MyOffice Plus

Руководство пользователя

ОПЕРАЦИОННАЯ СИСТЕМА АЛЬТ РАБОЧАЯ СТАНЦИЯ 10.0

ОПЕРАЦИОННАЯ СИСТЕМА

АЛЬТ РАБОЧАЯ СТАНЦИЯ 10.0

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

1.0

На 136 листах

Москва
2022

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам.

Товарные знаки «МойОфис» и «MyOffice» принадлежат ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ».

Товарные знаки «Альт Рабочая станция» и «Альт Сервер» принадлежат ООО «Базальт СПО».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем. Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращения, которые используются в настоящем документе, приведены в Таблице 1.

Таблица 1 – Сокращения и расшифровки

Сокращения	Расшифровка
ОС Альт Рабочая станция	Операционная система «Альт Рабочая станция»
ПЭВМ	Персональная электронно-вычислительная машина

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение MyOffice Plus

MyOffice Plus – комплексный продукт для организации рабочей среды в крупных государственных организациях и коммерческих предприятиях. Единая лицензия МойОфис Plus включает операционную систему, средства безопасного хранения файлов, работы с документами, ведения переписки по электронной почте и планирования рабочего времени.

ОС Альт Рабочая станция (продукт «Базальт СПО») входит в состав продукта MyOffice Plus.

1.2 Описание ОС Альт Рабочая станция

Операционная система «Альт Рабочая станция» предоставляет интегрированную операционную систему на единой оптимизированной пакетной базе с поддержкой различных аппаратных платформ.

ОС «Альт Рабочая станция» обладает следующими функциональными характеристиками:

- обеспечивает возможность обработки, хранения и передачи информации;
- обеспечивает возможность функционирования в многозадачном режиме (одновременное выполнение множества процессов);
- обеспечивает возможность масштабирования системы: возможна эксплуатация ОС как на одной ПЭВМ, так и в информационных системах различной архитектуры;
- обеспечивает многопользовательский режим эксплуатации;
- обеспечивает поддержку мультипроцессорных систем;
- обеспечивает поддержку виртуальной памяти;
- обеспечивает поддержку запуска виртуальных машин;
- обеспечивает сетевую обработку данных, в том числе разграничение доступа к сетевым пакетам.

ОС Альт Рабочая станция состоит из набора компонентов предназначенных для реализации функциональных задач необходимых пользователям (должностным лицам для выполнения определенных должностными инструкциями, повседневных действий) и поставляется в виде дистрибутива и комплекта эксплуатационной документации.

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

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

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

Основные преимущества ОС Альт Рабочая станция:

– русскоязычный пользовательский интерфейс;
– графическая рабочая среда MATE;
– выбор разворачиваемых решений (например, виртуализация, мультимедиа приложения) на этапе установки;
– возможность как развернуть, так и использовать только определенные 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.

1.3 Описание ОС Linux

1.3.1 Свободные программы

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

– запускать на любом количестве компьютеров;

– распространять бесплатно или за деньги без каких-либо ограничений;

– получать исходные тексты этих программ и вносить в них любые изменения.

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

1.3.2 Разработка Linux

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

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

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

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

1.3.3 Защищенность

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

1.3.4 Дистрибутивы Linux

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

1.3.5 Новым пользователям

Linux – самостоятельная операционная система. Все операционные системы разные: Linux – не Windows, не OS X и не FreeBSD. В Linux свои правила, их необходимо изучить и к ним необходимо привыкнуть. Терпение и настойчивость в изучении Linux обернется значительным повышением эффективности и безопасности вашей работы. То, что сегодня кажется странным и непривычным, завтра понравится и станет нормой. Не стесняйтесь задавать вопросы, ведь самый простой способ найти ответ – совет опытного специалиста. Взаимопомощь и общение – традиция в мире Linux. Всегда можно обратиться за помощью к сообществу пользователей и разработчиков Linux. Большинство вопросов повторяются, поэтому для начала стоит поискать ответ на свой вопрос в документации, затем в сети Интернет. Если вы не нашли ответа в перечисленных источниках, не стесняйтесь, пишите на форум или в списки рассылки так, как писали бы своим друзьям, и вам обязательно помогут.

1.4 Системы Альт

1.4.1 ALT Linux Team

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

1.4.2 Сизиф

Sisyphus – наш ежедневно обновляемый банк программ (часто называемый репозиторий). На его основе создаются все дистрибутивы ALT. Поддерживаемая ALT Linux Team целостность Sisyphus, оригинальная технология сборки программ, утилита aptget и ее графическая оболочка synaptic позволяют пользователям легко обновлять свои системы и быть в курсе актуальных новостей мира свободных программ.

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

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

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

Sisyphus, в первую очередь, – открытая лаборатория решений. Если вам это интересно, если вы хотите дополнить Sisyphus новыми решениями, если вы считаете, что можете собрать какую-то программу лучше – присоединяйтесь к проекту ALT Linux Team.

1.4.3 Десятая платформа

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

Десятая платформа (p10) была создана в июле 2021 года и ее поддержка продлится до июля 2024.

1.4.3.1 Основные новшества в десятой платформе

– Синхронная сборка p10 производится для пяти основных архитектур:
  - 64-битных x86_64, aarch64 и ppc64le;
  - 32-битных i586 и armh (armv7hf).

– Ядра реального времени – для архитектуры x86_64 собраны два realtime-ядра: Xenomai и Real Time Linux (PREEMPT_RT).

– Расширение набора групповых политик – групповые политики поддерживают параметры gsettings для управления рабочими средами MATE и Xfce.

– Центр администрирования Active Directory (admc) – графическое приложение для управления пользователями, группами и групповыми политиками домена Active Directory.
– Платформа Deploy – предназначена для развертывания системных служб на локальном компьютере с помощью Ansible. Поддерживаемые роли: Apache, MariaDB, MediaWiki, Nextcloud, PostgreSQL и Moodle.
– Модуль настройки многотерминального режима alterator-multiseat.

2 НАЧАЛО ИСПОЛЬЗОВАНИЯ ОС АЛЬТ РАБОЧАЯ СТАНЦИЯ

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

2.1 Загрузка системы

Запуск ОС Альт Рабочая станция выполняется автоматически после запуска компьютера и отработки набора программ BIOS. На экране появляется меню, в котором перечислены возможные варианты загрузки операционной системы.

При первом старте, в условиях установки нескольких ОС на один компьютер, возможно отсутствие в загрузочном меню пункта/пунктов с другой/другими операционными системами, они будут добавлены в список при последующей перезагрузке. Все перечисленные в меню после перезагрузки варианты могут быть загружены загрузчиком Linux.

Стрелками клавиатуры **Вверх** и **Вниз** выберите нужную операционную систему. Дополнительно к основным вариантам запуска ОС из этого меню можно загрузить Linux в безопасном режиме или запустить проверку памяти. Загрузка операционной системы по умолчанию (первая в списке) начинается автоматически после небольшого времени ожидания (обычно несколько секунд). Нажав клавишу **Enter**, можно начать загрузку немедленно.

Нажатием клавиши **E** можно вызвать редактор параметров текущего пункта загрузки. Если система настроена правильно, то редактировать их нет необходимости.

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 быть занять больше времени, чем обычно. Подробную информацию о шагах загрузки можно получить, нажав клавишу **Esc**.

2.2 Получение доступа к зашифрованным

В случае, если вы создали шифрованный раздел, вам потребуется вводить пароль при обращении к этому разделу.

Например, если был зашифрован домашний раздел */home*, то для того, чтобы войти в систему под своим именем пользователя, вам 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 вам следует перезагрузить систему, нажав для этого два раза **Enter**, а затем клавиши **Ctrl** + **Alt** + **Delete**.

2.3 Вход в систему

2.3.1 Вход и работа в консольном режиме

Стандартная установка ОС Альт Рабочая станция включает базовую систему, работающую в консольном режиме.

При загрузке в консольном режиме работа загрузчика ОС Альт Рабочая станция завершается запросом на ввод логина и пароля учетной записи. 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. В случае успешного прохождения процедуры аутентификации и идентификации будет выполнен вход в систему. ОС Альт Рабочая станция перейдет к штатному режиму работы и предоставит дальнейший доступ к консоли.

2.3.2 Виртуальная консоль

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

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

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

2.3.3 Вход и работа в системе в графическом режиме

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

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

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

Настройка возможности ввода логина и пароля пользователя с виртуальной клавиатуры рассмотрена в разделе Виртуальная (экранная) клавиатура.

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

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

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

2.4 Блокирование сеанса доступа

2.4.1 Блокирование сеанса доступа после времени бездействия или по запросу

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

Если вы оставляете свой компьютер на короткое время, вы должны заблокировать свой экран, чтобы другие пользователи не могли получить доступ к вашим файлам или работающим приложениям.

Заблокировать сеанс доступа можно по запросу пользователя: **Меню MATE** > **Система** > **Заблокировать экран**.

Для разблокировки требуется ввести пароль пользователя и нажать кнопку **Разблокировать**.

Настройка возможности ввода пароля пользователя с виртуальной клавиатуры рассмотрена в разделе Виртуальная (экранная) клавиатура.

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

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 MATE** > **Приложения** > **Параметры** > **Хранитель экрана**.

2.4.2 Блокировка виртуальных текстовых консолей

Программа vlock позволяет заблокировать сеанс при работе в консоли.

Должен быть установлен пакет vlock:

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

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

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

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

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

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

2.5 Завершение сеанса пользователя

2.5.1 Консольный режим

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

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

2.5.2 Настройки завершения сеанса пользователя в консоли

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

```
TMOUT=300
```

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

2.5.3 Графический режим

Для завершения сеанса пользователя в графическом режиме в **Меню MATE** в разделе **Система** выбрать пункт **Завершить сеанс**.

Далее откроется окно, в котором предоставляется выбор дальнейших действий:

– **Переключить пользователя** – сеанс пользователя в графическом режиме блокируется, другой пользователь может войти в систему под своим именем;

– **Завершить сеанс** – выполняется завершение сеанса пользователя в графическом режиме.

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

2.6 Выключение/перезагрузка компьютера

2.6.1 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
```

2.6.2 Графический режим

Для выключения/перезагрузки компьютера следует в **Меню MATE** в разделе **Система** выбрать пункт **Выйти**.

Далее откроется окно, в котором предоставляется выбор дальнейших действий:

– **Ждущий режим** – компьютер переводится в режим экономии энергии;

– **Спящий режим** – компьютер переводится в режим энергосбережения, позволяющий отключить питание компьютера, сохранив при этом текущее состояние операционной системы;

– **Перезагрузить** – выполняется перезапуск ОС;

– **Выключить** – выполняется выключение компьютера.

Если при разбивке жесткого диска не создавался раздел подкачки (swap), то пункт **Спящий режим** в окне выключения компьютера будет отсутствовать.

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

3 РАБОЧИЙ СТОЛ MATE

MATE предоставляет традиционное окружение рабочего стола. В MATE поддерживается система панелей с разнообразными меню, апплетами, индикаторами, кнопками и т.д., которые могут настраиваться пользователем.

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).

3.1 MATE: Область рабочего стола

Область рабочего стола включает в себя три значка:

– **Компьютер** – предоставляет доступ к устройствам хранения данных;

– **Домашняя папка пользователя** – предоставляет доступ к домашнему каталогу пользователя */home/<имя пользователя>*. В этой папке по умолчанию хранятся пользовательские файлы (например, аудиозаписи, видеозаписи, документы). У каждого пользователя свой «Домашний» каталог. Каждый пользователь имеет доступ только в свой «Домашний» каталог;

– **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**).

3.2 Панель MATE

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

На левой части панели расположены:

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

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

– **Переключатель рабочих мест** – это группа квадратов в правом нижнем углу экрана. Они позволяют вам переключать рабочие места. Каждое рабочее место предоставляет отдельный рабочий стол, на котором можно расположить приложения. По умолчанию активно 2 рабочих места. Можно изменить это число, нажав правой кнопкой мышки на **переключателе рабочих мест** и выбрав пункт **Настройка**.

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

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

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

На правой части панели находятся:

– область уведомлений;

– регулятор громкости и апплет настройки звука;

– приложение «Сетевые соединения»;

– часы и календарь;

– параметры клавиатуры;

– параметры управления питанием.

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

3.3 Запуск приложений

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

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

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

– **Мой компьютер** – позволяет увидеть все файлы в компьютере и файлы на подключенных внешних носителях;

– **Домашний каталог** – в этой папке по умолчанию хранятся личные файлы пользователя;

– **Сеть** – позволяет просматривать сетевые подключения компьютера. Осуществляет получение доступа к файлам и другим ресурсам, доступным в этих сетях;

– **Рабочий стол** – папка внутри «Домашней папки», содержащая файлы и папки, отображаемые на рабочем столе;

– **Корзина** – позволяет получить доступ к «удаленным файлам».

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

– **Менеджер пакетов** – запускает программу для централизованного управления программным обеспечением;

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

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

Установленные приложения доступны в следующих разделах **Меню MATE**:
– **Все** – показывает полный список установленных приложений;
– **Аудио и видео**; **Графика**;
– **Интернет**;
– **Офис**;
– **Системные**;
– **Стандартные**;
– **Администрирование** – содержит инструменты позволяющие администрировать систему;
– **Параметры** – содержит инструменты позволяющие конфигурировать систему.

Этот список обновляется при установке или удалении программ.

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

Для добавления приложения в раздел **Избранное** нужно в контекстном меню нужного приложения выбрать пункт **Отображать в избранном**. 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).

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.

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

4 ОБЗОР ПРИЛОЖЕНИЙ ДЛЯ ОС

ОС Альт Рабочая станция содержит большое 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. Со временем вы сами сможете выбрать наиболее удобные для вас приложения.

Набор программ с диска покрывает обычные потребности. Если же определенная программа отсутствует в системе, то вы можете доустановить ее с диска или из огромного банка программного обеспечения ОС Альт Рабочая станция.

4.1 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. К базовым функциям современных веб-браузеров относятся:

– 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 вам 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.

Возможно, по опыту работы в других операционных системах вы уже знакомы с определенным браузером. Определить, какой браузер лучше, практически невозможно. Эту задачу каждый пользователь решает сам, ориентируясь на свои личные предпочтения. В любом случае рассмотрите основные предложения и выберите наиболее удобный для вас веб-навигатор.

4.1.1 Chromium

Программа Chromium – веб-браузер, поддерживающий большинство современных вебтехнологий и интернет-протоколов. Браузер Chromium предлагает пользователю логичный интерфейс и возможность полностью контролировать свою работу в Интернете.

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

4.1.1.1 Просмотр веб-страниц

Для того чтобы открыть интернет-страницу, введите ее адрес в адресную строку браузера и нажмите **Enter**. Если вы хотите открыть ссылку на следующую страницу в новой вкладке, то нажмите на ней средней кнопкой (колесом) мыши. Можно настроить одновременный просмотр нескольких страниц в разных вкладках одного окна.

4.2 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 вебинтерфейс, используя браузер. Подручных средств, предоставляемых популярными почтовыми сервисами, для повседневных почтовых нужд пользователя практически достаточно, но использование специально предназначенных программ дает некоторые преимущества:

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

Для ОС Linux создано большое количество почтовых клиентов. Все они обладают своими особенностями и, как правило, имеют все 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 ваших личных предпочтений. Для первоначальной настройки любого из них вам 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 вашей сети (в случае использования почтового сервера локальной сети).

4.2.1 МойОфис Почта

МойОфис Почта – почтовый клиент для работы с электронными сообщениями, календарями, задачами и адресными книгами.

4.3 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, занесенные 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 стационарные и мобильные 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 занесенных в список контактов пользователей (в сети, нет на месте и т.д.).

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

4.3.1 Pidgin

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

Возможности Pidgin:

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

– обмен файлами;

– многоязычный интерфейс.

4.3.1.1 Первоначальная настройка

После запуска Pidgin необходимо произвести его первоначальную настройку. При первом запуске Pidgin из меню **Уч.записи** > **Управление учетными записями** необходимо запустить диалоговое окно мастера создания учетной записи и создать учетную запись пользователя.

Из списка поддерживаемых служб выберите ту, которую собираетесь использовать. Возможно, вы уже решили, какую службу IM будете использовать (потому что вы уже пользовались ею, либо потому что ею пользуются ваши друзья). Если вы еще не остановили свой выбор на какой-то определенной службе IM, то выберите службу, основанную на открытых стандартах, например jabber.

Если вы еще не зарегистрированы ни в одной службе мгновенных сообщений, то предварительно необходимо создать аккаунт на соответствующем веб-сайте.

После настройки учетной записи добавьте в список контактов ваших собеседников (кнопка **Добавить собеседника…**) и, при условии, что нужный вам собеседник подключен к службе мгновенных сообщений, можете начинать общение.

За дополнительной информацией по использованию Pidgin можно обратиться к справке, вызываемой из меню **Помощь** > **Помощь в сети**.

4.4 Офисные приложения

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

4.4.1 МойОфис Текст

МойОфис Текст – редактор для быстрого и удобного создания и форматирования текстовых документов любой сложности.

4.4.2 МойОфис Таблица

МойОфис Таблица – редактор для создания электронных таблиц, ведения расчетов, анализа данных, формирования сводных отчетов и автоматизации обработки данных с использованием макрокоманд.

4.4.3 МойОфис Презентация

МойОфис Презентация – приложение для просмотра и демонстрации презентаций.

4.4.4 Редактор презентаций

Редактор презентаций – редактор на основе компонентов с открытым исходным кодом для быстрого и удобного создания и оформления презентаций.

4.5 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.

4.5.1 Файловый менеджер Caja

Caja – это современный файловый менеджер для рабочей среды MATE.

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 съемным носителям.

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

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

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

– в меню выбрать **Файл** > **Свойства**;

– в контекстном меню файла (папки) выбрать пункт **Свойства**;

– нажать **Alt** + **Enter**.

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

С помощью окна **Свойства объекта** можно выполнить следующие действия:

– изменить значок объекта;

– изменить файловые права на доступ к объекту;

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

4.5.1.1 Домашняя папка

Все файлы и папки пользователя хранятся в системе внутри домашней папки (каталог **/home/имя_пользователя**). Открыть ее можно, щелкнув 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.

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 ее подпапках можно создавать другие папки, например, выбрав в контекстном меню пункт **Создать папку…**.

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

4.5.1.2 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. Нажав на кнопку, можно быстро открыть нужную папку.

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

4.5.1.3 Копирование и перемещение файлов

Скопировать или переместить файл или папку можно различными способами:

– «перетащить» папку или файл из одного открытого окна Caja в другое (где открыта целевая папка). Перетаскивание можно осуществлять и в двупанельном режиме. В этом случае не потребуется запускать два экземпляра Caja. Нажмите на кнопку F3 и вы сможете перемещать и копировать файлы и папки, перетаскивая их между панелями;

– копировать и перемещать папку или файл можно, используя основное стандартное меню **Правка** (либо контекстное меню):

- необходимо выделить то, что вы желаете скопировать или переместить;
- из основного меню **Правка** или из контекстного меню выберите **Копировать** (для копирования) или **Вырезать** (для перемещения);
- открыть папку, в которую вы хотите скопировать или переместить объект;
- вызвать в этой папке из основного меню **Правка** (из контекстного меню) пункт **Вставить**.

Для выбора сразу нескольких файлов или папок можно отмечать их списком, удерживая при этом клавишу **Ctrl**.

4.5.1.4 Удаление файлов

По умолчанию фалы и папки удаляются в Корзину. Это позволяет восстановить объект при его ошибочном удалении.

Удалить выделенный объект можно из основного меню **Правка** (пункт **Удалить**). Можно использовать контекстное меню, или удалять объекты клавишей **Del**.

При ошибочном удалении можно восстановить объект из корзины. Для этого нужно открыть корзину, вызвать на удаленном файле или папке контекстное меню и в нем выбрать пункт **Восстановить**. Выбор в контекстном меню пункта Удалить окончательно может окончательно удалить ненужный файл или папку, без возможности ее восстановления.

Для того чтобы безвозвратно удалить все содержимое корзины, выберите в контекстном меню корзины пункт Очистить корзину.

4.5.1.5 Открытие файлов

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

Например, при щелчке на файл, являющийся изображением (например, .jpg файл) откроется программа просмотра изображений **Глаз MATE**, в которой откроется изображение. Таким образом, вы можете открывать интересующие вас файлы простым щелчком прямо из файлового менеджера Caja.

Если на компьютере установлено несколько программ для работы с изображениями, то можно запустить нужную, выбрав ее из контекстного меню (щелчок правой кнопкой мыши по файлу, далее **Открыть в другой программе**).

4.5.1.6 Создание ресурсов общего доступа

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

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 и нажать кнопку **Создать публикацию**.

Общие папки будут отображаться в разделе **Просмотреть сеть** файлового менеджера. Также для подключения к общей папке можно указать в адресной строке файлового менеджера протокол и адрес компьютера (**smb://<имя_компьютера>/ или smb:///**) и нажать клавишу **Enter**. Будут показаны ресурсы с общим доступом на данном компьютере.

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**.
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**.

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**.

В результате на боковой панели в разделе **Закладки** появится постоянная ссылка на сетевую папку.

4.6 Графика

ОС Альт Рабочая станция предлагает приложения для работы с растровой и векторной графикой. Ваш выбор зависит как от личных предпочтений, так и от задач, которые вы собираетесь решать, будь то простой просмотр графических файлов или, например, создание профессиональных макетов.

4.6.1 Программа сканирования и распознавания gImageReader

gImageReader программа для распознавания текста (GUI Tesseract).

Особенности gImageReader:

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

gImageReader можно применять без подключенного сканера и распознавать текст из имеющегося снимка.

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.

4.6.2 Глаз MATE

Глаз MATE – программа просмотра изображений.

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

4.7 Прочие приложения

4.7.1 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; o

– браз 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:
– 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.

4.7.1.1 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:

1. В контекстном меню файла/каталога, выбрать пункт **Сжать**.
2. В открывшемся окне необходимо ввести имя архива, выбрать из выпадающего списка тип архива, выбрать место для хранения архива и нажать кнопку **Создать**.

При создании нового архива можно указать дополнительные параметры, раскрыв пункт **Другие параметры** в окне создания архива.

Можно указать следующие дополнительные параметры:
– **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.

Для того чтобы извлечь файлы из архива, следует в контекстном меню архива выбрать пункт **Распаковать сюда** – файлы будут распакованы в текущий каталог, или **Распаковать в...** – можно указать каталог, куда будут извлечены файлы.

4.7.2 Системный монитор

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

Для запуска **Системного монитора** следует выбрать пункт **Меню MATE** > **Приложения** > **Системные** > **Системный монитор MATE**.

Вся информация распределена по четырем вкладкам:

– во вкладке **Система** выводится базовая информация о системе;

– вкладка **Процессы** позволяет просматривать и управлять запущенными процессами. Каждый процесс можно приостановить, остановить, изменить приоритет и выполнить некоторые другие действия;

– во вкладке **Ресурсы** в реальном времени выводится информация о ресурсах (в виде графиков) – использование процессора (CPU), использование оперативной памяти (RAM) и файла подкачки (SWAP), а также использование сети;

– во вкладке **Файловые системы** можно просматривать информацию о файловых системах.

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

Для изменения приоритета процесса необходимо:

1. Выбрать вкладку **Процессы**, чтобы отобразить список процессов;
2. Выбрать процесс, приоритет которого следует изменить.
3. В контекстном меню процесса выбрать пункт **Изменить приоритет**.
4. Если выбрать пункт **Вручную**, откроется диалоговое окно **Изменить приоритет процесса...**.
5. Можно использовать ползунок, чтобы установить уровень приоритета. Приоритет процесса задается уровнем nice. Меньшее значение nice соответствует более высокому приоритету.
6. Нажать кнопку **Изменить приоритет**.

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

4.7.3 Центр приложений

Центр приложений позволяет легко устанавливать и удалять программы, а так же выполнять поиск по названиям и описаниям среди доступных приложений.

Для запуска **Центра приложений** следует выбрать пункт **Меню MATE** > **Системные** > **Центр приложений**.

Вся информация распределена по двум вкладкам:

– на вкладке **Все (Explore)** показаны доступные приложения;

– на вкладке **Установлено** показаны установленные приложения.

На вкладке **Все (Explore)** доступные приложения разбиты на категории. Чтобы найти приложение, следует выбрать категорию приложения, дополнительно внутри группы, в выпадающем списке **Показать** можно выбрать подкатегорию, тем самым сократив, область поиска.

Быстро найти необходимое приложение можно используя поиск. Строка поиска открывается, при нажатии на кнопку  , 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.

Чтобы установить приложение, нужно нажать кнопку **Установить**.

4.7.4 Recoll — полнотекстовый поиск

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

Для запуска Recoll необходимо в Меню MATE выбрать пункт **Приложения** > **Стандартные** > **Recoll**.

4.7.4.1 Индексация файлов

Для поиска требуется предварительная индексация библиотекой Xapian заданных каталогов.

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.

Запустить индексацию можно при первом запуске программы.

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** можно установить каталог верхнего уровня, от которого рекурсивно начнется индексация (по умолчанию это домашний каталог пользователя); указать пути, которые следует пропустить при индексации файлов.

На вкладке **Частные параметры** 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.

Запустить индексацию можно, выбрав в главном меню **Recoll** пункт **Файл** > **Обновить индекс**.

Индексирование Recoll может выполняться в двух основных режимах:

– **Периодическая индексация** – выполняется в определенное 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** пункт **Настройка** > **Расписание индексирования**.

4.7.4.2 Поиск файлов

Recoll имеет два интерфейса поиска:

– Простой поиск – одно поле ввода (по умолчанию на главном экране), в которое можно ввести несколько слов.

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

Выполнение простого поиска:

1. Выбрать, если необходимо поисковый режим: **Любое слово**, **Все слова**, **Имя файла** или **Язык запроса**.
2. Ввести поисковые слова в текстовое поле.
3. Нажать кнопку **Поиск** или **Enter**.

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

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

4.7.4.3 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.

При нажатии ссылки **Просмотр** откроется внутреннее окно предварительного просмотра документа. При нажатии на ссылку **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.

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

По умолчанию Recoll 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**.

При нажатии кнопки **Выбор приложений-редакторов** откроется диалоговое окно, где можно выбрать приложение, которое будет использоваться для открытия каждого MIME-типа.

5 НАСТРОЙКА СИСТЕМЫ

5.1 Центр управления системой

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

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

5.1.1 Применение центра управления системой

Вы можете использовать ЦУС для разных целей, например:

– настройки **Даты и времени** (datetime);

– управления выключением и перезагрузкой компьютера (ahttpd-power, доступно только в вебинтерфейсе);

– управления **Системными службами** (services);

– просмотра **Системных журналов** (logs);

– управления политиками control: **Системные ограничения** (control);

– конфигурирования **Сетевых интерфейсов** (net-eth);

– изменения пароля **Администратора системы (root)** (root);

– создания, удаления и редактирования учетных записей **Пользователей** (users);

– настройки ограничения **Использования диска (квоты)** (quota).

Вы всегда можете воспользоваться кнопкой **Справка**. Все модули ЦУС имеют справочную информацию.

5.1.2 Запуск центра управления системой в графической

Центр управления системой можно запустить следующими способами:

– в графической среде MATE: **Меню MATE** > **Приложения** > **Администрирование** > **Центр управления системой**;

– из командной строки: командой **acc**.

При запуске необходимо ввести пароль администратора системы (root).

После успешного входа можно приступать к настройке системы.

5.1.3 Использование веб-ориентированного центра

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

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

```
# 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, для сервера задан IP-адрес **192.168.0.122**, то интерфейс управления будет доступен по адресу: **https://192.168.0.122:8080**.

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

```
$ ip addr
```

IP-адрес будет указан после слова inet:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
 inet 127.0.0.1/8 scope host lo
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
qlen 1000
 link/ether 60:eb:69:6c:ef:47 brd ff:ff:ff:ff:ff:ff
 inet 192.168.0.150/24 brd 192.168.0.255 scope global eth0
```

Например, тут мы видим, что на интерфейсе enp0s3 задан IP-адрес **192.168.0.150**.

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

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

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

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

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

5.2 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 **Меню MATE** > **Приложения** > **Параметры** > **Запускаемые приложения**.

5.2.1 Вкладка автоматического запуска программ

Список автоматически запускаемых программ представлен на вкладке **Автоматически запускаемые программы**. Этот список содержит краткое описание каждой программы и отметку, указывающую запускать программу или нет.

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

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

1. Нажать кнопку **Добавить**. Откроется окно **Новая автоматически запускаемая программа**.
2. Указать имя программы и команду, которая запустит приложение.
3. Нажать кнопку **Добавить**.

5.2.2 Вкладка настроек сессии

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

5.3 Настройка сети

5.3.1 NetworkManager

Для управления настройками сети в ОС Альт Рабочая станция используется программа **NetworkManager**.

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

NetworkManager доступен как апплет, находящийся в системном лотке.

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

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

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

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

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

В открывшемся окне можно изменить настройки сетевого интерфейса.

NetworkManager под именем **System enp2s0** показывает системное Ethernetсоединение, 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).

5.3.2 Настройка в ЦУС

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

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

5.4 Установка принтера

Перед началом установки убедитесь в том, что в случае локального подключения принтер присоединен к соответствующему порту компьютера и включен, а в случае сетевого подключения принтер корректно сконфигурирован для работы в сети.

5.4.1 Последовательность установки

Настройки принтера можно запустить следующими способами:

– в графической среде MATE: **Меню MATE** > **Приложения** > **Администрирование** > **Параметры печати**;

– из командной строки: командой **system-config-printer**.

Для добавления принтера необходимо нажать кнопку **Добавить**.

В открывшемся окне выберите принтер, который необходимо подключить и нажмите кнопку **Далее**.

В окне **Опишите принтер**, в строке **Имя принтера** при желании измените имя вашего принтера.

После нажатия кнопки **Применить** установка принтера завершена, принтер станет доступным для печати.

Далее вам будет предложена проверка печати. После проверки откроется диалог, в котором при желании вы можете 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**.

5.5 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.

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

Чтобы запустить Grub Customizer, следует выбрать **Меню MATE** > **Приложения** > **Администрирование** > **Grub Customizer**.

Для запуска модуля потребуется ввести пароль пользователя, находящегося в группе wheel.

На вкладке **Просмотреть настройки** показан список возможных вариантов загрузки операционных систем. Здесь можно переименовать, 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.

На вкладке **Настройки оформления** можно менять способы отображения GRUB и внешний вид меню.

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

5.6 Изменение пароля

Пароли пользователей в ОС Альт Рабочая станция первоначально определяет администратор системы при создании учетных записей пользователей.

Однако пользователи имеют возможность в любое время изменить свой пароль. Для запуска утилиты для смены своего пароля, следует выбрать **Меню MATE** > **Приложения** > **Параметры** > **UserPasswd**. Откроется окно, в котором необходимо ввести свой текущий (старый) пароль. Затем следует ввести новый пароль и повторить его.

5.7 Ввод рабочей станции в домен Active Directory

Инструкция по вводу рабочей станции под управлением Альт Рабочая станция в домен Active Directory (работающий под Windows или под Samba AD в режиме DC). Параметры домена:

– TEST.ALT – имя домена;

– TEST – рабочая группа;

– HOST-15 – имя компьютера в Netbios;

– Administrator – имя пользователя-администратора;

– Pa$$word – пароль администратора.

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

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

– В Центре управления системой в разделе **Сеть** > **Ethernet интерфейсы** задать имя компьютера, указать в поле DNS-серверы DNS-сервер домена и в поле Домены поиска – домен для поиска.

– В консоли:

- задать имя компьютера:

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

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

```
nameserver 192.168.0.122
```

где 192.168.0.122 – IP-адрес DNS-сервера домена.

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

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

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

- обновить DNS адреса:

```
# resolvconf -u
```

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

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

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

5.7.2 Ввод в домен

Ввод в домен можно осуществить следующими способами:

– В командной строке:

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

– В Центре управления системой в разделе **Пользователи** > **Аутентификация**:

- в открывшемся окне следует выбрать пункт **Домен Active Directory**, заполнить поля и нажать кнопку **Применить**;
- в открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку **ОК**.
- при успешном подключении к домену, отобразится соответствующая информация.

Перезагрузить рабочую станцию.

5.7.3 Проверка работы

```
# getent passwd ivanov
ivanov:*:1327601105:1327600513:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash
# net ads info
LDAP server: 192.168.0.122
LDAP server name: dc.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
LDAP port: 389
Server time: Чт, 03 июн 2021 13:37:50 EET
KDC server: 192.168.0.122
Server time offset: -1270
Last machine account password change: Чт, 03 июн 2021 13:34:58 EET
# net ads testjoin
Join is OK
```

Вы не увидите пользователей из AD с помощью команды:

```
# getent passwd
```

на клиентской машине. Этот функционал отключен по умолчанию, для того чтобы сократить нагрузку на серверы. Поэтому для проверки необходимо точно указать имя пользователя:

```
# getent passwd <имя_пользователя>
```

Список пользователей можно посмотреть на сервере командой:

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

5.7.4 Вход пользователя

В окне входа в систему необходимо ввести логин учетной записи пользователя домена и нажать кнопку **Войти**. В открывшемся окне ввести пароль, соответствующий этой учетной записи и нажать кнопку **Войти**.

5.7.5 Отображение глобальных групп на локальные

При вводе машины в домен создаются следующие локальные роли:

– роль пользователей (users);

– роль пользователей с расширенными правами (powerusers);

– роль локальных администраторов (localadmins).

Локальные роли users и localadmins назначаются для глобальных групп в домене. Список назначенных ролей и привилегий:

```
# rolelst
domain users:users
domain admins:localadmins
localadmins:wheel,vboxadd,vboxusers
powerusers:remote,vboxadd,vboxusers
users:cdwriter,cdrom,audio,video,proc,radio,camera,floppy,xgrp,scanner,uucp
,
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 введенной в домен добавить роль для данной группы:

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

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

5.7.6 Подключение файловых ресурсов

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

5.7.6.1 Подключение с использованием gio

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

– Установить необходимые пакеты:

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

– Включить пользователя в группу fuse:

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

– Разрешить для всех доступ к fuse под root:

```
# control fusermount public
```

– Войти под доменным пользователем.

– Открыть ресурс в файловом менеджере (например, по адресу smb://server/sysvol). Ресурс смонтирован по пути и **/var/run/<uid_пользователя>/gvfs** или **/var/run/user//gvfs/smb-share:server=сервер,share=ресурс**.

– Другой вариант (полезно для скриптов в автозапуске):

```
gio mount smb://server/sysvol/
```

Если необходимо открывать что-то с ресурса в WINE, в winecfg добавьте диск с путем **/var/run/uid_пользователя/gvfs**.

5.7.6.2 Подключение с использованием pam_mount

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

– Установить pam_mount:

```
# apt-get install pam_mount
```

– Прописать pam_mount в схему /etc/pam.d/system-auth-sss (перед auth substack systemauth-sss-only):

```
auth optional pam_mount.so
```

и в секцию session:

```
session optional pam_mount.so
```

Дополнительно, в секциях auth и session нужно изменить параметр success=4 на success=5, так как изменилась нумерация строк.

– Установить правило монтирования ресурса в файле /etc/security/pam_mount.conf.xml (перед тегом):

```
<volume uid="10000-2000200000" fstype="cifs" server="dc" 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 для доменных пользователей UID (подходит для Winbind и для SSSD);
- server="dc" – имя сервера с ресурсом;
- path="sysvol" – имя файлового ресурса;
- mountpoint="~/share" – путь монтирования в домашней папке пользователя.

Обязательно указывайте настоящее имя сервера в параметре server, а не имя домена.

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" path="sysvol"
mountpoint="~/share"
options="sec=krb5,vers=2.0,cruid=%(USERUID),nounix,uid=%(USERUID),gid=%
(USERGID),file_mode=0664,dir_mode=0775" />
```

Для проверки можно попробовать смонтировать ресурс в сессии:

```
mount.cifs //dc/sysvol /mnt/ -o vers=2.0,user=ivanov
```

Также можно проверить доступность ресурса с помощью smbclient, например:

```
smbclient -L dc -U ivanov -m SMB2
```

5.7.7 Групповые политики

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

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

Инструменты управления групповыми политиками будут установлены в систему, если при установке дистрибутива отметить пункт **Инструменты управления групповыми политиками** (см. документ «Операционная система Альт Рабочая станция. Руководство по установке»).

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:

– установки домашней страницы браузера Firefox/Chromium (экспериментальная политика). Возможно установить при использовании ADMX-файлов Mozilla Firefox (пакет admx-firefox) и Google Chrome (пакет admx-chromium) соответственно;
– установки запрета на подключение внешних носителей;
– управления политиками control (реализован широкий набор настроек). Возможно установить при использовании ADMX-файлов ALT;
– включения или выключения различных служб (сервисов systemd). Возможно установить при использовании ADMX-файлов ALT;
– подключения сетевых дисков (экспериментальная политика); генерирования (удаления/замены) ярлыков для запуска программ;
– создания каталогов;
– установки и удаления пакетов (экспериментальная политика).

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

5.7.7.1 Развертывание групповых политик

Процесс развертывание групповых политик:

1. Развернуть сервер Samba AD DC (например, на машине с установленной ОС Альт Рабочая станция).
2. Установить административные шаблоны на сервере Samba AD DC:
   – 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:

```
# 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 <admxmsi-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 рабочие станции в домен Active Directory и (см. Ввод рабочей станции в домен Active Directory).

Должен быть установлен пакет alterator-gpupdate: # apt-get install alterator-gpupdate

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

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

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

4. На рабочей станции, введенной 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:
   – ввести машину с ОС Windows в домен (управление сервером Samba с помощью RSAT поддерживается из среды до Windows 2012R2 включительно);
   – включить компоненты удаленного администрирования (этот шаг можно пропустить, если административные шаблоны были установлены на контроллере домена). Для задания конфигурации с помощью RSAT необходимо установить административные шаблоны (файлы ADMX) и зависящие от языка файлы ADML из репозитория http://git.altlinux.org/gears/a/admx-basealt.git (https://github.com/altlinux/admx-basealt) и разместить их в каталоге: \\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\PolicyDefinitions;

– корректно установленные административные шаблоны будут отображены на машине Windows в оснастке **Редактор управления групповыми политиками** в разделе **Конфигурация компьютера** > **Политики** > **Административные шаблоны** > **Система ALT**.

5.7.7.2 Пример создания групповой политики

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

В ADMC на рабочей станции, введенной в домен или в оснастке **Active Directory – пользователи и компьютеры** создать подразделение (OU) и переместить в него компьютеры и пользователей 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 MATE** > **Системные** > **ADMC**) или командой admc:

```
$ admc
```

Добавление доменных устройств в группу членства GPO:

1. Создать новое подразделение:
   – в контекстном меню домена выбрать пункт **Создать** > **Подразделение**:
   – в открывшемся окне ввести название подразделения (например, OU) и нажать кнопку **ОК**.

2. Переместить компьютеры и пользователей домена в созданное подразделение:
   – в контекстном меню пользователя/компьютера выбрать пункт **Переместить…** ;
   – в открывшемся диалоговом окне **Выбор контейнера – ADMC** выбрать контейнер, в который следует переместить учетную запись пользователя.

Создание политики для подразделения:

1. В контекстном меню папки **Объекты групповой политики** выбрать пункт **Создать политику**.

2. В открывшемся окне ввести название политики и нажать кнопку **ОК**.
3. В контекстном меню политики выбрать пункт **Добавить связь…**.
4. Выбрать объекты, которые необходимо связать с политикой и нажать кнопку **ОК**.

Для редактирования настроек групповой политики, необходимо выполнить следующие действия:

1. В контекстном меню созданной политики выбрать пункт **Изменить…**.
2. Откроется окно редактирования групповых политик (GPUI):
3. Перейти в **Компьютер** > **Система ALT**. Здесь есть несколько разделов, соответствующих категориям control. Выбрать раздел **Сетевые приложения**, в правом окне редактора отобразится список политик.
4. Дважды 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**.
5. После обновления политики на клиенте, выполнять команду ping сможет только администратор:

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

В настоящее время GPUI позволяет управлять только политиками, предпочтения пока не реализованы. Для управления предпочтениями могут использоваться средства удаленного администрирования сервера для Windows (RSAT).

Пример создания групповой политики на машине с ОС Windows:

1. На машине с установленным RSAT открыть оснастку **Управление групповыми политиками** (gpmc.msc).
2. Создать новый объект групповой политики (GPO) и связать его с подразделением (OU), в который входят машины или учетные записи пользователей.

3. В контекстном меню GPO, выбрать пункт **Изменить…**. Откроется редактор GPO.
4. Перейти в **Конфигурация компьютера** > **Политики** > **Административные шаблоны** > **Система ALT**. Здесь есть несколько разделов, соответствующих категориям control. Выбрать раздел **Сетевые приложения**, в правом окне редактора отобразится список политик.
5. Дважды щелкнуть левой кнопкой мыши на политике **Разрешения для /usr/bin/ping**. Откроется диалоговое окно настройки политики. Выбрать параметр **Включить**, в выпадающем списке **Кому разрешено выполнять** выбрать пункт **Только root** и нажать кнопку **Применить**.

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.

5.7.8 Ввод рабочей станции в домен FreeIPA

Инструкция по вводу рабочей станции под управлением Альт Рабочая станция в домен FreeIPA.

5.7.8.1 Установка FreeIPA клиента

Установить необходимые пакеты:

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

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

5.7.8.2 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:

1. В Центре управления системой в разделе **Сеть** > **Ethernet интерфейсы** задать имя компьютера, IP-адрес FreeIPA сервера и в поле **Домены поиска** – домен для поиска.
2. В консоли:

   – задать имя компьютера:

```
# hostnamectl set-hostname comp01.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
```

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

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

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

5.7.8.3 Подключение к серверу в ЦУС

Для ввода рабочей станции в домен FreeIPA, необходимо в Центре управления системой перейти в раздел **Пользователи** > **Аутентификация**.

В открывшемся окне следует выбрать пункт **Домен FreeIPA**, заполнить поля **Домен** и **Имя компьютера**, затем нажать кнопку **Применить**.

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

В случае успешного подключения, будет выведено соответствующее сообщение.

Перезагрузить рабочую станцию.

5.7.8.4 Подключение к серверу в консоли

Запустить скрипт настройки клиента в пакетном режиме:

```
# ipa-client-install -U -p admin -w 12345678
```

или интерактивно:

```
# ipa-client-install
```

Если все настроено, верно, скрипт должен выдать такое сообщение:

```
'''Discovery was successful!'''
Client hostname: comp01.example.test
Realm: EXAMPLE.TEST
DNS Domain: example.test
IPA Server: ipa.example.test
BaseDN: dc=example,dc=test
Continue to configure the system with these values? [no]:
```

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

Если при входе в домен возникает такая ошибка:

```
Hostname (comp01.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
```

5.7.8.5 Вход пользователя

В окне входа в систему 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, затем у пользователя запрашивается новый пароль и его подтверждение.

6 СРЕДСТВА УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ

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

6.1 Вход в систему

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

6.2 Обслуживание компьютера под управлением ОС Альт Рабочая станция

6.2.1 Мониторинг состояния системы

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

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

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

6.2.2 Системные службы

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

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

6.2.3 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 сохранен при обновлении системы.

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

Для переключения состояния следует выбрать режим и нажать кнопку **Сохранить**.

6.2.4 Обновление системы

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

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

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

Процесс обновления системы будет запускаться автоматически согласно заданному расписанию.

6.2.5 Обновление систем, не имеющих выхода в Интернет

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

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

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

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

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

При выборе любой архитектуры также будет добавлен источник с noarch.

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

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

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.

2. **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 нем **Обновление системы управляемое сервером**.

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

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

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

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

6.2.5.1 Настройка веб-сервера

Установить веб-сервер (в данном примере nginx):

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

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

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

  access_log /var/log/nginx/repo-access.log;
  error_log /var/log/nginx/repo-error.log;
  location /mirror {
    root /srv/public;
    autoindex on;
  }
}
```

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

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

Запустить nginx и добавить его в автозагрузку:

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

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

```
# apt-repo rm all # apt-repo add http:///mirror/p10/branch
```

Проверить правильность настройки репозиториев:

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

6.2.5.2 Настройка FTP-сервера

Установить, настроить и запустить сервер 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
```

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:///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
```

6.2.6 Локальные учётные записи

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

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

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

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

Профиль киоска – файл **.desktop** (обычно из **/usr/share/applications**), размещаемый в каталог **/etc/kiosk**.

Для создания профиля можно просто скопировать файл **.desktop** (например, **firefox.desktop**) из **/usr/share/applications**, в каталог **/etc/kiosk**, но лучше создать свой desktop-файл и скрипт, содержащий требуемое ПО.

Пример настройки режима «киоск»:

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 учетные 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**.

6.2.7 Администратор системы

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

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

6.2.8 Дата и время

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

Системное время зависит от следующих факторов:

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

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

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

6.2.9 Ограничение использования диска

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

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

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

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

При задании ограничений различают жесткие и мягкие ограничения:

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

Значение 0 при задании ограничений означает отсутствие ограничений.

6.2.10 Выключение и перезагрузка компьютера

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

Модуль **Выключение компьютера** позволяет:

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

Возможна настройка ежедневного применения данных действий в заданное время.

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

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

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

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

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

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

```
Tue Jun 16 11:46:59 EET 2022: The server.test.alt is about to start.
```

При выключении:

```
Tue Jun 16 12:27:02 EET 2022: The server.test.alt is about to shutdown.
```

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

6.3 Конфигурирование сетевых интерфейсов

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

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

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

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

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

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

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

– **IP** – ввести IP-адрес вручную и выбрать в выпадающем поле предпочтительную маску сети, затем нажать 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 DNSсерверов, которые будут получать информацию о доменах, выполнять маршрутизацию почты и управлять обслуживающими узлами для протоколов в домене;

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

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

В случае наличия DHCP-сервера можно все вышеперечисленные параметры получить автоматически – выбрав в списке Конфигурация пункт Использовать DHCP.

Если в компьютере имеется несколько сетевых карт, то возможна ситуация, когда при очередной загрузке ядро присвоит имена интерфейсов (enp0s3, enp0s8) в другом порядке. В результате интерфейсы получат не свои настройки. Чтобы этого не происходило, можно привязать интерфейс к имени по его аппаратному адресу (MAC) или по местоположению на системной шине.

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

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

1. **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>.

2. **NetworkManager (etcnet)**

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

3. **NetworkManager (native)**

В данном режиме управление настройками интерфейса передается **NetworkManager** и не зависит от файлов Etcnet. Управлять настройками можно через графический интерфейс NetworkManager.

Файлы с настройками находятся в директории **/etc/NetworkManager/system-connections**. Этот режим особенно актуален для задач настройки сети на клиенте, когда IP-адрес 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.

4. **Не контролируется**

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

6.4 Сетевая установка операционной системы

Одной из удобных возможностей Альт Рабочая станция при разворачивании инфраструктуры является сетевая установка. При помощи сетевой установки можно производить установку Альт Рабочая станция не с DVD-диска, а загрузив инсталлятор по сети.

6.4.1 Подготовка сервера

Перед началом установки рабочих станций следует произвести предварительную настройку сервера: задать имя сервера (модуль **Ethernet-интерфейсы в ЦУС**), включить DHCP-сервер, задать имя домена (модуль **Домен**).

При сетевой установке с сервера будут переняты настройки домена, и включена централизованная аутентификация. Если вы устанавливаете ОС 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 Альт Рабочая станция, предварительно вставив его в DVD-привод сервера, либо используя образ диска, расположенный на файловой системе на сервере. Можно также использовать URL вида:
http://ftp.altlinux.org/pub/distributions/ALTLinux/images/p10/workstation/x86_64/alt-workstation-10.0- x86_64.iso

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

В разделе **Сервер сетевых установок** (пакет alterator-netinst), укажите откуда импортировать новый образ и нажмите кнопку **Добавить**.

Процесс добавления образа занимает какое-то время. Пожалуйста, дождитесь окончания этого процесса.

После добавления образа он появится в списке **Доступные образы дисков**. Необходимо выбрать из списка один из образов и нажать кнопку **Выбрать**.

На этом подготовка сервера к сетевой установке рабочих станций завершена.

Далее следует выбрать направление соединения. Удаленный доступ к компьютеру может быть 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-приемник соединений задается IP-адресом или именем.

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 удаленно, отметьте пункт **Включить установку по VNC** и пункт **Подключение со стороны VNC** сервера раздела **Направление соединения**, и там укажите адрес компьютера, с которого будет происходить управление. Для приема подключения можно запустить, например, vncviewer **-listen**.

Не забудьте отключить сетевую установку по окончании процесса установки ОС на рабочих станциях. Это можно сделать, выбрав в списке **Доступные образы дисков** пункт **Нет образа** и подтвердив действие нажатием кнопки **Выбрать**.

За дополнительной информацией по настройке обращайтесь к встроенной справке соответствующих модулей **Центра управления системой**.

6.4.2 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".

Некоторые материнские платы позволяют выбрать источник загрузки во время включения компьютера. Эта возможность может называться, например, "Select boot device" или "Boot menu".

Последовательность установки при установке с DVD-диска и при сетевой установке не отличаются друг от друга. Обратитесь к документу «Операционная система Альт Рабочая станция. Руководство по установке».

6.5 Соединение удалённых офисов (OpenVPN-сервер)

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

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

6.5.1 Настройка OpenVPN-сервера

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

Используя модуль OpenVPN-сервер можно:

– включить/отключить OpenVPN-сервер;

– настроить параметры сервера: тип, сети сервера, использование сжатия и т.д.;

– управлять сертификатами сервера;

– настроить сети клиентов.

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

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

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

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

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

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

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

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

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**.

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

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

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

Появится сообщение: «Сертификат УЦ успешно загружен».

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

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

6.5.2 Настройка клиентов

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

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

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

Помимо этого нужно подписать ключ **openvpn** в модуле **Удостоверяющий Центр** (пакет alterator-ca) из раздела **Система**.

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

– Состояние – «запустить»;

– Сервер – IP адрес сервера или домен;

– Порт – 1194;

– Ключ – выбрать подписанный на сервере ключ.

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

Проверить, появилось ли соединение с сервером можно командой:

```
ip addr
```

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

```
tun1: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UNKNOWN qlen 100
    link/[none]
    inet 10.8.0.6 peer 10.8.0.5/32 scope global tun0
```

6.6 Доступ к службам сервера из сети Интернет

6.6.1 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, вы делаете их доступными для соединений на внешних сетевых интерфейсах. Если вы хотите предоставить доступ к службе, отсутствующей в списке, задайте используемые этой службой порты в соответствующих полях.

Можно выбрать один из двух режимов работы:

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

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.

За дополнительной информацией по настройке обращайтесь к встроенной справке модуля ЦУС.

6.6.2 Список блокируемых хостов

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

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

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

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

6.7 Прочие возможности ЦУС

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

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

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

Прочие пакеты для ЦУС можно найти, выполнив команду:

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

Модули можно дополнительно загружать и удалять как обычные программы:

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

6.8 Права доступа к модулям

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

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

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

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

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

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

7 ФУНКЦИОНАЛ ОПЕРАЦИОННОЙ СИСТЕМЫ

7.1 ГОСТ в OpenSSL

7.1.1 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
```

7.1.2 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
```

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

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

7.2.1 Задание хешей паролей в ЦУС

Для измения типа хеша по умолчанию на ГОСТ Р 34.11-2012 необходимо в Центре управления системой перейти в раздел **Система** > **Настройки безопасности**.

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**.

Проверить настройку можно, установив новый пароль пользователю и выполнив команду:

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

7.2.2 Задание хешей паролей 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
```

7.3 Подпись и проверка ЭЦП ГОСТ

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

– создание электронной подписи (отсоединенной и присоединенной);

– создание электронной подписи в zip-контейнере; п

– проверка электронной подписи;

– просмотр содержимого zip-контейнера с документом и электронной подписью.

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

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

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

7.3.1 Запуск

Запустить **ALT CSP КриптоПро можно**:

– из меню рабочей среды: **Меню MATE** > **Системные** > **ALT CSP КриптоПро**;

– из контекстного меню файла в файловом менеджере Caja (**Действия** > **Caja-Actions actions**).

Для возможности запуска **ALT CSP КриптоПро** из контекстного меню файла должен быть установлен пакет mate-file-manager-actions.

– из командной строки:

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

7.3.2 Создание электронной подписи

7.3.2.1 Отсоединённая подпись

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**, в разделе **Документ** нажать кнопку **Выбрать** и выбрать электронный документ. Нажав кнопку **Просмотреть**, можно просмотреть содержимое электронного документа.

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

Далее следует выбрать сертификат, которым будет подписан документ.

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.

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.

7.3.2.2 Присоединённая подпись

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**. В том же каталоге, в котором хранился исходный документ, появится файл, содержащий как саму электронную подпись, так и исходный документ (в данном примере **21-10-21_10-58-22_test.pdf.p7b**).

Пример извлечения файла с данными из файла электронной подписи:

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

файл test_new.pdf будут извлечены данные.

7.3.3 Проверка электронной подписи

Проверка электронной подписи выполняется во вкладке **Проверка**.

7.3.3.1 Отсоединённая подпись

Для проверки отсоединенной электронной 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**.

Если программа ALT CSP КриптоПро была запущена из контекстного меню файла, документ будет выбран автоматически. Если программа была запущена из контекстного меню файла электронной подписи, подпись и документ будут выбраны автоматически.

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

7.3.3.2 Присоединённая подпись

Для проверки присоединенной электронной подписи необходимо выбрать подписанный электронный документ и нажать кнопку **Проверить**.

7.4 Управление шифрованными разделами

Зашифрованный раздел может быть создан, например, при установке системы см. документ «Операционная система Альт Рабочая станция. Руководство по установке».

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 изменен или удален необратимо.

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

Просмотреть текущее состояние всех слотов:

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

где /dev/sdb1 – шифрованный раздел.

Определить является ли устройство LUKS-разделом:

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

Определить какой раздел является шифруемым:

```
# 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:
```

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

Сброс забытого пароля на зашифрованный раздел:

1. Получить зашифрованные пароли всех разделов:

```
# dmsetup table --showkey
luks-7853363d-e7e2-1a42-b5b9-0af119e19920: 0 37730304 crypt aes-
cbcessiv: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-
cbcessiv: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:
```

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

7.5 Создание ssh-туннелей

В разделе рассмотрено создание ssh-туннелей, использующих контроль целостности заголовков IP-пакетов в соответствии с ГОСТ Р 34.12-2015.

7.5.1 Настройка сервера ssh

Должна быть включена Поддержка шифрования по ГОСТ в OpenSSL.

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 или в командной строке, например

```
# apt-repo add rpm [p10] http://mirror.yandex.ru/altlinux/ p10/branch/
x86_64 gostcrypto
```

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

Установить пакеты:

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

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
```

7.5.2 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
127.0.0.1:2222:127.0.0.1:22
```

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

```
$
ssh <пользователь>@127.0.0.1 -p 2222 -oCiphers=grasshopper-ctr@altlinux.org
- oMACs=grasshopper-mac@altlinux.org,hmac-streebog-512@altlinux.org
```

7.6 Создание защищенных VPN-туннелей

В разделе рассмотрено 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
```

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 или в командной строке, например

```
# apt-repo add rpm [p10] http://mirror.yandex.ru/altlinux/ p10/branch/
x86_64 gostcrypto
```

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

7.6.1 Настройка в ЦУС

Выполнить настройку сервера OpenVPN-сервера.

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)**.

На стороне клиента, необходимо указать алгоритмы шифрования, такие же как и на стороне сервера.

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 Channel: 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 Channel: 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 Channel: Using 128 bit message hash 'grasshopper-mac' for MAC
authentication Настрой-ка OpenVPN-сервера
```

7.6.2 Настройка в командной строке

7.6.2.1 Создание ключей для OpenVPN туннеля средствами утилиты openssl

Для генерации всех необходимых ключей и сертификатов необходимо выполнить следующие действия:

1. Изменить значение параметра policy в файле /var/lib/ssl/openssl.cnf для возможности подписывать любые сертификаты:

```
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 ключ и запрос на сертификат для клиента:

```
# 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, client.crt, client.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.

7.6.2.2 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.

Каждый файл конфигурации по маске **/etc/openvpn/*.conf** является конфигурацией отдельного экземпляра демона openvpn.

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.

Пример конфигурации:

```
# 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
```

7.6.2.3 Настройка VPN-подключения по протоколу OpenVPN в Network

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**.
2. В списке выбора типа соединения выбрать пункт **OpenVPN** и нажать кнопку **Создать**.

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.

3. Указать IP-адрес OpenVPN сервера, сертификат УЦ, приватный ключ и сертификат пользователя.
4. Нажать кнопку **Дополнительно**, чтобы указать параметры подключения. Настройки соединения находятся на разных вкладках, например на вкладке **Защита** можно указать алгоритм шифрования:
5. Сохранить сделанные изменения, нажав кнопку **ОК** и затем **Сохранить**.
6. Выполнить подключение.

Выполнить настройку OpenVPN клиента можно также в командной строке. Для этого:

1. Скопируйте файл **/usr/share/doc/openvpn-gostcrypto-2.4.9/client.conf** в каталог **/etc/openvpn/**.
2. Скопируйте ранее сгенерированные ключи и сертификаты в каталог **/etc/openvpn/keys/** и укажите их в /**etc/openvpn/client.conf**.
3. В файле **/etc/openvpn/client.conf** в поле remote укажите IP-адрес OpenVPN сервера, другие параметры приведите 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
```

4. Запустите клиент OpenVPN:

```
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
```

7.7 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 директорию **/mnt/filesystem**, в которую будет монтироваться раздел:

```
# mkdir /mnt/filesystem
```

4. Отформатировать раздел в проверяемую файловую систему:
   – для ext2:

```
# mkfs.ext2 /dev/vdc1
```

   – для ext3:

```
# mkfs.ext3 /dev/vdc1
```

   – для ext4:

```
# mkfs.ext4 /dev/vdc1
```

– для fat16:

```
# mkfs.fat -F 16 /dev/vdc1
```

– для fat32:

```
# mkfs.fat -F 32 /dev/vdc1
```

– для ntfs:

```
# mkfs.ntfs /dev/vdc1
```

– для iso9660 –создать iso-файл из каталога /etc:

```
# mkisofs -r -jcharset koi8-r -o /root/cd.iso /etc
```

5. Для проверки поддержки файловых систем ext2, ext3, ext4, fat16, fat32, ntfs:
   – примонтировать раздел с файловой системой в каталог **/mnt/filesystem**:

```
# mount /dev/vdc1 /mnt/filesystem
```

– проверить возможность записи файла на текущую файловую систему:

```
# echo test_content > /mnt/filesystem/test.fs
```

проверить командой:

```
# ls -l /mnt/filesystem/test.fs
-rw-r--r--. 1 root root 13 май 23 20:10 /mnt/filesystem/test.fs
```

– проверить возможность чтения файла с текущей файловой системой:

```
# cat /mnt/filesystem/test.fs
```

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

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

7.8 Поддержка сетевых протоколов

7.8.1 Протокол 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.

7.8.1.1 Настройка Samba

Samba настраивается с помощью конфигурационного файла **/etc/samba/smb.conf**.

После редактирования файла **smb.conf**, запускайте команду **testparm** для проверки файла на синтаксические ошибки.

7.8.1.1.1 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.
```

7.8.1.1.2 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
```

7.8.1.1.3 Создание ресурсов общего доступа от имени пользователя

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

7.8.1.2 Настройка клиента

7.8.1.2.1 Подключение по протоколу SMB в графической среде

Для создания подключения по протоколу SMB в графической среде MATE можно, запустить файловый менеджер, указать в адресной строке протокол и адрес сервера. Нажать клавишу **Enter**. Будут показаны ресурсы с общим доступом.

Для доступа к папке, необходимо указать имя пользователя, пароль и нажать кнопку **Подключиться**.

7.8.1.2.2 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 -Uuser_samba
Enter TEST\user_samba's password:
           Sharename  Type    Comment
           ---------  ----    -------
           public     Disk    Public
           IPC$       IPC     IPC Service (Samba Server Version 4.14.7)
           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/sambacreds**, надо установить так, чтобы файл был доступен на чтение и запись только пользователю-владелецу файла:

```
# chmod 600 /etc/samba/sambacreds
```

и принадлежать root:

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

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

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

Например:

```
//192.168.0.131/public /mnt/server_public cifs
users,_netdev,xsystemd.automount,credentials=/etc/samba/sambacreds 0 0
```

7.8.2 Протокол NFS

7.8.2.1 Настройка сервера NFS

Должен быть установлен пакет nfs-server:

```
# apt-get install nfs-server
```

Пакет nfs-server не входит в состав ISO-образа дистрибутива, его можно установить из репозитория p10. О добавлении репозиториев с использованием графических приложений вы можете почитать в документе «Операционная система Альт Рабочая станция. Руководство по установке».

Запустить NFS-сервер и включить его по умолчанию:

```
# systemctl enable --now nfs
```

В файле /etc/exports следует указать экспортируемые каталоги (каталоги, которые будет разрешено монтировать с других машин):

```
/mysharedir ipaddr1(rw)
```

Например, 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
```

7.8.2.2 Использование NFS

Подключение к NFS-серверу можно производить как вручную, так и настроив автоматическое подключение при загрузке. Для ручного монтирования необходимо:

1. Создать точку монтирования:

```
# mkdir /mnt/nfs
```

2. 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 удаленный каталог.

3. 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,xsystemd.automount 0 0
```

Прежде чем изменять **/etc/fstab**, попробуйте смонтировать вручную и убедитесь, что все работает.

7.8.3 Протокол FTP

7.8.3.1 Настройка сервера FTP

Установить пакеты vsftpd и anonftp:

```
# apt-get install vsftpd anonftp
```

Пакеты vsftpd и anonftp не входят в состав ISO-образа дистрибутива, их можно установить из репозитория p10.

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

```
local_enable=YES
chroot_local_user=YES
local_root=/var/ftp/
```

Запустить vsftpd:

```
# systemctl start 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
```

7.8.3.2 Подключение рабочей станции

Для создания подключения по протоколу FTP в графической среде MATE можно запустить файловый менеджер, указать в адресной строке протокол и адрес сервера. Нажать клавишу **Enter**. В появившемся окне указать имя пользователя, пароль и нажать кнопку **Подключиться**.

Должен отобразиться список файлов каталога **/var/ftp/**, расположенного на сервере FTP:

7.8.4 Протокол NTP

7.8.4.1 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;

– chronyc – утилита командной строки для контроля и мониторинга программы. Утилита используется для тонкой настройки различных параметров демона, например позволяет добавлять или удалять серверы времени.

Выполнить настройку NTP-сервера можно следующими способами:

– В ЦУС настроить модуль **Дата и время** на получение точного времени с NTP сервера и работу в качестве NTP-сервера и нажать кнопку **Применить**.

– Указать серверы NTP в директиве server или pool в файле конфигурации NTP **/etc/chrony.conf**:

```
allow all #Разрешить NTP-клиенту доступ из локальной сети
pool pool.ntp.org iburst #параметр iburst используется для ускорения
начальной синхронизации
```

и перезапустить сервис командой:

```
# systemctl restart chronyd
```

Убедиться в нормальной работе NTP-сервера, выполнив команду:

```
# systemctl status chronyd.service
```

7.8.4.2 Настройка рабочей станции

Настроить модуль Дата и время на получение точного времени с NTP-сервера (в качестве NTPсервера указать IP-адрес сервера NTP) и нажать кнопку **Применить**.

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
```

7.8.5 Протокол HTTP(S)

7.8.5.1 Настройка сервера HTTP

Установить пакет apache2-base:

```
# apt-get install apache2-base
```

Пакет apache2-base не входит в состав ISO-образа дистрибутива, его можно установить из репозитория p10.

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
```

7.8.5.2 Настройка рабочей станции

Запустить браузер, перейти по адресу http://<ip-сервера>.

Также можно выполнить команду:

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

Происходит обращение к серверу и получение данных по протоколу http.

7.9 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).

Должен быть установлен пакет onboard:

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

7.9.1 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 щелкнуть значок человека на верхней панели, а затем отметить пункт **Экранная клавиатура**.

На экране появится виртуальная клавиатура, ее можно использовать для ввода имени пользователя и пароля.

7.9.2 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"
```

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 в /etc/dconf/db/local.d/00_screensaver следующего содержания:

```
[org/mate/screensaver]
embedded-keyboard-enabled=true
embedded-keyboard-command="onboard --xid"
```

4. Обновить системные базы данных, выполнив команду:

```
# dconf update
```

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

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

В результате при разблокировке экрана появится виртуальная клавиатура, ее можно использовать для ввода пароля.

7.9.3 Настройки onboard

Onboard имеет множество настроек, сворачивается в системный трей и/или в «индикатор действия», имеет несколько тем оформления, с возможностью настройки цвета и формы клавиш (можно создать собственную тему полностью), прозрачности, включения/выключения рамки окна.

Запустить виртуальную клавиатуру Onboard можно, выбрав пункт: **Меню MATE** > **Приложения** > **Стандартные** > **Onboard**.

Окно настроек Onboard можно открыть, нажав правой клавишей мыши по значку Onboard в системном трее и выбрав пункт **Параметры**.

В настройках можно:

– подобрать стилевое оформление экранной клавиатуры; з
– акрепить к верхнему или нижнему краю экрана рабочего стола;
– включить или отключить звук нажатых клавиш, а также показывать нажатые клавиши;
– изменить раскладку клавиатуры (например, выбрать эргономичную клавиатуру или клавиатуру для небольших экранов).

7.10 Настройка мультитерминального режима

Модуль **Настройка нескольких рабочих мест** – графическое средство настройки мультитерминального режима, позволяющего обеспечить одновременную работу нескольких пользователей на одном компьютере.

Модуль **Настройка нескольких рабочих мест** доступен в Центре управления системой (раздел **Система**).

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**. Это рабочее место нельзя удалить или изменить.

В списке **Рабочие места** перечислены дополнительные рабочие места (если они есть), в скобках приводится количество подключенных к данному месту устройств. Чтобы просмотреть устройства, подключенные к дополнительному рабочему месту, необходимо выделить его в списке **Рабочие места**, устройства будут показаны в списке **Устройства рабочего места**.

Для создания дополнительного рабочего места следует 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**.

Имя рабочего места может содержать только символы a-z, A-Z, 0-9, "-" и "_" и должно начинаться с префикса seat. По умолчанию будут сгенерированы имена: seat1, seat2 и т.д.

Выделить нужное рабочее место в списке **Рабочие места**, а в списке **Устройства seat0** выбрать устройство, которое будет назначено выбранному рабочему месту. Нажать кнопку **Добавить**. Устройство появится в списке устройств выбранного рабочего места. Выделить дополнительному рабочему месту видеокарту, клавиатуру и мышь.

Основную видеокарту нельзя переключать на другие рабочие места.

Аналогичным образом настроить все рабочие места.

Для подключения назначенных устройств к дополнительным рабочим местам необходимо нажать кнопку **Применить**. Чтобы настройки вступили в силу необходимо перезагрузить компьютер.

Если после перезагрузки на мониторы не выводится никакая информация, это означает, что «закрепленная» за seat0 видеокарта была передана на другое рабочее место. Чтобы исправить данную проблему необходимо сбросить настройки. Для этого следует залогиниться во второй текстовой консоли, удалить дополнительные рабочие места, выполнив команду (от root):

```
# loginctl flush-devices
```

И перезагрузить компьютер.

8 ОГРАНИЧЕНИЕ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ

8.1 Ограничение полномочий пользователей

8.1.1 Ограничение полномочий пользователей по использованию консолей

8.1.1.1 Настройка ограничения в ЦУС

Модуль Центра управления системой **Блокировка терминала** позволяет ограничить определенным пользователям возможность использования определенных TTY. Модуль является интерфейсом для файла конфигурации **/etc/security/access.conf**.

Должен быть установлен пакет alterator-secsetup:

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

Для каждого отдельного пользователя системы можно заблокировать любые необходимые TTY, для этого в окне **Список TTY** необходимо отметить консоли, которые должны быть заблокированы для данного пользователя, перенести их в окно **Заблокированные TTY** и нажать кнопку **Применить**.

8.1.1.2 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**.

Формат файла /etc/security/access.conf:

```
permission:users:origins
```

где:

– permission – знак «+» (плюс) – предоставление доступа, или знак «-» (минус) – отказ в доступе;

– users – список пользователей или групп пользователей или ключевое слово ALL;

– origins – список TTY (для локального доступа), имен хостов, доменных имен, IPадресов, ключевое слово ALL или LOCAL.

Чтобы ограничить доступ для всех пользователей, кроме пользователя root, следует внести следующие изменения:

```
# vim /etc/security/access.conf
-:ALL EXCEPT root: tty2 tty3 tty4 tty5 tty6
```

Доступ может быть ограничен для конкретного пользователя:

```
# vim /etc/security/access.conf
-:user: tty2 tty3 tty4 tty5 tty6
```

Доступ может быть ограничен для группы, содержащей несколько пользователей:

```
# vim /etc/security/access.conf
-:group: LOCAL
```

Далее необходимо сконфигурировать стек PAM для использования модуля **pam_access.so** для ограничения доступа на основе ограничений, определенных в файле **/etc/security/access.conf**. Для этого дописать в файл **/etc/pam.d/system-auth-local-only** строку account required pam_access.so после строки account required pam_tcb.so:

```
auth            required  pam_tcb.so shadow fork nullok
account         required  pam_tcb.so shadow fork
account         required  pam_access.so
password        required  pam_passwdqc.so config=/etc/passwdqc.conf
password        required  pam_tcb.so use_authtok shadow fork nullok
write_to=tcb
session required pam_tcb.so
```

8.1.2 Ограничение числа параллельных сеансов доступа

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.

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.

Элементом ограничения (item) может быть:

– core – ограничение размера файла core (Кбайт);

– data – максимальный размер данных (Кбайт);

– fsize – максимальный размер файла (Кбайт);

– memlock – максимальное заблокированное адресное пространство (Кбайт);

– nofile – максимальное число открытых файлов;

– stack – максимальный размер стека (Кбайт);

– cpu – максимальное время процессора (минуты);

– nproc – максимальное число процессов;

– as – ограничение адресного пространства;

– maxlogins – максимальное число одновременных регистраций в системе;

– locks – максимальное число файлов блокировки.

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 регистрации шестнадцатый пользователь увидит сообщение:

```
There were too many logins for ' group1'.
```

Следующая запись ограничит число параллельных сеансов доступа для каждой учетной записи пользователей:

```
* - maxlogins 5
```

Ограничения также можно настраивать в Центре управления системой (раздел **Система** > **Настройки ограничений**).

Для этого необходимо установить пакет alterator-limits (из репозитория p10):

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

8.2 Блокировка макросов в приложениях

Для того чтобы включить блокировку макросов в приложениях необходимо в Центре управления системой перейти в раздел **Система** > **Настройки безопасности**.

Должен быть установлен пакет alterator-secsetup:

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

В открывшемся окне следует отметить пункт **Блокировать макросы** приложений и нажать кнопку **Применить**. Макросы будут заблокированы.

8.3 Модуль AltHa

AltHa – это модуль безопасности Linux, который в настоящее время имеет три варианта защиты пользовательского пространства:

– игнорировать биты SUID в двоичных файлах (возможны исключения);

– запретить запуск выбранных интерпретаторов в интерактивном режиме;

– отключить возможность удаления открытых файлов в выбранных каталогах.

Для включения модуля AltHa необходимо передать ядру параметр altha=1. Для этого в файле **/etc/sysconfig/grub2** в строке GRUB_CMDLINE_LINUX_DEFAULT следует добавить опцию: altha=1. Например:

```
# vim /etc/sysconfig/grub2
...
GRUB_CMDLINE_LINUX_DEFAULT='vga=0x314 quiet resume=/dev/disk/by-uuid/
187504b7-7f78-486d-b383-1b638370d3eb panic=30 splash altha=1'
```

Обновить загрузчик, выполнив команду:

```
# update-grub
```

Перезагрузить систему.

Данную настройку можно также выполнить в модуле Настройка загрузчика GRUB2.

8.3.1 Запрет бита исполнения (SUID)

При включенном подмодуле altha.nosuid, биты SUID во всех двоичных файлах, кроме явно перечисленных, игнорируются в масштабе всей системы.

8.3.1.1 Отключение влияния бита SUID в ЦУС

Для включения запрета бита исполнения необходимо в Центре управления системой перейти в раздел **Система** > **Настройки безопасности**.

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**.

Исключения это список включенных двоичных файлов SUID, разделенных двоеточиями.

8.3.1.2 Отключение влияния бита SUID в консоли

Для включения запрета бита исполнения следует установить значение переменной kernel.altha.nosuid.enabled равным 1:

```
# sysctl -w kernel.altha.nosuid.enabled=1
```

И добавить, если это необходимо, исключения (список включенных двоичных файлов SUID, разделенных двоеточиями), например:

```
# sysctl -w kernel.altha.nosuid.exceptions="/bin/su:/usr/libexec/hasher-
priv/
hasher-priv"
```

Проверка состояния режима запрета бита исполнения выполняется командой:

```
# sysctl -n kernel.altha.nosuid.enabled
1
```

Результат выполнения команды:

– 1 –режим включен;

– 0 – режим выключен.

8.3.2 Блокировка интерпретаторов (запрет запуска)

При включении блокировки интерпретаторов блокируется несанкционированное использование интерпретатора для выполнения кода напрямую из командной строки.

8.3.2.1 Блокировка интерпретаторов (запрет запуска скриптов) в ЦУС

Для включения режима блокировки интерпретаторов необходимо в Центр управления системой 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 разделенный запятыми список ограниченных интерпретаторов.

8.3.2.2 Блокировка интерпретаторов (запрет запуска скриптов) в консоли

Для включения режима блокировки интерпретаторов следует установить значение переменной kernel.altha.rstrscript.enabled равным 1:

```
# sysctl -w kernel.altha.rstrscript.enabled=1
```

Переменная kernel.altha.rstrscript.interpreters должна содержать разделенный двоеточиями список ограниченных интерпретаторов. Для изменения значения переменной kernel.altha.rstrscript.interpreters выполнить команду:

```
# sysctl -w kernel.altha.rstrscript.enabled=1
```

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
```