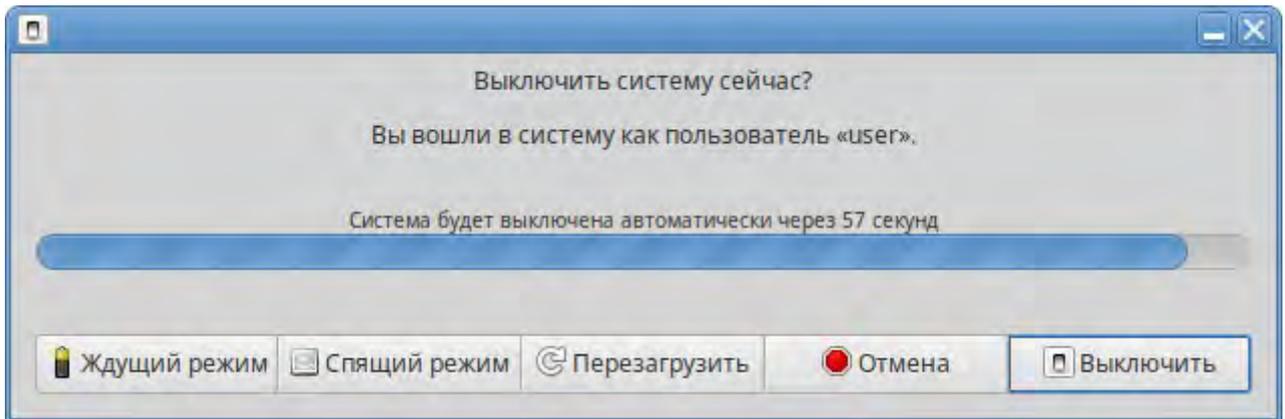


Рис. 13

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.

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

Окно выключения компьютера*Рис. 14*

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 «Иридиум» 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 «Иридиум».

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

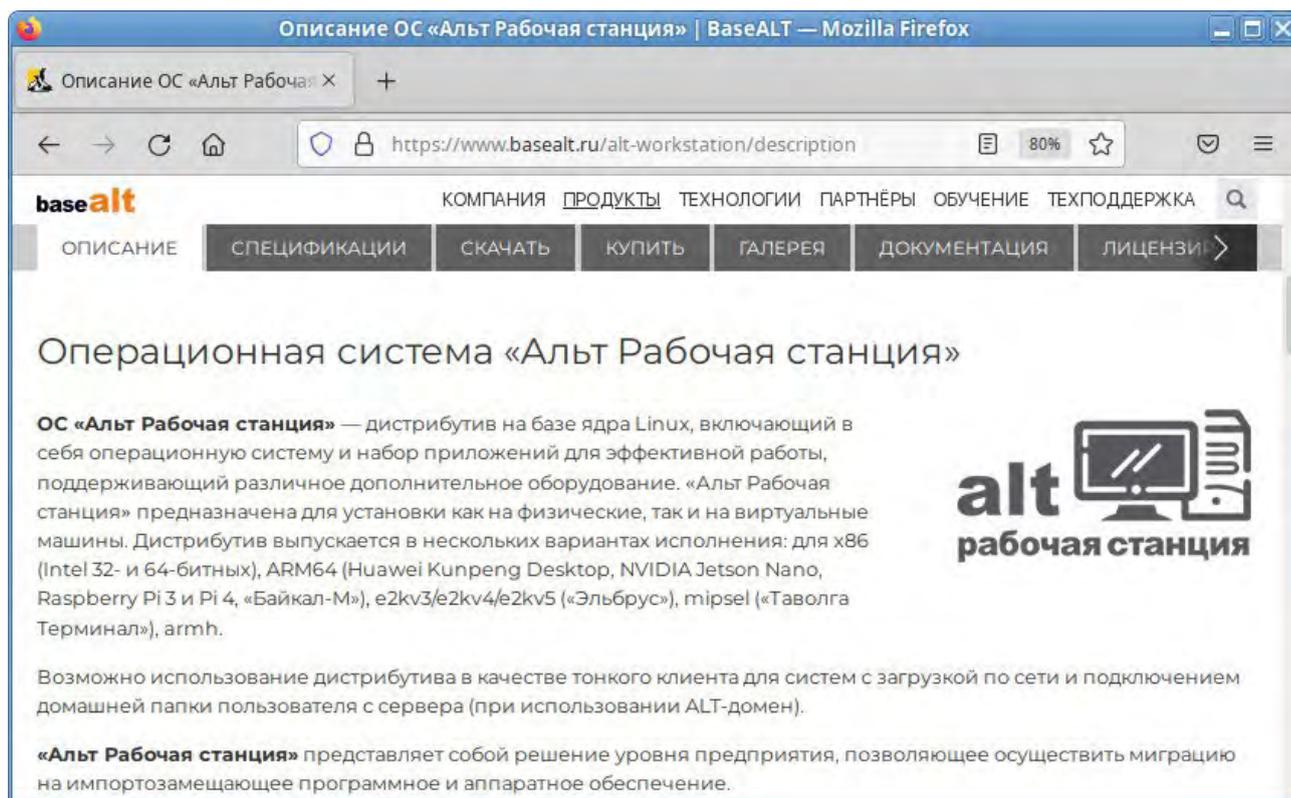


Рис. 15

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

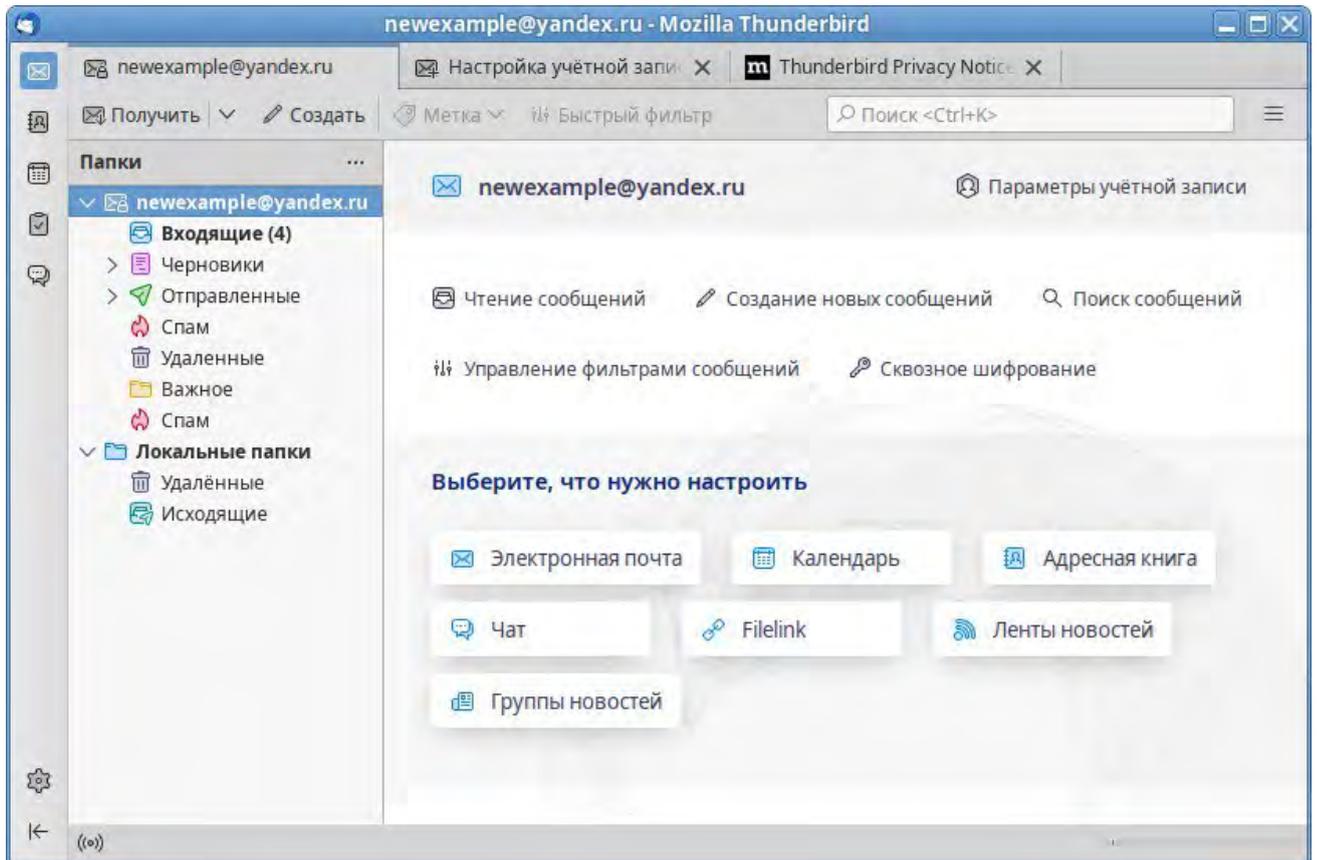


Рис. 16

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.

Почтовый клиент Mozilla Thunderbird. Настройка учётной записи почты

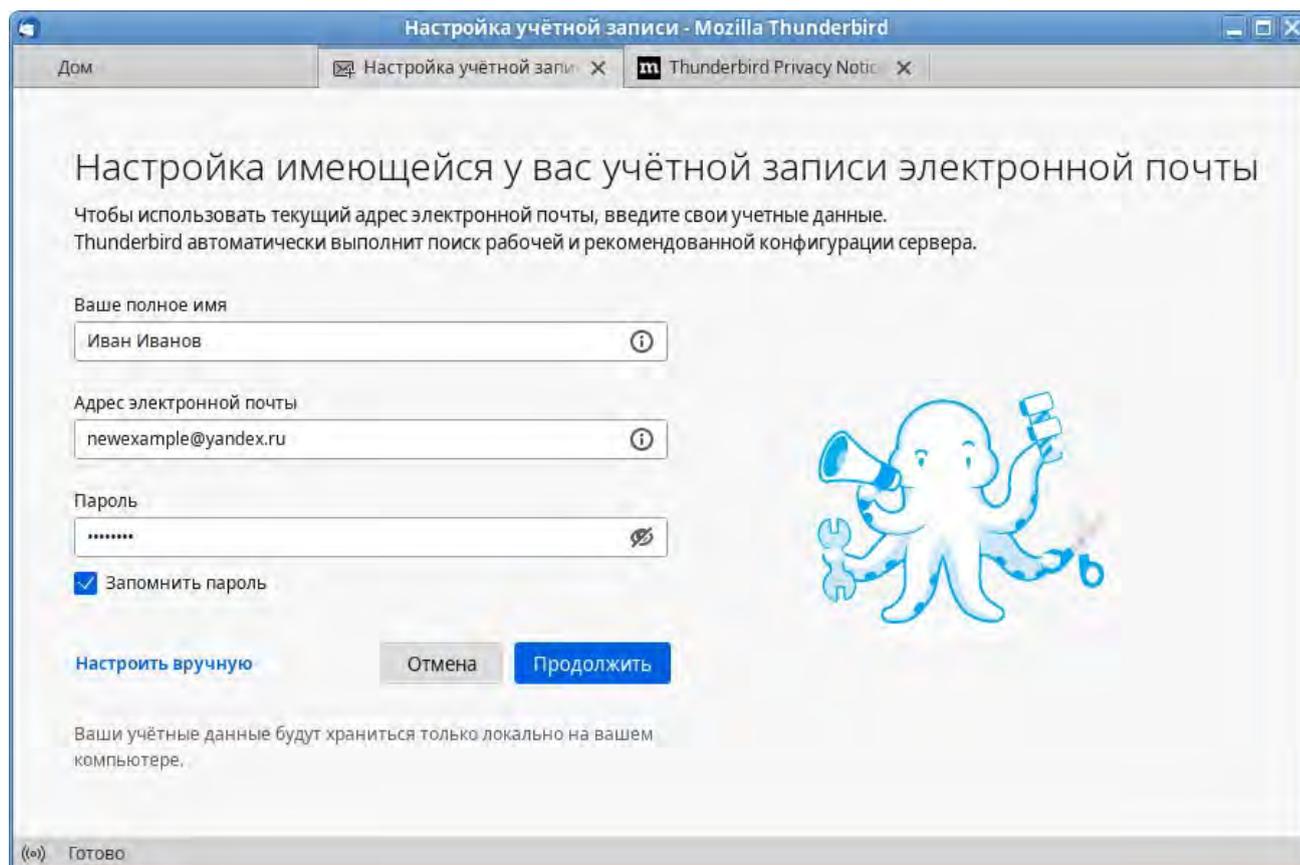


Рис. 17

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.

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

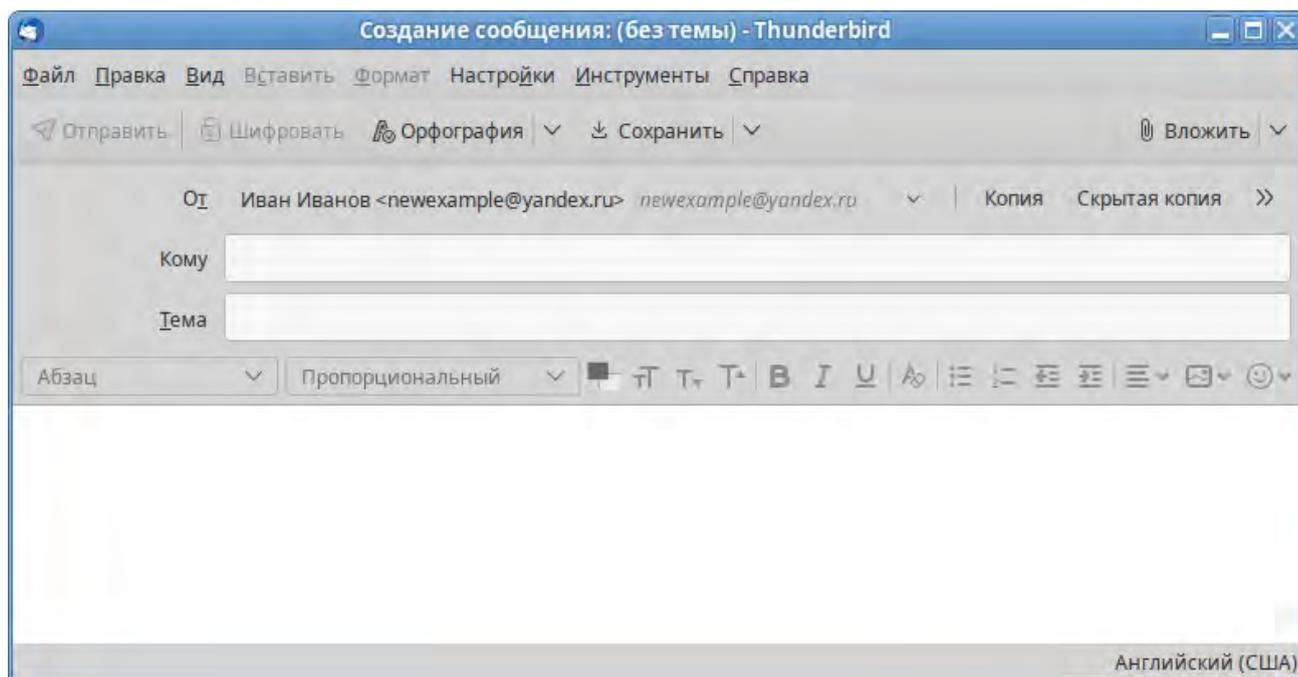


Рис. 18

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

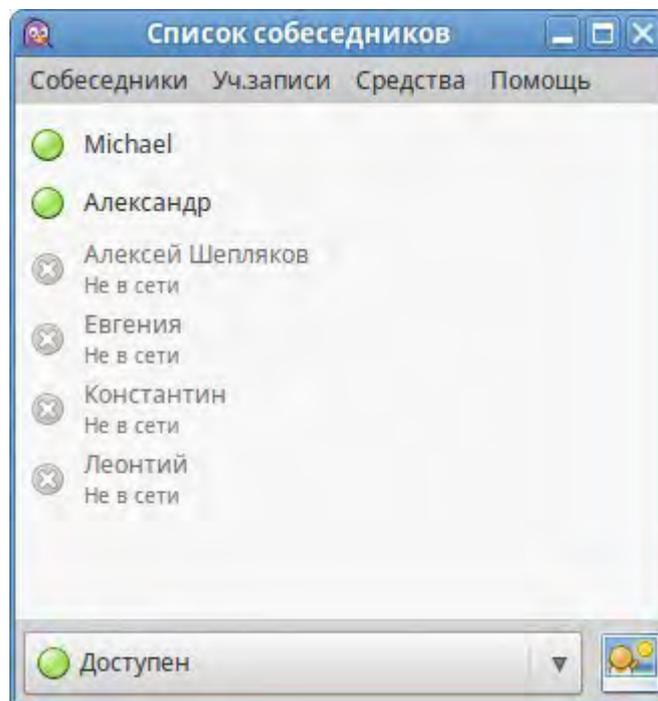


Рис. 19

Возможности Pidgin:

- поддержка особенностей различных сетей (статус сообщения, значки друзей, уведомление о наборе текста...);
- зашифрованный 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

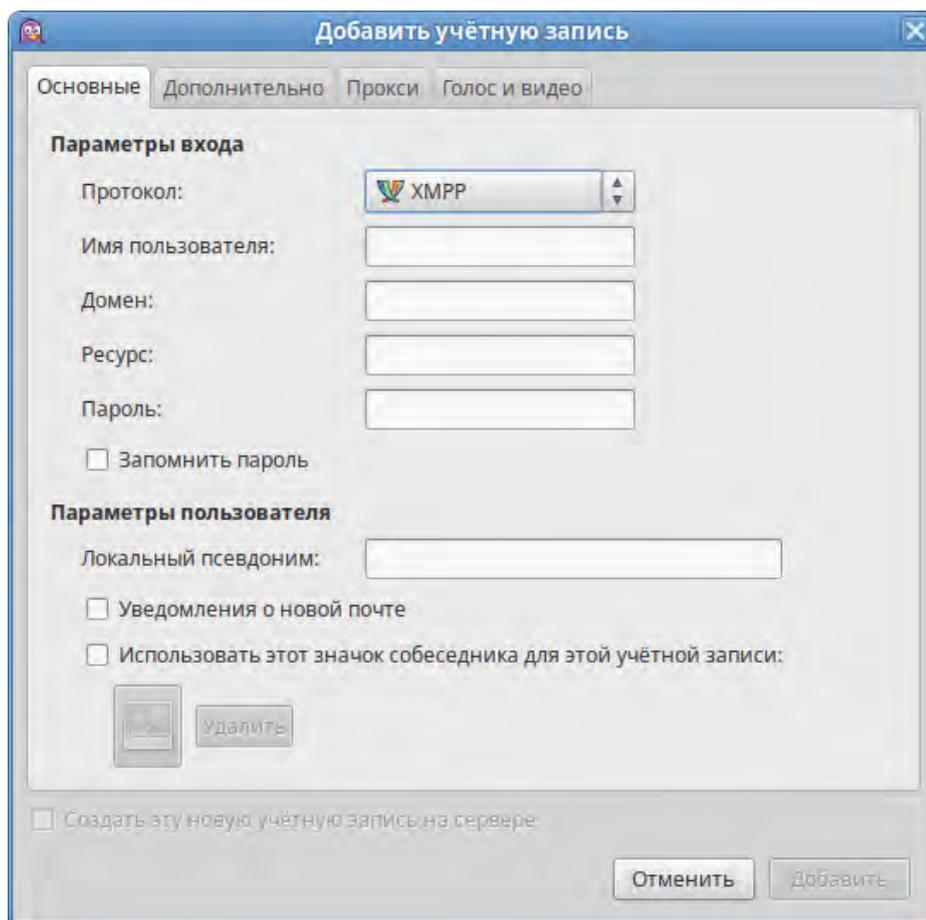


Рис. 20

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

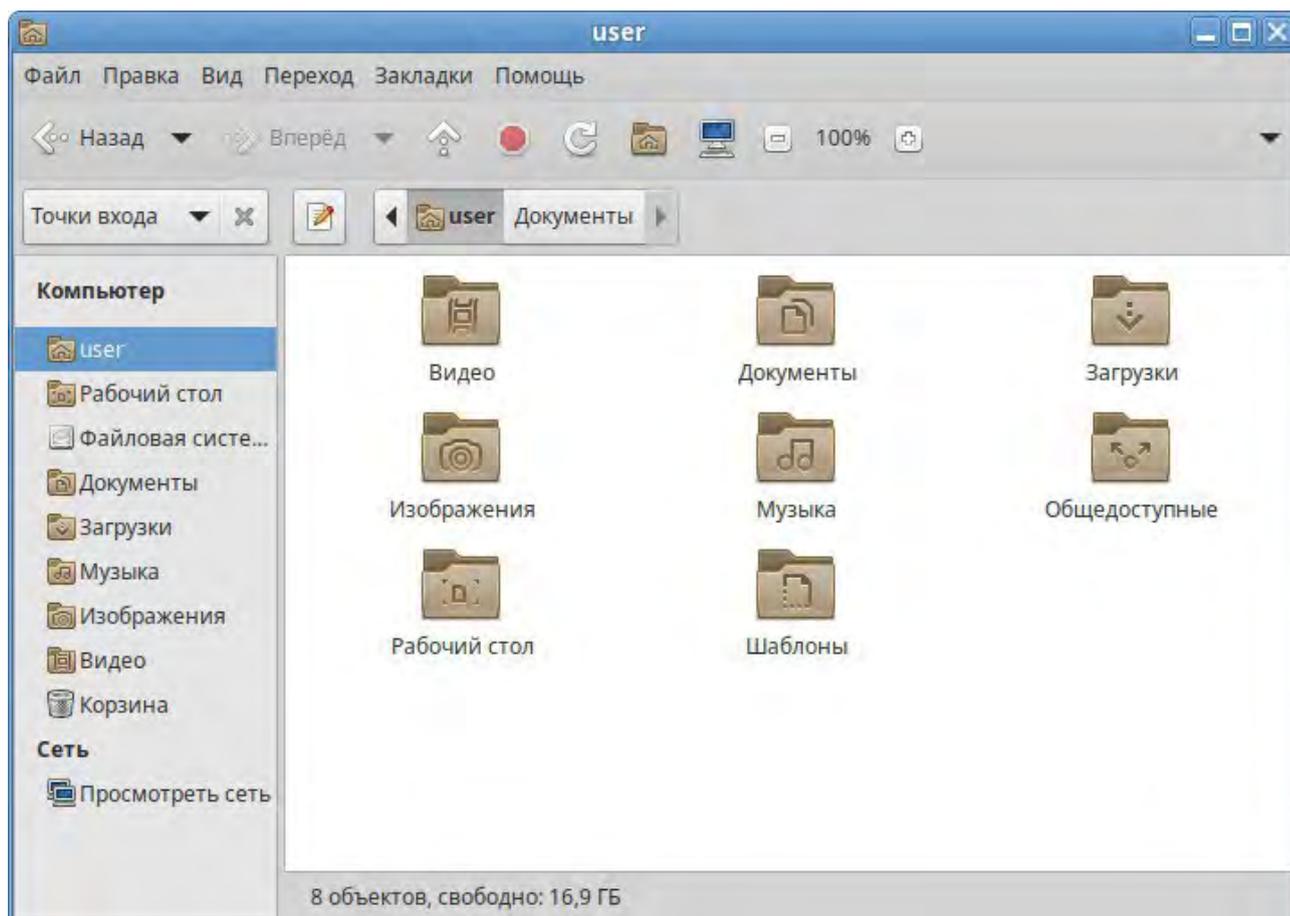


Рис. 22

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 (Рис. 23) могут сильно отличаться друг от друга.

Контекстное меню Саја

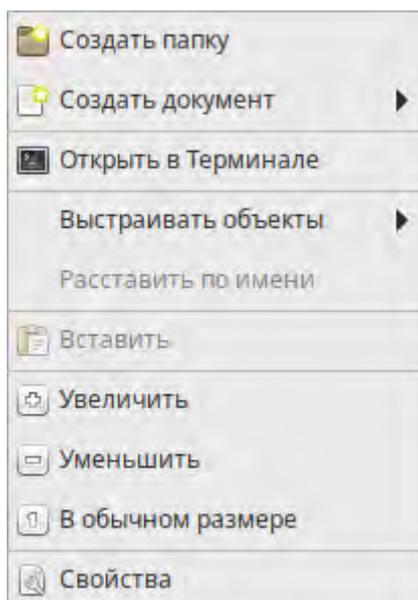


Рис. 23

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. 24).

Пункт «Создать папку» в контекстном меню Caja

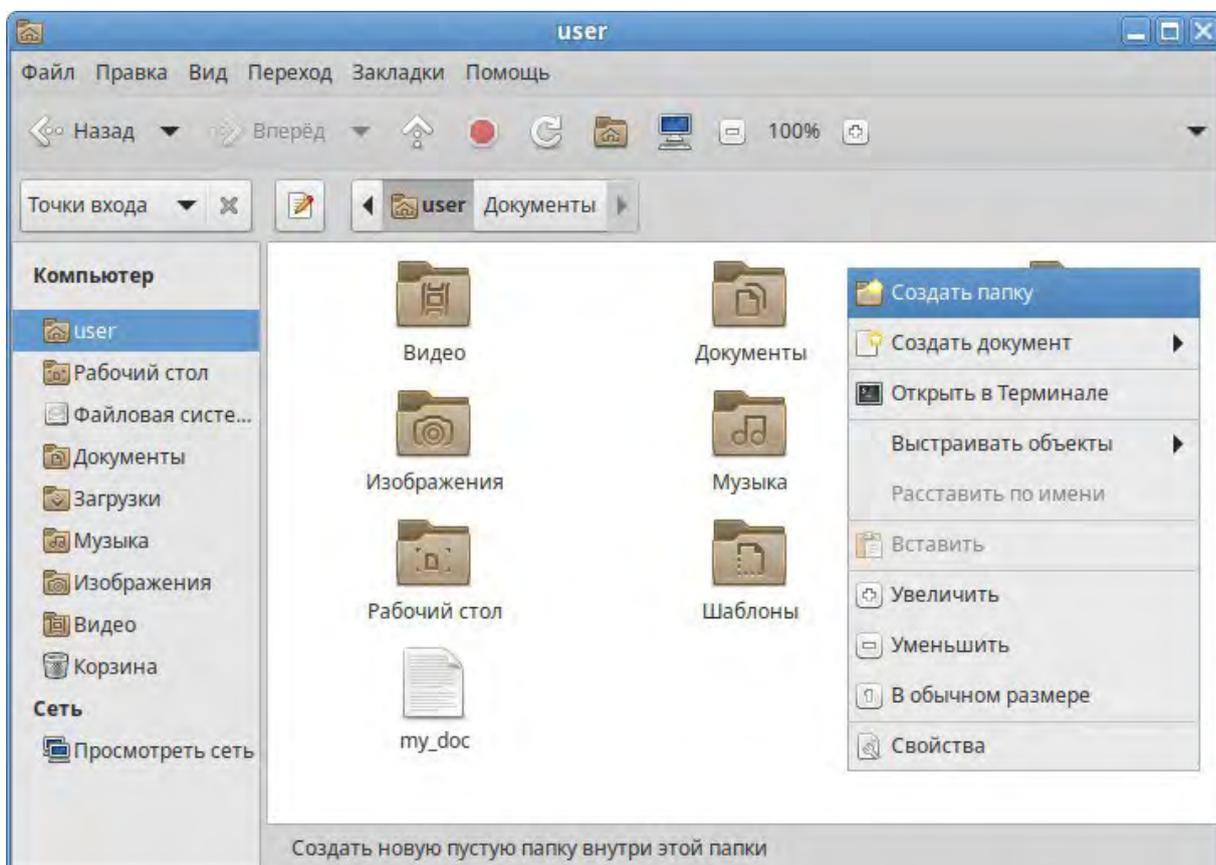


Рис. 24

Саја, как и прочие приложения ОС «Иридиум», 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 Саја.

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. 25). Нажав на кнопку, можно быстро открыть нужную папку.

Адресная строка

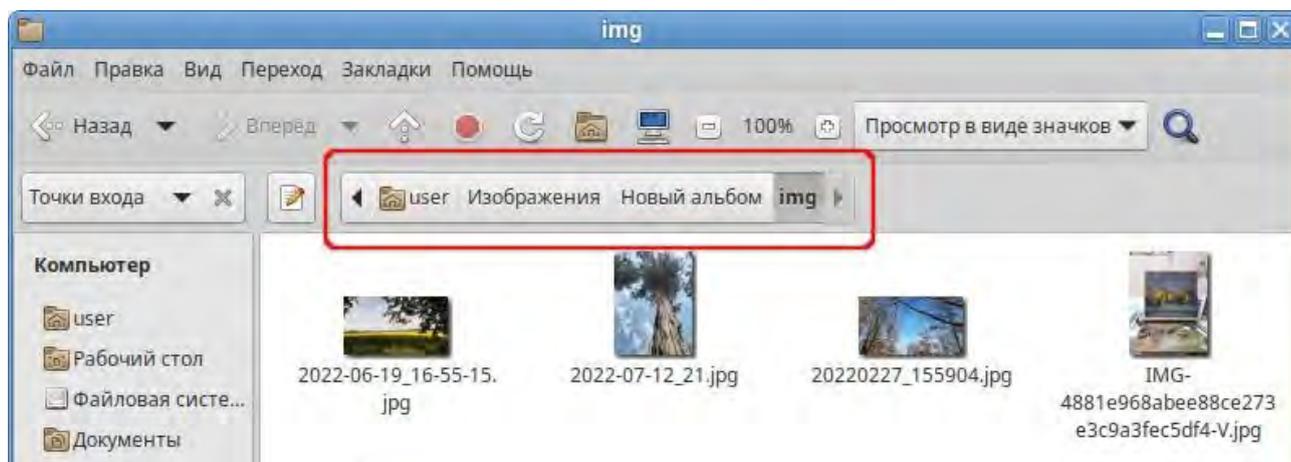


Рис. 25

Строка адреса может быть также представлена в виде редактируемой строки (Рис. 26). Чтобы переключить адресную строку из вида хлебных крошек к редактируемой версии и обратно можно нажать <Ctrl>+<L> или нажать кнопку .

Редактируемая строка адреса

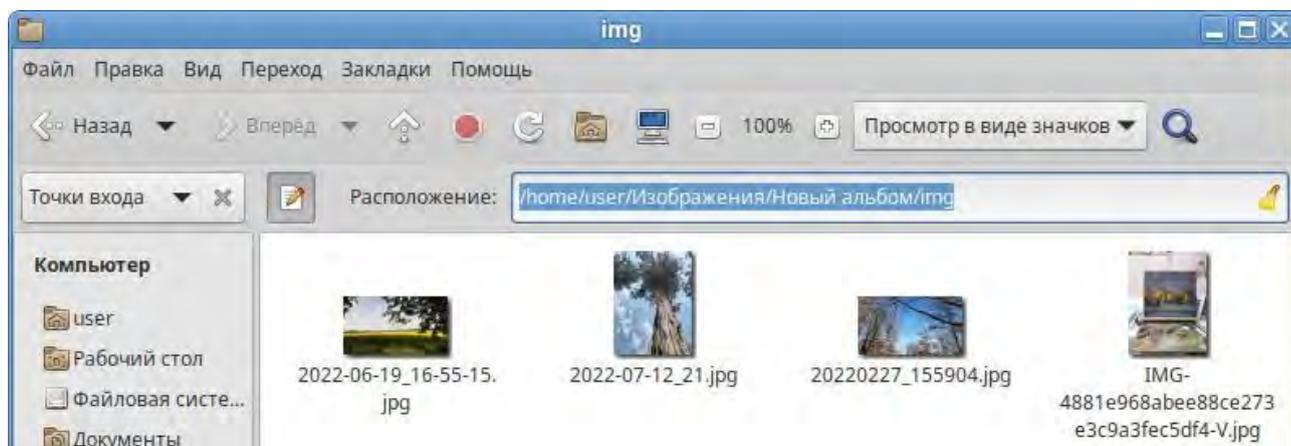


Рис. 26

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 Саја в другое (где открыта целевая папка). Перетаскивание можно осуществлять и в двухпанельном режиме (Рис. 27). В этом случае не потребуется запускать два экземпляра Саја – можно перемещать и копировать файлы и папки, перетаскивая их между панелями. Двухпанельный 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 Саја

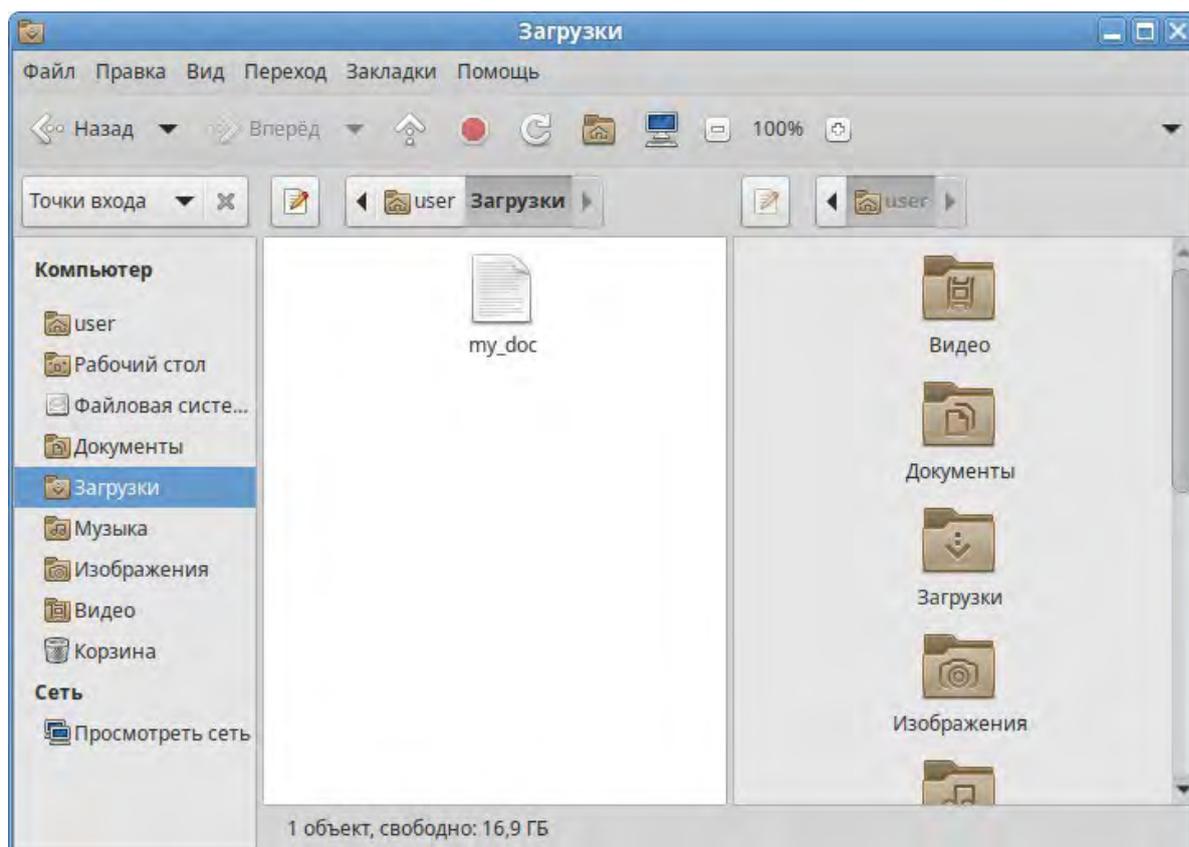


Рис. 27

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 использовать контекстное меню (Рис. 28), или удалять объекты клавишей . В этом случае файлы и папки удаляются в «Корзину». Это позволяет восстановить объект при его ошибочном удалении.

Сaja. Удаление файла

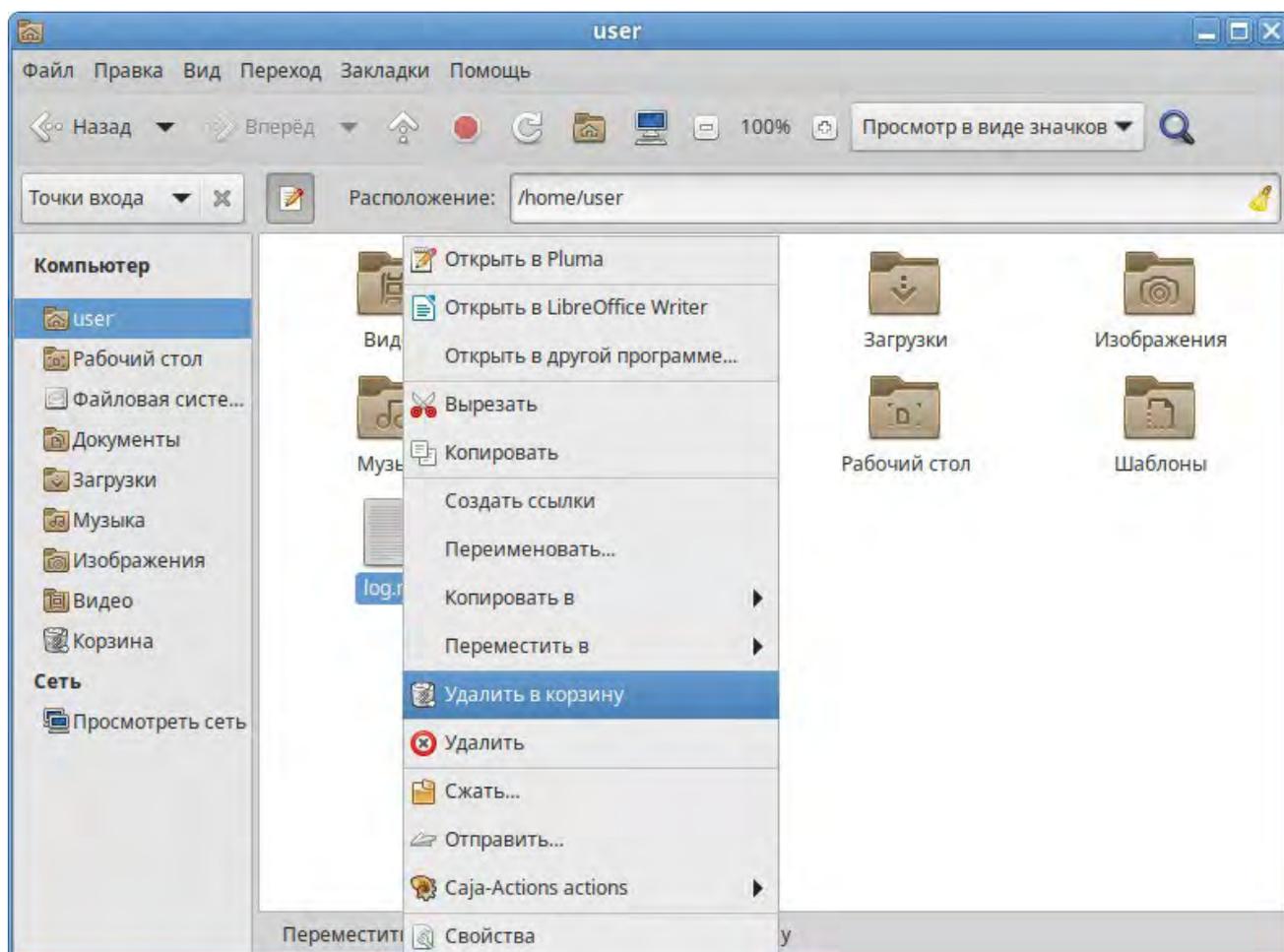


Рис. 28

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» может окончательно удалить ненужный файл или папку, без возможности её 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>+).

3.5.1.5 Открытие файлов

Открыть файл из Сажа – 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 МАТЕ» → «Параметры» → «Предпочтительные приложения»). Для каждой категории предпочтительных приложений (Рис. 29) предусмотрено раскрывающееся меню со списком доступных для выбора приложений.

Предпочтительные приложения

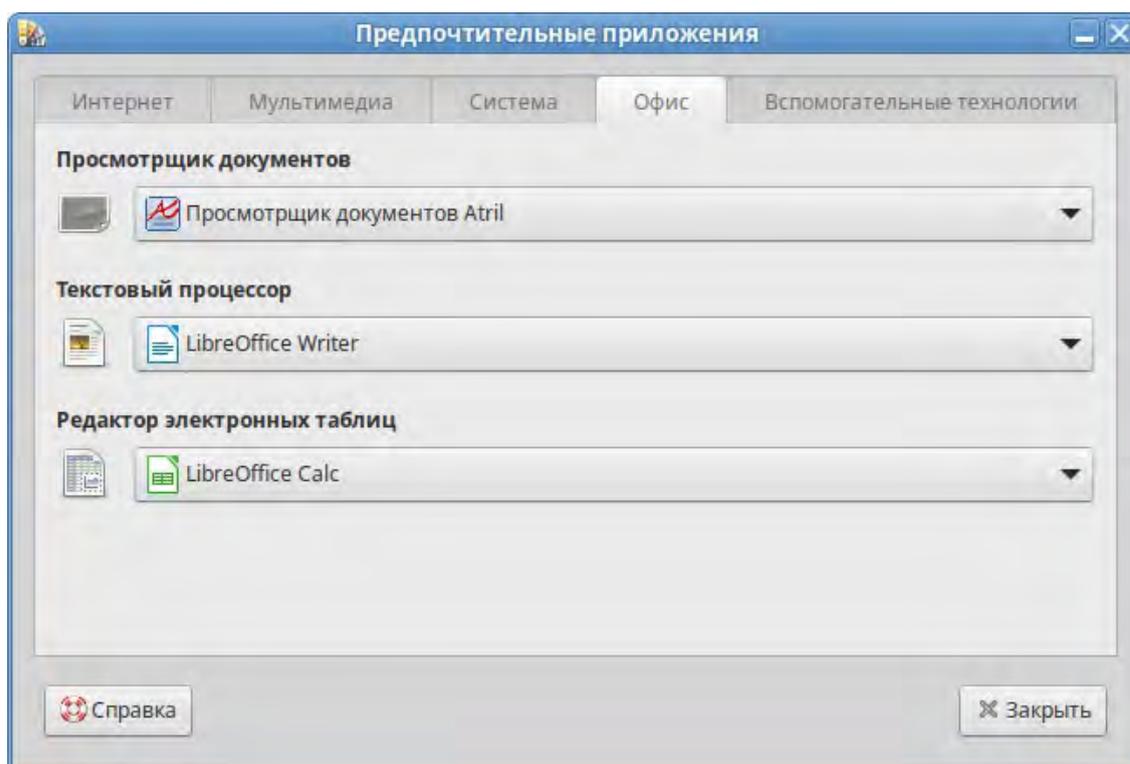


Рис. 29

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

Если на компьютере установлено несколько программ для работы с изображениями, то можно запустить нужную, выбрав её из контекстного меню (Рис. 30) (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...»).

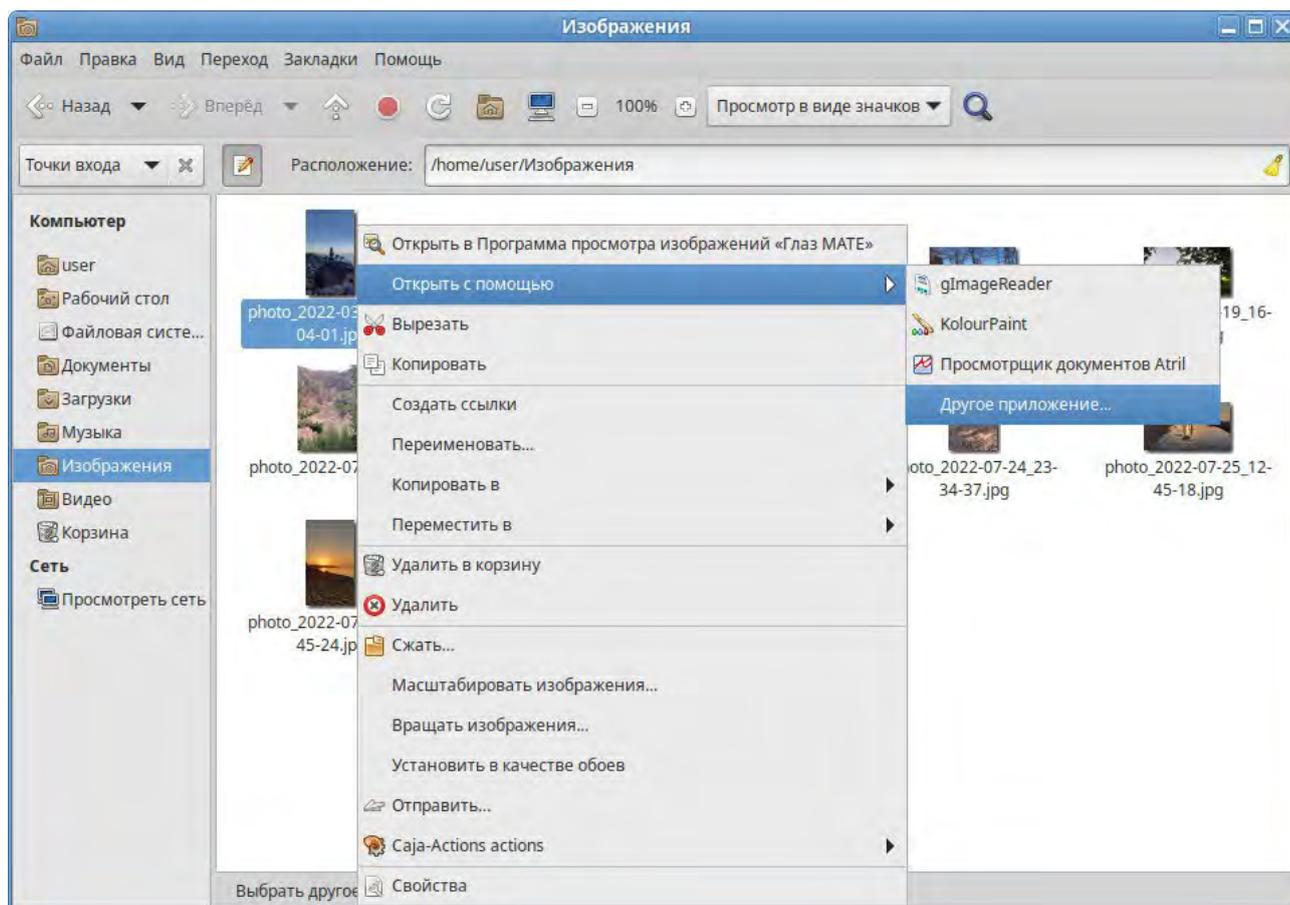
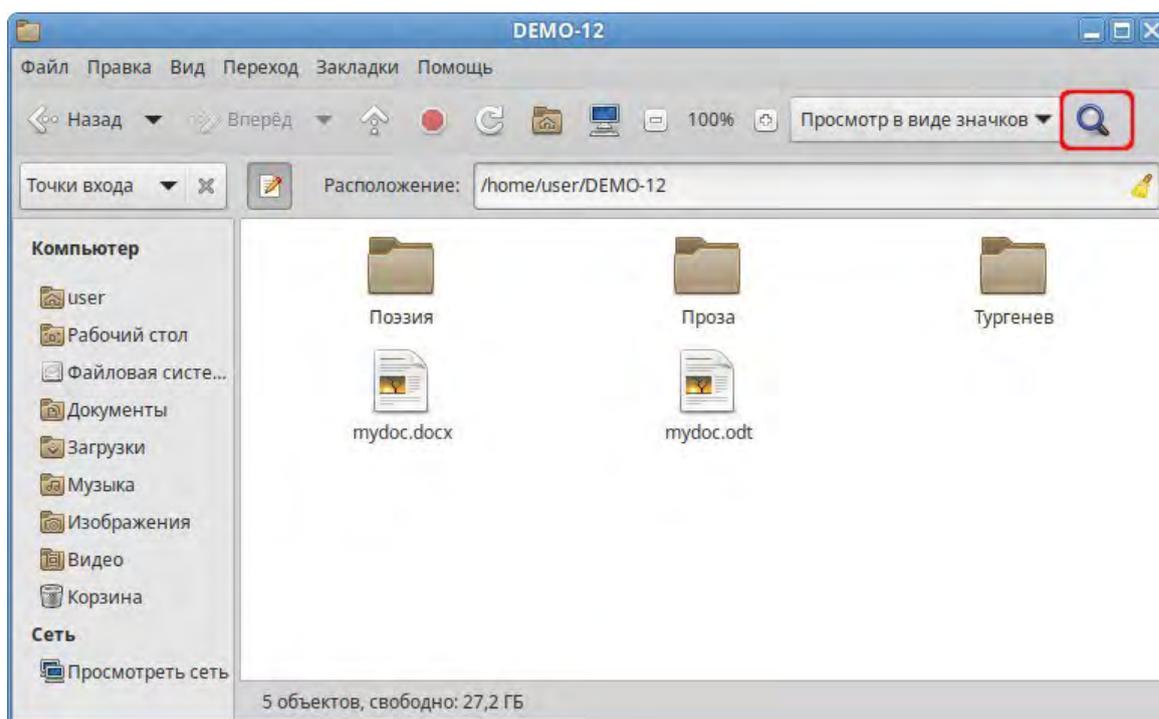
Саја. Выбор приложения

Рис. 30

3.5.1.6 Поиск файлов

В Саја можно выполнить поиск файлов по имени.

Панель поиска вызывается щелчком по значку лупы (<Ctrl>+<F>) (Рис. 31).

Саја. Вызов панели поиска*Рис. 31*

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. 32).

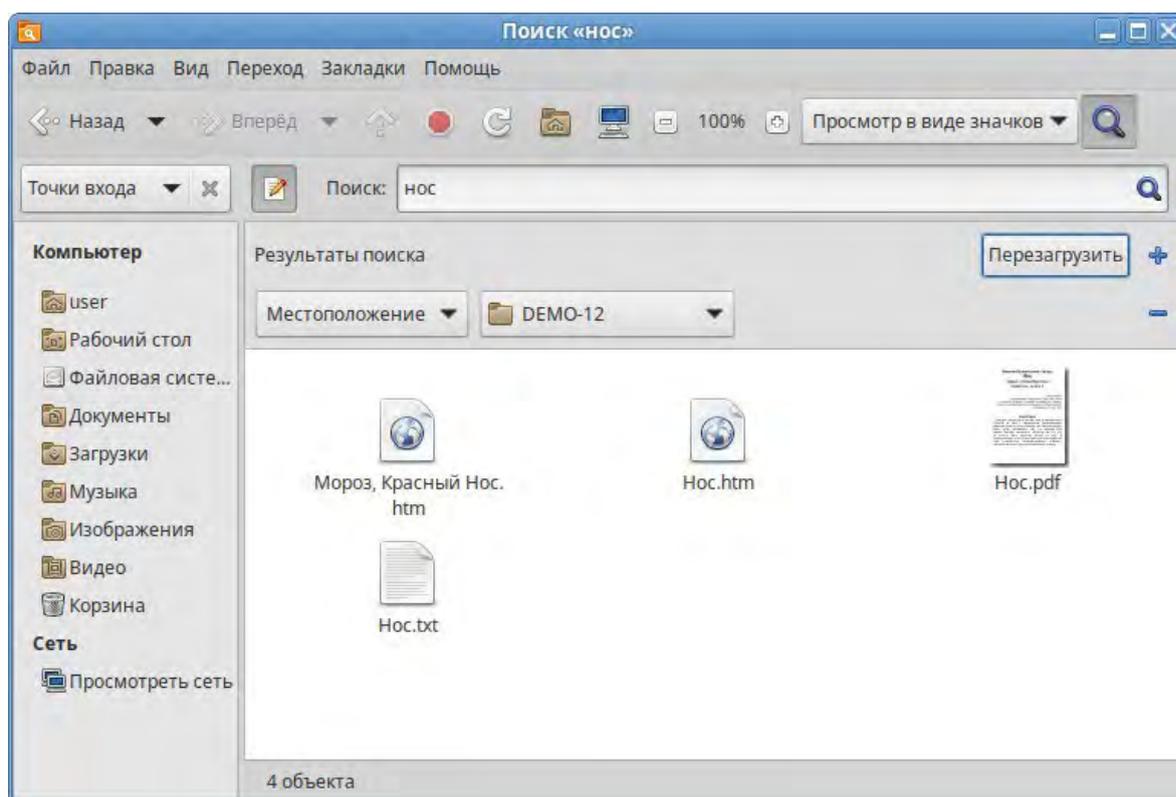
Саја. Панель поиска

Рис. 32

Для сокращения результатов поиска дополнительно можно указать тип файлов (Рис. 33).

Сaja. Параметры поиска

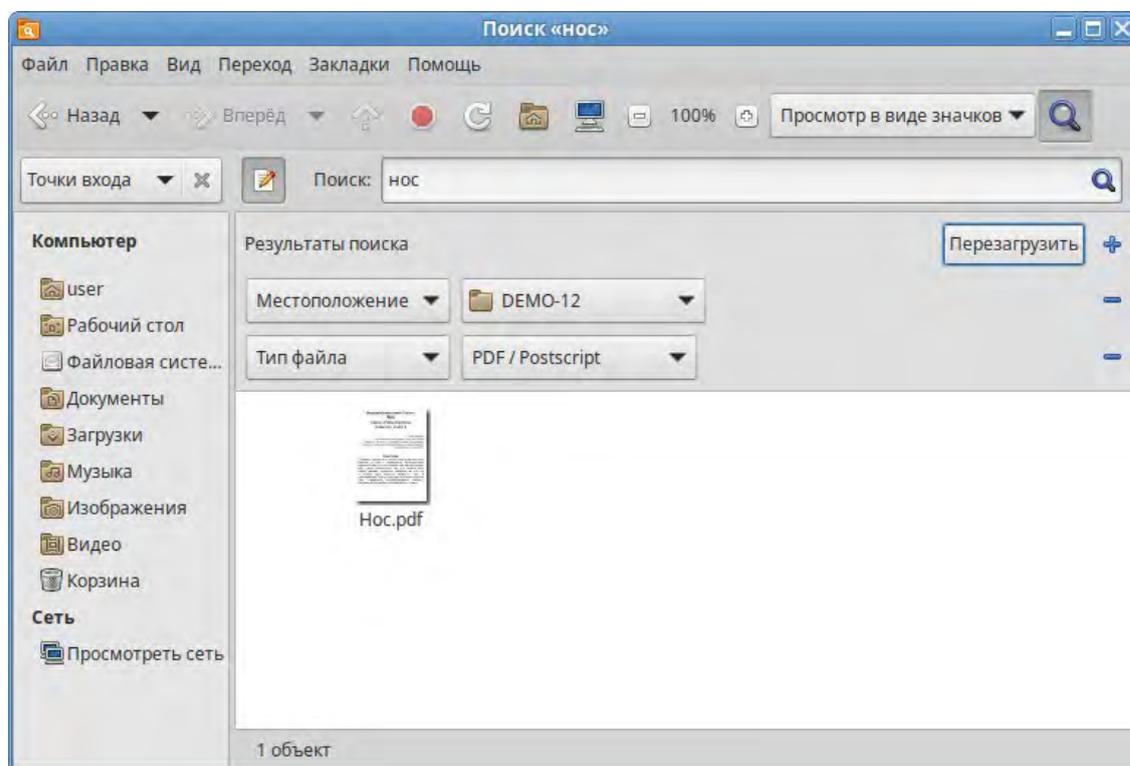


Рис. 33

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 «Иридиум» 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. 34).

Содержимое USB-накопителя в окне Caja

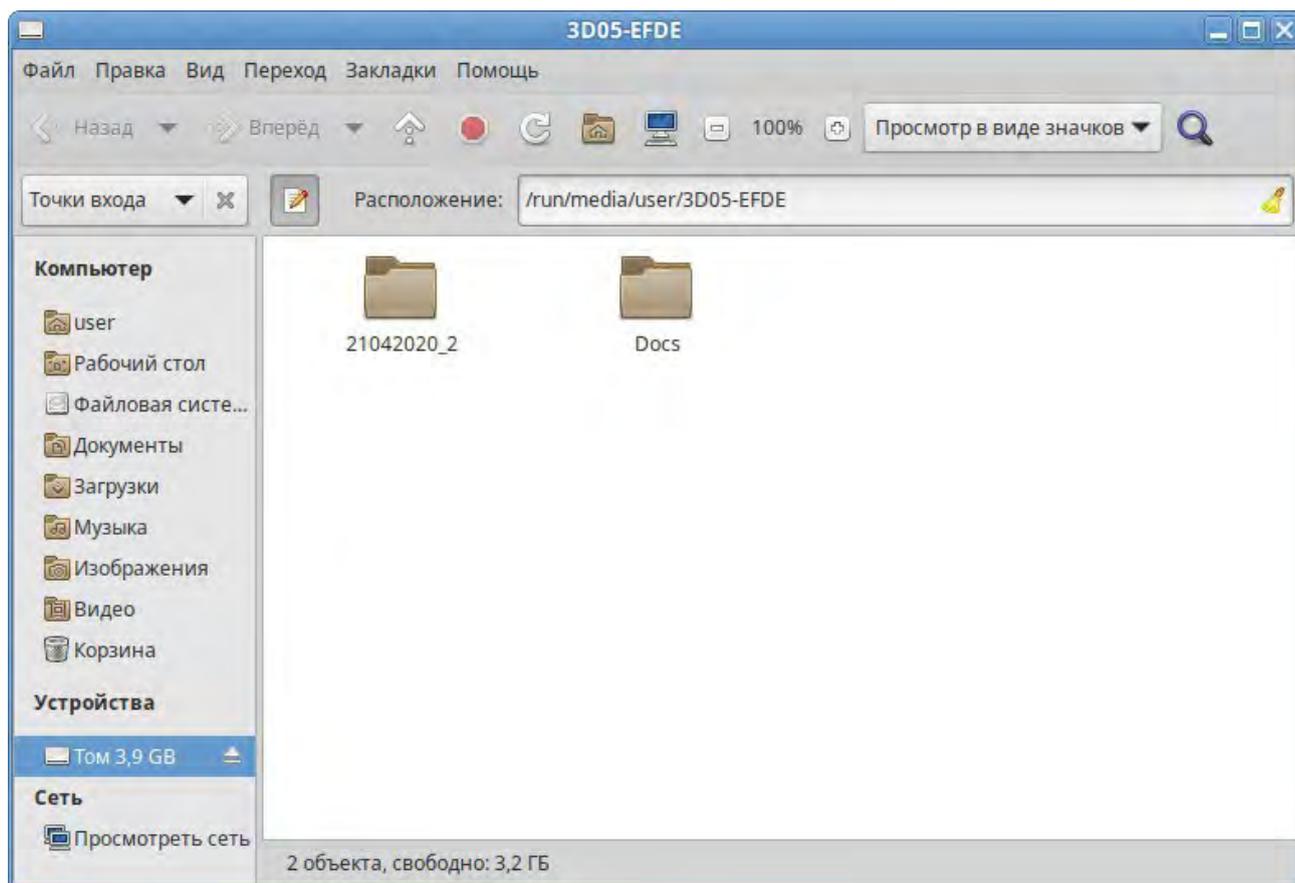


Рис. 34

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. Закрывать все окна диспетчера файлов, окна терминала и любые другие окна, осуществляющие доступ к USB-накопителю.
2. В контекстном меню носителя выбрать пункт «Извлечь» (Рис. 35).
3. Подождать, пока не исчезнет значок носителя (в окне файлового менеджера/с рабочего стола), затем извлечь носитель.

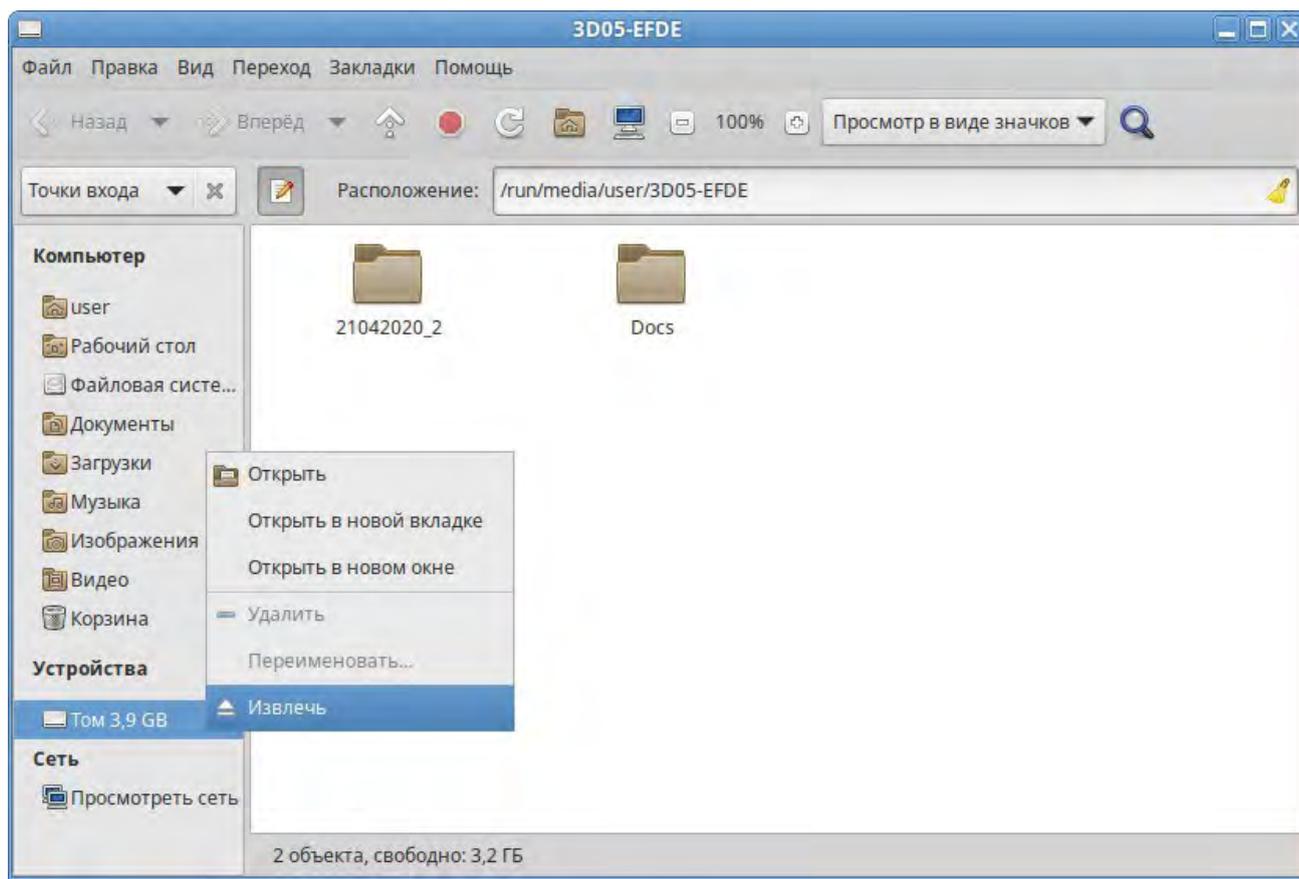
Извлечь носитель

Рис. 35

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 совпадать с основным паролем пользователя). Следует учитывать, что в базу данных Samba можно добавлять 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. 36) и нажать кнопку «Создать публикацию».

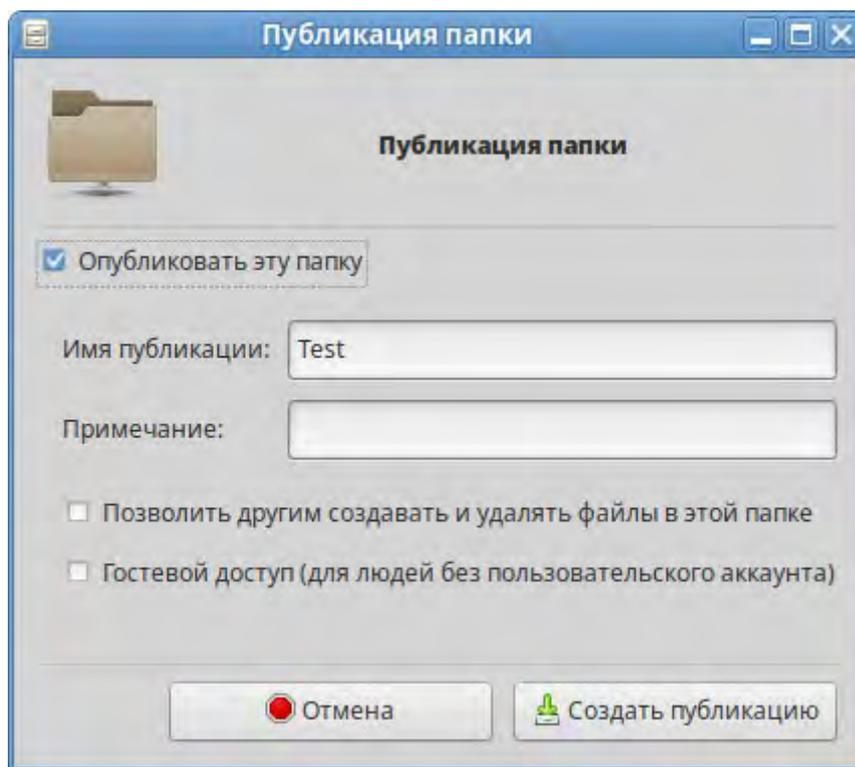
Разрешить общий доступ к папке

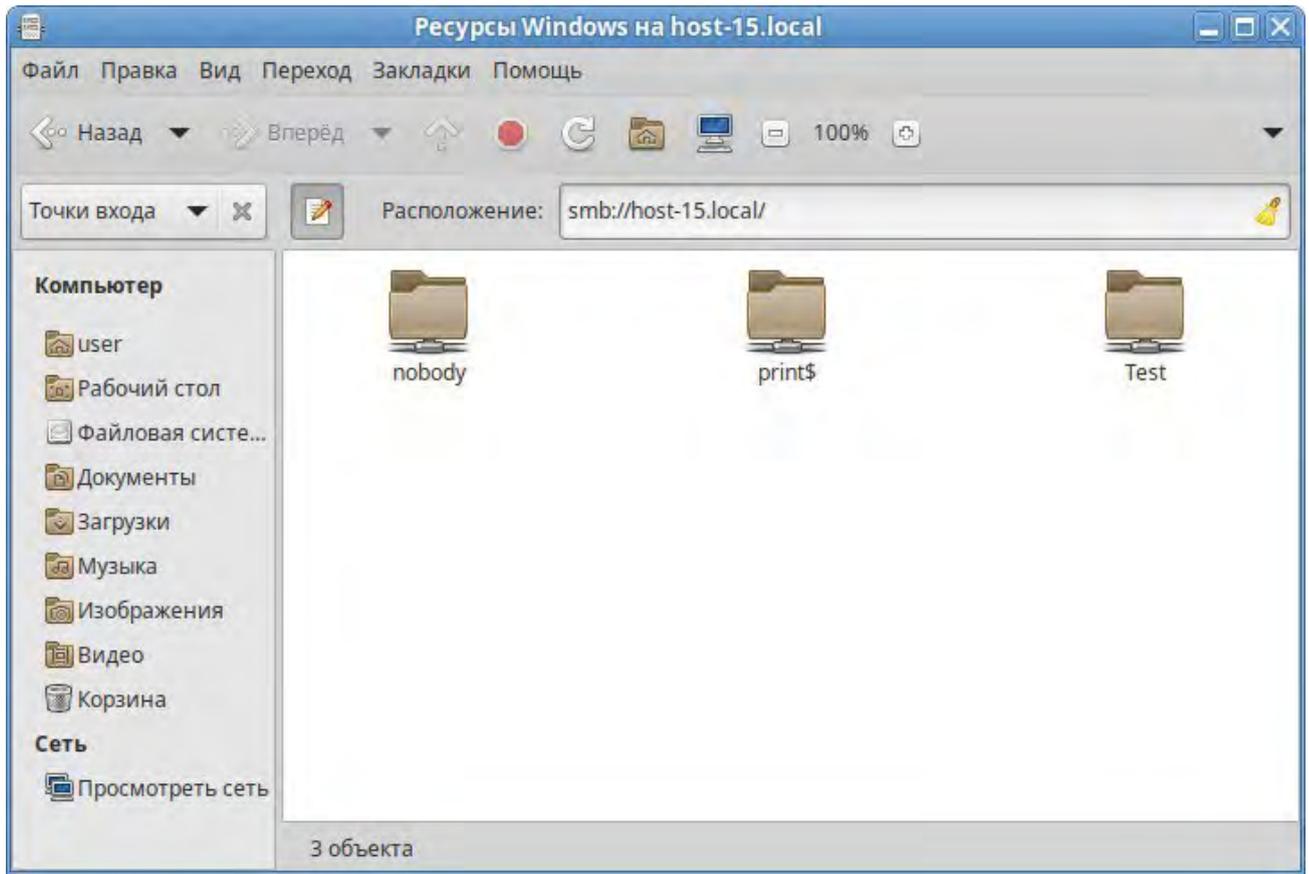
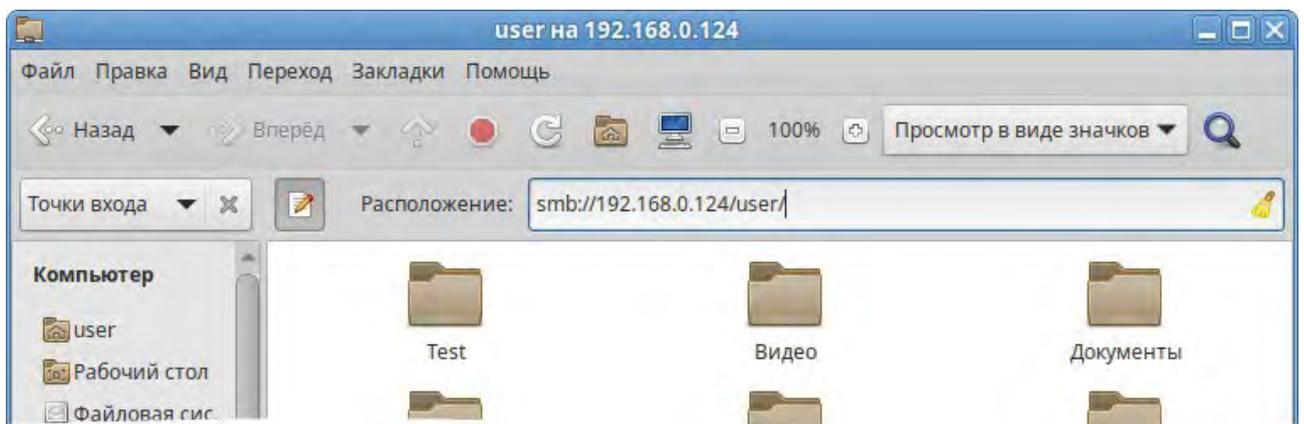
Рис. 36

Общие папки будут отображаться в разделе «Просмотреть сеть» файлового менеджера (Рис. 37). Также 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 `192.168.0.124`, необходимо указать в адресной строке `smb://192.168.0.124/user` (Рис. 38). Для возможности получения доступа к домашней папке по сети, необходимо добавить каждого локального пользователя в список пользователей Samba.

Для доступа к папке, к которой запрещен гостевой доступ, необходимо указать имя и пароль пользователя Samba, и нажать кнопку «Подключиться» (Рис. 39).

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. 40). В результате на боковой панели в разделе «Закладки» появится постоянная ссылка на сетевую папку.

Ресурсы с общим доступом*Рис. 37**Обращение к домашней папке пользователя user по сети**Рис. 38*

Параметры подключения к общей папке

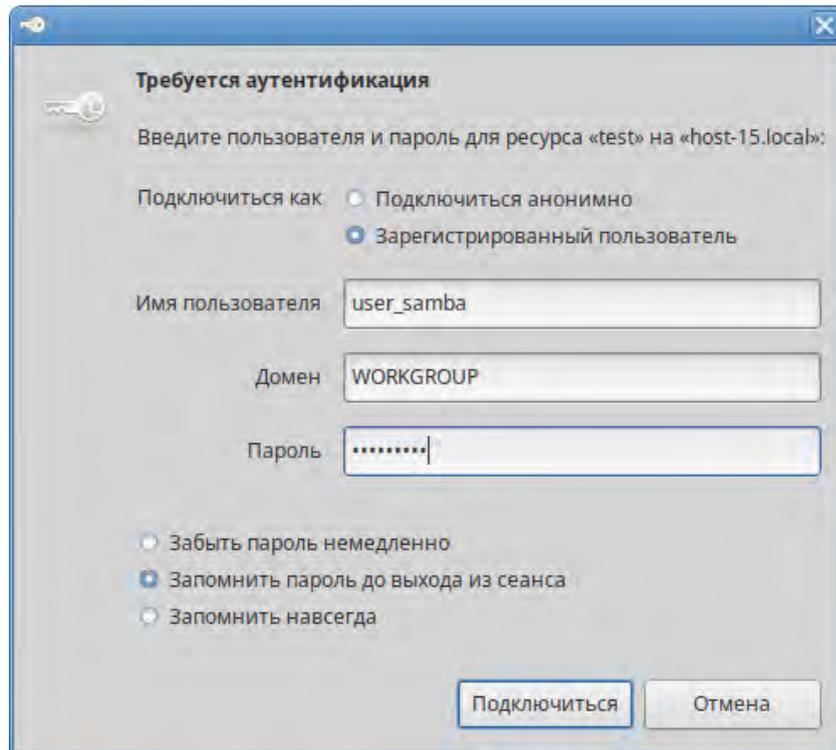


Рис. 39

Добавление закладки на сетевую папку

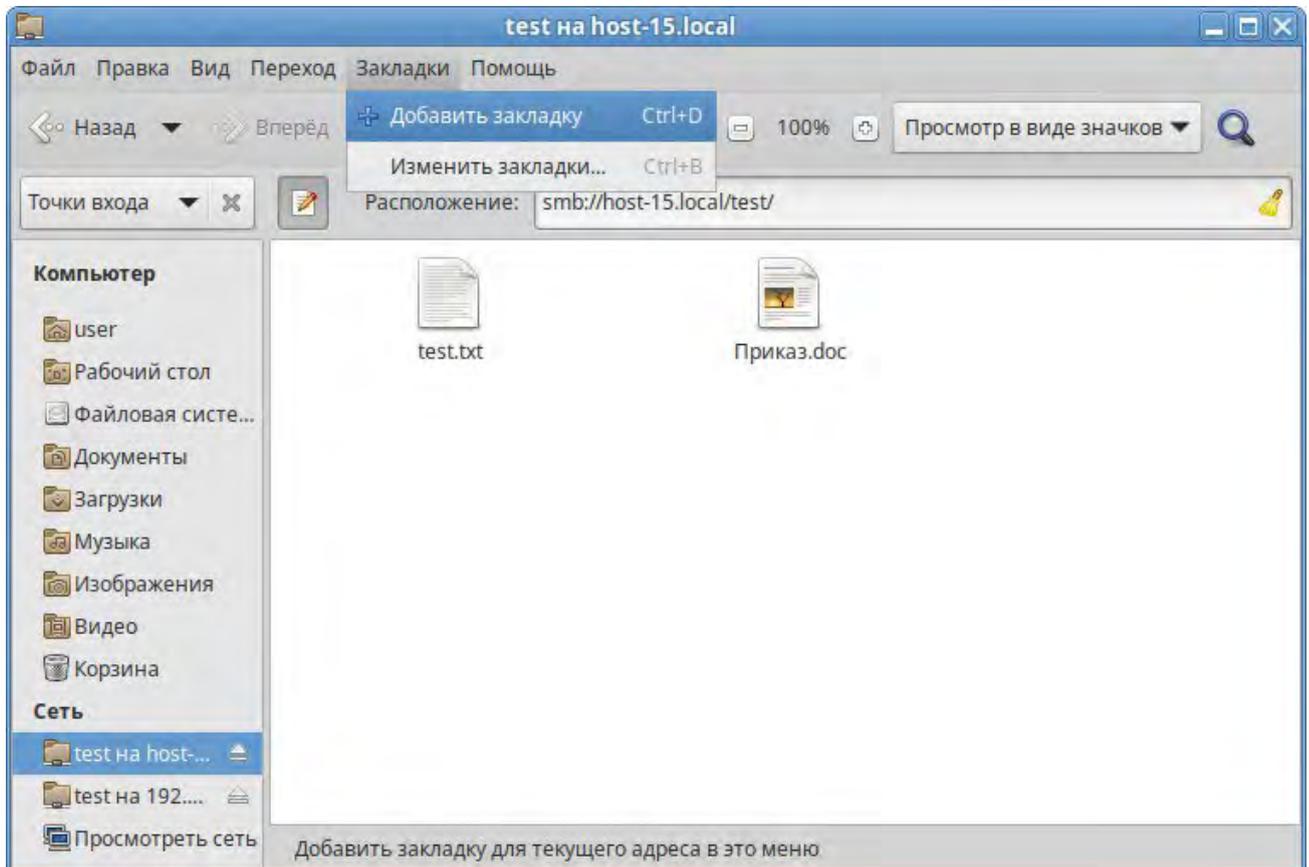


Рис. 40

3.6 Графика

ОС «Иридиум» 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 Программа для распознавания текста gImageReader

gImageReader программа для распознавания текста (GUI Tesseract).

Особенности gImageReader:

- поддерживаемые форматы изображений: jpeg, png, tiff, gif, pnm, psx, 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. 41). 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.

Распознанный текст отображается непосредственно рядом с изображением. Базовое редактирование текста включает поиск/замену и удаление сломанных строк, если это возможно. Также 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. 42).

Окно программы gImageReader

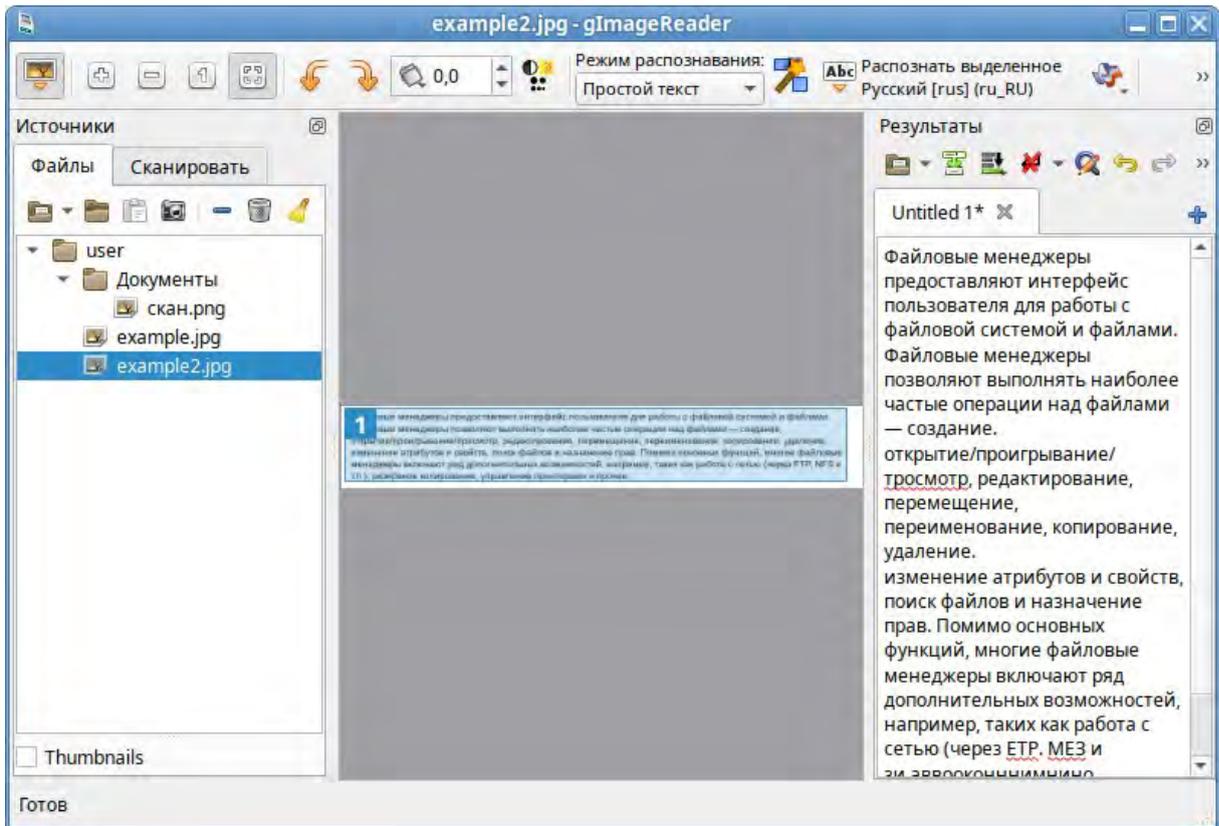


Рис. 41

Сканирование в окне программы gImageReader

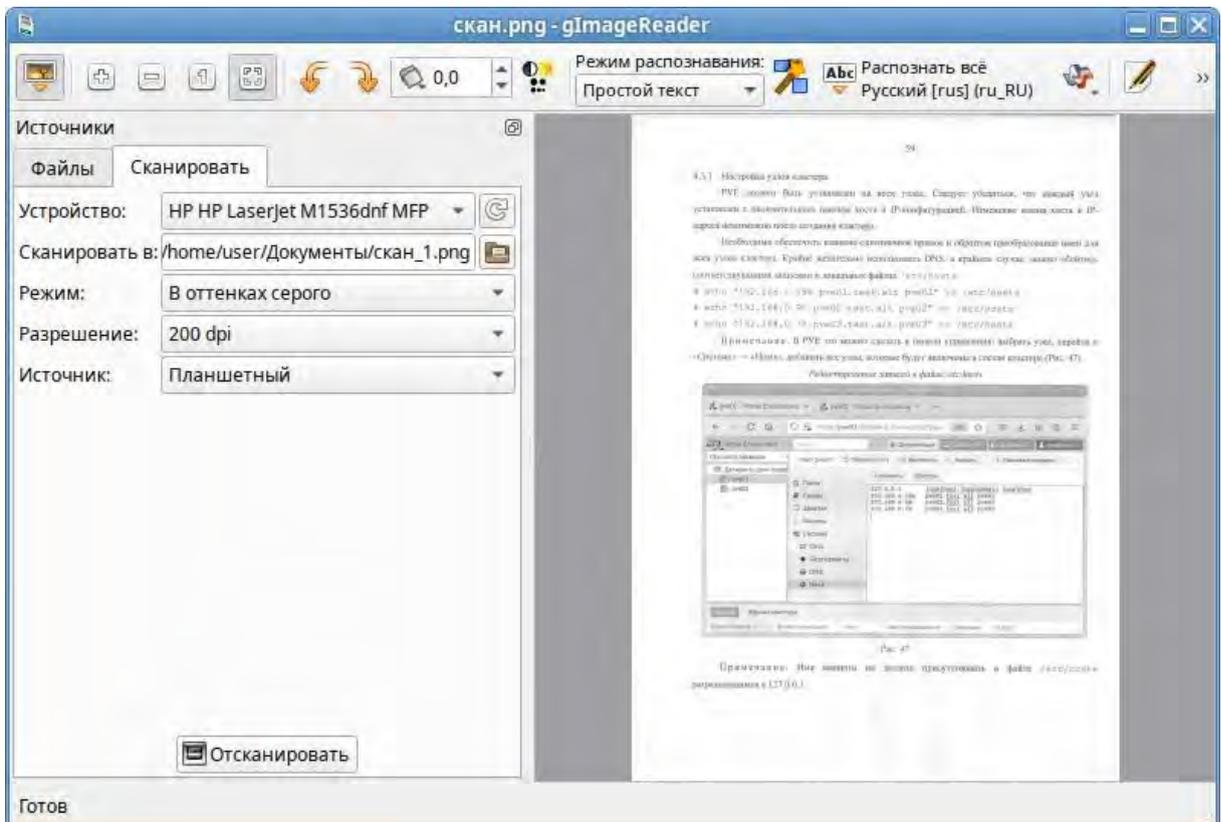


Рис. 42

3.6.2 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.

Если программа нашла подключенный к системе сканер, будет открыт основной интерфейс приложения Xsane (Рис. 43).

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.

Интерфейс приложения Xsane

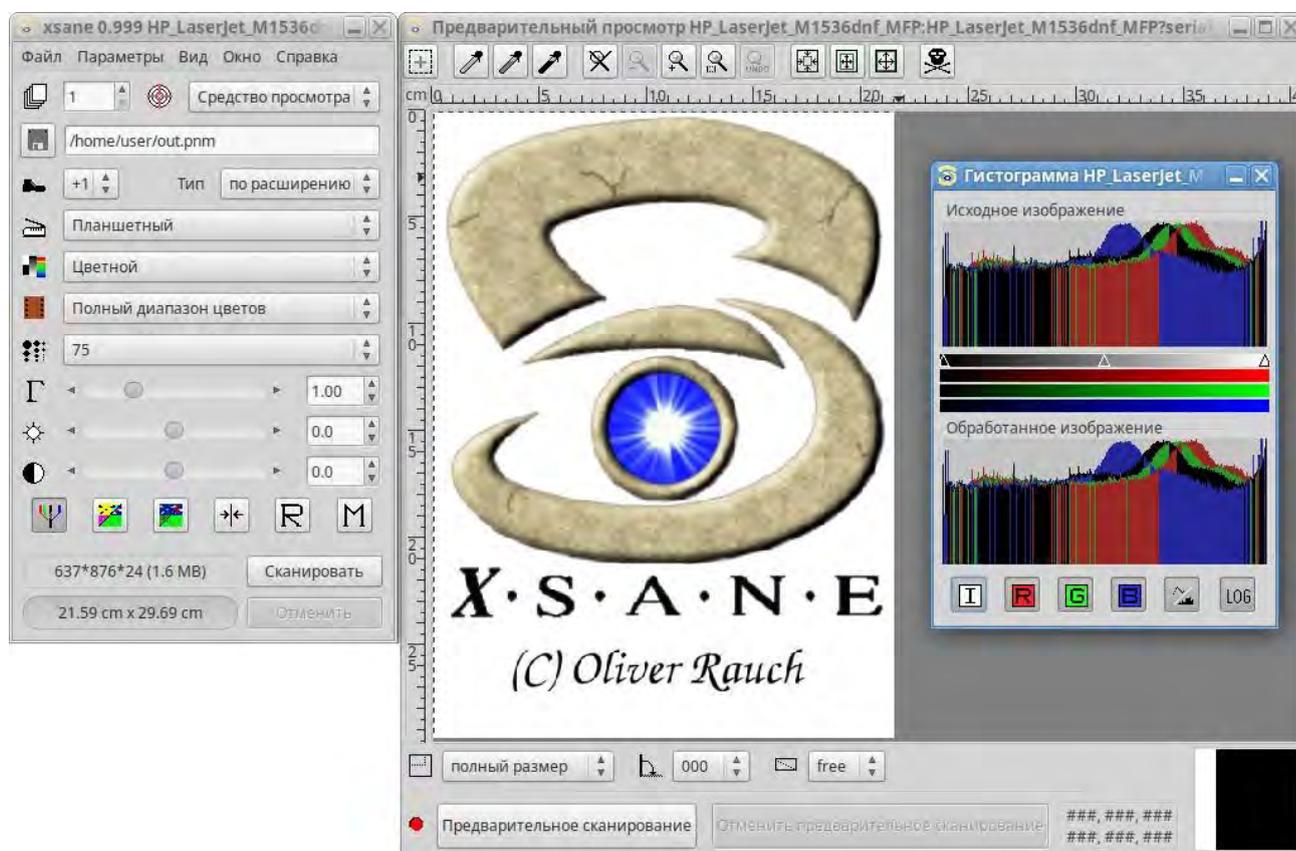


Рис. 43

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. 44) можно воспользоваться инструментами преобразования изображений (поворот, отражение, масштабирование и т.п.) и затем сохранить скорректированную сканкопию.

Результат сканирования в окне просмотра

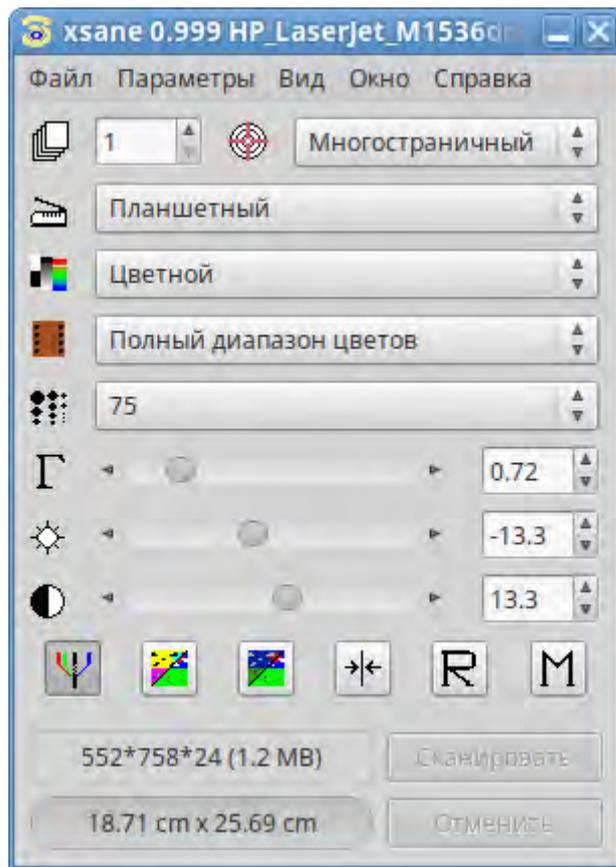
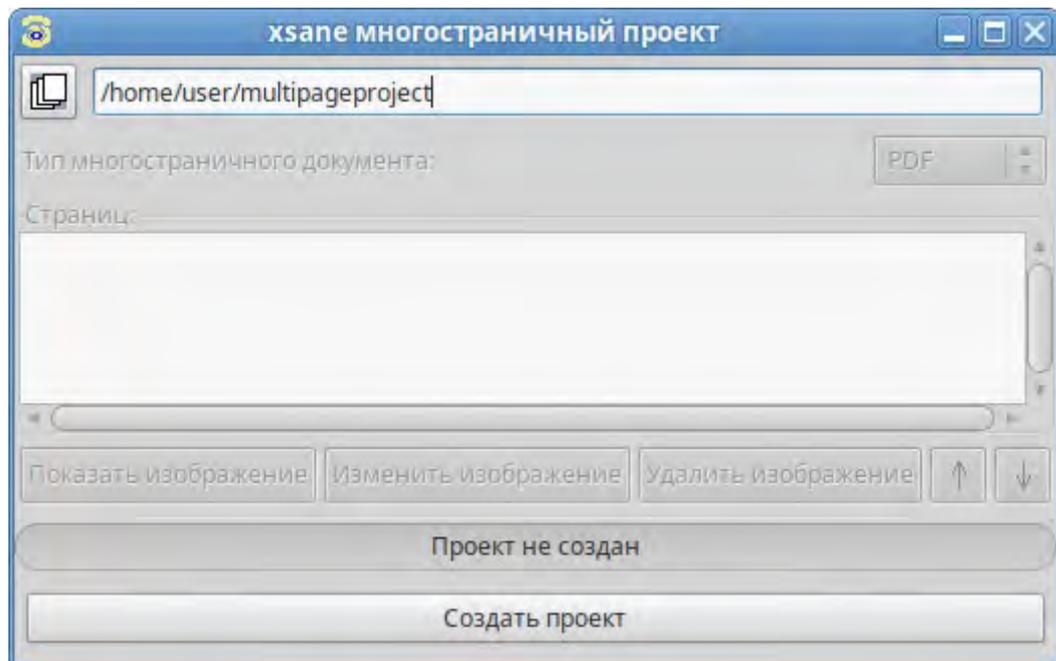


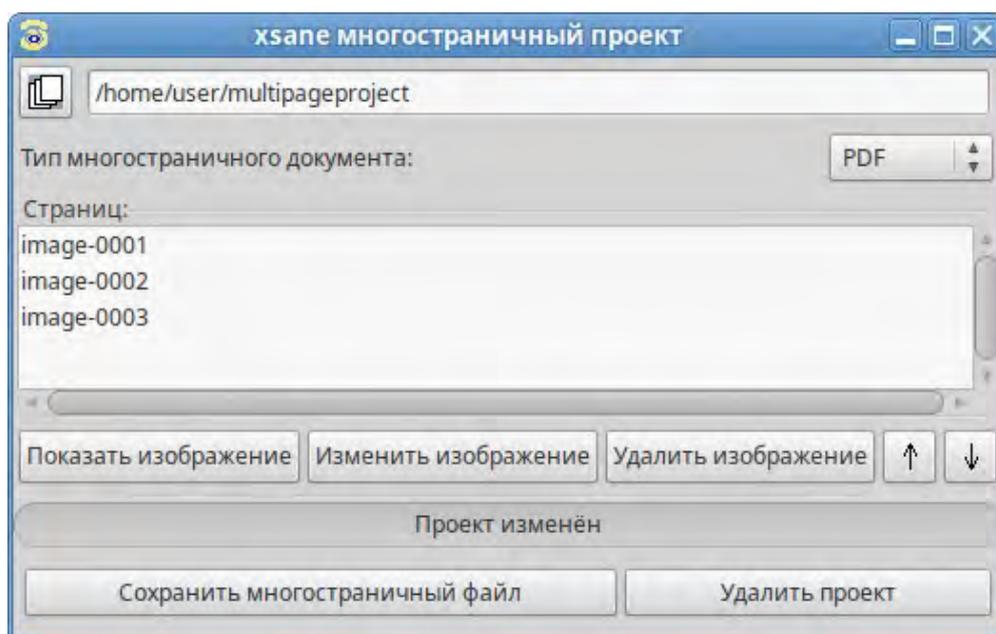
Рис. 44

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:

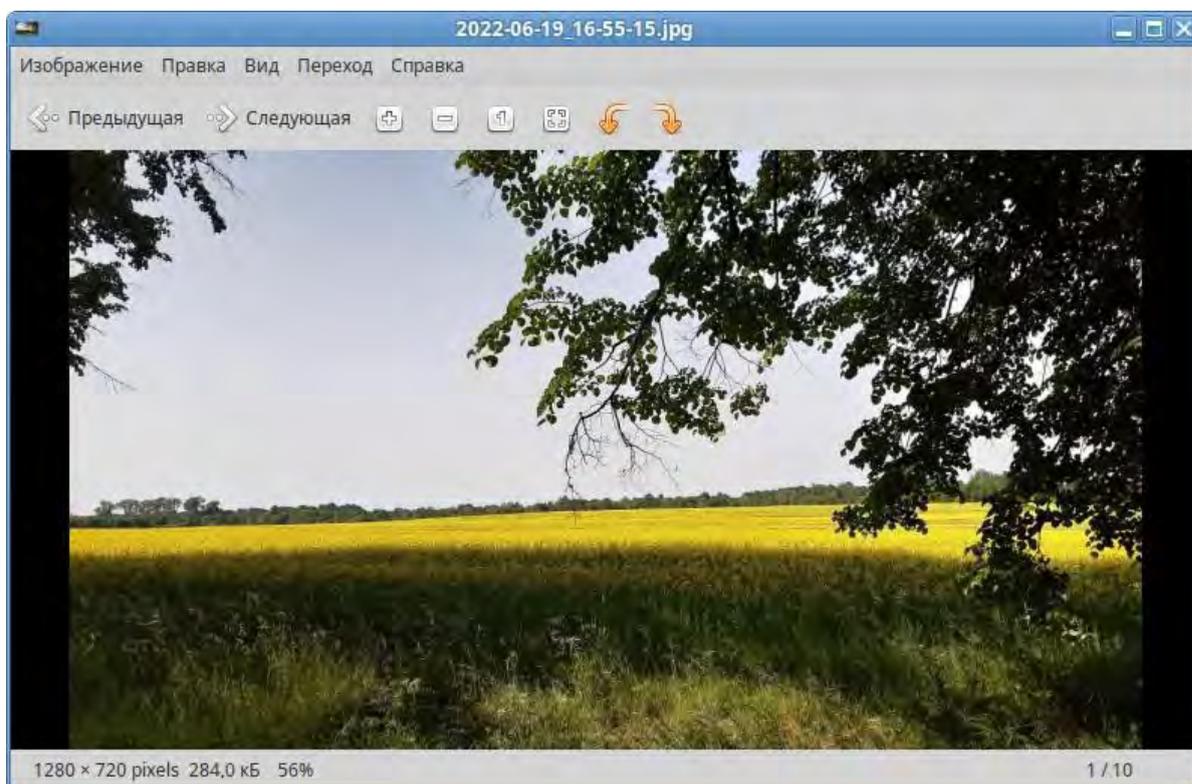
- в основном окне Xsane выбрать назначение сканирования «Многостраничный» (Рис. 45);
- в открывшемся окне «Многостраничный проект», ввести имя создаваемого многостраничного файла и нажать кнопку «Создать проект» (Рис. 46);
- перейти в окно «Предварительный просмотр» и отметить область сканирования (если 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. 47);
- выбрать тип многостраничного документа (pdf, tiff или PostScript) в соответствующем выпадающем списке и нажать кнопку «Сохранить многостраничный файл».

Xsane. Настройки сканирования*Рис. 45**Xsane. Создание многостраничного документа**Рис. 46*

Xsane. Многостраничный проект*Рис. 47*

3.6.3 Глаз МАТЕ

Глаз МАТЕ является простым приложением для просмотра изображений. После загрузки изображения (Рис. 48), можно увеличивать его масштаб, вращать изображение, а также просматривать другие изображения из каталога, в котором находится открытое изображение.

Окно программы Глаз МАТЕ*Рис. 48*

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.

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. 49):

- 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

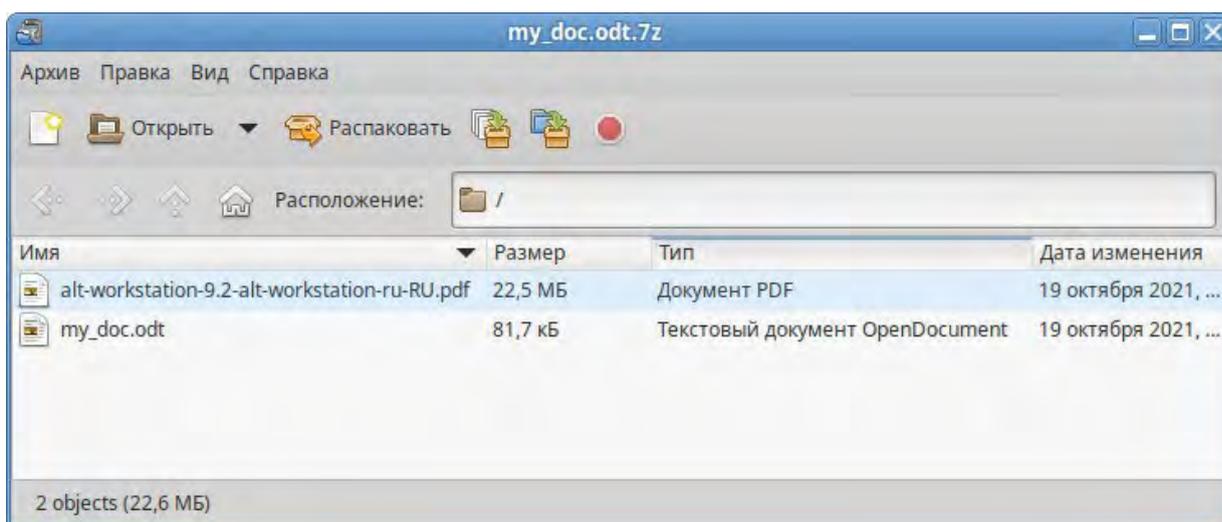


Рис. 49

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. 50);
- в открывшемся окне необходимо ввести имя архива, выбрать из выпадающего списка тип архива, выбрать место для хранения архива и нажать кнопку «Создать» (Рис. 51).

Добавление файлов в архив

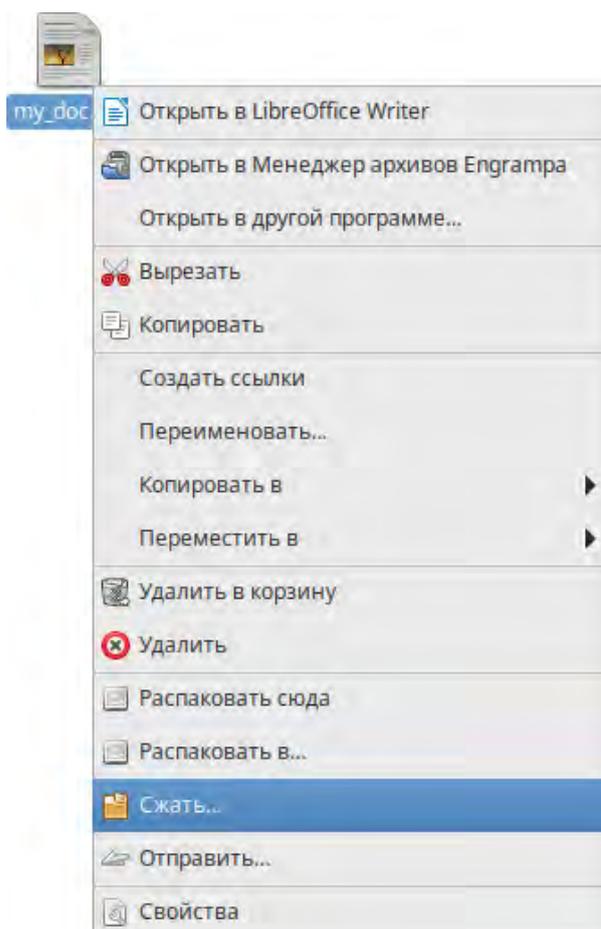


Рис. 50

Создание архива

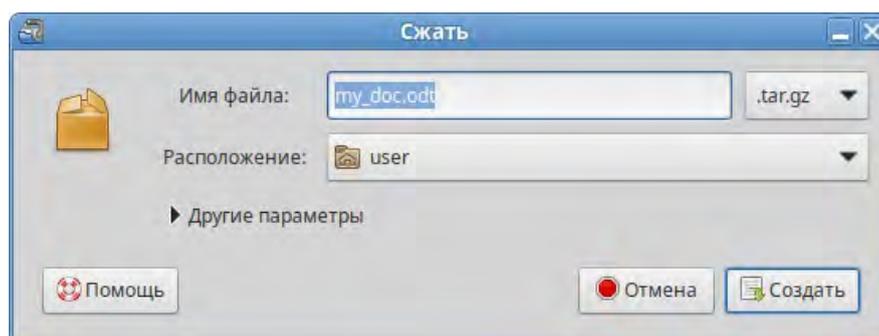


Рис. 51

При создании нового архива можно указать дополнительные параметры, раскрыв пункт «Другие параметры» в окне создания архива. Можно указать следующие дополнительные параметры (Рис. 52):

- «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

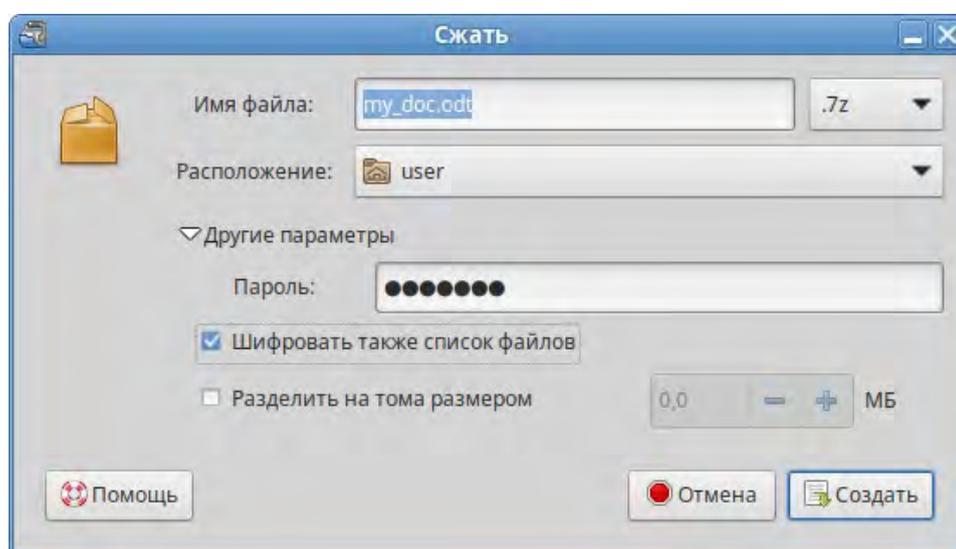


Рис. 52

Для того чтобы извлечь файлы из архива, следует в контекстном меню архива выбрать пункт «Распаковать сюда» (Рис. 53) – файлы будут распакованы в текущий каталог, или «Распаковать в...» – можно указать каталог, куда будут извлечены файлы.

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 МАТЕ» → «Приложения» → «Системные» → «Системный монитор МАТЕ».

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. 54) 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.

Извлечение файлов из архива

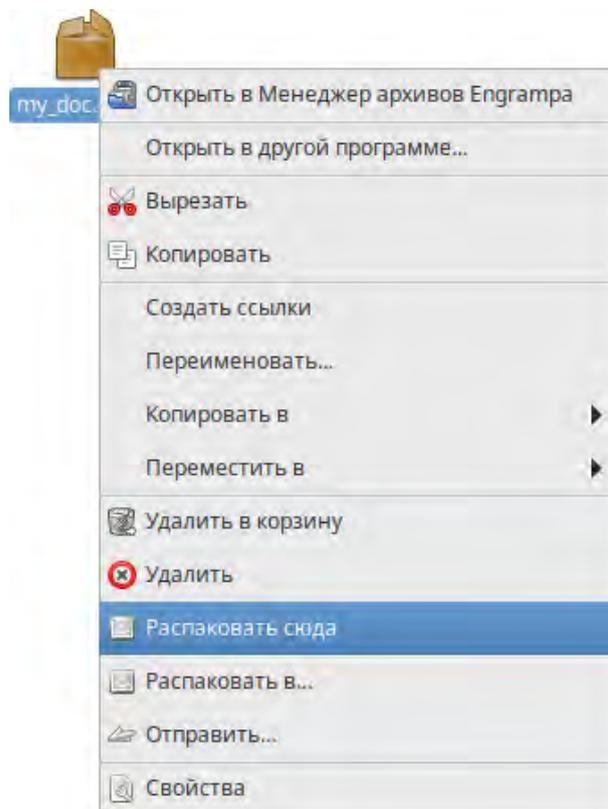


Рис. 53

При щелчке правой кнопкой мыши по любому запущенному процессу, открывается контекстное меню (Рис. 55), 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

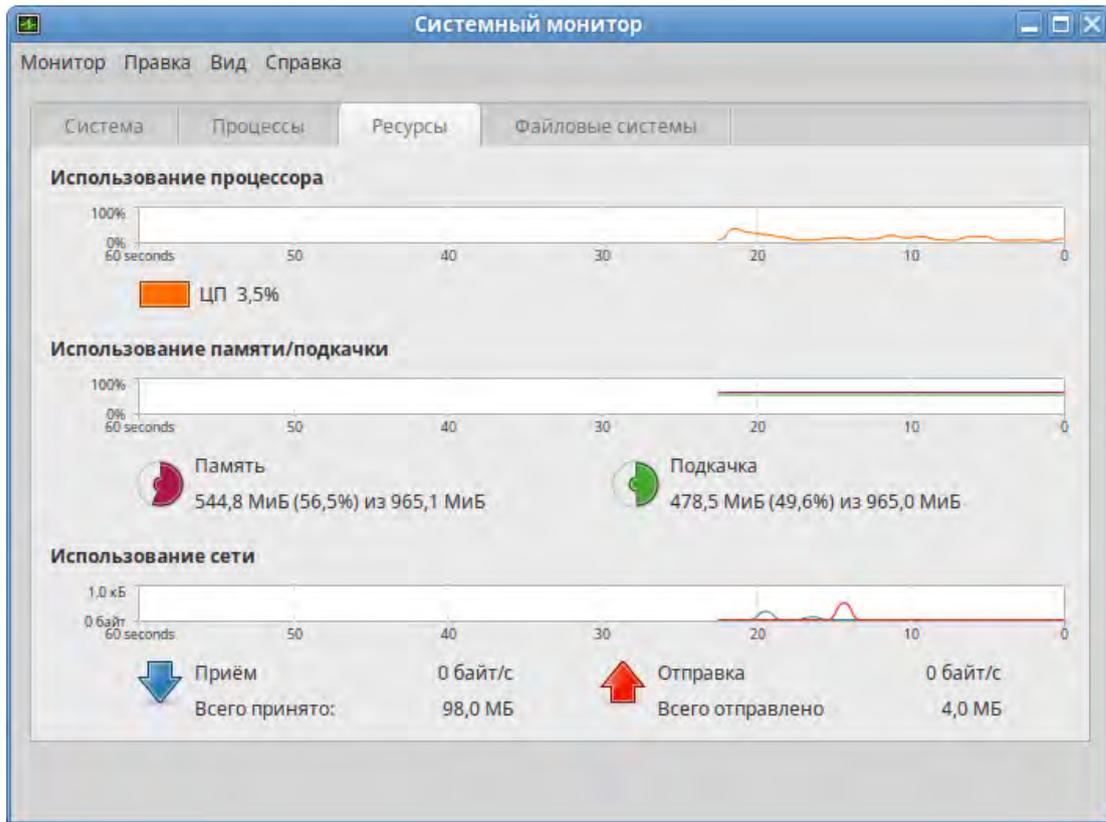


Рис. 54

Контекстное меню процесса

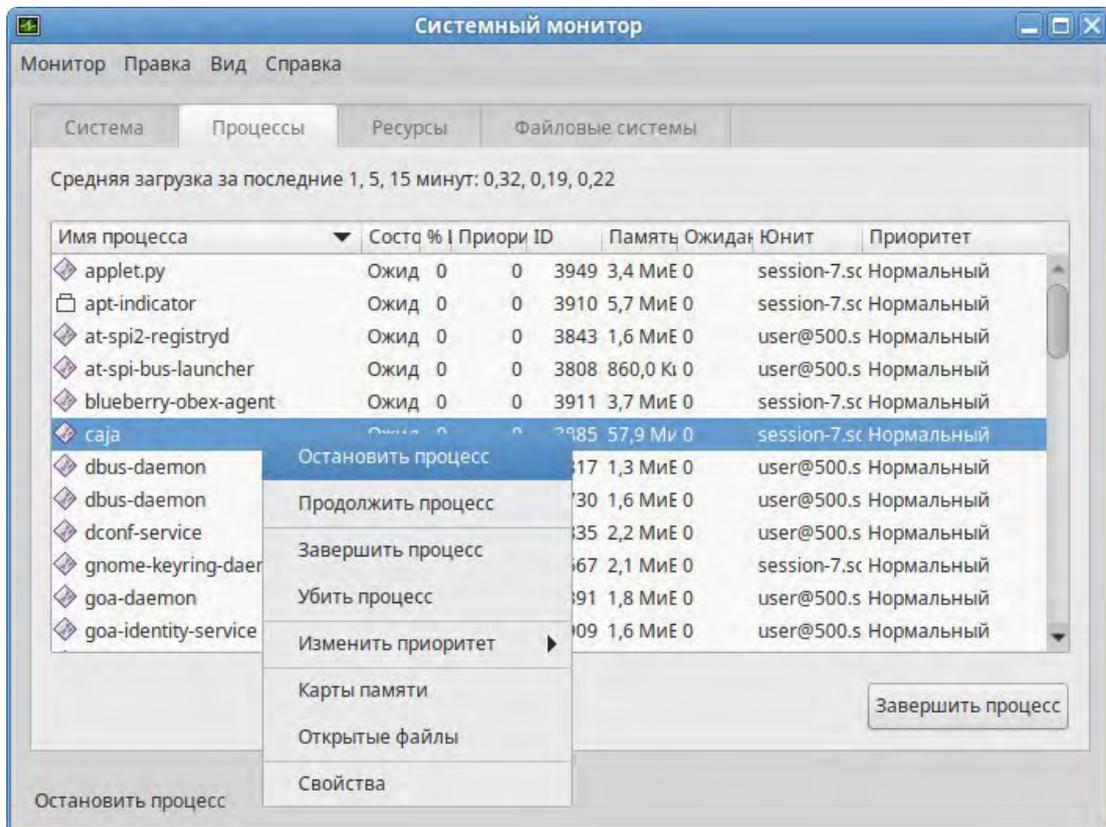


Рис. 55

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. 56);
- если выбрать пункт «Вручную», откроется диалоговое окно «Изменить приоритет процесса...» (Рис. 57), 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

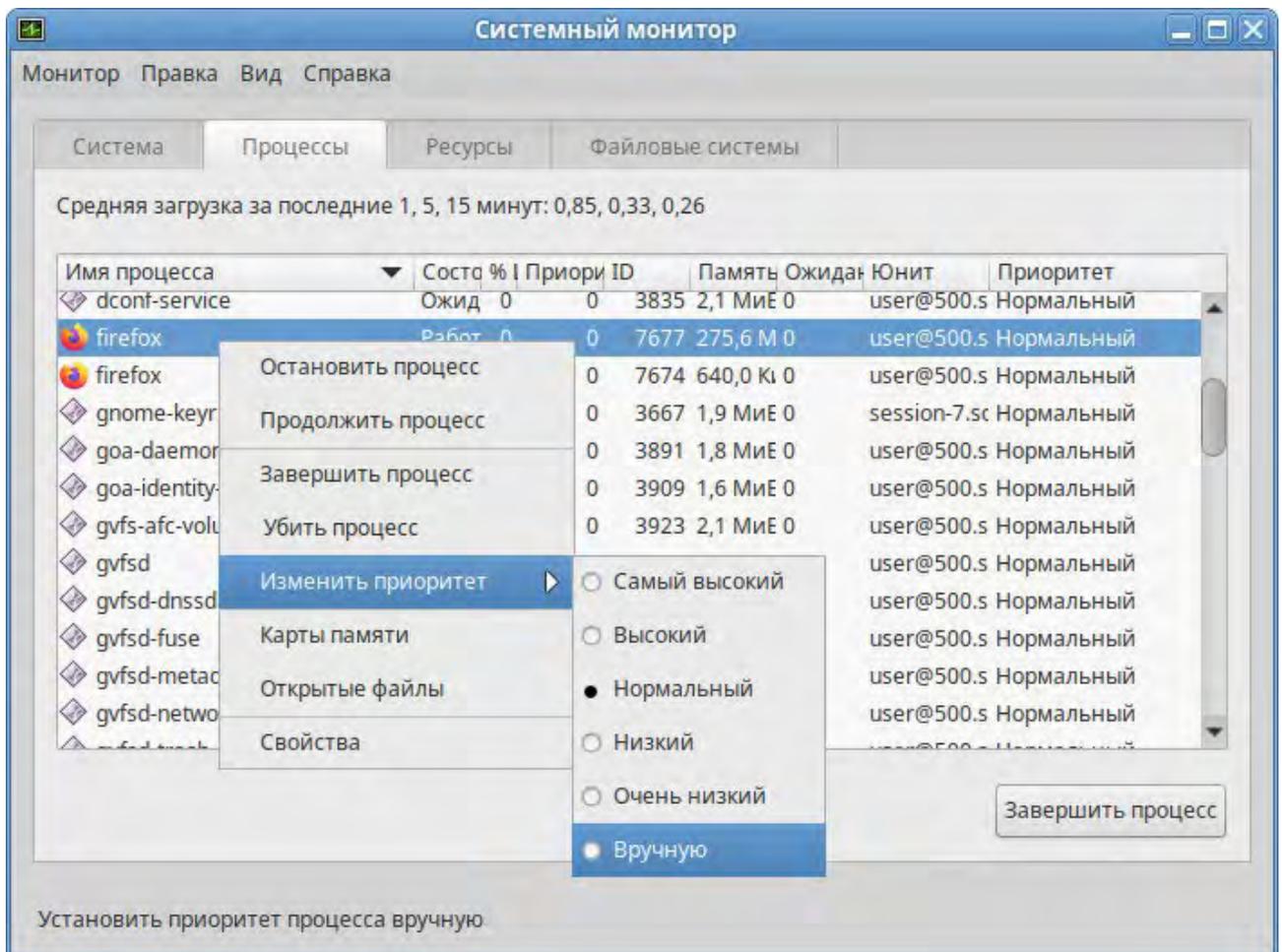


Рис. 56

Диалоговое окно «Изменить приоритет процесса...»

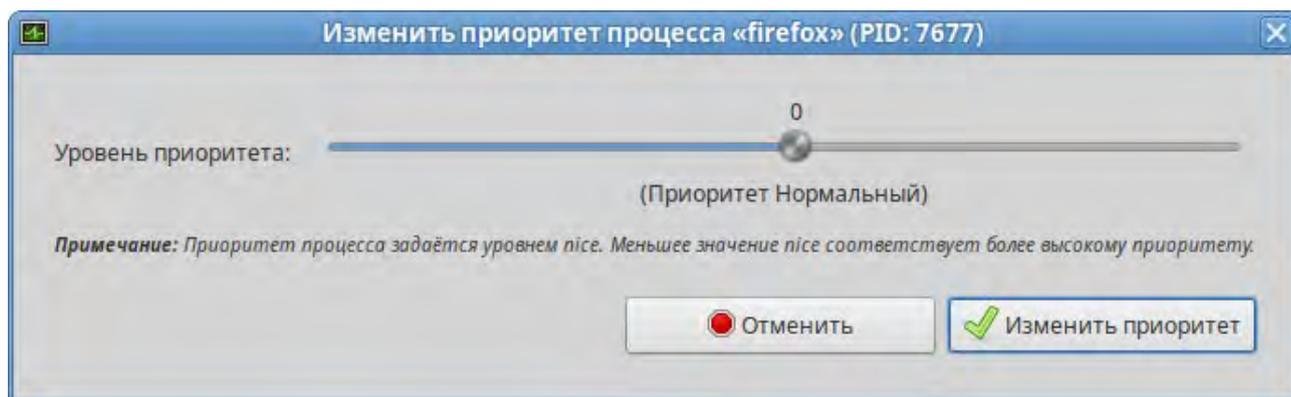


Рис. 57

Примечание. Для установки более высокого приоритета, чем тот, который уже установлен у процесса, потребуется ввести пароль пользователя, находящегося в группе wheel.

3.9 Центр приложений

Центр приложений позволяет легко устанавливать и удалять программы из репозитория 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 МАТЕ» → «Приложения» → «Системные» → «Центр приложений».

Вся информация распределена по двум вкладкам (Рис. 58):

- на вкладке «Все» («Explore») показаны доступные приложения;
- вкладка «Установлено» позволяет просматривать и удалять установленные приложения (Рис. 59).

Центр приложений

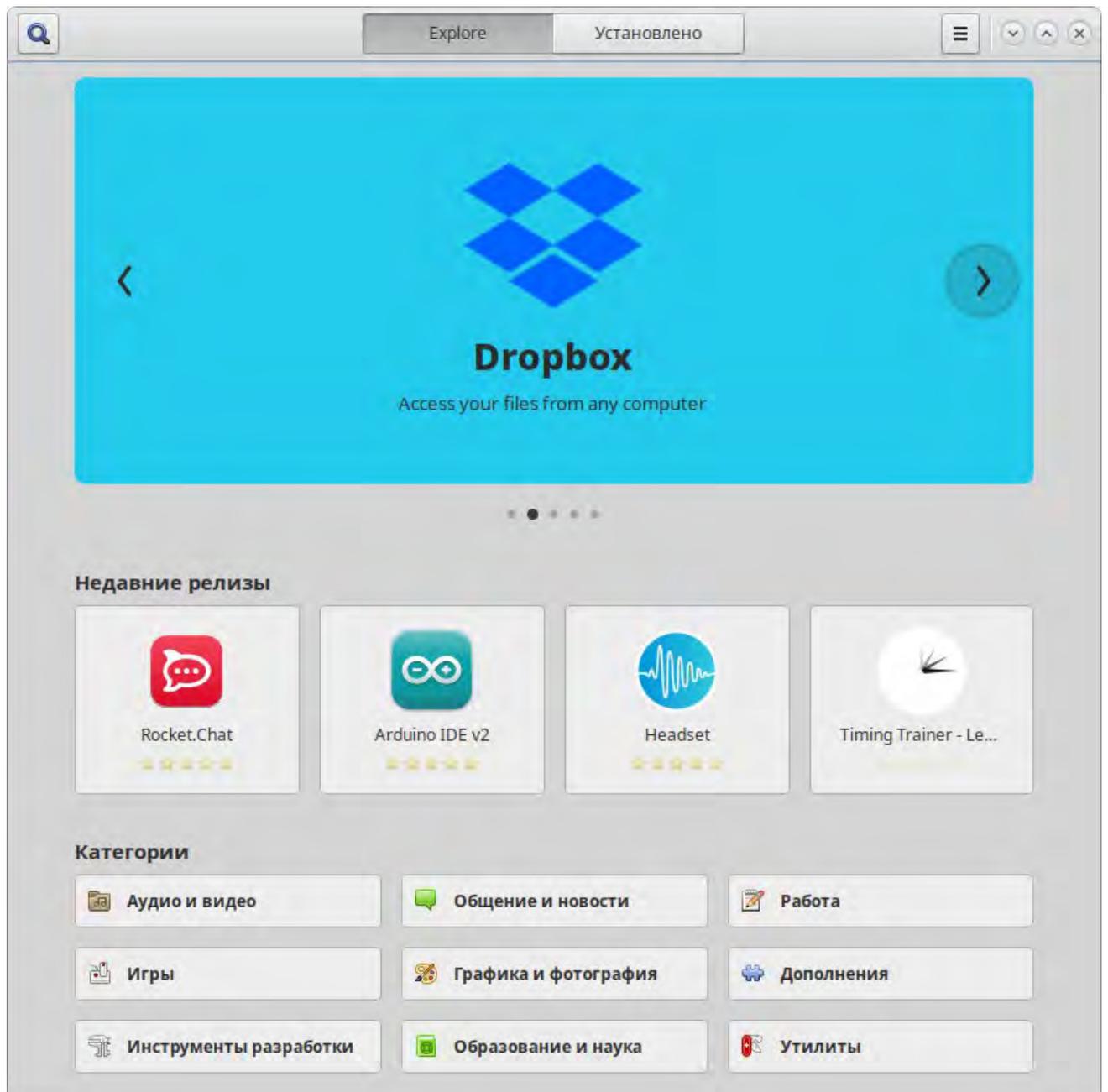


Рис. 58

Центр приложений. Вкладка «Установлено»

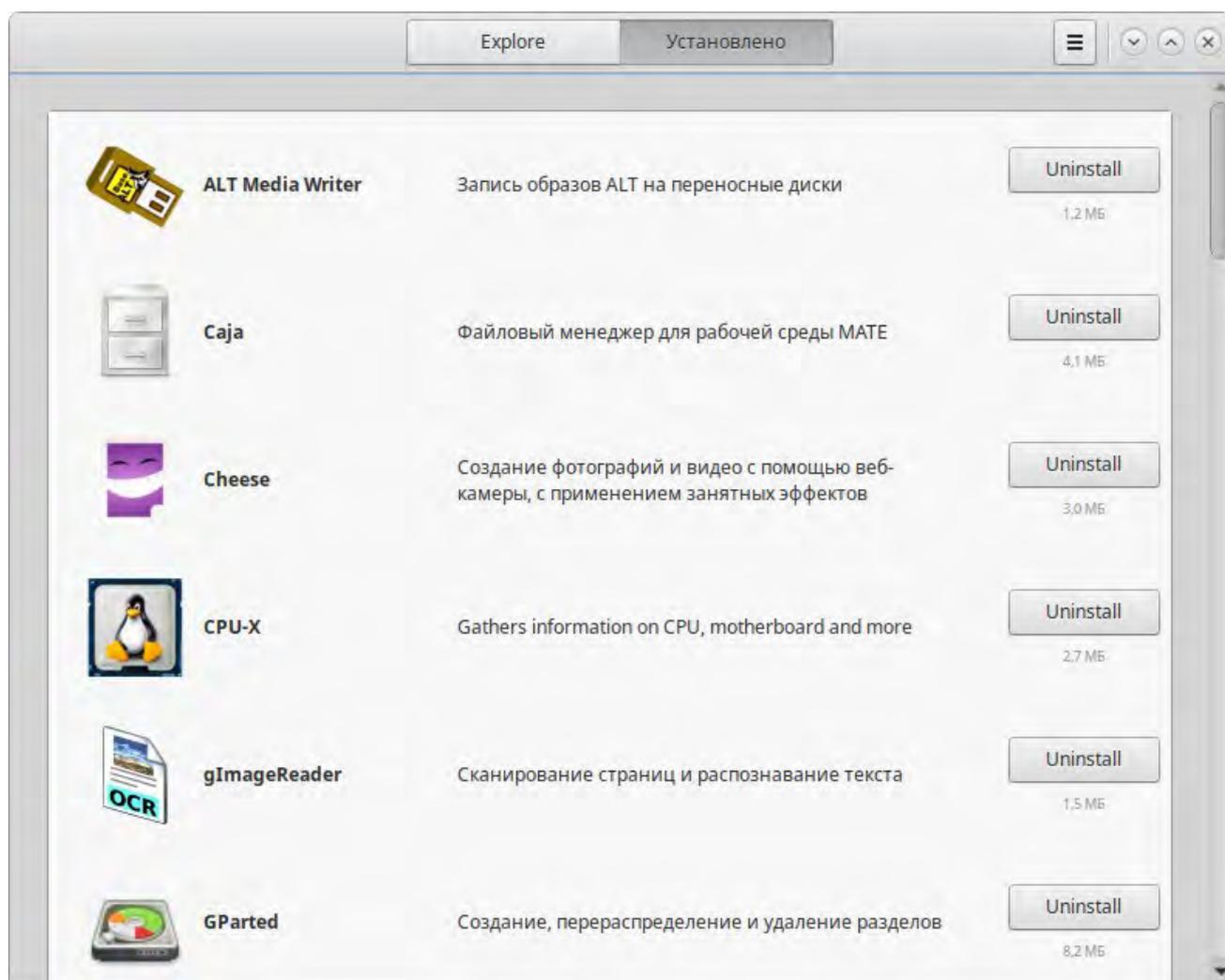
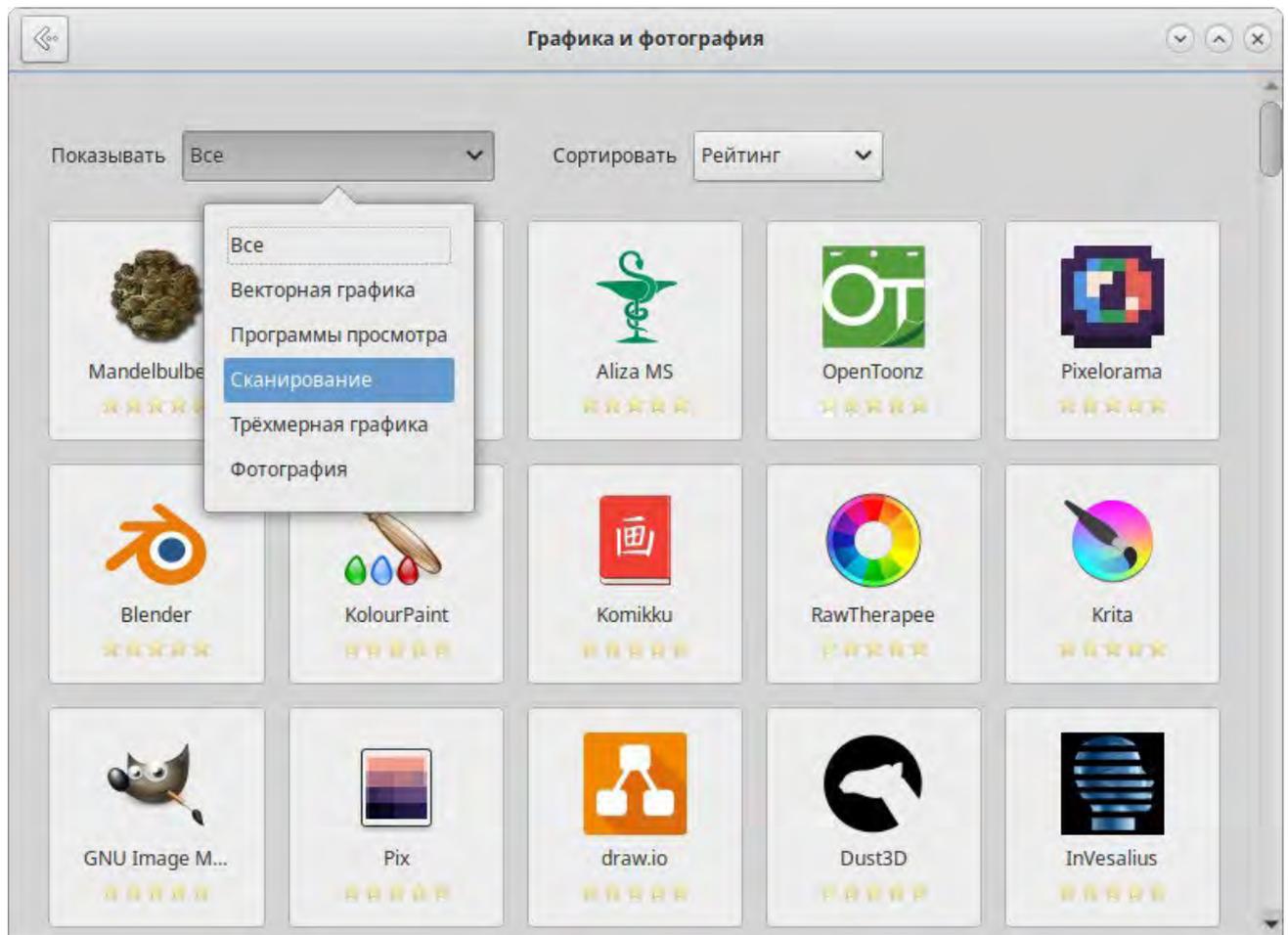


Рис. 59

На вкладке «Все» («Explore») доступные приложения разбиты на категории. Чтобы найти приложение, следует выбрать категорию приложения. Внутри группы, в выпадающем списке «Показывать», можно дополнительно выбрать подкатеорию, тем самым сократив область поиска (Рис. 60).

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. 61). Чтобы установить какое-либо приложение сначала нужно его найти, затем выбрать из списка и нажать на кнопку «Установить».

Центр приложений. Категория «Графика и фотография»*Рис. 60*

Центр приложений. Детальный просмотр приложения «Krita»

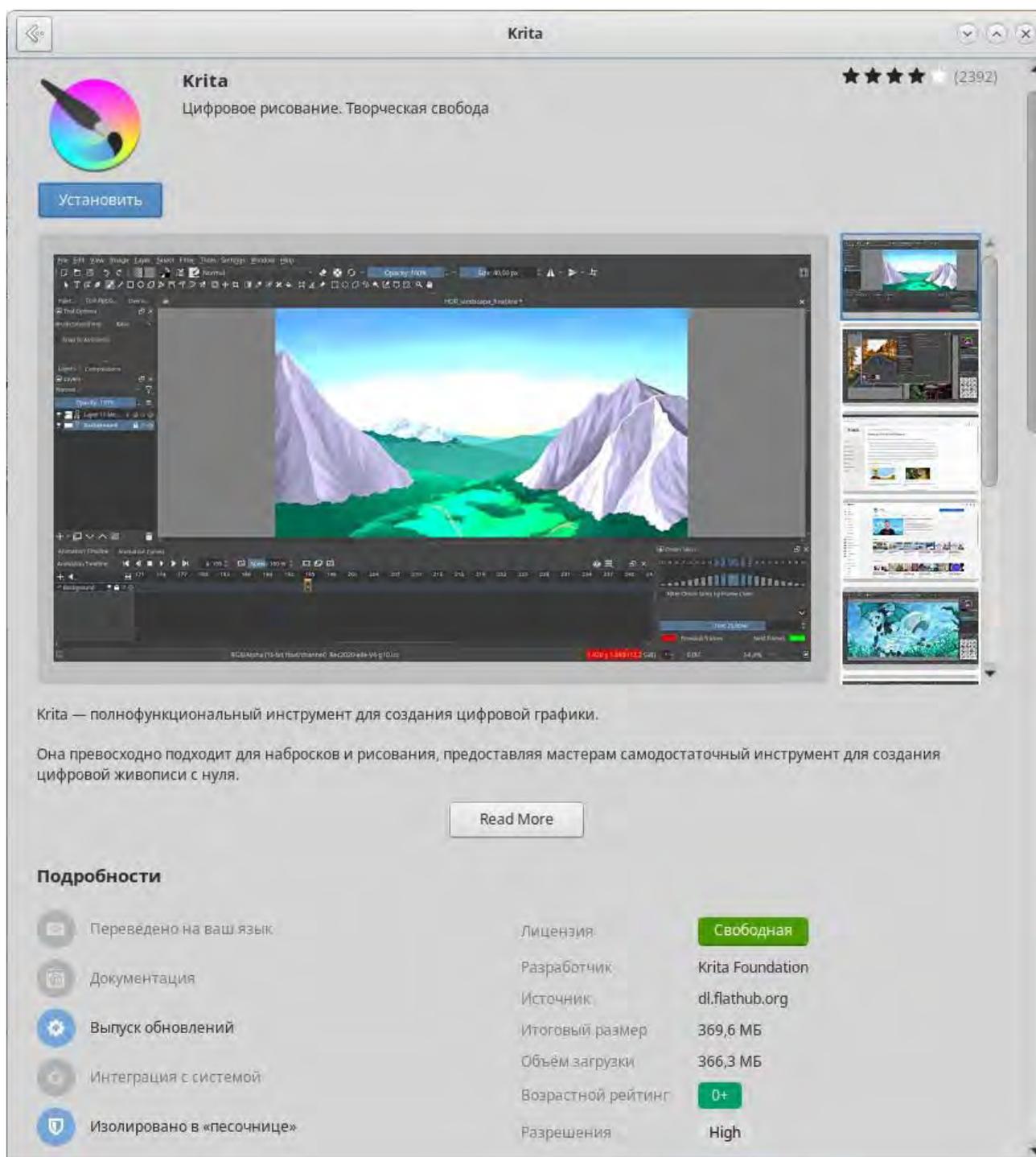
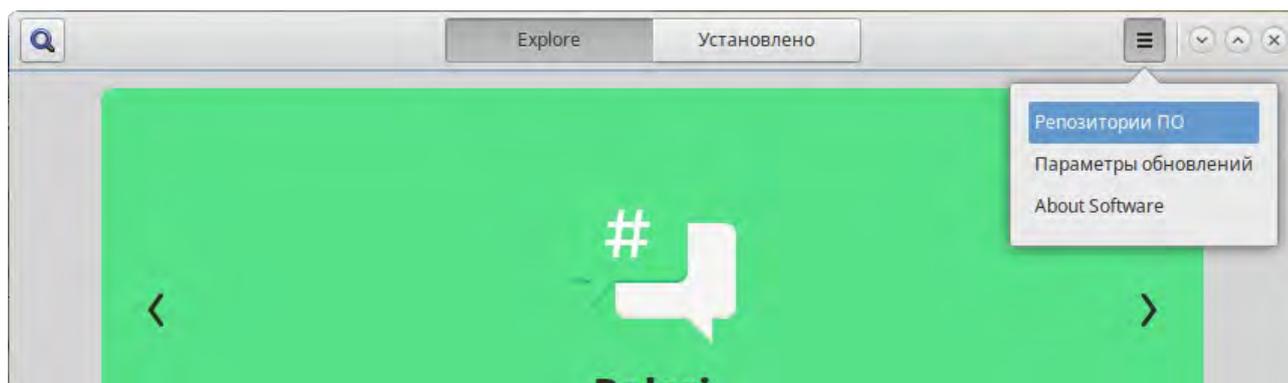


Рис. 61

Чтобы установить приложение, нужно нажать на кнопку «Установить».

Примечание. При установке/удалении программ потребуется ввести пароль пользователя входящего в группу wheel.

Список подключенных репозиторийов можно просмотреть, нажав на кнопку дополнительных сведений (Рис. 62) и выбрав пункт «Репозитории ПО».

Центр приложений. Кнопка дополнительных сведений*Рис. 62*

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 `erpm play` (см. раздел «Единая команда управления пакетами (`erpm`)»).

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. 63).

Графический интерфейс к *ert play*

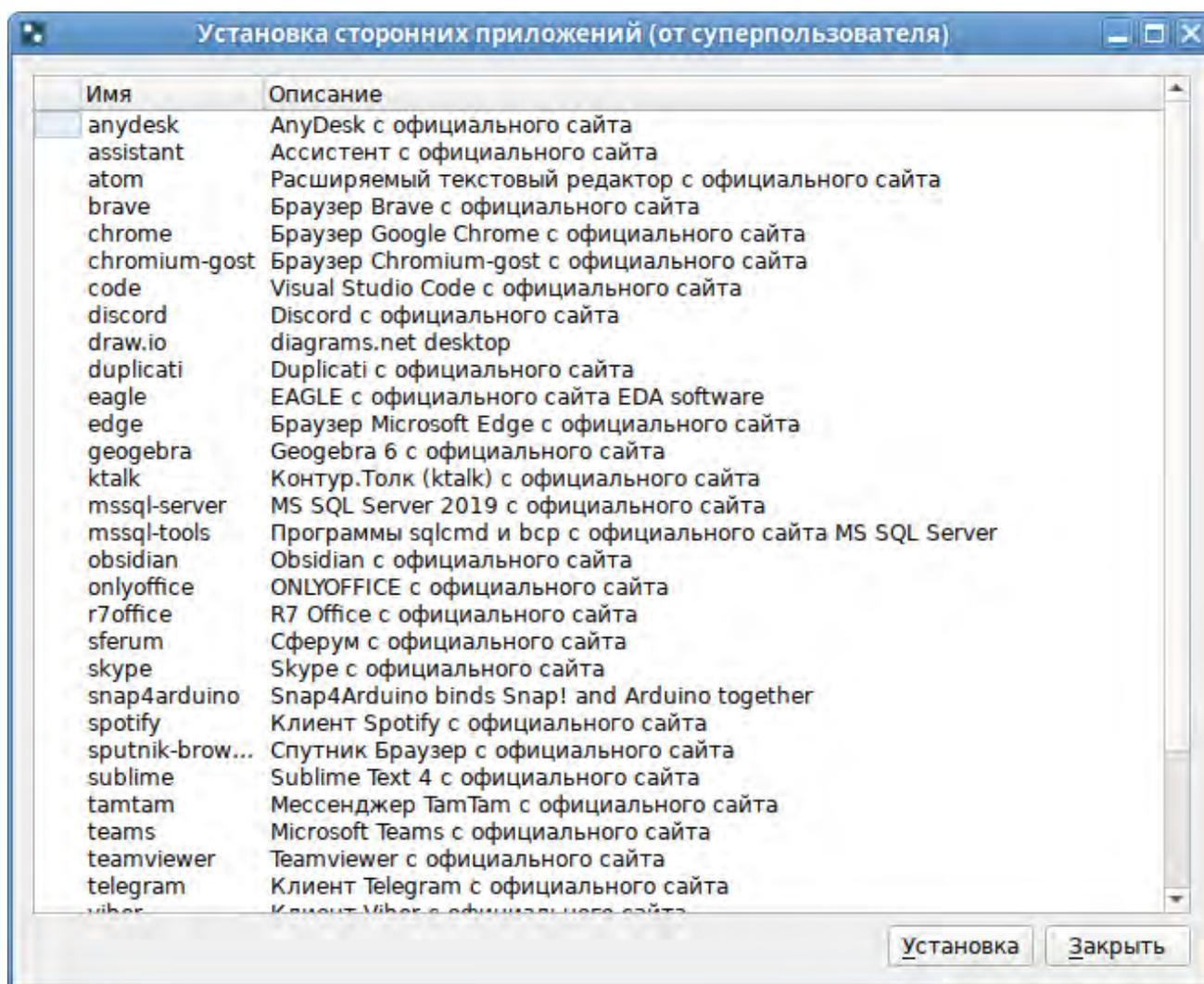


Рис. 63

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 МАТЕ» 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. 64).

Настройка первого индексирования

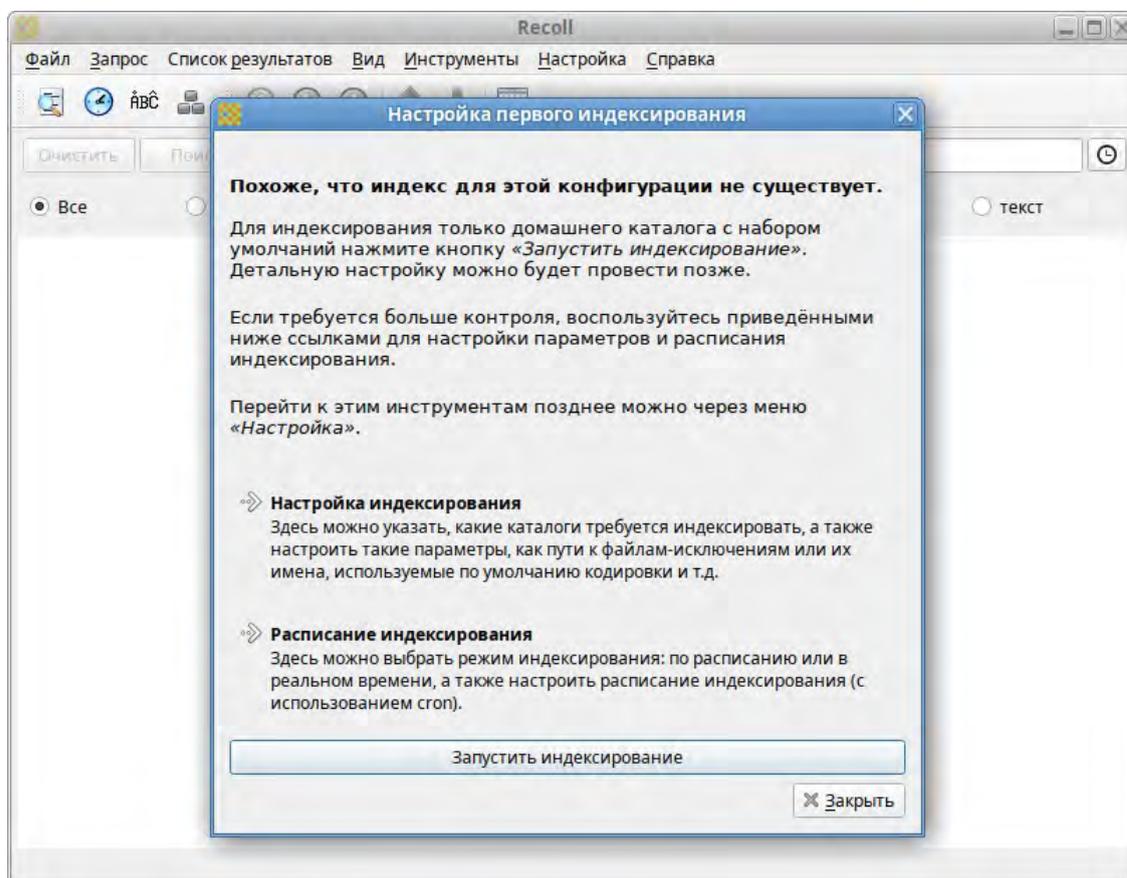


Рис. 64

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 «Настройка» → «Настройка индекса». Окно настройки индексации разделено на четыре вкладки: «Общие параметры», «Частные параметры», «Просмотренные веб-страницы» и «Параметры поиска».

На вкладке «Общие параметры» (Рис. 65) 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

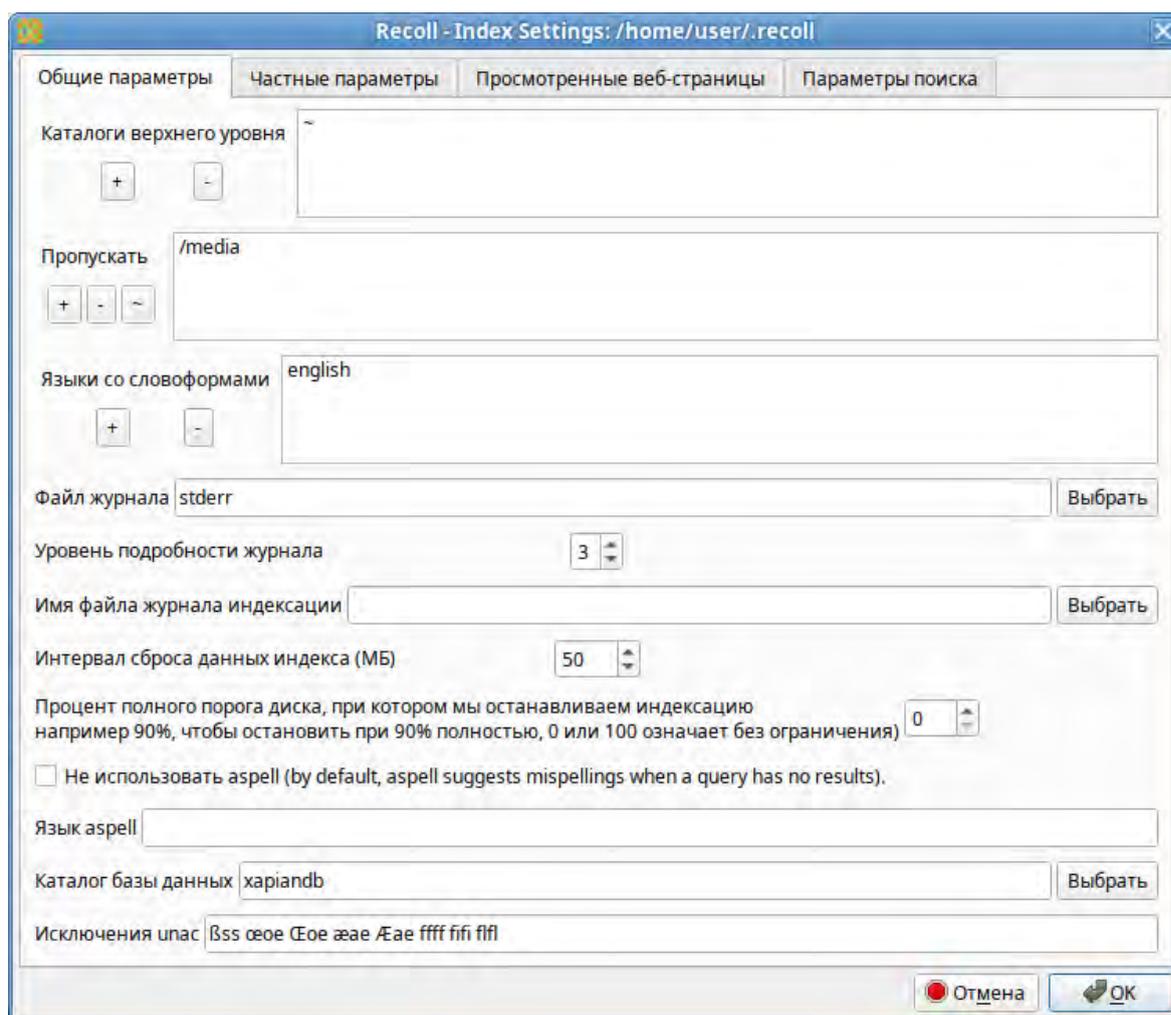


Рис. 65

На вкладке «Частные параметры» (Рис. 66) 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 каталоги» 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

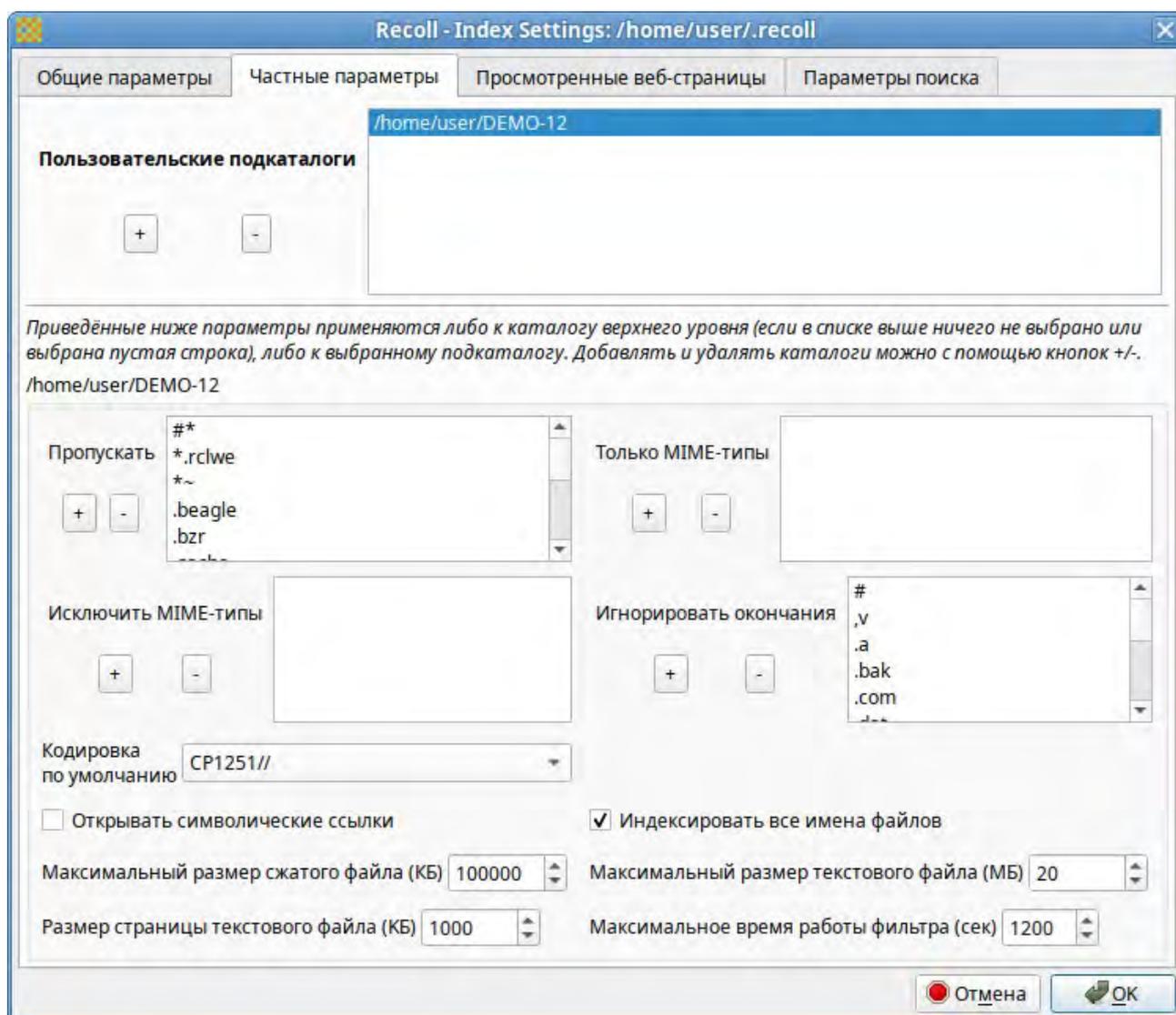


Рис. 66

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 «Настройка» → «Расписание индексирования» (Рис. 67).

Настройка расписания индексирования

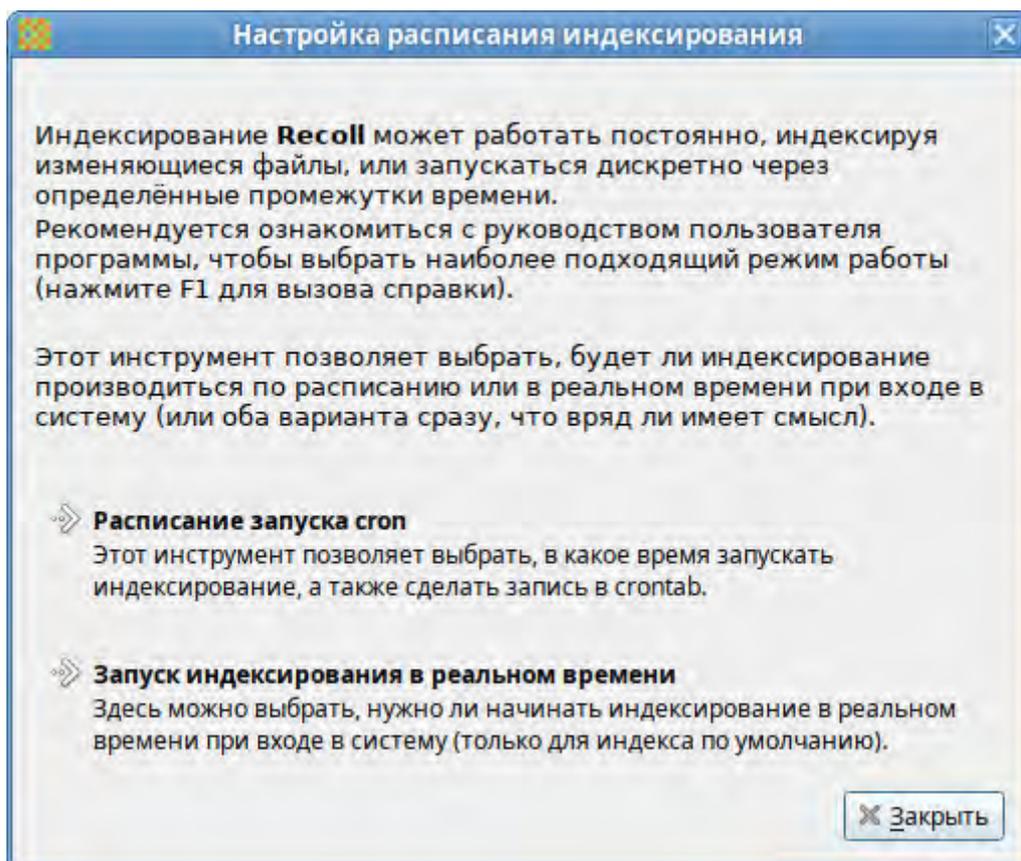


Рис. 67

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. 68);
- расширенный поиск – панель, доступ к которой осуществляется через меню («Инструменты» → «Сложный поиск») или значок панели инструментов. Расширенный поиск имеет несколько полей ввода (Рис. 69), которые можно использовать для создания логического условия, с дополнительной фильтрацией по типу файла, местоположению в файловой системе, дате изменения и размеру.

Простой поиск

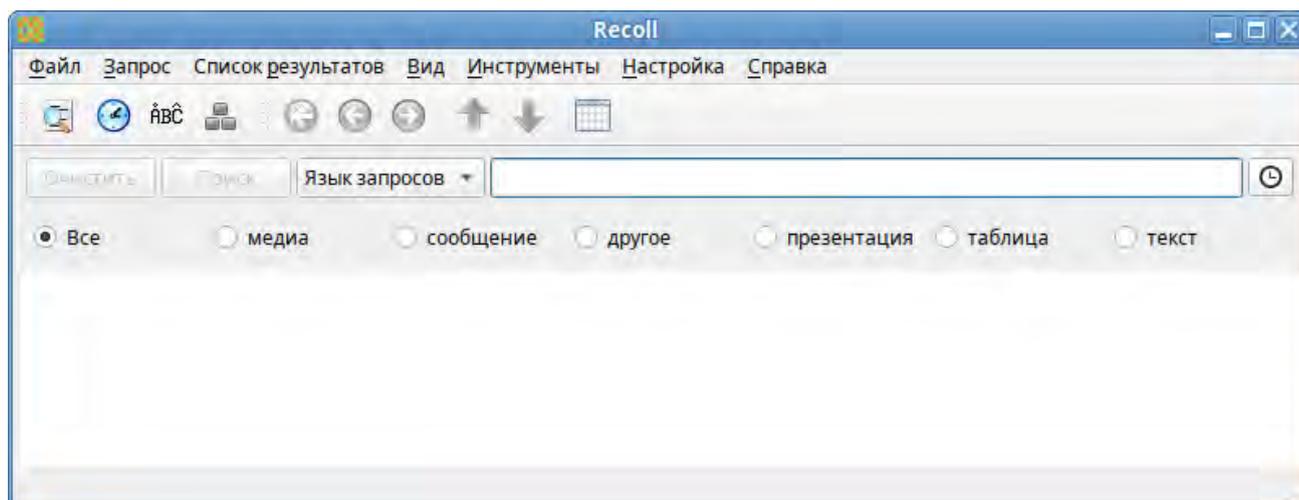


Рис. 68

Сложный поиск

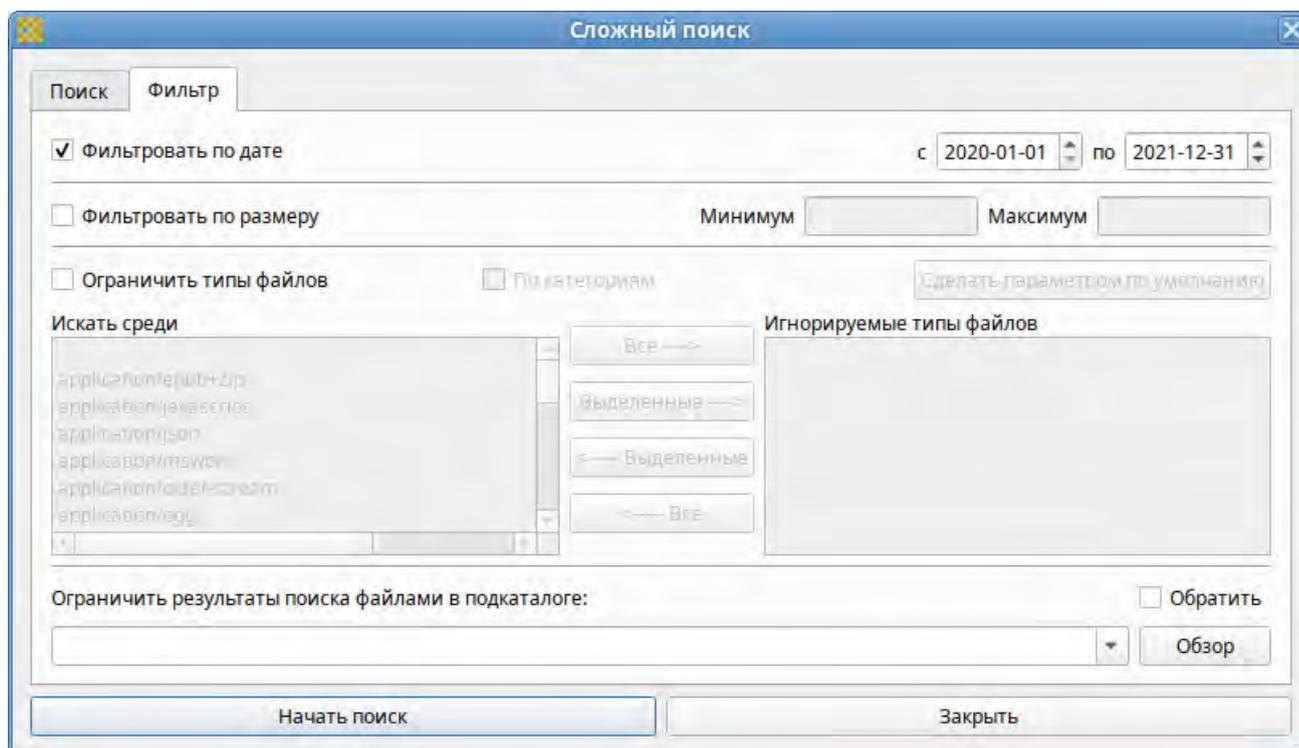


Рис. 69

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. 70).

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.

Поиск файлов

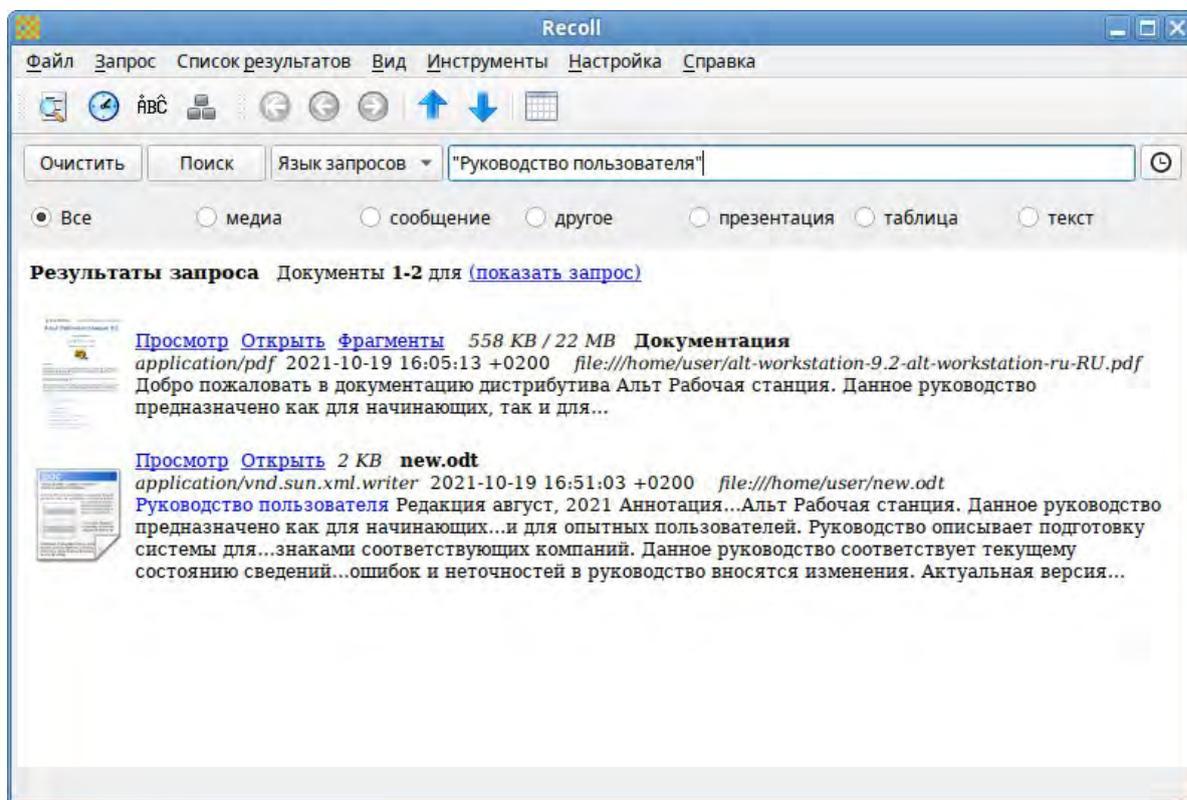


Рис. 70

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. 70).

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. 71).

Результаты поиска можно представить в виде таблицы. Щелчок по заголовку столбца позволит выполнить сортировку по значениям в столбце (Рис. 72).

Контекстное меню результата запроса

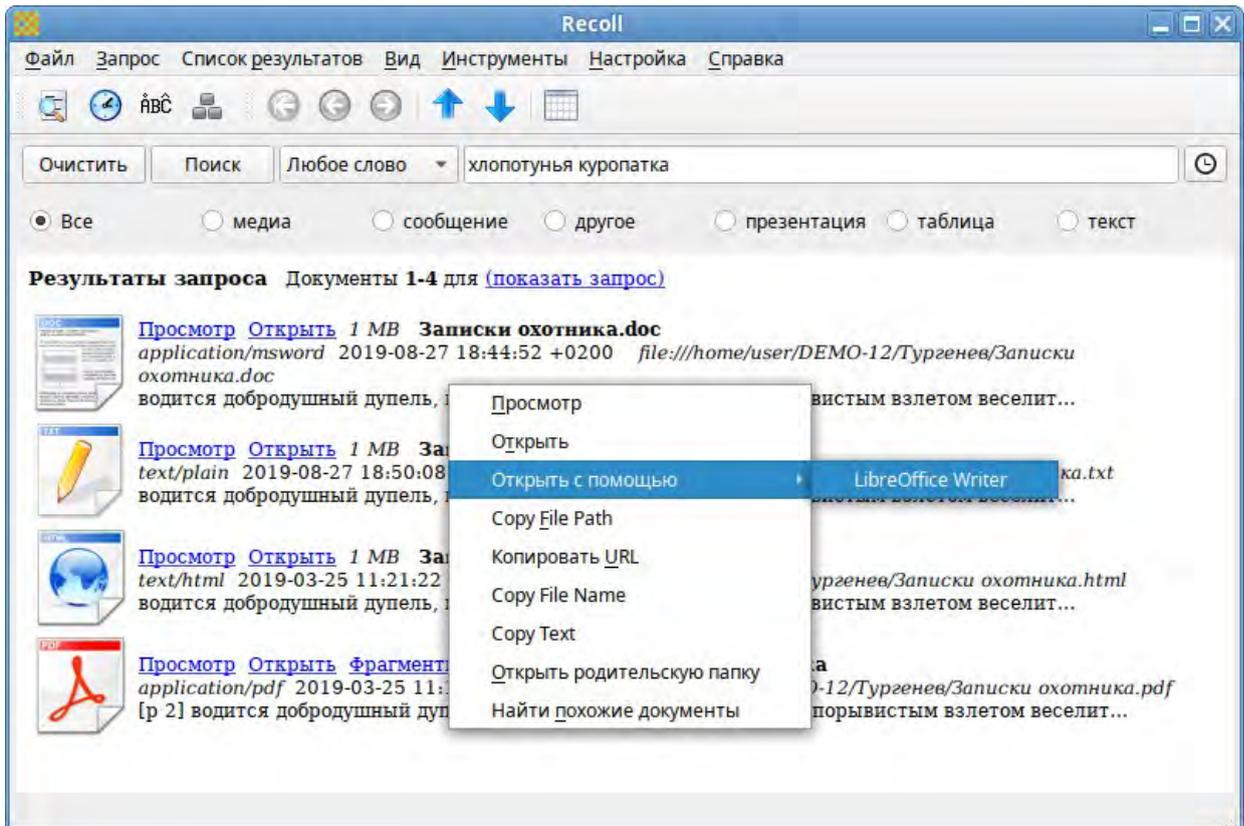


Рис. 71

Результаты поиска в виде таблицы

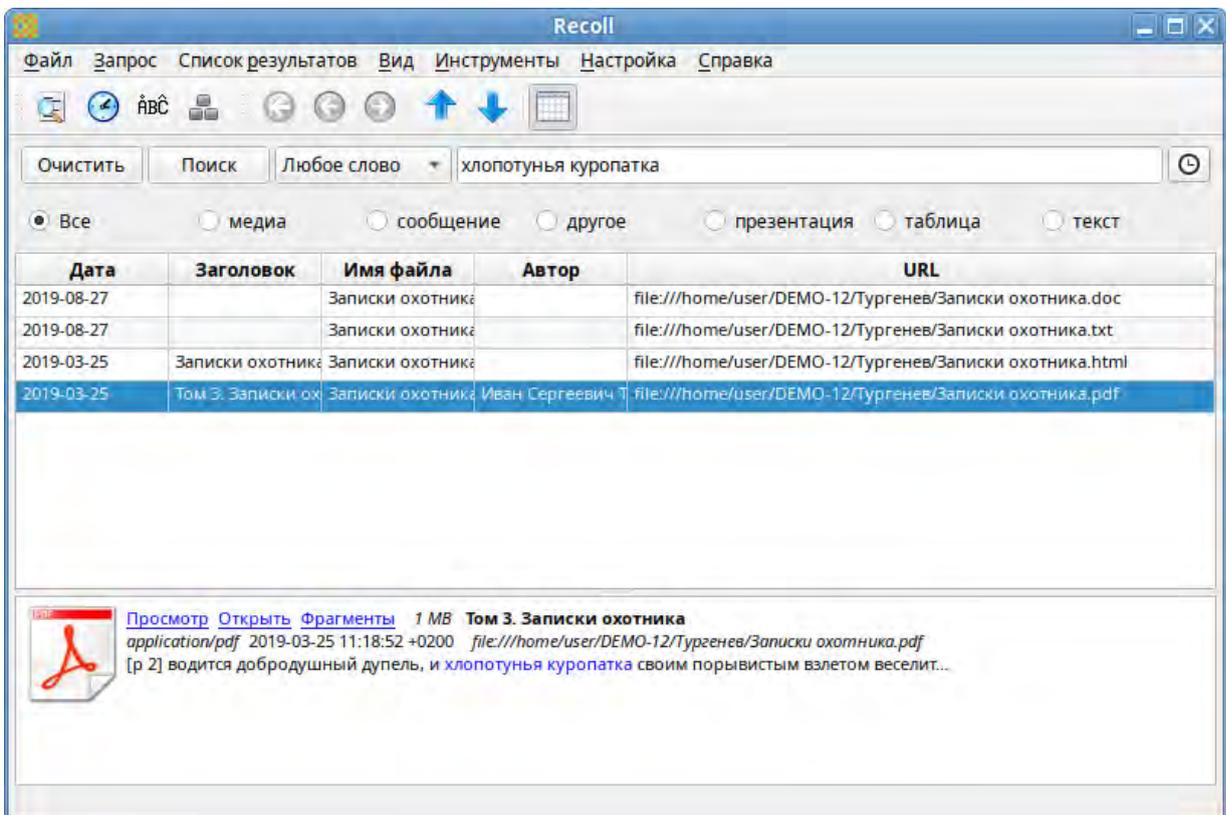


Рис. 72

По умолчанию Resoll позволяет рабочему окружению выбирать, какое приложение следует использовать для открытия документа данного типа. Настроить это действие можно с помощью меню «Настройка» → «Настройка интерфейса» → «Интерфейс пользователя» (Рис. 73).

Пользовательская настройка

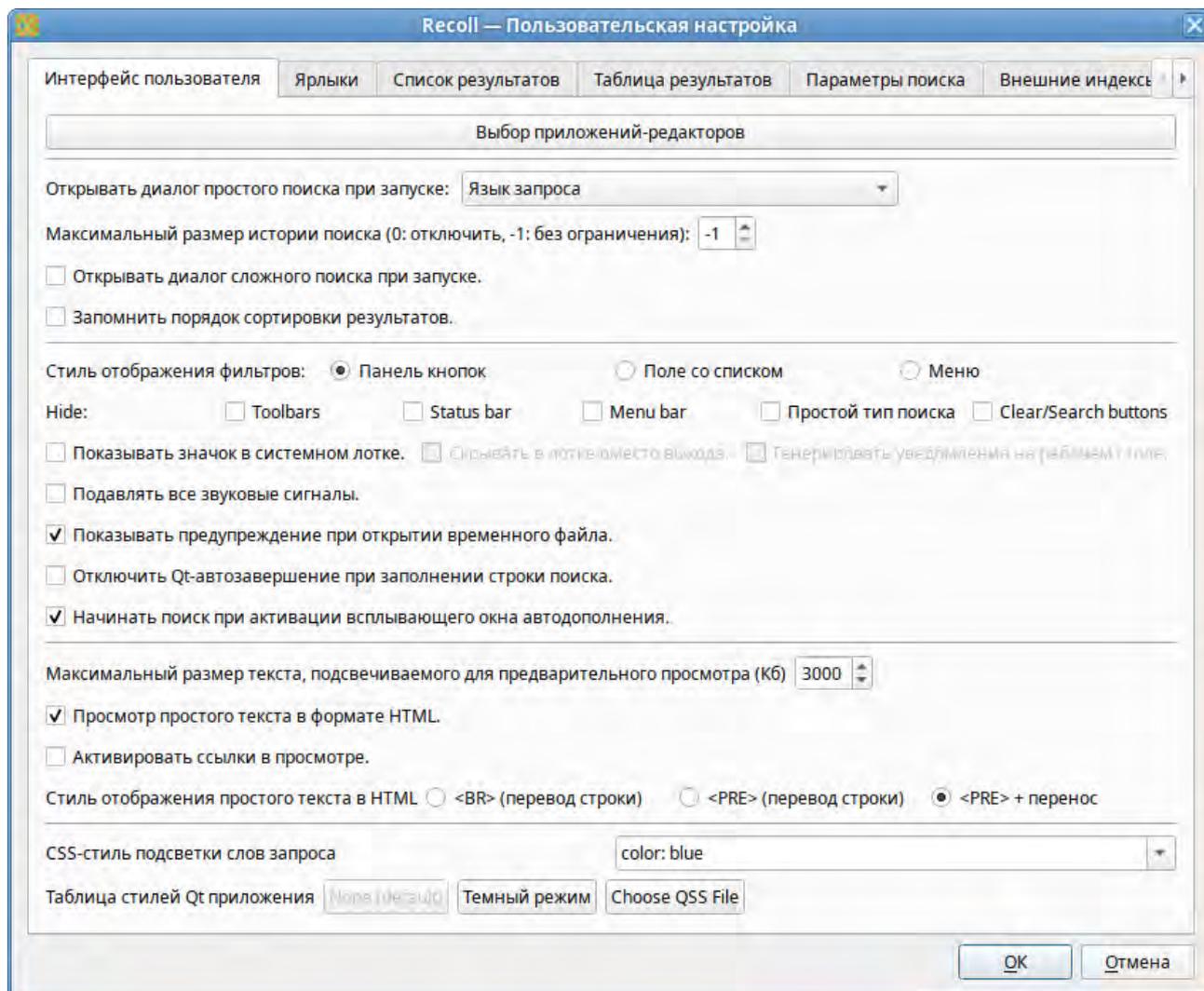
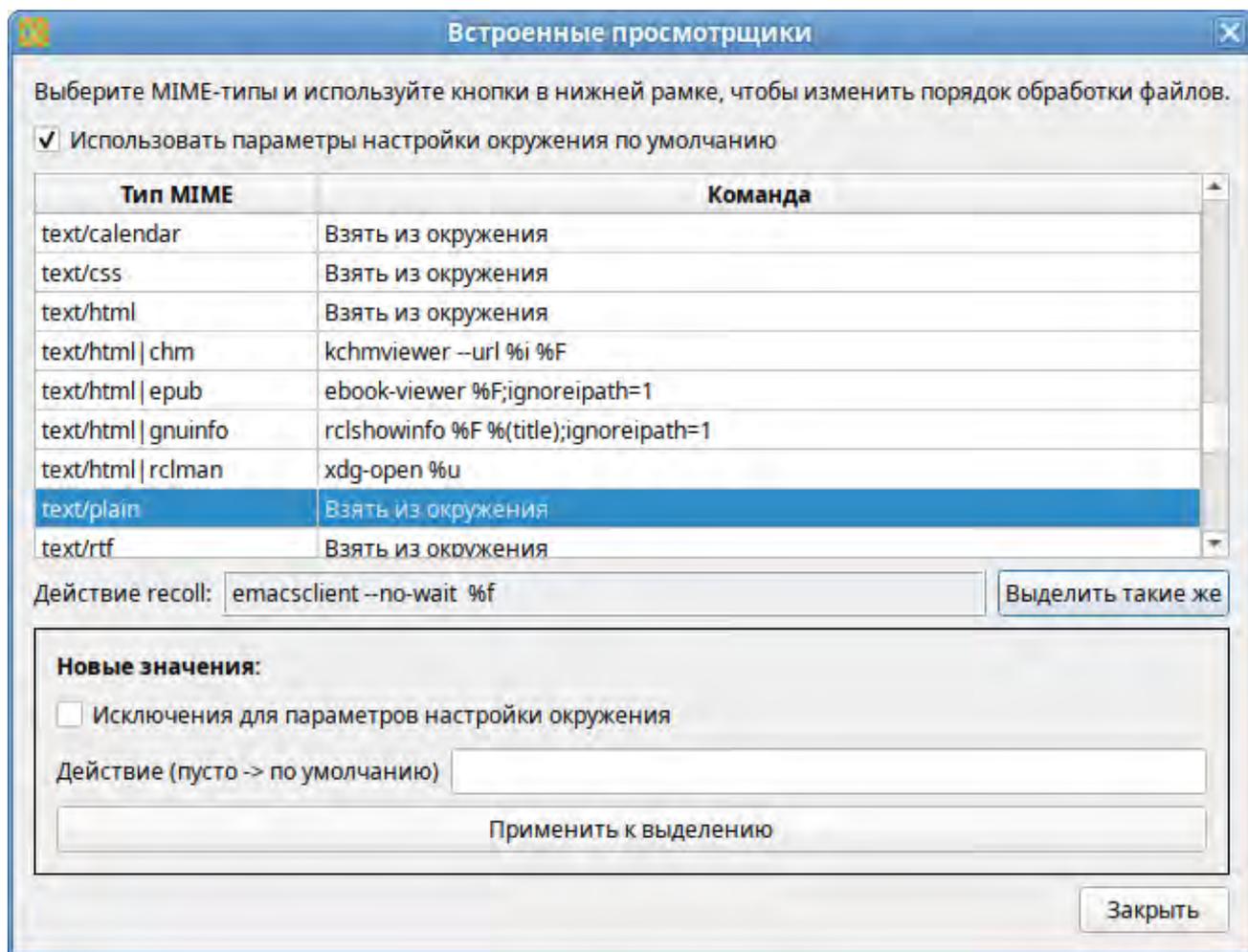


Рис. 73

При нажатии кнопки «Выбор приложений-редакторов» откроется диалоговое окно, где можно выбрать приложение, которое будет использоваться для открытия каждого MIME-типа (Рис. 74).

Пользовательская настройка*Рис. 74*

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:

- настройка даты и времени;
- управление системными службами;
- просмотр системных журналов;
- управление выключением удаленного компьютера (доступно только в веб-интерфейсе);
- настройка ограничений выделяемых ресурсов памяти пользователям (квоты);
- настройка ограничений на использование внешних носителей (доступно только в веб-интерфейсе);
- управлению политиками control (системные ограничения);
- конфигурирование сетевых интерфейсов;
- настройка межсетевого экрана;
- изменения пароля администратора системы (root);
- создание, удаление и редактирование учётных записей пользователей.

4.1.2 Запуск ЦУС в графической среде

ЦУС можно запустить следующими способами:

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

При запуске необходимо ввести пароль администратора системы (root) (Рис. 75).

Запуск Центра управления системой

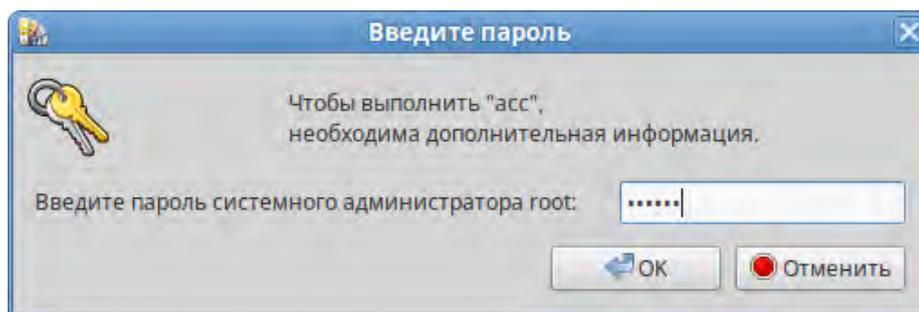


Рис. 75

После успешного входа можно приступить к настройке системы (Рис. 76).

Центр управления системой

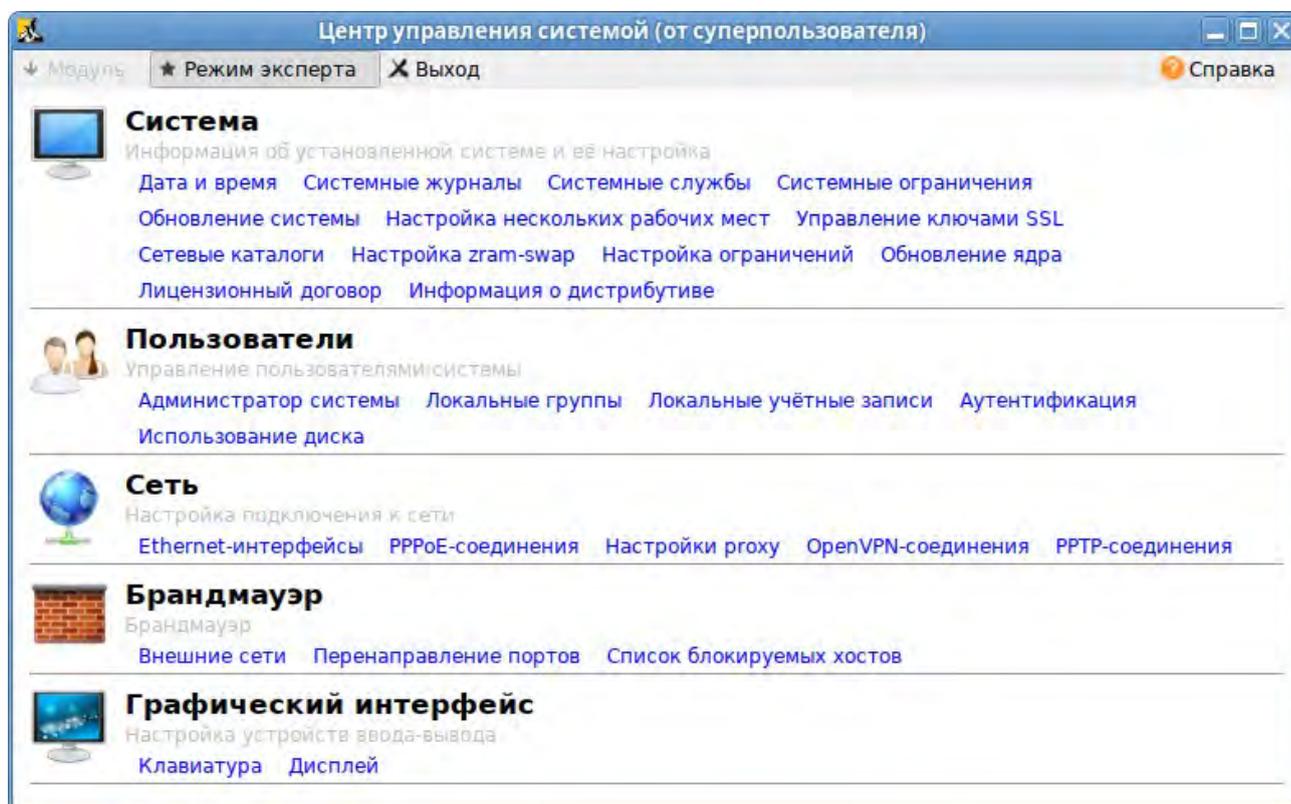


Рис. 76

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 «Иридиум» 192.168.0.150, то интерфейс управления будет доступен по адресу: <https://192.168.0.150:8080/>

При запуске ЦУС необходимо ввести в соответствующие поля имя пользователя (root) и пароль пользователя (Рис. 77).

Запрос пароля администратора для запуска веб-интерфейса ЦУС

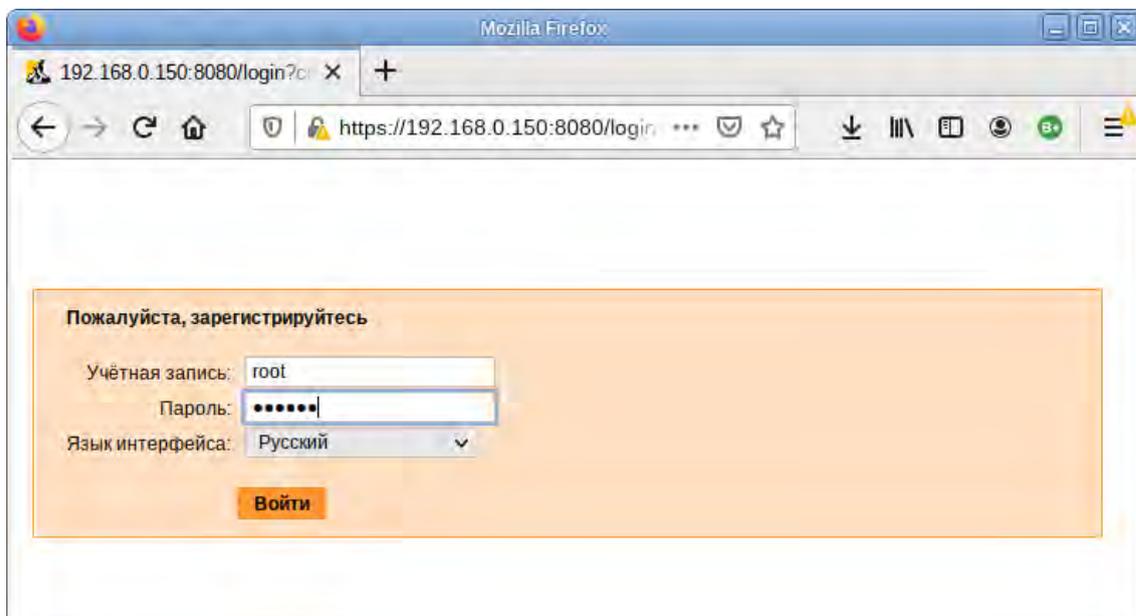


Рис. 77

После этого будут доступны все возможности ЦУС на той машине, к которой было произведено подключение через веб-интерфейс (Рис. 78).

ЦУС содержит справочную информацию по включённым в него модулям. Об использовании самого интерфейса системы управления можно прочитать (Рис. 79), нажав на кнопку «Справка» на начальной странице ЦУС.

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».

Окно веб-интерфейса ЦУС

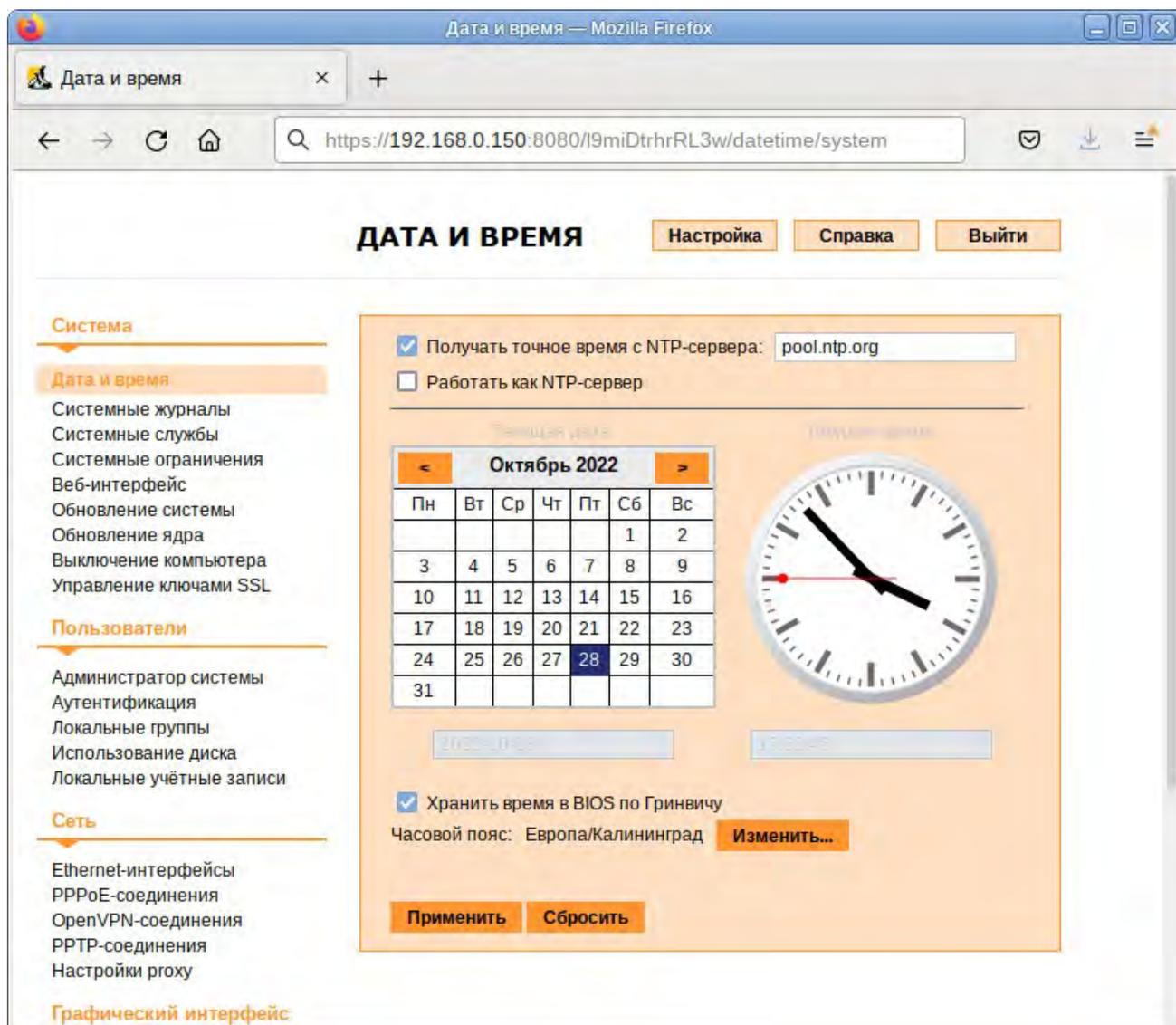


Рис. 78

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 МАТЕ» → «Приложения» → «Параметры» → «Запускаемые приложения».

4.2.1 Вкладка автоматического запуска программ

Список автоматически запускаемых программ представлен на вкладке «Автоматически запускаемые программы» (Рис. 80). Этот список содержит краткое описание каждой программы и отметку, указывающую запускать программу или нет.

Веб-интерфейс ЦУС. Справка

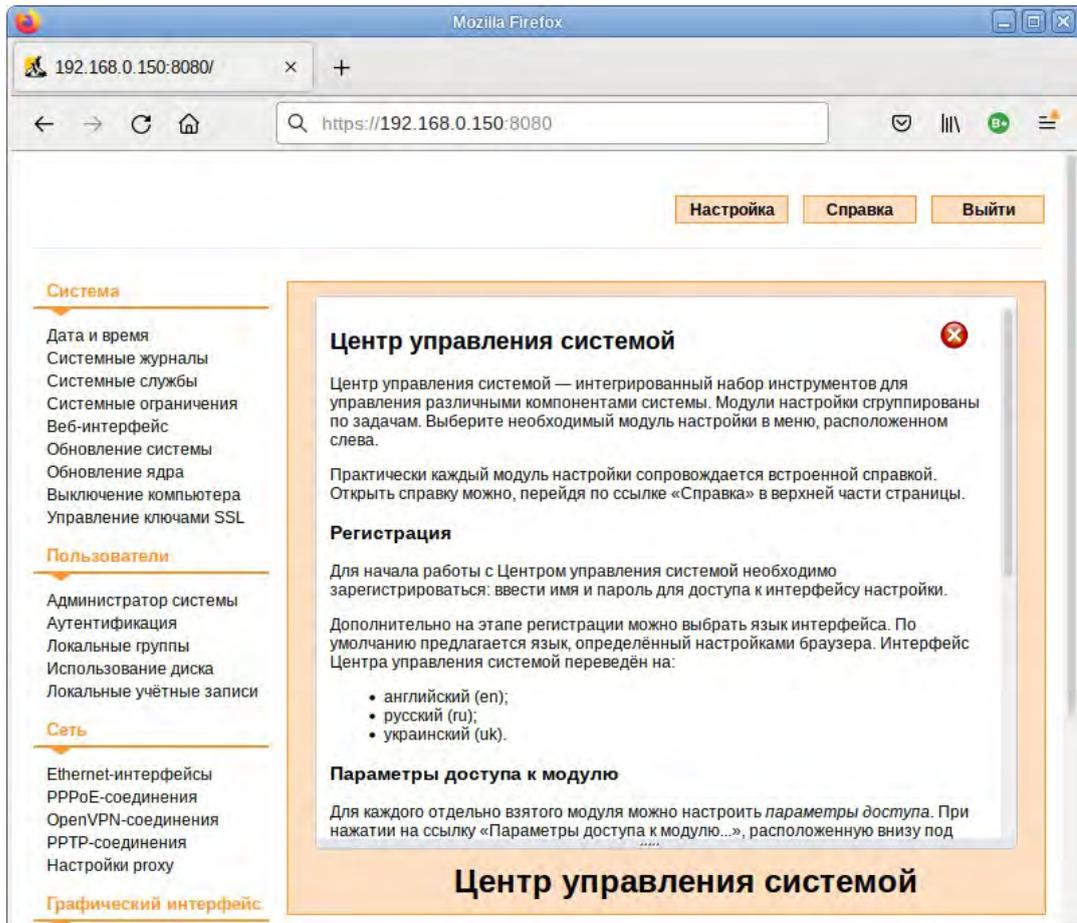


Рис. 79

Автоматически запускаемые программы

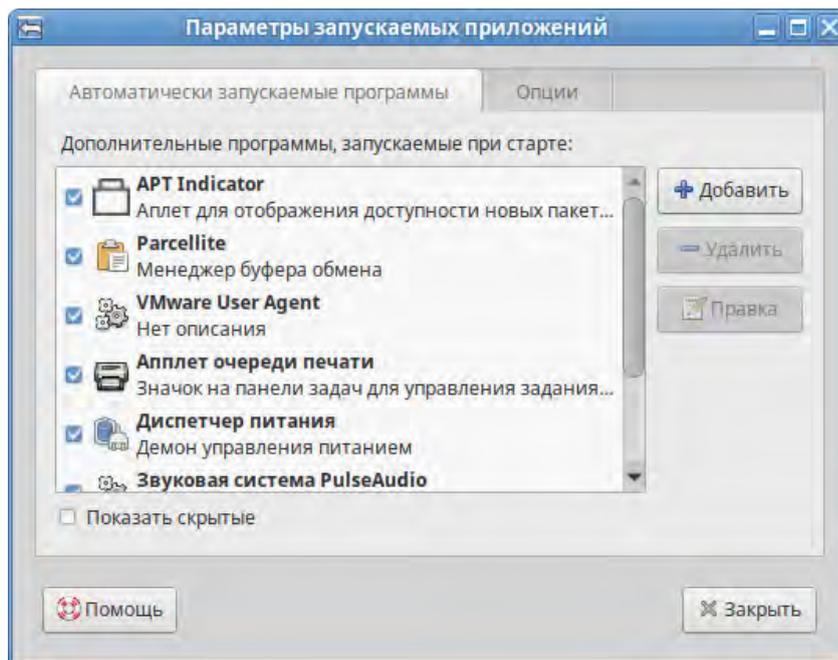


Рис. 80

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. 81);
- нажать кнопку «Добавить».

Добавление автоматически запускаемой программы

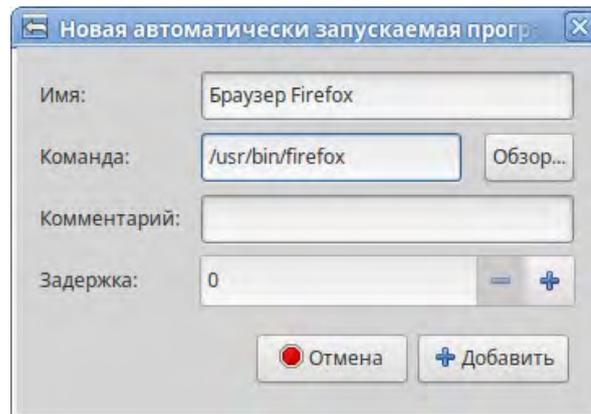


Рис. 81

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. 82).

Запоминать запущенные приложения при выходе из сеанса

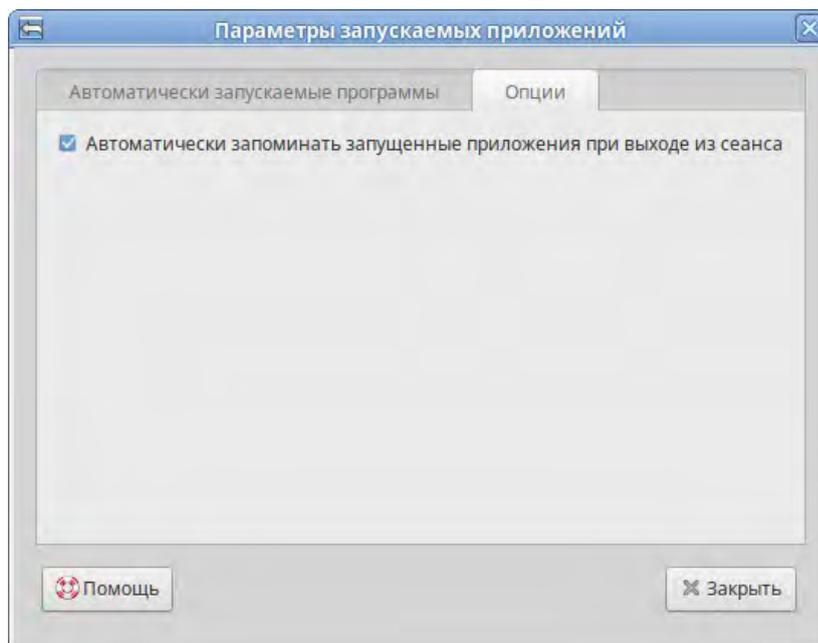


Рис. 82

4.3 Настройка сети

4.3.1 NetworkManager

Для управления настройками сети в ОС «Иридиум» 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. 83).

NetworkManager

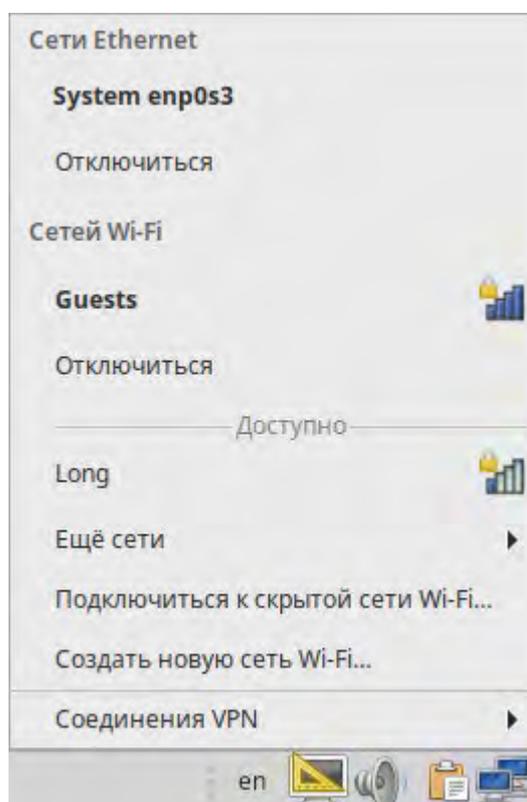


Рис. 83

П р и м е ч а н и е . 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. 84). Здесь можно посмотреть версию программы, получить сведения о соединении, изменить соединения (например, удалить Wi-Fi сеть, чтобы не подключаться к ней автоматически).

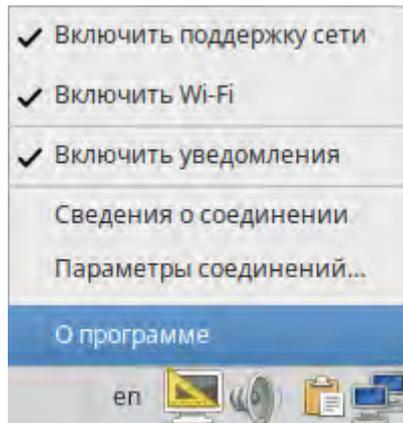
Контекстное меню NetworkManager

Рис. 84

Для того чтобы просмотреть информацию о сетевом соединении, следует в меню NetworkManager, вызываемом нажатием правой кнопкой мыши, выбрать пункт «Сведения о соединении». Сведения об активных соединениях будут отображены в диалоговом окне «Сведения о соединении», каждое в отдельной вкладке (Рис. 85).

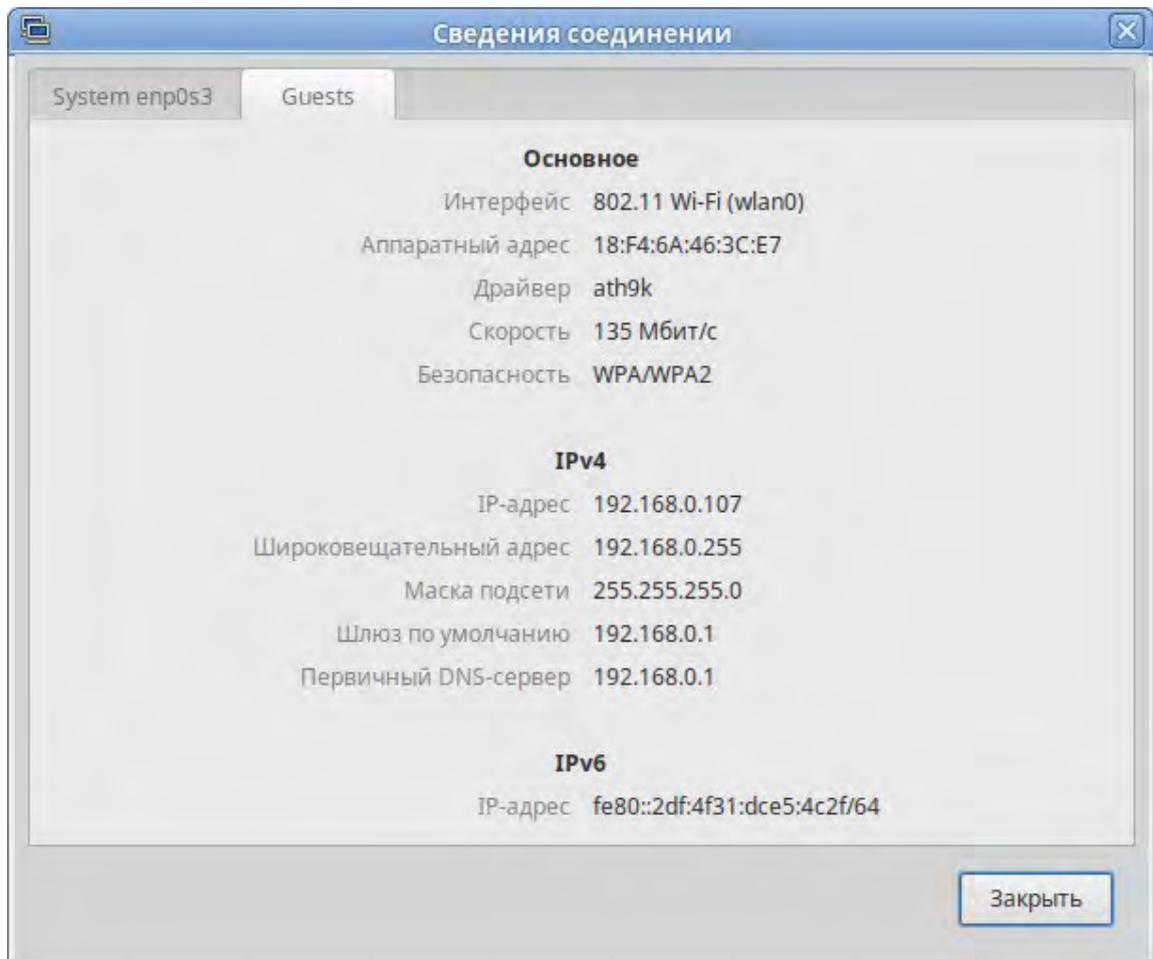
Информация о сетевом соединении

Рис. 85

Для настройки соединений, следует в меню NetworkManager, вызываемом нажатием правой кнопкой мыши, выбрать пункт «Параметры соединений...». В открывшемся окне будет показан сгруппированный по типам список соединений. Необходимо выбрать нужную сеть и нажать кнопку «Изменить» (Рис. 86).

Изменение настроек сетевых соединений

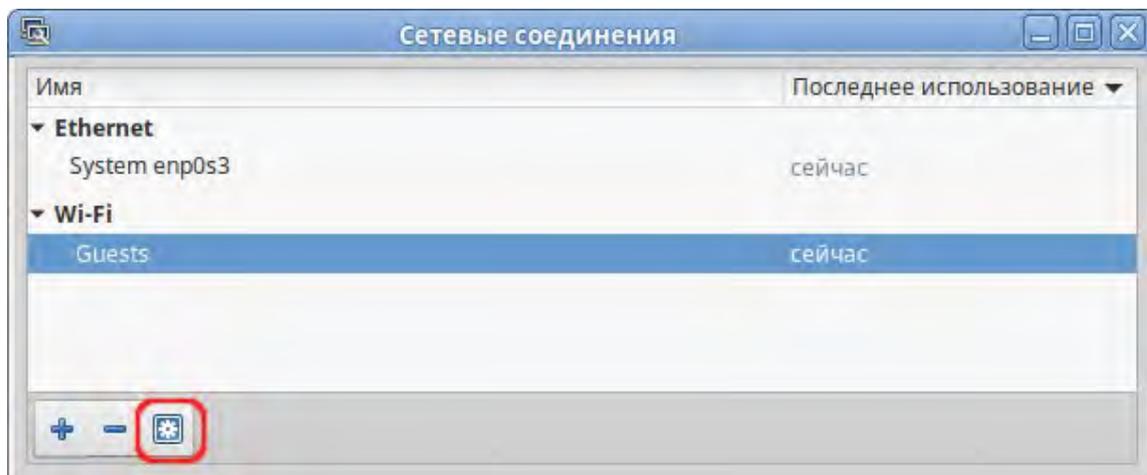


Рис. 86

В открывшемся окне можно изменить настройки сетевого интерфейса (Рис. 87).

Окно изменения настроек сетевого интерфейса

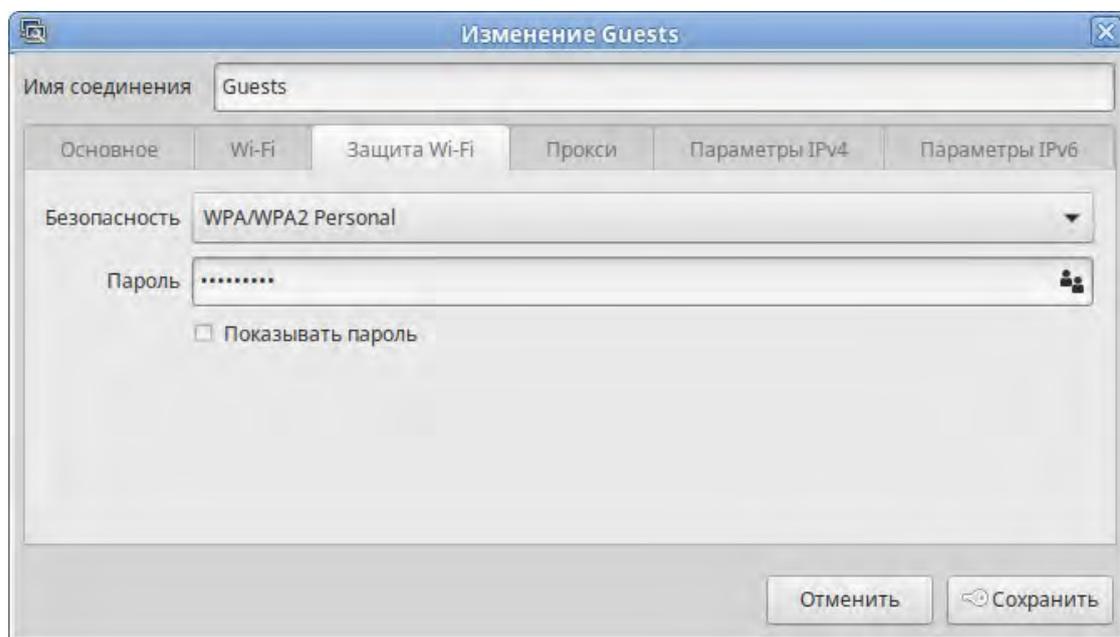


Рис. 87

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

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. 88), следует нажать кнопку «Запустить службу». Потребуется ввести пароль пользователя, находящегося в группе wheel.

Также можно 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»

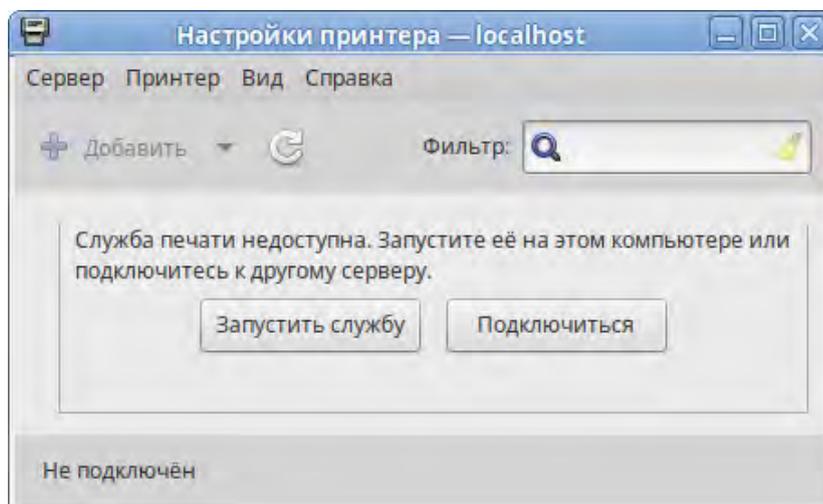


Рис. 88

Для добавления принтера необходимо нажать кнопку «Добавить» (Рис. 89).

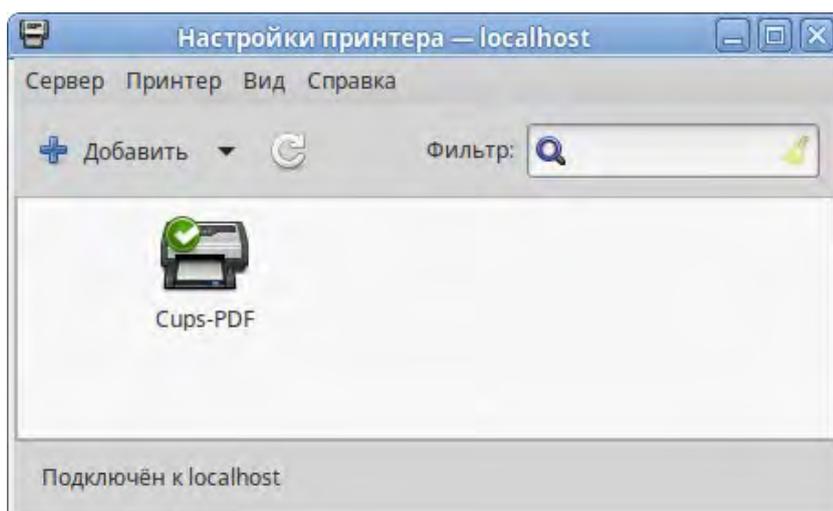
Настройка печати

Рис. 89

В открывшемся окне необходимо определить устройство из предложенных в списке «Устройства» (Рис. 90). Также необходимо удостовериться, что тип соединения указан корректно. Переход к следующему шагу осуществляется нажатием кнопки «Вперёд».

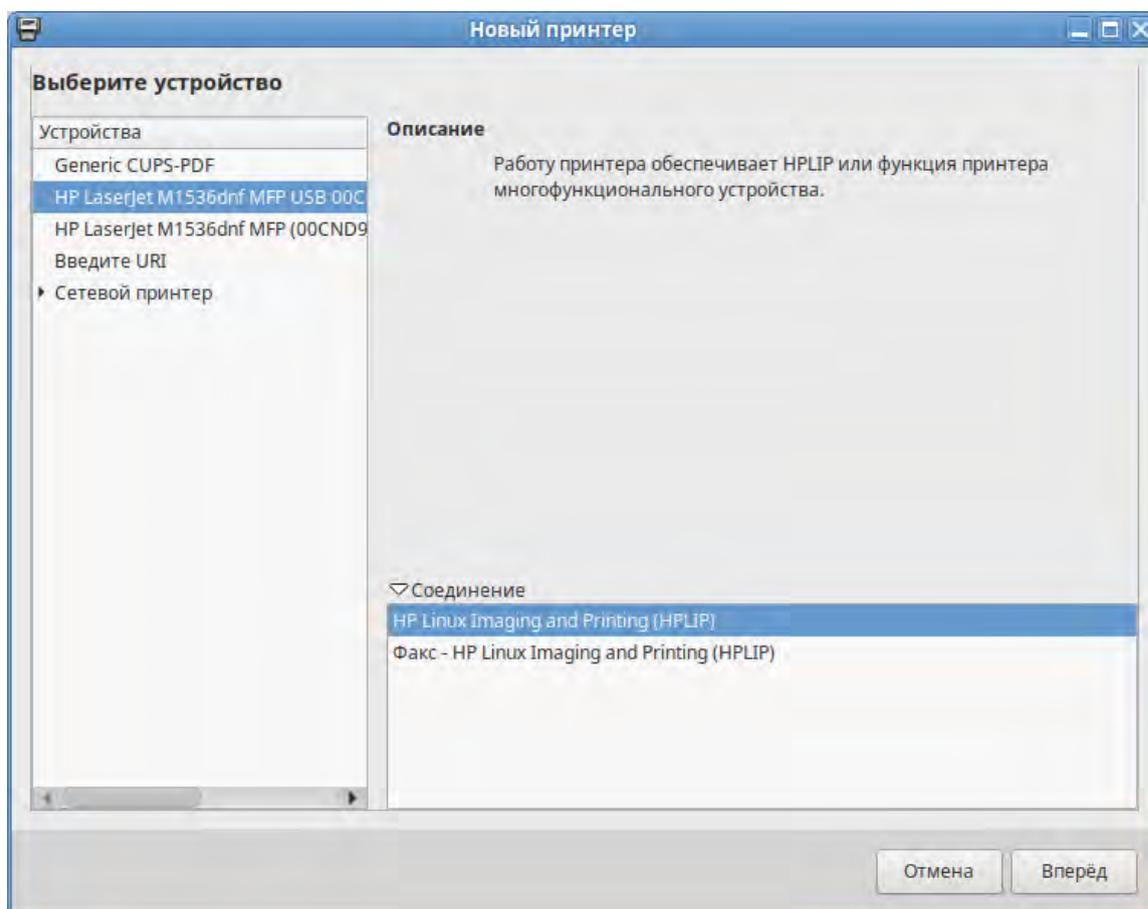
Настройка печати

Рис. 90

В окне «Опишите принтер», в строке «Имя принтера» можно изменить имя принтера и добавить описание (Рис. 91).

После нажатия кнопки «Применить» установка принтера завершена, принтер станет доступным для печати (Рис. 92).

Настройка печати

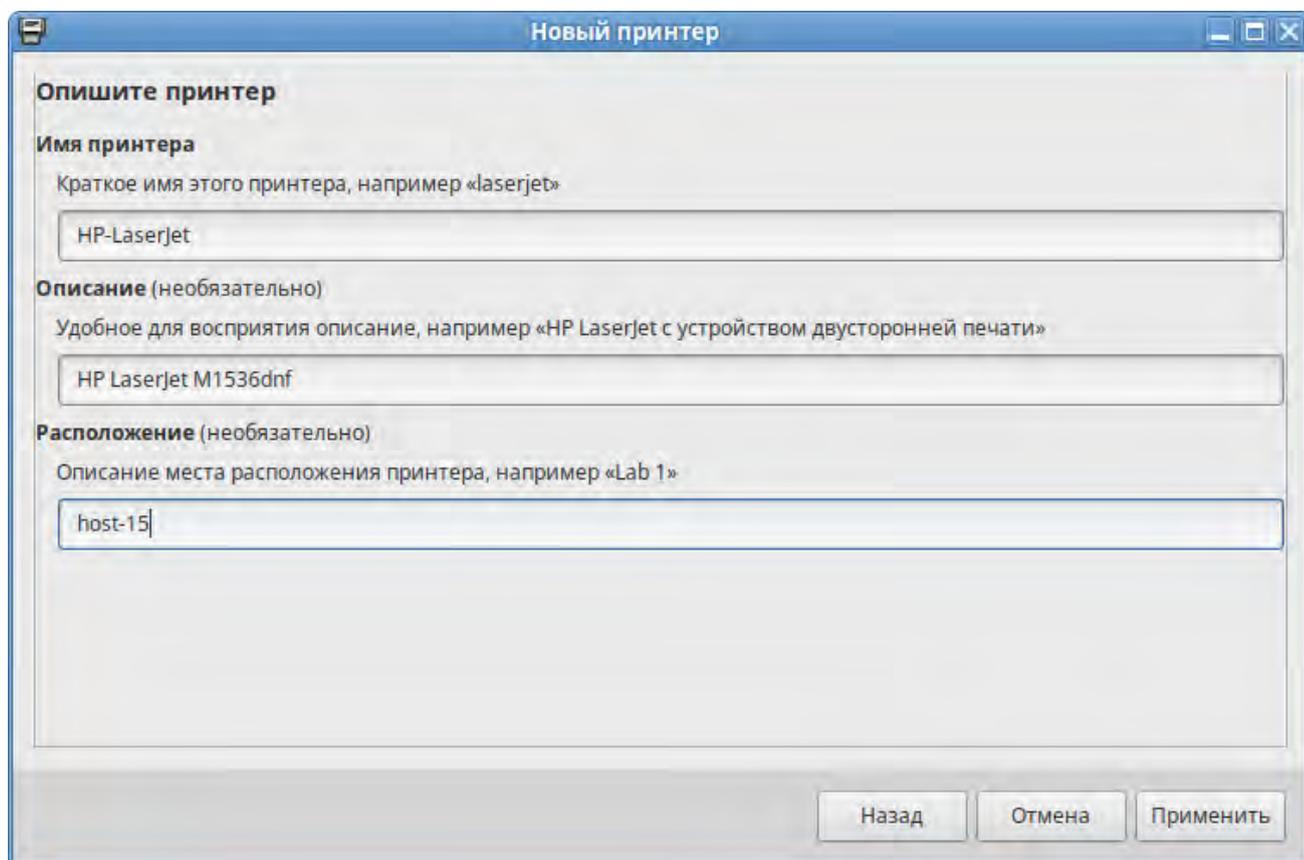


Рис. 91

Настройка печати

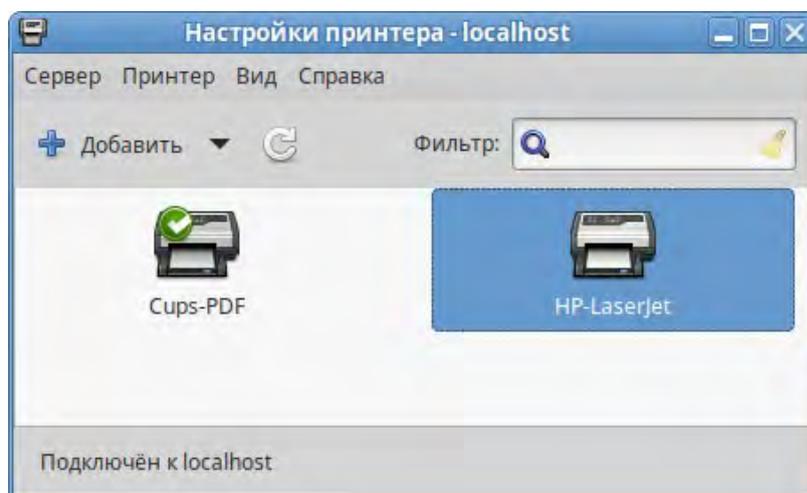


Рис. 92

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 «Иридиум» 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 `epsonscan2`, `imagescan-sane`, `iscan-free`, `iscan-data` и `firmware-iscan` из репозитория:

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

Также для работы со сканерами Epson 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.

Примечание. Любая ошибка при редактировании настроек загрузчика может привести к неспособности системы загрузиться.

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

Для запуска модуля потребуется ввести пароль администратора (Рис. 93).

Запуск Grub Customizer

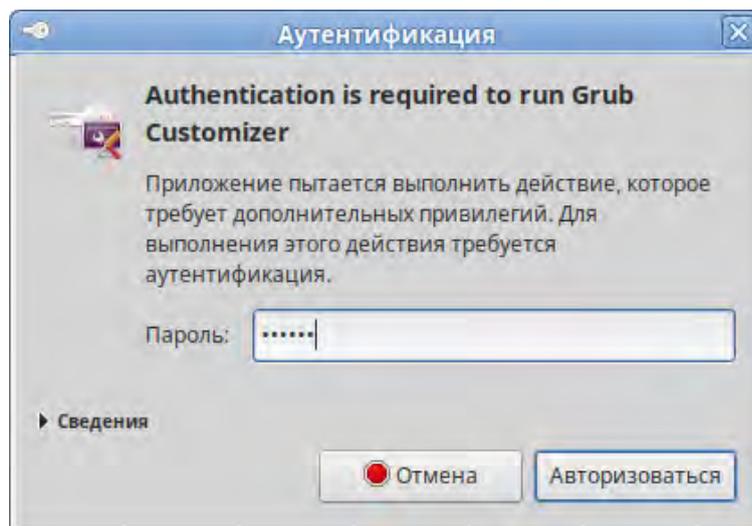


Рис. 93

На вкладке «Просмотреть настройки» показан список возможных вариантов загрузки операционных систем (Рис. 94).

Вкладка «Просмотреть настройки»

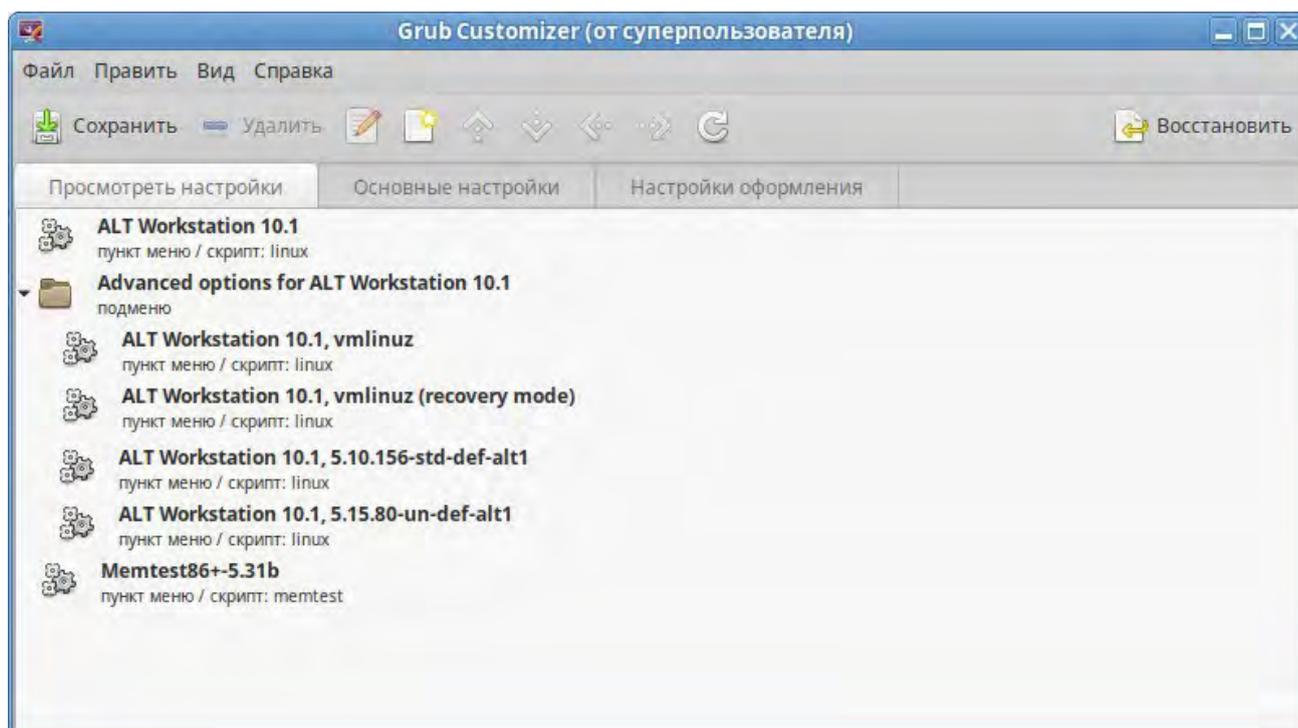


Рис. 94

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

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. 95).

Вкладка «Основные настройки»

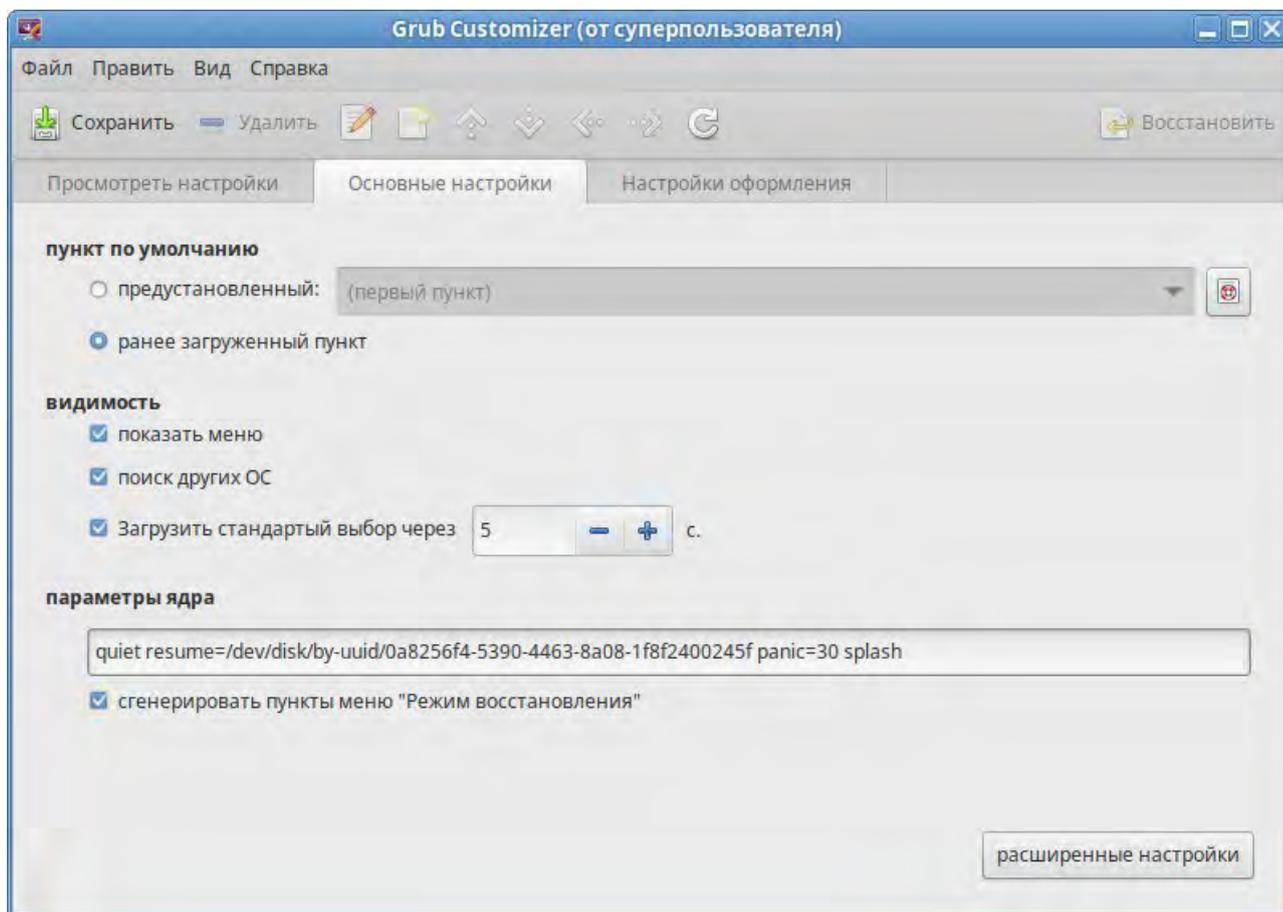


Рис. 95

На вкладке «Настройки оформления» можно менять способы отображения GRUB и внешний вид меню (Рис. 96).

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

4.7 Изменение пароля пользователя

Пароли пользователей в ОС «Иридиум» 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».

Вкладка «Настройки оформления»

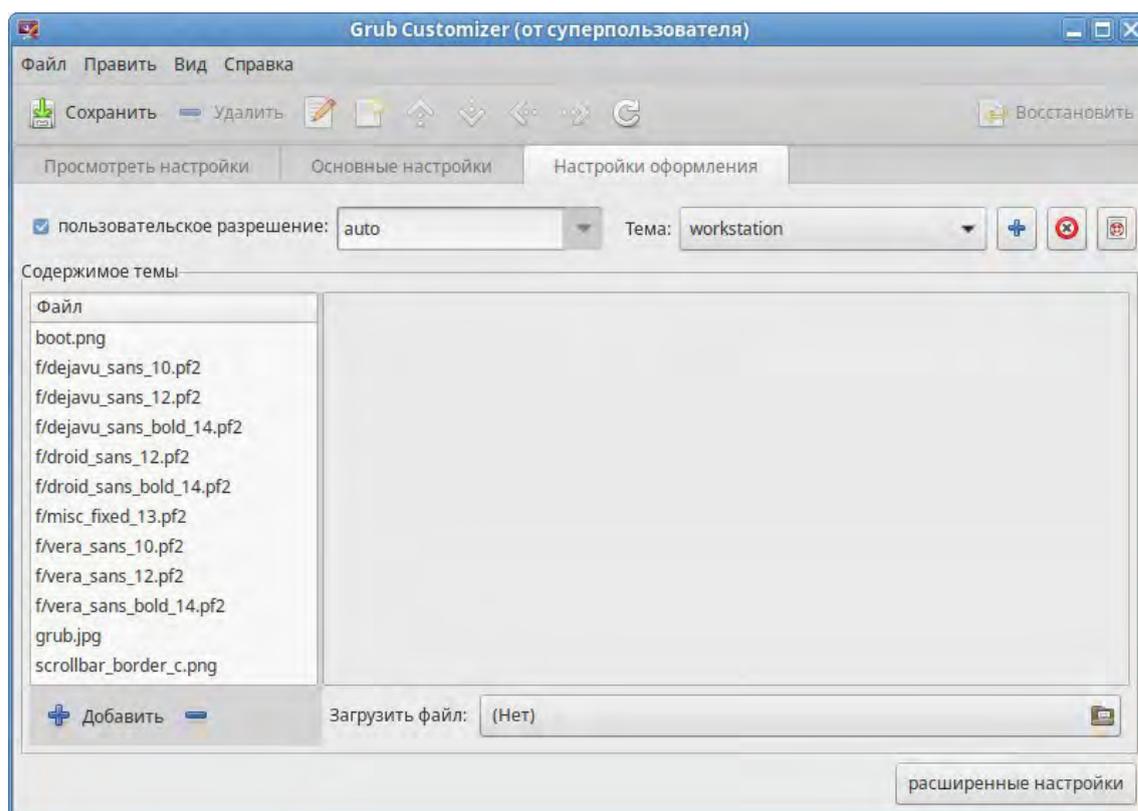


Рис. 96

Откроется окно, в котором необходимо ввести свой текущий (старый) пароль (Рис. 97).

Запрос старого пароля пользователя

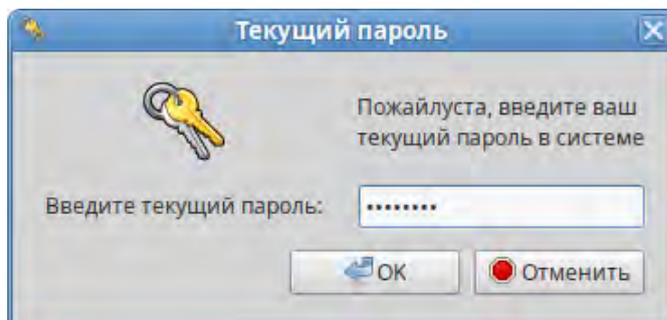


Рис. 97

Затем следует ввести новый пароль (Рис. 98) и повторить его (Рис. 99).

Новый пароль пользователя

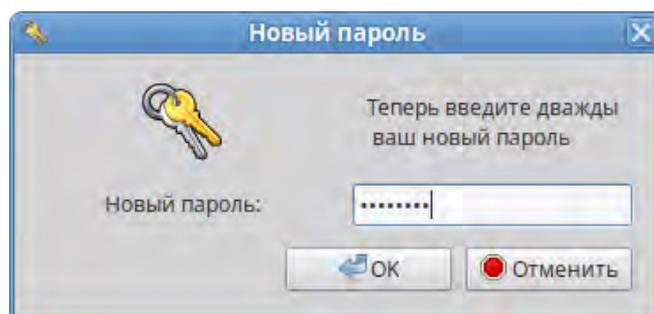


Рис. 98

Повторный ввод нового пароля пользователя

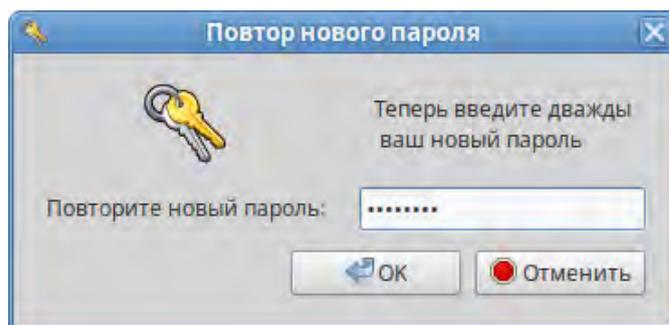


Рис. 99

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

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

- в 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. 100);
- 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 содержанием:

```
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
```

Настройка на использование DNS-сервера домена

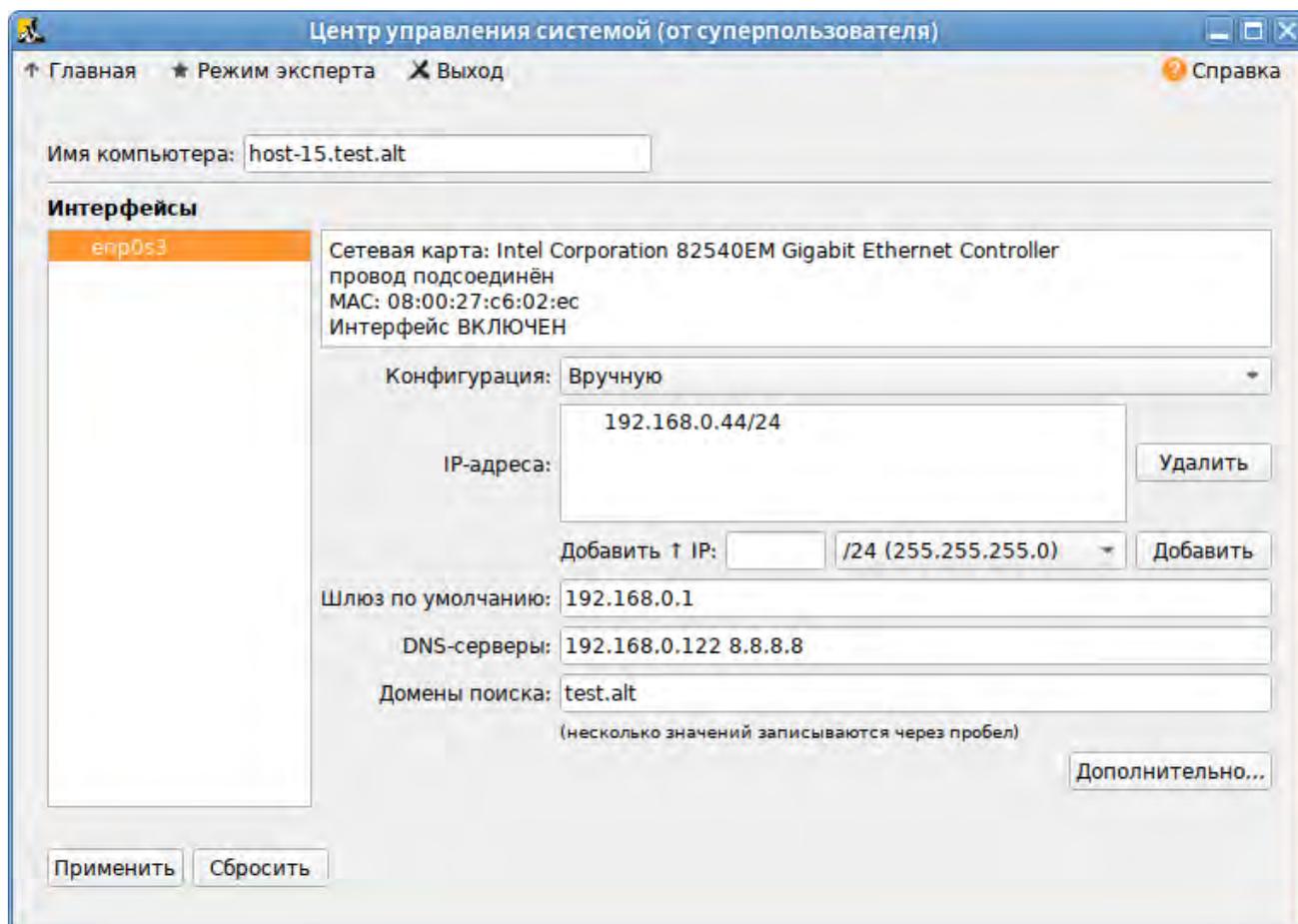


Рис. 100

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.

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 МАТЕ» → «Приложения» → «Администрирование» → «Центр управления системой»). В ЦУС следует перейти в раздел «Пользователи» → «Аутентификация». Здесь необходимо выбрать пункт «Домен Active Directory» (Рис. 101) и заполнить поля, после чего нажать кнопку «Применить».

Ввод в домен в «Центре управления системой»

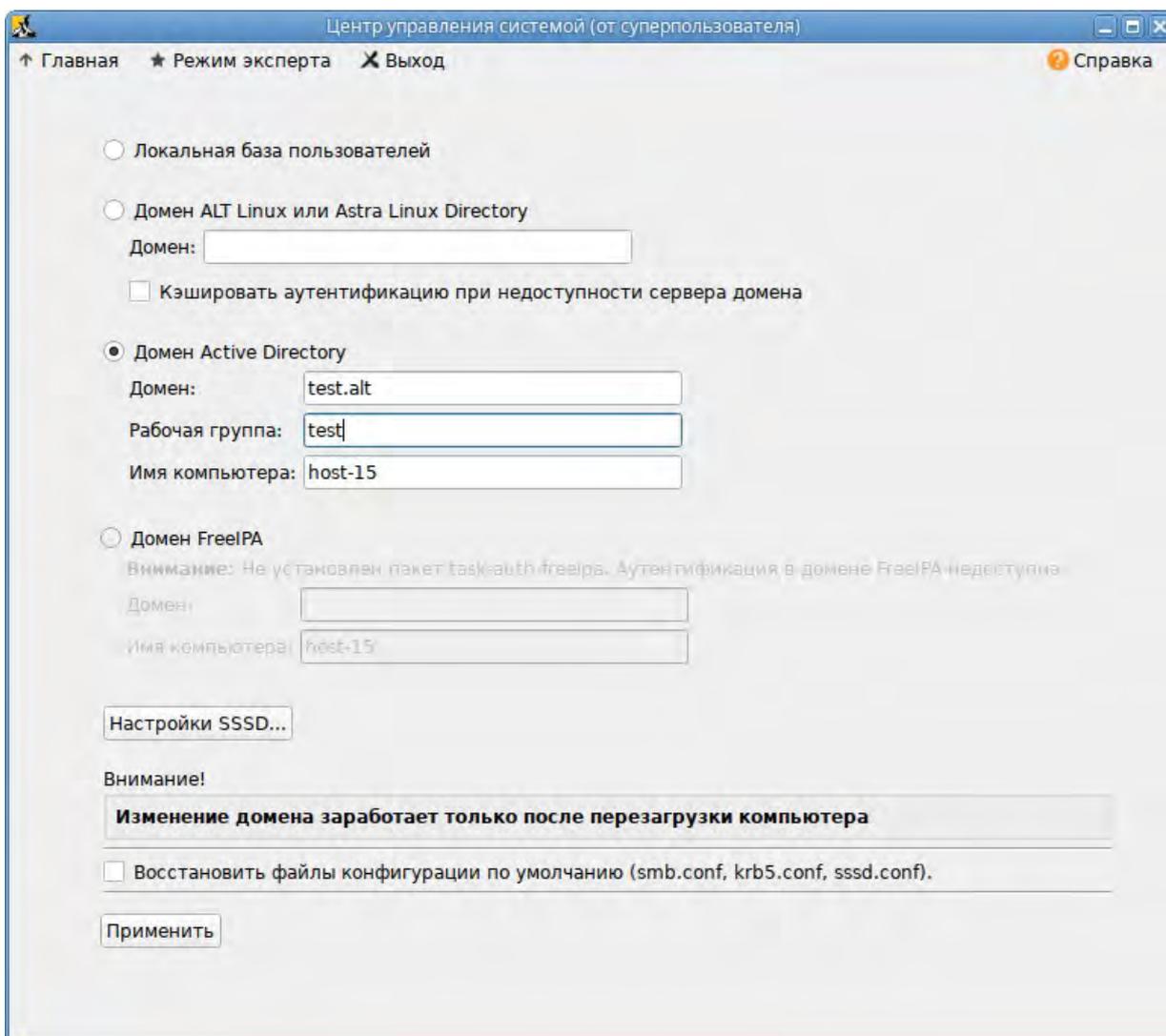


Рис. 101

В открывшемся окне (Рис. 102) необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку «ОК».

Параметры учетной записи с правами подключения к домену

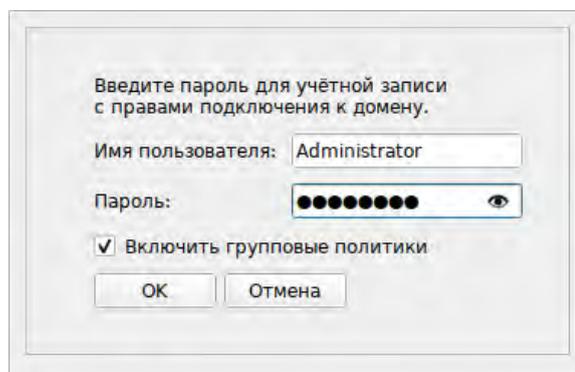


Рис. 102

При успешном подключении к домену, отобразится соответствующая информация (Рис. 103).

Успешное подключение к домену

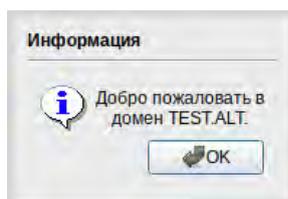


Рис. 103

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:*:54401104:54400513:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash

# net ads info
LDAP server: 192.168.0.122
LDAP server name: dc.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
```

```
LDAP port: 389
```

```
Server time: Вт, 19 июл 2022 15:54:05 ЕЕТ
```

```
KDC server: 192.168.0.122
```

```
Server time offset: -1270
```

```
Last machine account password change: Вт, 19 июл 2022 15:54:05 ЕЕТ
```

```
# 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. 104), в открывшемся окне ввести пароль, соответствующий этой учетной записи и нажать кнопку «Войти» (Рис. 105).

Вход пользователя

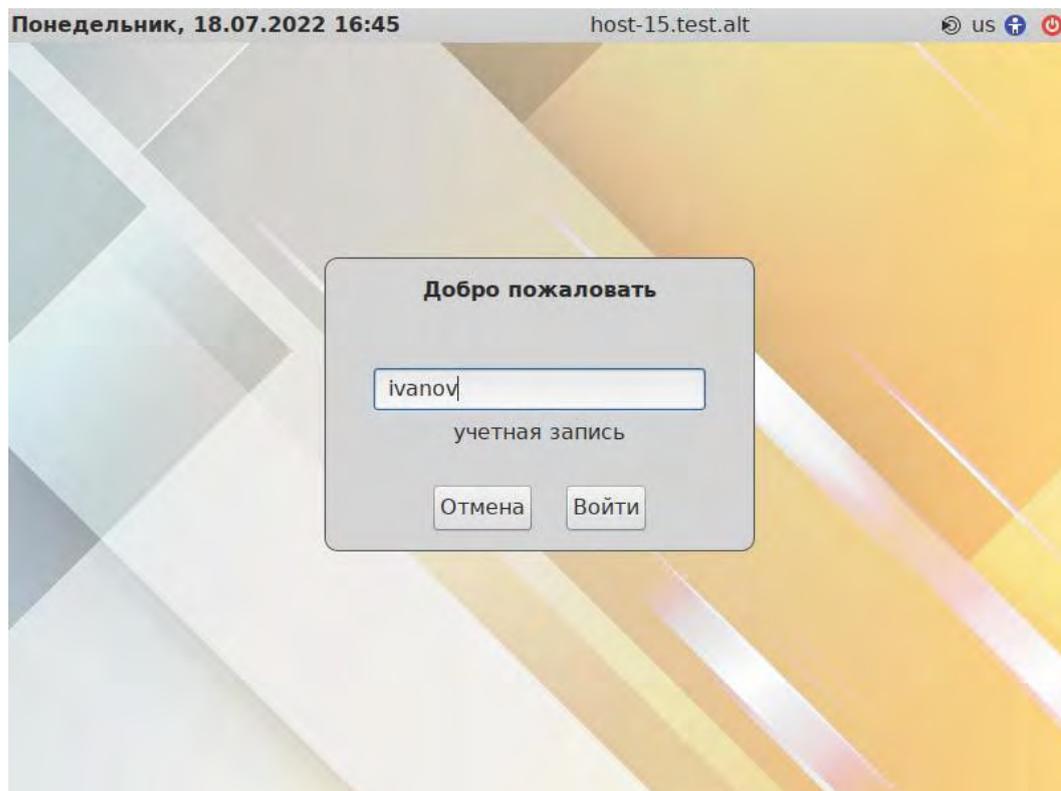


Рис. 104

Запрос пароля

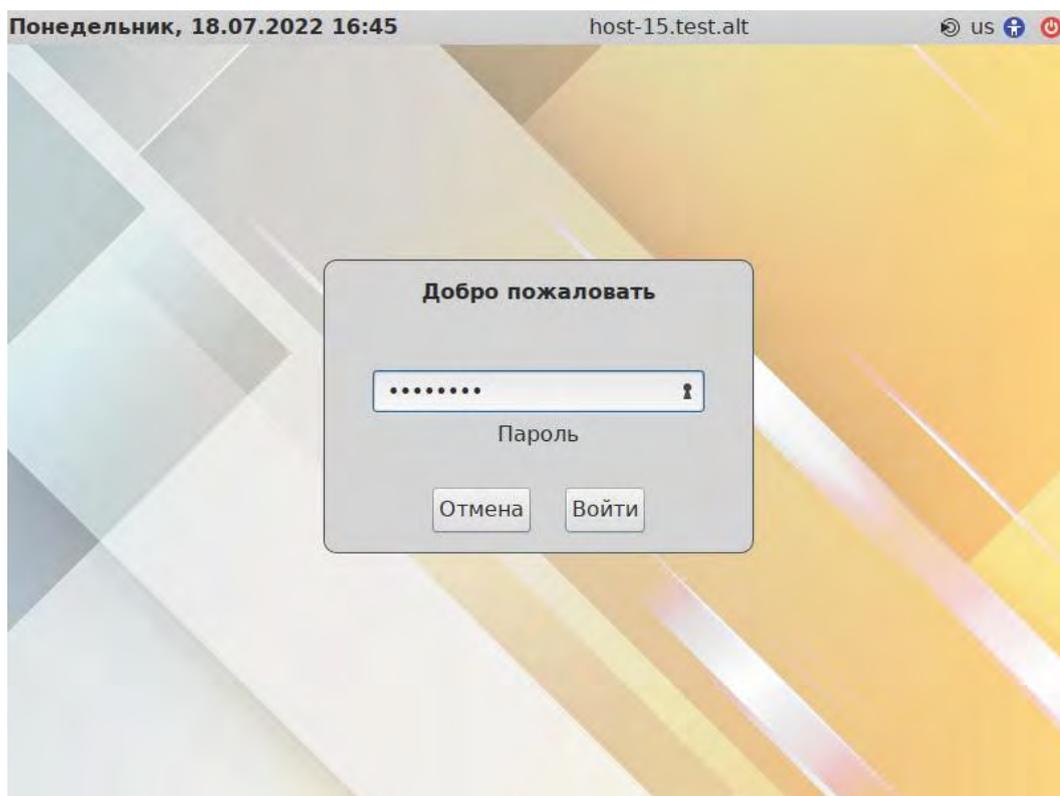


Рис. 105

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
us-
ers:cdwriter,cdrom,audio,video,proc,radio,camera,floppy,xgrp,scanner,u
ucp,vboxusers,fuse,vboxadd
vboxadd:vboxsf
# id ivanov
```

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

Если необходимо выдать права администраторов пользователям, которые не являются администраторами домена (Domain Admins), то нужно завести новую группу в AD (например, PC Admins), добавить туда необходимых пользователей. 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
us-
ers:cdwriter,cdrom,audio,video,proc,radio,camera,floppy,xgrp,scanner,u
ucp,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, Rcmannfm). 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="dc.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="dc.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="dc.test.alt "
path="sysvol" mountpoint="~/share"
options="sec=krb5,vers=2.0,cruid=%(USERUID),nounix,uid=%(USERUID),gid=%(USERG
ID),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 `grpupdate`. Инструмент рассчитан на работу на машине, введённой в домен Samba.

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

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

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

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

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

Групповые политики можно использовать для разных целей, например:

- управления интернет-браузерами Firefox/Chromium. 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;
- подключения сетевых дисков (экспериментальная политика);
- управления общими каталогами (экспериментальная политика);
- генерирования (удаления/замены) ярлыков для запуска программ;
- создания каталогов;
- управления файлами (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 развёртывания 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-samba`, `admx-chromium`, `admx-firefox` и утилиту `admx-msi-setup`:

```
# apt-get install admx-basealt admx-samba admx-chromium admx-firefox
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. 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. 102).

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. 106).

Модуль ЦУС «Групповые политики»

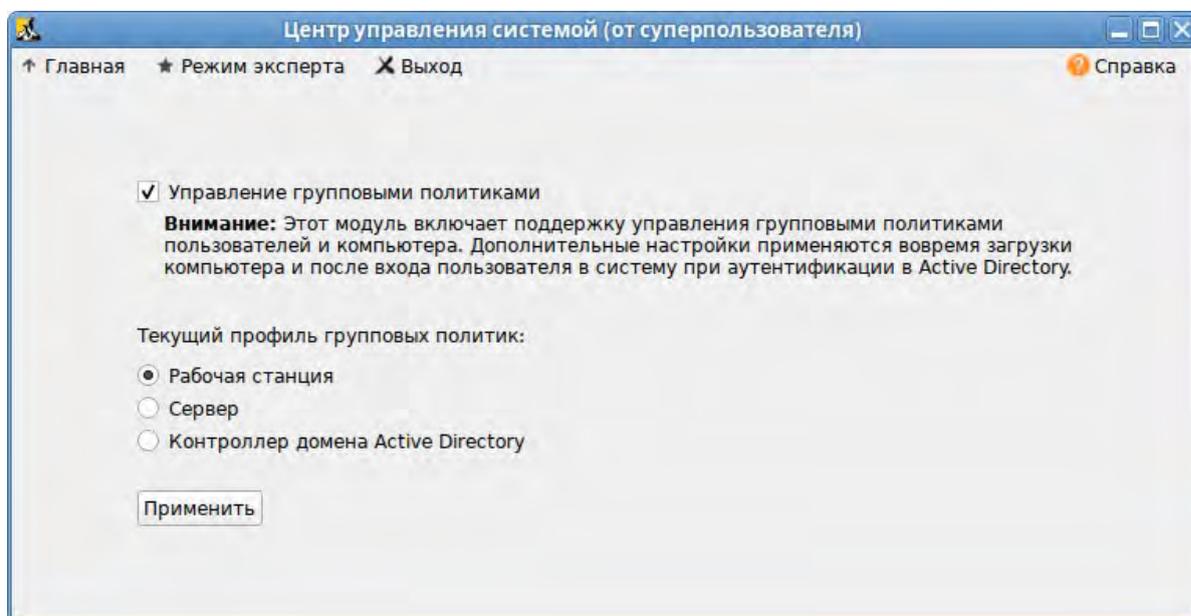


Рис. 106

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 admx-basealt
```

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. 107).

Административные шаблоны в консоли gpmc.msc

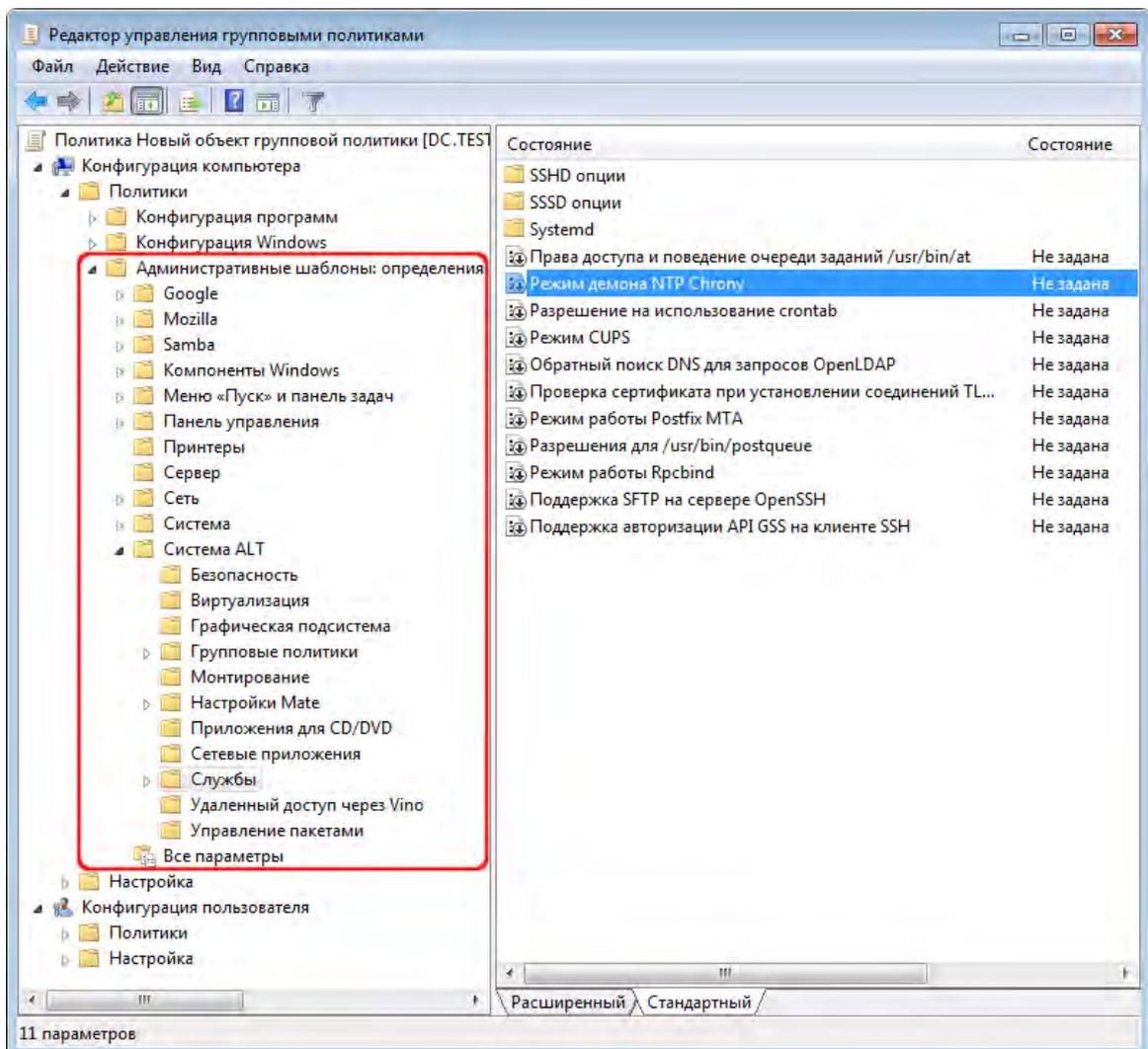


Рис. 107

4.9.2 Пример создания групповой политики

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

В ADMC на рабочей станции, введённой в домен или в оснастке Active Directory – пользователи и компьютеры создать подразделение (OU) и переместить в него компьютеры и пользователи домена.

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

```
$ kinit administrator
```

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

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

```
$ admc
```

Интерфейс ADMC показан на Рис. 108.

Интерфейс ADMC

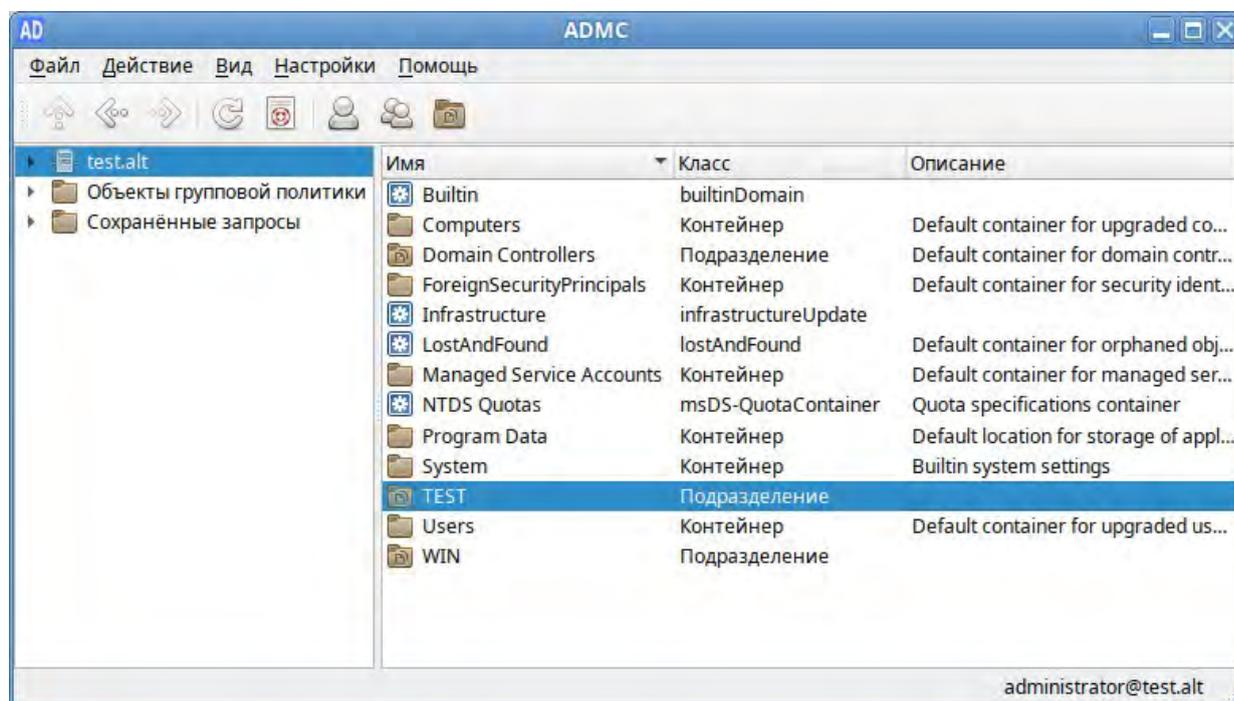


Рис. 108

Для создания подразделения следует:

- в контекстном меню домена выбрать пункт «Создать» → «Подразделение» (Рис. 109);
- в открывшемся окне ввести название подразделения (например, OU) и нажать кнопку «ОК» (Рис. 110).

ADMC. Создание нового подразделения

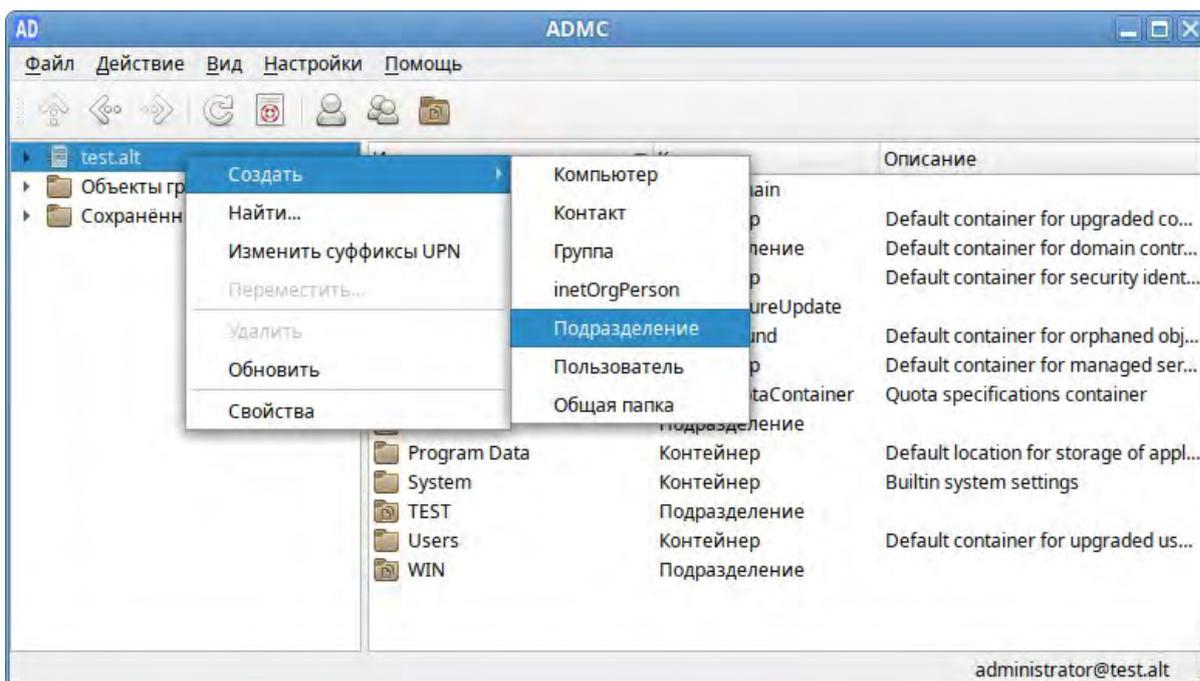


Рис. 109

ADMC. Новое подразделение

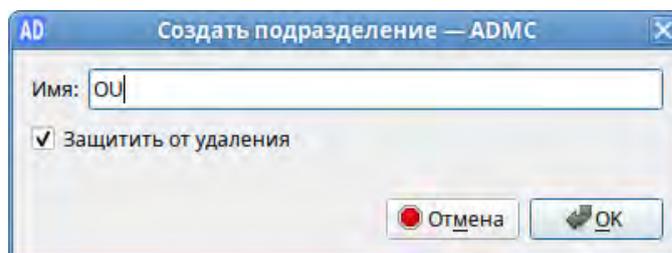


Рис. 110

Далее необходимо переместить компьютеры и пользователей домена в подразделение OU (Рис. 111):

- 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. 112);
- в открывшемся окне ввести название политики и нажать кнопку «ОК» (Рис. 113).

Компьютеры и пользователи в подразделении OU

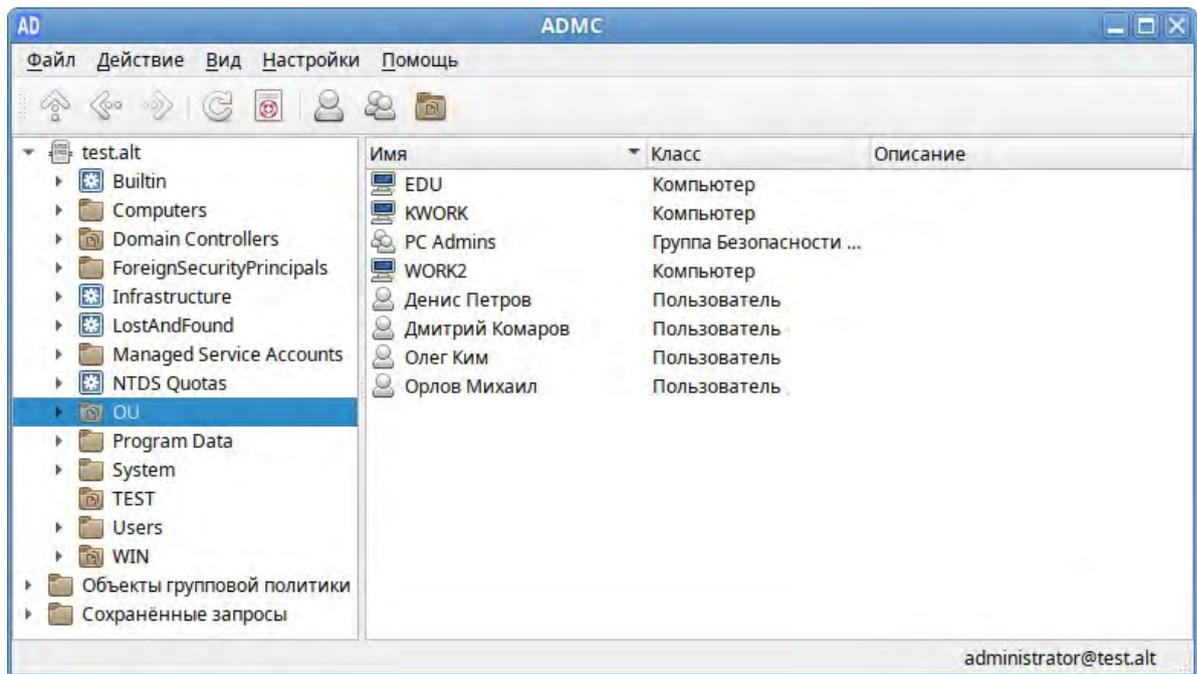


Рис. 111

ADMS. Контекстное меню подразделения в объектах групповых политик

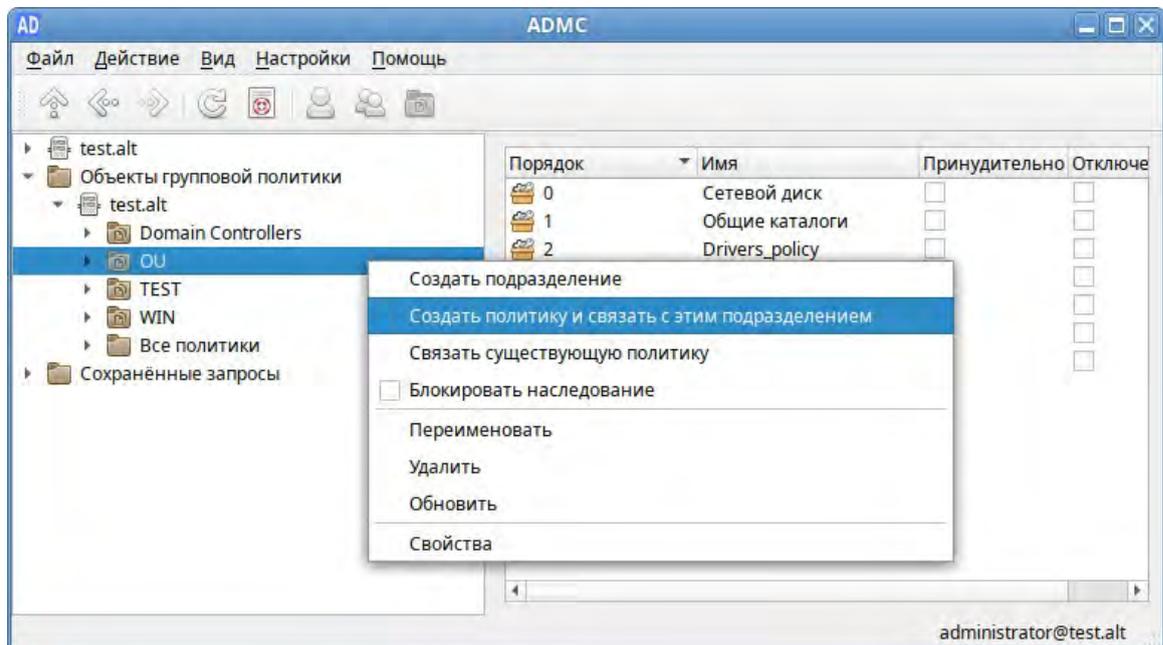


Рис. 112

ADMS. Создание объекта групповой политики

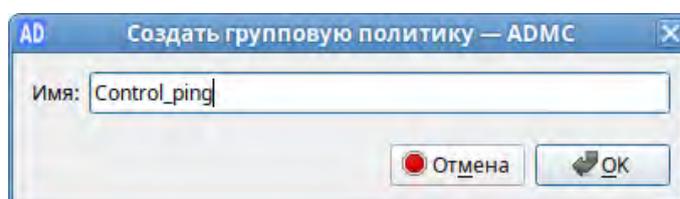


Рис. 113

Для редактирования настроек групповой политики, необходимо выполнить следующие действия:

- в контекстном меню политики выбрать пункт «Изменить...» (Рис. 114);
- откроется окно редактирования групповых политик (GPO) (Рис. 115);
- 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. 116);
- щелкнуть левой кнопкой мыши на политике «Разрешения для /usr/bin/ping». Откроется диалоговое окно настройки политики. Выбрать параметр «Включено», в выпадающем списке «Кому разрешено» выбрать пункт «Только root» и нажать кнопку «ОК» (Рис. 117);
- 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

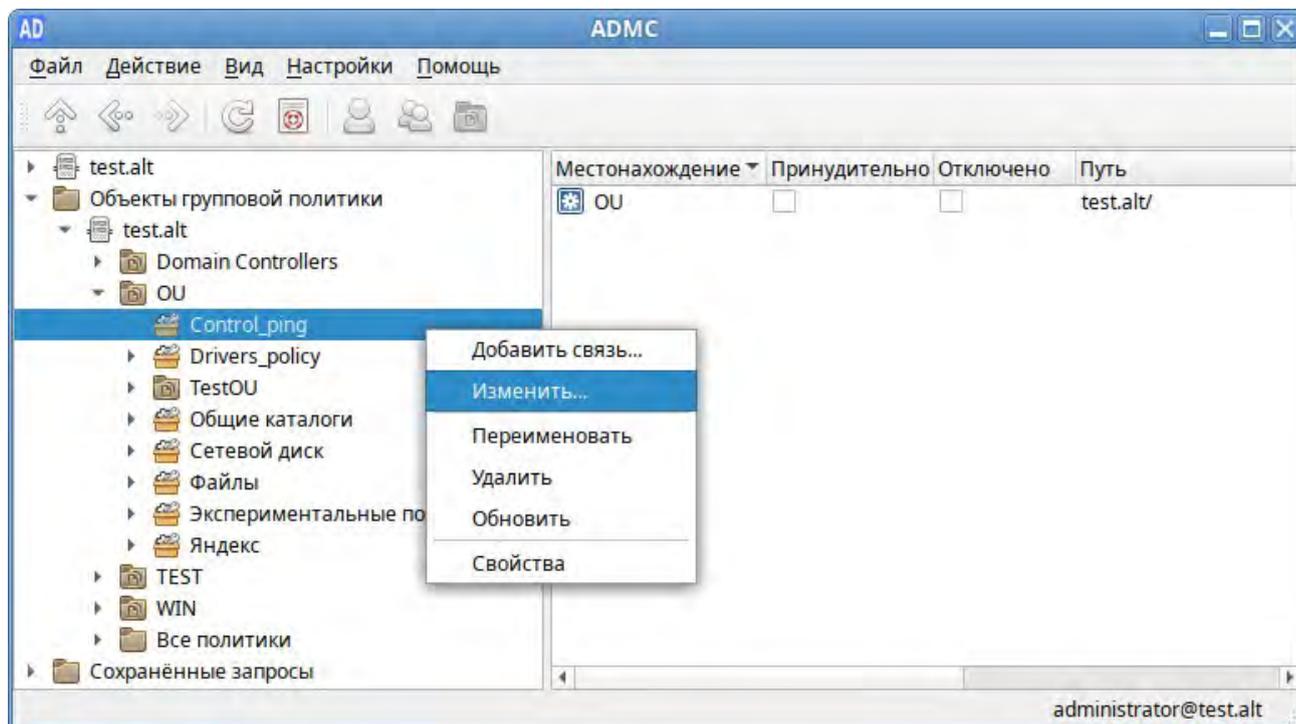


Рис. 114

Модуль редактирования настроек клиентской конфигурации (GPUI)

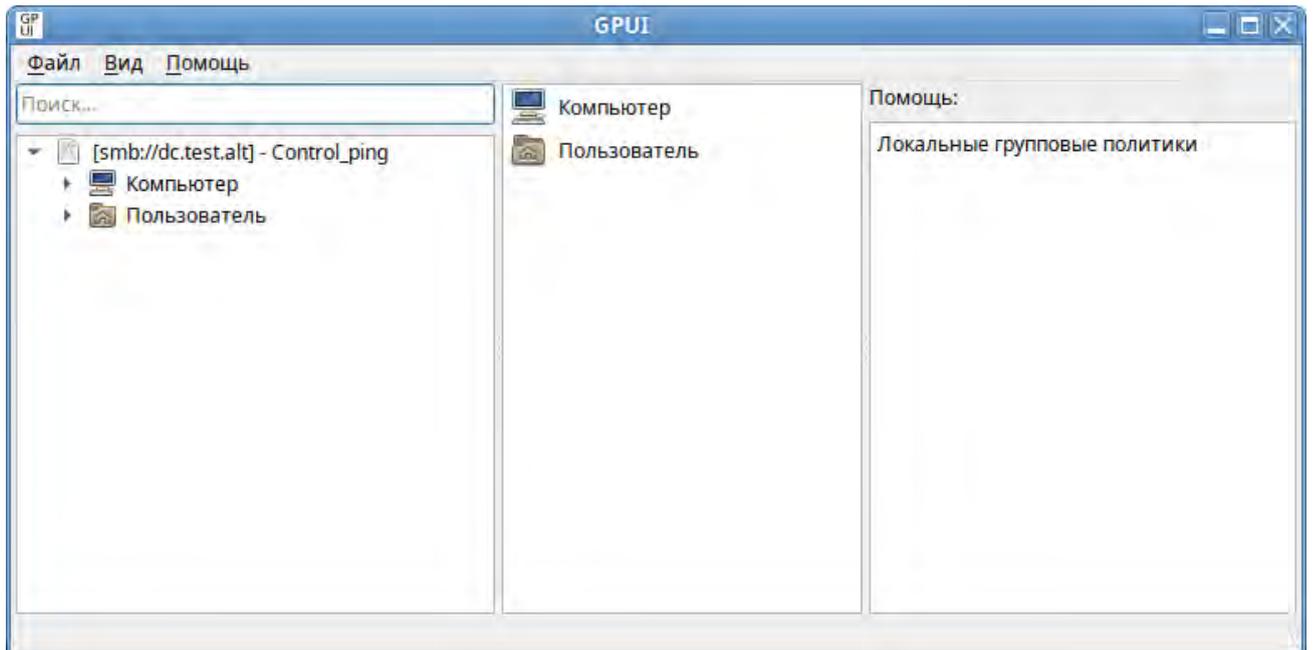


Рис. 115

Модуль редактирования настроек клиентской конфигурации (GPUI)

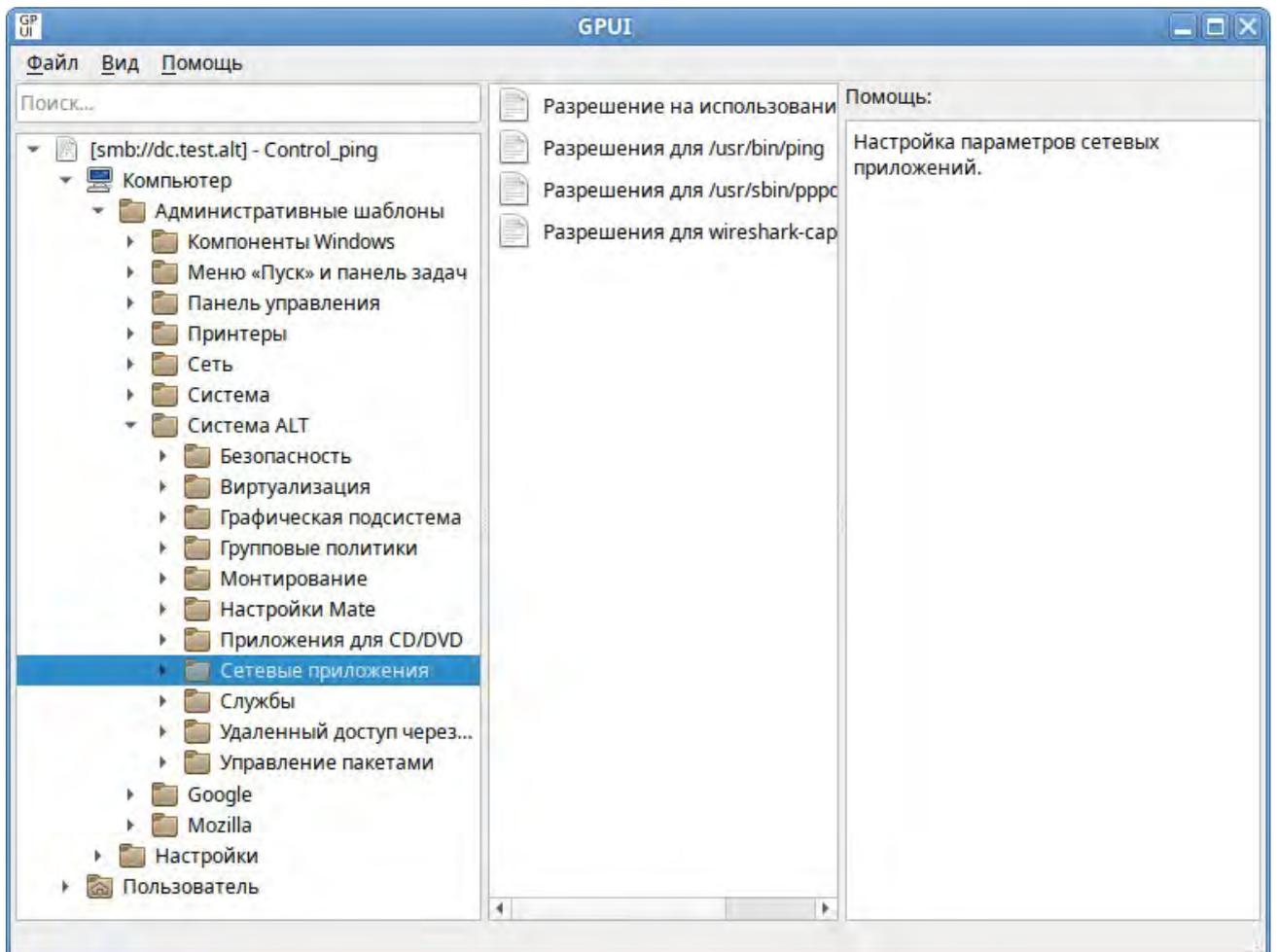


Рис. 116

GPUI. Диалоговое окно настройки политики

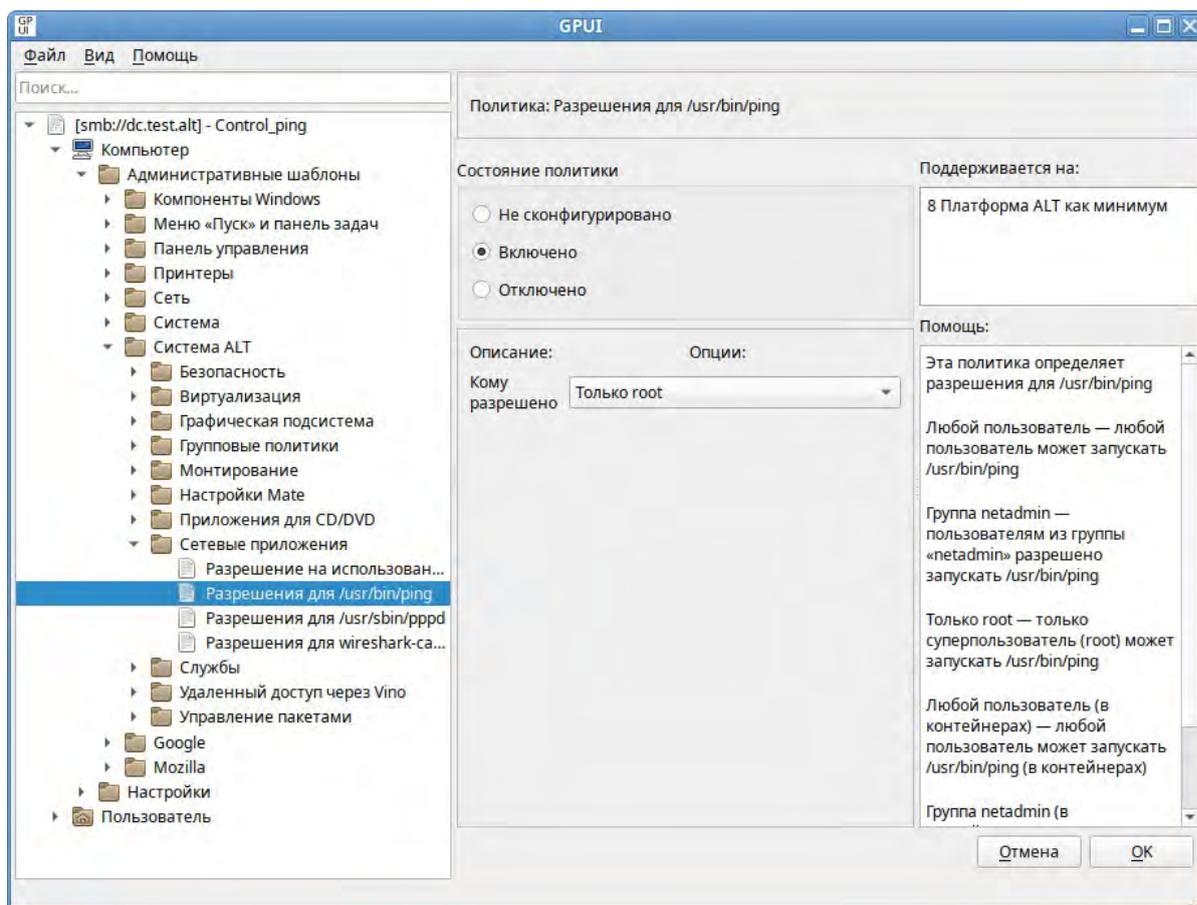


Рис. 117

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. 118);
- дважды щелкнуть левой кнопкой мыши на политике «Разрешения для /usr/bin/ping». Откроется диалоговое окно настройки политики (Рис. 119). Выбрать параметр «Включить», в выпадающем списке «Кому разрешено выполнять» выбрать пункт «Только root» и нажать кнопку «Применить».

Раздел «Сетевые приложения»

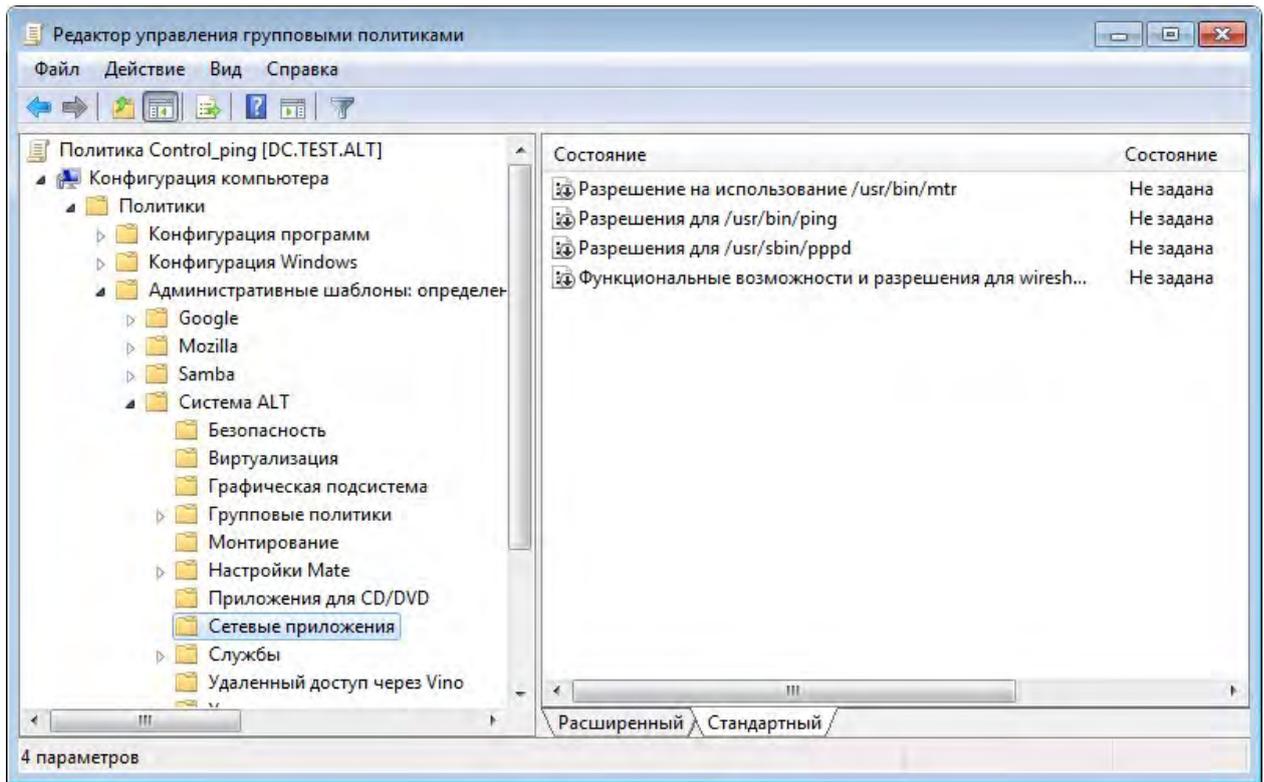


Рис. 118

Политика «Разрешения для /usr/bin/ping»

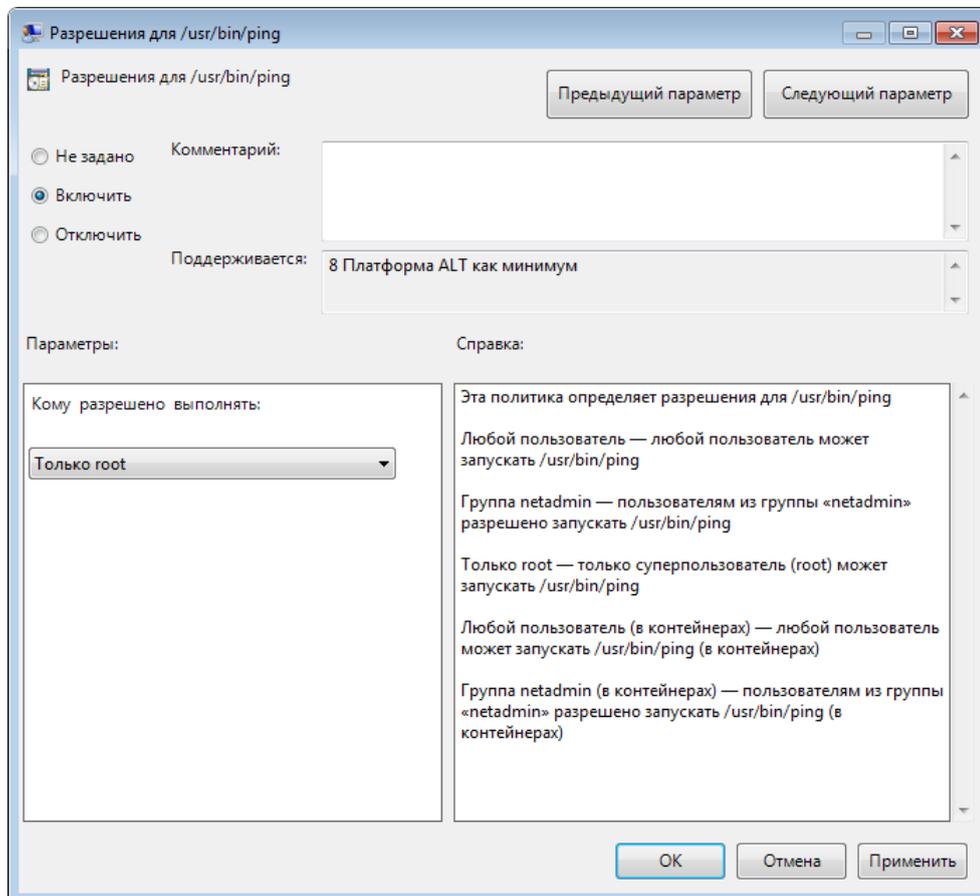


Рис. 119

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 «Иридиум» 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. 120);

- 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

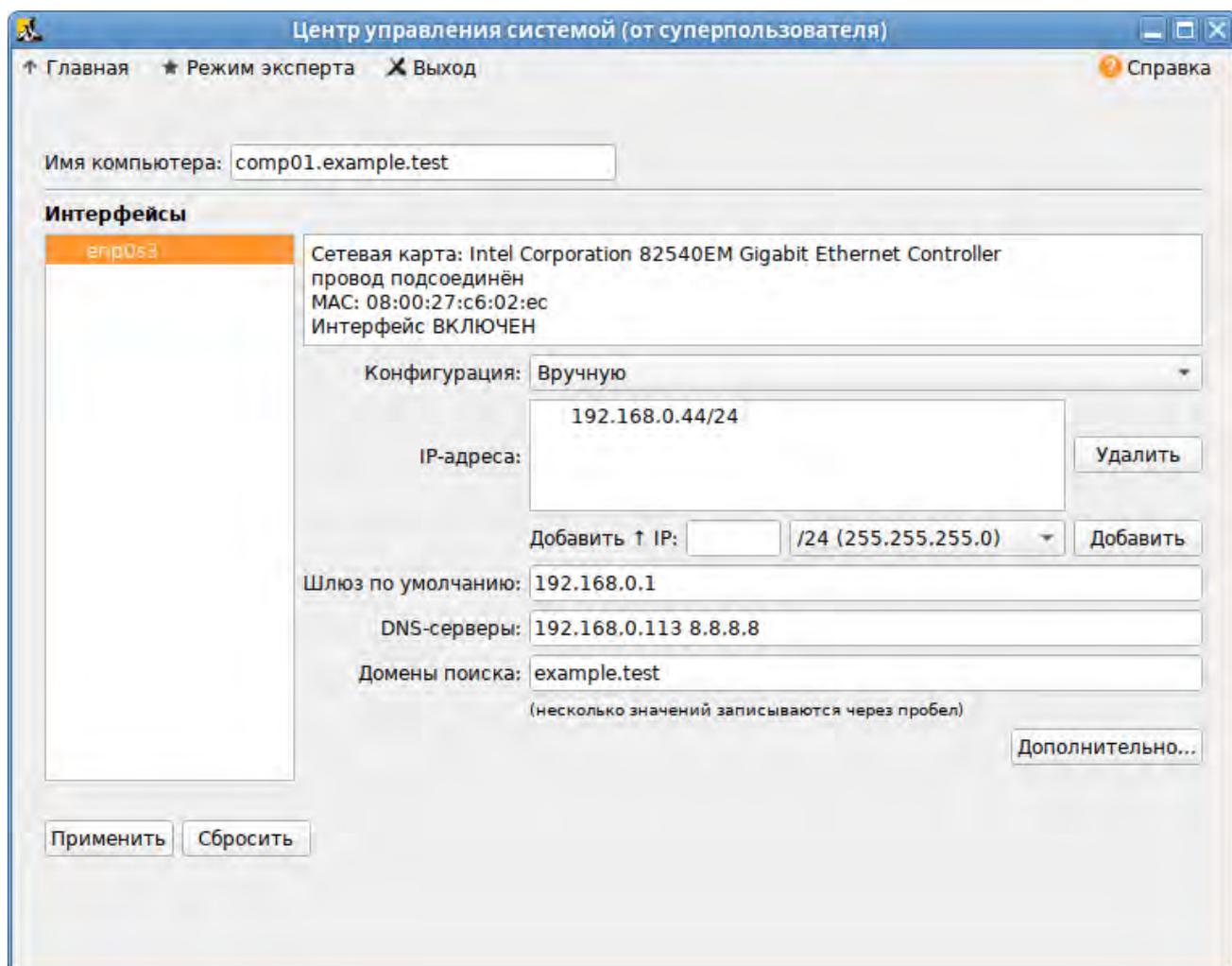


Рис. 120

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. 121), затем нажать кнопку «Применить».

Ввод в домен FreeIPA в Центре управления системой

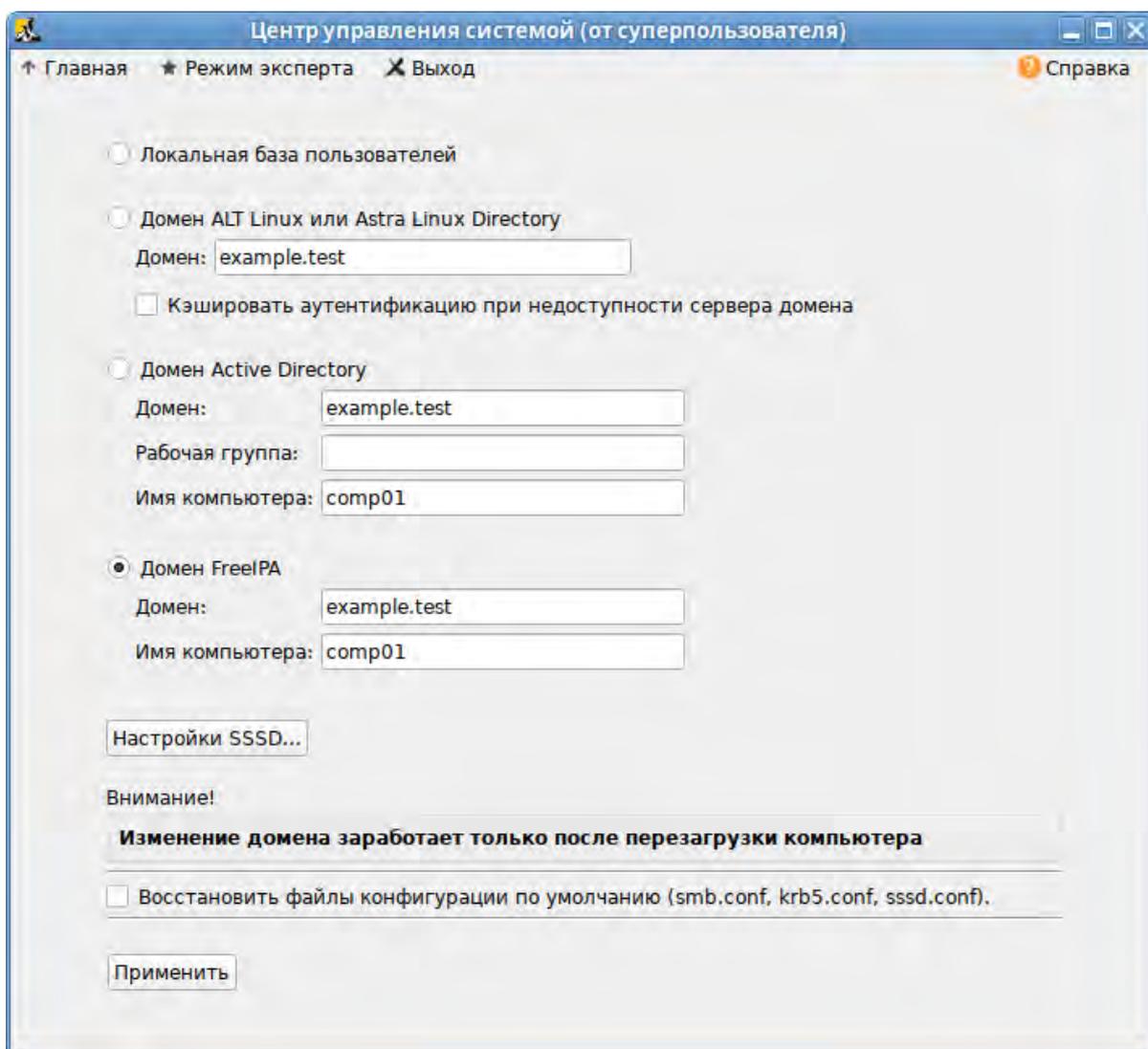
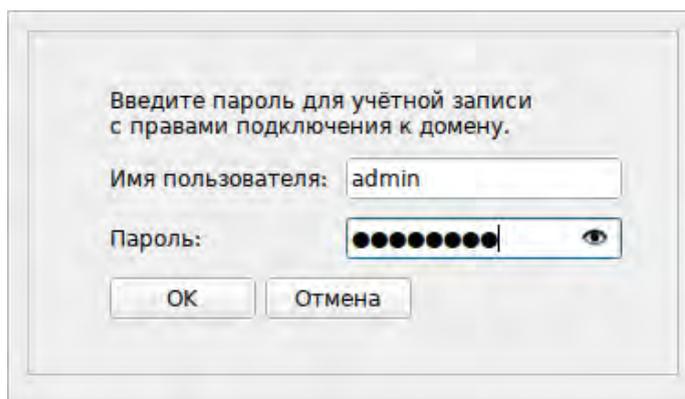
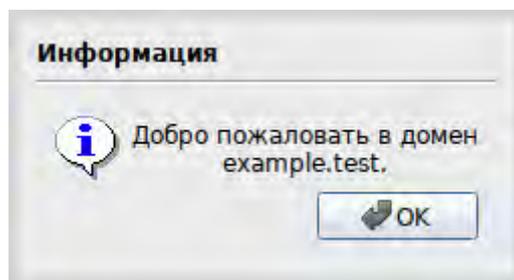


Рис. 121

В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль (Рис. 122) и нажать кнопку «ОК».

Параметры учётной записи с правами подключения к домену*Рис. 122*

В случае успешного подключения, будет выведено соответствующее сообщение (Рис. 123).

Подключение к серверу FreeIPA*Рис. 123*

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. 124) необходимо ввести логин учетной записи пользователя FreeIPA и нажать кнопку «Войти», в открывшемся окне ввести пароль, соответствующий этой учетной записи и нажать кнопку «Войти».

При первом входе пользователя будет запрошен текущий (установленный администратором) пароль и затем у пользователя запрашивается новый пароль и его подтверждение (Рис. 125).

Вход пользователя

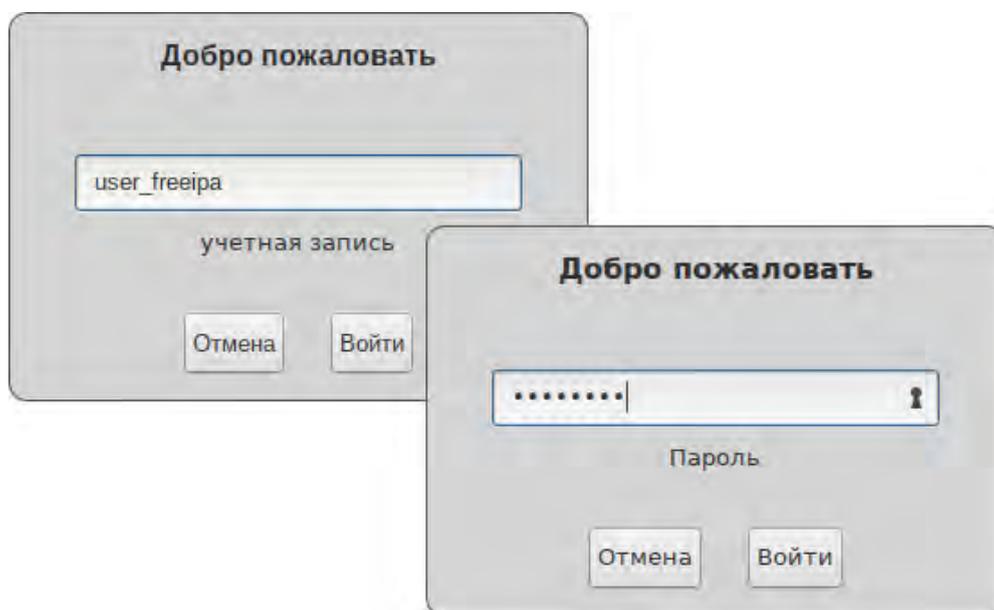


Рис. 124

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

Срок действия пароля истёк. Необходимо сейчас изменить ваш пароль.

.....|

Текущий пароль

Отмена Войти

Срок действия пароля истёк. Необходимо сейчас изменить ваш пароль.

.....|

Новый пароль

Отмена Войти

Рис. 125

5 СРЕДСТВА УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ

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 «Иридиум» 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. 126).

Настройка модуля «Ethernet-интерфейсы»

Рис. 126

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

- «Имя компьютера» – указать сетевое имя ПЭВМ в поле для ввода имени компьютера (это общий сетевой параметр, не привязанный к какому либо конкретному интерфейсу). Имя компьютера, в отличие от традиционного имени хоста в Unix (hostname), не содержит названия сетевого домена;
- «Интерфейсы» – выбрать доступный сетевой интерфейс, для которого будут выполняться настройки;
- «Версия протокола IP» – указать в выпадающем списке версию используемого протокола IP (IPv4, IPv6) и убедиться, что пункт «Включить», обеспечивающий поддержку работы протокола, отмечен;
- «Конфигурация» – выбрать способ назначения IP-адресов (службы DHCP, Zeroconf, вручную);
- «IP-адреса» – пул назначенных IP-адресов из поля «IP», выбранные адреса можно удалить нажатием кнопки «Удалить»;

- «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. 127).

Автоматическое получение настроек от DHCP сервера

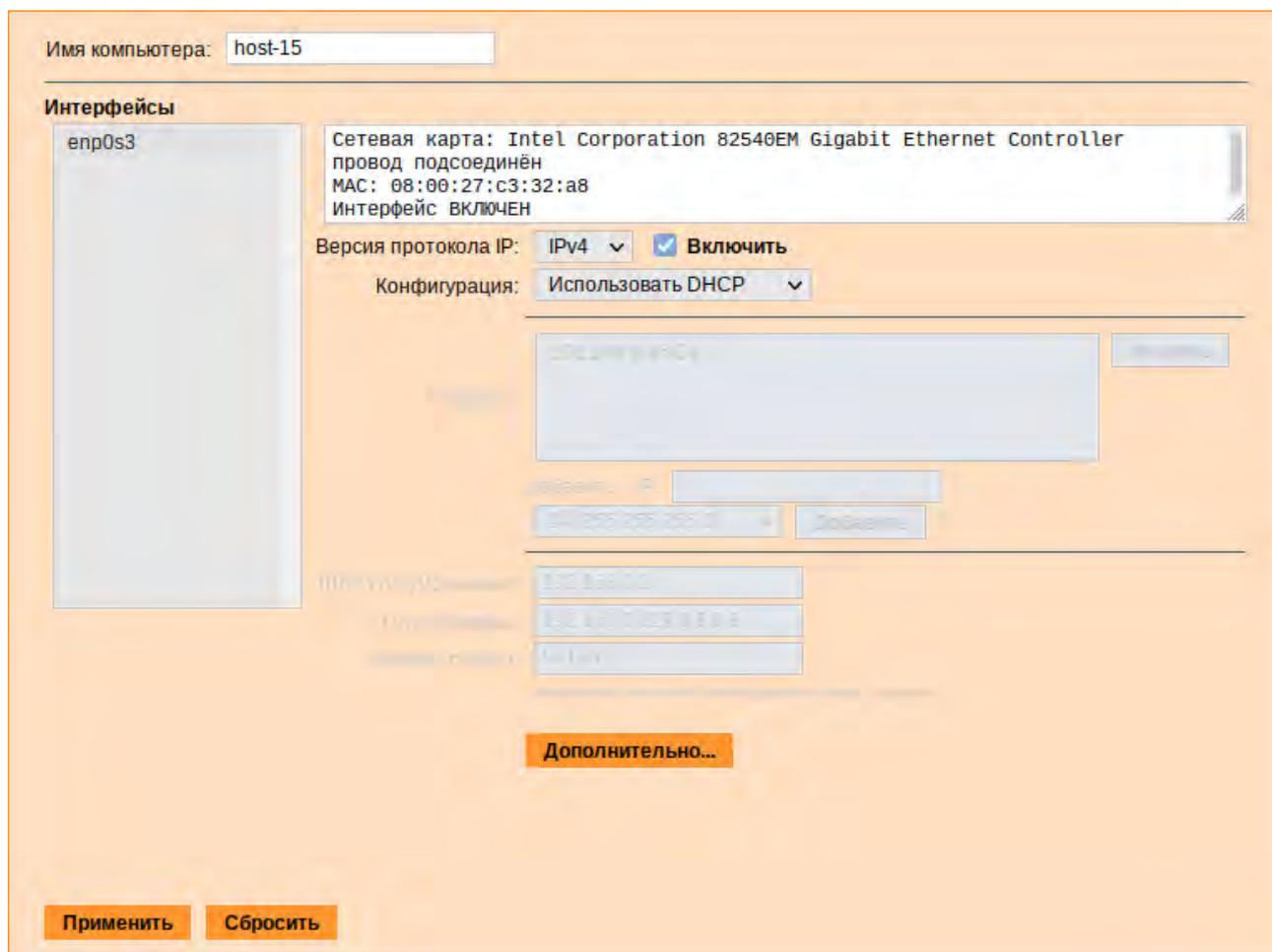


Рис. 127

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 получают 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. 128).

Выбор сетевой подсистемы

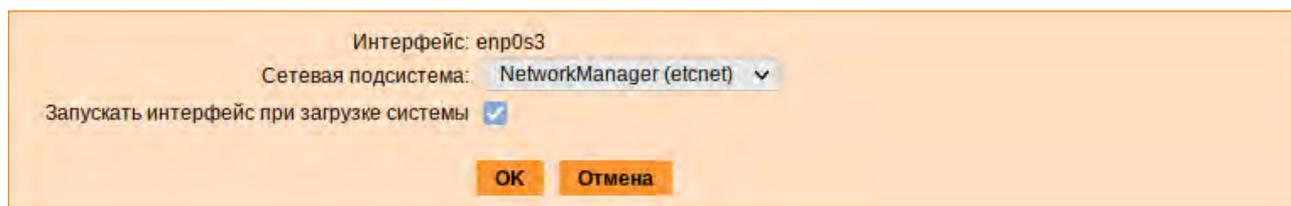


Рис. 128

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 иницирует сеть, используя в качестве параметров – настройки из файлов Etcnet. Настройки сети могут изменяться либо в ЦУС в данном модуле, либо напрямую через редактирование файлов `/etc/net/ifaces/<интерфейс>`. В этом режиме можно просмотреть настройки сети, например полученный по DHCP IP-адрес, через графический интерфейс NetworkManager;
- «NetworkManager (native)» – в данном режиме управление настройками интерфейса передается NetworkManager и не зависит от файлов Etcnet. Управлять настройками можно через графический интерфейс NetworkManager. Файлы с настройками находятся в 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).

5.3 Сетевая установка операционной системы на рабочие места

Одной из удобных возможностей ОС «Иридиум» при разворачивании инфраструктуры является сетевая установка. При помощи сетевой установки можно производить установку дистрибутивов не с DVD-диска, а загрузив инсталлятор по сети.

5.3.1 Подготовка сервера сетевых установок

Перед началом установки рабочих станций следует произвести предварительную настройку сервера сетевых установок (например, на базе ОС «Альт Сервер» или ОС «Иридиум»): задать имя сервера (модуль «Ethernet-интерфейсы» в «Центре управления системой»), включить DHCP-сервер, задать, если необходимо, имя домена.

Примечание. При сетевой установке с сервера будут переняты настройки домена, и будет включена централизованная аутентификация. Если ОС «Иридиум» устанавливается с DVD-диска, то настройку домена и аутентификации надо будет производить отдельно на каждой рабочей станции.

Перед активацией сетевой установки потребуется импортировать установочный DVD-диск ОС, предварительно вставив его в DVD-привод сервера, либо можно использовать образ диска, расположенный на файловой системе на сервере. Можно также использовать URL вида

http://ftp.altlinux.org/pub/distributions/ALTLinux/images/p9/workstation/x86_64/alt-workstation-9.2-x86_64.iso.

Примечание. Локальный файл должен быть доступен для nobody и должен находиться на сервере, где запущен alterator-netinst.

В разделе «Сервер сетевых установок» (пакет alterator-netinst) (Рис. 129), необходимо указать, откуда импортировать новый образ и нажать кнопку «Добавить». Процесс добавления занимает какое-то время.

Импорт установочного образа



Рис. 129

После добавления образа он появится в списке «Доступные образы дисков». Необходимо выбрать из списка один из образов (Рис. 130) и нажать кнопку «Выбрать». На этом подготовка сервера к сетевой установке рабочих станций завершена.

Выбор образа диска

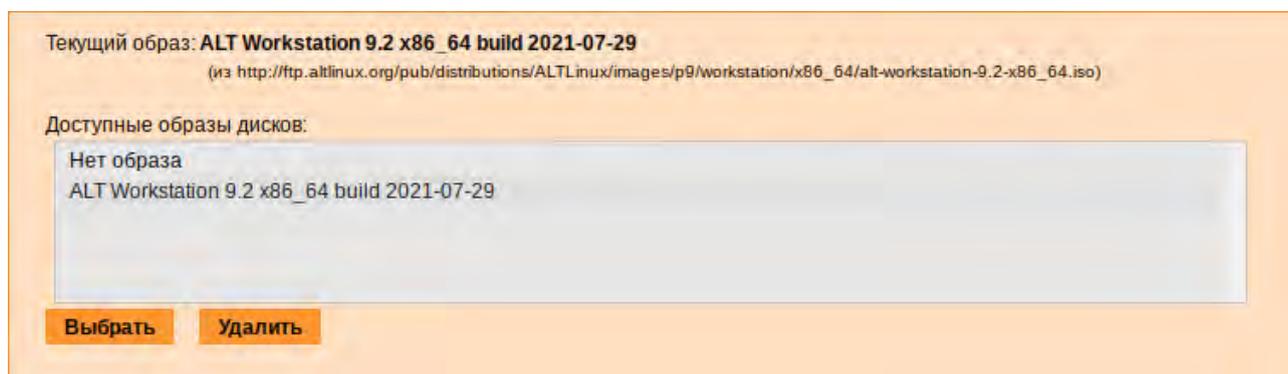


Рис. 130

Дополнительно данный модуль позволяет выбрать вариант загрузки (например, непосредственно загружать ОС некоторых Live-версий дистрибутивов).

Далее необходимо выбрать направление соединения (Рис. 131). Удалённый доступ к компьютеру бывает двух видов:

1. Со стороны клиента. Во время установки администратор может с помощью VNC-клиента подключиться к компьютеру, на которой производится установка, зная его IP-адрес и заданный пароль.
2. Со стороны сервера. Во время установки с каждого компьютера инициируется подключение к запущенному на заданном компьютере VNC-клиенту. Компьютер-приёмник соединений задаётся IP-адресом или именем.

Выбор направления соединения

Вариант загрузки: установка системы

Включить установку по VNC

Только по VNC

Направление соединения:

Подключение со стороны VNC клиента

Подключение со стороны VNC сервера

Применить

Рис. 131

В случае, когда работа с аппаратной подсистемой ввода-вывода невозможна (например, если клавиатура, мышь или монитор отсутствуют), можно использовать вариант «Только по VNC».

Если необходимо управлять установкой удалённо, необходимо отметить пункт «Включить установку по VNC» и пункт «Подключение со стороны VNC сервера» раздела «Направление соединения», и там указать адрес компьютера, с которого будет происходить управление. Для приёма подключения можно запустить, например, `vncviewer -listen`.

Примечание. По окончании процесса установки ОС на рабочих станциях необходимо отключить сетевую установку. Это можно сделать, выбрав в списке «Доступные образы дисков» пункт «Нет образа» и подтвердив действие нажатием кнопки «Выбрать».

5.3.2 Подготовка рабочих станций

Для сетевой установки следует обеспечить возможность загрузки по сети рабочих станций, на которых будет производиться установка ОС.

Большинство современных материнских плат имеют возможность загрузки по сети, однако она по умолчанию может быть отключена в BIOS. Различные производители материнских плат дают разные названия данной возможности, например: «Boot Option ROM» или «Boot From Onboard LAN».

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

5.4 Соединение удалённых офисов (OpenVPN-сервер)

ОС «Иридиум» предоставляет возможность безопасного соединения удалённых офисов, используя технологию VPN (англ. Virtual Private Network – виртуальная частная сеть), которая позволяет организовать безопасные зашифрованные 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.

5.4.1 Настройка OpenVPN-сервера

OpenVPN-сервер может быть развернут, например, на базе ОС «Альт Сервер» или ОС «Иридиум. Модуль «OpenVPN-сервер» (пакет alterator-openvpn-server) из раздела «Серверы» позволяет задать параметры OpenVPN-сервера (Рис. 132).

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.

Модуль «OpenVPN-сервер»

Рис. 132

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. 133).

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. 134).

Модуль «Управление ключами SSL»

Настройки SSL

Общее имя (CN):
(имя компьютера для сервера или что-либо другое для клиента)

Страна (C):
(двухбуквенный код страны)

Местоположение (L):
(название города или области, написанное латинскими буквами)

Организация (O):
(название организации, написанное латинскими буквами)

Подразделение (OU):
(название подразделения, написанное латинскими буквами)

E-mail адрес:
(ваш адрес электронной почты)

(Пере)создать ключ и запрос на подпись **Подтвердить**

Рис. 133

Забрать запрос на подпись

Подпись

Забрать запрос на подпись

Положить сертификат, подписанный УЦ:

Рис. 134

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. 135).

Ключ openvpn-server

SSL ключи:

ahhttpd (истекает: 07.12.2022)
 openvpn-server (Нет сертификата)

Удалить ключ, сертификат и запрос на подпись

Рис. 135

Чтобы подписать сертификат необходимо перейти в модуль «Удостоверяющий Центр» → «Управление сертификатами», нажать кнопку «Обзор», указать путь до полученного файла `openvpn-server.csr` и загрузить запрос (Рис. 136).

Запрос на подпись сертификата



Рис. 136

В результате на экране появится две группы цифр и кнопка «Подписать» (Рис. 137). Необходимо нажать на кнопку «Подписать» и сохранить файл `output.pem` (подписанный сертификат).

Запрос на подпись сертификата

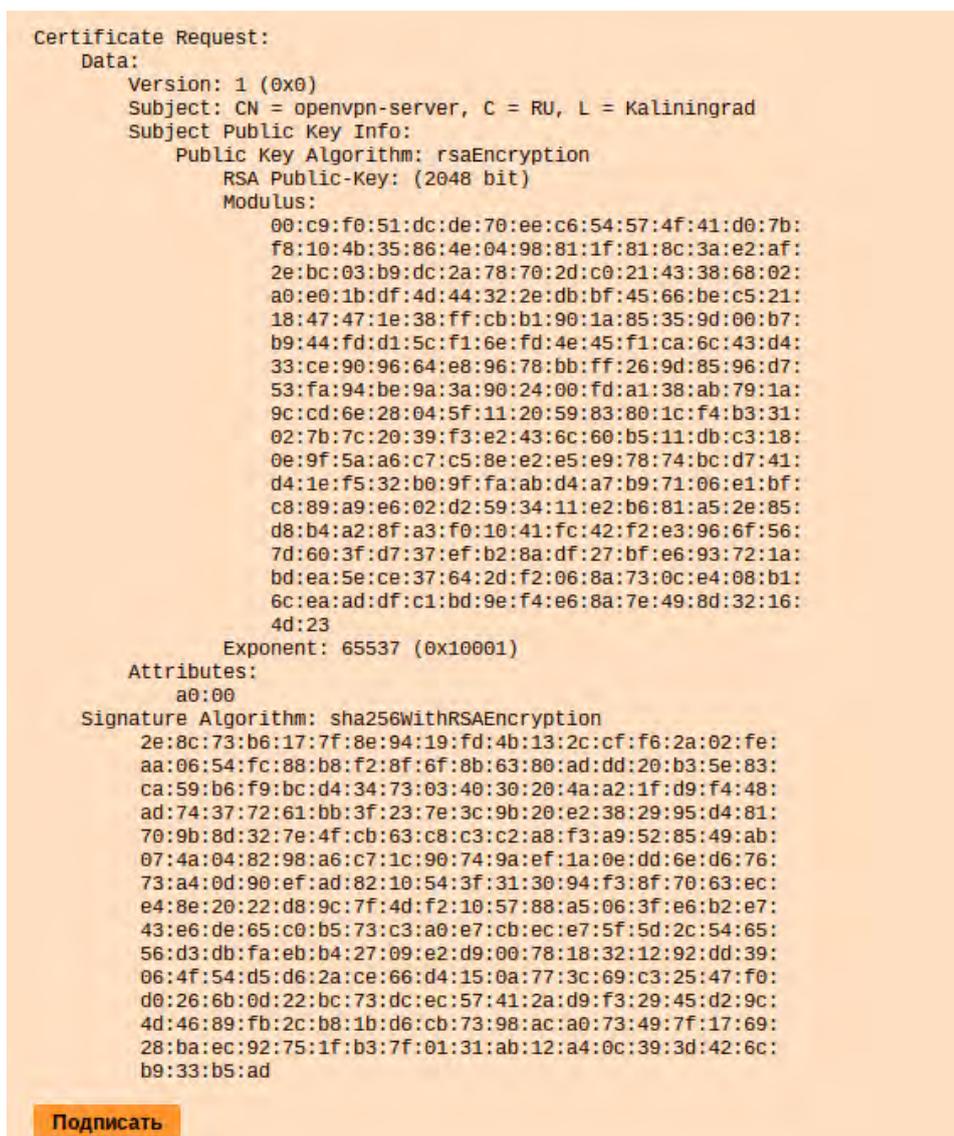


Рис. 137

Далее в разделе «Управление ключами SSL», необходимо выделить ключ «openvpn-server (Нет сертификата)» и нажать кнопку «Изменить». В появившемся окне, в пункте «Положить сертификат, подписанный УЦ» нужно нажать кнопку «Обзор», указать путь до файла `output.pem` и нажать кнопку «Положить» (Рис. 138).

Сертификат, подписанный УЦ

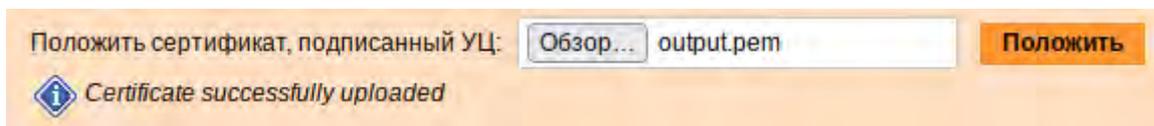


Рис. 138

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

Для того чтобы положить сертификат УЦ, необходимо найти его в модуле «Удостоверяющий Центр», нажать на ссылку «Управление УЦ» и забрать сертификат, нажав на ссылку «Сертификат: `ca-root.pem`» (Рис. 139).

Сертификат УЦ



Рис. 139

В модуле «OpenVPN-сервер», в графе «Положить сертификат УЦ»: при помощи кнопки «Обзор» указать путь к файлу `ca-root.pem` и нажать кнопку «Положить» (Рис. 140).

Выбор сертификата УЦ в модуле «OpenVPN-сервер»



Рис. 140

Появится сообщение: «Сертификат УЦ успешно загружен».

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

5.4.2 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. 141). Должен быть выбран тот же тип, что и на стороне сервера.

Создание нового OpenVPN- соединения

Рис. 141

Необходимо 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 подписать ключ `openvpn` в модуле «Удостоверяющий Центр» (пакет `alterator-ca`) на сервере.

В результате станут доступны настройки соединения (Рис. 142).

Модуль «OpenVPN- соединения»

Рис. 142

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

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

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

Проверить, появилось ли соединение с сервером можно командой:

```
$ ip addr
```

Должно появиться новое соединение tun1. При обычных настройках это может выглядеть так:

```
tun0:    <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP>    mtu    1500    qdisc
pfifo_fast state UNKNOWN qlen 100
    link/[none]
    inet 10.8.0.6 peer 10.8.0.5/32 scope global tun0
```

5.5 Доступ к службам из сети Интернет

5.5.1 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. 143). Если необходимо предоставить доступ к службе, отсутствующей в списке, то нужно задать используемые этой службой порты в соответствующих полях.

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.

Модуль «Внешние сети»

Версия IP: Включить брандмауэр

Выберите режим работы:

Выберите внешние интерфейсы: enp0s3 (Intel Corporation 82540EM Gigabit Ethernet Controller) 192.168.0.45/24

Разрешить входящие соединения на внешних интерфейсах:

Службы:

- Центр управления системой (www)
- Система печати CUPS
- DHCP
- DNS
- Передача файлов (FTP)
- Почтовый сервер (IMAP)
- LDAP
- OpenVPN
- Почтовый сервер (POP3)
- Прокси-сервер
- Файловый сервер (Samba)
- Почтовый сервер (SMTP)
- Управление сетью (SNMP)
- Удалённый доступ (SSH)
- Удалённый доступ (telnet)
- HTTP/HTTPS
- Zeroconf
- SIP/H.323
- STUN
- VPN
- Служебные пакеты (ICMP)

Дополнительные порты TCP:

(разделенные запятыми или пробелами)

Дополнительные порты UDP:

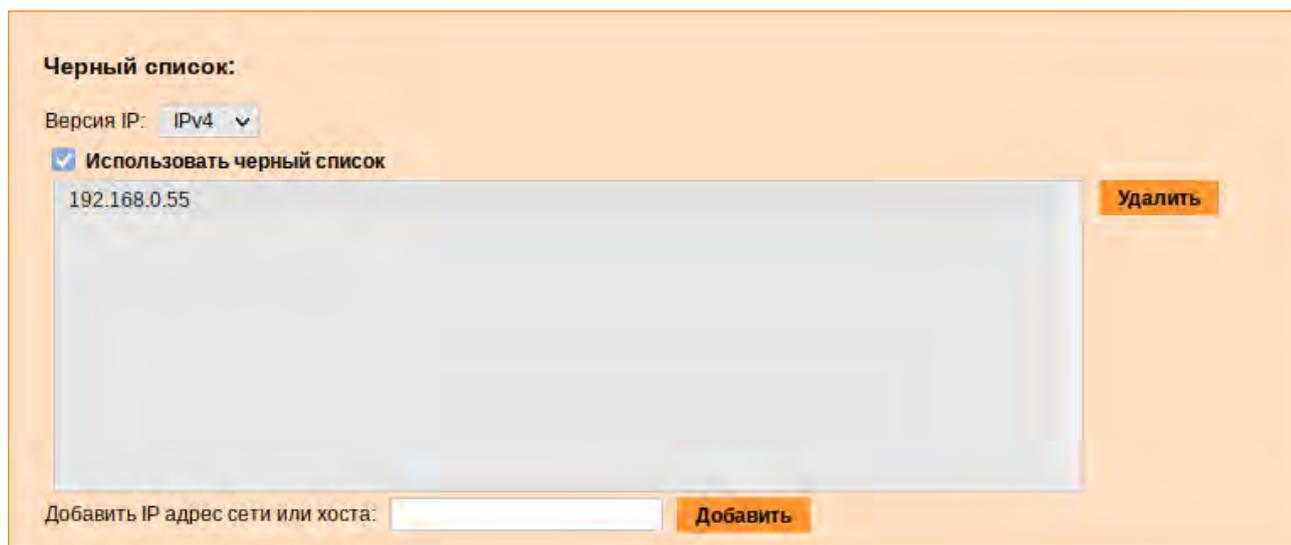
(разделенные запятыми или пробелами)

Рис. 143

5.5.2 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. 144).

Модуль «Список блокируемых хостов»*Рис. 144*

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».

5.6 Обслуживание рабочей станции

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

5.6.1 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. 145).

Модуль «Системные журналы»

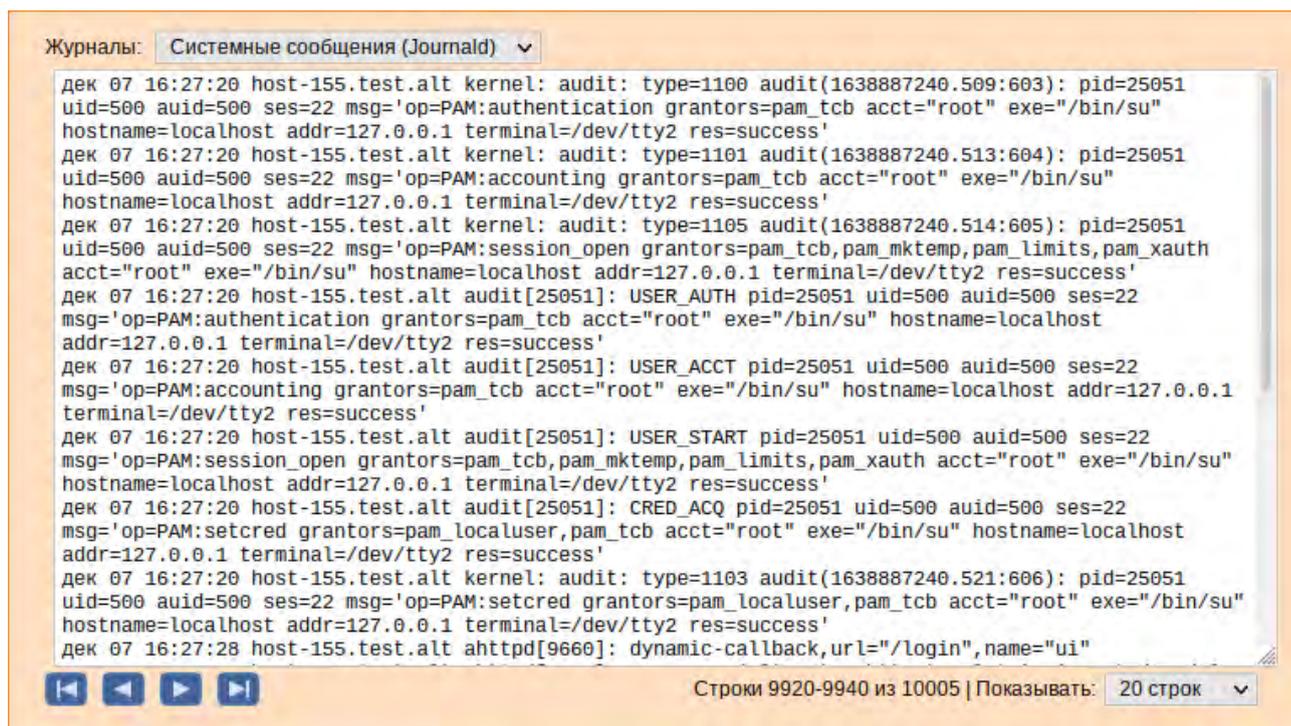


Рис. 145

Доступны следующие виды журналов:

- «Брандмауэр» – отображаются события безопасности, связанные с работой межсетевого экрана ОС;
- «Системные сообщения» – сообщения от системных служб (сообщения с типом DAEMON).

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

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

5.6.2 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. 146).

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

Модуль «Системные службы»

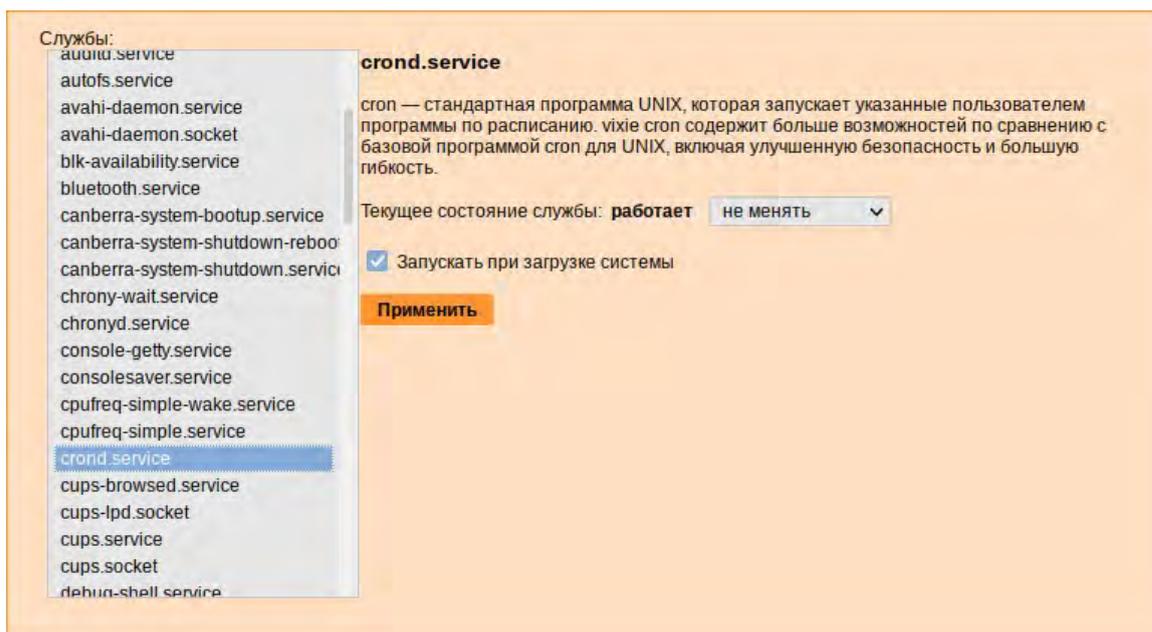


Рис. 146

5.6.3 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.

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

На Рис. 147 показаны политики для команды fusermount.

Модуль «Системные ограничения»

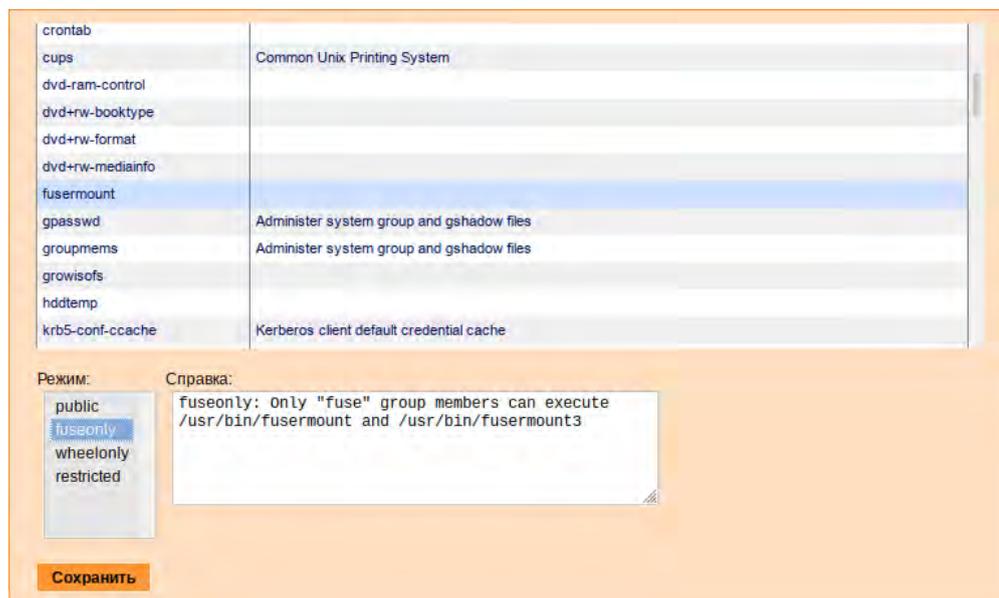


Рис. 147

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

5.6.4 Обновление системы

После установки системы крайне важно следить за обновлениями ПО. Обновления для ОС «Иридиум» 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. 148).

Модуль «Обновление системы»

Рис. 148

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»).

Также необходимо 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. 149).

Указание источника обновлений

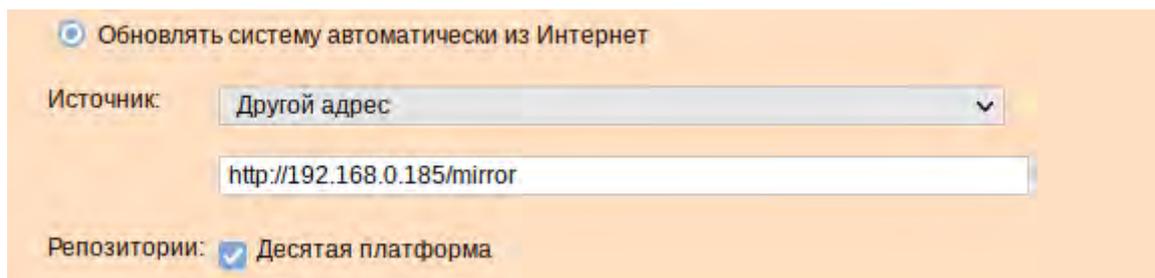


Рис. 149

5.6.5 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 «Иридиум»), находящегося вне защищенного контура и организация ограниченного доступа к этому серверу.

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

На странице модуля можно выбрать, как часто выполнять загрузку пакетов, можно выставить время, когда начинать зеркалирование (Рис. 150).

Здесь также можно выбрать репозитории, локальные срезы которых необходимы. При нажатии на название репозитория, появляются настройки этого репозитория (Рис. 151). Необходимо выбрать источник, архитектуру процессора (если их несколько, то стоит выбрать соответствующие).

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

Модуль «Сервер обновлений»

Репозиторий	Источник	Архитектуры	Локальное зеркало	Опубликовано
Стабильная ветка ALT Linux 5.1			<input type="checkbox"/>	<input type="checkbox"/>
Репозиторий обновлений для Альт 8 СП			<input type="checkbox"/>	<input type="checkbox"/>
Десятая платформа	ftp.altlinux.org	x86_64 x86_64-i586	<input checked="" type="checkbox"/> (27 Гб)	<input type="checkbox"/>
Пятая платформа			<input type="checkbox"/>	<input type="checkbox"/>
Шестая платформа			<input type="checkbox"/>	<input type="checkbox"/>
Седьмая платформа			<input type="checkbox"/>	<input type="checkbox"/>
Восьмая платформа			<input type="checkbox"/>	<input type="checkbox"/>
Девятая платформа			<input type="checkbox"/>	<input type="checkbox"/>
Девятая платформа (mirror)			<input type="checkbox"/>	<input type="checkbox"/>
ALT Linux Sisyphus			<input type="checkbox"/>	<input type="checkbox"/>
ALT Linux Sisyphus (mirror)			<input type="checkbox"/>	<input type="checkbox"/>
ALT Linux Sisyphus (i586)			<input type="checkbox"/>	<input type="checkbox"/>
Публичный бранч TEAM 16			<input type="checkbox"/>	<input type="checkbox"/>
Публичный бранч TEAM 17			<input type="checkbox"/>	<input type="checkbox"/>

Свободное место: 161Гб

Предупреждение: зеркалирование потребует наличия большого количества места на диске.

Отключить зеркалирование
 Зеркалировать ежедневно
 Зеркалировать еженедельно в:
 Зеркалировать ежемесячно в день:

Время:

Применить **Сбросить**

Рис. 150

Настройки репозитория

Репозиторий: Десятая платформа

Источник:

Архитектуры: i586
 x86_64
 x86_64-i586

Локальное зеркало репозитория
 Опубликовать как репозиторий для автоматических обновлений

Исключить каталоги и файлы (каждый шаблон в отдельной строке)

```
SRPMS
RPMS.debuginfo
* -debuginfo-*
```

Применить **Сбросить** **Очистить локальное зеркало**

Рис. 151

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.

5.6.5.1 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 репозитория:

```
# 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
```

5.6.5.2 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
```

5.6.6 Локальные учётные записи

Модуль «Локальные учётные записи» (пакет `alterator-users`) из раздела «Пользователи» предназначен для администрирования системных пользователей (Рис. 152).

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 учётные записи» (только GUI) можно задать профиль киоска для пользователя (Рис. 153). Режим «киоск» служит для ограничения прав пользователей в системе.

Веб-интерфейс модуля `alterator-users`

The screenshot shows a web form for creating a new user account. At the top, there is a text input field labeled "Новая учётная запись:" with a "Создать" button next to it. Below this, on the left, is a vertical list of existing users: "user", "test", and "kiosk". The main form area contains several fields: "Комментарий:" (empty), "Домашний каталог:" (set to "/home/user"), and "Интерпретатор команд:" (set to "/bin/bash"). There is a checked checkbox for "Входит в группу администраторов". Under "Назначенные системные роли:", there are checkboxes for "localadmins", "powerusers", and "users" (which is checked). A checkbox for "Создать автоматически" is unchecked. The "Пароль:" field has two input boxes for password entry, with instructions "(введите фразу)" and "(повторите фразу)". At the bottom, there are "Применить" and "Удалить пользователя" buttons. On the right side, there is a list of groups that the user belongs to, including "audio", "camera", "cdrom", "cdwriter", "floppy", "fuse", "mytest2", "proc", "radio", "sambashare", "scanner", "user", "users", "uucp", "vboxadd", "vboxsf", "vboxusers", "video", "vmusers", and "wheel".

Рис. 152

Настройка режима «киоск» для пользователя *kiosk*

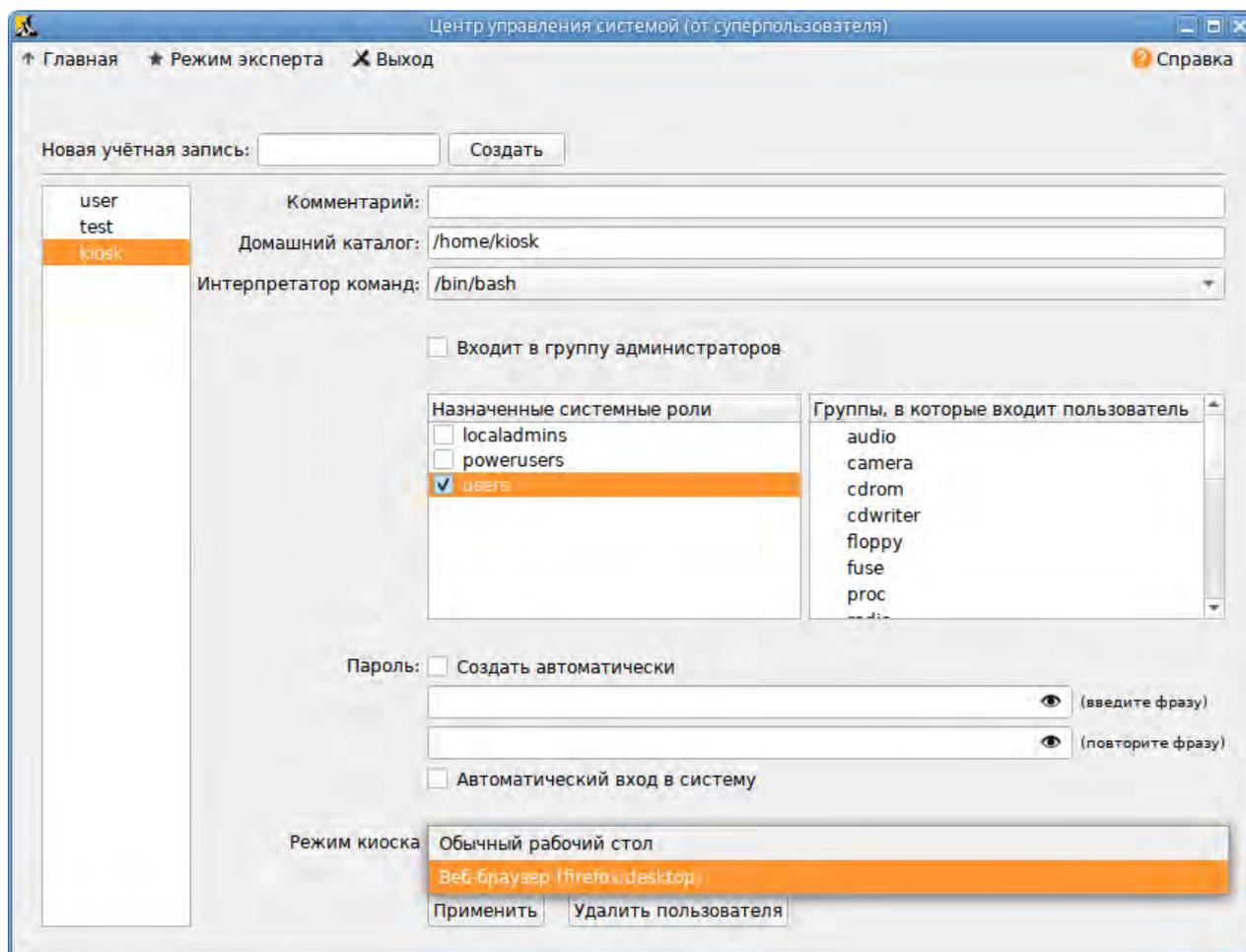


Рис. 153

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/webkiosk.desktop` со следующим содержимым:

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

```
Icon=start
```

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 «WEB-kiosk (webkiosk.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`.

5.6.7 Администратор системы

В модуле «Администратор системы» (пакет `alterator-root`) из раздела «Пользователи» можно изменить пароль суперпользователя (`root`), заданный при начальной настройке системы (Рис. 154).

Модуль «Администратор системы»

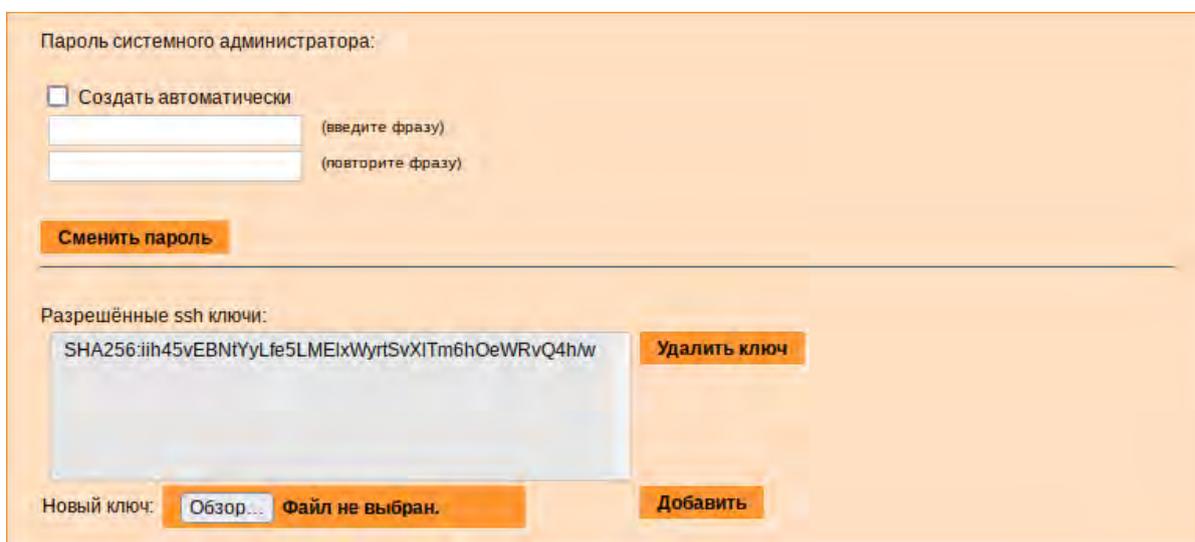


Рис. 154

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

5.6.8 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. 155).

Модуль «Дата и время»

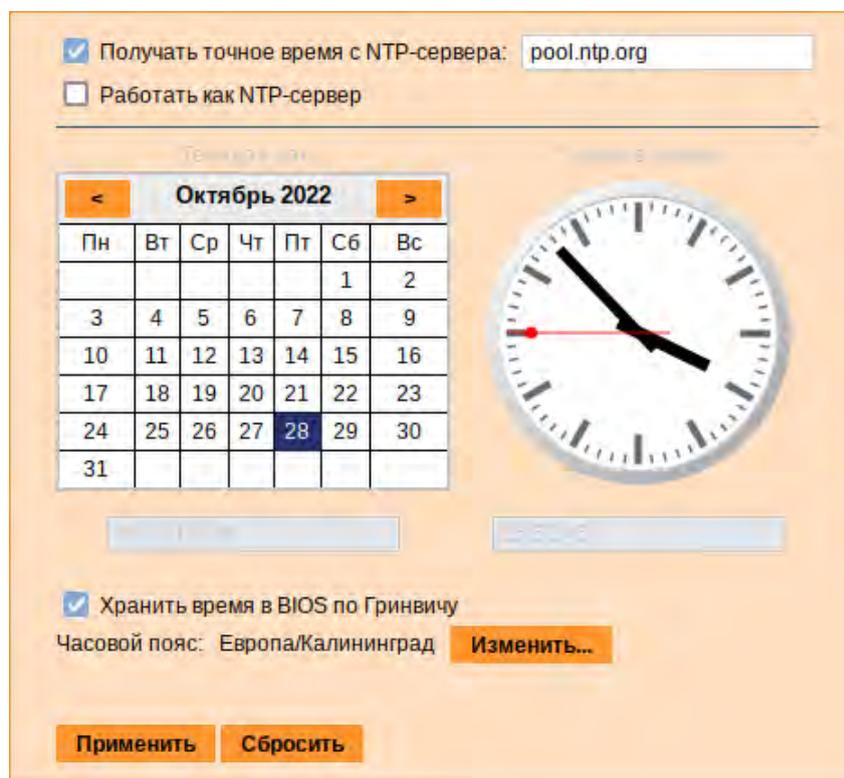


Рис. 155

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».

5.6.9 Настройка прокси-сервера

Модуль «Настройки проху» (пакет alterator-sysconfig) из раздела «Система» позволяет настроить параметры прокси-сервера, используемого для выхода в Интернет (Рис. 155).

Модуль «Настройки проху»

Прокси-сервер: 10.0.66.55 Порт: 3128

Учётная запись:

Пароль:

Не использовать прокси для:

Применить Сбросить

Рис. 156

Данный модуль позволяет настроить:

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

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

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

5.6.10 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. 157).

Модуль «Использование диска»

Файловая система: / Текущее использование диска: 0 КБ

Включено:

Пользователь: user

Мягкое ограничение: КБ

Жесткое ограничение: КБ

Количество файлов: 0

Мягкое ограничение:

Жесткое ограничение:

Применить Сбросить

Рис. 157

Для управления квотами файловая система должна быть подключена с параметрами usquota, grquota. Для этого следует выбрать нужный раздел в списке «Файловая система» и установить отметку в поле «Включено» (Рис. 158).

Модуль «Использование диска»

Файловая система: /home ▾ Текущее использование диска: 498696 КБ

Включено: Мягкое ограничение: 0 КБ

Пользователь: Жесткое ограничение: 0 КБ

Количество файлов: 3650

Мягкое ограничение: 100

Жесткое ограничение: 100

Рис. 158

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.

5.6.11 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. 159). 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. 159

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. 160).

Модуль «Выключение компьютера». Настройка оповещений

Рис. 160

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

```
Tue Dec 7 16:55:31 EET 2021: The host-15.test.alt is about to start.
```

При выключении:

```
Tue Dec 7 16:55:02 EET 2021: The host-15.test.alt is about to
shutdown.
```

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

5.7 Прочие возможности ЦУС

Возможности ЦУС ОС «Иридиум» 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
```

5.8 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. 161).

Ссылка «Параметры доступа к модулю»

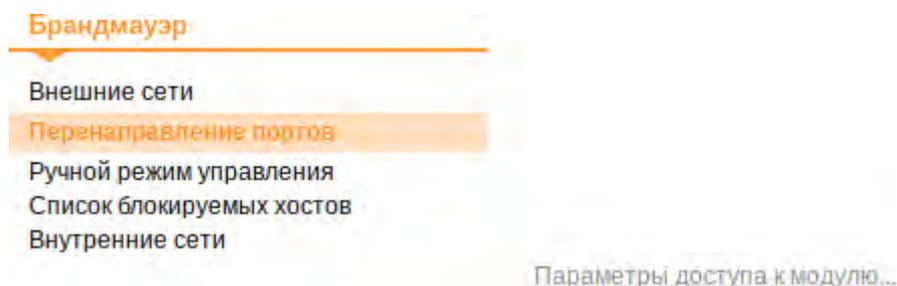


Рис. 161

В открывшемся окне, в списке «Новый пользователь» необходимо выбрать пользователя, который получит доступ к данному модулю, и нажать кнопку «Добавить» (Рис. 162). Для

сохранения настроек необходимо перезапустить HTTP-сервер, для этого достаточно нажать кнопку «Перезапустить HTTP-сервер».

Параметры доступа к модулю

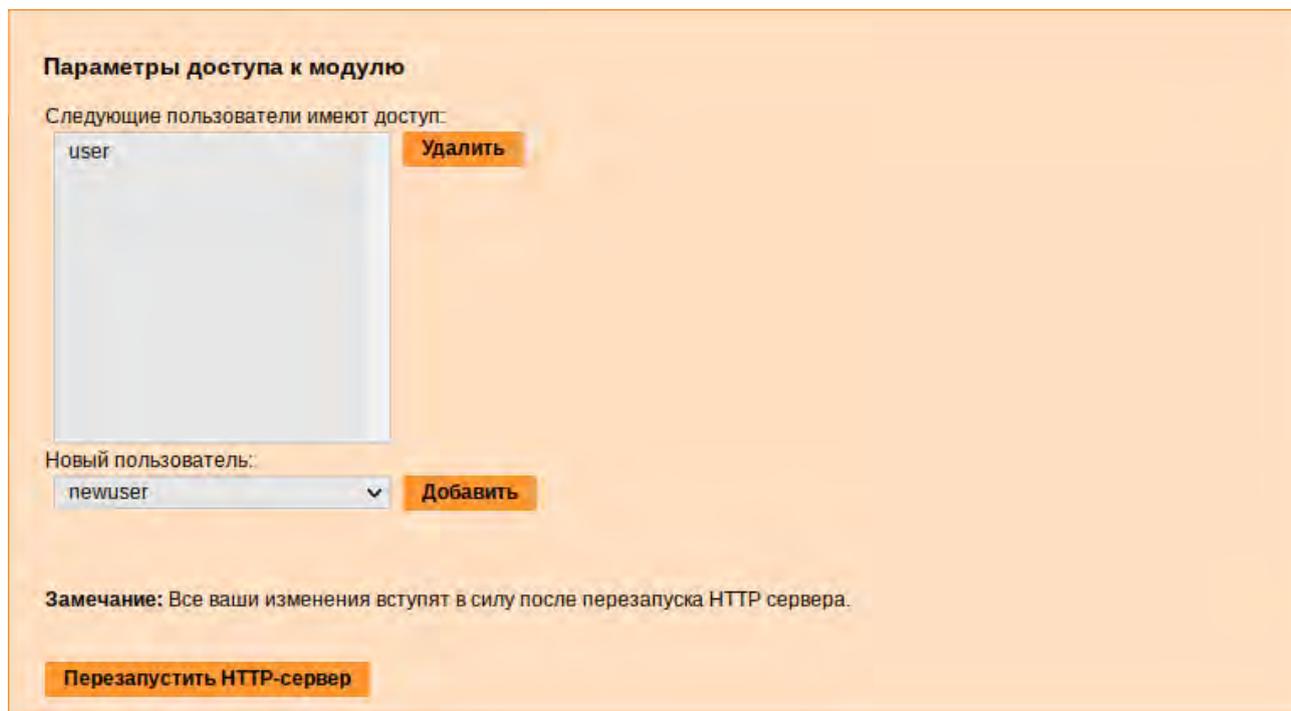


Рис. 162

Для удаления доступа пользователя к определенному модулю, администратору, в окне этого модуля необходимо нажать ссылку «Параметры доступа к модулю», в открывшемся окне в списке пользователей которым разрешен доступ, должен выбрать пользователя, нажать кнопку «Удалить» (Рис. 162) 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: Jun 3 16:13:22 2021 GMT

Not After : Jun 3 16:13:22 2022 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 изменения 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 хэширование паролей пользователей по алгоритму ГОСТ Р 34.11-2012» и нажать кнопку «Применить» (Рис. 163).

Задание хешей паролей в соответствии с ГОСТ Р 34.11-2012

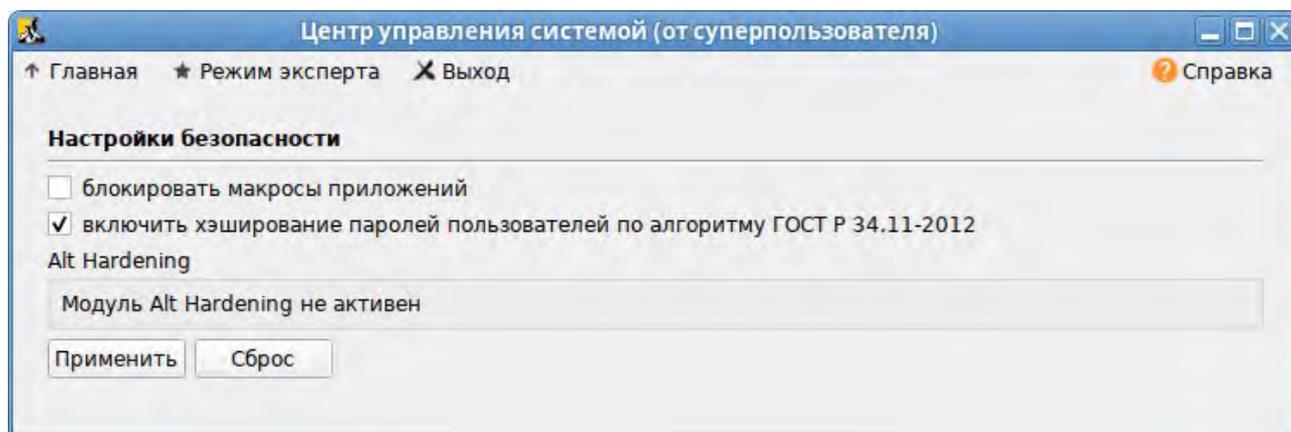


Рис. 163

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
```

Установить пароль пользователю:

```
# passwd user
```

Проверка:

```
# passwd -S user
```

Password set, gost-yescrypt encryption.

Список возможных хэш-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 хэш-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 «Иридиум» можно использовать программу ALT CSP КриптоПро (Подпись и проверка ЭЦП ГОСТ). Возможности ALT CSP КриптоПро:

- создание электронной подписи (отсоединенной и присоединенной);

- 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. Также у пользователя должен существовать контейнер с сертификатом (в локальном считывателе или на токене).

Запустить ALT CSP КриптоПро можно:

- из меню рабочей среды: «Меню МАТЕ» → «Системные» → «ALT CSP КриптоПро»;
- из контекстного меню файла в файловом менеджере Caja: «Caja-Actions actions» → «Подписать документ» (Рис. 164). 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

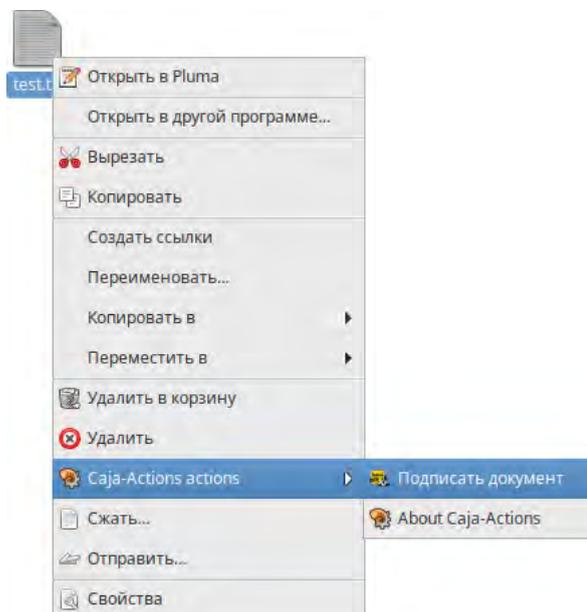


Рис. 164

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. 165), в разделе «Документ» нажать кнопку «Выбрать» и выбрать электронный документ. Нажав кнопку «Просмотреть», можно просмотреть содержимое электронного документа.

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 (по умолчанию), sig или .sign.

Выбор документа для создания электронной подписи

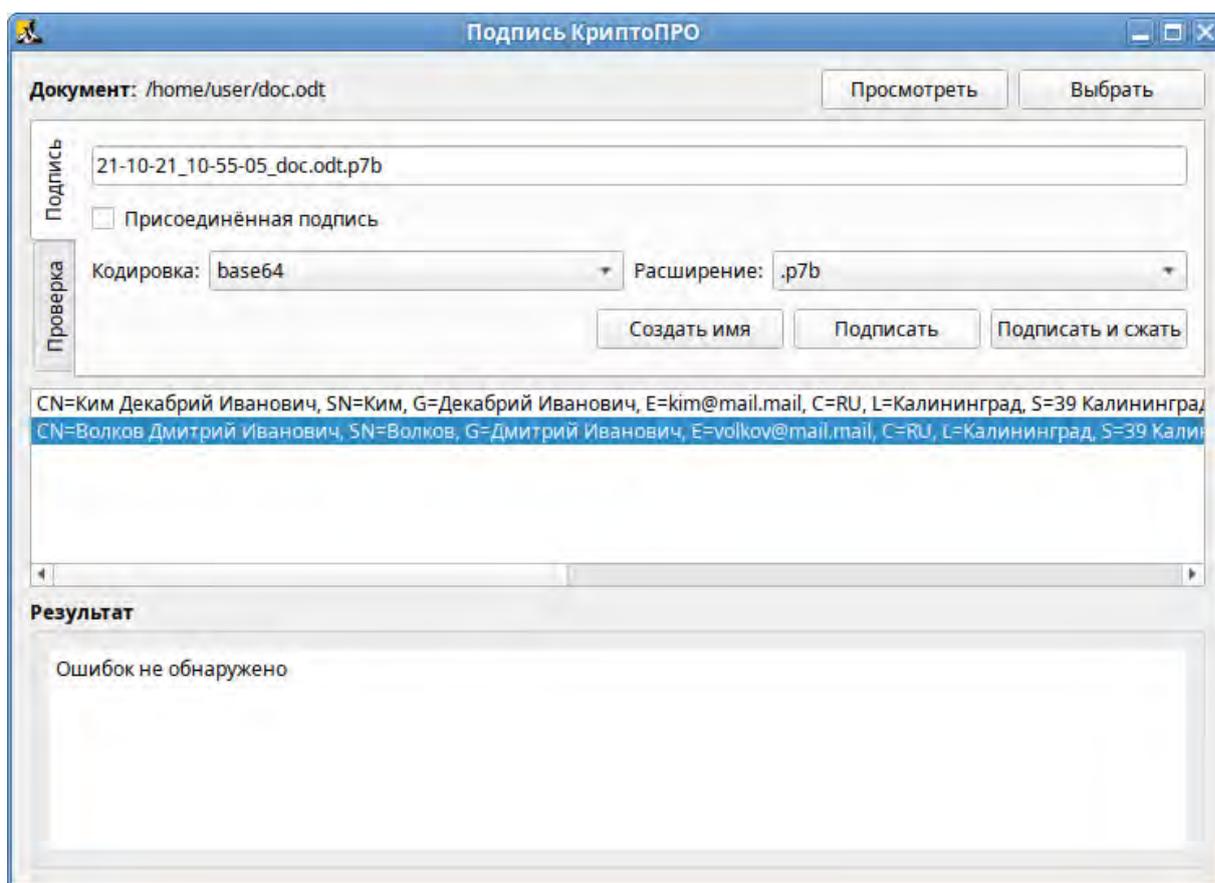


Рис. 165

Название файла цифровой подписи по умолчанию будет сформировано путем добавления к имени файла информации о текущей дате и времени: гг-мм-дд_чч-мм-сс_ИМЯ_ФАЙЛА>.p7b. 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 создания 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. 166). В том же каталоге, в котором хранился исходный документ, появится файл, содержащий как саму электронную подпись, так и исходный документ.

Создание присоединенной подписи

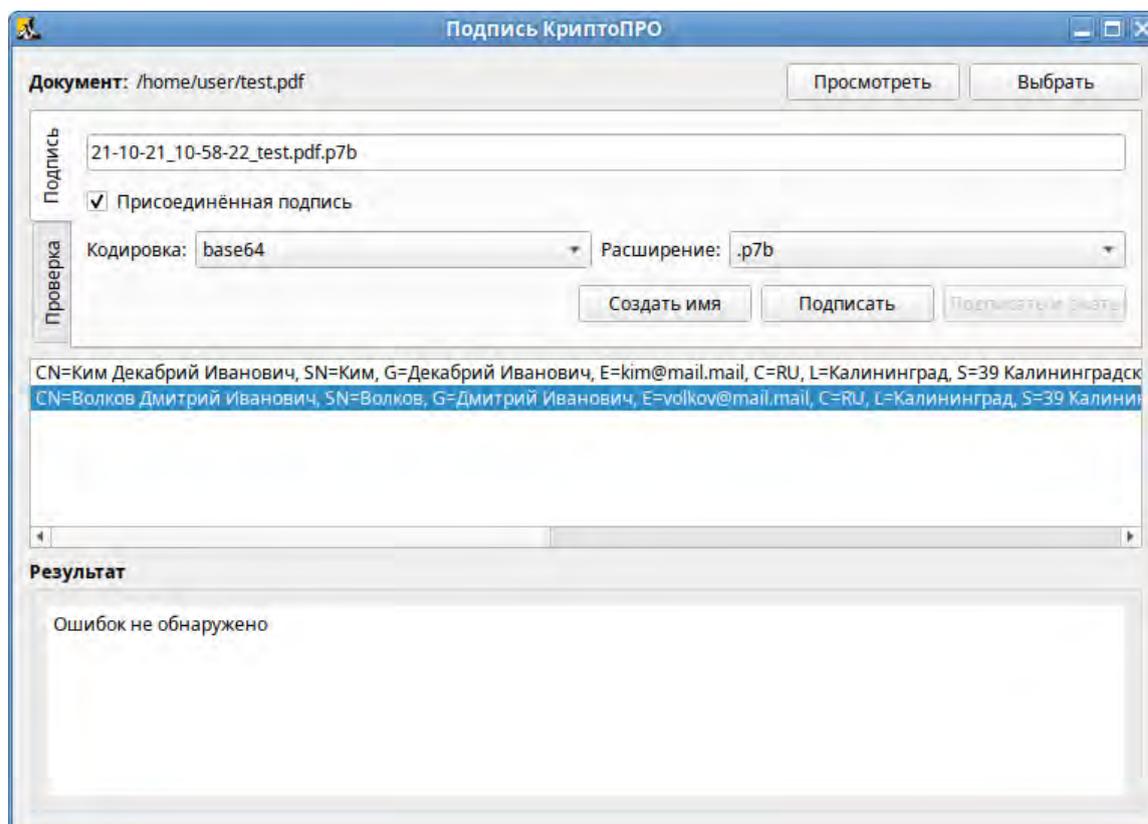


Рис. 166

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

```
$ cryptcp -verify 21-10-21_10-58-22_test.pdf.p7b test_new.pdf
```

В файл test_new.pdf будут извлечены данные.

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. 167).

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.

Проверка отсоединенной электронной подписи

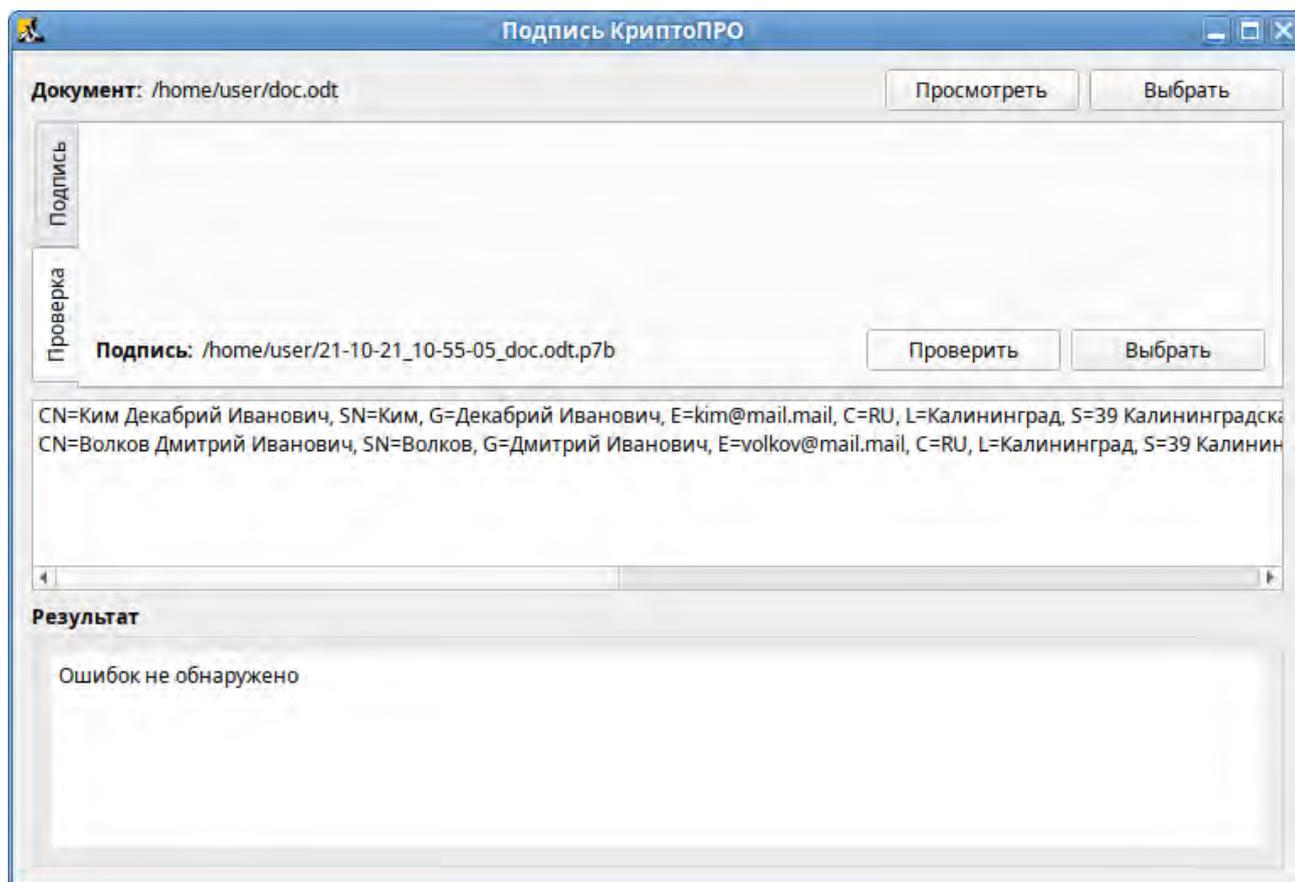
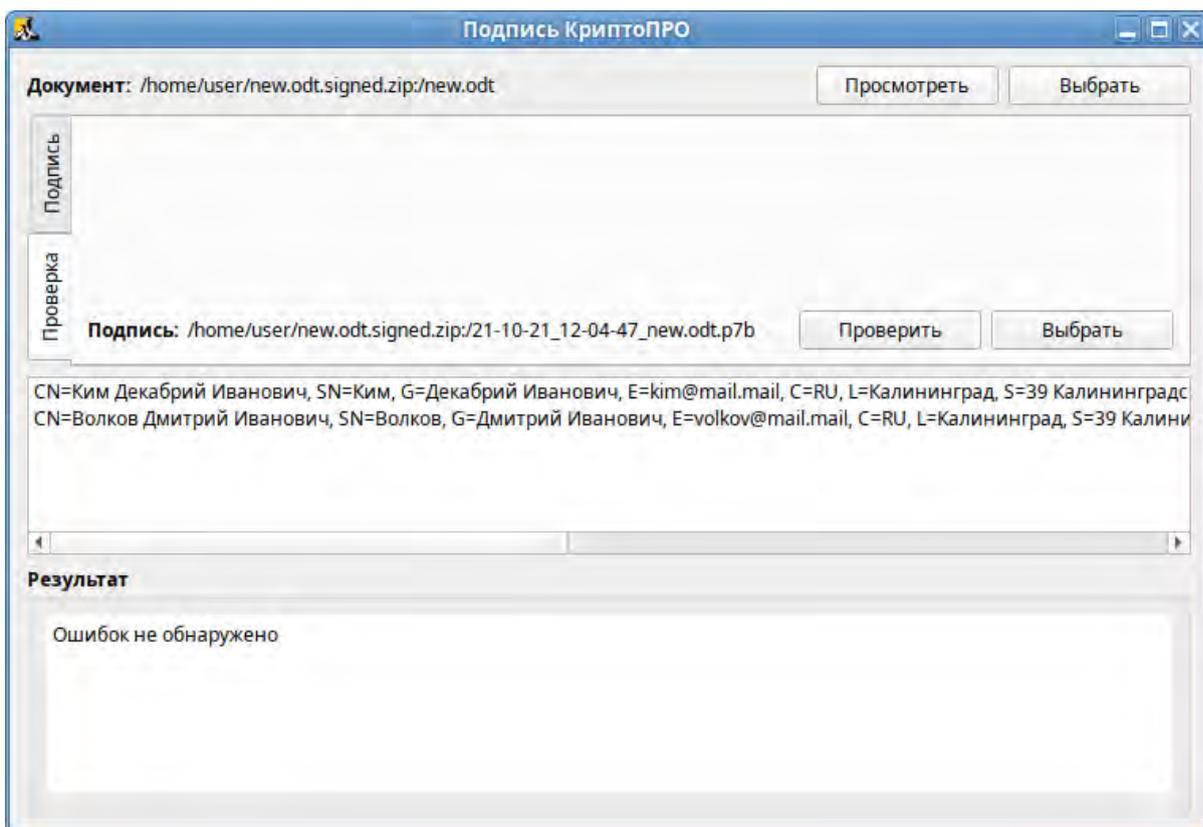
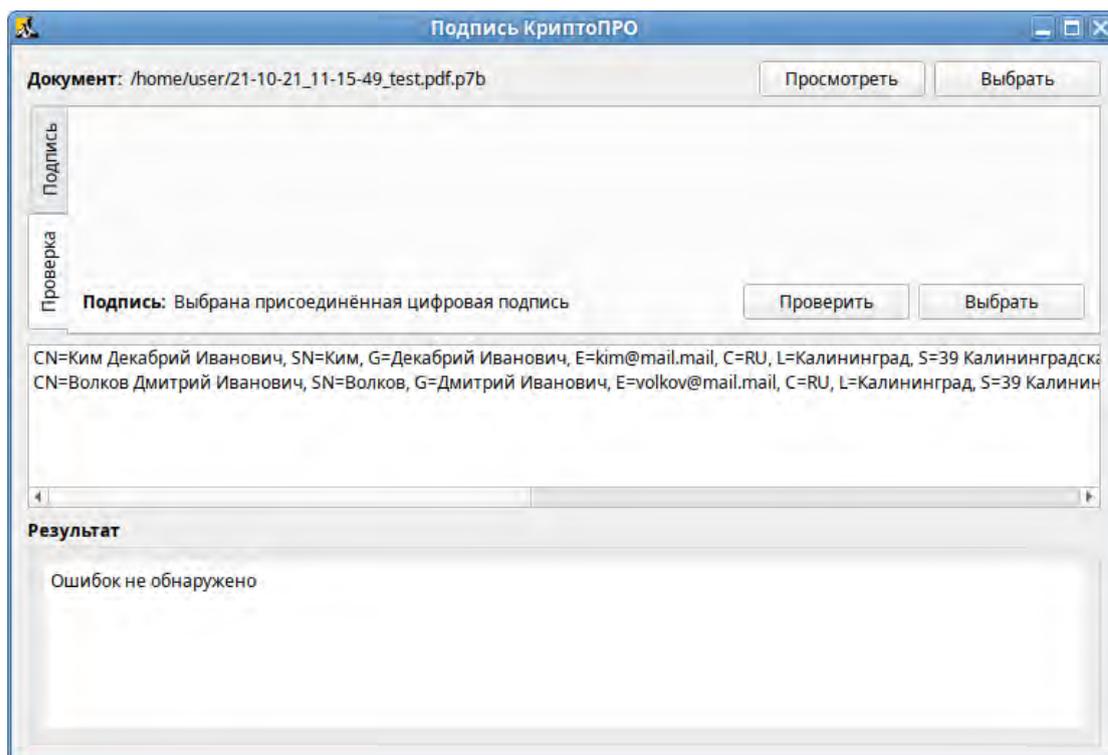


Рис. 167

Для проверки электронной подписи в контейнере достаточно выбрать zip-архив (документ и подпись будут выбраны автоматически) и нажать кнопку «Проверить» (Рис. 168).

Проверка электронной подписи в zip-архиве*Рис. 168*

Для проверки присоединённой электронной подписи необходимо выбрать подписанный электронный документ и нажать кнопку «Проверить» (Рис. 169).

Проверка присоединенной электронной подписи*Рис. 169*

6.4 Управление зашифрованными 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 зашифрованными 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` – зашифрованный 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 произойдет 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 затерт 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 Создание ssh-туннелей, использующих контроль целостности заголовков IP-пакетов в соответствии с ГОСТ Р 34.12-2015

6.5.1 Настройка сервера ssh

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

Примечание. Для установки пакетов gostcrypto, в список репозитория должен быть добавлен репозиторий gostcrypto. Сделать это можно в программе управления пакетами Synaptic, написав для дистрибутива «p10/branch/x86_64» в поле «Раздел(ы)» значение gostcrypto (Рис. 170).

Добавление репозитория gostcrypto в Synaptic

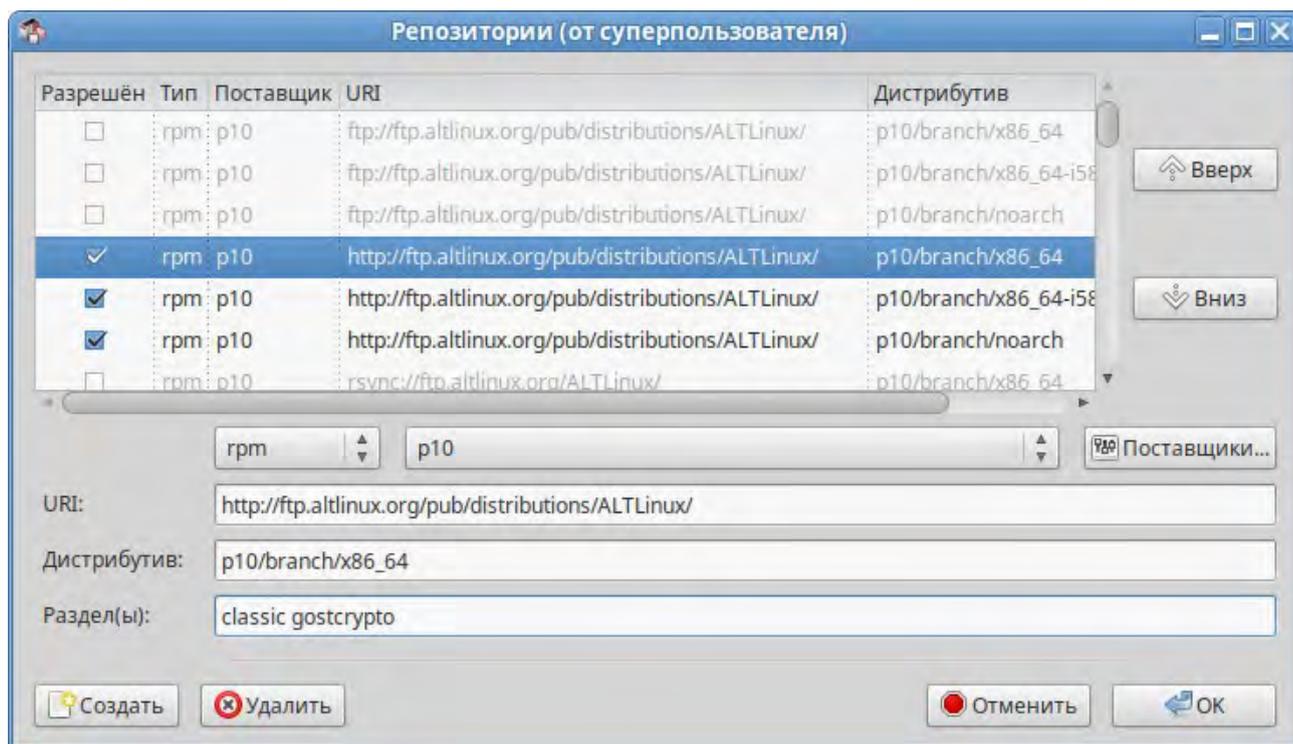


Рис. 170

После изменения списка репозитория, необходимо получить сведения о находящихся в них пакетах.

Установить пакеты:

```
# 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 1409кВ архивов.

После распаковки потребуется дополнительно 421кВ дискового
пространства.

Вы делаете нечто потенциально опасное!

Введите фразу 'Yes, do as I say!' чтобы продолжить.

Yes, do as I say!

Список поддерживаемых алгоритмов шифрования трафика:

```
$ 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

```

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:

```
# service sshd restart
```

6.5.2 Подключение к серверу ssh

Зайти на сервер по ssh:

```
$ 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 тоннель (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
```

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

Для возможности использования ГОСТ алгоритмов шифрования и хэширования 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. 170).

После изменения списка репозиториев, необходимо получить сведения о находящихся в них пакетах.

6.6.1 Настройка в ЦУС

Выполнить настройку сервера OpenVPN-сервера (см. «Соединение удалённых офисов (OpenVPN-сервер)»).

Выбрать алгоритмы шифрования и алгоритм хэширования. 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. 171).

На стороне клиента, необходимо указать алгоритмы шифрования, такие же, как и на стороне сервера (Рис. 172).

Включить службу OpenVPN

Тип: **Маршрутизируемое (TUN)** ▾

Сети сервера: **Удалить**

Новая сеть:

Маска сети: ▾

Добавить

VPN сеть:

Маска сети: ▾

Алгоритм шифрования: ▾

Алгоритм шифрования TLS: ▾

Алгоритм хэширования: ▾

Отключить согласование алгоритмов шифрования (NCP)

Порт:

Сжатие LZO

Использовать соединение TCP

Сертификат и ключ SSL...

Положить сертификат УЦ: **Положить**

 Сертификат УЦ успешно загружен

Сети клиентов...

Применить **Сбросить**

Рис. 171

Проверка подключения на стороне сервера:

```
# journalctl -f | grep openvpn
дек 07 20:57:08 dc.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 dc.test.alt openvpn[262676]: TLS: Initial packet from
[AF_INET]192.168.0.145:1194, sid=393e755a d49a39a8
дек 07 20:57:08 dc.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 dc.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 dc.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 dc.test.alt openvpn[254812]: 192.168.0.145:55939 Incoming Data Chan-
nel: Using 128 bit message hash 'grasshopper-mac' for MAC authentication
Настройка OpenVPN-сервера
```

Создание нового OpenVPN-соединения

Новое соединение:

Сетевой туннель (TUN)
 Виртуальное Ethernet устройство (TAP)

Создать соединение

tun1

Состояние: выключено не менять ▾

Сервер:

Порт:

Ключ: openvpn ▾

Управление ключами...

Запускать при загрузке
 Маршрут по умолчанию через VPN
 Сжатие LZO
 Использовать соединение TCP

Алгоритм шифрования: grasshopper-cbc ▾

Алгоритм шифрования TLS: GOST2012-GOST8912-GOST8912 ▾

Алгоритм хэширования: grasshopper-mac ▾

Отключить согласование алгоритмов шифрования (NCP)

Применить **Сбросить** **Удалить соединение**

Положить сертификат УЦ: **Положить**

 Сертификат УЦ успешно загружен

Рис. 172

6.6.2 Настройка в командной строке

6.6.2.1 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`.

6.6.2.2 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
```

6.6.2.3 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 «Соединения VPN» → «Добавить VPN-соединение» (Рис. 173).

Создание нового OpenVPN-соединения

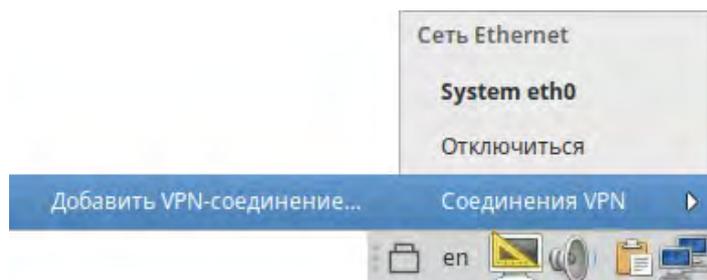


Рис. 173

2. В списке выбора типа соединения выбрать пункт «OpenVPN» и нажать кнопку «Создать» (Рис. 174).

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

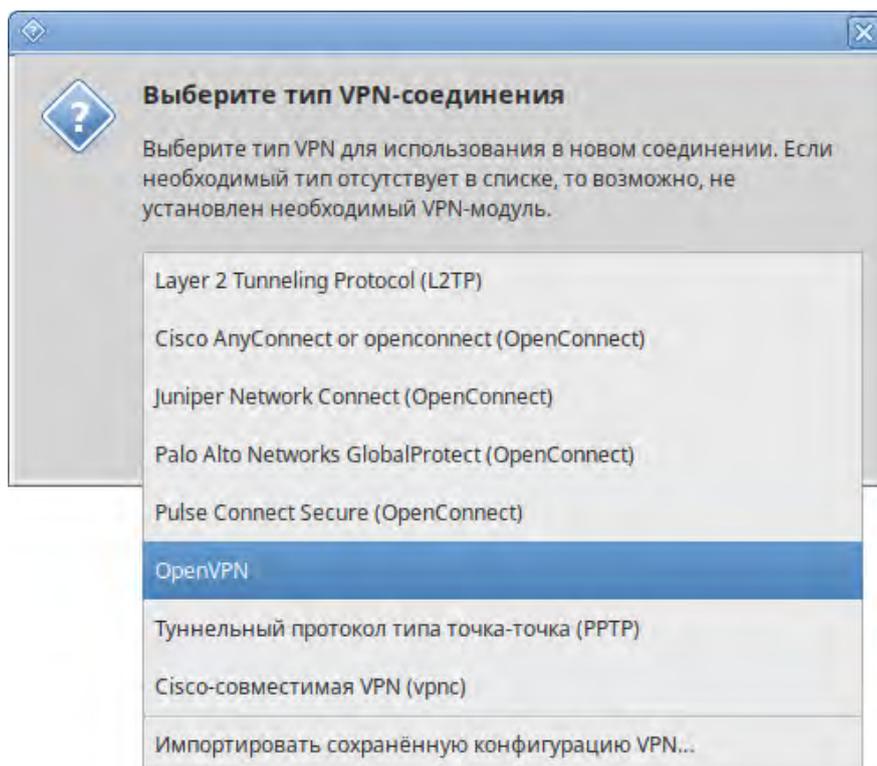


Рис. 174

3. В открывшемся окне указать IP-адрес OpenVPN сервера, сертификат УЦ, приватный ключ и сертификат пользователя (Рис. 175).

Параметры VPN-соединения

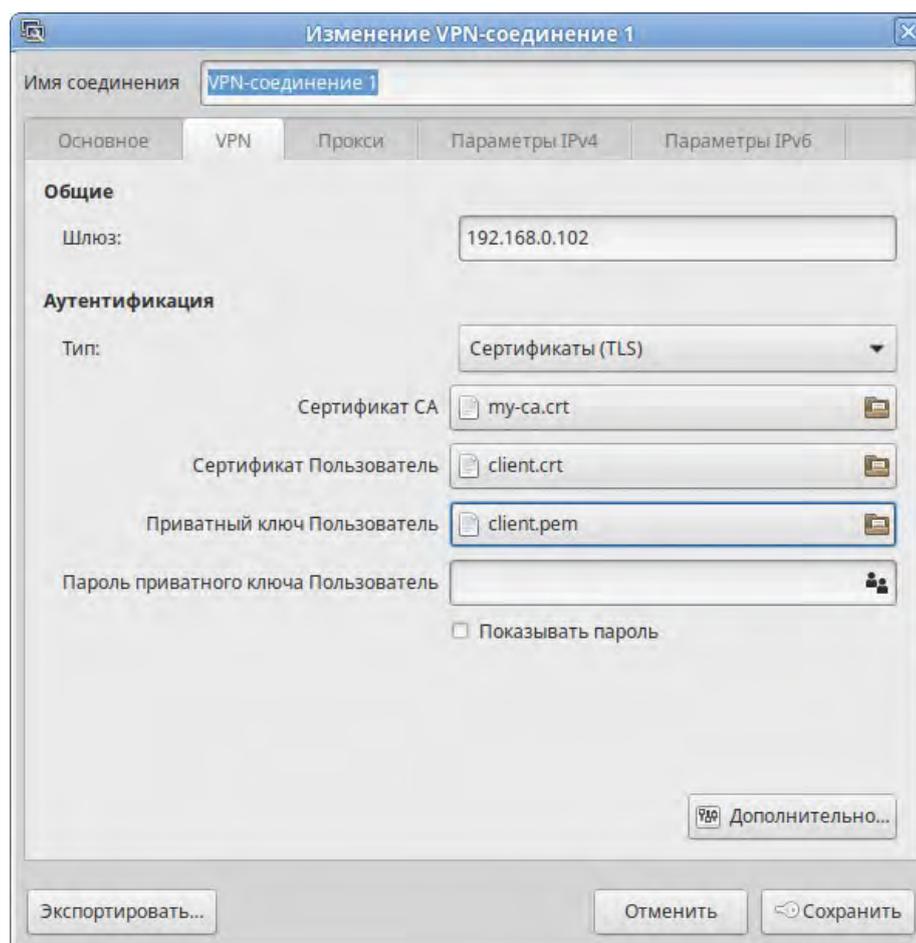


Рис. 175

4. Нажать кнопку «Дополнительно» чтобы указать параметры подключения. Настройки соединения находятся на разных вкладках, например на вкладке «Защита» можно указать алгоритм шифрования (Рис. 176).

Дополнительные параметры OpenVPN

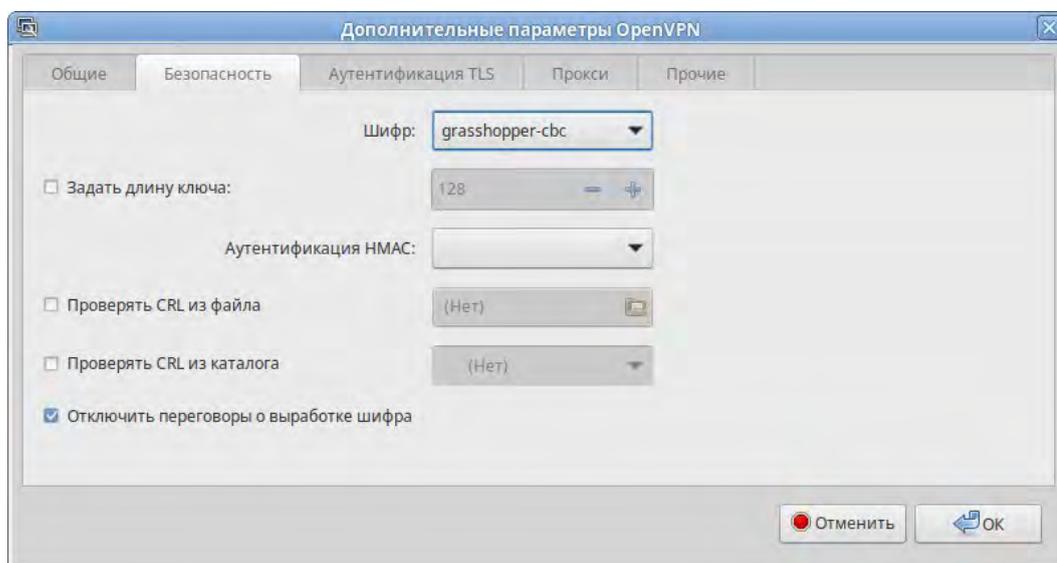


Рис. 176

5. Сохранить сделанные изменения, нажав кнопку «ОК» и затем «Сохранить».
6. Выполнить подключение (Рис. 177).

Создание VPN-соединения

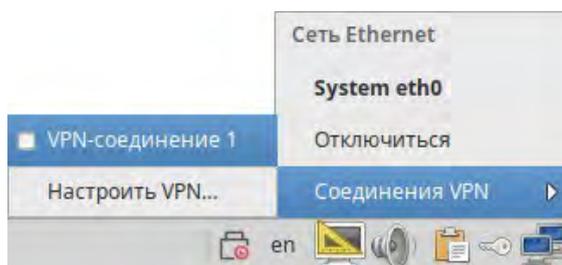


Рис. 177

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 указать 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
```

6.7 Поддержка файловых систем

Файловая система представляет из себя набор правил, определяющих то, как хранятся и извлекаются документы, хранящиеся на устройстве.

Проверка поддержки файловых систем `ext2`, `ext3`, `ext4`, `iso9660`, `fat16`, `fat32`, `ntfs`:

1. Создать раздел объемом менее 4 Гбайт на flash-накопителе (например, `/dev/vdc1`).
2. Для создания iso файла установить пакет `genisoimage`:

```
# apt-get install genisoimage
```
3. Создать 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 системой:
cat /mnt/filesystem/test.fs

6. Для проверки поддержки файловой системы iso9660 смонтировать созданный iso файл в каталог /mnt/filesystem/ (файл образа диска будет примонтирован в режиме «только для чтения»):

```
# mount -o loop,ro /root/cd.iso /mnt/filesystem/
```

6.8 Поддержка сетевых протоколов

6.8.1 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.

6.8.1.1 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.

6.8.1.1.1 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.
```

6.8.1.1.2 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
```

6.8.1.1.3 Создание ресурсов общего доступа от имени обычного пользователя

Создание ресурсов общего доступа от имени обычного пользователя рассмотрено в разделе «Создание ресурсов общего доступа».

6.8.1.2 Настройка клиента

6.8.1.2.1 Подключение по протоколу SMB в графической среде

Для создания подключения по протоколу SMB в графической среде МАТЕ можно, запустить файловый менеджер, указать в адресной строке протокол и адрес сервера (Рис. 178). Нажать клавишу <Enter>. Будут показаны ресурсы с общим доступом (Рис. 179). Для доступа к папке, необходимо указать имя пользователя, пароль и нажать кнопку «Подключиться» (Рис. 180).

Создание подключения по протоколу SMB

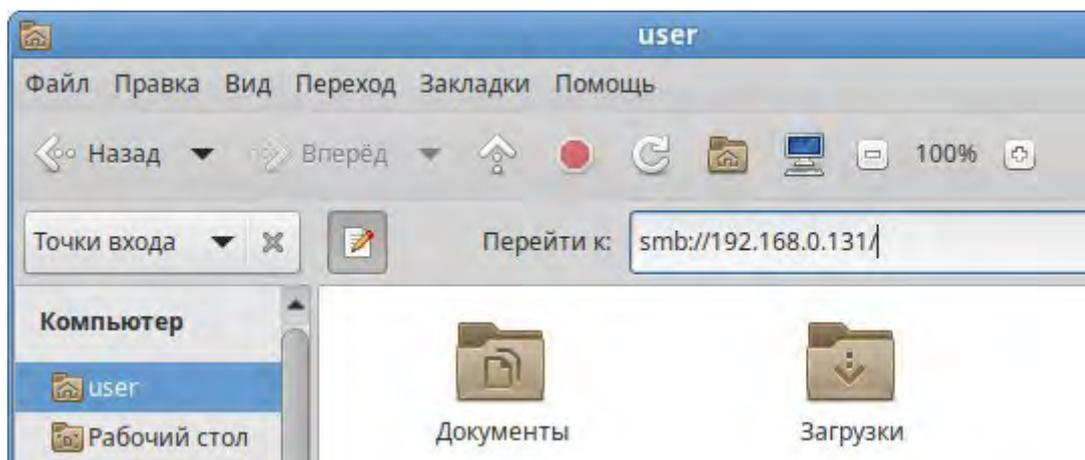


Рис. 178

Создание подключения по протоколу SMB

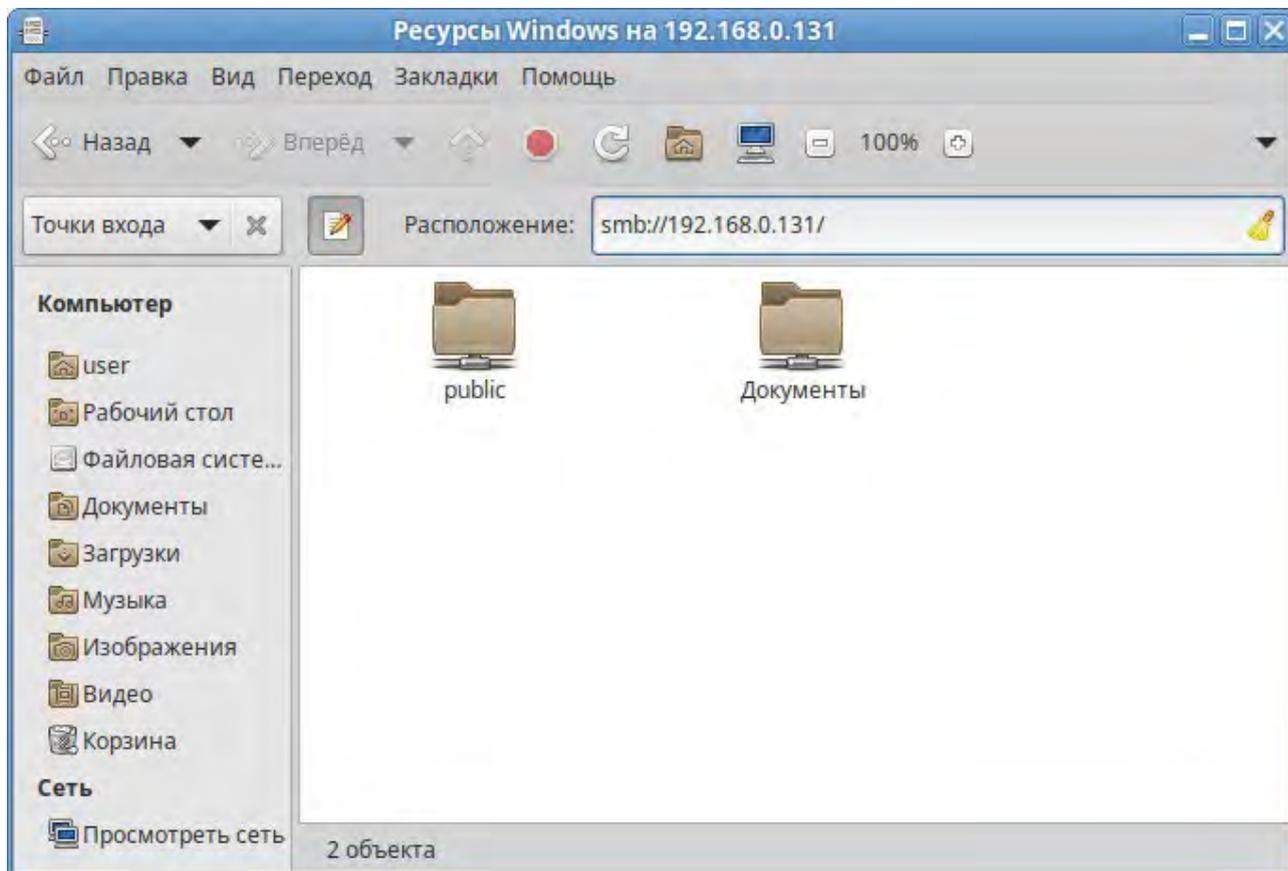


Рис. 179

Создание подключения по протоколу SMB

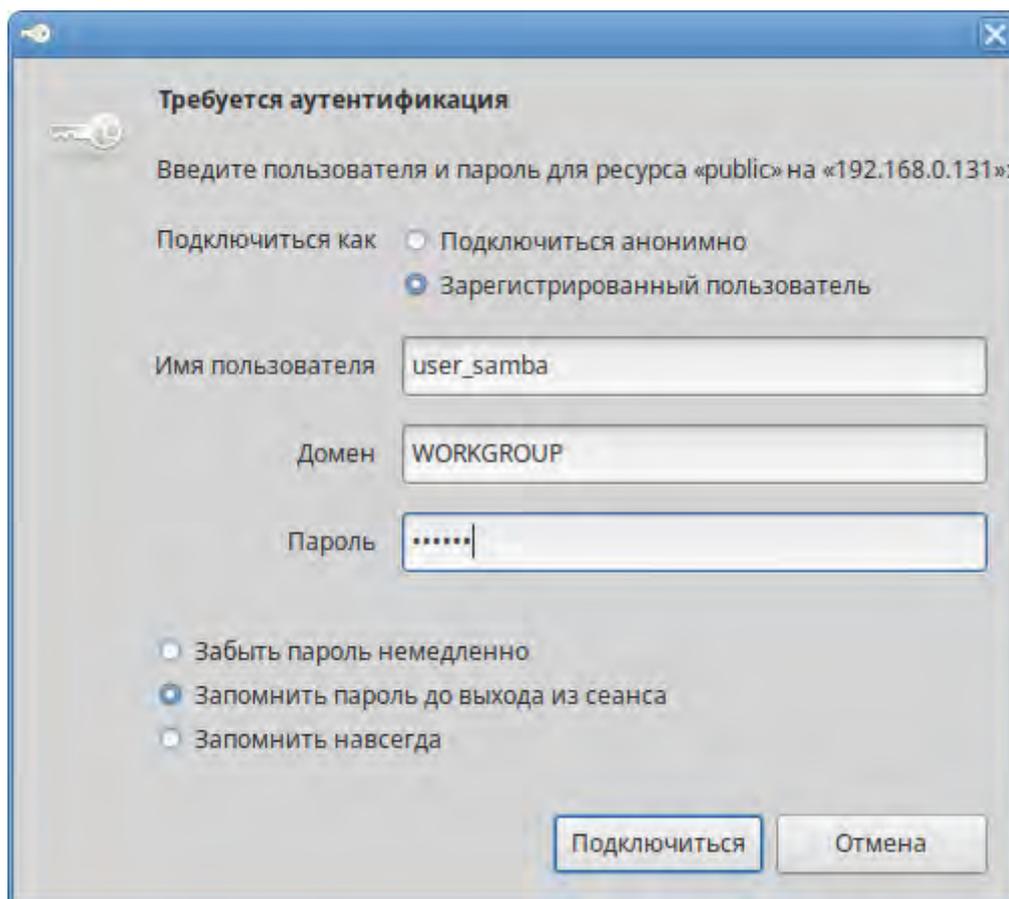


Рис. 180

6.8.1.2.2 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 -User_samba
```

```
Enter TEST\user_samba's password:
```

Sharename	Type	Comment
-----	----	-----
public	Disk	Public
IPC\$	IPC	IPC Service (Samba Server Version 4.16.6)
user_samba	Disk	Home Directories
Cups-PDF	Printer	Cups-PDF
Документы	Disk	

```
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/smbacreds`, надо установить так, чтобы файл был доступен на чтение и запись только пользователю-владельцу файла:

```
# chmod 600 /etc/samba/smbacreds
```

и принадлежать root:

```
# chown root: /etc/samba/smbacreds
```

Для монтирования ресурса Samba в `/etc/fstab` необходимо прописать, строку вида:

```
//СЕРВЕР/ИМЯ_РЕСУРСА /mnt/точка_монтирования cifs
credentials=/путь/к/полномочиям/smbacreds 0 0
```

Например:

```
//192.168.0.131/public /mnt/server_public cifs users,_netdev,x-
systemd.automount,credentials=/etc/samba/smbacreds 0 0
```

6.8.2 NFS

6.8.2.1 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):

```
/myshare dir ipaddr1(rw)
```

Например, разрешить монтировать `/home` на сервере:

```
# vim /etc/exports
```

```
/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
```

6.8.2.2 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 /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.

6.8.3 FTP

6.8.3.1 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
```

6.8.3.2 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. 181) и нажать клавишу <Enter>. В появившемся окне указать имя пользователя, пароль и нажать кнопку «Подключиться» (Рис. 182).

Создание подключения по протоколу FTP

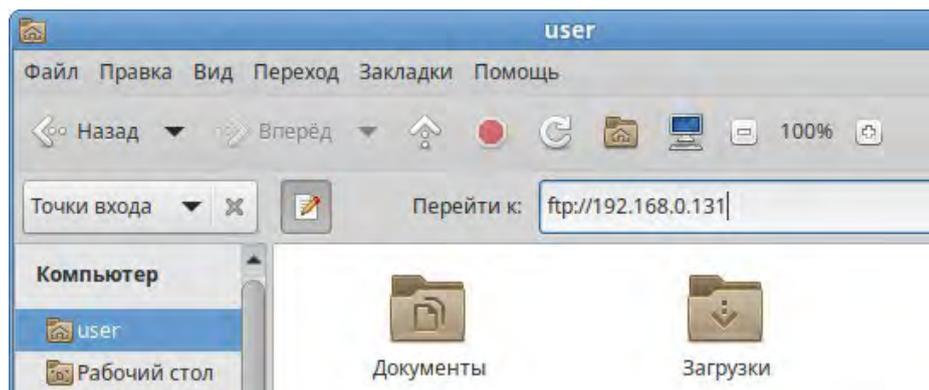


Рис. 181

Создание подключения по протоколу FTP

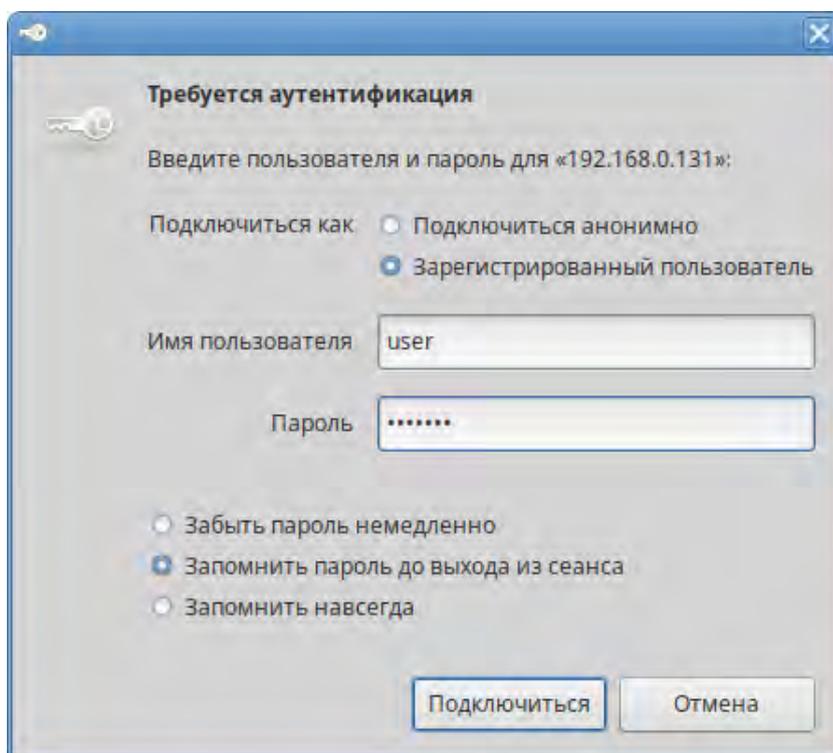


Рис. 182

Должен отобразиться список файлов каталога `/var/ftp/`, расположенного на сервере FTP (Рис. 183).

Файл на FTP сервере

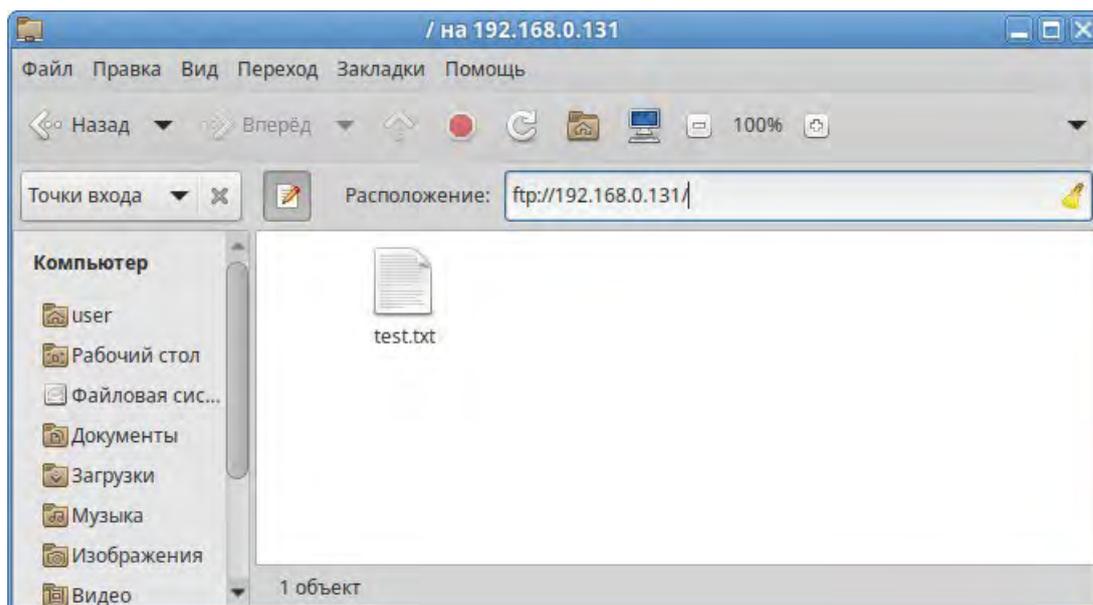


Рис. 183

6.8.4 NTP

6.8.4.1 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.
- `chronus` – 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. 184).
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»

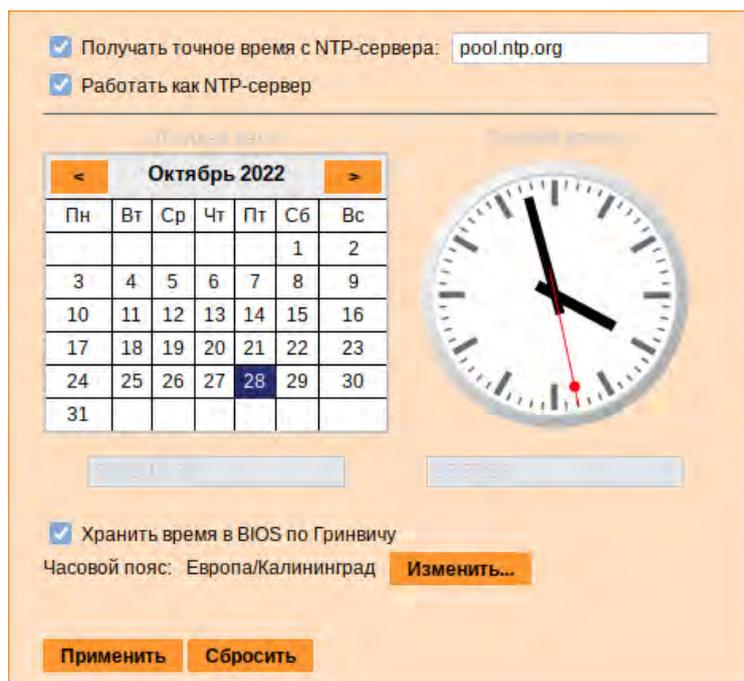


Рис. 184

6.8.4.2 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. 185).

Настройка модуля «Дата и время» на рабочей станции

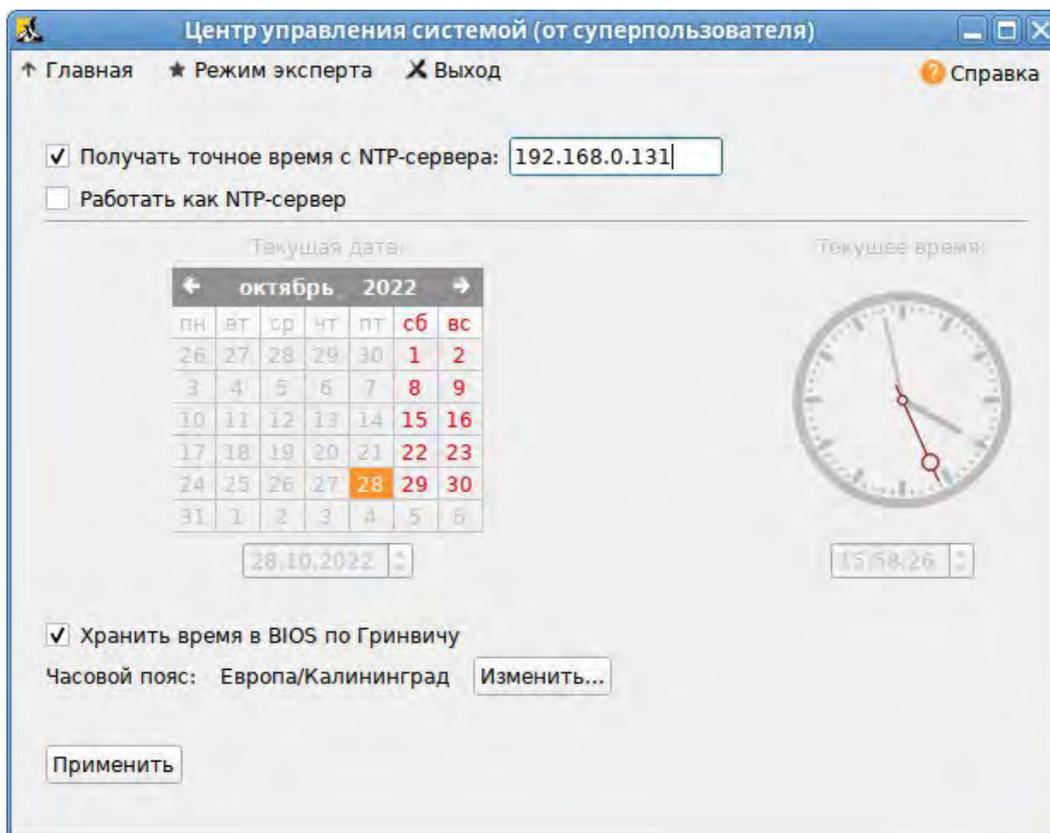


Рис. 185

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
```

6.8.5 HTTP(S)

6.8.5.1 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
```

6.8.5.2 Настройка рабочей станции

Запустить браузер, перейти по адресу `http://<IP-адрес>` (Рис. 186).

Обращение к серверу и получение данных по протоколу `http`

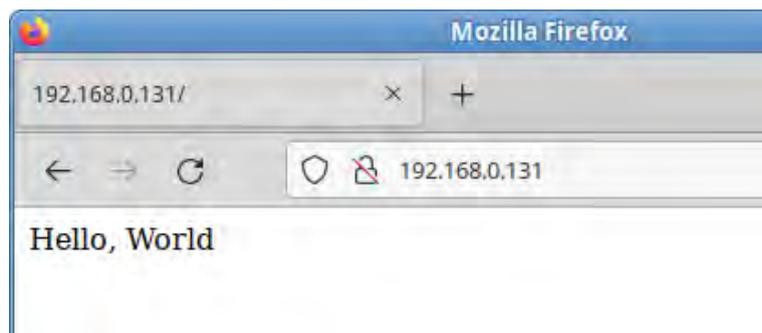


Рис. 186

Также можно выполнить команду:

```
$ curl http://192.168.0.131
Hello, World
```

Происходит обращение к серверу и получение данных по протоколу http.

6.9 Виртуальная (экранная) клавиатура

Onboard – гибкая в настройках виртуальная (экранная) клавиатура.

Виртуальная клавиатура полезна тогда, когда по каким либо причинам, нет возможности использовать обычную клавиатуру. Так же виртуальная клавиатура может оказаться удобной пользователям сенсорных экранов (touchscreen).

Примечание. Должен быть установлен пакет onboard:

```
# apt-get install onboard
```

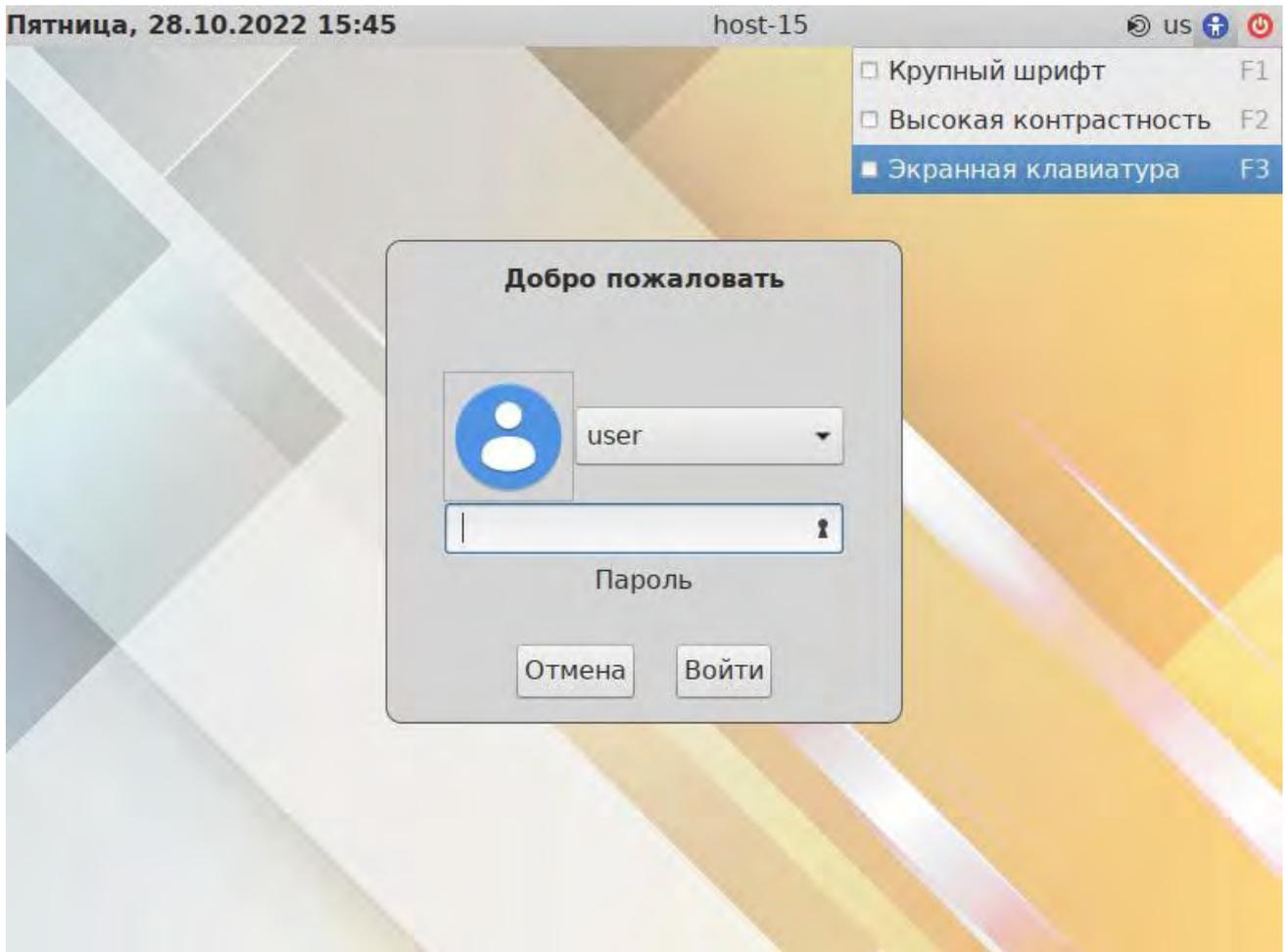
6.9.1 Клавиатура onboard при входе в систему

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. 187).

На экране появится виртуальная клавиатура (Рис. 188), её можно использовать для ввода имени пользователя и пароля.

Страница входа в систему*Рис. 187***6.9.2 Клавиатура onboard при разблокировке экрана**

Для того чтобы клавиатура работала при разблокировке экрана, следует выставить следующие параметры dconf:

```
org.mate.screensaver.embedded-keyboard-enabled=true
```

```
org.mate.screensaver.embedded-keyboard-command="onboard --xid"
```

Установить параметры dconf для конкретного пользователя можно, выполнив команды (под этим пользователем):

```
$ gsettings set org.mate.screensaver embedded-keyboard-enabled true
```

```
$ gsettings set org.mate.screensaver embedded-keyboard-command "onboard --xid"
```

Виртуальная клавиатура при входе в систему

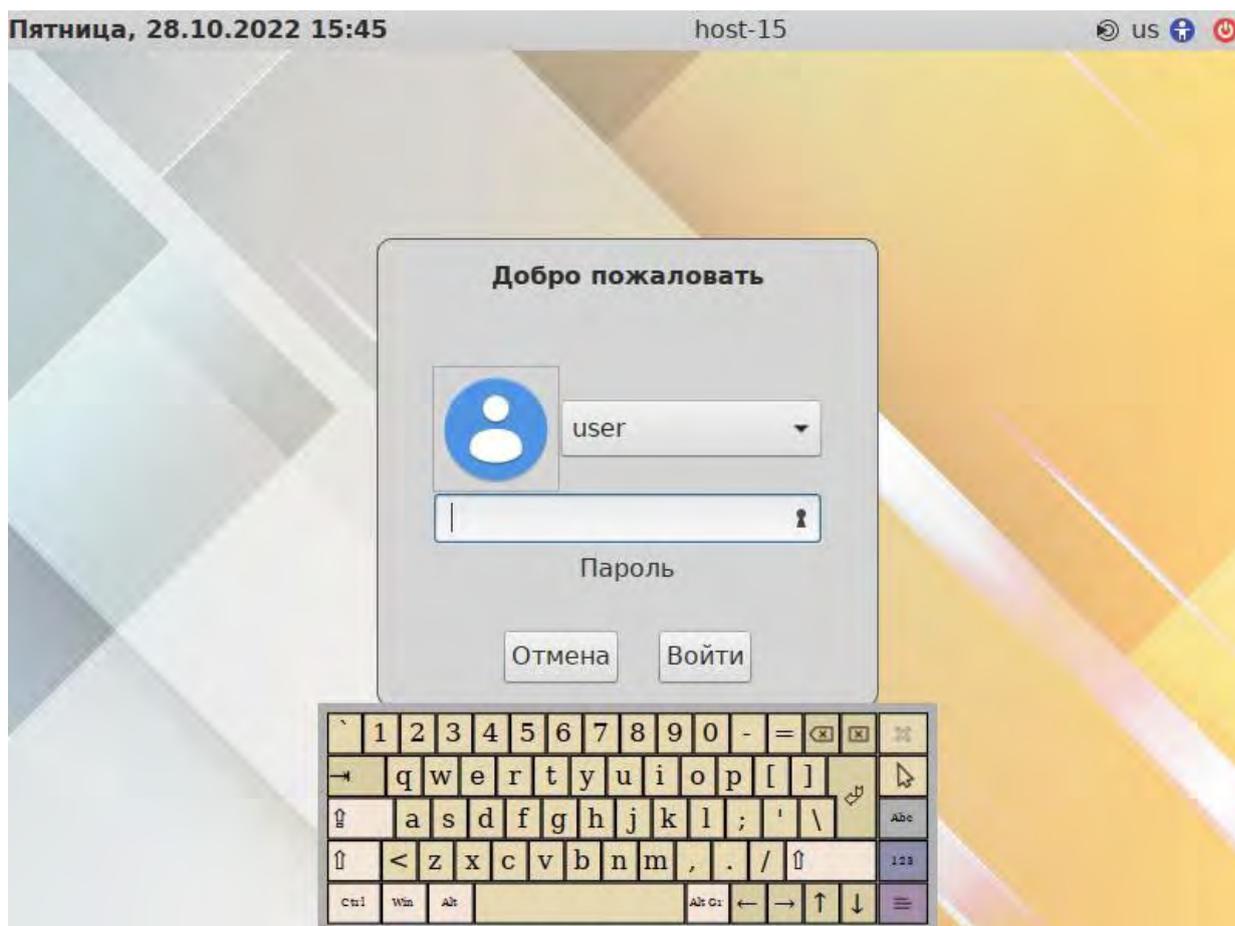


Рис. 188

Для того чтобы выставить настройки dconf глобально для всех пользователей, необходимо (все действия выполняются от имени root):

1. Создать файл `/etc/dconf/profile/user` следующего содержания:


```
user-db:user
system-db:local
```
2. Создать, если он еще не создан, каталог `/etc/dconf/db/local.d`:


```
# mkdir /etc/dconf/db/local.d
```
3. Создать файл для локальной базы данных `/etc/dconf/db/local.d/00_screensaver` следующего содержания:


```
[org/mate/screensaver]
embedded-keyboard-enabled=true
embedded-keyboard-command="onboard --xid"
```
4. Обновить системные базы данных, выполнив команду:


```
# dconf update
```

Просмотреть настройки `org.mate.screensaver` можно, выполнив команду:

```
$ gsettings list-recursively org.mate.screensaver
```

```

org.mate.screensaver mode 'single'
org.mate.screensaver status-message-enabled true
org.mate.screensaver lock-dialog-theme 'default'
org.mate.screensaver logout-command ''
org.mate.screensaver user-switch-enabled true
org.mate.screensaver embedded-keyboard-enabled true
org.mate.screensaver idle-activation-enabled true
org.mate.screensaver lock-delay 0
org.mate.screensaver logout-delay 120
org.mate.screensaver cycle-delay 10
org.mate.screensaver lock-enabled false
org.mate.screensaver logout-enabled false
org.mate.screensaver embedded-keyboard-command 'onboard --xid'
org.mate.screensaver themes ['screensavers-gnomelogo-floaters']
org.mate.screensaver power-management-delay 30

```

В результате при разблокировке экрана появится виртуальная клавиатура (Рис. 189), её можно использовать для ввода пароля.

Виртуальная клавиатура при разблокировке экрана

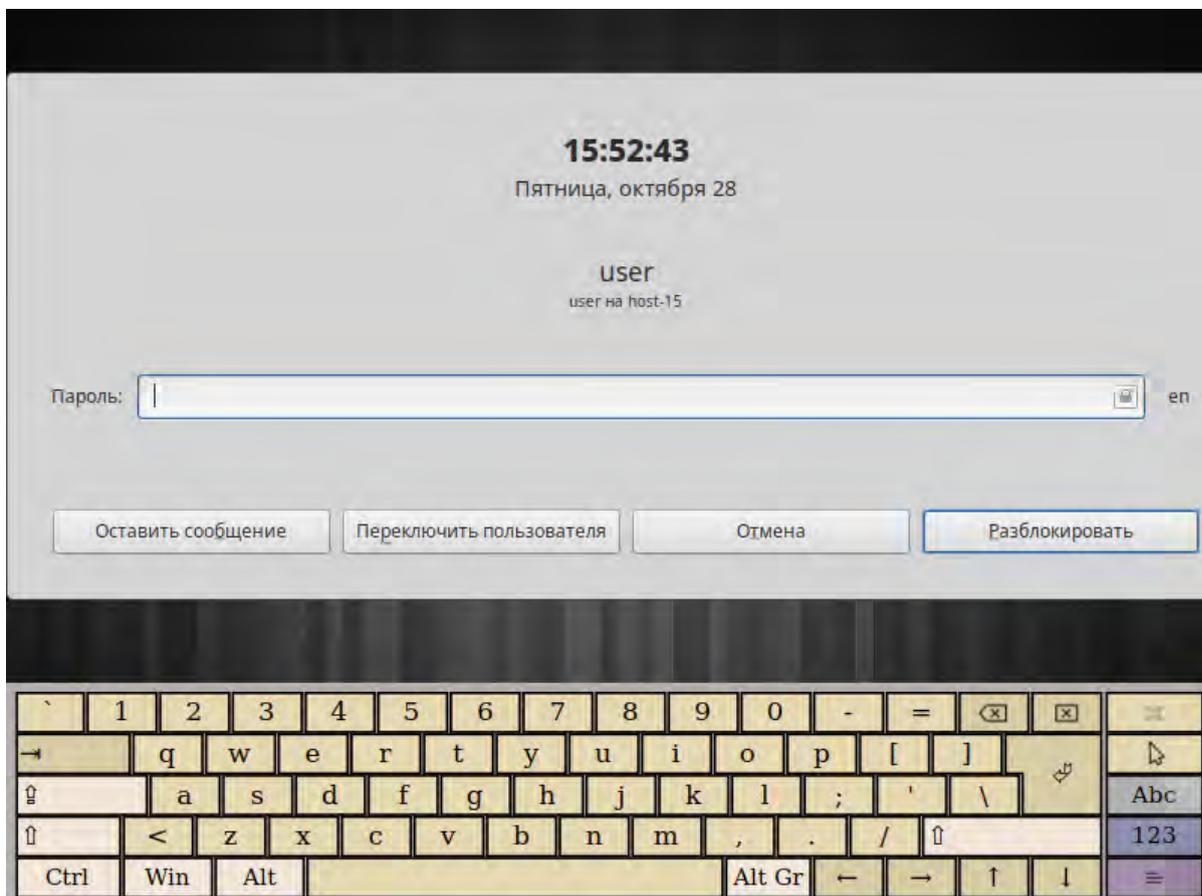


Рис. 189

6.10 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. 190). Это рабочее место нельзя удалить или изменить.

Интерфейс модуля «Настройка нескольких рабочих мест»

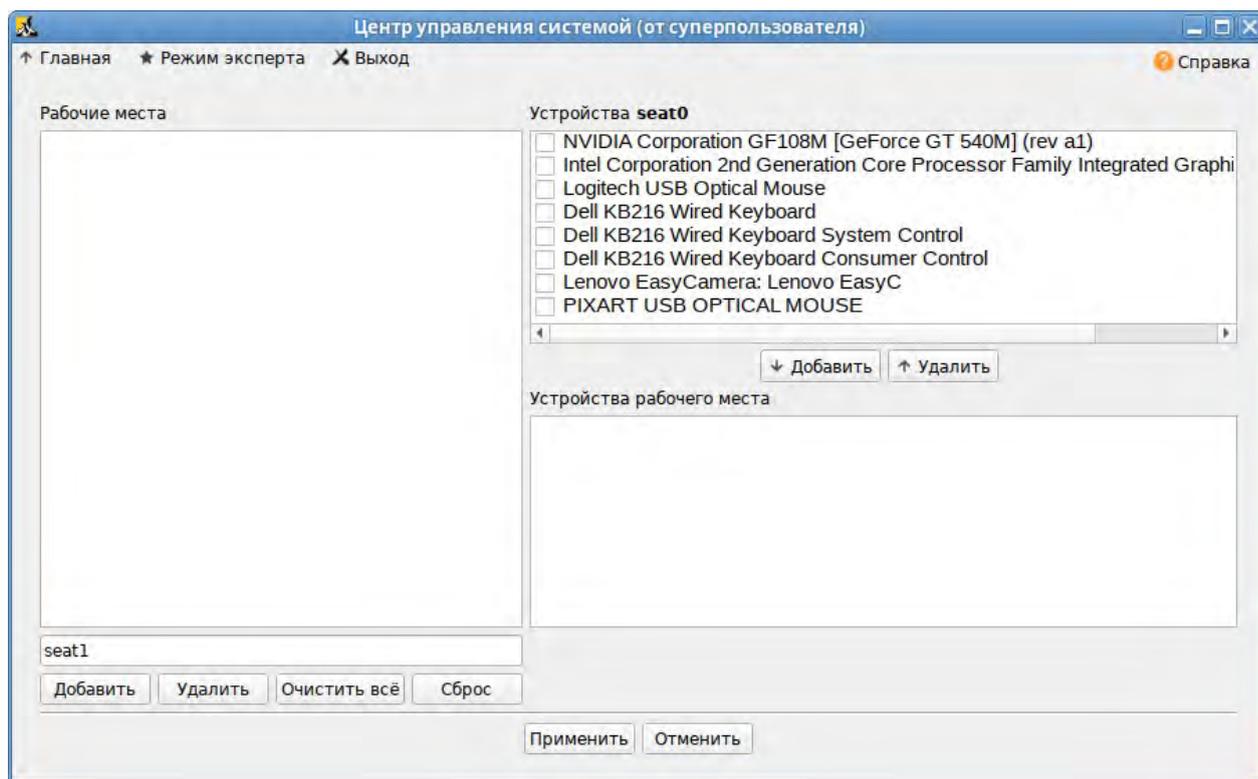


Рис. 190

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. 191).

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. 192).

Устройства рабочего места

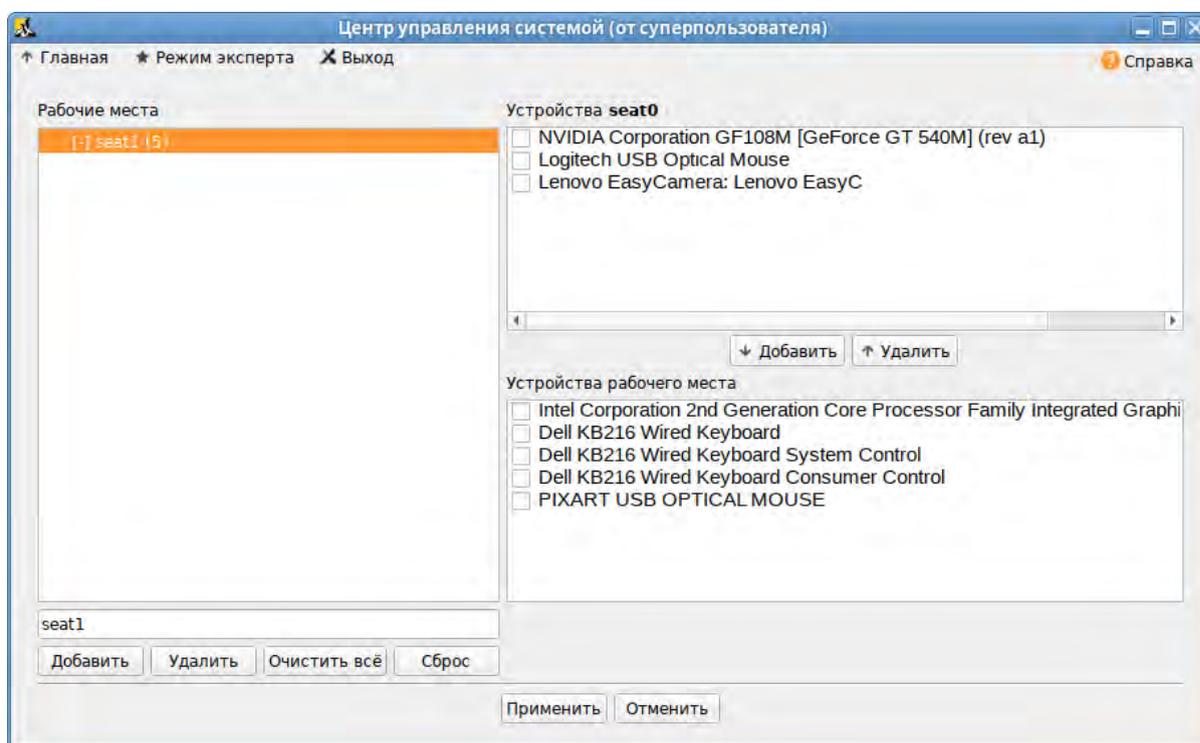


Рис. 191

Активация многоместного режима

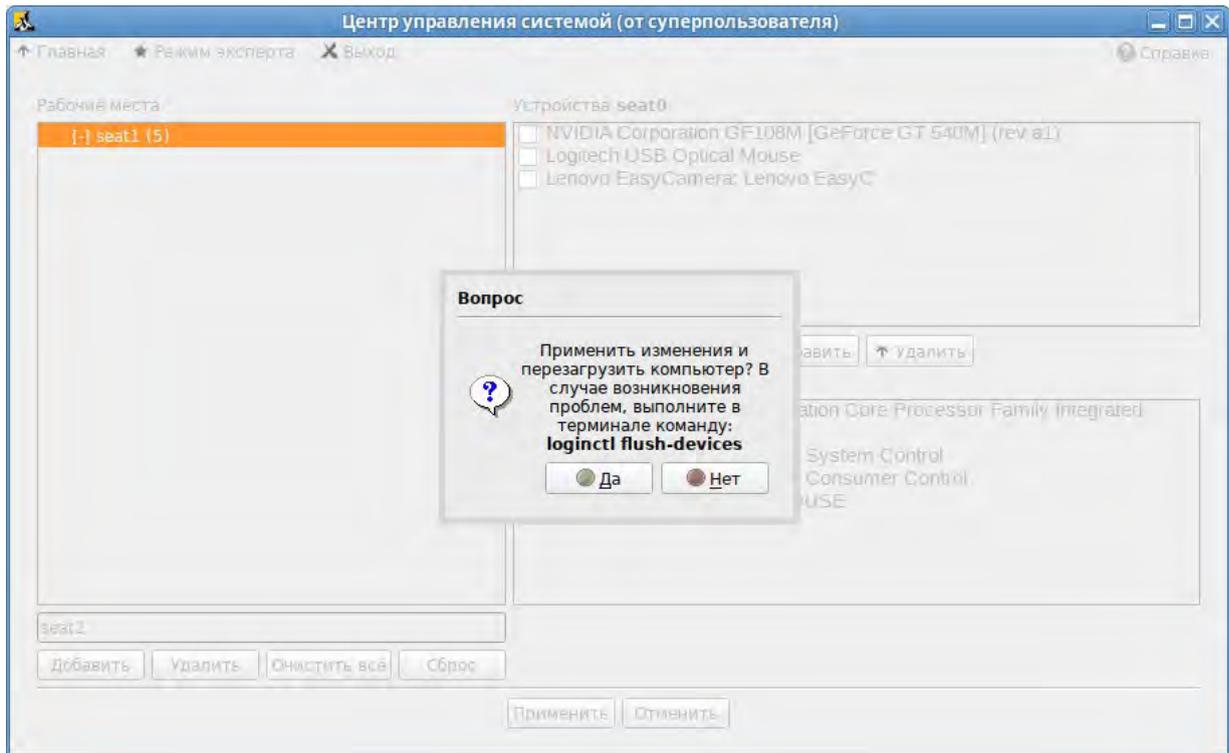


Рис. 192

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 за-
логиниться во второй текстовой консоли, удалить дополнительные рабочие места, выполнив ко-
манду (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 ТТУ» отметить консоли, которые должны быть заблокированы для данного пользователя, перенести их в окно «Заблокированные ТТУ» и нажать кнопку «Применить» (Рис. 193).

Ограничение полномочий пользователей по использованию консолей

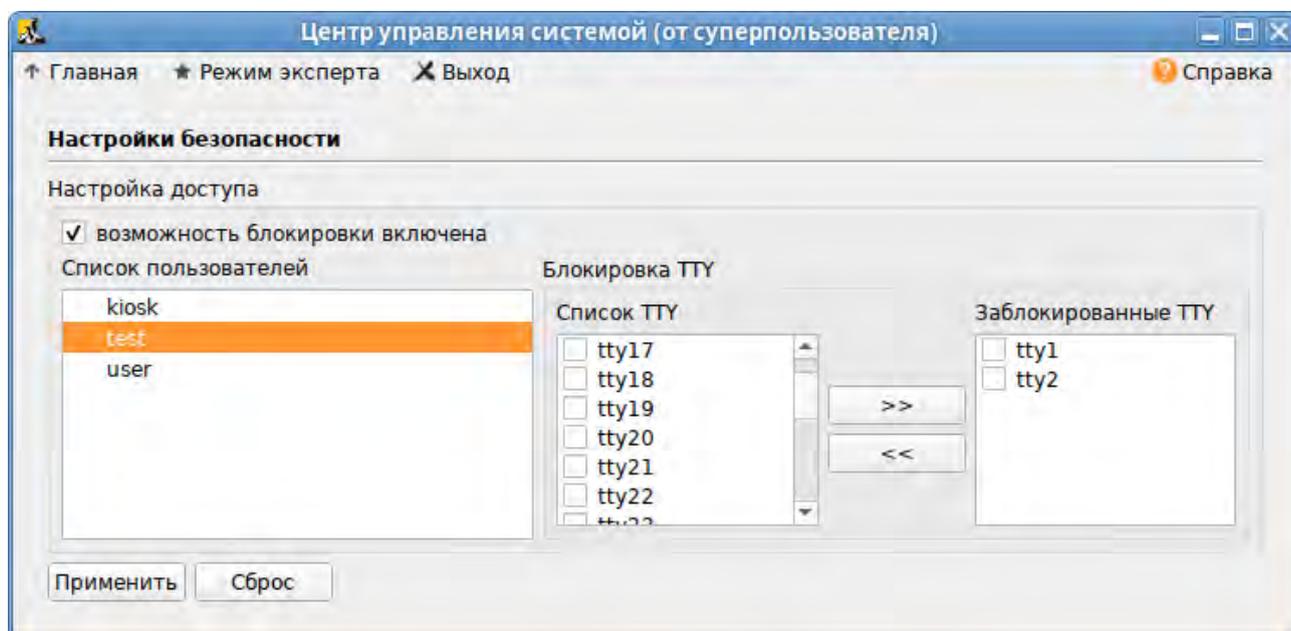


Рис. 193

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 ТТУ (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 con-
fig=/etc/passwdqc.conf
password            required          pam_tcb.so use_authok 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);
- `prproc` – 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. 194). Для этого необходимо установить пакет alterator-limits (из репозитория p10):

```
# apt-get install alterator-limits
```

Установка ограничений ресурсов, доступных пользователю

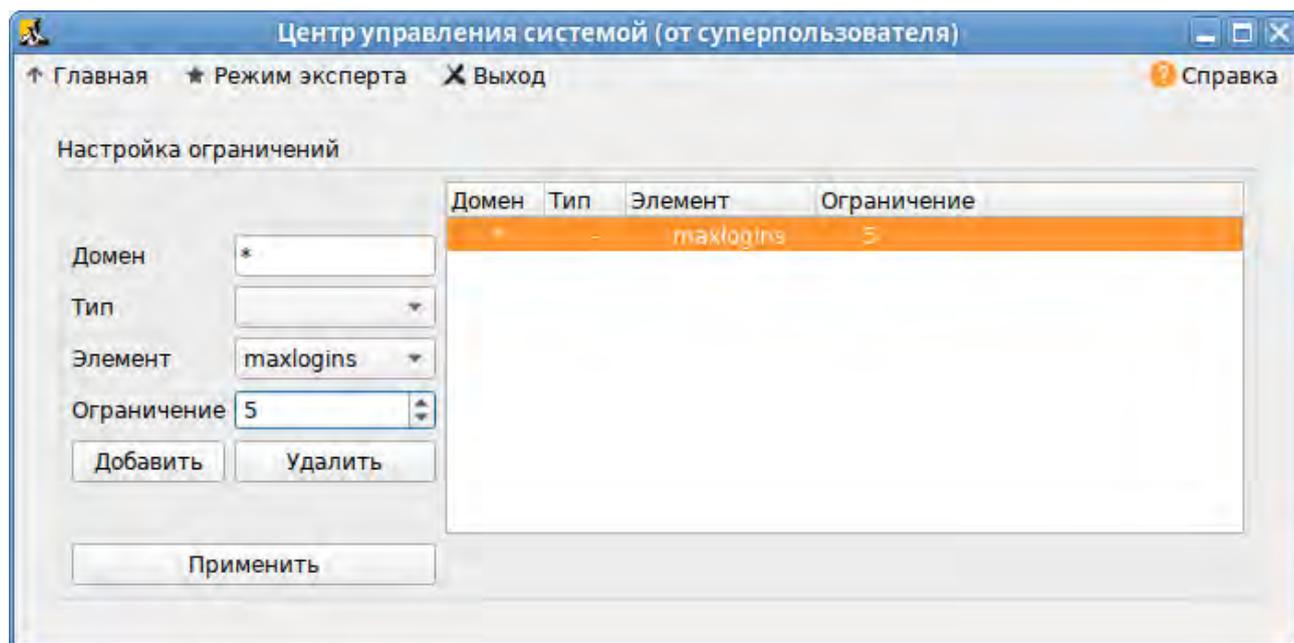


Рис. 194

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. 195).

Блокировка макросов в приложениях

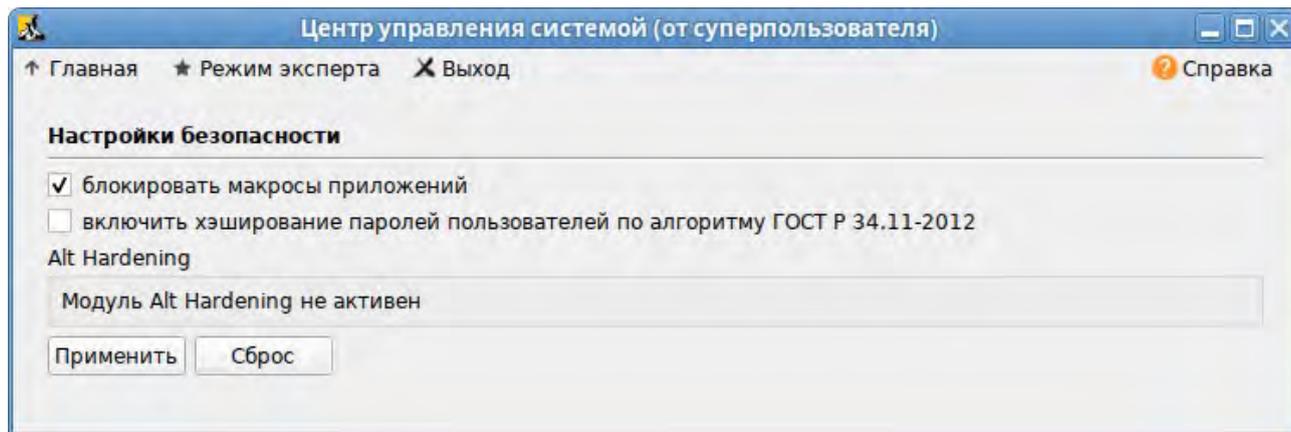


Рис. 195

Макросы будут заблокированы.

7.3 Модуль AltНа

AltНа – 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 AltНа 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 AltНа 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. 196).

Отключение влияния бита SUID на привилегии порождаемого процесса

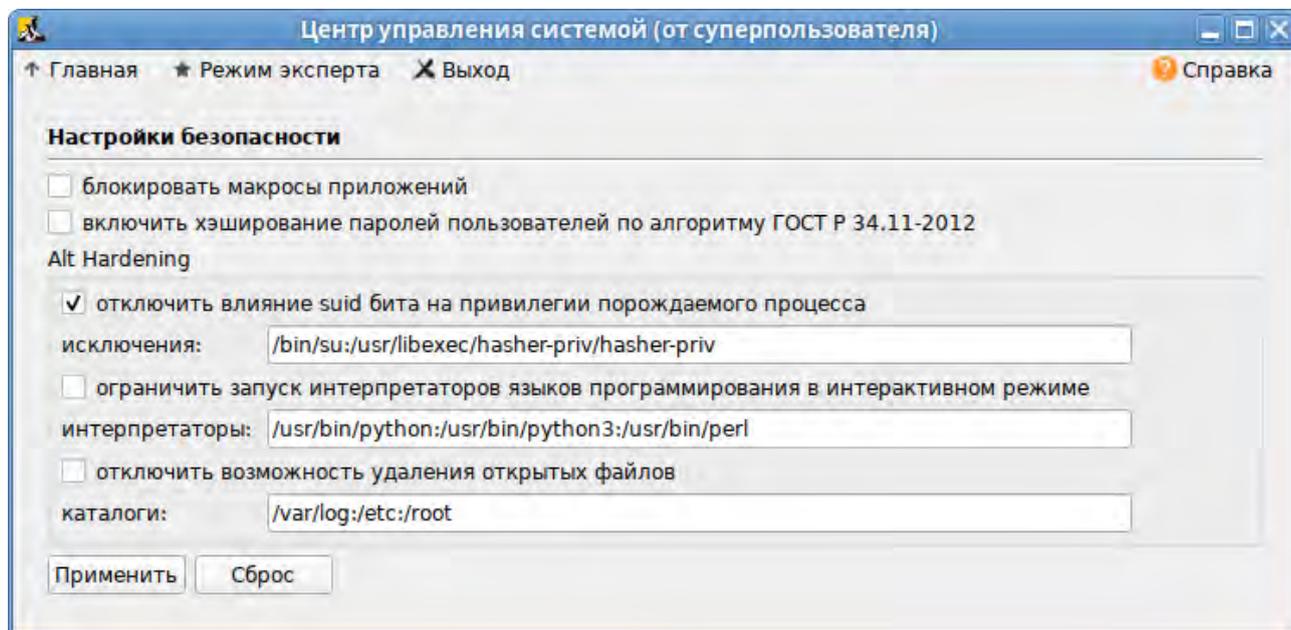


Рис. 196

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/hashepriv/hashepriv"
```

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. 197).

Блокировка интерпретаторов (запрет запуска скриптов)

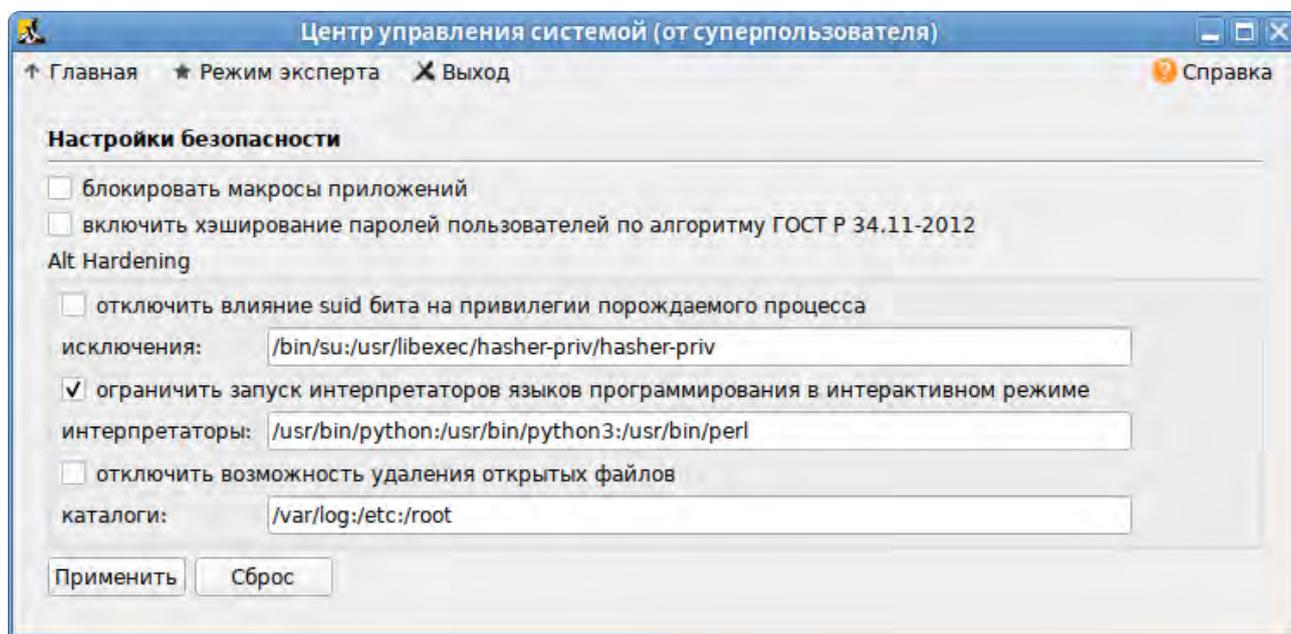


Рис. 197

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 разделённый 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 «Иридиум», 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.

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 МАТЕ» → «Приложения» → «Параметры» → «Программа управления пакетами Synaptic».

При запуске необходимо ввести пароль администратора системы (Рис. 198).

Synaptic. Запрос пароля администратора

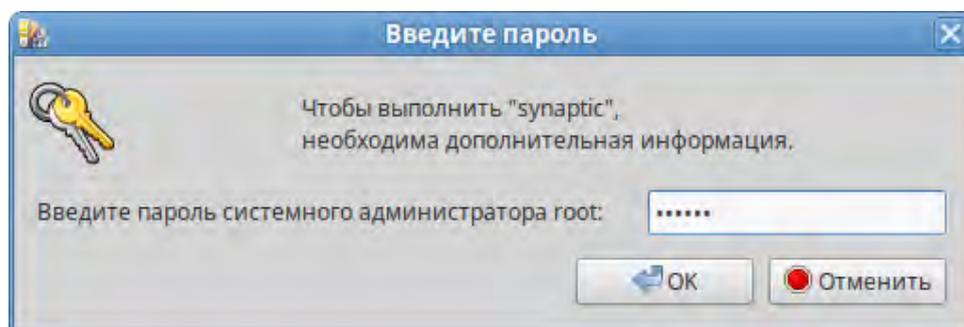


Рис. 198

Для облегчения поиска доступные для установки программы разделены на группы, выводимые в левой части окна программы (Рис. 199).

Программа управления пакетами Synaptic

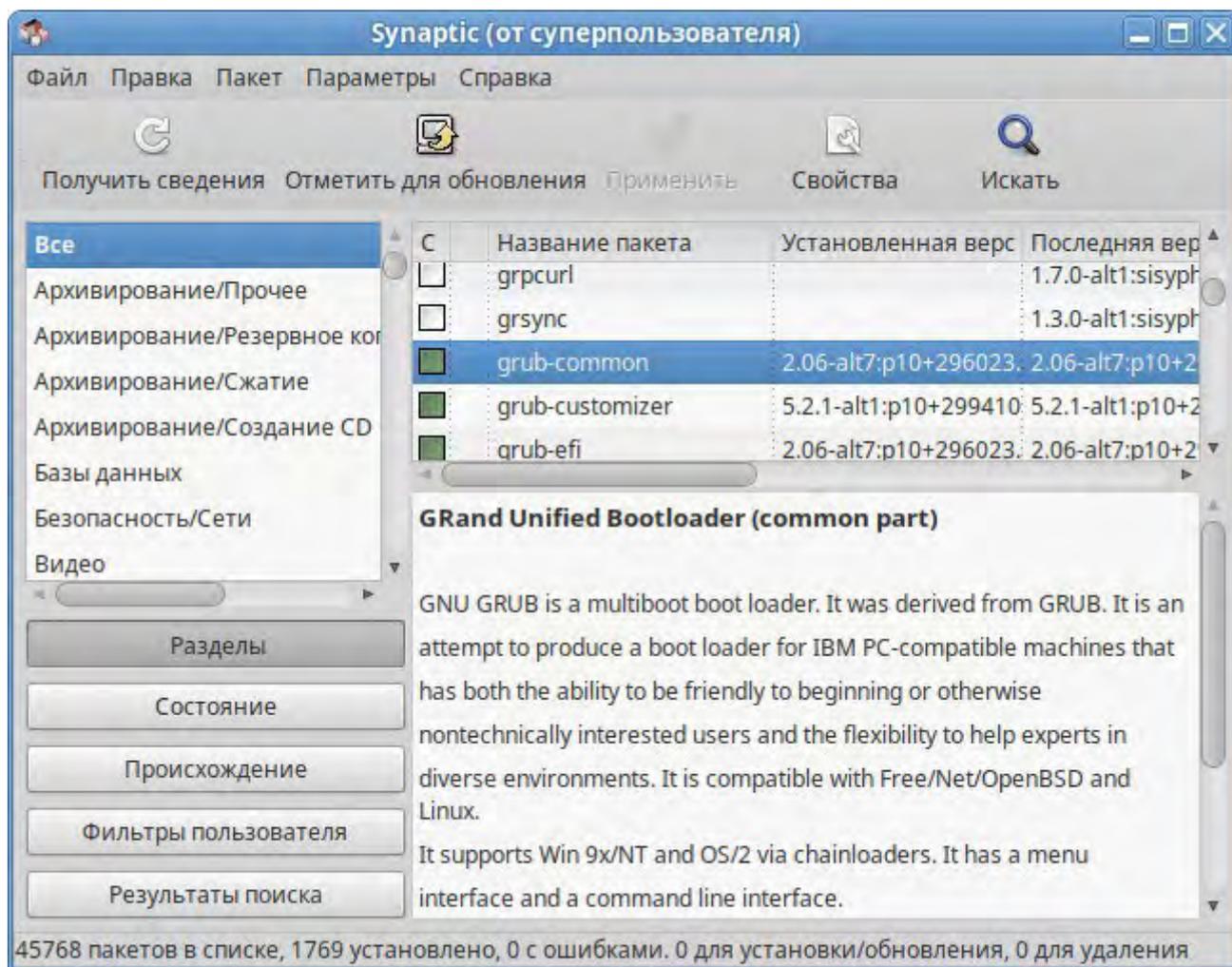


Рис. 199

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 репозитория 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 «ОК» (Рис. 200). К

предложенному списку можно добавить любые репозитории, нажав на кнопку «Создать» и введя необходимые данные.

Добавление репозитория в Synaptic

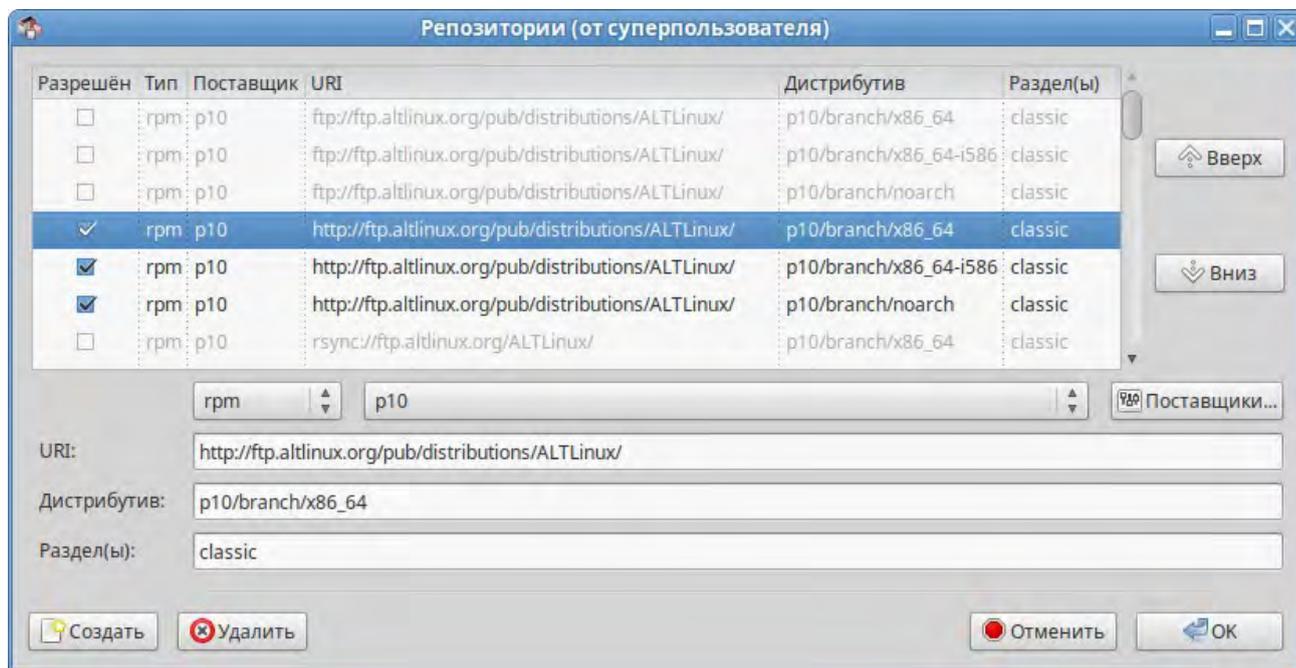


Рис. 200

После выбора и добавления репозитория необходимо получить сведения о находящихся в них пакетах (кнопка «Получить сведения» см. Рис. 199). 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 «Основные» в списке «Обновить систему» выбрать требуемый способ.

Для обновления системы необходимо (Рис. 201):

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

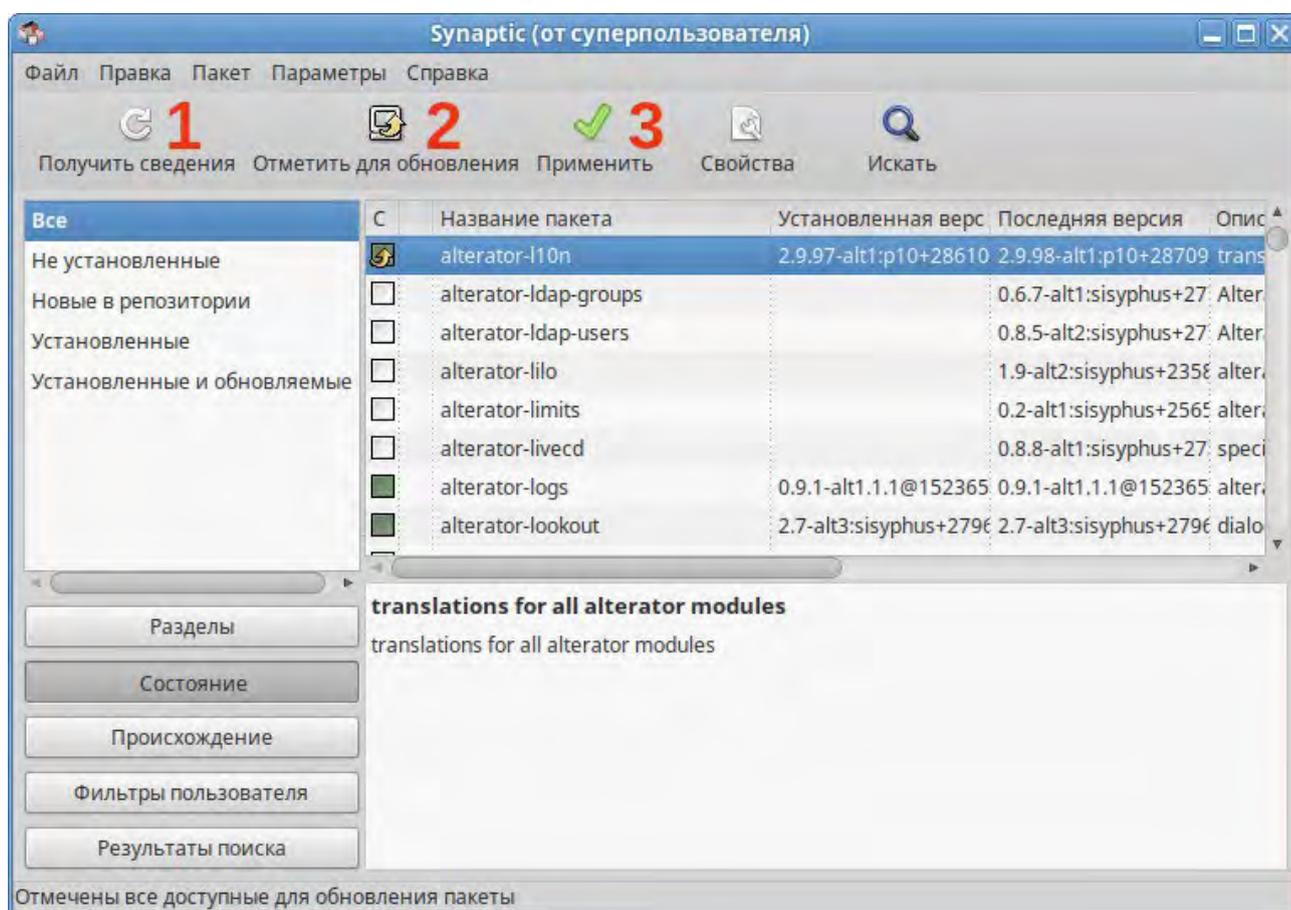


Рис. 201

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. 202).

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»

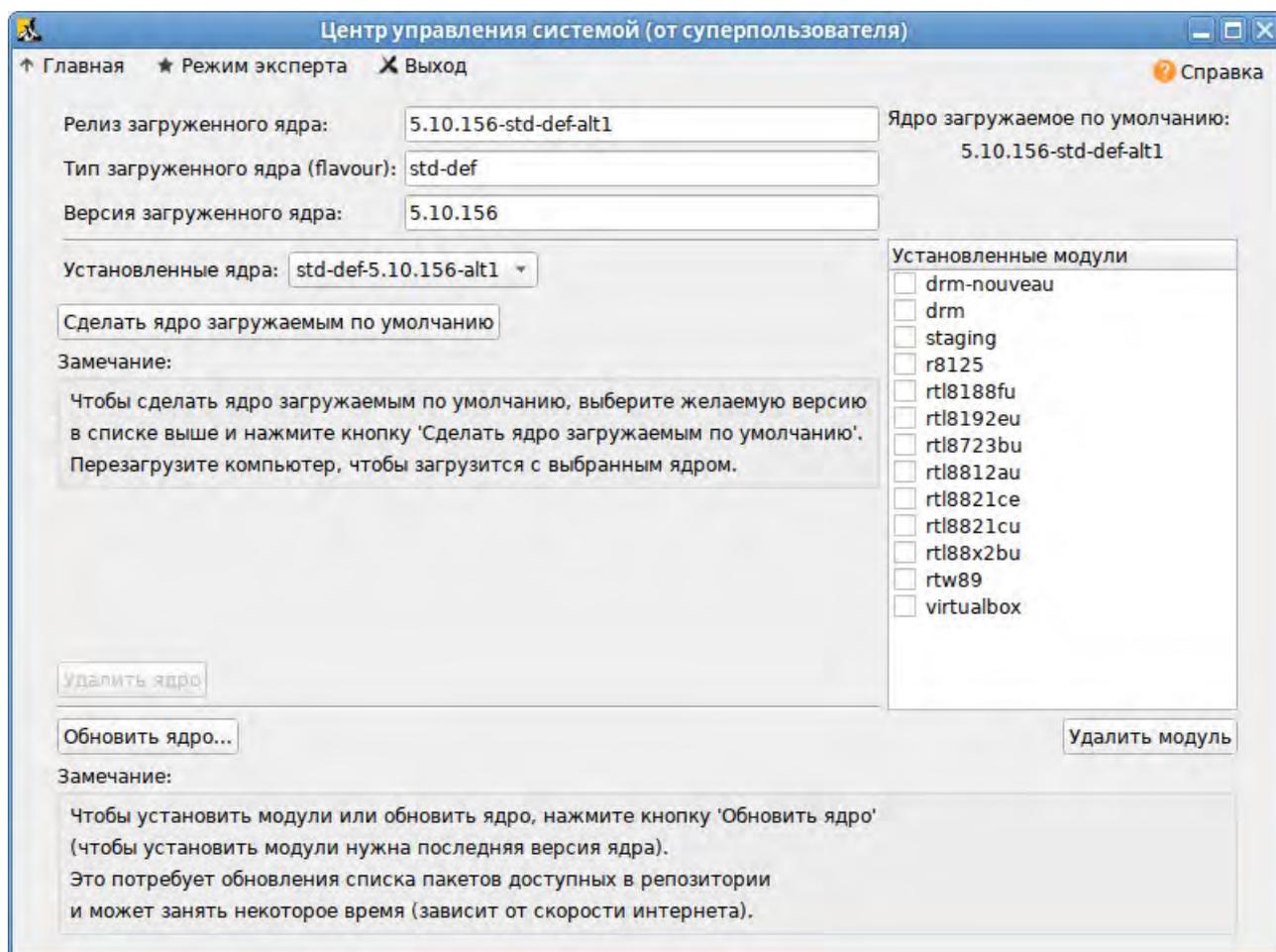


Рис. 202

Если в системе уже установлено последнее ядро, сообщение об этом появится в открывшемся окне (Рис. 203), иначе в этом окне будет показано доступное к установке ядро.

Доступное к установке ядро

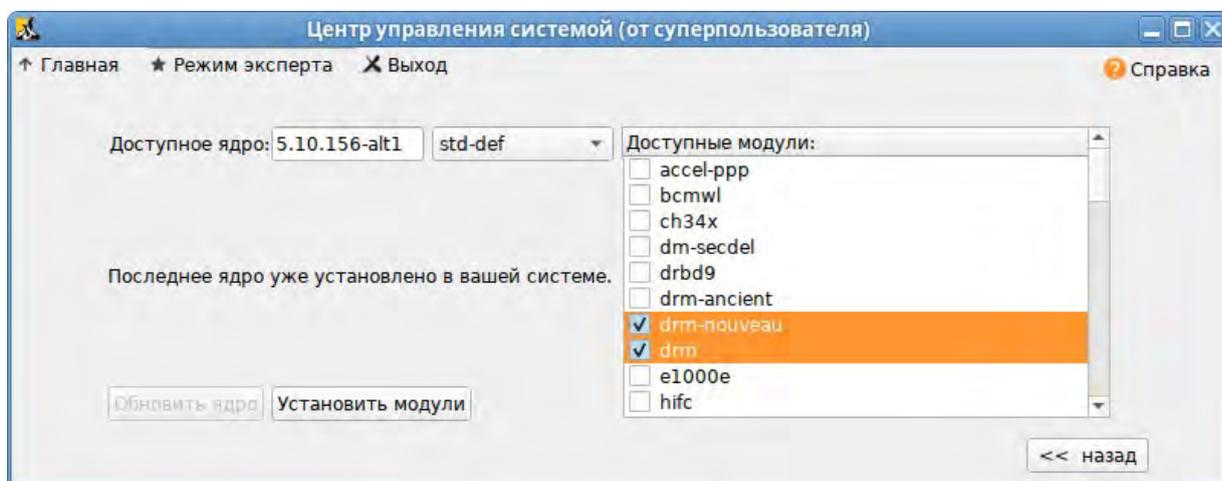


Рис. 203

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 репозиториях, 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 репозиториях 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, АРТ в рамках одной операции установки группы пакетов может пользоваться несколькими репозиториями.

Примечание. Для одновременного подключения нескольких репозиторияв необходимо отслеживать их совместимость друг с другом, т.е. их пакетная база должна отражать один определённый этап разработки. Совместное использование репозиторияв, относящихся к разным дистрибутивам, или смешивание стабильного репозитория с нестабильной веткой разработки (Sisyphus) может привести к различным неожиданностям и трудностям при обновлении пакетов.

АРТ позволяет взаимодействовать с репозиторием с помощью различных протоколов доступа. Наиболее популярные – НТТР и FТР, однако существуют и некоторые дополнительные методы.

Для того чтобы АРТ 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 репозиторияв заносятся в эти файлы в следующем виде:

```
гpm [подпись] метод: путь база название
гpm-src [подпись] метод: путь база название
```

где:

- `гpm` или `гpm-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 АРТ 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, АРТ начнет загружать данный пакет по сети.

8.3.1.1 Добавление репозиторияв

Непосредственно после установки дистрибутива «Иридиум» в `/etc/apt/sources.list`, а также в файлах `/etc/apt/sources.list.d/*.list` обычно указывается несколько репозиторияв:

- 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 репозитория можно воспользоваться утилитой `apt-repo`.

Примечание. Для выполнения большинства команд необходимы права администратора.

Просмотреть список активных репозитория можно, выполнив команду:

```
$ apt-repo list
```

Команда добавления репозитория в список активных репозитория:

```
apt-repo add <репозиторий>
```

Команда удаления или выключения репозитория:

```
apt-repo rm <репозиторий>
```

Команда удаления всех репозитория:

```
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 АРТ 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 АРТ (`/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 репозитория вручную

Для редактирования списка репозитория 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 строка 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 АРТ, необходимо синхронизировать локальную базу данных с удалённым сервером.

Обновление данных осуществляется командой:

```
# apt-get update
```

После выполнения этой команды, `art` обновит свой кэш новой информацией.

Локальная база данных создается заново каждый раз, когда в репозитории происходит изменение: добавление, удаление или переименование пакета. Для репозитория, находящегося на извлекаемых носителях информации и подключённых командой `apt-cdrom add`, синхронизация производится единожды в момент подключения.

Практически любое действие с системой `art` начинается с обновления данных от активированных 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 АРТ выполняется командой:

```
# apt-get install <имя_пакета>
```

П р и м е ч а н и е. 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 АРТ (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 0В/24,6МВ архивов.
```

```
После распаковки потребуется дополнительно 105МВ дискового  
пространства.
```

```
Продолжить? [Y/n] y
```

```
. . .
```

```
Получено 24,6МВ за 0s (44,1МВ/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 АРТ можно установить и отдельный бинарный `rpm`-пакет, не входящий ни в один из репозиториях. Для этого достаточно выполнить команду `apt-get install путь_к_файлу.rpm`. При этом АРТ проведет стандартную процедуру проверки зависимостей и конфликтов с уже установленными пакетами.

В результате операций с пакетами без использования АРТ может нарушиться целостность ОС «Иридиум», и `apt-get` в таком случае откажется выполнять операции установки, удаления или обновления.

Для восстановления целостности ОС «Иридиум» 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 0В архивов. После распаковки 588кБ будет освобождено.
```

```
Вы делаете нечто потенциально опасное!
```

```
Введите фразу 'Yes, do as I say!' чтобы продолжить.
```

Каждую ситуацию, в которой АРТ 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 ко-

манд:

```
# 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 АРТ 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 АРТ 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 (eepm)

Основное назначение единой команды управления пакетами – унифицировать управление пакетами в дистрибутивах с разными пакетными менеджерами. Утилита `eepm` упрощает процедуру управления пакетами, может использоваться в скриптах и установщиках, сервисных программах, в повседневном администрировании различных систем. В `eepm` 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 `eepm`, если она еще не установлена, выполняется командой:

```
# apt-get install eepm
```

Подробную информацию об утилите `epm` и её опциях можно получить, выполнив команду:

```
$ epm --help
```

Ниже описаны лишь некоторые возможности утилиты `epm`.

Установка пакета из репозитория или из локального файла в систему:

```
# epm install <имя_пакета>
```

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
```

Run with a name of a play script to run:

```
anydesk          - Install AnyDesk from the official site
assistant        - Install Assistant (Ассистент) from the
official site
...
yandex-browser   - Install Yandex browser from the official site
yandex-disk      - Install Yandex Disk from the official site
zoom             - Install Zoom client from the official site
```

Команда `epm play` требует наличия доступа в сеть Интернет.

Примечание. Для некоторых сторонних `rpm`-пакетов, написаны дополнительные правила для перепаковки (при перепаковке пакета создаётся пакет, учитывающий, что нужно для работы исходного пакета). Установить такие пакеты можно, выполнив команду:

```
# epm install --repack <имя_пакета>
```

Для `deb`-пакетов ключ `--repack` применяется автоматически.

Удаление пакета из системы:

```
# epm remove <имя_пакета>
```

Поиск пакета в репозитории:

```
# epm search <текст>
```

Получить список установленных пакетов:

```
$ epm list
```

Удалить пакеты, от которых не зависят какие-либо другие пакеты, установленные в системе:

```
# rpm autoremove
```

Обновить все установленные пакеты и ядро ОС:

```
# rpm full-upgrade
```

Примечание. Утилита `yum` (должен быть установлен пакет `eepm-yum`), позволяет имитировать работу менеджера пакетов `yum`, например:

```
# yum search docs-alt-kworkstation
```

```
# apt-cache search -- docs-alt-kworkstation | grep -E -i --color --  
"(docs-alt-kworkstation) "
```

```
docs-alt-kworkstation - ALT KWorkstation documentation
```

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 «Иридиум» 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 перевода 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 символами:

- 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 (ТСВ) 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 находящихся 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 (`swp`). 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 «Иридиум»:

- `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 учётной записи группы;
- groupdel – удаление учётной записи группы;
- groupmod – изменение учётной 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 используются 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 ведёт историю команд и предоставляет возможность их редактирования.

`pdksh` – клон `korn shell`, хорошо известной оболочки в UNIX^(TM) 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 получить права администратора. При вводе команды `su`, будет запрошен пароль суперпользователя (`root`). И в случае ввода корректного пароля, оператор получит привилегии суперпользователя. Чтобы вернуться к правам оператора, 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 [-CFRacdilqrtl] [[-H] | [-L]] [-fgmnoptsx] [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.

Пример. 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` используется для удаления файлов.

Синтаксис:

```
rm [-fiRr] 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...]
```

Команда `rmdir` часто заменяется командой `rm -rf`, которая позволяет удалять каталоги, даже если они не пусты.

Команда cp

Команда `cp` предназначена для копирования файлов.

Синтаксис:

```
cp [-fir] [исх_файл] [цел_файл]
```

```
cp [-fir] [исх_файл...] [каталог]
```

```
cp [-R] [[-H] | [-L] | [-P]] [-fir] [исх_файл...] [каталог]
```

Основные опции:

-r – 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.

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 [параметры] [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 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 символической строки в файле.

Синтаксис:

```
grep шаблон_поиска файл
```

Команда **chmod**

Команда `chmod` изменяет права доступа к файлу.

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:

```
[ugoа...][[+|=] [разрешения...]]...
```

Здесь разрешения – это ноль или более букв из набора «`gwxXst`» или одна из букв из набора «`ugo`».

Каждый аргумент – это список символьных команд изменения прав доступа, разделены запятыми. Каждая такая команда начинается с нуля или более букв «`ugoа`», 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 «`gwxXst`» задают биты доступа для пользователей: «`g`» – 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.

Примеры. Позволить всем выполнять файл `f2`:

```
$ chmod +x f2
```

Запретить удаление файла `f3`:

```
$ chmod+t f3
```

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 символического ВЛАДЕЛЬЦА стоит символ «:», подразумевается изменение группы на основную группу текущего пользователя. Поля ВЛАДЕЛЕЦ и ГРУППА могут быть как числовыми, так и символическими.

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
```

10.1.2.3 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] [-Oуровень] [-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 [options] <name>
```

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, предваренный 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, 1К 234М 2G);
- h, --human-readable – печатать размеры в удобочитаемом формате (например, 1К 234М 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 «Иридиум» – 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 останутся, 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, предваренный знаком «%».

Команда fg

Команда `fg` позволяет перевести задание на передний план.

Синтаксис:

```
fg [идентификатор ...]
```

Идентификатор – PID ведущего процесса задания или номер задания, предваренный 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.

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 АТ системного блока);
- выключить принтер;
- выключить монитор компьютера (если питание монитора не от системного блока);
- выключить стабилизатор, если компьютер подключен через стабилизатор напряжения.