50 1190 0101

Утвержден

РУСБ.10015-01-УД

ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION»

Руководство администратора. Часть 1

РУСБ.10015-01 95 01-1

Листов 334

2015

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

АННОТАЦИЯ

Настоящий документ является первой частью руководства администратора операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (далее по тексту — ОС).

Руководство администратора состоит из двух частей:

– РУСБ.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1»;

– РУСБ.10015-01 95 01-2 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 2».

В первой части руководства приведено назначение, установка и настройка ОС. Рассмотрены системные компоненты, сервисы и команды, базовые сетевые службы, средства организации ЕПП, защищенная графическая подсистема, управление программными пакетами, резервное копирование и восстановление данных, система печати, защищенная СУБД, защищенные комплексы программ гипертекстовой обработки данных и электронной почты, средства контроля целостности, централизованного протоколирования и разграничения доступа к подключаемым устройствам.

Приведен список сообщений для администратора.

В приложении А приведен перечень пакетов ОС.

Документ предназначен для администраторов системы и сети.

Во второй части руководства приведено описание работы с защищенной СУБД.

СОДЕРЖАНИЕ

РУСБ.10015-01 95 01-2 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 2»

1. АДМИНИСТРИРОВАНИЕ ОС

Административное управление в ОС отделено от общего доступа пользователей.

Большинство операций по настройке и администрированию ОС требуют привилегий суперпользователя `root`, например:

– монтирование и размонтирование ФС;
– изменение корневого каталога процесса командой `chroot`;
– создание файлов устройств;
– установка системных часов;
– изменение принадлежности файлов;
– задание host-имени системы;
– конфигурирование сетевых интерфейсов.

ВНИМАНИЕ! После установки ОС интерактивный вход в систему суперпользователя `root` по умолчанию заблокирован. Создаваемый при установке операционной системы пользователь включается в группу `astra-admin`. Пользователям, входящим в названную группу, через механизм `sudo` (см. 1.1.2) предоставляются права для выполнения действий по настройке ОС, требующих привилегий суперпользователя `root`. Далее по тексту такой пользователь именуется администратором.

ВНИМАНИЕ! К паролю пользователей, обладающих административным доступом, предъявляются повышенные требования к качеству и надежности (см. 3.3.1.2).

ВНИМАНИЕ! Действия по администрированию ОС необходимо выполнять в мандатном контексте безопасности субъекта с нулевым уровнем и пустым набором категорий

1.1. Доступ к учетной записи суперпользователя

Существует несколько способов доступа к учетной записи суперпользователя:

– вход в систему от имени суперпользователя `root` (по умолчанию заблокирован);
– использование команды `su` (по умолчанию заблокирован);
– использование команды `sudo` (рекомендуется).

1.1.1. su

Команда `su` используется пользователем для запуска команд от имени другого пользователя. В том числе могут быть запущены команды от имени суперпользователя `root`.

ВНИМАНИЕ! После установки ОС интерактивный вход в систему суперпользователя `root` по умолчанию заблокирован. Для выполнения действий по настройке системы рекомендуется использование механизма `sudo` 1.1.2.

При запуске команды `su` без параметров подразумевается, что пользователь хочет

запустить командный интерпретатор shell от имени суперпользователя. При этом система просит ввести его пароль. При вводе правильного пароля запускаемый интерпретатор команд получает права и привилегии суперпользователя, которые сохраняются до завершения его работы. Для получения прав суперпользователя пользователю не требуется завершать свою сессию и вновь входить в систему.

С помощью команды su пользователь может исполнять отдельные команды от имени суперпользователя без запуска командного интерпретатора shell. Для этого используется опция -c. Преимущество такого способа состоит в том, что пользователь получает права и привилегии суперпользователя на строго ограниченное время, а именно, на время исполнения заданной команды. Предположим, что требуется поменять атрибуты файла от имени суперпользователя. Тогда пользователь может написать:

```
su -c 'chmod 0777 /tmp/test.txt'
```

В этом случае (после ввода пароля суперпользователя) команда chmod получит права и привилегии суперпользователя, но по ее завершении пользователь останется в своей сессии и не будет обладать правами и привилегиями суперпользователя.

Кроме выполнения команд от имени суперпользователя, команда su позволяет выполнять команды от имени любого другого пользователя. Для этого необходимо знать пароль этого пользователя. Если пользователь вошел в систему под именем root и выполняет команду su, то знание пароля пользователя не требуется. Тогда любые команды от имени любого пользователя исполняются свободно.

Недостаток команды su состоит в том, что она не регламентирует команды, разрешенные конкретному пользователю на запуск от имени суперпользователя. Таким образом, если у пользователя есть права на запуск команды su, то он может выполнить от имени суперпользователя любые команды. Поэтому ее запуск должен быть разрешен только доверенным пользователям. Также рекомендуется при вводе команды использовать полное путевое имя /bin/su, а не просто su.

Описание команды приведено в man su.

1.1.2. sudo

Команда sudo используется обычным пользователем для запуска команд от имени суперпользователя. Для работы команда sudo просматривает конфигурационный файл /etc/sudoers, который содержит список пользователей, имеющих полномочия на ее применение и перечень команд, которые они имеют право выполнять. В качестве аргументов команда sudo принимает командную строку, которую следует выполнить с правами суперпользователя. Если данному пользователю разрешено выполнять указанную им команду, то sudo просит пользователя ввести его собственный пароль. Таким образом, для каждого пользователя установлен набор команд, которые он может исполнять от имени суперполь-

зователя, и нет необходимости передавать пользователям пароль суперпользователя.

Кроме выполнения указанной команды, `sudo` ведет файл регистрации выполненных команд, вызвавших их лиц, каталогов, из которых вызывались команды, и времени их вызова. Эта информация регистрируется с помощью системы `syslog`.

Для изменения администратором файла `/etc/sudoers` следует использовать специальную команду `visudo`.

Преимущество механизма `sudo` в том, что обычные пользователи могут выполнять рутинные задачи от имени суперпользователя, не имея при этом неограниченных прав и привилегий.

Описание команды приведено в `man sudo`.

1.2. Механизмы разделения полномочий

К механизмам разделения полномочий между системными администраторами ОС могут быть отнесены:

– механизм привилегий;

– механизм повышения полномочий на время выполнения команды (программы);

– механизм автоматической установки ACL на файлы.

Описание механизмов разделения полномочий приведено в документе РУСБ.10015-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1».

1.2.1. Механизм привилегий

Механизм привилегий ОС предназначен для передачи отдельным пользователям прав выполнения отдельных, строго оговоренных, административных действий. Обычный пользователь системы не имеет дополнительных привилегий.

Привилегии наследуются процессами от своих «родителей» и не могут быть переданы сторонним процессам. Процессы, запущенные от имени суперпользователя, независимо от наличия у них привилегий, имеют возможность осуществлять все привилегированные действия.

Распределение (первоначальная настройка) привилегий выполняется только суперпользователем.

1.2.2. Механизм повышения полномочий

Механизм повышения полномочий позволяет повысить полномочия пользователя на время выполнения определенной программы. Настройка механизма может быть выполнена только суперпользователем.

1.2.3. Механизм автоматической установки ACL на файлы

Механизм автоматической установки ACL на файлы облегчает задачу администрирования, при которой пользователю предоставляется доступ к тем файловым объектам, к которым необходим доступ в соответствии с его ролью. Такую настройку выполняет суперпользователь.

2. УСТАНОВКА И НАСТРОЙКА ОС

2.1. Общие положения

DVD-диск с дистрибутивом ОС содержит все необходимые файлы для выполнения процесса ее полной или частичной установки на жесткий диск целевого компьютера, имеющего устройство чтения DVD-дисков. ОС можно также установить с USB-накопителя или по сети.

2.2. Установка с DVD-диска (запуск программы установки)

Выполнение программы установки ОС начинается с ее запуска, а затем, после выбора во входном меню конкретных параметров пользовательского интерфейса, начинается работа самой программы в интерактивном или автоматическом режимах.

В самом начале загрузки программы установки на экране монитора появляется логотип ОС, меню, переключатель «Русский»–«English» (для изменения языка меню). Меню программы установки содержит следующие пункты:

1) «Графическая установка»;
2) «Установка»;
3) «Быстрая установка»;
4) «Режим восстановления».

В нижней части экрана приведен список функциональных клавиш, подключающих дополнительные возможности программы установки:

– **[F1]** — «Язык»;
– **[F2]** — «Параметры».

Чтобы начать установку ОС, следует выбрать пункт «Графическая установка» или «Установка» с помощью клавиш со стрелками на клавиатуре и нажать **<Enter>** для запуска программы. Произойдет переход к программе установки в графическом или в текстовом режиме, соответственно.

Пункт «Быстрая установка» запускает программу установки в режиме с минимальным количеством действий пользователя, которые сводятся к ответам на вопросы, связанные с настройкой сети, разметкой жесткого диска и установкой пароля администратора и пароля на доступ к системному загрузчику. Остальные шаги программы установки будут выполняться автоматически с использованием значений параметров установки по умолчанию.

Пункт «Режим восстановления» запускает ОС в текстовом режиме непосредственно с DVD-диска с дистрибутивом для использования при восстановлении нарушенной работоспособности уже установленной ОС.

Если необходимо добавить какие-то параметры загрузки для программы установки или ядра, то следует нажать **<F2>**, а затем **<Esc>**. После этого на экране будет показана командная строка загрузки, и можно будет ввести дополнительные параметры.

Программа установки в графическом и в текстовом режимах имеет одинаковую функциональность, т. к. в обоих случаях используются одни и те же модули, т. е. отличаются они только на уровне пользовательского интерфейса. Графическая программа обеспечивает поддержку в процессе установки несколько большего числа языков, управление в ней можно осуществлять с помощью мыши, а также на одном экране может быть выведено одновременно значительно большее количество информации.

2.2.1. Графическая установка и первичная настройка

Для графической установки ОС необходимо:

1) загрузить программу установки ОС с носителя;
2) выбрать настройки программы установки и оборудования;
3) активировать (если есть) подключение к сети Ethernet;
4) создать учетную запись и пароль пользователя;
5) настроить время;
6) создать и смонтировать дисковые разделы, на которые будет установлена ОС;
7) выбрать и установить необходимое программное обеспечение (ПО). После установки базовой системы (список пакетов базовой системы приведен в А.1) предоставляется возможность установить по своему выбору ПО, которое включает в себя: базовые средства (А.2), рабочий стол Fly А.3, средства работы в сети А.4, офисные средства А.5, сетевые сервисы А.6, СУБД А.7, средства мультимедиа А.8, режим киоска А.9, службу ALD А.10;
8) выбрать и установить дополнительные настройки безопасности ОС 2.2.2;
9) установить и настроить системный загрузчик `GRUB`;
10) загрузить установленную ОС в первый раз.

Подробное описание последовательности действий при графической установке ОС и ее первичной настройке см. в инструкции, содержащейся в каталоге `/install-doc` на DVD-диске с дистрибутивом.

ВНИМАНИЕ! Если на компьютере, на который устанавливается ОС, присутствуют другие операционные системы, то, возможно, для их корректной загрузки потребуется дополнительная настройка загрузчика Grub. Для этого необходимо в ОС от имени администратора выполнить команду `update-grub`.

2.2.2. Дополнительные настройки безопасности ОС

В окне «Дополнительные настройки ОС» (рис. 1) можно отключить автоматическую настройку сети и включить дополнительные настройки безопасности ОС.

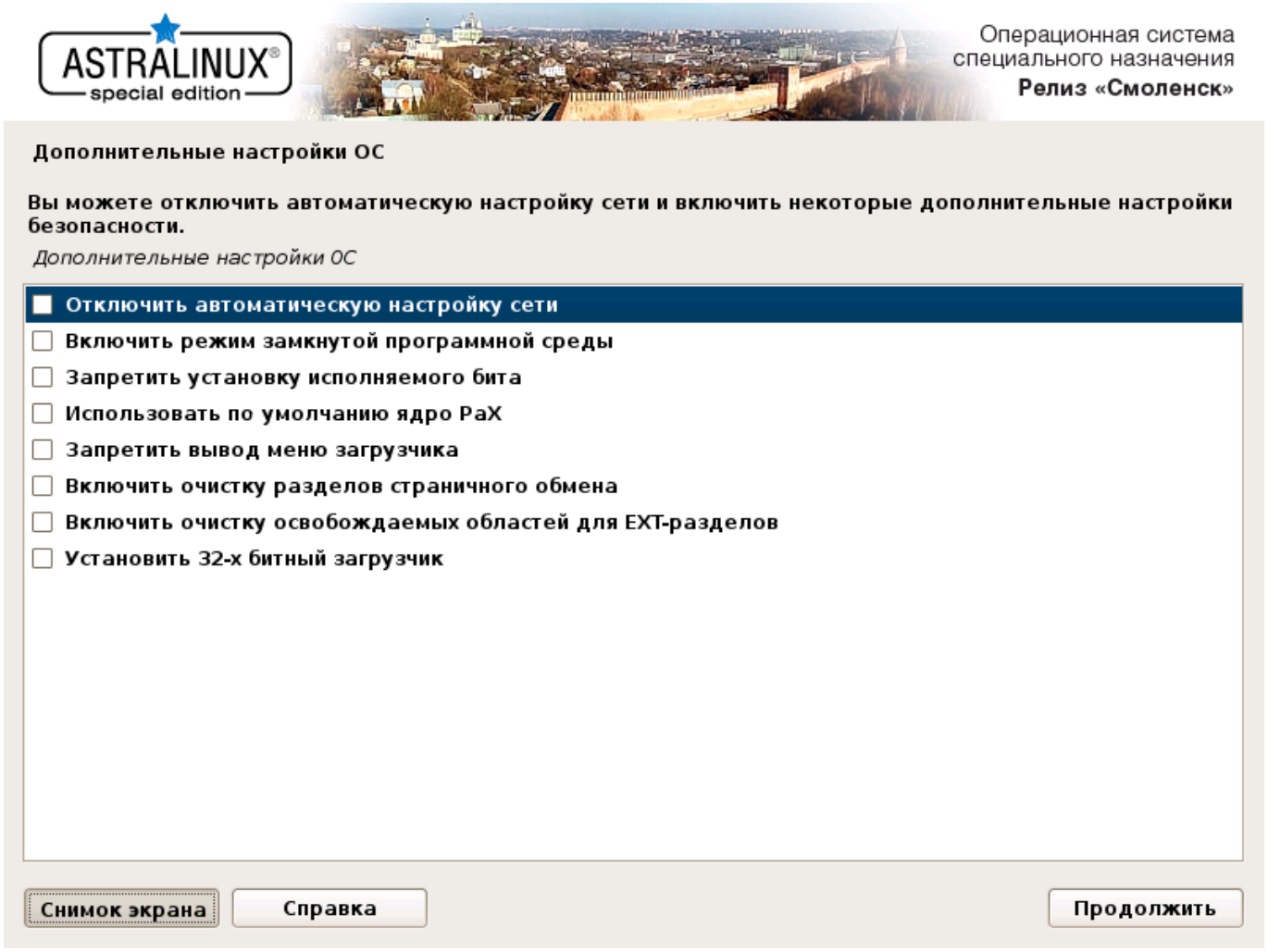


Рис. 1

Дополнительные функции безопасности ОС:

1) «Включить режим замкнутой программной среды»

При выборе данного пункта будет включен механизм, обеспечивающий проверку неизменности и подлинности загружаемых исполняемых файлов формата ELF (см. п.13.5 документа РУСБ.10015-01 97 01-1).

2) «Запретить установку исполняемого бита»

При выборе данного пункта будет включен режим запрета установки исполняемого бита, обеспечивающий предотвращение несанкционированного создания пользователями или непреднамеренного создания администратором исполняемых сценариев для командной оболочки (см. раздел 16 документа РУСБ.10015-01 97 01-1).

3) «Использовать по умолчанию ядро PaX»

При выборе данного пункта будет обеспечено использование средств ограничения

доступа к страницам памяти (см. раздел 12 документа РУСБ.10015-01 97 01-1).

4) «Запретить вывод меню загрузчика»

При выборе данного пункта будет запрещен вывод меню загрузчика Grub. В процессе загрузки будет загружаться ядро ОС, выбранное по умолчанию.

5) «Включить очистку разделов страничного обмена»

При выборе данного пункта будет включен режим очистки памяти разделов подкачки `swap` (см. раздел 5 документа РУСБ.10015-01 97 01-1).

6) «Включить очистку освобождаемых областей для EXT-разделов»

При выборе данного пункта будет включен режим очистки блоков ФС непосредственно при их освобождении (см. раздел 5 документа РУСБ.10015-01 97 01-1).

7) «Установить 32-х битный загрузчик»

При выборе данного пункта из системы будет удален 64-х битный загрузчик EFI и установлен 32-х битный загрузчик EFI.

ВНИМАНИЕ! При установке на 64-х битную вычислительную машину с поддержкой EFI выбор данной опции может привести к тому, что установленная система не загрузится.

2.3. Создание LiveCD

LiveCD - это ОС, предназначенная для работы сразу после загрузки с оптического носителя (CD, DVD) без установки на жесткий диск.

В составе ОС имеется специальная программа для создания LiveCD — `live-build-astra`.

Опции программы приведены в таблице 1.

Таблица 1

Опция	Описание
`-h, --help`	Вывести справку
`-o, --output <filename>`	Задать имя результирующего ISO-образа
`-D, --distribution <distribution>`	Задать имя варианта ОС Astra Linux. Поддерживаются варианты smolensk и orel
`-T, --tasks`	Задать списки пакетов, установленных в результирующей ОС
`-P, --packages-list <filename>`	Название файла с дополнительным списком пакетов для установки в результирующей ОС
`-p, --additional-packages <list>`	Названия одиночных пакетов для установки в результирующей ОС
`-e, --exclude-packages <list>`	Названия пакетов, которые нужно исключить из списков, указанных выше

Окончание таблицы 1

Опция	Описание
-b, --build-directory <dirname>	Название сборочной директории
-c, --clean-before	Очистить сборочную директорию перед сборкой
-C, --clean-after	Уничтожить сборочную директории после сборки
-k, --hooks <dirname>	Название директории со сценариями оболочки которые нужно выполнить в результирующей ОС после установки ПО
-l, --includes-binary <dirname>	Название директории с файлами, которые нужно включить в состав результирующего ISO-образа
-m, --includes-chroot <dirname>	Название директории с файлами, которые нужно включить в состав результирующей ОС
-t, --tarball <filename>	Сформировать архив с содержимым коневой ФС результирующей ОС
-i, --image <filename>	Сформировать образ карты памяти с результирующей ОС
-q, --partition-script <filename>	Файл с описанием таблицы разделов на карте памяти
-s, --source-iso <filename>	Исходный ISO-образ
-r, --repositories <URL>	Адрес репозитория с пакетами ПО для установки в результирующей ОС
-a, --arch <ARCHITECTURE>	Целевая архитектура результирующей ОС. По умолчанию используется текущая архитектура

LiveCD ОС можно собирать, используя ISO-образы двух установочных дисков ОС (диск с дистрибутивом ОС и диск со средствами разработки) в качестве источников пакетов. Для этого необходимо указать путь к ним в кавычках через точку с запятой, например:

```
live-build-astra -o smolensk_live.iso -D smolensk
 -s "/home/user/smolensk-current.iso;/home/user/devel-smolensk-current.iso"
```

Если при сборке в качестве одного из источников пакетов не предоставляется установочный диск ОС, то получившийся образ LiveCD не сможет быть загружен с помощью UEFI, а только «старым» способом с помощью BIOS. Некоторые компьютеры (в основном современные ноутбуки) не предоставляют возможность загрузки без использования UEFI.

По умолчанию собирается образ ОС, пригодный для сетевой установки ОС на жесткий диск компьютера.

Если требуется добавить какие-либо файлы на диск с LiveCD или в ОС LiveCD, то рекомендуется скопировать папки, используемые по умолчанию:

```
/usr/share/live-build-astra/includes.binary/
/usr/share/live-build-astra/includes.chroot/
```

(соответственно) и добавить туда желаемые файлы, после чего указать копии папок в качестве параметров ключей `--includes-binary` и `--includes-chroot`, например:

```
cp /usr/share/live-build-astra/includes.binary/ ~/Desktop/includes.binary
cp /usr/share/live-build-astra/includes.chroot/ ~/Desktop/includes.chroot
echo "My custom LiveCD" > ~/Desktop/includes.binary/custom.txt
echo "File in root directory." > ~/Desktop/includes.chroot/root/file.txt
live-build-astra -o smolensk_live.iso -D smolensk
   -s "/home/user/smolensk-current.iso;/home/user/devel-smolensk-current.iso"
   --tasks "Base Fly"
   -p "gimp firefox" --includes-binary ~/Desktop/includes.binary
   --includes.chroot ~/Desktop/includes.chroot
```

Файл `custom.txt` будет в корне файловой системы LiveCD. Файл `file.txt` будет в `/root` загруженной ОС LiveCD.

Кроме того, если требуется чтобы в ОС LiveCD были произведены какие-то действия на этапе сборки, то можно использовать ключ `--hooks` аналогично `--includes-chroot`, т.е. скопировать:

```
/usr/share/live-build-astra/hooks/
```

Поместить в копию необходимые сценарии оболочки и передать путь к копии в качестве ключа к параметру `--hooks`.

ISO-образ, получающийся в результате работы `live-build-astra`, является гибридным, в том смысле, что его можно использовать для загрузки как с DVD, так и с USB-накопителя. Для того, чтобы загрузить ОС с USB-накопителя, необходимо ISO-образ побайтово записать на USB-накопитель, например с помощью команды `dd`.

Например, если подключенный USB-накопитель обозначен в системе как `/dev/sdb`, то запуск команды:

```
dd if=smolensk_live.iso of=/dev/sdb bs=1M
```

запишет ISO-образ на USB-накопитель.

ВНИМАНИЕ! Команда `dd` записывает новое содержимое, затирая старое. Если ошибиться с параметрами, то можно испортить данные или сделать свою ОС незагружаемой.

3. СИСТЕМНЫЕ КОМПОНЕНТЫ

3.1. Управление устройствами

3.1.1. Типы устройств

В ОС существует два типа устройств: блочные с прямым доступом (например, жесткие диски) и символьные (например, последовательные порты), некоторые из них могут быть последовательными, а некоторые — с прямым доступом. Каждое поддерживаемое устройство представляется в ФС файлом устройства. При выполнении операций чтения или записи с подобным файлом происходит обмен данными с устройством, на которое указывает этот файл. Такой способ доступа к устройствам позволяет не использовать специальные программы (а также специальные методы программирования, такие как работа с прерываниями).

Так как устройства отображаются как файлы в ФС (в каталоге `/dev`), их можно обнаружить с помощью команды `ls`. После выполнения команды:

```
ls -l
```

на экран монитора выводится список файлов, причем в первой колонке содержится тип файла и права доступа к нему. Например, для просмотра файла, соответствующего звуковому устройству, используется следующая команда:

```
ls -l /dev/dsp
crw-rw---T+ 1 root audio 14, 3 Июл 1 13:05 /dev/dsp
```

Первый символ в первой колонке (`c`) показывает тип файла, в данном случае — символьное устройство. Для обычных файлов используется символ «`-`» (дефис), для каталогов — `d`, для блочных устройств — `b` (описание команды приведено в `man ls`).

Наличие большого количества файлов устройств не означает, что эти устройства на самом деле установлены. Наличие файла `/dev/sda` ни о чем не говорит и совсем не означает, что на компьютере установлен жесткий диск SCSI. Это предусмотрено для облегчения установки программ и нового оборудования (нет необходимости искать нужные параметры и создавать файлы для новых устройств).

3.1.2. Жесткие диски

При администрировании дисков могут возникнуть вопросы разделения жесткого диска на разделы, создания ФС, монтирования ФС, форматирование диска и др.

Одна из причин разделения жесткого диска — это хранение разных ОС на одном жестком диске. Другая причина — хранение пользовательских и системных файлов в разных разделах, что упрощает резервное копирование и восстановление, а также защиту системных файлов от повреждений.

Для использования диска или раздела необходимо создание ФС. Только после это-

го возможна работа с файлами.

Монтирование различных ФС для формирования единой структуры каталогов как автоматически, так и вручную (ФС, монтируемые вручную, должны быть вручную размонтированы), и вопросы буферизации дисков и работы с виртуальной памятью также необходимы при работе с дисками.

Центральный процессор и жесткий диск обмениваются информацией через дисковый контроллер. Это упрощает схему обращения и работы с диском, т. к. контроллеры для разных типов дисков могут быть построены с использованием одного интерфейса для связи с компьютером.

Каждый жесткий диск представлен отдельным файлом устройства в каталоге `/dev`: `/dev/hda` и `/dev/hdb` для первого и второго диска, подключенного по IDE шине, и `/dev/sda` и `/dev/sdb` и т. д. для дисков, использующих SCSI или SATA-интерфейс.

3.1.3. Разделы жесткого диска

Весь жесткий диск может быть разбит на несколько разделов, причем каждый раздел представлен так, как если бы это был отдельный диск. Разделение используется, например, при работе с двумя ОС на одном жестком диске. При этом каждая ОС использует для работы отдельный раздел и не взаимодействует с другими. Таким образом, две различные системы могут быть установлены на одном жестком диске.

Главная загрузочная запись MBR (Master Boot Record) диска содержит место для четырех основных разделов, пронумерованных от 1 до 4. Если необходимо добавить еще разделы на диск, то следует преобразовать основной раздел в дополнительный (extended). Далее дополнительный раздел разделяется на один или несколько логических разделов с номерами от 5 до 15.

3.1.3.1. Расширенные и логические разделы

В ОС swap-область для повышения скорости обмена чаще всего размещается в основном отдельном разделе.

Схема, использующая расширенные разделы, позволяет разбивать основной раздел на подразделы. Основной раздел, разбитый таким образом, называется «расширенным разделом», а подразделы называются «логическими разделами». Они функционируют так же, как и основные разделы, различие состоит в схеме их создания.

3.1.3.2. Разбиение жесткого диска

`fdisk` — программа разбиения жесткого диска на разделы.

Каждый раздел должен содержать четное количество секторов, т. к. в ОС используются блоки размером в 1 КБ, т. е. два сектора. Нечетное количество секторов приведет к тому, что последний из них будет не использован. Это ни на что не влияет, но при запуске `fdisk` будет выдано предупреждение.

При изменении размера раздела обычно требуется сначала сделать резервную копию всей необходимой информации, удалить раздел, создать новый раздел, а затем восстановить всю сохраненную информацию в новом разделе.

Описание программы приведено в `man fdisk`.

3.1.3.3. Файлы устройств и разделы

Каждому основному и расширенному разделу соответствует отдельный файл устройства. Существует соглашение для имен подобных файлов, которое состоит в добавлении номера раздела к имени файла самого диска. Разделы 1–4 являются основными (вне зависимости от того, сколько существует основных разделов), а разделы 5–15 — логическими (вне зависимости от того, к какому основному разделу они относятся). Например, `/dev/hda1` соответствует первому основному разделу первого IDE-диска, а `/dev/sdb7` — третьему логическому разделу второго диска с интерфейсом SCSI или SATA.

3.1.4. Форматирование

Форматирование — это процесс записи специальных отметок на магнитную поверхность, которые используются для разделения дорожек и секторов. Диск не может использоваться до тех пор, пока он не будет отформатирован.

Для IDE- и некоторых SCSI-дисков форматирование производится при их изготовлении и, обычно, не требуется повторения этой процедуры.

3.1.5. Программная организация дисковых разделов в RAID и тома LVM

В ядро ОС встроена программная реализация технологии RAID (уровни: `RAID 0`, `RAID 1`, `RAID 5` и их сочетания). Команда `mdadm` предоставляет административный интерфейс пользователя для создания и управления массивами.

После создания массива его устройство, например `/dev/md0`, используется точно также, как `/dev/hda1` или `/dev/sdb7` в примере выше.

LVM, с точки зрения ядра системы, использует унифицированные механизмы VFS, не нуждаясь в специальных конфигурациях ядра. В ОС обеспечивается полнофункциональное управление томами LVM, которое осуществляется стеком команд управления (около 30 программ).

LVM обеспечивает более высокий уровень абстракции, чем традиционные диски и разделы Linux. Это позволяет добиться большей гибкости при выделении пространства для хранения данных. Логические тома можно легко перемещать с одного физического устройства на другое, а их размер изменять. Физические устройства можно относительно просто добавлять и удалять. Томам, управляемым посредством LVM, можно назначать практичные названия, такие как «database» или «home», а не малопонятные «sda» или «hda», как у устройств.

3.2. Управление ФС

Файловая система — это методы и структуры данных, которые используются ОС для хранения файлов на диске или его разделе.

Перед тем, как раздел или диск могут быть использованы для хранения информации (файлов), он должен быть инициализирован, а требуемые данные перенесены на этот диск. Этот процесс называется «созданием ФС».

ФС ОС по умолчанию соответствует типу Ext4, обеспечивает поддержку длинных имен, символических связей, а также обеспечивает поддержку ФС ISO9660, FAT (MS-DOS), NTFS и др. Также предусмотрена возможность представления имен файлов русскими буквами.

Все данные ОС состоят из множества файлов (программы, библиотеки, системные и пользовательские файлы) и все они располагаются в ФС.

ОС состоит из множества файлов и каталогов. Структура ФС имеет вид «перевернутого дерево», верхнюю вершину которого называют корнем (`/root` — корневой каталог).

В зависимости от выбора, сделанного в процессе установки, каталоги могут относиться к различным ФС.

После начальной установки ФС ОС может состоять, например, из следующих частей:

- `root`:
  - `/bin` — находятся выполняемые программы (точнее, их двоичные файлы). Они необходимы для работы системы. Многие команды ОС на самом деле являются программами из этого каталога;
  - `/dev` — расположены особые файлы, называемые «файлами устройств» (device files). С их помощью осуществляется доступ ко всем физическим устройствам, установленным в системе;
  - `/boot` — содержит необходимую информацию для загрузки системы (ядро (ядра), образ `initrd`, файлы загрузчика);
  - `/root` — домашний каталог суперпользователя;
  - `/tmp` — используется для хранения временных файлов, создаваемых программами в процессе своей работы. Работая с программами, создающими много больших временных файлов, лучше иметь отдельную ФС, чем простой каталог корневой ФС;
  - `/etc` — содержит конфигурационные файлы ОС. Здесь находится файл паролей `passwd`, а также список ФС, подключаемых при начальной загрузке `fstab`. В этом же каталоге хранятся сценарии загрузки (startup scripts), список узлов (hosts) с их IP-адресами и множество других данных о конфигурации;

– /lib — содержатся разделяемые библиотеки, используемые многими программами во время своей работы. Применяя разделяемые библиотеки, хранящиеся в общедоступном месте, можно уменьшить размер программ за счет повторного использования одного и того же кода;

– /proc — является виртуальной ФС и используется для чтения из памяти информации о системе;

– /sbin — хранятся системные двоичные файлы (большинство из них используется для нужд системного администрирования);

– /usr — хранятся различные программы и данные, не подлежащие изменению. Каталог /usr и его подкаталоги необходимы для функционирования ОС, т. к. содержат наиболее важные программы. Данный каталог почти всегда является отдельной ФС;

– /var — содержатся изменяемые файлы (такие как log-файлы и др.);

– /home — состоит из личных каталогов пользователей. Общепринято иметь здесь отдельную ФС, чтобы обеспечить пользователям достаточное пространство для размещения своих файлов. Если пользователей в системе много, возможно, придется разделить этот каталог на несколько ФС. Тогда, например, можно создать подкаталоги /home/staff и /home/admin для персонала и администрации, соответственно, установить каждый как самостоятельную ФС и уже в них создавать рабочие каталоги пользователей.

В личных каталогах каждого пользователя наряду с другими файлами имеются несколько конфигурационных файлов, которые для практических целей являются скрытыми. Они модифицируются редко. Файл становится скрытым, если поставить точку в начале имени файла. Можно увидеть эти файлы, введя команду:

```
ls -a
```

3.2.1. Установка

ФС устанавливается, т. е. инициализируется при помощи команды mkfs. Она запускает требуемую программу в зависимости от типа устанавливаемой системы. Тип ФС указывается при помощи опции -t fstype (описание команды приведено в man mkfs).

3.2.2. Монтирование

Перед работой с ФС она должна быть смонтирована. При этом ОС выполняет некоторые действия, обеспечивающие функционирование монтируемой системы. Так как все файлы в ОС принадлежат одной структуре каталогов, то эта операция обеспечивает работу с ФС, как с каталогом, называемым точкой подключения (монтирования).

Для монтирования (подключения) ФС к дереву каталогов ОС необходимо убедиться, что каталог, к которому следует подключить ФС (точка подключения), действительно

существует.

Если использовать для точки монтирования (подключения) непустой каталог, то его содержимое станет недоступно до размонтирования. Поэтому рекомендуется иметь специально созданные каталоги для монтирования разделов/устройств. Обычно они располагаются в `/mnt` и `/media`.

Предположим, что требуется монтировать файл `ISO9660` к точке подключения `/mnt`. Каталог `/mnt` должен уже существовать, иначе подключение окончится неудачей. После подключения к этому каталогу все файлы и подкаталоги ФС появятся в нем. В противном случае каталог `/mnt` будет пустым.

Для того чтобы узнать, какой ФС принадлежит текущий каталог, следует воспользоваться командой:

```
df -h
```

Будет видна ФС и объем свободного пространства.

3.2.2.1. mount

В ОС для подключения ФС используется команда `mount`. Синтаксис команды:

```
mount device mountpoint
```

где `device` означает физическое устройство, которое необходимо подключить, а `mountpoint` — точку подключения.

В целях системной безопасности использовать команду `mount` может только суперпользователь.

Кроме опций, указанных выше, команда `mount` может иметь в командной строке еще несколько опций, приведенных в таблице 2.

Таблица 2

Опция	Описание
`-f`	Имитирует подключение ФС. Выполняются все действия, кроме системного вызова для настоящего подключения
`-v`	Подробный отчет, предоставляет дополнительную информацию о своих действиях
`-w`	Подключает ФС с доступом для чтения и записи
`-r`	Подключает ФС с доступом только для чтения
`-n`	Выполняет подключение без записи в файл `/etc/mtab`
`-t type`	Указывает тип подключаемой ФС
`-a`	Подключить все ФС, перечисленные в `/etc/fstab`
`-o list_of_options`	Применить список опций к подключаемой ФС. Опции в списке перечислены через запятую. За полным списком возможных опций следует обратиться к руководству `man`

Если необходимая опция не указана, mount попытается определить ее по файлу /etc/fstab.

Распространенные формы команды mount:

```
mount /dev/hdb3 /mnt
```

подключает раздел жесткого диска /dev/hdb3 к каталогу /mnt.

```
mount -vat nfs
```

подключает все ФС NFS, перечисленные в файле /etc/fstab.

Если правильно подключить ФС не удается, воспользоваться командой:

```
mount -vf device mountpoint
```

чтобы узнать, что именно пытается сделать команда mount. В этом случае она выполнит все действия, кроме подключения, и даст о них подробный отчет.

Описание команды приведено в man mount.

3.2.2.2. fstab

Если список используемых ФС изменяется редко (а это бывает в большинстве случаев), то удобно указать ОС подключать их сразу же при загрузке и отключать при завершении работы. Эти ФС перечисляются в специальном конфигурационном файле /etc/fstab по одной в строке. Поля в строках разделяются пробелами или символами табуляции. В таблице 3 показаны поля файла /etc/fstab.

Таблица 3

Поле	Описание
ФС	Подключаемое блочное устройство или удаленная ФС
Точка подключения	Место подключения ФС. Чтобы сделать систему невидимой в дереве каталогов (например, для файлов подкачки), используется слово none
Тип	Указывает тип подключаемой ФС
Опции подключения	Список разделенных запятыми опций для подключаемой ФС, должен содержать, по крайней мере, тип подключения. Более подробную информацию см. в руководстве man команды mount
Периодичность резервного копирования	Указывает, как часто следует выполнять резервное копирование с помощью команды dump. Если в поле стоит значение 0, то dump считает, что ФС не нуждается в резервном копировании
Номер прохода	Задает порядок проверки целостности ФС при загрузке с помощью команды fsck. Для корневой ФС следует указывать значение 1, для остальных — 2. Если значение не указано, целостность ФС при загрузке проверяться не будет

Рекомендуется подключать ФС во время загрузки через /etc/fstab вместо команды mount. Пример файла fstab.

Пример

```
# /etc/fstab: static file system information.
#
# Use ’blkid’ to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda11 during installation
UUID=a50cefb7-a198-4240-b198-581200027898 / ext4  usrquota,errors=remount-ro,secdel=2 0 1
# /home was on /dev/sda10 during installation
UUID=c94bba8d-95d4-467b-b3e0-2cd7f92c3355 /home  ext4  usrquota,secdelrnd  0  2
# swap was on /dev/sda5 during installation
UUID=ce71b251-2405-4eed-8130-5f92a56b67ac none            swap    sw       0  0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0
# /etc/fstab.d/PDAC: parsec devices access control mount instructions
#
#<file system><mount point><type><options><dump><pass>
### usb flash
/dev/*fat /*home/*/media/*  auto  owner,group,noauto,nodev,noexec,iocharset=utf8,defaults 0 0
/dev/*ntfs* /*home/*/media/*  auto  owner,group,noauto,nodev,noexec,iocharset=utf8,defaults 0 0
/dev/sd*ext* /*home/*/media/*  auto  owner,group,nodev,noexec,noauto,defaults                0 0
### [cd|dvd|bd]rom
/dev/s*udf /*home/*/media/*  udf   owner,group,nodev,noexec,noauto,defaults 0 0
/dev/s*iso9660 /*home/*/media/*  iso9660  owner,group,nodev,noexec,noauto,defaults 0 0
### other
/dev/sd* /*home/*/media/*  auto  owner,group,nodev,noexec,noauto,iocharset=utf8,defaults 0 0
```

Комментарии в файле начинаются с символа #.

Слово defaults в поле options указывает, что при подключении ФС следует применить набор опций по умолчанию, а именно — ФС следует подключить с разрешенным доступом для чтения и записи; она должна рассматриваться как отдельное блочное устройство; весь файловый ввод-вывод должен выполняться асинхронно; разрешено выполнение программных файлов; ФС может подключаться с помощью команды:

```
mount -a
```

биты UID и GID файлов в этой ФС интерпретируются; обычным пользователям не разрешено подключать эту ФС.

Раздел подкачки /dev/sda3 используется ядром ОС для организации виртуальной памяти. Он должен присутствовать в файле /etc/fstab, чтобы система знала, где он находится. Чтобы он не появлялся в дереве каталогов, точка подключения указана как none. Кроме того, разделы подкачки подключаются с опцией sw.

Виртуальная ФС /proc указывает на информационное пространство процессов в памяти. Соответствующий физический раздел для нее отсутствует.

ФС VFAT также можно подключать автоматически. Раздел /dev/sdb1 — это первый раздел второго жесткого диска SCSI. Он подключается как раздел VFAT, где vfat указывается в качестве типа ФС и /win — в качестве точки подключения.

Для получения полной информации о допустимых в файле /etc/fstab опциях см. руководство man для fstab.

3.2.3. Размонтирование

Для размонтирования (отключения) ФС используется команда umount. Отключение может понадобиться для проверки и восстановления ФС с помощью команды fsck. Удаленные ФС отключаются в случае неполадок в сети.

Команда umount имеет три основные формы:

```
umount device : mountpoint
umount -a
umount -t fstype
```

device означает физическое устройство, которое необходимо отключить, а mountpoint — имя каталога точки подключения (указывать только device или mountpoint). У команды umount всего два параметра. Параметр -a отключает все ФС, а параметр -t fstype — только ФС указанного типа.

Команда umount не отключает ФС, если они используются в текущий момент.

Например, если какую-либо ФС подключить к /mnt и попытаться выполнить команды:

```
cd /mnt
umount /mnt
```

то появится сообщение об ошибке, т. к. ФС занята. Перед отключением `/mnt` необходимо перейти в каталог другой ФС.

Для принудительного размонтирования устройства, вне зависимости используется оно или нет, можно воспользоваться опцией `-f` команды `umount`:

```
umount -f /cdrom
```

Для размонтирования и освобождения устройства от сменных носителей информации можно пользоваться командой `eject`.

Служебная программа `fuser` отображает сведения о процессах, использующих ФС. Например:

```
fuser -v  точка_монтирования
```

Для завершения всех процессов, использующих ФС, можно воспользоваться командой:

```
fuser -km точка_монтирования
```

Описание команды приведено в `man umount`.

3.3. Управление пользователями

3.3.1. Работа с пользователями

Управление пользователями означает добавление, удаление пользователей и определение их привилегий.

Управление пользователями предусматривает:

– добавление имен пользователей для возможности их работы в системе;

– определение их привилегий;

– создание и назначение рабочих каталогов;

– определение групп пользователей;

– удаление имен пользователей.

Каждый пользователь должен иметь уникальное регистрационное имя, дающее возможность идентифицировать пользователя и избежать ситуации, когда один пользователь может стереть файлы другого. Кроме того, каждый пользователь должен иметь свой пароль для входа в систему.

3.3.1.1. Добавление

При добавлении пользователя в файл `/etc/passwd` вносится учетная запись в такой форме:

```
login_name: encrypted_password: user_ ID: group_ ID: user_ information:
login_directory: login_shell
```

В этой записи поля разделены двоеточиями, а значения этих полей приведены в таблице 4.

Таблица 4

Поле	Назначение
login_name	Регистрационное имя пользователя
encrypted_password	Указатель на теневой файл паролей (shadow)
user_ID	Уникальный номер, используемый ОС для идентификации пользователя. Для локальных пользователей не должен превышать 2499
group_ID	Уникальный номер или имя, используемые для идентификации первичной группы пользователя. Если пользователь является членом нескольких групп, он может (если это разрешено системным администратором) в процессе работы менять группу
user_information	Описание пользователя, например, его имя и должность
login_directory	Рабочий каталог пользователя (в котором он оказывается после входа в систему)
login_shell	Оболочка, используемая пользователем, после входа в систему (например, /bin/bash)

Также описание файла /etc/passwd приведено в man 5 passwd.

Для добавления пользователя применяется команда adduser с параметром — именем добавляемого пользователя, например:

```
adduser User1
```

Команда adduser добавляет пользователя, создает домашний каталог, создает почтовый ящик, а также копирует файлы, имена которых начинаются с точки, из каталога /etc/skel в рабочий каталог пользователя. Каталог /etc/skel должен содержать все файлы-шаблоны, которые имеет каждый пользователь. Обычно это персональные конфигурационные файлы, такие как .profile, .cshrc и .login для настройки оболочки. Команда adduser представляет собой файл сценария bash, находящийся в каталоге /usr/sbin. Можно добавить запрос дополнительной информации о пользователе. Чтобы это сделать, необходимо воспользоваться командой chfn для изменения стандартных записей о пользователе.

Описание команд приведено в man adduser и man chfn.

ВНИМАНИЕ! Для обеспечения нормальной работы пользователя с сетевыми сервисами в системе должны быть явно заданы диапазоны его мандатных уровней и категорий при помощи утилиты usermac или fly-admin-smc, даже если ему недоступны уровни и категории выше 0.

3.3.1.2. Установка пароля

Для установки пароля пользователя предназначена команда passwd. Необходимо определить пароли для каждого пользователя. Войдя в систему, пользователь сможет сам изменить свой пароль. Для установки пароля пользователя выполнить, например, следую-

щее:

1) ввести команду и регистрационное имя пользователя, например:

```
passwd User1
```

и нажать клавишу **<Enter>**;

2) после появления приглашения:

```
New password:
```

ввести пароль (он не будет отображаться на экране монитора);

3) после появления сообщения повторить ввод пароля еще раз, ввести его снова.

Пароль будет зашифрован и внесен в файл `/etc/shadow`. При выборе пароля необходимо учесть следующие правила: пароль должен иметь не менее шести символов (предпочтительно — восемь символов) и желательно, чтобы пароль содержал как прописные, так и строчные буквы, знаки препинания и цифры.

ВНИМАНИЕ! Пароль рекомендуется создавать способом, максимально затрудняющем его подбор. Наиболее безопасный пароль состоит из случайной (псевдослучайной) последовательности букв, знаков препинания, специальных символов и цифр.

Необходимо периодически изменять пароль.

После выполнения всех действий запись в файле будет выглядеть примерно так:

```
anna:x:123:121:Anna_M.:/home/anna:/bin/bash
```

Второе поле записи содержит пароль в зашифрованном виде.

Описание команды приведено в `man passwd`.

Примечание. Если пользователь забыл свой пароль, то администратор системы не может напомнить его пользователю, т. к. в явном виде пароль нигде не хранится. Поэтому действия по восстановлению доступа пользователя в систему сводятся к замене администратором пароля пользователя на новый пароль с помощью команды:

```
passwd user_name
```

3.3.1.3. Удаление

Есть несколько степеней удаления пользователя:

– лишение пользователя возможности входа в систему;

– удаление учетной записи;

– удаление пользователя и всех его файлов.

Лишение пользователя возможности входа в систему полезно в случае его длительного перерыва в работе.

На время отсутствия пользователя можно заблокировать его запись с помощью команды:

```
usermod -L user_name
```

При этом все пользовательские файлы и каталоги остаются нетронутыми, но войти в систему под его именем становится невозможно.

Для разблокировки записи необходимо выполнить команду:

```
usermod -U user_name
```

Одним из вариантов лишения пользователя возможности входа может быть смена имени пользователя. При этом вход под старым именем становится невозможным. Для этого необходимо выполнить команду:

```
usermod -l new_user_name  old_user_name
```

Примечание. Имена домашнего каталога и почтового ящика при таком изменении имени пользователя не меняются. Эти параметры должны быть изменены вручную.

Удаление учетной записи пользователя производится либо путем непосредственного редактирования файла `/etc/passwd`, либо с помощью команды:

```
deluser user_name
```

По умолчанию, учетная запись удаляется без уничтожения домашнего каталога и файлов системы, принадлежащих удаляемому пользователю. Для удаления домашнего каталога может использоваться дополнительная опция `--remove-home`, а для поиска и удаления всех файлов системы, принадлежащих удаляемому пользователю — опция `--remove-all-files`. Также указанные действия могут быть выполнены вручную, как показано далее.

Удаление пользователя и всех его файлов — это окончательное и полное удаление пользователя из системы с помощью команды:

```
find / -user user_name -exec rm -r {} \;
```

Затем следует удалить рабочий каталог пользователя с помощью команды:

```
rmdir user_home_dir
```

и запись о пользователе из файла `/etc/passwd`.

Для удаления файлов, не принадлежащих ни одному пользователю в системе, выполнить команду:

```
find / -nouser -exec rm -r {} \;
```

Описание команд приведено в `man usermod`, `man deluser` и `man find`.

3.3.1.4. Неудачный вход в систему

Команда `faillog` показывает содержимое журнала неудачных попыток (файл `/var/log/faillog`) входа в систему. Также она может быть использована для управления счетчиком неудачных попыток и их ограничением. При запуске `faillog` без параметров выводятся записи `faillog` только тех пользователей, у которых имеется хотя бы одна неудачная попытка входа.

Предельное число попыток входа для каждой учетной записи равно 10. Для сброса неудачных попыток входа необходимо пользоваться опцией `-r`.

Описание команды, а также файла `/var/log/faillog` приведено в `man faillog` и `man 5 faillog`.

3.3.2. Работа с группами

Каждый пользователь является членом группы. Различным группам можно назначить различные возможности и привилегии.

Информация о группах содержится в файле `/etc/group`. Пример записи из этого файла:

```
Admin :: 21: user1, user2, user3
```

Здесь имя группы — `admin`, идентификатор — `21`, членами группы являются `user1`, `user2`, `user3`. Пользователь может быть членом нескольких групп и переходить из одной в другую в процессе работы.

Описание файла `/etc/group` приведено в `man 5 group`.

3.3.2.1. Добавление

Добавление группы производится с помощью команды:

```
addgroup users
```

Данная команда добавляет группу `users`.

Также новая группа создается путем непосредственного редактирования файла `/etc/group`, ввода необходимой информации о группе. Каждой группе присваивается свой уникальный идентификационный номер (ОС при работе учитывает номер, а не имя группы), поэтому, если присвоить двум группам один номер, для ОС получится одна и та же группа.

Описание команды приведено в `man addgroup`.

3.3.2.2. Удаление

Удаление группы производится с помощью команды:

```
delgroup users
```

Данная команда удаляет группу `users`.

Также удаление группы производится путем удаления записи о ней в файле `/etc/group`.

Описание команды приведено в `man delgroup`.

3.3.3. Рабочие каталоги пользователей

Рабочие каталоги пользователей на одном компьютере следует разместить в отдельном каталоге верхнего уровня (по умолчанию — `/home`) . Если пользователей достаточно много, то оптимально разделить их домашние каталоги по группам (подразделениям), например `/home/hr` (отдел персонала) `/home/admins`, `/home/buhg` и т. д.).

Таким образом, они будут достаточно логично сгруппированы, что в дальнейшем облегчит администрирование системы.

3.4. Перезагрузка и останов

Перезагрузка необходима в следующих случаях:

1) при подключении нового устройства или если работающее устройство «зависает» так, что его невозможно сбросить;

2) при модификации файла конфигурации, который используется только при начальной загрузке, т. к. для того чтобы изменения вступили в силу, необходимо загрузить систему заново;

3) если систему «заклинило» так, что невозможно зарегистрироваться и правильно поставить диагноз.

Перезагрузку можно выполнить несколькими способами:

1) дать команду `shutdown`;

2) использовать команду `reboot`;

3) использовать команду `init 6`.

Выключение системы предполагает корректное выключение системы, позволяющее избежать потерь информации и сбоев ФС.

Останов системы можно выполнить несколькими способами:

1) выключить питание;

2) дать команду `shutdown`;

3) использовать команду `halt`;

4) использовать команду `init 0`.

Работая с ОС, следует быть аккуратным при выходе из системы. Нельзя просто выключить компьютер, т. к. ОС хранит информацию ФС в оперативной памяти, при отключении питания информация может быть потеряна, а ФС повреждена.

Выключение питания может привести не только к потере данных и повреждению системных файлов. Есть риск повредить жесткий диск, если он относится к числу тех, на которых перед отключением питания необходимо установить в соответствующее положение защитный переключатель либо провести парковку головок.

3.4.1. shutdown

Команда `shutdown` — самый безопасный и наиболее корректный способ инициирования останова, перезагрузки или возврата в однопользовательский режим.

Можно дать указание `shutdown` делать паузу перед остановом системы. Во время ожидания она посылает зарегистрированным пользователям через постепенно укорачивающиеся промежутки времени сообщения, предупреждая их о приближающемся останове. По умолчанию в сообщениях просто говорится о том, что система заканчивает работу, и указывается время, оставшееся до останова. При желании администратор может доба-

вить собственное короткое сообщение, в котором содержится информация о том, почему система останавливается, и сколько примерно времени придется подождать, прежде чем пользователи вновь смогут войти в систему.

Команда `shutdown` позволяет указать, что конкретно должен сделать компьютер: остановиться, перейти в однопользовательский режим или перезагрузиться. Иногда можно также указать, следует ли перед перезагрузкой проверить диски с помощью команды `fsck`.

Синтаксис команды:

```
shutdown [flags] time [warning-message]
```

где `[warning-message]` — сообщение, посылаемое всем пользователям, в настоящий момент зарегистрированным в системе, а `time` представляет собой время выполнения отключения системы. Значение может быть также задано в формате `+m`, где `m` — количество минут ожидания до остановки системы. Значение `+0` может быть заменено словом `now`.

В таблице 5 перечислены основные опции команды `shutdown`.

Таблица 5

Опция	Назначение
`-k`	Послать предупреждение без реального завершения работы системы
`-r`	Перезагрузка компьютера после завершения работы
`-h`	Отключение компьютера после завершения работы
`-n`	Не синхронизировать диски. Эту опцию следует использовать крайне осторожно, т. к. могут быть потеряны или повреждены данные
`-f`	«Быстрая» перезагрузка. Создается файл `/etc/fastboot`, при наличии которого во время загрузки ОС не запускается программа `fsck`
`-c`	Отказаться от уже запущенного процесса завершения работы. Опция `time` при этом не может быть использована

Описание команды приведено в `man shutdown`.

Команда `shutdown` посылает всем пользователям предупреждающее сообщение, затем ожидает определенное в командной строке время и посылает всем процессам сигнал `SIGTERM`. Затем вызывается команда `halt` или `reboot` — в зависимости от опций командной строки.

3.4.2. halt и reboot

Команда `halt` выполняет все основные операции, необходимые для останова системы. Для вызова этой команды можно в командной строке указать:

```
shutdown -h
```

или непосредственно `halt`, которая регистрирует останов, уничтожает несущественные процессы, осуществляет системный вызов `sync`, дожидается завершения операций записи ФС, а затем прекращает работу ядра.

При указании `halt -n` вызов `sync` подавляется. Эта команда используется после исправления корневого раздела программой `fsck` для того, чтобы ядро не могло затереть исправления старыми версиями суперблока. Команда `halt -q` инициирует почти немедленный останов, без синхронизации, уничтожения процессов и записи в файлы регистрации. Этот флаг используется редко.

Команда `reboot` почти идентична команде `halt`. Различие заключается в том, что компьютер перезагружается с нуля, а не останавливается. Команда `reboot` вызывается командой:

```
shutdown -r
```

Описание команд приведено в `man halt` и `man reboot`.

4. СИСТЕМНЫЕ СЕРВИСЫ И КОМАНДЫ

4.1. Сервисы

Сервисы — это программы, которые запускаются и останавливаются через инициализированные скрипты, расположенные в каталоге `/etc/init.d`. Многие из этих сервисов запускаются на этапе старта ОС. `/usr/sbin/service` обеспечивает интерфейс (взаимодействие) пользователя с инициализированными скриптами. А сами эти скрипты обеспечивают интерфейс для управления сервисами, предоставляя пользователю опции для запуска, остановки, перезапуска, запроса состояния сервиса и выполнения других воздействий на сервис. К примеру, инициализированный скрипт сервиса `syslog` имеет следующие опции:

```
/usr/sbin/service cron
Usage: /etc/init.d/cron {start|stop|status|restart|reload|force-reload}
```

В ОС можно просмотреть текущее состояние всех системных служб с помощью опции `--status-all` команды `service`:

```
/usr/sbin/service --status-all
acpid (pid 2481) is running...
anacron (pid 2647) is running...
atd (pid 2657) is running...
auditd (pid 2189) is running...
```

Информация об уровне выполнения этих сервисов, т. е. установка того, на каком из системных уровней выполнения запускается тот или иной сервис во время загрузки системы, может быть получена или изменена с помощью команды `chkconfig`. Например, для службы системного протоколирования `syslog` установки по умолчанию выглядят следующим образом:

```
/sbin/chkconfig --list syslog
syslog   0:off   1:off   2:on   3:on   4:on   5:on   6:off
```

Сервис `syslog` автоматически запускается при переходе на уровни 2–5. Для того чтобы отключить его запуск на уровнях 3 и 4, можно воспользоваться следующей опцией команды `chkconfig`:

```
/sbin/chkconfig --levels 34 syslog off
```

В ОС существует шесть системных уровней выполнения, каждый из которых определяет список служб (сервисов), запускаемых на данном уровне. Уровни 0 и 6 соответствуют выключению и перезагрузке системы.

При загрузке системы процесс `init` запускает все сервисы, указанные в каталоге `/etc/rc(0-6).d/` для уровня по умолчанию. Поменять его можно в конфигурационном файле `/etc/inittab`. Строка:

```
id:2:initdefault:
```

соответствует второму уровню выполнения.

Команда `telinit` наиболее эффективна для тестирования изменений, внесенных в файл `inittab`. При указании аргумента `-q` процесс `init` повторно читает `inittab`.

Для перехода системы на нужный уровень выполнения можно воспользоваться командой `init`, например:

```
init 3
```

Данная команда переведет систему на третий уровень выполнения, запустив все сервисы, указанные в каталоге `/etc/rc3.d/`.

Описание данных команд и сервисов приведено на страницах руководства `man`.

4.2. Команды

Основные системные команды ОС приведены в таблице 6.

Таблица 6

Команда	Назначение
`addgroup`	Создание новой учетной записи группы
`adduser`	Создание новой учетной записи пользователя
`ar`	Создание и работа с библиотечными архивами
`at`	Формирование или удаление отложенного задания
`awk`	Язык обработки строковых шаблонов
`bc`	Строковый калькулятор
`chfn`	Управление информацией учетной записи пользователя (имя, описание)
`chsh`	Управление выбором командного интерпретатора (по умолчанию — для учетной записи)
`cut`	Разбивка файла на секции, задаваемые контекстными разделителями
`delgroup`	Удаление учетной записи группы
`deluser`	Удаление учетной записи пользователя и соответствующих файлов окружения
`df`	Вывод отчета об использовании дискового пространства
`dmesg`	Вывод содержимого системного буфера сообщений
`du`	Вычисление количества использованного пространства элементов ФС
`echo`	Вывод содержимого аргументов на стандартный вывод
`egrep`	Поиск в файлах содержимого согласно регулярных выражений
`fgrep`	Поиск в файлах содержимого согласно фиксированных шаблонов
`file`	Определение типа файла
`find`	Поиск файла по различным признакам в иерархии каталогов
`gettext`	Получение строки интернационализации из каталогов перевода
`grep`	Вывод строки, содержащей шаблон поиска

Продолжение таблицы 6

Команда	Назначение
groupadd	Создание новой учетной записи группы
groupdel	Удаление учетной записи группы
groupmod	Изменение учетной записи группы
groups	Вывод списка групп
gunzip	Распаковка файла
gzip	Упаковка файла
hostname	Вывод и задание имени хоста
install	Копирование файла с установкой атрибутов
ipcrm	Удаление ресурса IPC
ipcs	Вывод характеристик ресурса IPC
kill	Прекращение выполнения процесса
killall	Удаление процессов по имени
lpr	Система печати
ls	Вывод содержимого каталога
lsb_release	Вывод информации о дистрибутиве
m4	Макропроцессор
mknod	Создание файла специального типа
mktemp	Генерация уникального имени файла
more	Постраничный вывод содержимого файла
mount	Монтирование ФС
msgfmt	Создание объектного файла сообщений из файла сообщений
newgrp	Смена идентификатора группы
nice	Изменение приоритета процесса перед его запуском
nohup	Работа процесса после выхода из системы
od	Вывод содержимого файла в восьмеричном и других видах
passwd	Смена пароля учетной записи
patch	Применение файла описания изменений к оригинальному файлу
pidof	Вывод идентификатора процесса по его имени
ps	Вывод информации о процессах
renice	Изменение уровня приоритета процесса
sed	Строковый редактор
sendmail	Транспорт системы электронных сообщений
sh	Командный интерпретатор
shutdown	Команда останова системы

Окончание таблицы 6

Команда	Назначение
su	Изменение идентификатора запускаемого процесса
sync	Сброс системных буферов на носители
tar	Файловый архиватор
umount	Размонтирование ФС
useradd	Создание новой учетной записи пользователя или обновление существующей
userdel	Удаление учетной записи пользователя и соответствующих файлов окружения
usermod	Модификация информации об учетной записи пользователя
w	Список пользователей, кто в настоящий момент работает в системе и с чем
who	Вывод списка пользователей системы

Описание команд приведено на страницах руководства man.

4.2.1. Средства архивирования файлов

Команды tar, cpio, gzip представляют собой традиционные инструменты создания резервных копий и архивирования ФС. При создании архива командами tar и gzip передается список файлов и каталогов, указываемых как параметры командной строки. Любой указанный каталог просматривается рекурсивно. При создании архива с помощью команды cpio ей предоставляется список объектов (имена файлов и каталогов, символические имена любых устройств, гнезда доменов UNIX, поименованные каналы и т. п.).

Описание команд приведено на страницах руководства man.

4.2.1.1. tar

Команда tar может работать с рядом дисковых накопителей. Она проста в использовании, надежна, позволяет прочесть архивы в ОС.

В таблице 7 приведены некоторые наиболее часто используемые опции команды tar.

Таблица 7

Опция	Назначение
--acls	Сохраняет (восстанавливает) списки контроля доступа (ACL) каталогов и файлов, вложенных в архив
-c, --create	Создает архив
-x, --extract, --get	Восстанавливает файлы из архива на устройстве, заданном по умолчанию или определенном опцией f
--xattrs	Сохраняет (восстанавливает) расширенные атрибуты каталогов и файлов, вложенных в архив
-f, --file name	Создает (или читает) архив с name, где name — имя файла или устройства, определенного в /dev, например /dev/rmt0

Окончание таблицы 7

Опция	Назначение
`-Z, --compress, --uncompress`	Сжимает или распаковывает архив с помощью `compress`
`-z, --gzip, --gunzip`	Сжимает или распаковывает архив с помощью `gzip`
`-M, --multi-volume`	Создает многотомный архив
`-t, --list`	Выводит список сохраненных в архиве файлов
`-v, --verbose`	Выводит подробную информацию о процессе

Подробное описание команды приведено в `man tar`.

ВНИМАНИЕ! Для сохранения и восстановления мандатных атрибутов файлов требуется использование опций сохранения расширенных атрибутов `–xattrs` (см. примеры ниже и 9.5).

Примеры:

1. Копирование каталога `/home` на специальный раздел жесткого диска `/dev/hda4`

```
tar -cf /dev/hda4 /home
```

В этом примере опция `f` определяет создание архива на устройстве `/dev/hda4`.

2. Применение сжатия при архивировании

```
tar -cvfz /dev/hda4 /home | tee home.index
```

В этом примере опция `v` заставляет `tar` выводить подробную информацию, опция `z` говорит о том, что архив должен быть сжат с помощью утилиты `gzip`. Список скопированных файлов направляется в `home.index`.

3. Использование команды `find` для поиска измененных в течение одного дня файлов в каталоге `/home` и создание архива `home.new.tar` с этими файлами:

```
find /home -mtime 1 -type f -exec tar -rf home.new.tar {} \;
```

4. Если надо посмотреть содержимое архива, то можно воспользоваться опцией `–t` команды `tar`:

```
tar -tf home.new.tar
```

5. Восстановление из архива. Для извлечения файлов из архива необходимо указать путь к архиву либо устройству и путь к месту извлечения. Если архив (каталога `/home`) был создан командой:

```
tar -czf /tmp/home.tar /home
```

то извлекать его надо командой:

```
tar -xzf /tmp/home.tar /
```

6. Использование команды `tar` для создания архивов в ФС ОС, а не только на устройствах для архивирования (можно архивировать группу файлов с их структу-

рой каталогов в один файл, для чего передать имя создаваемого файла с помощью опции f вместо имени устройства)

```
tar cvf /home/backup.tar /home/dave
```

С помощью tar архивируется каталог с вложенными подкаталогами.

При этом создается файл /home/backup.tar, содержащий архив каталога /home/dave и всех файлов в его подкаталогах.

7. Использование tar, при котором будут восстановлены расширенные атрибуты каталогов и файлов, вложенных в архив.

ВНИМАНИЕ! Перед выполнением операции восстановления домашнего каталога должен быть создан пользователь, домашний каталог которого сохранялся.

Создание архива выполняется с помощью команды:

```
tar --xattrs -cvzf /opt/home.tgz /home/.pdp/user1
```

где

– опция --xattrs означает включение поддержки расширенных атрибутов;

– опции -cvzf необходимы для создания архива (create), включения режима отображения обрабатываемых файлов (verbose), применения метода сжатия (gzip), указания файла (file). соответственно.

Путь /opt/home.tgz означает место расположения созданного архива и его имя, путь /home/.pdp/user1 означает, что именно будет вложено в архив.

Извлечение выполняется с помощью команды:

```
tar --xattrs --xattrs-include=security.PDPL -xvf /opt/home.tgz -C /opt/
home2/
```

где

– опция --xattrs-include=security.PDPL означает подключаемый шаблон ключа xattrs для мандатных атрибутов;

– опции -xvf необходимы для извлечения архива (extract), включения режима отображения обрабатываемых файлов (verboze), указания файла (file), соответственно.

После извлечения архива необходимо выполнить команду для проверки сохраненных атрибутов:

```
pdp-ls -M /opt/home2
```

которая покажет вывод аналогичный этому:

```
drwx------m  2 user1 user1 Уровень_0:low:Нет:0x0 0:0:0:0
drwx------m 15 user1 user1 Уровень_1:low:Нет:0x0 1:0:0:0
drwx------m 15 user1 user1 Уровень_2:low:1:0x0   2:0:1:0
```

где наличие записей об уровне отличном от Уровень_0 означает, что извлечение архива выполнено с сохранением расширенных атрибутов.

Обычно при использовании команды tar стоит делать входом верхнего уровня каталог. В таком случае файлы при восстановлении будут располагаться в подкаталоге рабочего каталога и не будут его засорять.

Предположим, в рабочем каталоге имеется подкаталог data, содержащий несколько сотен файлов. В распоряжении есть два основных пути создания архива этого каталога. Можно войти в подкаталог и создать в нем архив, например:

```
pwd
/home/dave
cd data
pwd
/home/dave/data
tar cvf .. /data.tar *
```

Будет создан архив в каталоге /home/dave, содержащий файлы без указания их расположения в структуре каталогов. При попытке восстановить файлы из архива подкаталог не будет создан, и все сотни файлов окажутся в текущем каталоге.

Другой путь состоит в создании архива каталога, например:

```
pwd
/home/dave
tar cvf data.tar data
```

Будет создан архив каталога, в котором первой будет следовать ссылка на каталог. При восстановлении файлов из такого архива будет создан подкаталог в текущем каталоге, и файлы будут создаваться уже в нем.

Можно автоматизировать выполнение всех этих команд, поместив их в файл crontab суперпользователя. Например, следующая запись в файле crontab выполняет резервное копирование каталога /home ежедневно в 01:30:

```
30 01 *** tar -cvfz /dev/hda4 /home > home index
```

При необходимости более сложного архивирования есть язык сценариев оболочки, которые также могут быть запущены с помощью cron (4.2.2.2).

4.2.1.2. cpio

cpio — это команда общего назначения для копирования файлов.

Ее можно использовать с опцией -o для создания резервных архивов и с опцией -i — для восстановления файлов. Команда получает информацию от стандартного устройства ввода и посылает выводимую информацию на стандартное устройство вывода.

cpio может архивировать любой набор файлов, может архивировать специальные файлы, хранит информацию более эффективно, чем tar, пропускает сбойные сектора или блоки при восстановлении данных, ее архивы могут быть восстановлены в ОС.

Недостатком команды cpio является то, что для обновления архива следует ис-

пользовать язык программирования оболочки, чтобы создать соответствующий сценарий.

В таблице 8 приведены основные опции команды cpio.

Таблица 8

Опция	Назначение
-o	Создание архива в стандартное устройство вывода
-l	Восстановление файлов из архива, передаваемого на стандартное устройство ввода
-t	Создание списка содержимого стандартного устройства ввода

Подробное описание команды приведено в man cpio.

Примеры:

1. Копирование файлов из каталога /home в архив home.cpio

```
find /home/* | cpio -o > /tmp/home.cpio
```

2. Восстановление файлов из архива home.cpio с сохранением дерева каталогов и создание списка в файле bkup.index

```
cpio -id < /tmp/home.cpio > bkup.index
```

3. Использование команды find для поиска измененных за последние сутки файлов и сохранение их в архив home.new.cpio

```
find /home -mtime 1 -type f | cpio -o > /tmp/home.new.cpio
```

4. Восстановление файла /home/dave/notes.txt из архива home.cpio

```
cpio -id /home/dave/notes.txt < home.cpio
```

Для восстановления файла с помощью cpio следует указывать его полное имя.

Все эти команды могут выполняться автоматически путем их размещения в файле crontab суперпользователя. Пример записи, выполняющей резервное копирование каталога /home ежедневно в 01:30:

```
30 01 *** ls /home : cpio -o > /tmp/home.cpio
```

При необходимости более сложного резервного копирования можно создать соответствующий сценарий оболочки. Запуск подобных сценариев также может быть осуществлен посредством cron.

Создание резервных копий означает определение политики создания резервных копий для снижения потерь и восстановления информации после возможной аварии системы.

4.2.1.3. Комплекс программ Bacula

Bacula представляет собой комплекс программ, позволяющий системному администратору управлять процессами резервного копирования и восстановления данных, а также проверять резервные копии, в том числе в гетерогенных сетях.

Bacula — это сетевая клиент-серверная система резервного копирования. Про-

грамма обладает множеством возможностей, позволяющих легко находить и восстанавливать утраченные или поврежденные файлы. Из-за своей модульной архитектуры Bacula может масштабироваться от небольших автономных систем до больших сетей, состоящих из сотен компьютеров.

Bacula состоит из следующих составных частей:

– Bacula Director service — центральная программа, координирующая все выполняемые операции (функционирует в фоне);

– Bacula Console services — программа, позволяющая администратору взаимодействовать с центральной программой;

– Bacula File services — клиентская программа, устанавливаемая на каждый обслуживаемый компьютер;

– Bacula Storage services — программа, обычно функционирующая на компьютере, к которому присоединены внешние устройства для хранения резервных копий;

– Catalog services — программа, отвечающая за индексирование и организацию базы резервных данных.

Программа Bacula обеспечивает поддержку сохранения расширенных атрибутов каталогов и файлов и, при необходимости, их последующее восстановление.

ВНИМАНИЕ! После восстановления объектов ФС с установленными мандатными атрибутами необходимо выполнить перемонтирование ФС, в которой восстанавливались объекты, или перезагрузить ОС.

Описание установки и настройки Bacula приведено в 9.3.

4.2.2. Планирование запуска команд

4.2.2.1. at

Для запуска одной или более команд в заранее определенное время используется команда at. В ней можно определить время и/или дату запуска той или иной команды. Команда at требует двух (или большего числа) параметров. Как минимум, следует указать время запуска и какая команда должна быть запущена.

Например, если необходимо запустить команды в 8:00, следует ввести:

```
at 8:00
lpr /usr/sales/reports/.
echo "Files printed"
```

Команды для запуска с помощью команды at вводятся как список в строках, следующих за ней. Ввод каждой строки завершается нажатием клавиши **<Enter>**. По окончании ввода всей команды нажать клавиши **<Ctrl+D>** для ее завершения.

В примере в 8:00 будут распечатаны все файлы каталога /usr/sales/reports, и

пользователю будет выведено сообщение на экран монитора.

После ввода всей команды отобразится следующая запись:

```
job 756603300.a at Tue Jul 8 08:00:00 2014
```

Это означает, что указанные команды будут запущены, как и было заказано, в 8:00. Здесь приведен также идентификатор задания (`756603300.a`), который понадобится, например, если необходимо отменить задание:

```
at -d 756603300.a
```

Если список команд находится в файле, например, `getdone` и необходимо запустить все перечисленные в нем команды в 17:30, следует воспользоваться одной из двух форм команды `at`:

```
at 17:30 < getdone
```

или:

```
at 10:30 -f getdone
```

Обе приведенные команды эквивалентны. Разница заключается в том, что в первой команде используется механизм перенаправления потоков ввода-вывода, во второй команде — дисковый файл.

Кроме времени, в команде `at` может быть также определена дата, например:

```
at 10:00 Jul 14
lp /usr/sales/reports/
echo "Files printed"
```

Задания, определяемые администратором системы, помещаются в очередь, которую ОС периодически просматривает. Администратору необязательно находиться в системе для того, чтобы `at` отработала задания. В данном случае команда работает в фоновом режиме.

Для того чтобы просмотреть очередь заданий, ввести:

```
at -l
```

Если предыдущие примеры были запущены, то будет выведено:

```
job 756603300.a at Sat Jul 8 08:00:00 2014 job 756604200.a at Sat Jul 14
  17:00:00 2014
```

Администратор системы видит только свои задания по команде `at`.

Для удаления задания из очереди следует запустить `at` с опцией `-d` и номером удаляемого задания, например:

```
at -d 756604200.a
```

В таблице 9 показаны различные варианты использования команды `at`.

Окончание таблицы 9

Формат команды	Назначение

Таблица 9

Формат команды	Назначение
`at hh:mm`	Выполнить задание во время `hh:mm` в 24-часовом формате
`at hh:mm месяц день год`	Выполнить задание во время `hh:mm` в 24-часовом формате в соответствующий день
`at -l`	Вывести список заданий в очереди; псевдоним команды — `atq`
`at now+count time-units`	Выполнить задание через определенное время, которое задано параметром `count` в соответствующих единицах — неделях, днях, часах или минутах
`at -d job_ID`	Удалить задание с идентификатором `job_ID` из очереди; псевдоним команды — `atrm`

Администратор системы может применять все эти команды. Для других пользователей права доступа к команде `at` определяются файлами `/etc/at.allow` и `/etc/at.deny`. Если существует файл `/etc/at.allow`, то применять команду `at` могут только перечисленные в нем пользователи. Если же такого файла нет, проверяется наличие файла `/etc/at.deny`, в котором отражено, кому запрещено пользоваться командой `at`. Если ни одного файла нет, значит, команда `at` доступна только суперпользователю.

Подробное описание команды приведено в `man at`.

4.2.2.2. cron

Для регулярного запуска команд в ОС существует команда `cron`. Администратор системы определяет время и даты, когда должна запускаться та или иная программа в минутах, часах, днях месяца, месяцах года и днях недели.

Команда `cron` запускается один раз при загрузке системы. Отдельные пользователи не должны иметь к ней непосредственного доступа. Кроме того, запуск `cron` никогда не осуществляется вручную, путем ввода имени программы в командной строке, а только из сценария загрузки ОС.

При запуске `cron` проверяет очередь заданий команды `at` и задания пользователей в файлах `crontab`. Если ничего для запуска не нашлось, `cron` «засыпает» на одну минуту и затем вновь приступает к поискам команды, которую следует запустить в этот момент. Большую часть времени команда `cron` проводит в «спящем» состоянии, и для ее работы используется минимум системных ресурсов.

Чтобы определить список задач для `cron`, используется команда `crontab`. Для каждого пользователя с помощью этой команды создается его собственный файл `crontab` со списком заданий, находящийся в каталоге `/usr/spool/cron/crontabs` и имеющий то

же имя, что и имя пользователя.

Примечание. Пользователи, которым разрешено давать задания команде cron, перечислены в файле etc/cron/.d/cron.allow. Хотя можно создать файл заданий для команды cron с помощью обычного текстового редактора, нельзя просто заменить им существующий файл задания (в каталоге /usr/spool/cron/crontabs). Для передачи cron сведений о новых заданиях обязательно должна использоваться команда crontab.

Каждая строка в файле crontab содержит шаблон времени и команду. Команда выполняется тогда, когда текущее время соответствует приведенному шаблону. Шаблон состоит из пяти частей, разделенных пробелами или символами табуляции.

Синтаксис команд в файле crontab:

```
минуты часы день_месяца месяц_ года день_недели задание
```

Первые пять полей представляют шаблон времени и обязательно должны присутствовать в файле. Для того чтобы cron игнорировала то или иное поле шаблона времени, следует поставить в ней символ * (звездочка).

Примечание. С точки зрения программы символ * означает скорее не «игнорировать поле», а «любое корректное значение», т. е. соответствие чему угодно.

Например, шаблон

```
02 00 01 * *
```

говорит о том, что команда должна быть запущена в две минуты пополуночи (поле часов нулевое) каждого первого числа любого (первая звездочка) месяца, каким бы днем недели оно не было (вторая звездочка).

В таблице 10 приведены допустимые значения полей записей crontab.

Таблица 10

Поле	Диапазон
минуты	00–59
часы	00–23 (полночь — 00)
день_месяца	01–31
день_года	01–12
день_недели	01–07 (понедельник — 01, воскресенье — 07)

Можно создать любое количество команд для cron, их число ничем не ограничено. Например, необходимо сортировать и отправлять пользователю pav файл /usr/sales/weekly каждый понедельник в 7:30. Соответствующая запись будет выглядеть так:

```
30 07 * * 01 sort /usr/sales/weekly | mail -s"Weekly Sales" pav
```

Поле команд может содержать все, что может быть в команде, вводимой в команд-

ной строке оболочки. В нужное время cron для выполнения команд запустит стандартную оболочку (bash) и передаст ей команду для выполнения.

Для того чтобы определить несколько значений в поле, используется в качестве разделяющего символа запятая. Например, если программа chkquotes должна выполняться в 9, 11, 14 и 16 часов по понедельникам, вторникам и четвергам 10 марта и 10 сентября, то запись выглядит так:

```
. 09,11,14,16 10 03,09 01,02,04 chkquotes
```

Опции командной строки crontab приведены в таблице 11.

Таблица 11

Опция	Описание
-e	Позволяет редактировать компоненты файла (при этом вызывается редактор, определенный в переменной EDITOR оболочки)
-r	Удаляет текущий файл crontab из каталога
-l	Используется для вывода списка текущих заданий cron

В любом случае crontab работает с файлом согласно регистрационному имени.

В случае команды cron как администратор системы, так и пользователи несут ответственность за корректное ее использование, которое не должно, например, вызвать перегрузку системы.

Подробное описание команд и файла crontab приведено в man cron, man crontab и man 5 crontab.

4.2.3. Администрирование многопользовательской и многозадачной среды

4.2.3.1. who

Для получения списка пользователей, работающих в ОС, используется команда who, перечисляющая идентификаторы активных пользователей, терминалы и время входа в систему.

Для получение списка зарегистрировавшихся в системе пользователей ввести команду who, и на экране монитора появится список, например:

```
who
root console May 19 07:00
```

Команда who имеет несколько опций, однако здесь рассмотрены только две из них:

1) -u — перечисляет пользователей с указанием времени бездействия (точка . означает, что пользователь активно работал в последнюю минуту, old — что последний раз он нажимал клавиши более суток назад);

2) -H — заставляет команду выводить подробную информацию о пользователях; при этом выводит строку заголовка таблицы пользователей, столбцы которой пока-

заны в таблице 12.

Таблица 12

Поле	Описание
NAME	Имена пользователей
LINE	Использованные линии и терминалы
TIME	Время, прошедшее после регистрации пользователя в системе
IDLE	Время, прошедшее со времени последней активной работы пользователя
PID	Идентификатор процесса входной оболочки пользователя
COMMENT	Комментарий (если таковые имеются в файле /etc/inittab)

С помощью опций -u и -H можно увидеть:

```
who -uH
NAME LINE    TIME           IDLE    PID     COMMENT
root console Dec 12 08:00   .       10340
```

В список включен идентификатор процесса оболочки пользователя.

Подробное описание команды приведено в man who.

4.2.3.2. ps

Для получения информации о состоянии запущенных процессов используется команда ps. Она выдает: какие из них выполнены, какие вызвали проблемы в системе, как долго выполняется тот или иной процесс, какие он затребовал системные ресурсы, идентификатор процесса (который будет необходим, например, для прекращения работы процесса с помощью команды kill) и т. д. Вся эта информация полезна как для рядового пользователя, так и для системного администратора. Запущенная без опций командной строки ps выдает список процессов, порожденных администратором.

Наиболее распространенное применение команды ps — отслеживание работы фоновых и других процессов в системе. Поскольку в большинстве случаев фоновые процессы никак не взаимодействуют ни с экраном, ни с клавиатурой, команда ps остается основным средством наблюдения за ними.

Команда ps выводит четыре основных поля информации для каждого процесса (таблица 13).

Таблица 13

Поле	Описание
PID	Идентификатор процесса
TTY	Терминал, с которого был запущен процесс
TIME	Время работы процесса

Окончание таблицы 13

Поле	Описание
COMMAND	Имя выполненной команды

Подробное описание команды приведено в `man ps`.

4.2.3.3. nohup

Обычно дочерний процесс прекращается после родительского. Таким образом, если запущен фоновый процесс, он будет прекращен при выходе из системы. Для того чтобы процесс продолжал выполняться даже после выхода из системы, применяется команда `nohup`. Ее следует поместить в начало командной строки, например:

```
nohup sort sales.dat &
```

Эта команда заставляет ОС игнорировать выход из нее и продолжать выполнение до тех пор, пока процесс не закончится сам по себе. Таким образом, будет запущен процесс, который будет выполняться длительное время, не требуя контроля администратора системы.

Подробное описание команды приведено в `man nohup`.

4.2.3.4. nice

Команда `nice` позволяет запустить другую команду с предопределенным приоритетом выполнения, предоставляя администратору системы возможность определять приоритет при выполнении своих задач. При обычном запуске все задачи имеют один и тот же приоритет, и ОС равномерно распределяет между ними процессорное время. С помощью команды `nice` можно понизить приоритет какой-либо «неспешной» задачи, предоставив другим задачам больше процессорного времени. Повысить приоритет той или иной задачи имеет право только суперпользователь.

Синтаксис команды `nice`:

```
nice –number command
```

Уровень приоритета определяется параметром `number`, при этом большее его значение означает меньший приоритет команды. Значение по умолчанию равно 10, и `number` представляет собой число, на которое он должен быть уменьшен. Например, если запущен процесс сортировки:

```
sort sales.dat > sales.srt &
```

и ему следует дать преимущество над другим процессом, например печати, запустить этот второй процесс с уменьшенным приоритетом:

```
nice –5 lp mail_list &
```

Для того чтобы назначить процессу печати самый низкий возможный приоритет, ввести:

```
nice –10 lp mail_list &
```

Примечание. В случае команды nice тире означает знак опции.

Только суперпользователь может повысить приоритет того или иного процесса, применяя для этого отрицательное значение аргумента. Максимально возможный приоритет — 20; присвоить его процессу суперпользователь может с помощью команды:

```
nice --10 job &
```

Наличие & в примере достаточно условно, можно изменять приоритеты как фоновых процессов, так и процессов переднего плана.

Подробное описание команды приведено в man nice.

4.2.3.5. renice

Команда renice позволяет изменить приоритет работающего процесса. Формат этой команды подобен формату команды nice:

```
renice -number PID
```

Для изменения приоритета работающего процесса необходимо знать его идентификатор, получить который можно с помощью команды ps, например, вызвав:

```
ps -e : grep name
```

В данной команде необходимо заменить name именем интересующего процесса. Команда grep отфильтрует только те записи, в которых будет встречаться имя нужной команды, и можно будет узнать идентификатор ее процесса. Если необходимо изменить приоритет всех процессов пользователя или группы пользователей, в команде renice используется идентификатор пользователя или группы.

Рассмотрим пример использования команды renice, предположив, что имя пользователя — pav:

```
ps -ef : grep $LOGNAME
pav 11805 11804 0 Dec 22 ttysb 0:01 sort sales.dat > sales srt
pav 19955 19938 4 16:13:02 ttypo 0:00 grep pav
pav 19938    1 0 16:11:04 ttypo 0-00 bash
pav 19940 19938 42 16:13:02 ttypo 0:33 find . -name core -exec nn {};
```

Теперь, чтобы понизить приоритет процесса find с идентификатором 19940, ввести:

```
renice -5 19940
```

В случае команды renice работают те же правила, что и в случае команды nice, а именно:

– ее можно использовать только со своими процессами;

– суперпользователь может применить ее к любому процессу;

– только суперпользователь может повысить приоритет процесса.

Подробное описание команды приведено в man renice.

4.2.3.6. kill

Иногда необходимо прекратить выполнение процесса, не дожидаясь его нормального завершения. Это может произойти в следующих случаях:

1) процесс использует слишком много времени процессора и ресурсов компьютера;
2) процесс работает слишком долго, не давая ожидаемых результатов;
3) процесс производит слишком большой вывод информации на экран или в файл;
4) процесс привел к блокировке терминала или другой сессии;
5) из-за ошибки оператора или программы используются не те файлы или параметры командной строки;
6) дальнейшее выполнение процесса бесполезно.

Если процесс работает не в фоновом режиме, нажатие клавиш **<Ctrl+C>** должно прервать его выполнение, но если процесс фоновый, это не поможет. В этом случае прервать его выполнение можно только с помощью команды `kill`, которая посылает процессу сигнал, требующий от процесса завершения. Для этого используются две формы:

```
kill PID(s)
kill –signal PID(s)
```

Для завершения процесса с идентификатором `127` ввести:

```
kill 127
```

Для того чтобы завершить процессы `115`, `225` и `325`, ввести:

```
kill 115 225 325
```

С помощью опции `–signal` можно, например, заставить процесс перечитать конфигурационные файлы без прекращения работы. Список доступных сигналов можно получить с помощью команды:

```
kill –l
```

При успешном завершении процесса никакое сообщение не выводится. Сообщение появится при попытке завершения процесса без наличия соответствующих прав доступа или при попытке завершить несуществующий процесс.

Завершение родительского процесса иногда приводит к завершению дочерних, однако для полной уверенности в завершении всех процессов, связанных с данным, следует указывать их в команде `kill`.

Если терминал оказался заблокированным, можно войти в систему с другого терминала:

```
ps –ef: grep $LOGNAME
```

и завершить работу оболочки на блокированном терминале.

При выполнении команда `kill` посылает процессу соответствующий сигнал. Программы ОС могут посылать и принимать более 20 сигналов, каждый из которых имеет свой номер. Например, при выходе администратора ОС посылает всем его процессам сигнал 1,

который заставляет все процессы (кроме запущенных с помощью `nohup`) прекратить работу. Программы могут быть написаны и таким образом, что будут игнорировать посылаемые им сигналы, включая сигнал 15, который возникает при запуске команды `kill` без указания конкретного сигнала.

Однако сигнал 9 не может быть проигнорирован — процесс все равно будет завершен. Таким образом, если команда:

```
kill PID
```

не смогла завершить процесс (он виден при использовании команды `ps`), необходимо воспользоваться командой:

```
kill -9 PID
```

Команда:

```
kill -9
```

прекращает процесс, не давая возможности, например, корректно закрыть файлы, что может привести к потере данных. Использовать эту возможность следует только в случае крайней необходимости.

Для завершения всех фоновых процессов ввести:

```
kill 0
```

Преимущественное право контроля над процессом принадлежит владельцу. Права владельца могут отменяться только суперпользователем.

Ядро назначает каждому процессу четыре идентификатора: реальный и эффективный UID, реальный и эффективный GID. Реальные ID используются для учета использования системных ресурсов, а эффективные — для определения прав доступа. Как правило, реальные и эффективные ID совпадают. Владелец процесса может посылать в процесс сигналы, а также понижать приоритет процесса.

Процесс, приступающий к выполнению другого программного файла, осуществляет один из системных вызовов семейства `exec`. Когда такое случается, эффективные UID и GID процесса могут быть установлены равными UID и GID файла, содержащего образ новой программы, если у этого файла установлены биты смены идентификатора пользователя и идентификатора группы. Системный вызов `exec` — это механизм, с помощью которого такие команды, как `passwd`, временно получают права суперпользователя (команде `passwd` они нужны для того, чтобы изменить `/etc/passwd`).

Подробное описание команды приведено в `man kill`.

4.3. Графические утилиты

В состав рабочего стола Fly входит большое количество графических утилит, которые могут быть использованы для администрирования системы. Большинство из этих утилит представляет собой графические оболочки над соответствующими текстовыми ути-

литами командной строки.

Список утилит приведен в разделе 7, а описание утилит см. в электронной справке.

5. БАЗОВЫЕ СЕТЕВЫЕ СЛУЖБЫ

5.1. Сеть TCP/IP

5.1.1. Пакеты и сегментация

Данные передаются по сети в форме сетевых пакетов, каждый из которых состоит из заголовка и полезной нагрузки. Заголовок содержит сведения о том, откуда прибыл пакет и куда он направляется. Заголовок, кроме того, может включать контрольную сумму, информацию, характерную для конкретного протокола, и другие инструкции по обработке. Полезная нагрузка — это данные, подлежащие пересылке.

5.1.2. Адресация пакетов

Сетевые пакеты могут достичь пункта назначения только при наличии правильного сетевого адреса. Протокол TCP/IP использует сочетание нескольких схем сетевой адресации.

Самый нижний уровень адресации задается сетевыми аппаратными средствами.

На следующем, более высоком, уровне используется адресация Интернет (которую чаще называют «IP-адресацией»). Каждому включенному в сеть устройству присваивается один четырехбайтовый IP-адрес (в соответствии с протоколом IPv4). IP-адреса глобально уникальны и не зависят от аппаратных средств.

IP-адреса идентифицируют компьютер, но не обеспечивают адресацию отдельных процессов и служб. Протоколы TCP и UDP расширяют IP-адреса, используя порты. Порт в данном случае представляет собой двухбайтовое число, добавляемое к IP-адресу и указывающее конкретного адресата той или иной сетевой службы. Все стандартные UNIX-службы связываются с известными портами, которые определены в файле `/etc/services`. Для того чтобы предотвратить попытки нежелательных процессов замаскироваться под эти программы, установлено, что порты с номерами до 1024 могут использоваться только суперпользователем. Описание файла `/etc/services` приведено в `man services`.

5.1.3. Маршрутизация

5.1.3.1. Таблица

Маршрутизация — это процесс направления пакета по ряду сетей, находящихся между источником и адресатом.

Данные маршрутизации хранятся в таблице маршрутизации. Каждый элемент этой таблицы содержит несколько параметров, включая поле надежности, которое расставляет маршруты по приоритетам, если таблица содержит противоречивую информацию. Для направления пакета по конкретному адресу подбирается наиболее подходящий маршрут.

Если нет ни такого маршрута, ни маршрута по умолчанию, то отправителю возвращается ошибка: «network unreachable» (сеть недоступна).

Таблицу маршрутизации компьютера можно вывести на экран монитора с помощью команды `route`.

5.1.3.2. Организация подсетей

Организация подсетей задается маской подсети, в которой биты сети включены, а биты компьютера выключены. Маска подсети задается во время начальной загрузки, когда конфигурируется сетевой интерфейс командой `ifconfig`. Ядро, как правило, использует сам класс IP-адресов для того, чтобы выяснить, какие биты относятся к сетевой части адреса; если задать маску явно, то эта функция просто отменяется.

При организации подсетей необходимо учесть, что если вычислительная сеть имеет более одного соединения с сетью Интернет, то другие сети должны уметь отличать подсети сети пользователя, чтобы определить в какой маршрутизатор следует послать пакет.

5.1.4. Создание сети TCP/IP

Процесс создания сети TCP/IP состоит из следующих этапов:

– планирование сети;
– назначение IP-адресов;
– настройка сетевых интерфейсов;
– настройка статических маршрутов.

5.1.4.1. Планирование сети

Планирование сети включает: определение сегментов сети, определение технических и программных средств, с помощью которых сегменты объединяются в сеть, определение серверов и рабочих станций, которые будут установлены в каждом сегменте, и определение типа среды (витая пара и др.).

5.1.4.2. Назначение IP-адресов

Адреса назначают сетевым интерфейсам, а не компьютерам. Если у компьютера есть несколько интерфейсов, у него будет несколько сетевых адресов.

Назначая компьютеру IP-адрес, следует указать соответствие между этим адресом и именем компьютера в файле `/etc/hosts`. Это соответствие позволит обращаться к компьютерам по их именам.

5.1.4.3. Настройка сетевых интерфейсов

Команда `ifconfig` используется для включения и выключения сетевого интерфейса, задания IP-адреса, широковещательного адреса и связанной с ним маски подсети, а также для установки других опций и параметров. Она обычно выполняется во время первоначальной настройки, но может применяться и для внесения изменений в дальнейшем.

В большинстве случаев команда `ifconfig` имеет следующий формат:

```
ifconfig интерфейс [семейство] адрес up опция ...
```

Пример

```
ifconfig eth0 128.138.240.1 up netmask 255.255.255.0 broadcast 128.138.240.255
```

Здесь интерфейс обозначает аппаратный интерфейс, к которому применяется команда. Как правило, это двух-трехсимвольное имя устройства, за которым следует число. Примеры распространенных имен `eth1`, `lo0`, `ppp0` образуются из имени драйвера устройства, используемого для управления им. Для того чтобы выяснить, какие интерфейсы имеются в системе, можно воспользоваться командой:

```
netstat-i
```

Ключевое слово `up` включает интерфейс, а ключевое слово `down` выключает его.

Описание команды приведено в `man ifconfig`.

5.1.4.4. Настройка статических маршрутов

Команда `route` определяет статические маршруты — явно заданные элементы таблицы маршрутизации, которые обычно не меняются даже в тех случаях, когда запускается серверный процесс маршрутизации.

Маршрутизация выполняется на уровне IP. Когда поступает пакет, предназначенный для другого компьютера, IP-адрес пункта назначения пакета сравнивается с маршрутами, указанными в таблице маршрутизации ядра. Если номер сети пункта назначения совпадает с номером сети какого-либо маршрута, то пакет направляется по IP-адресу следующего шлюза, связанного с данным маршрутом.

Существующие маршруты можно вывести на экран командой `route`.

Описание команды приведено в `man route`.

5.1.5. Проверка и отладка сети

5.1.5.1. ping

Команда `ping` служит для проверки соединений в сетях на основе TCP/IP.

Она работает в бесконечном цикле, если не задан аргумент `число пакетов`. Чтобы прекратить работу команды `ping`, необходимо нажать **<Ctrl+C>**.

Описание команды приведено в `man ping`.

5.1.5.2. netstat

Команда `netstat` выдает информацию о состоянии, относящуюся к сетям:

– проверка состояния сетевых соединений;

– анализ информации о конфигурации интерфейсов;

– изучение таблицы маршрутизации;

– получение статистических данных о различных сетевых протоколах.

Команда `netstat` без аргументов выдает информацию о состоянии активных портов TCP и UDP. Неактивные серверы, ожидающие установления соединения, как правило, не показываются (их можно просмотреть командой `netstat -a`).

Команда `netstat -i` показывает состояние сетевых интерфейсов.

Команда `netstat -r` выдает таблицу маршрутизации ядра.

Команда `netstat -s` выдает содержимое счетчиков, разбросанных по сетевым программам.

Описание команды приведено в `man netstat`.

5.1.5.3. arp

Команда `arp` обращается к таблице ядра, в которой задано соответствие IP-адресов аппаратным адресам. В среде Ethernet такие таблицы ведутся с помощью протокола ARP и не требуют администрирования.

Команда `arp -a` распечатывает содержимое таблицы соответствий.

Описание команды приведено в `man arp`.

5.2. Служба FTP

В ОС передача файлов обеспечивается с помощью интерактивной команды `lftp`, вызываемой на клиентской стороне, и сервера `vsftpd`, который запускается на компьютере, выполняющем функцию сервера службы FTP. Обе команды реализуют протокол передачи файлов FTP. Для копирования файлов клиенту обычно (хотя существует и вариант анонимного доступа) необходимо знание имени и пароля пользователя, которому принадлежат файлы на сервере службы FTP.

5.2.1. Клиентская часть

Вызов команды `lftp` осуществляется командой:

```
lftp имя сервера
```

Интерактивный доступ к серверу службы FTP обеспечивается следующими основными внутренними командами `lftp`:

- `open`, `user`, `close` — связь с удаленным компьютером;
- `lcd`, `dir`, `mkdir`, `lpwd` — работа с каталогами в FTP-сервере;
- `get`, `put`, `ftpcopy` — получение и передача файлов;
- `ascii`, `binary`, `status` — установка параметров передачи.

Выход из команды `lftp` осуществляется по команде `exit`.

Описание команды приведено в `man lftp`.

5.2.2. Сервер VSFTPD

В ОС программный пакет `vsftpd` устанавливается командой:

```
apt-get install vsftpd
```

Пакет также может быть установлен в процессе установки ОС. Для этого следует в окне программы установки «Выбор программного обеспечения» отметить группу пакетов «Сетевые сервисы».

После установки следует обратить внимание на файлы документации в каталоге /usr/share/doc/vsftpd, где каталог EXAMPLE содержит различные примеры конфигурационного файла сервера vsftpd.conf. В руководстве man подробно описаны все возможности программы.

Сама команда располагается в каталоге /usr/sbin/vsftpd.

5.2.2.1. Конфигурационный файл

После установки сервера vsftpd он сразу готов к работе с опциями по умолчанию. Если для работы сервера необходимы другие значения опций, следует отредактировать конфигурационный файл /etc/vsftpd.conf.

В файле vsftpd.conf представлены три вида опций:

– BOOLEAN — опции, которые могут содержать значения: YES, NO;

– NUMERIC — опции, содержащие различные цифровые значения (к примеру, время в секундах или номер порта соединения);

– STRING — опции, содержащие текстовую строку (к примеру, путь к каталогу на диске).

Следует заметить, что некоторые опции могут явно отсутствовать в конфигурационном файле. Это означает, что для них используется значение, заданное по умолчанию и обозначаемое как Default: в руководстве man.

Не все опции следует указывать напрямую, иначе конфигурационный файл может вырасти до очень больших размеров. В большинстве случаев необходимо записать в файл всего лишь несколько строк, а для остальных настроек использовать значения по умолчанию.

Многие настройки зависят от других опций. Если те опции, от которых они зависят, отключены, то и данные настройки не будут работать. Некоторые опции являются взаимоисключающими и, следовательно, не будут работать в паре с другими такими включенными опциями.

Описание службы vsftpd и файла vsftpd.conf приведено на страницах руководства man.

5.3. Служба DHCP

На компьютере, выполняющем роль сервера динамической конфигурации сети, должна быть установлена служба dhcpd. Настройки этой службы хранятся в файле /etc/dhcpd.conf. Файл настройки содержит инструкции, которые определяют, какие под-

сети и узлы обслуживает сервер и какую информацию настройки он им предоставляет.

Сервер динамически назначает IP-адреса DHCP-клиентам обеих подсетей и осуществляет поддержку нескольких клиентов BOOTP. Первые несколько активных строк файла определяют ряд параметров и режимов, действующих для всех обслуживаемых сервером подсетей и клиентов. Конструкция каждой строки есть реализация шаблона «параметр — значение». «Параметр» может быть общим или стоять перед ключевым словом `option`. Параметры, следующие за словом `option`, — это ключи настройки. Они также состоят из имени ключа и его значения.

Кроме общих параметров, существуют т. н. «операторы топологии сети» или «объявления».

Описание некоторых параметров настройки сервера `dhcpd`, содержащихся в файле `dhcpd.conf`, приводится в таблице 14.

Таблица 14

Параметр	Описание
`max-lease-time`	Определяет максимально допустимое время аренды. Независимо от длительности аренды, фигурирующей в запросе клиента, этот срок не может превышать значение, заданное данным параметром
`get-lease-hostnames`	Предписывает `dhcpd` предоставлять каждому клиенту наряду с динамическим адресом имя узла. Имя узла должно быть получено от DNS. Данный параметр — логический. При значении `FALSE` назначается адрес, но не имя узла. Значение `TRUE` используется только в сетях с небольшим количеством хостов, которым выделяются имена, т. к. поиск имен в DNS замедляет запуск демона
`hardware type address`	Параметр определяет аппаратный адрес клиента. Значение `type` может быть `ethernet` или `token-ring`. `address` должен быть соответствующим устройству физическим адресом. Параметр должен быть связан с оператором `host`. Он необходим для распознавания клиента BOOTP
`filename file`	Указывает файл загрузки для бездисковых клиентов. `file` — это ASCII-строка, заключенная в кавычки
`range [dynamic-bootp]`	Данный параметр указывает диапазон адресов. После него через пробел указывается нижний адрес диапазона и опционально верхний адрес. Если верхний адрес не указан, занимается весь теоретически возможный диапазон от нижнего адреса. Этот параметр всегда связан с оператором `subnet`. Все адреса должны принадлежать этой подсети. Флаг `dynamic-bootp` указывает, что адреса могут автоматически назначаться клиентам BOOTP так же, как и клиентам DHCP. Если оператор `subnet` не содержит параметра `range`, для такой подсети динамическое распределение адресов не действует
`server-name name`	Имя сервера DHCP, передаваемое клиенту. `name` — это ASCII-строка, заключенная в кавычки

Окончание таблицы 14

Параметр	Описание
`next-server name`	Имя узла или адрес сервера, с которого следует получить загрузочный файл
`fixed-address`	Назначает узлу один или несколько фиксированных адресов. Действителен только в сочетании с параметром `host`. Если указано несколько адресов, выбирается адрес, корректный для данной сети, из которой выполняет загрузку клиент. Если такого адреса нет, никакие параметры не передаются
`dynamic-bootp-lease-cuttof date`	Устанавливает дату завершения действия адресов, назначенных клиентам BOOTP. Клиенты BOOTP не обладают способностью обновлять аренду и не знают, что срок аренды может истечь. Этот параметр меняет поведение сервера и используется только в особых случаях
`dynamic-bootp-lease-length`	Длительность аренды в секундах для адресов, автоматически назначаемых клиентам BOOTP. Данный параметр используется в особых ситуациях, когда клиенты используют образ загрузки BOOTP PROM. В ходе загрузки клиент действует в качестве клиента BOOTP, а после загрузки работает с протоколом DHCP и умеет обновлять аренду
`use-host-decl-names`	Предписывает передавать имя узла, указанное в операторе `host`, клиенту в качестве его имени. Логический параметр, может иметь значения `TRUE` или `FALSE`
`server-identifier hostname`	Определяет значение, передаваемое в качестве идентификатора сервера. По умолчанию передается первый IP-адрес сетевого интерфейса
`authoritative not authoritative`	Указывает, является ли сервер DHCP компетентным. `not authoritative` используется, когда в компетенцию сервера не входит распределение адресов клиентам
`use-lease-addr-for-default-route`	Логический параметр (`TRUE` или `FALSE`). Предписывает передавать клиенту арендованный адрес в качестве маршрута по умолчанию. Параметр используется только тогда, когда локальный маршрутизатор является сервером-посредником ARP. Оператор настройки `routers` имеет более высокий приоритет
`always-replay-rfc1048`	Логический параметр. Предписывает посылать клиенту BOOTP ответы в соответствии с RFC 1048
`allow keyword deny keyword`	Определяет необходимость отвечать на запросы различных типов. Ключевое слово `keyword` указывает тип разрешенных и запрещенных запросов. Существуют следующие ключевые слова: – `unknown-clients` — определяет возможность динамического назначения адресов неизвестным клиентам; – `bootp` — определяет необходимость отвечать на запросы BOOTP (по умолчанию обслуживаются); – `booting` — используется внутри объявления `host` для указания необходимости отвечать тому или иному клиенту. По умолчанию сервер отвечает всем клиентам

Каждый из операторов топологии может многократно встречаться в файле настрой-

ки. Операторы определяют иерархическую структуру. Операторы топологии, встречающиеся в файле dhcp.conf, приведены в таблице 15.

Таблица 15

Оператор	Описание
group {[parameters] [options]}	Группирует операторы shared-network, subnet, host и другие операторы group. Позволяет применять наборы параметров и опций ко всем элементам группы
shared-network name {[parameters] [options]}	Используется только в случае, когда несколько подсетей находятся в одном физическом сегменте. В большинстве случаев различные подсети находятся в различных физических сетях. В качестве имени name может использоваться любое описательное имя. Оно используется только в отладочных сообщениях. Параметры и опции, связанные с общей сетью, объявляются внутри фигурных скобок и действуют на все подсети общей сети. Каждый оператор shared-network содержит не менее двух операторов subnet, в противном случае нет необходимости использовать группирование

Общеупотребительные опции, следующие за ключевым словом option в файле dhcp.conf, приведены в таблице 16.

Таблица 16

Опция	Описание
subnet-mask	Определяет маску подсети в формате десятичной записи через точку. Если subnet-mask отсутствует, dhcpd использует маску подсети из оператора subnet
time-offset	Указывает разницу данного часового пояса с временем UTC в секундах
routers	Перечисляет адреса доступных клиентам маршрутизаторов в порядке предпочтения
domain-name-servers	Перечисляет адреса доступных клиентам серверов DNS в порядке предпочтения
lpr-servers	Перечисляет адреса доступных клиентам серверов печати LPR в порядке предпочтения
host-name	Указывает имя узла для клиента
domain-name	Определяет имя домена
interface-mtu	Определяет значение MTU для клиента в байтах. Минимально допустимое значение — 68
broadcast-address	Определяет широковещательный адрес для подсети клиента
static-routes destination gateway	Перечисляет доступные клиенту статические маршруты. Маршрут по умолчанию не может быть указан таким способом. Для его указания используется опция routers

Окончание таблицы 16

Опция	Описание
`trailer-encapsulation`	Определяет, следует ли клиенту выполнять инкапсуляцию завершителей (оптимизация, основанная на изменении порядка данных). Значение 0 означает, что инкапсуляцию выполнять не следует, 1 имеет противоположный смысл
`nis-domain string`	Строка символов, определяющая имя домена NIS
`dhcp-client-identifier string`	Используется в операторе `host` для определения идентификатора клиента DHCP. `dhcpd` может использовать данное значение для идентификации клиента вместо аппаратного адреса

Запуск службы `dhcpd` можно осуществить с помощью команды:

```
service dhcpd start
```

или включить одним из известных способов в список служб, запускаемых при старте системы.

Описание службы `dhcpd` и файла `dhcp.conf` приведено на страницах руководства `man`.

5.4. Служба NFS

Служба сетевого доступа к ФС NFS позволяет использовать ФС удаленных серверов и компьютеров. Доступ к ФС удаленных компьютеров обеспечивается с помощью нескольких программ на сторонах сервера и клиента.

На стороне сервера существуют следующие программы, используемые для обеспечения службы NFS:

– `rpc.idmapd` — перенаправляет обращения, сделанные с других компьютеров к службам NFS;

– `rpc.nfsd` — переводит запросы к службе NFS в действительные запросы к локальной ФС;

– `rpc.svcgssd` — поддерживает создание защищенного соединения;

– `rpc.statd` — поддерживает восстановление соединения при перезагрузке сервера;

– `rpc.mountd` — запрашивается для монтирования и размонтирования ФС.

Описание программ приведено на страницах руководства `man`.

На стороне сервера выполняется экспортирование ФС. Это означает, что определенные поддеревья, задаваемые каталогами, объявляются доступными для клиентских компьютеров. Информация об экспортированных ФС заносится в файл `/etc/exports`, в котором указывается, какие каталоги доступны для указанных клиентских компьютеров и какими правами доступа обладают клиентские компьютеры при выполнении операций на сервере. Запросы монтирования поступают от клиентских компьютеров к серверу монтиро-

вания mountd, который проверяет правильность клиентского запроса на монтирование и разрешает серверу службы NFS (nfsd) обслуживать запросы клиента, выполнившего монтирование. Клиенту разрешается выполнять различные операции с экспортированной ФС в пределах своих полномочий. Для получения хорошего качества обслуживания клиентов рекомендуется на сервере службы NFS одновременно запускать несколько копий процесса nfsd.

На стороне клиента для поддержки службы NFS4 используется модифицированная команда mount (если указывается ФС NFS4, то автоматически вызывается команда mount.nfs4). Дополнительно команда модифицирована таким образом, чтобы она могла понимать запись:

```
имя_компьютера: каталог
```

где имя_компьютера — имя сервера NFS, каталог — экспортированный каталог сервера службы NFS. Для удаленных ФС, которые являются частью постоянной конфигурации клиента, записи о монтируемых ФС службы NFS должны быть перечислены в файле /etc/fstab для автоматического монтирования во время начальной загрузки клиентского компьютера.

Кроме того, для поддержки защищенных соединений на клиентской стороне должна запускаться команда rpc.gssd.

При работе с сетевой ФС любые операции над файлами, производимые на локальном компьютере, передаются через сеть на удаленный компьютер.

5.5. Служба DNS

Система доменных имен DNS (Domain Name System) представляет собой иерархическую распределенную систему для получения информации о компьютерах, сервисах и ресурсах, входящих в глобальную или приватную компьютерную сеть. Чаще всего используется для получения IP-адреса по имени компьютера или устройства, получения информации о маршрутизации почты и т.п.

Основой DNS является представление об иерархической структуре доменного имени и зонах. Распределенная база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определенному протоколу. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу, что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

Основными важными понятиями DNS являются:

– Домен (область) — именованная ветвь или поддерево в дереве имен. Структура доменного имени отражает порядок следования узлов в иерархии; доменное имя читается справа налево от младших доменов к доменам высшего уровня (в порядке

повышения значимости).

– Полное доменное имя (FQDN) — полностью определенное доменное имя. Включает в себя имена всех родительских доменов иерархии DNS.

– Зона — часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на некотором сервере доменных имен.

– DNS-запрос — запрос от клиента (или сервера) серверу для получения информации.

Служба доменных имен `named` предназначена для генерации ответов на DNS-запросы. Существуют два типа DNS-запросов:

– прямой — запрос на преобразование имени компьютера в IP-адрес;

– обратный — запрос на преобразование IP-адреса в имя компьютера.

5.5.1. Настройка сервера службы доменных имен `named`

Конфигурационные параметры службы `named` хранятся в файлах каталога `/etc/bind/`, в первую очередь, в файле `/etc/bind/named.conf` (см. таблицу 17).

Таблица 17 – Конфигурационные файлы службы доменных имен `named`

Файл	Описание
`/etc/bind/named.conf`	Основной конфигурационный файл. Содержит значения конфигурационных параметров для всего сервера и включения других конфигурационных файлов.
`named.conf.default-zones`	Конфигурационный файл зон по умолчанию. В большинстве случаев не требует правки.
`named.conf.options`	Конфигурационный файл основных параметров сервера, важным из которых является параметр `directory`, содержащий каталог конфигурационных файлов зон. Значение по умолчанию `/var/cache/bind`.
`/etc/bind/named.conf.local`	Конфигурационный файл описания локальных зон сервера. Для каждой зоны указываются пути к конфигурационным файлам для прямого и обратного разыменования (как правило в указанном ранее каталоге `/var/cache/bind`).

Настройка сервера доменных имен является сложной задачей. Перед использованием DNS следует ознакомиться с существующей документацией, файлами помощи и страницами руководства `man` сервиса `named`, конфигурационного файла `named.conf` и сопутствующих утилит.

Далее приведен типовой пример настройки службы доменных имен `named`, обслуживающей одну доменную зону. Пример достаточен для демонстрации функционирующего домена ЕПП ОС «Astra Linux Special Edition».

Допустим, необходимо настроить сервер DNS домена `my.dom` подсети `192.168.1`. В конфигурационный файл `/etc/bind/named.conf.local` необходимо добавить следу-

ющие строки:

```
zone "my.dom" {
        type master;
        file "/var/cache/bind/db.my.dom";
};

zone "1.168.192.in-addr.arpa" {
        type master;
        file "/var/cache/bind/db.192.168.1";
};
```

Примечание. Имена конфигурационных файлов следует выбирать так, чтобы было понятно для какой конфигурации они используются. В приведенном примере имя конфигурационного файла для зоны обратного просмотра может быть, например: `/var/cache/bind/1.168.192.in-addr.arpa.zone` или `/var/cache/bind/db.my.dom.inv`.

Конфигурационный файл `/var/cache/bind/db.my.dom` содержит информацию зоны прямого просмотра.

```
;
; BIND data file for my.dom zone
;
$TTL    604800
@       IN      SOA     my.dom. root.my.dom. (
                         2014031301     ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      server.my.dom.
@       IN      A       192.168.1.100
@       IN      MX      1       server.my.dom.

server          IN      A       192.168.1.100
client1         IN      A       192.168.1.101
client2         IN      A       192.168.1.102
client3         IN      A       192.168.1.103

ns      IN      CNAME   server
```

```
;gw CNAMEs
ftp     IN      CNAME   server
repo    IN      CNAME   server
ntp     IN      CNAME   server

_https._tcp  IN SRV     10 10 443 server.my.com.

client1      IN TXT    "MAKS"
```

Конфигурационный файл `/var/cache/bind/db.my.dom` содержит информацию зоны обратного просмотра.

```
;
; BIND reverse data file for my.dom zone
;
$TTL    86400
@       IN      SOA my.dom. root.my.dom. (
                         2014031301     ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
@       IN      NS      server.my.dom.

100     IN      PTR     server.my.dom.
101     IN      PTR     client1.my.dom.
102     IN      PTR     client2.my.dom.
103     IN      PTR     client3.my.dom.
```

Описание зон может содержать следующие основные типы записей:

– `NS` — имя DNS сервера;

– `A` — связь имени с IP адресом;

– `CNAME` — связь псевдонима с другим именем (возможно псевдонимом);

– `PTR` — обратная связь IP адреса с именем;

– `SRV` — запись о сетевом сервисе;

– `TXT` — текстовая запись.

ВНИМАНИЕ! Перевод строки в конце конфигурационных файлов зон обязателен. В большинстве применений необходимо указание точки в конце имен компьютеров для предотвращения вывода корневого суффикса имени вида «`1.168.192.in-addr.arpa`».

Могут оказаться полезными следующие DNS утилиты (из состава пакетов `bind9utils` и `dnsutils`):

– `named-checkconf` — проверка синтаксиса, но не семантики конфигурации службы доменных имен `named`;

– `nslookup` — интерактивная терминал запросов к службе доменных имен;

– `rndc` — утилита управления службы доменных имен `named`.

Примечание. Обновление конфигурации сервера может выполняться без перезапуска самой службы доменных имен `named` вызовом: `rndc reload`.

5.5.2. Настройка клиентов для работы со службой доменных имен

Для работы со службой доменных имен на компьютерах необходимо наличие конфигурационного файла `/etc/resolv.conf`, содержащего информацию о доменах и именах серверов DNS, например:

```
domain my.dom
search my.dom
nameserver 192.168.1.100
```

Также может быть рассмотрена установка системы поддержки работы со службой доменных имен, содержащейся в пакете `resolvconf`.

ВНИМАНИЕ! Для взаимодействия DNS-сервера с клиентами, функционирующими в разных мандатных контекстах требуется дополнительная настройка механизма `privsock`. Описание настройки сетевых сервисов для работы с использованием механизма `privsock` приведено в документе РУСБ.10015-01 97 01-1.

5.6. Фильтр сетевых пакетов

При помощи фильтра сетевых пакетов можно осуществлять контроль сетевого трафика, проходящего через данный компьютер.

Фильтрацию пакетов выполняет фильтр пакетов `iptables`. Данный фильтр позволяет выполнять следующие задачи:

1) фильтрацию пакетов — это механизм, который, основываясь на некоторых правилах, разрешает или запрещает передачу информации, проходящей через него, с целью ограждения некоторой подсети от внешнего доступа, или, наоборот, для недопущения выхода наружу. Фильтр пакетов может определять правомерность передачи информации на основе только заголовков IP-пакетов, а может анализировать и их содержимое, т. е. использовать данные протоколов более высокого уровня;

2) трансляцию сетевых адресов (т. н. «маскарадинг») — это подмена некоторых параметров в заголовках IP-пакетов. Используется для сокрытия реальных IP-адресов

компьютеров защищаемой ЛВС, а также для организации доступа из ЛВС с компьютерами, не имеющими реальных IP-адресов, к глобальной сети;

3) прозрачное проксирование — это переадресация пакетов на другой порт компьютера. Обычно используется для того, чтобы заставить пользователей из ЛВС пользоваться proxy-сервером маршрутизатора без дополнительного конфигурирования их клиентских программ.

Настройка рассмотренных механизмов (фильтрация пакетов, трансляция сетевых адресов и прозрачное проксирование) выполняется командой `iptables`.

5.6.1. Формирование правил

Каждое правило — это строка, содержащая в себе критерии, определяющие, подпадает ли пакет под заданное правило, и действие, которое необходимо выполнить в случае выполнения критерия.

Правила записываются следующим образом:

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

Если в правило не включается спецификатор `[-t table]`, то по умолчанию предполагается использование таблицы `filter`, если же предполагается использование другой таблицы, то это требуется указать явно. Спецификатор таблицы также можно указывать в любом месте строки правила, однако более или менее стандартным считается указание таблицы в начале правила.

Далее, непосредственно за именем таблицы, должна стоять команда. Если спецификатора таблицы нет, то команда всегда должна стоять первой. Команда определяет действие `iptables`, например вставить, добавить в конец цепочки или удалить правило и т. п.

Раздел `matches` задает критерии проверки, по которым определяется, подпадает ли пакет под действие этого правила или нет. Здесь можно указать самые разные критерии — и IP-адрес источника пакета или сети, и сетевой интерфейс, и т. д.

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

5.6.1.1. Порядок прохождения таблиц и цепочек

Когда пакет приходит на сетевой фильтр, то он сначала попадает на сетевое устройство, перехватывается соответствующим драйвером и далее передается в ядро. Затем пакет проходит несколько таблиц и после передается либо локальному приложению, либо переправляется на другой компьютер. Порядок следования пакета приводится в таблице 18.

Таблица 18

Шаг	Таблица	Цепочка	Описание
1	=	=	Кабель
2	=	=	Сетевой интерфейс (например, eth0)
3	mangle	PREROUTING	Используется для внесения изменений в заголовок пакета, например для изменения битов TOS и пр.
4	nat	PREROUTING	Используется для трансляции сетевых адресов DNAT. SNAT выполняется позднее, в другой цепочке. Любого рода фильтрация в этой цепочке может производиться только в исключительных случаях
5	=	=	Принятие решения о дальнейшей маршрутизации, т. е. в этой точке решается, куда пойдет пакет — локальному приложению или на другой узел сети
6	filter	FORWARD	Попадают только те пакеты, которые идут на другой компьютер. Вся фильтрация транзитного трафика должна выполняться здесь. Через эту цепочку проходит трафик в обоих направлениях, поэтому обязательно учитывать это обстоятельство при написании правил фильтрации
7	nat	POSTROUTING	Предназначена в первую очередь для SNAT. Не использовать для фильтрации без особой необходимости. Здесь же выполняется и маскарадинг
8	=	=	Выходной сетевой интерфейс (например, eth1)
9	=	=	Кабель

Пакет проходит несколько этапов, прежде чем он будет передан далее. На каждом из них пакет может быть остановлен. Цепочку FORWARD проходят все пакеты, которые движутся через сетевой фильтр. В таблице 19 представлен порядок движения пакета, предназначенного локальному процессу/приложению.

Таблица 19

Шаг	Таблица	Цепочка	Описание
1	=	=	Кабель
2	=	=	Входной сетевой интерфейс (например, eth0)
3	mangle	PREROUTING	Обычно используется для внесения изменений в заголовок пакета, например для установки битов TOS и пр.
4	nat	PREROUTING	Преобразование адресов DNAT. Фильтрация пакетов здесь допускается только в исключительных случаях
5	=	=	Принятие решения о маршрутизации
6	filter	INPUT	Фильтрация входящего трафика. Все входящие пакеты, адресованные локальному приложению, проходят через эту цепочку, независимо от того, с какого интерфейса они поступили
7	=	=	Локальный процесс/приложение

Важно помнить, что пакеты идут через цепочку INPUT, а не через FORWARD. В таблице 20 представлен порядок движения пакетов, созданных локальными процессами.

Таблица 20

Шаг	Таблица	Цепочка	Описание
1	=	=	Локальный процесс
2	mangle	OUTPUT	Внесение изменений в заголовок пакета. Фильтрация, выполняемая в этой цепочке, может иметь негативные последствия
3	filter		
4	=	=	Принятие решения о маршрутизации. Здесь решается — куда пойдет пакет дальше
5	nat	POSTROUTING	Здесь выполняется SNAT. Не следует в этой цепочке производить фильтрацию пакетов во избежание нежелательных побочных эффектов. Однако и здесь можно останавливать пакеты, применяя политику по умолчанию — DROP
6	=	=	Сетевой интерфейс (например, eth0)
7	=	=	Кабель

mangle

В этой таблице не следует производить любого рода фильтрацию, маскировку или преобразование адресов (DNAT, SNAT), в ней допускается выполнять действия, приведенные в таблице 21.

Таблица 21

Действие	Описание
TOS	Выполняет установку битов поля TOS. Это поле используется для назначения сетевой политики обслуживания пакета, т. е. задает желаемый вариант маршрутизации
TTL	Используется для установки значения поля TTL пакета
MARK	Устанавливает специальную метку на пакет, которая затем может быть проверена другими правилами в iptables или другими программами, например iproute2. С помощью меток можно управлять маршрутизацией пакетов, ограничивать трафик и т. п.

Таблица имеет две цепочки:

– PREROUTING — используется для внесения изменений на входе в сетевой фильтр перед принятием решения о маршрутизации;

– OUTPUT — для внесения изменений в пакеты, поступающие от приложений внутри сетевой фильтр.

nat

Только первый пакет из потока проходит через цепочки этой таблицы. Трансляция адресов или маскировка применяются ко всем последующим пакетам в потоке автомати-

чески. Для этой таблицы характерны действия, приведенные в таблице 22.

Таблица 22

Действие	Описание
DNAT	Производит преобразование адресов назначения в заголовках пакетов. Другими словами, этим действием перенаправляются пакеты на другие адреса, отличные от указанных в заголовках пакетов
SNAT	Используется для изменения исходных адресов пакетов. С помощью этого действия можно скрыть структуру локальной сети
MASQUERADE	Применяется в тех же целях, что и SNAT, но в отличие от последней дает более сильную нагрузку на систему. Происходит это потому, что каждый раз, когда требуется выполнение этого действия, производится запрос IP-адреса для указанного в действии сетевого интерфейса, в то время как для SNAT IP-адрес указывается непосредственно. Однако благодаря такому отличию, MASQUERADE может работать в случаях с динамическим IP-адресом

Таблица имеет две цепочки:

– PREROUTING — используется для внесения изменений в пакеты на входе в сетевой фильтр;

– OUTPUT — используется для преобразования пакетов, созданных приложениями внутри сетевого фильтра, перед принятием решения о маршрутизации.

filter

В этой таблице содержатся наборы правил для выполнения фильтрации пакетов. Пакеты могут пропускаться далее либо отвергаться в зависимости от их содержимого.

В таблице filter можно выполнить DROP, LOG, ACCEPT или REJECT без каких-либо сложностей, как в других таблицах. Имеется три встроенных цепочки:

– FORWARD — используется для фильтрации пакетов, идущих транзитом через сетевой фильтр;

– INPUT — проходят пакеты, которые предназначены локальным приложениям (сетевому фильтру);

– OUTPUT — используется для фильтрации исходящих пакетов, сгенерированных приложениями на самом сетевом фильтре.

5.6.1.2. Механизм трассировки соединений

Механизм трассировки соединений является частью сетевого фильтра iptables и устроен так, чтобы netfilter мог получить информацию о состоянии конкретного соединения. Наличие этого механизма позволяет создавать более надежные наборы правил.

В пределах iptables соединение может иметь одно из четырех базовых состояний: NEW, ESTABLISHED, RELATED и INVALID. Для управления пакетами на основе их состояния используется критерий --state. Трассировщик определяет четыре основных

состояния каждого TCP- или UDP-пакета и некоторые дополнительные характеристики. Для TCP- и UDP-пакетов — это IP-адреса отправителя и получателя, порты отправителя и получателя.

Трассировка производится в цепочке PREROUTING. Это означает, что iptables производит все вычисления, связанные с определением состояния, в пределах этой цепочки. Когда отправляется инициирующий пакет в потоке, то ему присваивается состояние NEW, а когда возвращается пакет ответа, то состояние соединения изменяется на ESTABLISHED и т. д.

Таблица трассировки

Таблицу трассировщика можно найти в файле /proc/net/ip_conntrack. Здесь содержится список всех активных соединений. Если модуль ip_conntrack загружен, то команда cat /proc/net/ip_conntrack должна вывести:

```
tcp 6 117 SYN_SENT src=192.168.1.6 dst=192.168.1.9 sport=32775 dport=22
  [UNREPLIED] src=192.168.1.9 dst=192.168.1.6 sport=22 dport=32775 use=2
```

В этом примере содержится вся информация, которая известна трассировщику по конкретному соединению. Первое, что можно увидеть — это название протокола, в данном случае — tcp. Далее следует некоторое число в обычном десятичном представлении. После него следует число, определяющее «время жизни» (т. е. количество секунд, через которое информация о соединении будет удалена из таблицы) записи в таблице. В приведенном примере запись в таблице будет храниться еще 117 с, если через это соединение более не проследует ни одного пакета, в противном случае это значение будет установлено в значение по умолчанию для заданного состояния. Это число уменьшается на 1 каждую секунду.

Далее следует фактическое состояние соединения. В примере это состояние имеет значение SYN_SENT. Внутреннее представление состояния несколько отличается от внешнего. Значение SYN_SENT говорит о том, что через данное соединение проследовал единственный пакет TCP SYN. Далее расположены адреса отправителя и получателя, порты отправителя и получателя. Здесь же видно ключевое слово, которое сообщает о том, что ответного трафика через это соединение еще не было.

Приводится дополнительная информация по ожидаемому пакету, это IP-адреса отправителя/получателя (те же самые, только поменявшиеся местами, т. к. ожидается ответный пакет), то же касается и портов.

После получения пакетом ответа трассировщик снимет флаг [unreplied] и заменит его флагом [assured]. Этот флаг сообщает, что соединение установлено уверенно, и эта запись не будет стерта по достижении максимально возможного количества трассируемых соединений. Максимальное количество записей, которое может содержаться в

таблице, зависит от значения по умолчанию, которое может быть установлено вызовом функции `ipsysctl`.

Для объема ОЗУ 256 МБ значение соответствует 16376 записям. Можно посмотреть и изменить это значение через:

`/proc/sys/net/ipv4/ip_conntrack_max`

Состояния

Сетевые пакеты могут иметь несколько различных состояний в пределах ядра в зависимости от типа протокола. Однако вне ядра имеется только четыре состояния, как было сказано выше. Параметры, описывающие состояние пакета, используются в критерии `--state`. Допустимыми являются: `NEW`, `ESTABLISHED`, `RELATED` и `INVALID`.

В таблице 23 подробно рассмотрены каждое из возможных состояний и приведены необходимые комментарии.

Таблица 23

Состояние	Описание
`NEW`	Сообщает о том, что пакет является первым для данного соединения. Это означает, что это первый пакет в данном соединении, который увидел модуль трассировщика
`ESTABLISHED`	Говорит о том, что это не первый пакет в соединении. Для перехода в состояние `ESTABLISHED` необходимо, чтобы один компьютер передал пакет и получил на него ответ от другого компьютера. После получения ответа признак соединения `NEW` будет заменен на `ESTABLISHED`
`RELATED`	Появляется, если данное соединение связано с другим соединением, имеющим признак `ESTABLISHED`, т. е. соединение инициировано из уже установленного соединения, имеющего признак `ESTABLISHED`
`INVALID`	Говорит о том, что пакет не может быть идентифицирован и поэтому не может иметь определенного статуса. Это может происходить по разным причинам, например, при нехватке памяти или при получении ICMP-сообщения, которое не соответствует какому-либо известному соединению. Наилучшим вариантом было бы применение действия `DROP` к таким пакетам

Таблицы

Опция `-t` указывает на используемую таблицу. По умолчанию используется таблица `filter`.

Команды

В таблице 24 приводится список команд, которые используются в `iptables`, и правила их использования. Посредством команд `iptables` узнает, что необходимо выполнить. Обычно предполагается одно из двух действий — это добавление нового правила в цепочку или удаление существующего правила из той или иной таблицы.

Таблица 24

Команда	Использование
-A, --append	Добавляет новое правило в конец заданной цепочки. Пример iptables -A INPUT ...
-D, --delete	Удаляет правило из цепочки. Команда имеет два формата записи, первый — когда задается критерий сравнения с опцией -D, второй — порядковый номер правила. Если задается критерий сравнения, то удаляется правило, которое имеет в себе этот критерий, если задается номер правила, то будет удалено правило с заданным номером. Счет правил в цепочках начинается с единицы. Пример iptables -D INPUT --dport 80 -j DROP, iptables -D INPUT 1
-E, --rename-chain	Выполняет переименование пользовательской цепочки. В примере цепочка allowed будет переименована в цепочку disallowed. Эти переименования не изменяют порядок работы. Пример iptables -E allowed disallowed Команда должна быть указана всегда
-F, --flush	Сброс (удаление) всех правил из заданной цепочки (таблицы). Если имя цепочки и таблицы не указывается, то удаляются все правила во всех цепочках. Пример iptables -F INPUT
-I, --insert	Вставляет новое правило в цепочку. Число, следующее за именем цепочки, указывает номер правила, перед которым следует вставить новое правило. В примере выше указывается, что данное правило должно быть первым в цепочке INPUT. Пример iptables -I INPUT 1 --dport 80 -j ACCEPT
-L, --list	Вывод списка правил в заданной цепочке. В нижеприведенном примере предполагается вывод правил из цепочки INPUT. Если имя цепочки не указывается, то выводится список правил для всех цепочек. Формат вывода зависит от наличия дополнительных ключей в команде, например -n, -v и пр. Пример iptables -L INPUT
-N, --new-chain	Создается новая цепочка с заданным именем в заданной таблице. В нижеприведенном примере создается новая цепочка с именем allowed. Имя цепочки должно быть уникальным и не должно совпадать с зарезервированными именами цепочек и действий (DROP, REJECT и т. п.). Пример iptables -N allowed

Окончание таблицы 24

Команда	Использование
`-P, --policy`	Определяет политику по умолчанию для заданной цепочки. Политика по умолчанию определяет действие, применяемое к пакетам, не попавшим под действие ни одного из правил в цепочке. В качестве политики по умолчанию допускается использовать `DROP`, `ACCEPT` и `REJECT`. Пример `iptables -P INPUT DROP`
`-R, --replace`	Данная команда заменяет одно правило другим. В основном она используется во время отладки новых правил. Пример `iptables -R INPUT 1 -s 192.168.0.1 -j`
`-X, --delete-chain`	Удаление заданной цепочки из заданной таблицы. Удаляемая цепочка не должна иметь правил и не должно быть ссылок из других цепочек на удаляемую цепочку. Если имя цепочки не указано, то будут удалены все цепочки, определенные командой `-N` в заданной таблице. Примеры: 1. `iptables -X allowed` 2. `iptables -P INPUT DROP`
`-Z, --zero`	Обнуление всех счетчиков в заданной цепочке. Если имя цепочки не указывается, то подразумеваются все цепочки. При использовании ключа `-v` совместно с командой `-L` на вывод будут поданы и состояния счетчиков пакетов, попавших под действие каждого правила. Допускается совместное использование команд `-L` и `-Z`. В этом случае будет выдан сначала список правил со счетчиками, а затем произойдет обнуление счетчиков

Ключи

Некоторые команды могут использоваться совместно с дополнительными ключами (таблица 25).

Таблица 25

Ключ	Описание
`c, --set-counters`	Используется вместе с командами `--insert`, `--append` и `--replace` при создании нового правила для установки счетчиков пакетов и байт в заданное значение. Например, ключ `--set-counters 20 4000` установит счетчик пакетов = 20, а счетчик байт = 4000
`--line-numbers`	Используется вместе с командой `--list`, включает режим вывода номеров строк при отображении списка правил командой `--list`. Номер строки соответствует позиции правила в цепочке
`--modprobe`	Может использоваться с любой командой, определяет команду загрузки модуля ядра. Данный ключ используется в случае, если команда `modprobe` находится вне пути поиска

Окончание таблицы 25

Ключ	Описание
`n, --numeric`	Используется вместе с командой `--list`. Заставляет `iptables` выводить IP-адреса и номера портов в числовом виде, предотвращая попытки преобразовать их в символические имена
`-v, --verbose`	Используется вместе с командами `--list`, `--append`, `--insert`, `--delete` и `--replace` для повышения информативности вывода. В случае использования с командой `--list` в вывод этой команды включаются так же имя интерфейса, счетчики пакетов и байт для каждого правила. Формат вывода счетчиков предполагает вывод, кроме цифр числа, еще и символьные множители `K` (x1000), `M` (x1,000,000) и `G` (x1,000,000,000). Для того чтобы заставить команду `--list` выводить полное число (без употребления множителей), требуется применять ключ `-x`, который описан ниже. При использовании с другими командами на вывод будет выдан подробный отчет о произведенной операции
`-x, --exact`	Используется вместе с командой `--list`. Для всех чисел в выходных данных выводятся их точные значения без округления и без применения множителей `K`, `M`, `G`. Важно то, что данный ключ используется только с командой `--list` и не применяется с другими командами

5.6.1.3. Критерии выделения пакетов

Выделяются следующие критерии:

1) общие — критерии, которые допустимо употреблять в любых правилах. Они не зависят от типа протокола и не требуют подгрузки модулей расширения. В эту группу добавлен критерий `--protocol`, несмотря на то, что он используется в некоторых специфичных от протокола расширениях. Например, при использовании TCP-критерия необходимо использовать и критерий `--protocol`, которому в качестве дополнительного ключа передается название протокола — TCP. Однако `--protocol` сам по себе является критерием, который используется для указания типа протокола;

2) неявные — это критерии, которые подгружаются неявно и становятся доступны, например, при указании критерия `--protocol`. Существует три автоматически подгружаемых расширения: TCP-, UDP- и ICMP-критерии. Загрузка этих расширений может производиться и явным образом с помощью ключа `-m`, `--match`, например: `-m tcp`

3) перед использованием вышеописанных расширений они должны быть загружены явно, с помощью ключа `-m` или `--match`. Так, например, если использовать критерии `--state`, то следует явно указать это в строке правила: `-m state` левее используемого критерия. Все отличие между явными и неявными критериями заключается только в том, что первые необходимо подгружать явно, а вторые подгружаются автоматически.

5.6.1.4. Действия и переходы

Действия и переходы сообщают правилу, что необходимо выполнить, если пакет соответствует заданному критерию. Чаще всего употребляются действия ACCEPT и DROP.

Описание переходов в правилах выглядит точно так же, как и описание действий, т. е. ставится ключ -j и указывается название цепочки правил, на которую выполняется переход. На переходы накладывается ряд ограничений, первое — цепочка, на которую выполняется переход, должна находиться в той же таблице, что и цепочка, из которой этот переход выполняется; второе — цепочка, являющаяся целью перехода, должна быть создана до того, как на нее будут выполняться переходы.

Например, создать цепочку tcp_packets в таблице filter с помощью команды:

```
iptables -N tcp_packets
```

Теперь можно выполнять переходы на эту цепочку подобно:

```
iptables -A INPUT -p tcp -j tcp_packets
```

т. е., встретив пакет протокола TCP, iptables произведет переход на цепочку tcp_packets и продолжит движение пакета по этой цепочке. Если пакет достиг конца цепочки, то он будет возвращен в вызывающую цепочку (в примере — это цепочка INPUT) и движение пакета продолжится с правила, следующего за правилом, вызвавшем переход. Если к пакету во вложенной цепочке будет применено действие ACCEPT, то автоматически пакет будет считаться принятым и в вызывающей цепочке и уже не будет продолжать движение по вызывающим цепочкам. Однако пакет пойдет по другим цепочкам в других таблицах.

Действие — это предопределенная команда, описывающая действие, которое необходимо выполнить, если пакет совпал с заданным критерием. Например, можно применить действие DROP или ACCEPT к пакету. В результате выполнения одних действий пакет прекращает свое прохождение по цепочке, например DROP и ACCEPT; в результате других, после выполнения неких операций, продолжает проверку, например LOG; в результате работы третьих — даже видоизменяется, например DNAT и SNAT, TTL и TOS, но так же продолжает продвижение по цепочке.

ACCEPT

Если над пакетом выполняется действие ACCEPT, то пакет прекращает движение по цепочке (и всем вызвавшим цепочкам, если текущая цепочка была вложенной) и считается принятым, тем не менее, пакет продолжит движение по цепочкам в других таблицах и может быть отвергнут там. Действие задается с помощью ключа -j ACCEPT. Дополнительных ключей не имеет.

DNAT

DNAT используется для преобразования адреса места назначения в IP-заголовке пакета. Если пакет подпадает под критерий правила, выполняющего DNAT, то этот пакет и все последующие пакеты из этого же потока будут подвергнуты преобразованию адреса назначения и переданы на требуемое устройство, компьютер или сеть.

Может выполняться только в цепочках PREROUTING и OUTPUT таблицы nat и во вложенных подцепочках.

Ключ для действия DNAT — --to-destination.

Пример

```
iptables -t nat -A PREROUTING -p tcp -d 15.45.23.67
--dport 80 -j DNAT --to-destination 192.168.1.1-192.168.1.10
```

Этот ключ указывает, какой IP-адрес должен быть подставлен в качестве адреса места назначения. В вышеприведенном примере во всех пакетах, пришедших на адрес .45.23.67, адрес назначения будет изменен на один из диапазона от 192.168.1.1 до 192.168.1.10. Все пакеты из одного потока будут направляться на один и тот же адрес, а для каждого нового потока будет выбираться один из адресов в указанном диапазоне случайным образом. Можно также определить единственный IP-адрес. Можно дополнительно указать порт или диапазон портов, на который (которые) будет перенаправлен трафик. Для этого после IP-адреса через двоеточие указать порт, например:

```
--to-destination 192.168.1.1:80
```

а указание диапазона портов выглядит так:

```
--to-destination 192.168.1.1:80-100
```

Синтаксис действий DNAT и SNAT во многом схож. Указание портов допускается только при работе с протоколом TCP или UDP, при наличии опции --protocol в критерии.

DROP

DROP сбрасывает пакет и iptables забывает о его существовании. Сброшенные пакеты прекращают свое движение полностью, т. е. они не передаются в другие таблицы, как это происходит в случае с действием ACCEPT. Следует помнить, что данное действие может иметь негативные последствия, поскольку может оставлять незакрытые сокеты как на стороне сервера, так и на стороне клиента, наилучшим способом защиты будет использование действия REJECT особенно при защите от сканирования портов.

LOG

LOG служит для журналирования отдельных пакетов и событий. В журнал могут заноситься заголовки IP-пакетов и другая интересующая информация. Информация из журнала может быть прочитана с помощью dmesg или syslogd, либо с помощью других команд.

Ключи действия LOG приведены в таблице 26.

Таблица 26

Ключ	Описание
--log-level	Используется для задания уровня журналирования. Можно задать следующие уровни: debug, info, notice, warning, warn, err, error, crit, alert, emerg и panic. Ключевое слово error означает то же самое, что и err, warn — warning и panic — emerg. Приоритет определяет различия в том, как будут заноситься сообщения в журнал. Все сообщения заносятся в журнал средствами ядра. Если установить строку kern.=info /var/log/iptables в файле syslog.conf, то все сообщения из iptables, использующие уровень info, будут заноситься в файл /var/log/iptables. Однако в этот файл попадут и другие сообщения, поступающие из других подсистем, которые используют уровень info. Пример iptables -A FORWARD -p tcp -j LOG --log-level debug
--log-prefix	Задает префикс, который будет стоять перед всеми сообщениями iptables. Сообщения со специфичным префиксом затем легко можно найти, к примеру, с помощью grep. Префикс может содержать до 29 символов, включая пробелы. Пример iptables -A INPUT -p tcp -j LOG --log-prefix "INPUT packets"
--log-tcp-sequence	Позволяет заносить в журнал номер TCP Sequence-пакета. Номер TCP Sequence идентифицирует каждый пакет в потоке и определяет порядок сборки потока. Этот ключ потенциально опасен для безопасности системы, если системный журнал разрешает доступ «на чтение» всем пользователям. Как и любой другой журнал, содержащий сообщения от iptables. Пример iptables -A INPUT -p tcp -j LOG --log-tcp-sequence
--log-tcp-options	Позволяет заносить в системный журнал различные сведения из заголовка TCP-пакета. Такая возможность может быть полезна при отладке. Этот ключ не имеет дополнительных параметров. Пример iptables -A FORWARD -p tcp -j LOG --log-tcp-options
--log-ip-options	Позволяет заносить в системный журнал различные сведения из заголовка IP-пакета. Во многом схож с ключом --log-tcp-options, но работает только с IP-заголовком. Пример iptables -A FORWARD -p tcp -j LOG --log-ip-options

MARK

MARK используется для установки меток для определенных пакетов. Это действие может выполняться только в пределах таблицы mangle. Установка меток обычно исполь-

зуется для нужд маршрутизации пакетов по различным маршрутам, для ограничения трафика и т. п. Метка пакета существует только в период времени, пока пакет не покинул брандмауэр, т. е. метка не передается по сети. Если необходимо как-то пометить пакеты, чтобы использовать маркировку на другом компьютере, то можно манипулировать битами поля TOS.

Ключ для действия MARK — --set- — устанавливает метку на пакет. После ключа --set-mark должно следовать целое число.

Пример

```
iptables -t mangle -A PREROUTING -p tcp --dport 22 -j MARK --set-mark 2
```

MASQUERADE

Маскарадинг подразумевает получение IP-адреса от заданного сетевого интерфейса, вместо прямого его указания, как это делается с помощью ключа --to-source в действии SNAT.

Действие MASQUERADE может быть использовано вместо SNAT, даже если имеется постоянный IP-адрес.

MASQUERADE допускается указывать только в цепочке POSTROUTING таблицы nat, так же как и действие SNAT. MASQUERADE имеет ключ, использование которого необязательно.

Ключ для действия MASQUERADE — --to-ports — используется для указания порта источника или диапазона портов исходящего пакета. Можно указать один порт, например:

```
--to-ports 1025
```

или диапазон портов:

```
--to-ports 1024-3100
```

Этот ключ можно использовать только в правилах, где критерий содержит явное указание на протокол TCP или UDP с помощью ключа --protocol.

Пример

```
iptables -t nat -A POSTROUTING -p TCP -j MASQUERADE --to-ports 1024-31000
```

REDIRECT

REDIRECT выполняет перенаправление пакетов и потоков на другой порт того же самого компьютера. К примеру, можно пакеты, поступающие на HTTP-порт перенаправить на порт HTTP-прокси. Действие REDIRECT очень удобно для выполнения прозрачного проксирования (transparent proxying), когда компьютеры в ЛВС даже не подозревают о существовании прокси.

REDIRECT может использоваться только в цепочках PREROUTING и OUTPUT таблицы nat, а также выполняться в подцепочках.

Ключ для действия REDIRECT — --to-ports — определяет порт или диапазон портов назначения. Без указания ключа --to-ports перенаправления не происходит, т. е. пакет идет на тот порт, куда и был назначен. В примере, приведенном ниже, --to-ports 8080 указан один порт назначения.

Пример

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-ports 8080
```

Если необходимо указать диапазон портов, то написать:

```
--to-ports 8080-8090
```

Этот ключ можно использовать только в правилах, где критерий содержит явное указание на протокол TCP или UDP с помощью ключа --protocol.

REJECT

REJECT используется, как правило, в тех же самых ситуациях, что и DROP, но в отличие от DROP, команда REJECT выдает сообщение об ошибке на компьютер, передавший пакет. Действие REJECT работает только в цепочках INPUT, FORWARD и OUTPUT (и во вложенных в них цепочках). Пока существует только единственный ключ, управляющий поведением команды REJECT.

Ключ для действия REJECT — --reject-with — указывает, какое сообщение необходимо передать в ответ, если пакет совпал с заданным критерием. При применении действия REJECT к пакету, сначала на компьютер-отправитель будет отослан указанный ответ, а затем пакет будет сброшен. Допускается использовать следующие типы ответов: icmp-net-unreachable, icmp-host-unreachable, icmp-port-unreachable, icmp-proto-unreachable, icmp-net-prohibited и icmp-host-prohibited. По умолчанию передается сообщение port-unreachable. Все вышеуказанные типы ответов являются ICMP error messages (сообщениями об ошибках). Тип ответа tcp-reset используется только для протокола TCP. Если указано значение tcp-reset, то действие REJECT передаст в ответ пакет TCP RST, который используется для закрытия TCP-соединения.

Пример

```
iptables -A FORWARD -p TCP --dport 22 -j REJECT --reject-with tcp-reset
```

RETURN

RETURN прекращает движение пакета по текущей цепочке правил и производит возврат в вызывающую цепочку, если текущая цепочка была вложенной, или, если текущая цепочка лежит на самом верхнем уровне (например, INPUT), то к пакету будет применена политика по умолчанию. В качестве политики по умолчанию назначают действия ACCEPT или DROP.

SNAT

SNAT используется для преобразования сетевых адресов, т. е. изменение исходящего IP-адреса в IP-заголовке пакета. SNAT допускается выполнять только в таблице nat, в цепочке POSTROUTING. Другими словами, только здесь допускается преобразование исходящих адресов. Если первый пакет в соединении подвергся преобразованию исходящего адреса, то все последующие пакеты из этого же соединения будут преобразованы автоматически и не пойдут через эту цепочку правил.

Ключ для действия SNAT — --to-source — используется для указания адреса, присваиваемого пакету.

Пример

```
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source
194.236.50.155-194.236.50.160:1024-32000
```

Указывается IP-адрес, который будет подставлен в заголовок пакета в качестве исходящего. Если необходимо перераспределить нагрузку между несколькими брандмауэрами, то можно указать диапазон адресов, где начальный и конечный адреса диапазона разделяются дефисом, например:

```
194.236.50.155-194.236.50.160
```

Тогда конкретный IP-адрес будет выбираться из диапазона случайным образом для каждого нового потока. Дополнительно можно указать диапазон портов, которые будут использоваться только для нужд SNAT.

TOS

TOS используется для установки бит в поле TOS IP-заголовка. Поле TOS содержит восемь бит, которые используются для маршрутизации пакетов. Это одно из нескольких полей, используемых iproute2. Данное поле может обрабатываться различными маршрутизаторами с целью выбора маршрута движения пакета. Как уже указывалось выше, это поле, в отличие от MARK, сохраняет свое значение при движении по сети, а поэтому может использоваться для маршрутизации пакета. Данное действие допускается выполнять только в пределах таблицы mangle.

Ключ для действия TOS — --set-tos — определяет числовое значение в десятичном или шестнадцатеричном виде.

Пример

```
iptables -t mangle -A PREROUTING -p TCP --dport 22 -j TOS --set-tos 0x10
```

Поскольку поле TOS является 8-битным, то можно указать число в диапазоне от 0 до 255 (0x00–0xFF). Большинство значений этого поля никак не используется. Лучше использовать мнемонические обозначения: Minimize-Delay (16 или 0x10), Maximize-Throughput (8

или 0x08), Maximize-Reliability (4 или 0x04), Minimize-Cost (2 или 0x02) или Normal-Service (0 или 0x00). По умолчанию большинство пакетов имеют признак Normal-Service или нуль. Список мнемоник можно получить, выполнив команду:

```
iptables -j TOS -h
```

TTL

TTL используется для изменения содержимого поля TTL в IP-заголовке. Один из вариантов применения этого действия — устанавливать значение поля TTL во всех исходящих пакетах в одно и то же значение.

Действие TTL можно указывать только в таблице mangle и нигде больше.

Ключи для действия TTL приведены в таблице 27.

Таблица 27

Ключ	Описание
--ttl-set	Устанавливает поле TTL в заданное значение. Оптимальным считается значение около 64. Пример `iptables -t mangle -A PREROUTING -o eth0 -j TTL --ttl-set 64`
--ttl-dec	Уменьшает значение поля TTL на заданное число. Например, пусть входящий пакет имеет значение TTL, равное 53, выполняется команда --ttl-dec 3. Тогда пакет покинет компьютер с полем TTL, равным 49. Сетевой код автоматически уменьшит значение TTL на 1, поэтому фактически получается: 53 - 3 - 1 = 49. Пример `iptables -t mangle -A PREROUTING -o eth0 -j TTL --ttl-dec 1`
--ttl-inc	Увеличивает значение поля TTL на заданное число. Пусть поступает пакет с TTL, равным 53, тогда после выполнения команды --ttl-inc 4 на выходе с компьютера пакет будет иметь TTL, равный 56, не стоит забывать об автоматическом уменьшении поля TTL сетевым кодом ядра, т. е. фактически получается выражение: 53 + 4 - 1 = 56. Пример `iptables -t mangle -A PREROUTING -o eth0 -j TTL --ttl-inc 1`

ULOG

ULOG предоставляет возможность журналирования пакетов в пользовательское пространство. Оно заменяет традиционное действие LOG, базирующееся на системном журнале. При использовании этого действия пакет через сокеты netlink передается специальному демону, который может выполнять очень детальное журналирование в различных форматах (например, обычный текстовый файл) и к тому же поддерживает возможность добавления надстроек (плагинов) для формирования различных выходных форматов и обработки сетевых протоколов.

Ключи для действия ULOG приведены в таблице 28.

Таблица 28

Ключ	Описание
--ulog-nlgroup	Сообщает ULOG, в какую группу netlink должен быть передан пакет. Всего существует 32 группы (от 1 до 32). Если необходимо передать пакет в пятую группу, то можно просто указать: --ulog-nlgroup 5 По умолчанию используется первая группа. Пример iptables -A INPUT -p TCP --dport 22 -j ULOG --ulog-nlgroup 2
--ulog-prefix	Имеет тот же смысл, что и аналогичная опция в действии LOG. Длина строки префикса не должна превышать 32 символа. Пример iptables -A INPUT -p TCP --dport 22 -j ULOG --ulog-prefix "SSH connection attempt: "
--ulog-cprange	Определяет, какую долю пакета, в байтах, надо передавать демону ULOG. Если указать число 100, как показано в примере, то демону будет передано только 100 Б из пакета, это означает, что демону будет передан заголовок пакета и некоторая часть области данных пакета. Если указать нуль, то будет передан весь пакет, независимо от его размера. Значение по умолчанию равно нулю. Пример iptables -A INPUT -p TCP --dport 22 -j ULOG --ulog-cprange 100
--ulog-qthreshold	Устанавливает величину буфера в области ядра. Например, если задать величину буфера, равной 10, как в примере, то ядро будет накапливать журналируемые пакеты во внутреннем буфере и передавать в пользовательское пространство группами по 10 пакетов. Пример iptables -A INPUT -p TCP --dport 22 -j ULOG --ulog-qthreshold 10

5.7. Настройка SSH

SSH — это клиент-серверная система для организации защищенных туннелей между двумя и более компьютерами. В таких туннелях защищаются все передаваемые данные, в т. ч. пароли.

5.7.1. Служба sshd

Служба sshd запускается на этапе начальной загрузки из сценария /etc/rc.d/init.d/sshd. Этот сценарий, а также ссылки на него в виде сценариев запуска и останова службы создаются в процессе установки программы. По умолчанию служба прослушивает порт 22. Когда поступает запрос на подключение, он порождает дочерний процесс, который управляет передачей данных в рамках конкретного соединения.

Служба берет свои конфигурации сначала из командной строки, затем из файла /etc/ssh/sshd_config.

Синтаксис:

```
sshd [-deiqtD46] [-b bits] [-f config_file] [-g login_grace_time]
[-h host_key_file] [-k key_gen_time] [-o option] [-p port] [-u len]
```

Параметры, которые могут присутствовать в файле /etc/ssh/sshd_config, описаны в таблице 29. Пустые строки, а также строки, начинающиеся с #, игнорируются. Названия параметров не чувствительны к регистру символов.

Таблица 29

Параметр	Описание
AllowGroups	Задает разделенный пробелами список групп. Эти группы будут допущены в систему
DenyGroups	То же, что AllowGroups, только смысл проверки обратный. Записанные в этот параметр группы не будут допущены в систему
AllowUsers	Задает разделенный пробелами список пользователей. Только перечисленные пользователи получают доступ в систему. По умолчанию доступ разрешен всем пользователям
DenyUsers	То же, с противоположным смыслом проверки
AFSTokenPassing	Указывает на то, может ли маркер AFS пересылаться на сервер. По умолчанию — yes
AllowTCPForwarding	Указывает на то, разрешены ли запросы на переадресацию портов (по умолчанию — yes)
Banner	Отображает полный путь к файлу сообщения, выводимого перед аутентификацией пользователя
ChallengeResponseAuthentication	Указывает на то, разрешена ли аутентификация по методу «оклик — ответ». По умолчанию — yes
Ciphers	Задает разделенный запятыми список методов защиты соединения, разрешенных для использования
CheckMail	Указывает на то, должна ли служба sshd проверять почту в интерактивных сеансах регистрации (по умолчанию — no)
ClientAliveInterval	Задает интервал ожидания в секундах, по истечении которого клиенту посылается запрос на ввод данных
ClientAliveCountMax	Задает число напоминающих запросов, посылаемых клиенту. Если по достижении указанного предела от клиента не поступит данных, сеанс завершается и сервер прекращает работу. Значение по умолчанию — 3
HostKey	Полный путь к файлу, содержащему личный ключ компьютера. (По умолчанию — /etc/ssh/ssh_host_key)

Продолжение таблицы 29

Параметр	Описание
GatewayPorts	Указывает на то, могут ли удаленные компьютеры подключаться к портам, для которых клиент запросил переадресацию (по умолчанию — no)
HostbasedAuthentication	Указывает на то, разрешена ли аутентификация пользователей с проверкой файлов .rhosts и /etc/hosts.equiv и открытого ключа компьютера. Значение по умолчанию — no
IgnoreRhosts	Указывает на то, игнорируются ли файлы $HOME/.rhosts и $HOME/.shosts. По умолчанию — yes
IgnoreUserKnownHosts	Указывает на то, игнорируется ли файл $HOME/.ssh/known_hosts в режимах аутентификации RhostsRSAAuthentication и HostbasedAuthentication (по умолчанию — no)
KeepAlive	Если равен yes (по умолчанию), демон sshd будет периодически проверять наличие связи с клиентом. В случае неуспешного завершения проверки соединение разрывается. Чтобы отключить этот механизм, надо задать параметр, равным no, в файле конфигурации и сервера, и клиента
KerberosAuthentication	Указывает на то, разрешена ли аутентификация с использованием Kerberos. По умолчанию — no
KerberosOrLocalPasswd	Указывает на то, должна ли использоваться локальная парольная аутентификация в случае неуспешной аутентификации на основе Kerberos
KerberosTgtPassing	Указывает на то, может ли структура TGT системы Kerberos пересылаться на сервер (по умолчанию — no)
KerberosTicketCleanup	Указывает на то, должен ли при выходе пользователя удаляться кэш-файл его пропуска Kerberos
ListenAddress	Задает интерфейс, к которому подключается служба sshd. Значение по умолчанию — 0.0.0.0, т. е. любой интерфейс
LoginGraceTime	Задает интервал времени в секундах, в течение которого должна произойти аутентификация пользователя. Если процесс аутентификации не успевает завершиться вовремя, сервер разрывает соединение и завершает работу. Значение по умолчанию — 600 с
LogLevel	Задает степень подробности журнальных сообщений. Возможные значения: QUIET, FATAL, ERROR, INFO (по умолчанию), VERBOSE, DEBAG (не рекомендуется)
MACs	Задает разделенный запятыми список доступных алгоритмов MAC (код аутентификации сообщений), используемых для обеспечения целостности данных
MaxStartups	Задает максимальное число одновременных неаутентифицированных соединений с демоном sshd

Продолжение таблицы 29

Параметр	Описание
PAMAuthenticationViaKbdInt	Указывает на то, разрешена ли парольная аутентификация с использованием PAM (по умолчанию — no)
PasswordAuthentication	Если равен yes (по умолчанию), и ни один механизм беспарольной аутентификации не приносит положительного результата, тогда пользователю выдается приглашение на ввод пароля, который проверяется самим демоном sshd. Если параметр равен no, парольная аутентификация запрещена
PermitEmptyPasswords	Если равен yes, пользователи, не имеющие пароля, могут быть аутентифицированы службой sshd. Если параметр равен no (по умолчанию), пустые пароли запрещены
PermitRootLogin	Указывает на то, может ли пользователь root войти в систему с помощью команды ssh. Возможные значения: yes (по умолчанию), without-password, forced-command-only и no
PidFile	Задает путь к файлу, содержащему идентификатор главного процесса (по умолчанию — /var/run/sshd.pid)
Port	Задает номер порта, к которому подключается sshd. По умолчанию — 22
PrintLastLog	Указывает на то, должна ли служба sshd отображать сообщение о времени последнего доступа. По умолчанию — yes
PrintMotd	Указывает на то, следует ли после регистрации в системе отображать содержимое файла /etc/motd. По умолчанию — yes
Protocol	Задает разделенный запятыми список версий протокола, поддерживаемых службой sshd
PubKeyAuthentication	Указывает на то, разрешена ли аутентификация с использованием открытого ключа (по умолчанию — yes)
ReverseMappingCheck	Указывает на то, должен ли выполняться обратный поиск имен. По умолчанию — no
StrictModes	Если равен yes (по умолчанию), sshd будет запрещать доступ любому пользователю, чей начальный каталог и/или файл .rhosts принадлежат другому пользователю либо открыты для записи
Subsystem	Предназначается для конфигурирования внешней подсистемы. Аргументами является имя подсистемы и команда, выполняемая при поступлении запроса к подсистеме
SyslogFacility	Задает название средства, от имени которого регистрируются события в системе Syslog. Возможны значения: DAEMON, USER, AUTH (по умолчанию), LOCAL0-7

Окончание таблицы 29

Параметр	Описание
UseLogin	Указывает на то, должна ли применяться команда login для организации интерактивных сеансов регистрации (по умолчанию — no)
X11Forwarding	Указывает на то, разрешена ли переадресация запросов к системе X Window (по умолчанию —no)
X11DisplayOffset	Задает номер первого дисплея (сервера) системы X Window, доступного демону sshd для переадресации запросов (по умолчанию — 10)
XAuthLocation	Задает путь к команде xauth (по умолчанию — /usr/X11R6/bin/xauth)

5.7.2. Клиент ssh

Клиентом является команда ssh. Синтаксис командной строки:

```
ssh [-afgknqstvxACNTX1246] [-b bind_address] [-c cipher_spec] [-e escape_char]
[-i identity_file] [-login_name] [-m mac_spec] [-o option] [-p port]
[-F configfile] [-L port:host:hostport] [-R port:host:hostport]
[-D port] hostname | user@hostname [command]
```

Подробно со значениями флагов можно ознакомиться в руководстве man. В простом варианте инициировать соединение с сервером sshd можно командой:

```
ssh 10.1.1.170
```

где 10.1.1.170 — IP-адрес компьютера с запущенной службой sshd. При этом sshd будет считать, что пользователь, запрашивающий соединение, имеет такое же имя, под каким он аутентифицирован на компьютере-клиенте. Теоретически клиент ssh может заходить на сервер sshd под любым именем, используя флаг:

```
-l <имя_клиента>
```

Однако сервер будет согласовывать ключ сеанса (например, при беспарольной аутентификации по открытому ключу пользователя), проверяя открытые ключи в домашнем каталоге пользователя именно с этим именем на компьютере-клиенте. Если же используется парольная аутентификация, на компьютере-сервере должна существовать учетная запись с таким именем. Использовать беспарольную аутентификацию по открытым ключам компьютера настоятельно не рекомендуется, т. к. при этом способе в системе должны существовать потенциально опасные файлы: /etc/hosts.equiv, /etc/shosts.equiv, $HOME/.rhosts, $HOME/.shosts.

Команда ssh берет свои конфигурационные установки сначала из командной строки, затем из пользовательского файла $HOME/.ssh/config и из общесистемного файла /etc/ssh/ssh_config. Если идентичные параметры заданы по-разному, выбирается самое первое значение.

В таблице 30 описаны параметры, которые могут присутствовать в файле $HOME/.ssh/config или /etc/ssh/ssh_config. Пустые строки и комментарии игнорируются.

Таблица 30

Параметр	Описание
CheckHostIP	Указывает на то, должна ли команда ssh проверять IP-адреса в файле known_hosts (по умолчанию — yes)
Ciphers	Задает разделенный запятыми список методов защиты сеанса, разрешенных для использования. По умолчанию — aes122b-cbc, 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes192-cbc, aes256-cbc
Compression	Указывает на то, должны ли данные сжиматься с помощью команды gzip (по умолчанию — no). Эта установка может быть переопределена с помощью опции командной строки -C
ConnectionAttempts	Задает число неудачных попыток подключения (одна в секунду), после чего произойдет завершение работы. Значение по умолчанию — 4
EscapeChar	Задает escape-символ, используемый для отмены специального назначения следующего символа в сеансах с псевдотерминалом. По умолчанию — ~. Значение none запрещает использование escape-символа
ForwardAgent	Указывает на то, будет ли запрос к команде ssh-agent переадресован на удаленный сервер (по умолчанию — no)
ForwardX11	Указывает на то, будут ли запросы к системе X Window автоматически переадресовываться через SSH-туннель с одновременной установкой переменной среды DISPLAY (по умолчанию — no)
GatewayPorts	Указывает на то, могут ли удаленные компьютеры подключаться к локальным портам, для которых включен режим переадресации (по умолчанию — no)
GlobalKnownHostsFile	Задает файл, в котором хранится глобальная база ключей компьютера (по умолчанию — /etc/ssh/ssh_known_hosts)
HostbasedAuthentication	Указывает на то, разрешена ли аутентификация пользователей с проверкой файлов .rhosts, /etc/hosts.equiv и открытого ключа компьютера. Этот параметр рекомендуется установить в значение no
HostKeyAlgorithm	Задает алгоритмы получения ключей компьютеров в порядке приоритета. Выбор по умолчанию — ssh-rsa, ssh-dss
HostKeyAlias	Задает псевдоним, который должен использоваться при поиске и сохранении ключей компьютера
HostName	Задает имя или IP-адрес компьютера, на котором следует регистрироваться. По умолчанию выбирается имя, указанное в командной строке

Продолжение таблицы 30

Параметр	Описание
IdentityFile	Задает файл, содержащей личный ключ пользователя (по умолчанию — $HOME/.ssh/identity). Вместо имени начального каталога пользователя может стоять символ ~. Разрешается иметь несколько таких файлов. Все они будут проверены в указанном порядке
KeepAlive	Если равен yes (по умолчанию), команда ssh будет периодически проверять наличие связи с сервером. В случае неуспешного завершения проверки (в т. ч. из-за временных проблем с маршрутизацией) соединение разрывается. Чтобы отключить этот механизм, следует задать данный параметр, равным no, в файлах /etc/ssh/sshd_config и /etc/ssh/ssh_config (либо $HOME/.ssh/config)
KerberosAuthentication	Указывает на то, разрешена ли аутентификация с применением Kerberos
KerberosTgtPassing	Указывает на то, будет ли структура TGT системы Kerberos пересылаться на сервер
LocalForward	Требует значения в формате порт:узел:удаленный_порт. Указывает на то, что запросы к соответствующему локальному порту перенаправляются на заданный порт удаленного узла
LogLevel	Задает степень подробности журнальных сообщений команды ssh. Возможные значения: QUIET, FATAL, ERROR, INFO (по умолчанию), VERBOSE, DEBAG
MACs	Задает разделенный запятыми список доступных алгоритмов аутентификации сообщений для обеспечения целостности данных. Стандартный выбор: hmac-md5, hmac-sha1, hmac-ripemd160@openssh.com, hmac-sha1-96, hmac-md5-96
NumberOfPasswordPrompts	Задает число допустимых попыток ввести пароль (по умолчанию — 3)
PasswordAuthentication	Если равен yes (по умолчанию), то в случае необходимости команда ssh пытается провести парольную аутентификацию
Port	Задает номер порта сервера (по умолчанию — 22)
PreferredAuthentications	Задает порядок применения методов аутентификации (по умолчанию — publickey, password, keyboard-interactive)
Protocol	Задает в порядке приоритета версии протокола SSH
ProxyCommand	Задает команду, которую следует использовать вместо ssh для подключения к серверу. Эта команда выполняется интерпретатором /bin/sh. Спецификация %p соответствует номеру порта, а %h — имени удаленного узла
PubkeyAuthentication	Указывает на то, разрешена ли аутентификация с использованием открытого ключа (по умолчанию — yes)

Окончание таблицы 30

Параметр	Описание
RemoteForward	Требует значения в формате удаленный_порт:узел:порт. Указывает на то, что запросы к соответствующему удаленному порту перенаправляются на заданный порт заданного узла. Переадресация запросов к привилегированным портам разрешена только после получения прав суперпользователя на удаленной системе. Эта установка может быть переопределена с помощью опции командной строки -R
StrictHostKeyCheking	Если равен yes, команда не будет автоматически добавлять ключи компьютера в файл $HOME/.ssh/known_hosts и откажется устанавливать соединение с компьютерами, ключи которых изменились. Если равен no, команда будет добавлять непроверенные ключи сервера в указанные файлы. Если равен ask (по умолчанию), команда будет спрашивать пользователя о том, следует ли добавлять открытый ключ сервера в указанные файлы
UsePrivilegedPort	Указывает на то, можно ли использовать привилегированный порт для установления исходящих соединений. Значение по умолчанию — no
User	Задает пользователя, от имени которого следует регистрироваться в удаленной системе. Эта установка может быть переопределена с помощью опции командной строки -l
UserKnownHostsFile	Задает файл, который используется для автоматического обновления открытых ключей
XAuthLocation	Задает путь к команде xauth (по умолчанию — /usr/X11R6/bin/xauth)

Клиентские конфигурационные файлы бывают глобальными, на уровне системы (/etc/ssh/ssh_config), и локальными, на уровне пользователя ($HOME/.ssh/config). Следовательно, пользователь может полностью контролировать конфигурацию клиентской части SSH.

Конфигурационные файлы разбиты на разделы, установки которых относятся к отдельному компьютеру, группе компьютеров или ко всем компьютерам. Установки разных разделов могут перекрывать друг друга.

5.8. Настройка сервера единого сетевого времени

Сервер единого сетевого времени предназначен для синхронизации времени компьютера в ЛВС. В основе лежит протокол NTP. Алгоритм коррекции временной шкалы включает внесение задержек, коррекцию частоты часов и ряд механизмов, позволяющих достичь точности порядка нескольких миллисекунд, даже после длительных периодов, когда потеряна связь с синхронизирующими источниками. Для надежной защиты передаваемого сигнала используется аутентификация при помощи криптографических ключей. Целост-

ность данных обеспечивается с помощью IP- и UDP-контрольных сумм.

5.8.1. Режимы работы

Существует четыре режима работы сервера единого сетевого времени. Каждый режим определяет способ взаимодействия рабочих станций в сети синхронизации:

1) клиент-сервер — в этом режиме клиент посылает запрос серверу, который обрабатывает его и немедленно посылает ответ. Такой режим работы обеспечивает синхронизацию времени клиента со временем сервера, но сам сервер при этом с клиентом не синхронизируется. Режим «клиент-сервер» используется в тех случаях, когда нужна максимальная точность синхронизации времени и надежная защита передаваемой информации;

2) симметричный — может быть активным или пассивным:

– в активном режиме каждый компьютер в сети периодически посылает сообщения другому компьютеру вне зависимости от ее достижимости и слоя. При этом компьютер оповещает о своем намерении синхронизировать и быть синхронизированным своим партнером. Адреса партнеров известны заранее. Этот режим обычно используется серверами с большим номером слоя;

– в пассивном режиме адрес партнера заранее не известен. Взаимодействие в этом режиме начинается по прибытии сообщения от партнера (с неизвестным адресом), работающего в симметрично активном режиме, и сохраняется до тех пор, пока партнер достижим и функционирует в слое ниже или равном слою данного компьютера. Пассивный режим обычно используется первичными или вторичными серверами.

Симметричный режим обеспечивает высокую надежность синхронизации, т. к. при выходе из строя одного из источников времени система автоматически переконфигурируется таким образом, чтобы исключить его из сети синхронизации;

3) широковещательный — в этом режиме один или более серверов времени рассылают широковещательные сообщения, клиенты определяют время исходя из предположения, что задержка составляет несколько миллисекунд. Сервер при этом не принимает ответных ntp-сообщений.

Такой режим используется в быстрых локальных сетях с большим числом рабочих станций и без необходимости в высокой точности;

4) межсетевой — аналогичен широковещательному, но в отличие от него ntp-сообщения передаются не в рамках одной подсети, ограниченной локальным широковещательным адресом, а распространяются так же и в другие сети. Для работы службы единого времени в межсетевом режиме выделен специальный групповой IP-адрес (`224.0.1.1`), который используется как для серверов, так и для клиентов.

Межсетевой режим используется в сетях, разделенных на подсети с помощью маршрутизаторов и мостов, которые не способны ретранслировать широковещательные IP-дейтаграммы.

При реализации службы единого сетевого времени на сети системы могут играть четыре возможные роли:

1) серверы — предоставляют сервис времени другим системам;

2) равноправные узлы — многие серверы единого времени вступают в равноправные отношения с другими серверами того же уровня (`stratum level`). Если сервер второго уровня теряет связь со своим источником времени первого уровня, он может временно использовать сервис времени, предоставляемый равноправным узлом второго уровня;

3) опросные клиенты — регулярно опрашивают, как минимум, один сервер единого времени, сличают ответы серверов и синхронизируют системные часы по наиболее точному источнику времени;

4) вещательные клиенты — пассивно принимают вещательные пакеты от серверов на ЛВС. Вещательные клиенты порождают меньший сетевой трафик, чем опросные клиенты, но обеспечивают меньшую точность.

Серверы второго уровня опрашивают серверы первого, получая от них текущее системное время. Рекомендуется, чтобы каждый сервер единого времени второго уровня сверялся, как минимум, с тремя серверами первого уровня для обеспечения надежности.

Демон `ntpd` будет автоматически опрашивать оба сервера первого уровня и синхронизироваться по источнику, который он считает наиболее точным. Чтобы еще более повысить надежность, каждый сервер второго уровня должен установить равноправные отношения, как минимум, еще с одним сервером второго уровня.

5.8.2. Установка

Действия, которые необходимо выполнить для установки сервера:

1) установить сервер NTP из соответствующего deb-пакета (при стандартной установке ОС сервер включается в состав пакетов по умолчанию);

2) изменить конфигурационный файл `ntp.conf` на сервере. Вместо

```
server 0.debian.pool.ntp.org iburst
server 1.debian.pool.ntp.org iburst
server 2.debian.pool.ntp.org iburst
server 3.debian.pool.ntp.org iburst
```

необходимо написать:

```
server 127.127.1.0
fudge 127.127.1.0 startum 10
```

изменить пункт:

```
# Clients from this (example!) subnet have unlimited access, but only if
# cryptographically authenticated.
```

задать свою подсеть:

```
restrict 10.0.0.0 mask 255.255.255.0 nomodify notrap
```

3) для автоматического запуска NTP выполнить команду:

```
update-rc.d ntp defaults
```

4) подстроить приблизительное время часов вручную. Точность настройки не должна быть хуже 1000 с от реального времени;

5) перезапустить ОС.

Для клиентов нужно создать файл `/etc/cron.d/ntpdate` со следующим содержимым:

```
*/10 * * * * root /usr/sbin/ntpdate <ntp-сервер>
```

где вместо `<ntp-сервер>` нужно указать доменное имя или IP-адрес машины, на которой настроен сервер NTP. В примере: обращение к серверу один раз в 10 мин.

5.8.3. Настройка и конфигурация

Настройка и управление сервером осуществляется либо путем задания опций в командной строке, либо путем редактирования конфигурационного файла. Первый способ предоставляет ограниченные возможности настройки, второй — наиболее полные.

Во время своего запуска сервер `ntpd` читает конфигурационный файл `ntp.conf`, который обычно находится в каталоге `/etc`, но может быть перемещен в любой другой каталог (см. опцию командной строки `-c conffile`).

Формат файла аналогичен формату других конфигурационных файлов ОС: комментарии начинаются с символа # и действуют до конца строки, пустые строки игнорируются. Конфигурационные команды состоят из ключевого слова и следующих за ним аргументов, разделенных пробелами. Любая команда должна занимать строго одну строку. Аргументами могут быть имена и адреса хостов (в форме IP-адресов и доменных имен), целые и дробные числа, текстовые строки. Далее необязательные аргументы заключены в квадратные скобки `[ ]`, альтернативные аргументы отделены символом `|`. Нотация вида `[...]` означает, что стоящий перед ней необязательный аргумент может повторяться несколько раз.

5.8.3.1. Конфигурационный файл ntp.conf

Синтаксис:

```
server address [key key | autokey] [version version] [prefer]
[minpoll minpoll] [maxpoll maxpoll]
peer address [key key | autokey] [version version] [prefer]
[minpoll minpoll] [maxpoll maxpoll]
```

```
broadcast address [key key | autokey] [version version]
[minpoll minpoll] [ttl ttl]
manycastclient address [key key | autokey] [version version] [minpoll minpoll
[maxpoll maxpoll] [ttl ttl]
```

Описание команд приведено в таблице 31.

Таблица 31

Команда	Описание
`server`	Позволяет установить постоянное соединение (организовать постоянную ассоциацию) клиента с удаленным сервером. При этом локальное время может быть синхронизировано с удаленным сервером, но удаленный сервер не может синхронизировать свое время с локальным
`peer`	Устанавливается постоянное соединение (ассоциация) в симметрично-активном режиме с указанным удаленном сервером (`peer` — симметричным). В данном режиме локальные часы могут быть синхронизированы с удаленным симметричным сервером или удаленный сервер может синхронизироваться с локальными часами
`broadcast`	Организуется постоянная широковещательная ассоциация
`manycastclient`	Организуется межсетевой режим синхронизации с указанным групповым адресом
`vmanycast`	Указывает, что локальный сервер должен работать в клиентском режиме с удаленными серверами, которые обнаруживаются в процессе работы при помощи широковещательных/межсетевых пакетов

Описание опций команд приведено в таблице 32.

Таблица 32

Опция	Описание
`autokey`	Все отсылаемые пакеты включают аутентификационные поля, зашифрованные в автоматическом режиме
`key key`	Все отправляемые и принимаемые пакеты включают поля аутентификации, зашифрованные при помощи ключа шифрования с заданным идентификатором, значения которого составляют от 1 до 65534. По умолчанию поля аутентификации не используются
`minpoll minpoll`, `maxpoll maxpoll`	Указание временных задержек
`noselect`	Указывает, что сервер используется только в демонстративных целях
`prefer`	Отмечает, что сервер является предпочтительным
`ttl ttl`	Указывает время жизни пакета, используется только в широковещательном и межсетевом режимах
`version version`	Указывает версию протокола отправляемых пакетов (по умолчанию — 4)

5.8.3.2. Конфигурирование процесса аутентификации

Поддержка аутентификации позволяет клиенту службы единого времени удостовериться, что сервер является именно тем, за кого он себя выдает. Конфигурирование производится в файле `ntp.conf` с использованием дополнительных опций команд `peer`, `server`, `broadcast` и `multicast`.

– `autokey [logsec]` — указывает интервалы в секундах между генерациями нового ключа;

– `controlkey key` — указывает идентификатор ключа для использования командой `ntpq`;

– `keys keyfile` — указывает местонахождение файла, хранящего ключи и их идентификаторы, используемые командами `ntpd`, `ntpq` и `ntpdc`. Данная команда эквивалентна использованию опции `-k` командной строки;

– `keysdir путь_к_директории` — указывает путь к каталогу, хранящему ключи (по умолчанию — `/usr/local/etc/`);

– `trustedkey key [...]` — указывает идентификаторы ключей, которые являются доверенными для аутентификации с симметричным ключом.

Для создания ключей используется команда `ntp-keygen`. Для запуска необходимо иметь права суперпользователя. При запуске она генерирует новые ключи и записывает их в соответствующие файлы.

5.8.3.3. Конфигурация сервера уровней 1 и 2

Чтобы настроить конфигурацию сервера уровня 1, необходимо добавить в файл `/etc/ntp.conf` следующие строки:

```
server символический_IP_адрес
peer DNS_имя_соседнего_сервера_1
peer DNS_имя_соседнего_сервера_2
```

Символический IP-адрес в первой строке используется службой `ntpd` для того, чтобы определить, какого типа радиочасы подсоединены к системе. Конфигурация сервера уровня 2:

```
server DNS_имя_сервера_уровня_1
server DNS_имя_сервера_уровня_1
peer DNS_имя_соседнего_сервера_уровня_2
driftfile /etc/ntp.drift
broadcast _IP_адрес
```

где записи `server` — определяют, какие серверы уровня 1 должен опрашивать данный сервер, чтобы воспользоваться сервисом времени;

`peer` — определяет равноправные отношения с другим сервером уровня 2;

driftfile — задает имя файла, который будет использоваться для отслеживания долгосрочного сдвига локальных часов;

broadcast — указывает демону ntpd регулярно сообщать вещательным клиентам сети об официальном времени.

5.8.4. Методы синхронизации системных часов

Система единого времени предусматривает два механизма для синхронизации системных часов с другими узлами в сети.

Команда ntpdate, выполняемая с опцией -b, опрашивает, как минимум, один сервер единого времени, затем синхронизирует системные часы с наиболее точным сервером единого сетевого времени. Выполняется только при запуске системы до того, как запускаются приложения.

После того, как во время загрузки команда ntpdate первоначально синхронизирует системные часы, демон ntpd постоянно работает в фоновом режиме, периодически опрашивая серверы службы единого времени, заданные в /etc/ntp.conf, и по мере необходимости, «подкручивая» системные часы, чтобы поддерживать синхронизацию. Эти незначительные постепенные корректировки во времени должны быть прозрачными для приложений. Файл сдвига, определяемый в записи driftfile, используется для отслеживания различий между временем клиента и временем сервера. По мере стабилизации файла сдвига сервер будет опрашиваться все реже.

5.8.4.1. ntpd

Синтаксис:

```
ntpd [-опции]
```

Команда ntpd является демоном ОС, который устанавливает и поддерживает системное время, синхронизируя его с остальными серверами единого времени. Демон ntpd обменивается сообщениями с одним или более серверами с установленной периодичностью.

Опции командной строки приведены в таблице 33.

Таблица 33

Опция	Описание
-4	Форсирование разрешения доменных имен в пространство имен протокола IP версии 4
-6	Использование пространства имен протокола IP версии 6
-A	Не использовать криптографические алгоритмы
-b	Разрешить клиенту синхронизировать системное время с вещательными клиентами

Продолжение таблицы 33

Опция	Описание
`-c конфигурационный_файл`	Указать имя и путь конфигурационного файла (по умолчанию — `/etc/ntp.conf`)
`-d`	Отладочный режим
`-D уровень`	Указать уровень отладки
`-f driftfile`	Указать имя файла сдвига частоты локальных системных часов (по умолчанию — `/etc/ntp.drift`). Эта опция аналогична команде `driftfile` в `/etc/ntp.conf`
`-g`	Обычно процесс `ntpd` завершается с соответствующим сообщением в файле журналирования, если локальное время отличается от реального времени более, чем на 1000 с. Данная опция позволяет устанавливать время без каких-либо ограничений, однако, это может быть сделано только один раз. Если порог будет превышен и после этой операции демон `ntpd` будет завершен с соответствующим сообщением в файл журнала. Эта опция может использоваться с опциями `-q` и `-x`
`-i директория`	Поменять корневой каталог на каталог, указанный в команде. Данная опция подразумевает, что сервер пытается при запуске понизить привилегии суперпользователя, иначе могут возникнуть некоторые проблемы с безопасностью. Это возможно, если ОС поддерживает работу сервера без полных привилегий `root`
`-k keyfile`	Указать имя и путь к файлу симметричного ключа (по умолчанию — `/etc/ntp.keys`). Эта опция аналогична команде `keyfile` в файле `/etc/ntp.conf`
`-l путь_и_имя_файла`	Указать имя и путь к файлу логического журнала. По умолчанию используется системный файл логического журнала. Данная опция эквивалентна команде `logfile` в конфигурационном файле `/etc/ntp.conf`
`-L`	Не прослушивать виртуальные IP-адреса. По умолчанию прослушиваются
`-m`	Разрешить клиенту синхронизировать межсетевые сервера IP версии 4 с групповым адресом `224.0.1.1`
`-n`	Не использовать системный вызов `fork`
`-N`	Запускать `ntpd` с максимальным приоритетом
`p файл_процесса`	Указать имя и путь к файлу, хранящему идентификатор процесса `ntpd` в системе. Данная опция эквивалентна команде `pidfile` в конфигурационном файле
`-P приоритет`	Указать приоритет запускаемого серверного процесса
`-q`	Завершить процесс `ntpd` сразу после синхронизации времени

Окончание таблицы 33

Опция	Описание
`-r задержка_распространения_вещательного_пакета`	Задержка распространения вещательного пакета от сервера клиенту. Данная опция необходима только, если задержка не может быть вычислена автоматически протоколом NTP
`-s директория`	Указать путь к каталогу с файлами, создаваемыми командой подсчета статистики
`-u пользователь [:группа]`	Указать пользователя (группу), от чьего имени запускается процесс. Данная опция возможна только в ОС, в которой процесс `ntpd` может быть запущен без прав `root`
`-x`	Запустить процесс в обычном режиме. Локальное системное время корректируется процессом только, если «ошибка» составляет менее, чем установленная величина порога (по умолчанию — 128 мс). Данная опция устанавливает величину порога в 600 с

5.8.4.2. ntpq

Синтаксис:

```
ntpq [-ip] [-c команда] [хост] [...]
```

Команда `ntpq` используется для мониторинга деятельности демона `ntpd` и определения производительности. Может быть запущена как в интерактивном режиме, так и с использованием опций командной строки. Она может получать и выводить на терминал список серверов того же уровня синхронизации в обычном формате, запрашивая все сервера.

Опции командной строки приведены в таблице 34.

Таблица 34

Опция	Описание
`-4`	Форсирование разрешения доменных имен в пространство имен протокола IP версии 4
`-6`	Использование пространства имен протокола IP версии 6
`-d`	Отладочный режим
`-i`	Форсирование интерактивного режима. Команды принимаются со стандартного выхода
`-p`	Вывод всех известных соседних серверов

Интерактивные команды

Интерактивная команда состоит из командного слова и следующих за ним аргументов (возможно использование от 0 до 4 аргументов). Вывод результата выполнения команды направляется на стандартный вывод (`stdout`). Другими словами, можно перенаправлять вывод команды в файл, используя `> имя_файла`. Список интерактивных команд приведен в таблице 35.

Таблица 35

Команда	Описание
? [командное_слово] help1 [командное_слово]	Если задана опция ?, на терминал будет выдана информация о возможном использовании данной команды
addvars имя_переменной [= значение] [...] rmvars имя_переменной [...] clearvars	Данные, передаваемые протоколом NTP, содержат ряд сущностей вида: имя_переменной=значение. Команда ntpq поддерживает внутренний список, в котором данные встраиваются в контрольные сообщения. Команда addvars добавляет переменные в список, rmvars удаляет переменные из списка, clearvars полностью очищает список
cooked	Позволяет преобразовать вывод переменных и их значения в удобный для пользователя вид
debug more | less | off	Позволяет включить/выключить внутреннюю команду запросов
delay миллисекунды	Указывает временный интервал для добавления к временной отметке (timestamp), которая включается в запросы, требующие аутентификации. Это используется для возможности переконфигурации сервера
host имя_хоста	Устанавливает имя хоста, к которому будут отсылаться последующие запросы
hostnames [yes | no]	Если указывается yes, доменные имена хостов выводятся на терминал. Иначе выводятся на терминал численные адреса. По умолчанию стоит yes
keyid идентификатор_ключа	Позволяет указать номер ключа для использования его в запросах, требующих аутентификацию
ntpversion 1 | 2 | 3 | 4	Устанавливает номер версии NTP. По умолчанию используется протокол версии 6
passwd	Запрашивает пароль, который будет использоваться в запросах, требующих аутентификации
quit	Выход из интерактивного режима ntpq
raw	Заставляет выводить результаты запросов команды, как будто они пришли от удаленного сервера
timeout миллисекунды	Устанавливает временной интервал запросов серверам. По умолчанию составляет 5000 мс

Команды контрольных сообщений

Каждая ассоциация, известная NTP-серверу, имеет личный 16-битный целочисленный идентификатор. Ассоциация с идентификатором 0 играет особую роль — определяет системные переменные, чьи имена лежат вне локального пространства имен. Команды контрольных сообщений приведены в таблице 36.

Таблица 36

Команда	Описание
associations	Получение и вывод списка идентификаторов ассоциаций и текущее состояние соседних серверов. Список выводится в виде колонок
cv [assocID] [variable_name [= value [...]][...]	Запрос на переменные серверных часов. На данный запрос отвечают серверы, имеющие внешние источники синхронизации времени
lassociations	Получает и выводит список идентификаторов ассоциаций и соседних серверов (peer), с которыми общается сервер
lpassociations	Выводит сведения о всех ассоциациях из кэшированного списка
peers	Получение текущего списка соседних серверов (peer)

5.8.4.3. ntpdate

Синтаксис:

```
ntpdate [ -опции]
```

Команда ntpdate устанавливает локальное системное время, используя NTP. Должна быть запущена с правами root. Возможен запуск как из командной строки (вручную), так и из стартового скрипта, выполняемого при загрузке ОС. Есть возможность выполнения ntpdate из сценария демона cron.

Данная команда завершается, если обнаруживается, что на том же хосте запущен сервер ntpd.

Опции командной строки приведены в таблице 37.

Таблица 37

Опция	Описание
-4	Форсирование разрешения доменных имен в пространство имен протокола IP версии 4
-6	Использование пространства имен протокола IP версии 6
-a ключ	Разрешение аутентификации и указание ключа для использования. По умолчанию аутентификация отключена
-d	Отладочный режим
-q	Только запрос. Никаких изменений локальных часов не производится
-t время_в_секундах	Установка максимального времени ожидания ответа сервера

5.8.4.4. ntptrace

Синтаксис:

```
ntptrace [ -vdn ] [ -r retries ] [ -t timeout ] [ server ]
```

Программа `ntptrace` определяет, где сервера NTP получают время, и проходит по цепочке серверов до источника точного времени.

Если на вход команде не поступает никаких аргументов, то началом поиска будет локальный хост.

Опции командной строки приведены в таблице 38.

Таблица 38

Опция	Описание
`-d`	Отладочный режим
`-n`	В результатах запроса вместо доменных имен хостов выдаются их IP-адреса. Данная опция удобна, когда в сети отсутствует DNS
`-r retries`	Установка количества попыток передачи (по умолчанию — 5)
`-t временная_задержка`	Установка временной задержки передачи данных в секундах (по умолчанию — 2)
`-v`	Выдача многословной информации о NTP-серверах

5.8.4.5. fly-admin-ntp

В состав ОС входит графическая утилита `fly-admin-ntp`, которая позволяет администратору произвести большинство настроек системы NTP в графическом режиме (см. электронную справку).

5.8.4.6. Перевод времени

При переводе часов на..... периодически может возникать проблема циклической перезагрузки ЭВМ.

5.9. Сетевая защищенная файловая система

5.9.1. Назначение и возможности

Для организации защищенных файловых серверов предназначена сетевая защищенная ФС (СЗФС), в основу которой положена CIFS, работающая по протоколу SMB/CIFS. Протокол СЗФС содержит в себе сообщения, которые передают информацию о стандартных и расширенных атрибутах (атрибутах безопасности), а также сообщения для передачи мандатной метки субъекта доступа.

Условием корректного функционирования СЗФС является использование механизма ЕПП, обеспечивающее в рамках данной ЛВС однозначное соответствие между логическим именем пользователя и его идентификатором (а также именем группы и ее идентификатором) на всех компьютерах (рабочих станциях и серверах), на которых данный пользователь может работать. Для корректной работы СЗФС необходима синхронизация UID/GID в системах клиента и сервера, т. к. информация о пользователях и группах передается в сеть в численных значениях.

СЗФС состоит из сервера и клиента. Сервер представляет собой расширенный сервер Samba и выполняет следующие задачи:

1) управление разделяемыми ресурсами;

2) контроль доступа к разделяемым ресурсам. При подключении клиента сервер устанавливает мандатную метку процесса, обслуживающего запросы клиента, в соответствии с мандатной меткой этого клиента. Этим обеспечивается мандатный контроль доступа к разделяемым файлам на стороне сервера.

Клиент представляет собой сетевую ФС в составе системы управления файлами ядра ОС и реализует интерфейс между виртуальной ФС ядра и сервером СЗФС. Клиент СЗФС выполняет следующие задачи:

1) отображение каталогов и файлов смонтированного сетевого ресурса;

2) передача на сервер дополнительной информации о классификационной метке пользователя (процесса), работающего с разделяемым ресурсом.

С точки зрения пользователя, СЗФС выглядит как стандартная ФС, поддерживающая все механизмы защиты ОС и позволяющая работать с удаленной ФС с помощью стандартных команд.

СЗФС предоставляет следующие базовые возможности:

– разделение ФС ОС «Astra Linux Special Edition», ОС типа Windows и, наоборот;

– совместное использование принтеров, подключенных к ОС «Astra Linux Special Edition», ОС типа Windows и, наоборот.

5.9.2. Состав

СЗФС состоит из нескольких компонентов:

– `smbd` — сервисная служба, которая обеспечивает работу службы печати и разделения файлов для клиентов типа ОС Windows. Конфигурационные параметры сервисной службы `smbd` описываются в файле `smb.conf`;

– `nmbd` — сервисная служба, которая обеспечивает работу службы имен NetBIOS, а также может использоваться для запроса других сервисных служб имен;

– `smbclient` — сервисная служба, которая реализует клиент, используемый для доступа к другим серверам и для печати на принтерах, подключенных к серверам;

– `testparm` — команда, позволяющая протестировать конфигурационный файл `smb.conf`;

– `smbstatus` — команда, сообщающая, кто в настоящее время пользуется сервером `smbd`.

В состав ОС входит графическая утилита `fly-admin-samba`, которая устанавливается при установке `smbd` и позволяет настроить пользовательский доступ к ресурсам СЗФС (см. электронную справку).

5.9.3. Настройка

СЗФС устанавливается в процессе установки ОС.

Настройка СЗФС в ОС осуществляется посредством настройки параметров главного конфигурационного файла.

Главный конфигурационный файл называется `smb.conf` и находится в каталоге `/etc/samba`.

Файл `smb.conf` состоит из именованных разделов, начинающихся с имени раздела в квадратных скобках (например, `[global]`). Внутри каждого раздела находится ряд параметров в виде `key = value`. Файл конфигурации содержит три специальных раздела: `[global]`, `[homes]` и `[printers]` и несколько пользовательских разделов.

В разделе `[global]` описаны параметры, управляющие сервером `smb` в целом, а также находятся значения параметров по умолчанию для других разделов.

```
[global];
;workgroup = NT-Domain-Name или Workgroup-Name
workgroup = WORKGR1
;comment эквивалентен полю описания NT (Description field)
comment = Сервер СЗФС
```

Этот фрагмент определяет рабочую группу `WORKGR1`, к которой относится данный компьютер, а также описывает саму систему.

```
;printing = BSD или SYSV или A1X (и т.д.)
printing = bsd
printcap name = /etc/printcap
load printers = yes
```

Этот фрагмент описывает тип системы печати, доступный на сервере администратора, а также местонахождение конфигурационного файла принтера.

Последняя строка говорит о том, что все принтеры, определенные в файле `printcap`, должны быть доступны в сети.

```
;Раскомментируйте это поле, если вам нужен гостевой вход
;guest = pcguest
log file = /var/log/samba-log.%m
max log size = 50
```

В этом фрагменте определяется, будет ли сервер поддерживать гостевой вход. Следующие два параметра определяют работу с журнальными файлами. Параметр `m` сообщает службе Samba, что для каждого клиента ведется свой файл, а последняя строка говорит о том, что максимальный размер создаваемого журнального файла — 50 КБ.

Раздел `[homes]` позволяет подключаться к рабочим каталогам пользователей без их явного описания. При запросе клиентом определенной службы ищется соответствующее

ей описание в файле и, если такового нет, просматривается раздел [homes]. Если этот раздел существует, просматривается файл паролей для поиска рабочего каталога пользователя, сделавшего запрос, и, найдя его, он становится доступным по сети.

```
[homes]
comment = Home Directories
browseable = no
case sensitive = yes
read only = yes
create mask = 0700
directory mask = 0700
ea support = yes
```

Параметр comment выводится для клиента при запросе о доступных ресурсах; параметр browseable определяет, как выводить ресурс в списке просмотра. Параметр read only определяет, может ли пользователь создавать и изменять файлы в своем рабочем каталоге при подключении по сети. Параметр create mask определяет права доступа для вновь создаваемых файлов в рабочем каталоге пользователя.

В разделе [printers] описаны параметры управления печатью при отсутствии иного явного описания. Используется для предоставления доступа к принтерам, определенным в файле /etc/ (данная возможность в ОС заблокирована по умолчанию, для чего закомментированы все строки раздела [printers]).

```
[printers]
;    comment = All Printers
;    browseable = no
;    path = /var/spool/samba
;    printable = no
;    guest ok = no
;    read only = yes
;    create mask = 0700
```

Параметры comment, browseable, create mode описаны выше, см. раздел [homes]. Параметр path определяет местонахождение файла спулера при печати через SMB. Параметр printable определяет, может ли использоваться данный ресурс для печати, параметр guest ok — может ли воспользоваться принтером гостевой пользователь.

После настройки параметров сервера по умолчанию можно создать разделяемые каталоги, доступ к которым могут получать определенные пользователи, группы пользователей или все пользователи. Рассмотрим пример создания разделяемого каталога с доступом только для одного пользователя. Для этого необходимо создать отдельный раздел файла smb.conf и заполнить его необходимой информацией (обычно это пользователь, каталог и конфигурационная информация).

```
[User1]
comment = User1' s remote source code directory
path = /usr/locaI/src
valid users = victor
browseable = yes
public = no
writeable = yes
create mode = 0700
```

В этом разделе создается разделяемый каталог с именем User1. На локальном сервере его путь — /usr/local/src, browseable = yes, поэтому ресурс будет виден в списках ресурсов сети, но т. к. public = no, получить доступ к нему сможет только пользователь victor. Предоставить доступ и другим пользователям можно, поместив их в запись valid users.

После создания конфигурационного файла необходимо протестировать его корректность при помощи команды testparm, которая проверяет наличие в файле /etc/smb.conf внутренних противоречий и несоответствий.

Примечание. Применение testparm не дает гарантии, что все сервисы и ресурсы, описанные в конфигурации, доступны и будут корректно работать.

Синтаксис testparm:

```
testparm [configfile [hostname hostip]]
```

Параметр configfile определяет местоположение конфигурационного файла (если это не файл /etc/smb.conf). Параметр hostname hostip указывает команде testparm проверить доступ к сервисам со стороны узла, определяемого параметром.

Если ошибки не будут обнаружены, на экране появится примерно следующее сообщение (в случае обнаружения ошибок о них будет предоставлена полная информация):

```
it testparm
Load smb config files from /etc/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Loaded services file OK.
Press enter to see a dump of your service definitions
```

При нажатии **<Enter>** testparm протестирует каждый раздел, определенный в конфигурационном файле.

5.9.4. Запуск сервера

Сервер состоит из двух сервисных команд — smbd и nmbd. smbd обеспечивает работу службы разделения файлов и принтеров, а nmbd поддерживает имена NetBIOS.

Сервер запускается либо из инициализирующих сценариев, либо из inetd в каче-

стве системного сервиса.

Если сервер запускается из сценариев инициализации, то можно воспользоваться для запуска и остановки работы сервера следующей командой:

```
/etc/rc.d/init.d/samba start:stop
```

Доступ пользователей ОС к ресурсам сервера осуществляется с помощью монтирования СЗФС. Другой возможностью является использование графической утилиты `fly-admin-samba` (см. электронную справку).

Опции командной строки `smbclient` позволяют сделать запрос о разделяемых ресурсах или перенести файлы.

Например, для запроса списка доступных ресурсов на удаленном сервере `win.netwhart.com` используется командная строка:

```
smbclient -L -I win.netwhart.com
```

Здесь опция `-L` указывает, что требуется вывести список разделяемых ресурсов, а опция `-I` — что указанное далее имя следует рассматривать как имя DNS, а не NetBIOS.

Для пересылки файла необходимо сначала подключиться к серверу с использованием команды:

```
smbclient '\\WORKGR1\PUBLIC' -I win.netwhart.com -U tackett
```

Параметр `\\WORKGR1\PUBLIC` определяет удаленный сервис на другом компьютере (обычно это каталог ФС или принтер). Опция `-U` позволяет определить имя пользователя для подключения к ресурсу (при этом, если необходимо, СЗФС запросит соответствующий пароль). После подключения появится приглашение:

```
Smb:\
```

где `\` — текущий рабочий каталог.

В этой командной строке можно указать команды для передачи файлов и работы с ними (см. руководство `man`).

6. СРЕДСТВА ОРГАНИЗАЦИИ ЕПП

Единое пространство пользователей представляет собой средства организации работы пользователя в сети компьютеров, работающих под управлением ОС. В основу положен доменный принцип построения сети, подразумевающий объединение в одну сеть логически связанных компьютеров, например принадлежащих одной организации. При этом пользователь получает возможность работы с сетевыми ресурсами сети и взаимодействия с другими пользователями.

Организация ЕПП обеспечивает:

– сквозную аутентификацию в сети;

– централизацию хранения информации об окружении пользователей;

– централизацию хранения настроек системы защиты информации на сервере.

Сетевая аутентификация и централизация хранения информации об окружении пользователя основана на использовании двух основных механизмов: NSS (6.1) и PAM (6.2).

Сквозная доверенная аутентификация реализуется технологией Kerberos (6.4).

В качестве источника данных для базовых системных сервисов на базе механизмов NSS и PAM используется служба каталогов LDAP (6.3).

Централизация хранения информации об окружении пользователей подразумевает и централизованное хранение домашних каталогов пользователей. Для этого используется СЗФС CIFS (см. 5.9).

6.1. Механизм NSS

Механизм NSS предоставляет всем программам и службам, функционирующим на локальном компьютере, системную информацию через соответствующие программные вызовы. Он обращается к конфигурационному файлу `/etc/nsswitch.conf`, в котором указаны источники данных для каждой из системных служб. Краткое описание системных служб приведено в таблице 39.

Таблица 39

Сервис	Источник данных по умолчанию	Описание
`passwd`	`/etc/passwd`	Окружение пользователя (домашний каталог, идентификатор пользователя и пр.)
`shadow`	`/etc/shadow`	Пароли пользователей
`group`	`/etc/group`	Принадлежность пользователей группам
`hosts`	`/etc/hosts`	Соответствие имен хостов адресам
`services`	`/etc/services`	Характеристики сетевых сервисов (порт, тип транспортного протокола)

Каждый из базовых системных сервисов поддерживает ряд библиотечных программных вызовов, таких как `getpwent`, `getspent`, `getgrent`, `getservent`. При выполнении данных программных вызовов производится поиск в конфигурационном файле `/etc/nsswitch.conf` источника данных соответствующего сервиса (например, `passwd` для получения домашнего каталога пользователя). По умолчанию в качестве источника данных системных сервисов используются соответствующие конфигурационные файлы в каталоге `/etc` (источник `files`). NSS при получении имени источника данных из конфигурационного файла `/etc/nsswitch.conf` осуществляет поиск программной разделяемой библиотеки в каталоге `/lib` с именем `libnss_<имя_источника_данных>-<версия_библиотеки>.so`, где в качестве имени источника данных выступает строка, полученная из `/etc/nsswitch.conf`. Например, при вызове `getpwent`, при условии, что в `/etc/nsswitch.conf` находится строка:

```
passwd : files
```

будет вызвана соответствующая функция из библиотеки `/lib/libnss_files.so`.

6.2. Механизм PAM

Механизм PAM (Pluggable Authentication Modules — подключаемые модули аутентификации) позволяет интегрировать различные низкоуровневые методы аутентификации и предоставить единые механизмы для использования прикладных программ в процессе аутентификации. Механизм состоит из набора разделяемых библиотек и конфигурационных файлов — сценариев процедур аутентификации.

В каталоге `/etc/pam.d` расположены конфигурационные файлы PAM для соответствующих сервисов, в т. ч. и для `login` (авторизованный вход в систему). В конфигурационном файле сервиса дана информация по проведению аутентификации.

Модули PAM вызываются при выполнении следующих функций:

1) `auth` — аутентификация;
2) `account` — получение привилегий доступа;
3) `password` — управление паролями;
4) `session` — сопровождение сессий.

Для выполнения каждой функции может быть перечислено несколько модулей PAM, которые будут вызываться последовательно, образуя стек PAM для данной задачи. Каждый вызываемый модуль возвращает в стек результат своей работы: или успешный (`PAM_SUCCESS`), или неуспешный (`PAM_AUTH_ERR`), или игнорирующий (`PAM_IGNORE`), или иной. Для каждого вызова может быть указан набор управляющих флагов в виде соответствия кода возврата и того, как результат работы модуля скажется на обработке всей сервисной задачи, например `ignore`, `ok`, `die`. Для управления аутентификацией используются следующие флаги:

– `requisite` — немедленное прекращение дальнейшего выполнения сервисной задачи с общим неуспешным результатом в случае неуспешного результата выполнения данного модуля;

– `required` — требование удачного выполнения этого модуля одновременно с выполнением всех остальных, перечисленных в данной сервисной задаче;

– `sufficient` — немедленное прекращение дальнейшего выполнения сервисной задачи с общим позитивным результатом, в случае позитивного результата выполнения данного модуля и всех предыдущих с флагом `required` в стеке задачи, если же модуль вернул негативный результат, то его значение игнорируется;

– `optional` — выполнение данного модуля никак не сказывается на результате всей задачи, но играет дополнительную информационную роль.

6.3. Служба каталогов LDAP

Служба каталогов LDAP — общее название клиент-серверной технологии доступа к службе каталогов X.500 с помощью протокола LDAP. Служба каталогов X.500 является средством иерархического представления информационных ресурсов, принадлежащих некоторой отдельно взятой организации, и информации об этих ресурсах. При этом служба каталогов обеспечивает централизованное управление, как самими ресурсами, так и информацией о них, а также позволяет контролировать их использование третьими лицами. Каждый ресурс может принадлежать одному или более классам. Каждый класс показывает, что ресурс является определённым типом сущности, и имеет определённый набор свойств. Совокупности классов могут объединяться в схемы, которые описывают типы ресурсов, применяемые в отдельно взятой предметной области.

Информация, хранящаяся в каталоге, называется «информационной базой каталога» (DIB). Пользователь каталога, который может быть как человеком, так и компьютером, получает доступ к каталогу посредством клиента. Клиент от имени пользователя каталога взаимодействует с одним или более серверами. Сервер хранит фрагмент DIB.

DIB содержит два типа информации:

– пользовательская — информация, предоставляемая пользователям и, быть может, изменяемая ими;

– административная и функциональная — информация, используемая для администрирования и/или функционирования каталога.

Множество записей, представленных в DIB, организовано иерархически в структуру дерева, известную как «информационное дерево каталога» (DIT). При этом запись в каталоге LDAP состоит из одного или нескольких атрибутов, обладает уникальным именем (DN — Distinguished Name) и может состоять только из тех атрибутов, которые определе-

ны в описании класса записи. В схеме определено, какие атрибуты являются для данного класса обязательными, а какие — необязательными. Каждый атрибут, хранящийся в каталоге LDAP, имеет определенный синтаксис (например, тип данных), который накладывает ограничения на структуру и формат его значений. Сравнение значений не является частью определения синтаксиса, а задается отдельно определяемыми правилами соответствия. Правила соответствия специфицируют аргумент, значение утверждения, которое также имеет определенный синтаксис.

Предполагается, что информация каталога достаточно статична, т.е. чаще читается, чем модифицируется. Примером подобного каталога является специализированная БД, например телефонная книга, база данных сервиса DNS.

Службы каталогов LDAP могут быть использованы в качестве источника данных для базовых системных сервисов на базе механизмов NSS и PAM.

В результате вся служебная информация пользователей сети может располагаться на выделенном сервере в распределенной гетерогенной сетевой среде. Добавление новых сетевых пользователей в этом случае производится централизованно на сервере службы каталогов.

Благодаря предоставлению информации LDAP в иерархической древовидной форме разграничение доступа в рамках службы каталогов LDAP может быть основано на введении доменов. В качестве домена в данном случае будет выступать поддерево службы каталогов LDAP.

6.4. Доверенная аутентификация Kerberos

Kerberos является протоколом, обеспечивающим централизованную аутентификацию пользователей и применяющим техническое маскирование данных для противодействия различным видам атак.

Основным компонентом системы Kerberos является центр распределения ключей (KDC). Программы, настроенные на взаимодействие с Kerberos, называются «керберизованными приложениями». KDC отвечает за аутентификацию в некоторой области Kerberos. В процессе работы система Kerberos выдает билеты (tickets) на использование различных служб.

Сервером Kerberos называется компьютер, на котором выполняется серверная программа Kerberos, или сама программа KDC. Клиент Kerberos — это компьютер или программа, которые получают билет от сервера Kerberos. Обычно действия системы Kerberos инициирует пользователь, отправляющий запрос на получение услуг от некоторого сервера приложения (например, сервера почты). Kerberos предоставляет билеты принципалам, в роли которых выступают пользователи или серверные программы. Для описания принципала применяется идентификатор, состоящий из трех компонентов: основы (`primary`),

экземпляра (`instance`) и области (`realm`). Данный идентификатор имеет вид:
`основа/экземпляр@область`

Система Kerberos выполняет следующие задачи:

1) обеспечение аутентификации в сети. Для предотвращения НСД к службам сервер должен иметь возможность идентифицировать пользователей. Кроме того, в некоторых средах важно, чтобы клиент мог идентифицировать серверы. Это исключит работу пользователей с фальшивыми серверами, созданными для незаконного сбора конфиденциальной информации;

2) защиту паролей. Открытость паролей, используемых в ряде сетевых служб, создает угрозу безопасности системы, т. к. они могут быть перехвачены и использованы для незаконного доступа к системе. Для решения данной проблемы используется техническое маскирование билетов Kerberos.

Технология Kerberos представляет собой механизм аутентификации пользователей и сервисов, основным достоинством которой является повышенная защищенность при использовании в сети, которая достигается механизмом защищенного обмена билетами между пользователями, сервисами и сервером учетных записей Kerberos. При данном механизме пароли пользователей по сети не передаются, что обеспечивает повышенную защищенность от сетевых атак. С помощью механизма открытых и закрытых ключей, а также синхронизации часов клиентских компьютеров с сервером Kerberos обеспечивается уникальность билетов и их защищенность от подделки.

В ОС используется реализация MIT Kerberos;

3) обеспечение однократной регистрации в сети. Система Kerberos дает возможность пользователю работать с сетевыми сервисами, пройдя лишь единожды аутентификацию на своем компьютере. При этом для обмена с приложениями дополнительно вводить пароль не требуется.

Локальные системы учетных записей пользователей и система ЕПП существуют в ОС параллельно. Различие между ними проводится с помощью разграничения диапазонов UID (значения UID меньшие, чем 2500, относятся к локальным пользователям, а большие или равные 2500 — к пользователям ЕПП).

ВНИМАНИЕ! Обязательным требованием для функционирования аутентификации по Kerberos является синхронизация времени на клиенте и сервере. Синхронизация может быть обеспечена использованием сервера NTP (см. 5.8).

6.5. Централизация хранения атрибутов СЗИ в распределенной сетевой среде

В среде ОС пользователю поставлен в соответствие ряд атрибутов, связанных с механизмами СЗИ ОС, например:

– привилегии администрирования, вхождение в группы;

– разрешенные параметры входа (список разрешенных компьютеров домена);

– политики паролей и учетных записей;

– мандатные атрибуты (диапазон доступных уровней доступа и категорий, привилегии);

– разрешенные мандатные уровни целостности;

– параметры регистрации событий (маски регистрируемых успешных и неуспешных событий).

Часть из атрибутов характерна только для ЕПП, другая — является отражением общих атрибутов СЗИ ОС. Доступ к мандатным атрибутам пользователей осуществляется с использованием программной библиотеки `parsec`. Данная библиотека получает из соответствующего конфигурационного файла информацию об источнике данных для мандатных СЗИ системы. По умолчанию используются локальные текстовые файлы. Концепция ЕПП подразумевает хранение системной информации о пользователе (в т. ч. и его мандатные атрибуты) централизованно. В этом случае вся информация хранится в службе каталогов LDAP.

6.6. Служба Astra Linux Directory

Служба ALD представляет собой систему управления ЕПП.

Она является надстройкой над технологиями LDAP, Kerberos 5, CIFS и обеспечивает автоматическую настройку всех необходимых файлов конфигурации служб, реализующих перечисленные технологии, а так же предоставляет интерфейс управления и администрирования.

Настройка окружения пользователя при входе в систему обеспечивается PAM-модулем ALD, который выполняет следующие функции:

– получение параметров окружения пользователя с сервера домена;

– проверка возможности входа пользователя на данный компьютер по списку разрешенных пользователю компьютеров;

– проверка возможности использования пользователем типа ФС его домашнего каталога;

– настройка параметров окружения пользователя;

– монтирование домашнего каталога пользователя;

– включение доменного пользователя в заданные локальные группы.

Перечисленные параметры и ограничения входа пользователя задаются с помощью соответствующих команд утилиты администрирования `ald-admin` и параметрами конфигурационного файла `/etc/ald/ald.conf` (6.6.3).

В состав ОС входит графическая утилита `fly-admin-smc`, которая позволяет администратору произвести управление ЕПП в графическом режиме (см. электронную справку).

6.6.1. Состав

Все необходимые компоненты службы ALD входят в состав пакетов, приведенных в таблице 40.

Таблица 40

Наименование	Описание
`ald-client`	Клиентская часть ALD. Содержит утилиту конфигурирования клиентского компьютера `ald-client`, PAM-модуль ALD, службу обработки заданий ALD `aldd` и утилиту автоматического обновления пользовательских билетов `ald-renew-tickets`. Пакет должен устанавливаться на все клиентские компьютеры, входящие в домен.
`ald-admin`	Пакет администрирования ALD. Содержит утилиту администрирования ALD `ald-admin`. Пакет должен устанавливаться на компьютеры, с которых будет осуществляться администрирование ALD. При установке данного пакета также устанавливается клиентская часть.
`ald-client-fs`	Расширение для организации файл-сервера ALD. Содержит необходимые подгружаемые модули для конфигурирования файл-сервера ALD и расширение команд `ald-client` `ald-client-fs`. Пакет может устанавливаться на клиентские компьютеры, выступающие в роли файл-сервера.
`ald-server-dc`	Серверная часть ALD. Содержит утилиту конфигурирования сервера `ald-init`. Пакет должен устанавливаться на сервер домена. При установке данного пакета также устанавливается, средство администрирования `ald-admin` и клиентская часть.
`ald-server`	Метапакет для установки полного сервера ALD. Пакет должен устанавливаться на сервер домена. При установке данного пакета устанавливается пакет сервера домена ALD `ald-server-dc`.

Служба ALD обладает расширяемой архитектурой, состоящей из ядра, отвечающего за основной функционал системы, ряда интерфейсов (LDAP, Kerberos, Config, RPC) и модулей расширения, предназначенных для расширения командного интерфейса утилит и настройки необходимых служб и подсистем, что позволяет расширять функциональность ALD, устанавливая дополнительные пакеты. Наименование пакета расширения отражает его назначение:

– `ald-client-...` — расширение, необходимое клиентской части ALD;

– ald-admin-... — расширение утилиты администрирования ALD;

– ald-server-... — расширение, необходимое для организации хранения атрибутов на сервере ALD.

Реализованы следующие расширения для поддержки централизации хранения атрибутов СЗИ в распределенной сетевой среде:

– ald-client-parsec — конфигурирование подсистемы хранения атрибутов СЗИ;

– ald-admin-parsec — расширение команд утилиты администрирования ald-admin;

– ald-server-parsec — расширение функциональности севера ALD для хранения атрибутов СЗИ (необходимые схемы и правила LDAP).

ВНИМАНИЕ! Без установки пакетов расширения совместно с соответствующими основными пакетами невозможна централизация хранения атрибутов СЗИ в распределенной сетевой среде, что может привести к невозможности входа пользователей в систему.

Для снижения нагрузки на сервер ALD и повышения производительности служба обработки заданий ALD aldd выполняет кэширование редко изменяемых данных ALD в локальном кэше. Расширения ALD могут обрабатывать события службы кэширования для выполнения необходимых операций для обновления локального кэша.

ВНИМАНИЕ! Измененная на сервере информация может попасть в локальный кэш с задержкой. Период обновления локального кэша задается параметром CACHE_REFRESH_PERIOD в конфигурационном файле /etc/ald/ald.conf (6.6.3).

Описание пакетов и возможностей указанных утилит приведено в руководстве man (список статей см. в таблице 41).

Таблица 41

Наименование	Описание
ald 7	ALD
ald-client 8	Клиентская часть ALD и команды утилиты управления клиентом ALD ald-client
ald-admin 1	Команды утилиты администрирования ALD ald-admin
ald-init 8	Команды утилиты управления сервером домена ald-init
aldd 8	Служба обработки заданий ALD aldd
pam_ald 8	PAM-модуль ALD
ald-renew-tickets 1	Утилита автоматического обновления пользовательских билетов ald-renew-tickets
ald.conf 5	Формат конфигурационного файла ald.conf
ald-client-fs 8	Расширение для организации файл-сервера ALD

Окончание таблицы 41

Наименование	Описание
`ald-parsec-cfg 7`	Расширение конфигурирования подсистемы хранения атрибутов СЗИ
`ald-parsec-aud 7` `ald-admin-parsec-aud 1`	Расширение централизации настроек расширенного аудита
`ald-parsec-devac 7` `ald-admin-parsec-devac 1`	Расширение для подсистемы контроля доступа к подключаемым носителям

`ald-parsec-mac 7`
`ald-admin-parsec-mac 1`
`pam_ald_mac 8`
	Расширение централизации хранения атрибутов СЗИ

6.6.2. Установка

Установка службы ALD может осуществляться как при начальной установке ОС путем выбора соответствующих пунктов в программе установки, так и в ручном режиме уже в работающей системе.

ВНИМАНИЕ! В случае установки сервера ALD в ручном режиме возможно получения следующей ошибки установки:

```
insserv: Service nfs-common has to be enabled to start service nfs-kernel-server
insserv: exiting now!
update-rc.d: error: insserv rejected the script header
```

Данная ошибка вызвана тем, что в соответствии с политикой ОС по минимизации сетевых уязвимостей, большинство сетевых сервисов и служб по умолчанию выключены. Для успешной установки сервера ALD необходимо вручную включить необходимую службу:

```
chkconfig nfs-common on
```

ВНИМАНИЕ! Без установки пакетов расширения совместно с соответствующими основными пакетами невозможна централизация хранения атрибутов СЗИ в распределенной сетевой среде, что может привести к невозможности входа пользователей в систему.

Для облегчения установки службы ALD на конкретный компьютер предназначены метапакеты, обеспечивающие установку всех необходимых пакетов в зависимости от назначения данного компьютера:

– `ald-client-common` — установка клиентской части ALD;

– `ald-admin-common` — установка утилиты администрирования БД ALD;

– `ald-server-common` — установка сервера домена ALD.

При раздельной установке расширений ALD на сервере необходимо после установки выполнить операции инициализации расширений командой

```
ald-init install-ext
```

которая произведет необходимые настройки и изменения существующей БД ALD. При инициализации БД ALD при установленных пакетах расширения данные действия осуществ-

ляются автоматически.

6.6.3. Настройка

Настройка всех компонентов ALD осуществляется автоматически утилитами конфигурирования. Для нормального функционирования ALD необходимо выполнение следующих условий:

1) разрешение имен должно быть настроено таким образом, чтобы имя системы разрешалось, в первую очередь, как полное имя (например, `myserver.example.ru`).

Утилита `hostname` должна возвращать короткое имя компьютера, например, `myserver`.

Пример файла `/etc/hosts` (разрешение имен может быть настроено и с помощью сервера DNS (см. 5.5)):

```
127.0.0.1       localhost
192.168.1.1     myserver.example.ru myserver
```

2) должна быть выполнена синхронизация времени в ОС серверов и клиентов ALD для аутентификации по Kerberos. Например, с использованием сервера NTP (см. 5.8).

Настройки сервера и клиентов ALD содержатся в файле `/etc/ald/ald.conf`. Формат файла:

```
ИМЯ_ПАРАМЕТРА=значение # Комментарий
```

Описание параметров конфигурационного файла приведены в таблице 42.

По завершении первичной настройки конфигурационного файла сервера для инициализации домена необходимо выполнить команду:

```
ald-init init
```

Подробнее о создании домена см. 6.9.1.

Для ввода нового компьютера в домен после первичной настройки конфигурационного файла на клиенте необходимо выполнить команду:

```
ald-client start
```

Примечание. Для удобства ввод нового компьютера в домен может быть выполнен командой `ald-client join <имя сервера домена>`. В этом случае конфигурационный файл будет настроен автоматически.

В случае изменения конфигурационного файла `/etc/ald/ald.conf` необходимо выполнить команду `commit-config` для того, чтобы изменения вступили в силу:

```
ald-init commit-config
```

на сервере и

```
ald-client commit-config
```

на клиентах.

Таблица 42 – Параметры конфигурационного файла /etc/ald/ald.conf

Параметр	Описание
VERSION	Для текущей версии должно быть установлено значение «1.7». Значения версии «1.5», «1.4» может быть установлено для совместимости с предыдущими версиями
DOMAIN	Имя домена. Должно быть задано в формате .example.ru для сервера ALD. Если данный параметр меняется, то необходимо заново инициализировать сервер командой: ald-init init Можно также воспользоваться командами резервного копирования и восстановления для переименования домена.
SERVER	Полное имя серверного компьютера ALD. Например: my-server.example.ru
MINIMUM_UID	Минимальный номер глобального пользователя. Пользователи с номером меньше данного считаются локальными и аутентифицируются через локальные файлы /etc/passwd и /etc/shadow. Примечание. Для нормальной работы домена не рекомендуется пересечение по номерам локальных и глобальных пользователей и групп. Не рекомендуется задавать MINIMUM_UID меньше 1000
DEFAULT_LOGIN_SHELL	Командная оболочка, которая устанавливается при создании нового пользователя. Применяется при администрировании с данного компьютера. По умолчанию используется /bin/bash
DEFAULT_LOCAL_GROUPS	Перечень локальных групп, членство в которых устанавливается при создании нового пользователя. Применяется при администрировании с данного компьютера. При входе в домен пользователю будет добавляться членство в указанных группах для использования тех или иных возможностей компьютера, например воспроизведение звука
ALLOWED_LOCAL_GROUPS	Перечень разрешенных локальных групп, членство в которых устанавливается при входе пользователя. Применяется для данного компьютера. При входе в домен пользователю будет добавляться членство в установленных для него локальных группах в пределах разрешенных на данном компьютере.

Продолжение таблицы 42

Параметр	Описание
TICKET_MAX_LIFE=10h	Максимальное время жизни билета Kerberos (если его не обновлять). Формат параметра: NNd (дни), или NNh (часы), или NNm (минуты). При входе в домен пользователь получает билет. При выходе из домена билет уничтожается. Если билет не обновлять, то после истечения срока действия билета пользователь потеряет доступ к своему домашнему каталогу. Чтобы восстановить доступ, ему придется выполнить команду kinit или зайти в систему заново. Чтобы доступ не был потерян, билет следует периодически обновлять (до истечения срока действия). Настроить автоматическое обновление можно с помощью утилиты ald-renew-ticket. Для удобства можно настроить данный параметр на большое количество времени, например 30d. Но это менее безопасно
TICKET_MAX_RENEWABLE_ LIFE=7d	Максимальное обновляемое время жизни билета Kerberos. Формат параметра: NNd (дни), или NNh (часы), или NNm (минуты). По истечении данного срока билет не может быть обновлен. Данный параметр должен быть больше, чем параметр TICKET_MAX_LIFE. Примечание. Для клиентских компьютеров параметры TICKET_MAX_LIFE и TICKET_MAX_RENEWABLE_LIFE определяются как наименьшие значения этих параметров, заданных в файлах ald.conf на сервере и на клиентском компьютере
NETWORK_FS_TYPE	Определяет, какая сетевая ФС будет использоваться для глобальных пользовательских домашних каталогов. Возможные значения: – none — сетевая ФС не используется. Работает только аутентификация глобальных пользователей. Используются локальные домашние каталоги пользователей (следующие параметры, относящиеся к сетевой ФС, игнорируются); – cifs — используется Samba/CIFS
SERVER_EXPORT_DIR	Только для сервера. Задает абсолютный путь к каталогу на сервере, где будет располагаться хранилище домашних каталогов. Данный каталог будет экспортирован по Samba/CIFS
CLIENT_MOUNT_DIR	Задает абсолютный путь к точке монтирования хранилища домашних каталогов на клиентских компьютерах
SERVER_FS_KRB_MODES	Только для сервера. Задает режимы экспорта сервера Samba/CIFS (перечисленные через запятую). Возможные режимы: – krb5 — только Kerberos-аутентификация; – krb5i — (integrity) аутентификация и проверка целостности (подпись) пакетов. Должен быть указан хотя бы один режим
CLIENT_FS_KRB_MODE	Задает Kerberos-режим монтирования на клиентском компьютере. Должен быть указан один из режимов: krb5 или krb5i

Окончание таблицы 42

Параметр	Описание
SERVER_POLLING_PERIOD	Только для сервера. Задает период (в секундах) опроса заданий службой aldd. По умолчанию составляет 60 с
SERVER_PROPAGATE_PERIOD	Только для сервера. Задает период (в секундах) репликации БД ALD на резервные сервера. По умолчанию составляет 600 с
CACHE_REFRESH_PERIOD	Задает период (в секундах) обновления локального кэша службой aldcd. По умолчанию составляет 600 с
UTF8_GECOS	Только для сервера. Задает признак модификации схемы LDAP для возможности использования кириллицы в поле описания GECOS пользователя. По умолчанию установлен равным 1
USE_RPC	Разрешает администрирование с помощью RPC интерфейса. По умолчанию установлен равным 1
RPC_PORT	Порт RPC интерфейса. По умолчанию установлен равным 17302
RPC_RESTRICTED	Список запрещенных к исполнению RPC команд.
SERVER_ON	Отображает состояние сервера ALD (устаревшее). Возможные значения 0 и 1. Если SERVER_ON=0, то: – домашние каталоги не экспортируются; – разрешение имен по LDAP выключается в nsswitch.conf; – все принципалы Kerberos деактивируются (allow_tickets=0); – службы LDAP, Samba, Kerberos, nss-ldapd останавливаются; – служба nscd перезапускается. В настоящее время состояние ALD может быть получено командой status утилит ald-client, ald-init и ald-admin
CLIENT_ON	Отображает состояние клиентской части ALD (устаревшее). Возможные значения 0 и 1. Если CLIENT_ON=0, то: – домашние каталоги не монтируются; – разрешение имен по LDAP выключается в nsswitch.conf; – служба nscd перезапускается. В настоящее время состояние ALD может быть получено командой status утилит ald-client, ald-init и ald-admin

Пример файла /etc/ald/ald.conf:

```
VERSION=1.7
DOMAIN=.example.ru
SERVER=my-server.example.ru
MINIMUM_UID=2500
DEFAULT_LOGIN_SHELL=/bin/bash
DEFAULT_LOCAL_GROUPS=users,audio,video,scanner
ALLOWED_LOCAL_GROUPS=users,audio,video,scanner
TICKET_MAX_LIFE=10h
```

```
TICKET_MAX_RENEWABLE_LIFE=7d
NETWORK_FS_TYPE=cifs
SERVER_EXPORT_DIR=/ald_export_home
CLIENT_MOUNT_DIR=/ald_home
SERVER_FS_KRB_MODES=krb5,krb5i
CLIENT_FS_KRB_MODE=krb5i
SERVER_POLLING_PERIOD=60
SERVER_PROPAGATE_PERIOD=600
CACHE_REFRESH_PERIOD=600
UTF8_GECOS=1
SERVER_ON=1
CLIENT_ON=1
```

6.7. Шаблоны конфигурационных файлов

Служба ALD в процессе своей работы осуществляет конфигурирование необходимых сетевых служб (Samba, Kerberos, LDAP и т.п.) с помощью их конфигурационных файлов. Для удобства существуют шаблоны модифицируемых службой ALD конфигурационных файлов, расположенные в каталоге `/etc/ald/config-templates`.

ВНИМАНИЕ! При установке, инициализации, удалении или запуске/остановке службы ALD основные конфигурационные файлы различных служб могут быть перезаписаны на основе шаблонов, что может повлечь потерю внесенных вручную изменений.

Примечание. При необходимости дополнительной настройки служб внесение изменений должно осуществляться не только в основные конфигурационные файлы, но и в их шаблоны.

Состав шаблонов конфигурационных файлов приведен в табл 43.

Таблица 43

Шаблон	Служба	Описание
`ald-pam-profile`	`pam-auth-update`	шаблон PAM
`ald*.ldif`	OpenLDAP	LDAP схемы ALD
`base-init.ldif`	OpenLDAP	LDAP скрипт начальной инициализации БД ALD
`exim-mail.ldif`	OpenLDAP	LDAP схема для Exim
`idmapd.conf`	NFS	`/etc/idmapd.conf`
`kadm5.acl`	Kerberos admin server	`/etc/krb5kdc/kadm5.acl`
`kdc.conf`	Kerberos KDC	`/etc/krb5kdc/kdc.conf`
`kpropd.conf`	Kerberos	`/etc/krb5kdc/kpropd.conf`
`krb5.conf`	Kerberos клиенты	`/etc/krb5.conf`

Окончание таблицы 43

Шаблон	Служба	Описание
ldap.conf	LDAP клиенты	/etc/ldap/ldap.conf
mldap.conf	PARSEC	/etc/parsec/mldap.conf
nslcd.conf	NSLCD	/etc/nslcd.conf
sasl2_slapd.conf	OpenLDAP	описание для SASL2
slapd.d17.ldif	OpenLDAP	LDAP скрипт начальной инициализации LDAP сервера
smb.conf	Samba	/etc/samba/smb.conf

ВНИМАНИЕ! При ручной правке шаблонов конфигурационных файлов не рекомендуется удалять или менять строки, изначально содержащиеся в шаблоне или содержащие параметризованные значения.

ВНИМАНИЕ! При переустановке ALD или выполнении команд ALD install-config шаблоны в /etc/ald/config-templates будут перезаписаны из /usr/lib/ald/config-templates.

6.7.1. Конфигурационные файлы LDAP

К конфигурационным файлам LDAP относятся схемы LDAP и скрипты инициализации сервера LDAP и БД ALD.

Примечание. Скрипты инициализации используются только в процессе создания БД ALD.

При необходимости регистрации дополнительных LDAP схем, необходимо поместить требуемую схему в каталог /etc/ldap/schema и добавить ее включение в шаблон slapd.d17.ldif по аналогии с остальными.

При необходимости дополнительного начального заполнения БД ALD возможна правка шаблона base-init.ldif.

6.7.2. Конфигурационные файлы Kerberos

К конфигурационным файлам Kerberos относятся специальные конфигурационные файлы служб севера Kerberos и конфигурационный файл /etc/krb5.conf, содержащий основные настройки домена.

Важной характеристикой является алгоритм защиты аутентификационной информации (supported_enctypes в /etc/krb5kdc/kdc.conf и default_tgs_enctypes, default_tkt_enctypes, permitted_enctypes в /etc/krb5.conf).

Список используемых алгоритмов защиты аутентификационной информации приведен в табл 44.

Таблица 44

Тип шифрования	Назначение
gost-cts	отечественные алгоритмы по ГОСТ 28147-89 и ГОСТ Р 34.11-2012, применяется по умолчанию в ALD
aes256-cts	применяется по умолчанию в Kerberos
des-cbc-crc	слабый устаревший, применяется для поддержки NFS, и не рекомендуется к использованию
rc4-hmac	применяется для поддержки работы клиентов Samba, так как являлся основным в Windows

В случае отсутствия необходимости использования NFS или утилит Samba (smbclient) — типы шифрования des-cbc-crc и rc4-hmac могут не указываться.

Примечание. Для работы с NFS так же необходима установка параметра allow_weak_crypto в файле /etc/krb5.conf, что снижает надежность аутентификации.

ВНИМАНИЕ! Использование NFS не рекомендуется!

6.7.3. Конфигурационные файлы Samba

Конфигурационный файл /etc/smb.conf содержит описание глобальных настроек и разделяемых ресурсов.

Средства Samba используются в рамках ALD только для централизованного хранения домашних каталогов пользователей. Существует возможность использования других сетевых разделяемых файловых ресурсов путем описания их конфигурационном файле smb.conf согласно руководству man на smb.conf.

ВНИМАНИЕ! Возможности по созданию разделяемых ресурсов для сетевой печати не используются, так как не обеспечивают необходимой защиты выводимой информации.

Существует возможность работы с разделяемыми ресурсами с помощью стандартных утилит Samba (net, smbclient), в том числе с пользовательскими разделяемыми ресурсами (usershare). Для этого необходима поддержка сервером Kerberos типа шифрования ключей rc4-hmac (см. 6.7.2).

Примечание. В случае необходимости предоставления доступа к разделяемым файловым ресурсам пользователям другого домена (см.6.9.8) следует установить значение параметра allow trusted domains = yes.

6.7.4. Распространение конфигурационных файлов в домене

Существует возможность распространения конфигурационных файлов в домене. Для этого предназначены команды вида ald-admin doc-* (описание команд приведено в руководстве man ald-admin).

С помощью команды `ald-admin doc-add` подготовленный конфигурационный файл передается на сервер, где сохраняется в каталоге `/var/lib/ald/documents`. В команде с помощью опций `--location` и `--file` указываются путь целевого размещения файла на компьютерах домена и путь к загружаемому файлу соответственно.

Службы обработки заданий `aldd` компьютеров сети выполняют обновление указанного конфигурационного файла по указанному при создании пути (должен быть доступен на запись). При этом проверяется время модификации файла. Если время модификации целевого файла новее, перезапись доменной версией не производится.

ВНИМАНИЕ! Механизм должен использоваться с особой осторожностью, поскольку выполняет перезапись локальных конфигурационных файлов версиями с сервера. При этом создаются резервные копии предыдущих версий.

6.8. Сценарии сессии пользователя

Astra Linux Directory содержит средства выполнения дополнительных действий при создании новой сессии пользователя или ее завершения в случае работы пользователя в ЕПП.

Для этих целей PAM модуль ALD при создании и завершении сессии пользователя ЕПП исполняет следующие сценарии:

– `/etc/ald/ald.session` — скрипт исполняющий от имени суперпользователя дополнительные скрипты из каталога `/etc/ald/ald.session.d` во время создания сессии пользователя после монтирования домашнего каталога;

– `/etc/ald/ald.reset` — скрипт исполняющий от имени суперпользователя дополнительные скрипты из каталога `/etc/ald/ald.reset.d` во время завершения сессии пользователя до размонтирования домашнего каталога.

Примечание. Могут существовать и другие каталоги дополнительных скриптов, например `/etc/ald/ald.mac.session.d`, `/etc/ald/ald.mac.reset.d` для дополнительных этапов работы сессии пользователя.

Рассматриваемый механизм удобен для организации выполнения дополнительных действий при создании и завершении сессии пользователя. Например, одним из обязательных условий работы с домашними каталогами на сетевых ФС является обеспечение корректного их размонтирования. Помешать этому могут процессы, запущенные и не завершившиеся во время работы сессии пользователя и удерживающие открытые файлы в домашнем каталоге.

В случае возникновения подобной ситуации, следует определить такие процессы с помощью утилит `fuser` или `lsof`, в качестве аргументов которым передается путь к домашнему каталогу пользователя вида `/ald_home/имя_пользователя` и путь к точке монтирования вида `/run/ald.mounts/имя_пользователя`, например:

```
fuser /ald_home/user1
fuser /run/ald.mounts/user1
lsof /ald_home/user1
lsof /run/ald.mounts/user1
```

После этого, необходимо завершить определенные таким образом процессы. Данная последовательность действий должна быть оформлена в виде скрипта, расположенного в каталоге `/etc/ald/ald.reset.d`, что позволит обеспечить его выполнение во время завершения сессии пользователя.

Примечание. Настоящий скрипт может быть более интеллектуальным для учета различный свойств процессов или причин их появления.

ВНИМАНИЕ! Поскольку действия выполняются от имени суперпользователя, к разработке подобных сценариев необходимо подходить с особой осторожностью.

6.9. Администрирование домена

С помощью утилит администрирования ALD существует возможность выполнения следующих административных действий:

– создание нового домена;

– резервирование/восстановление конфигурации домена;

– контроль целостности конфигурации домена;

– добавление/удаление компьютеров в домен;

– управление учетными записями пользователей домена;

– управление учетными записями сетевых служб домена;

– управление атрибутами СЗИ.

Примечание. Расширения ALD могут изменять состав административных действий и комад утилит администрирования.

Утилиты администрирования могут быть запущены в пакетном режиме для массового выполнения операций. При этом, как правило, используется опция `--force`.

Примечание. При использовании опции `--force` необходимые для выполнения пароли администратора и пользователей должны быть переданы утилите с помощью файла паролей.

Операции по администрированию должны выполняться пользователями, обладающими определенными административными полномочиями. В зависимости от назначенных привилегий пользователей ALD можно разделить на следующие группы по полномочиям:

– корневой администратор `admin/admin` — корневой администратор домена. Обладает всеми полномочиями по управлению доменом;

– администраторы — пользователи с привилегией `admin`. Обладают полномочиями по управлению конфигурацией домена и учетными записями;

– ограниченные администраторы — пользователи с привилегиями `hosts-add` или `all-hosts-add`. Обладают полномочиями по добавлению компьютеров в домен;

– пользователи утилит администрирования — пользователи с привилегией `adm-user`. Обладают полномочиями по запуску утилит администрирования (используется пакетами расширения для детализации полномочий управления);

– обычные пользователи.

ВНИМАНИЕ! Расширения ALD могут привносить свое деление полномочий. Например, пакет `ald-admin-parsec` содержит набор команд управления мандатными атрибутами. При этом предусмотрена соответствующая группа администраторов МАС. Для возможности управления мандатными атрибутами конкретным пользователем ему должна быть предоставлена привилегия `adm-user` и он должен быть добавлен в группу командой `macadmin-add`.

6.9.1. Управление конфигурацией домена

Создание нового домена, а так же его резервирование/восстановление осуществляются с помощью утилиты управления сервером домена `ald-init`.

Перед созданием домена на контроллере домена должны быть установлены все требуемые пакеты серверных расширений, в этом случае конфигурация нового домена будет автоматически создана с их поддержкой. Так же корректным образом должны быть настроены система разрешения имен и конфигурационный файл `ald.conf` (см. 6.6.3).

В случае указания необходимости сервера ЕПП при начальной установке ОС с диска конфигурационный файл `ald.conf`, как правило, уже содержит корректные значения домена и имени сервера.

Создание или пересоздание домена осуществляется командой `init` утилиты управления сервером домена `ald-init`.

При необходимости может выполняться сохранение резервной копии конфигурации домена командами с префиксом `backup` утилиты управления сервером домена `ald-init`. Восстановление ранее сохраненных резервных копий осуществляется соответствующими командами с префиксом `restore-backup` утилиты управления сервером домена `ald-init` (см.6.9.7).

При возникновении в процессе работы сообщений об ошибках или некорректной работе механизмов ЕПП следует воспользоваться командой `test-integrity` утилиты администрирования `ald-admin` для проверки внутренней целостности конфигурации домена, что включает в себя проверку состояния и согласованности всех сущностей ALD. В ходе проверки может быть локализована причина ошибок и сбоев, что облегчит их устранение (см. 6.10).

6.9.2. Использование RPC интефейса

Штатным режимом работы ALD является управление доменом с помощью службы обработки заданий ALD `aldd` сервера с помощью RPC интерфейса.

Утилита `ald-admin` по умолчанию работает в интерактивном режиме с запросом пароля администратора. Также пароли администратора и пользователей могут быть переданы с помощью файла паролей.

Для доменных пользователей возможно выполнение утилиты с использованием существующей аутентификационной информации пользователя (при наличии у него привилегий администрирования домена). При этом указывается опция командной строки `-c`.

ВНИМАНИЕ! Для корректной работы RPC интерфейса, билеты Kerberos пользователей должны обладать свойством `forwardable`. Для домена ALD свойство `forwardable` используется по умолчанию. При получении билетов утилитой `kinit` следует использовать опцию `-f`. В противном случае выдается ошибка вида: «Ошибка подготовки сообщения KRB-CRED».

Существует ряд специальных RPC команд, применяемых к любому компьютеру домена ALD (в качестве аргумента команды может указываться имя компьютера):

– `rpc-status` — получение информации о роли компьютера в домене;

– `rpc-statistics` — получение статистической информации о RPC сервере `aldd` указанного компьютера;

– `rpc-execute` — выполнение указанного команды на удаленном компьютере (команда выполняется от имени инициировавшего запрос пользователя домена).

Описание команд может быть получено с помощью встроенной команды помощи `help`.

Примечание. Список RPC команд сервера может быть получен с помощью команды `rpc-statistics` с опцией `--commands`.

ВНИМАНИЕ! Существует возможность запрета исполнения выбранных RPC указанием параметра `RPC_RESTRICTED` в конфигурационном файле `/etc/ald.conf` конкретного компьютера.

6.9.3. Управление учетными записями

В ЕПП различаются учетные записи пользователей домена, учетные записи компьютеров домена и учетные записи сетевых служб, работающих в среде ЕПП.

Учетная запись пользователя домена содержит всю необходимую информацию о пользователе ЕПП, включая в себя: соответствующий принципал Kerberos, политику паролей, свойства, необходимые для входа пользователя в систему, настройки подключения домашнего каталога, привилегии пользователя ЕПП и его атрибуты СЗИ.

Привилегии ALD и указанные ограничения могут быть установлены для учетной

записи с помощью команды `user-ald-cap` утилиты администрирования `ald-admin`.

Также учетная запись пользователя может содержать ограничения по входу в домен. В качестве ограничений используется список компьютеров, на которых он может осуществлять вход, и признак временной блокировки.

ВНИМАНИЕ! После создания новой учетной записи список разрешенных для входа компьютеров пуст: пользователь не имеет права входа в систему. Список компьютеров, с которых ему будет разрешен вход, должен быть явно указан после создания учетной записи.

Учетная запись пользователя может обладать административными привилегиями или входить в группы администраторов, заданные расширениями ALD.

ВНИМАНИЕ! Удаление учетной записи пользователя может быть выполнено только администратором, обладающим доступом ко всем его атрибутам (входящим во все необходимые группы администраторов).

ВНИМАНИЕ! Существует некоторое время для распространения информации о создании или удаления пользователя. Это связано с механизмами кеширования NSS. При пересоздании пользователя с тем же именем могут возникать ошибки (например: входа в систему, монтирования домашнего каталога и т.п.) из-за выдачи на удаленных системах устаревшего идентификатора пользователя.

Учетная запись компьютера домена представляет собой набор принципалов Kerberos для функционирования компьютера в домене.

Ввод нового компьютера в домен осуществляется с помощью запущенной на нем утилиты `ald-client` командой `commit-config` (возможно с параметрами). При этом пользователь должен обладать полномочиями по добавлению компьютера в домен.

Примечание. Для удобства ввод нового компьютера в домен может быть выполнен командой `ald-client join <имя сервера домена>`. В этом случае конфигурационный файл будет настроен автоматически. Также автоматически будет создана учетная запись компьютера в домене.

С помощью утилиты `ald-admin` учетной записи компьютера может быть добавлено описание или она может быть удалена.

Учетная запись службы домена представляет собой принципал Kerberos для функционирования службы в домене.

ВНИМАНИЕ! Каждая служба, поддерживающая сквозную аутентификацию Kerberos, должна обладать принципалом Kerberos, т. е. быть зарегистрированной в домене. После регистрации в домене набор ключей службы должен быть выгружен в файл, указанный в ее конфигурации.

В ALD для предоставления службам определенных полномочий по получению ин-

формации из домена используется объединение служб в группы сервисов. Например, для получения мандатных атрибутов пользователей служба должна входить в группу сервисов `mac`.

Для облегчения конфигурирования сетевых служб, работающих в среде ЕПП, предусмотрены команды управления учетными записями служб утилиты `ald-admin` и команды выгрузки ключей утилиты `ald-client`.

Указанные команды имеют префиксы `service-` и `svc-`.

ВНИМАНИЕ! В случае добавления компьютера в домен, пересоздания домена или принципалов служб может потребоваться удаление файлов типа `krb5.keytab`, содержащих выгруженные ранее ключи.

Детальное описание команд приведено в руководстве `man`. Настройка некоторых сетевых служб приведена в 6.11.

6.9.4. Ограничения по выборке данных из LDAP

Существуют ограничения по получению данных от службы каталогов LDAP. По умолчанию разрешается получать не более 500 записей.

ВНИМАНИЕ! Возможны нарушения работы ЕПП в случае превышения числа пользователей или компьютеров этого значения.

Для гибкого управления ограничениями предусмотрены команды утилиты `ald-admin`: `ldap-limits` для просмотра и `ldap-setlimit` для установки.

Службы каталогов LDAP поддерживает ограничения для различных пользователей или групп пользователей по размеру и времени выполнения выборки. При этом существуют мягкие ограничения, применяемые по умолчанию и которые могут быть превышены заданием параметров выборки в прикладном ПО, и жесткие, которые не могут быть превышены.

Команда установки ограничений имеет следующий синтаксис:

```
ald-admin ldap-setlimit <кому> <вид ограничения>
```

где видами ограничения могут быть:

– `size=число` — единое задание мягкого и жесткого ограничении по размеру выборки;

– `size.soft=число` — задание мягкого ограничения по размеру выборки;

– `size.hard=число` — задание жесткого ограничения по размеру выборки;

– `time=секунды` — единое задание мягкого и жесткого ограничении по времени выполнения выборки;

– `time.soft=секунды` — задание мягкого ограничения по времени выполнения выборки;

– `time.hard=секунды` — задание жесткого ограничения по времени выполнения

выборки.

В качестве аргумента команды <кому> могут выступать следующие значения:

– * — все, включая анонимных и аутентифицированных пользователей;

– anonymous — анонимные пользователи;

– users — аутентифицированные пользователи;

– self — ассоциированный с целью пользователь;

– dn... — варианты синтаксиса DN;

– group... — варианты синтаксиса групп.

Примечание. Перед установкой ограничений LDAP рекомендуется ознакомиться с доступной документацией по работе служб каталогов LDAP.

Подробное описание команд работы с ограничениями LDAP приведены в руководстве man ald-admin.

6.9.5. Регистрация действий администратора и протоколирование

При работе компоненты ALD ведут журналы своей работы. В журналах фиксируются информация о выполняемых действиях и ошибках. При этом фиксируется дата и время возникновения события, тип события и имя исполняемого модуля с указанием идентификатора процесса.

Доступны следующие журналы работы:

– ~./ald/ald-admin.log

– ~./ald/ald-init.log

– ~./ald/ald-client.log — журналы работы утилит ald-admin, ald-init, ald-client соответственно. Располагаются в домашнем каталоге пользователя, который запускал их на исполнение.

– /var/log/ald/aldd.log — журнал работы службы обработки заданий ALD aldd.

Способ вывода журналов, их размещение и детализация могут быть заданы для каждой из утилит или служб при их запуске с помощью следующих параметров командной строки:

Таблица 45

Параметр	Описание
--log-dest=способы	задает способ журнализации, где аргумент принимается как набор разрядов: – 1 (0x1) — stderr; – 2 (0x2) — syslog; – 3 (0x4) — csvlog. По умолчанию для утилит используется stderr+csvlog, а для служб syslog+csvlog.

Окончание таблицы 45

Параметр	Описание
`--log-file=путь`	задает путь к файлу журнала (в случае использования способа `csvlog`).
`--log-level=уровень`	задает детализацию журнала: – 0 - ошибки; – 1 - предупреждения; – 2 - уведомления; – 3 - информация; – 4 - отладка.

Регистрация действий администратора по управлению доменом осуществляется централизовано на сервере домена. При этом по умолчанию вывод информации осуществляется в следующие файлы:

– `/var/log/ald/aldlog.log` — журнал регистрации изменений шаблонов протоколирования;

– `/var/log/ald/audit.log` — журнал регистрации согласно настроенным шаблонам протоколирования.

Примечание. В случае необходимости может быть настроена переадресация журналов регистрации действий администратора в системный журнал `syslog` с помощью конфигурационного файла следующего вида, размещаемого в каталоге `/etc/rsyslog.d/`:

```
$ModLoad imfile
$InputFileName /var/log/ald/audit.log
$InputFileTag ald_audit
$InputFileStateFile stat_ald_audit
$InputFileSeverity notice
$InputFilePollInterval 1
$InputRunFileMonitor
```

Управление регистрацией действий администратора производится с помощью команд вида `'ald-admin logging-*'`, которые позволяют изменять путь к файлу регистрации событий (журнал регистрации изменений шаблонов протоколирования имеет фиксированное расположение), создавать или изменять шаблоны протоколирования.

Шаблон протоколирования состоит из имени, ldap-суффикса и режима протоколирования:

– `all` — регистрация всех событий;

– `succ` — регистрация успешных событий;

– `fail` — регистрация неуспешных событий;

– `none` — отключение регистраций событий.

ВНИМАНИЕ! Не рекомендуется без особой необходимости добавлять или изменять суффиксы шаблонов протоколирования.

6.9.6. Домашние каталоги и особенности монтирования сетевых ФС

Централизация хранения информации об окружении пользователей подразумевает и централизованное хранение домашних каталогов пользователей. Для этого используется СЗФС CIFS (см. 5.9).

Для хранения домашних каталогов, содержащих незащищенные данные, могут быть использованы и другие сетевые ФС (например, NFS4). ALD в настоящее время поддерживает автоматическое монтирование только СЗФС CIFS и NFS4. Так же для хранения домашних каталогов пользователя может быть использована и локальная ФС компьютера.

Учетная запись пользователя ALD содержит информацию о типе ФС домашнего каталога пользователя и его расположении (сервер домашних каталогов для сетевых ФС и путь к каталогу для локальных ФС). По умолчанию в качестве типа ФС используется СЗФС CIFS, а в качестве расположения — контроллер домена.

Примечание. Особенность организации домашних каталогов пользователя включает в себя обеспечение возможности перехода пользователя к своим каталогам с другой мандатной меткой с помощью ссылки `mac`. Использование таких ссылок в samba по умолчанию запрещено. Для разрешения этой возможности используется глобальный параметр `allow insecure wide links` в шаблоне конфигурационного файла samba (см.6.7.3).

Пакет расширения `ald-client-fs` позволяет на любом компьютере домена развернуть сервер домашних каталогов, который впоследствии можно будет указать как расположение домашних каталогов. Регистрация, запуск и останов сервера осуществляется с помощью расширения командного интерфейса утилиты управления клиентом `ald-client`.

ВНИМАНИЕ! Существует возможность изменения сервера расположения домашнего каталога пользователя. В этом случае домашний каталог пользователя должен быть физически перемещен со старого сервера на новый, в противном случае пользователь не сможет войти в систему. Такая же ситуация может произойти при замене основного сервера резервным.

Монтирование домашних каталогов выполняется PAM-модулем ALD автоматически при входе пользователя. При этом могут проверяться ограничения на тип ФС домашнего каталога пользователя.

ВНИМАНИЕ! Существует некоторое время для распространения информации о создании или удаления пользователя. Это связано с механизмами кеширования NSS. При пересоздании пользователя с тем же именем могут возникать ошибки (например: входа в

систему, монтирования домашнего каталога и т.п.) из-за выдачи на удаленных системах устаревшего идентификатора пользователя. При возникновении таких ошибок следует перезапустить на используемых компьютерах службы `nscd`, `nslcd`, и обеспечить корректные значения прав доступа к каталогу пользователя на сервере домашних каталогов.

ВНИМАНИЕ! Для корректной работы с монтированием домашних каталогов необходимо обеспечить освобождение точек монтирования при завершении сессии пользователя (см.6.8).

Существует возможность на серверах домашних каталогов (файл-серверах) заводить общие папки, доступные для пользователей. Для конфигурирования файл-сервера следует руководствоваться документацией и справкой по используемой ФС. Монтирование таких каталогов может быть выполнено при помощи команды `mount` или редактированием конфигурационного файла `fstab`. Автоматическое монтирование может быть обеспечено PAM-модулем `pam_mount`.

Примечание. При необходимости работы с разделяемыми ресурсами с помощью стандартных утилит Samba (`net`, `smbclient`), в том числе с пользовательскими разделяемыми ресурсами (`usershare`), могут требоваться дополнительные настройки (см. 6.7.3).

6.9.7. Создание резервных копий и восстановление

В целях уменьшения времени на восстановление работоспособности сервера в случае возникновения программно-аппаратных сбоев предусмотрено создание резервной копии баз данных сервера домена.

Резервирование/восстановление домена осуществляются с помощью утилиты управления сервером домена `ald-init`.

ВНИМАНИЕ! Программная конфигурация ALD сервера, на котором будет выполнятся восстановление, должна точно соответствовать той, при которой выполнялось создание резервной копии. Должны быть установлены все требуемые пакеты серверных расширений ALD. Так же корректным образом должна быть настроены система разрешения имен (см. 6.6.3).

Существует несколько вариантов создания резервной копии следующими командами утилиты управления сервером ALD `ald-init`:

– `backup` — создание физической копии контроллера домена: в этом случае в подкаталоге `.ald` домашнего каталога пользователя, выполняющего операцию, создаются два архива `ald-base.tar.gz` и `ald-keys.tar.gz`, содержащие архив фрагментов ФС сервера с информационными БД и БД ключевой информации соответственно. Данный вариант является единственным, при котором сохраняется ключевая информация и пароли пользователей.

– backup-ldif — создание логической копии LDAP БД контроллера домена: в этом случае в подкаталоге .ald домашнего каталога пользователя, выполняющего операцию, создается LDIF файл БД LDAP контроллера домена с именем по умолчанию вида ald.{имя домена}.ldif.

– backup-portable — создание логической копии БД контроллера домена в переносимом текстовом формате: в этом случае в подкаталоге .ald домашнего каталога пользователя, выполняющего операцию, создается текстовый файл с именем по умолчанию вида ald.{имя домена}.pbk.gz.

Примечание. Для восстановления перечисленных вариантов резервных копий используются команды утилиты управления сервером ALD ald-init restore-backup, restore-backup-ldif и restore-backup-portable соответственно. При этом пересоздаются базы данных LDAP и Kerberos.

ВНИМАНИЕ! При использовании вариантов создания логической копии командами backup-ldif и backup-portable ключевая информация и пароли пользователей не сохраняются. После восстановления требуется назначение новых паролей пользователей, перевключение рабочих станций в домен и пересоздание локальных файлов ключей всех зарегистрированных служб. При этом в процессе восстановления необходимо задать пароль по умолчанию для пользователей. Важно обеспечить введение такого пароля, который будет удовлетворять требованиям всех парольных политик домена. В противном случае восстановление не может быть выполнено.

Примечание. После выполнения восстановления служба заданий ALD aldd выполняет настройку привилегий пользователей и другие необходимые действия. При этом может выполнятся перезапуск различных служб сервера, в том числе и службы администрирования Kerberos. Следует дождаться завершения всех настроек перед выполнением других административных действий.

После выполнения восстановления следует воспользоваться командой test-integrity утилиты администрирования ald-admin для проверки внутренней целостности конфигурации домена, что включает в себя проверку состояния и согласованности всех сущностей ALD.

6.9.8. Доверительные отношения между доменами

В случае наличия нескольких доменов ALD поддерживается возможность обращения клиентов одного домена к ресурсам другого домена. Для этого между доменами должны быть установлены доверительные отношения.

ВНИМАНИЕ! В ALD используются симметричные доверительные отношения между доменами. В случае необходимости ограничения доступа клиентам чужого домена к тому или иному сервису, соответствующие настройки ограничения доступа должны быть

выполнены средствами конфигурирования самого сервиса.

ВНИМАНИЕ! При работе с пользователями других доменов должны использоваться имена их учетных записей Kerberos, вида <имя_пользователя>@<REALM>.

Для установки доверительных отношений между доменами необходимо в каждом из них произвести добавление другого домена командой `ald-admin trusted-add`. Детальное описание команд приведено в руководстве `man` для утилиты `ald-admin`.

ВНИМАНИЕ! Введение доверительных отношений требует изменения конфигурационных файлов на каждом компьютере домена. Изменения будут внесены после перезагрузки компьютеров. Для оперативного изменения конфигурации на отдельном компьютере без перезагрузки может быть использована команда `ald-client restart`.

ВНИМАНИЕ! Доверительные отношения не сохраняются при создании резервной копии домена командами `backup-ldif` и `backup-portable`, и должны быть установлены заново после пересоздания домена (см.6.9.7).

Примечание. В случае необходимости предоставления доступа к разделяемым файловым ресурсам пользователям могут требоваться дополнительные настройки (см. 6.7.3).

6.9.9. Создание резервного сервера ALD

Под резервным сервером ALD подразумевается сервер, который может заменить собой основной контроллер домена в случае необходимости (например, в случае выхода из строя основного контроллера домена) без потери служебной информации: учетных записей пользователей, паролей, политик паролей и другой централизованной информации.

Примечание. Резервный сервер ALD позволяет обращаться за информацией к службе каталогов LDAP и службе аутентификации Kerberos, что обеспечивает работу пользователей даже при сбое основного контроллера домена. Для этого резервный сервер должен быть указан в соответствующих конфигурационных файлах. Администрирование выполняется только на основном контроллере домена.

ВНИМАНИЕ! Резервный сервер заменяет именно контроллер домена и не обеспечивает перенос домашних директорий пользователей. Для сохранения домашних директорий рекомендуется использовать выделенный сервер домашних директорий (см. 6.9.6).

ВНИМАНИЕ! Механизм резервных серверов ALD не является “горячим резервом”. Замена основного контроллера домена резервным предполагает действия системного администратора по замене основного сервера резервным (см. 6.9.10).

Для выполнения функции резервирования используются различные механизмы репликации, в том числе и собственные механизмы репликации служб LDAP и Kerberos.

Примечание. Репликация производится от имени системной учетной записи службы обработки заданий ALD `aldd`, запущенной на резервном сервере. Указанная учет-

ная запись входит в группу администраторов, что позволяет ей реплицировать данные домена.

ВНИМАНИЕ! Расширения ALD могут привносить свое деление полномочий, что может потребовать дополнительных настроек для обеспечения полной репликации баз данных ALD.

Создание и управление резервным сервером ALD осуществляется утилитой управления сервером ALD `ald-init`.

ВНИМАНИЕ! Состав установленных пакетов ALD на резервном сервере должен быть идентичен составу пакетов ALD, установленных на основном сервере.

Создание резервного сервера заключается в выполнении команды инициализации сервера `ald-init init` с указанием опции `--slave`. В ходе создания будет выведена информация об обнаруженном первичном сервере домена и произведены настройки резервного сервера.

После проведения указанных действий на резервный сервер будет осуществляться репликация всей необходимой информации с основного сервера. В случае необходимости резервный сервер может быть переведен в оперативный режим работы командой `ald-init promote`.

Примечание. Репликация баз данных выполняется в определенные промежутки времени. Например, базы Kerberos по умолчанию обновляются раз в 10 минут, что задается параметром `SERVER_PROPAGATE_PERIOD` в конфигурационном файле `/etc/ald/ald.conf` основного сервера (см. 6.6.3).

Удаление экземпляра сервера может быть выполнено командой `ald-init destroy`.

6.9.10. Замена основного сервера резервным

В случае выхода из строя основного контроллера домена администратор должен произвести действия по замене основного сервера домена резервным:

1) Перевести один из резервных серверов в оперативный режим работы командой `ald-init promote`.

ВНИМАНИЕ! При переводе резервного сервера в оперативный режим основной сервер принудительно исключается из домена во избежание конфликтов. После восстановления он может быть возвращен в домен в качестве резервного.

2) На всех клиентских машинах, включая сервер домашних директорий (если есть), в конфигурационном файле `/etc/ald/ald.conf` в качестве параметра `SERVER` указывается новый контроллер домена (бывший резервный сервер). После этого должна быть выполнена команда `ald-client commit-config`.

6.9.11. Совместимость с предыдущими версиями

Существует возможность совместного использования в одном домене компьютеров с разными версиями ALD.

При этом возможна как работа новых клиентов ALD со старым сервером домена, так и работа старых клиентов с новым сервером домена ALD.

ВНИМАНИЕ! В связи с отличием формата хранения расширенных атрибутов в версиях Astra Linux < 1.4 отсутствует совместимость на уровне доступа к сетевым файловым ресурсам. Совместимость доступа к не файловым сетевым ресурсам (почта, СУБД и т.п.) сохраняется.

ВНИМАНИЕ! В случае отличия версии клиента от версии сервера некоторые новые возможности ALD будут недоступны. При версии ОС «1.2» к таким возможностям относятся: размещение домашнего каталога на отдельном сервере, проверка возможности входа пользователя на данный компьютер по списку разрешенных пользователю компьютеров, включение доменного пользователя в заданные локальные группы и некоторые свойства политик паролей Kerberos.

Примечание. Использование в одном домене компьютеров с разными версиями ALD не рекомендуется, т. к. в этом случае не обеспечивается работа всех заявленных механизмов ЕПП.

6.9.11.1. Работа старых клиентов с новым сервером домена ALD

Для работы старых клиентов (версии ОС «1.2») с новым сервером необходимо после введения клиентов в домен выполнить на сервере команду `ald-admin host-renew`. Это достаточно сделать один раз после добавления всех старых клиентов.

Так же для монтирования домашних каталогов необходимо в файле `/etc/request-keys.conf` заменить строку

```
create cifs.spnego * * /usr/sbin/cifs.upcall %k
```

на

```
create cifs.spnego * * /usr/sbin/cifs.upcall -c %k
```

Примечание. Поскольку файл `/etc/request-keys.conf` переписывается при обновлении конфигурации командами `ald-client commit-config` рекомендуется внести изменение в соответствующий шаблон `/etc/ald/request_key.conf.pl`.

6.9.11.2. Работа новых клиентов со старым сервером домена ALD

Работа новых клиентов со старым сервером (версии ОС «1.2») домена ALD обеспечивается в режиме совместимости, который задается указанием в конфигурационном файле `/etc/ald/ald.conf` версии 1.4:

```
VERSION=1.4
```

Кроме того, для работы механизмов монтирования домашних каталогов необходимо на сервере домена создать принципала службы `cifs` и сохранить его ключ:

```
ald-admin service-add cifs/server.my_domain.org
ald-client update-svc-keytab cifs/server.my_domain.org
```

6.10. Проверка целостности и устранение ошибок

В ALD встроены средства проверки внутренней целостности конфигурации домена, что включает в себя проверку состояния и согласованности всех сущностей ALD.

При возникновении в процессе работы сообщений об ошибках или некорректной работе механизмов ЕПП следует воспользоваться командой `test-integrity` утилиты администрирования `ald-admin`.

В ходе проверки может быть локализована причина ошибок и сбоев, что облегчит их устранение.

При выполнении команды производиться проверка состояния и согласованности сущностей домена, при этом отображается текущая проверяемая группа сущностей и результат проверки (при указании опции `--verbose` дополнительно выводиться текущая проверяемая сущность). В результате выполнения проверки могут быть выведены диагностические сообщения:

```
Проверка целостности базы данных ALD сформировала диагностических сообщений: N
1: <диагностическое сообщение 1>
...
```

При обнаружении критичных ошибок, команда завершается с выдачей сообщения об ошибке:

```
Проверка целостности базы данных ALD выявила ошибок: N.
При нормальном функционировании ALD таких ошибок возникать не должно.
Попробуйте удалить ошибочные сущности и создать их заново. Если это
не поможет, или если появятся новые ошибки - обратитесь к разработчикам.
```

Диагностические сообщения могут содержать рекомендации по устранению выявленного нарушения. Список возможных диагностических сообщений приведен ниже.

ВНИМАНИЕ! Рекомендуется использовать предлагаемый вариант устранения нарушения средствами ALD, так как для ручного устранения нарушений требуются глубокие знания технологий, механизмов функционирования и инструментов администрирования LDAP и Kerberos.

ВНИМАНИЕ! Перед критичными исправлениями, требующими пересоздания домена, рекомендуется по возможности сохранить резервную копию домена. После восстановления из резервной копии некоторые ошибки могут исчезнуть.

Примечание. Часть ошибок может быть устранена автоматически. Для этого необходимо указание опции `--fix` при вызове команды `ald-admin test-integrity`. Автоматически выполняются следующие действия:

– создание недостающих индексов и ограничений уникальности в LDAP;

– удаление несуществующих членов групп пользователей, компьютеров, сервисов и администраторов;

– пересоздание политик паролей по существующей информации (LDAP или Kerberos);

– синхронизация компьютеров по информации из Kerberos (`host-renew`);

– синхронизация параметров политик паролей из LDAP в Kerberos;

– настройка глубины истории заданий и их ротация;

– корректировка списка разрешенных компьютеров и групп компьютеров;

– отбор административных прав при любом нарушении свойств пользователей.

ВНИМАНИЕ! При вызове команды `ald-admin test-integrity` с опцией `--fix` производятся действия по исправлению сразу всех ошибок. Во избежание неверных исправлений следует учитывать характер автоматических действий (см. в табл 46).

Список возможных ошибок и способов их устранения приведен в табл 46.

Примечание. В зависимости от установленных расширений состав проверок и диагностических сообщений может отличаться. Подход к устранению ошибок, не приведенных в таблице, может быть выполнен по аналогии с описанными.

Таблица 46

Ошибки	Способы устранения
Ошибки общего вида	
Какая-либо сущность ALD не найдена или нарушен синтаксис имени сущности.	Сущность может быть либо пересоздана заново, либо удалена командами утилиты `ald-admin`. Некоторые сущности могут быть созданы или удалены средствами администрирования LDAP и Kerberos.
Нарушен синтаксис или значение свойств и параметров сущностей ALD.	Сущность может быть модифицирована командами утилиты `ald-admin`. Некоторые сущности могут быть модифицированы средствами администрирования LDAP и Kerberos.
Проверка конфигурации домена	
Имя домена отличается от значения в ald.conf.	Исправление файла ald.conf, если имя домена верно.
Версия домена отличается от значения в ald.conf.	Исправление файла ald.conf, если не используется режим совместимости.
Проверки LDAP	

Продолжение таблицы 46

Ошибки	Способы устранения
Модуль LDAP не зарегистрирован.	Неверно задан шаблон домена `slapd.16.ldif`. Необходимо указать загрузку указанного модуля и пересоздать домен. Существует возможность решения средствами администрирования LDAP, но в этом случае без модификации шаблона ошибка может повториться после пересоздания домена.
Индекс LDAP не зарегистрирован. Ограничение уникальности LDAP не зарегистрировано.	При указании опции `--fix` автоматически создается.
Проверка системных принципалов	
Не найден системный принципал в БД Kerberos.	Необходимо его создать с помощью команды kadmin(1) и сгенерировать для него ключ в файле ключей. Или проинициализировать сервер заново с помощью команд `ald-init init` или `restore-backup(-ldif)`.
Проверка компьютеров	
`host\...` принципалы не найдены для следующих компьютеров...	Удалить и пересоздать с помощью команд `host-*` или создать с помощью команды kadmin(1) и сгенерировать для него ключ в файле ключей.
Следующие компьютеры не найдены в LDAP, хотя их принципалы присутствуют в Kerberos:...	Обновить информацию в LDAP командой `host-renew` или удалить их из БД Kerberos с помощью команды kadmin(1). При указании опции `--fix` выполняется команда `host-renew`.
Проверка групп компьютеров	
Компьютер в группе компьютеров неверен или не найден в LDAP.	Модифицировать состав группы компьютеров или ввести указанный компьютер в домен. При указании опции `--fix` компьютер удаляется из группы.
Проверка серверов ALD	
Компьютер для севера ALD не найден.	Критичная ошибка конфигурации. При необходимости следует пересоздать домен.
Сервер с идентификатором уже существует.	Изменить идентификатор одного из серверов путем модификации соответствующего файла `ald.conf`.
Основной контролер домена ALD уже был найден.	Критичная ошибка конфигурации. Выявить неверный сервер ALD. Если ошибка во флагах компьютера, следует исправить флаги с помощью `host-mod`, в противном случае вывести неверный сервер из домена.
Проверка политик паролей	
Следующие политики паролей не найдены в LDAP/Kerberos (но присутствуют в Kerberos/LDAP):...	Удалить их и создать заново. При указании опции `--fix` пересоздаются по оставшейся части информации.

Продолжение таблицы 46

Ошибки	Способы устранения
Политика паролей `default` не найдена в Kerberos.	Создать вручную командой kadmin(1). При указании опции `--fix` создается.
Политика паролей не найдена в Kerberos/LDAP.	Удалить ее и создать заново. При указании опции `--fix` пересоздается по оставшейся части информации.
Политика паролей в LDAP не совпадает с аналогичной в Kerberos.	Установить параметры политики заново. При указании опции `--fix` обновляется из LDAP.
Проверка пользователей	
Для принципала отсутствует соответствующий пользователь в БД LDAP.	Если принципал не создан вручную для других целей, следует удалить его утилитой kadmin(1) и создать пользователя заново.
Отсутствует принципал Kerberos для пользователя.	Создать принципал вручную с помощью kadmin(1) или удалить и создать пользователя заново.
Политика паролей пользователя в LDAP не совпадает с Kerberos.	Установить политику пользователя заново. При указании опции `--fix` пользователю назначается политика паролей из LDAP.
Пользователь имеет UID, который меньше, чем MINIMUM_UID.	Ошибка создания пользователя. Удалить пользователя и создать его заново с правильным UID или изменить с помощью команды `user-mod.`.
Пользователь ссылается на несуществующую политику.	Изменить неправильные параметры пользователя. При указании опции `--fix` пользователю назначается политика паролей по умолчанию «`default`».
Пользователь ссылается на несуществующую группу.	Изменить неправильные параметры пользователя. При указании опции `--fix` пользователю назначается группа по умолчанию «`Domain Users`».
Неправильный синтаксис домашнего каталога пользователя. Неправильный синтаксис командной оболочки пользователя. Неправильный синтаксис GECOS пользователя.	Изменить неправильные параметры пользователя.
Следующие компьютеры, указанные в списке привилегий пользователя, неверны или не найдены в БД LDAP.	Добавить их в домен или изменить привилегии пользователя командой `user-ald-cap`. При указании опции `--fix` компьютеры удаляются из списка привилегий пользователя.
Следующие группы компьютеров, указанные в списке привилегий пользователя, неверны или не найдены в БД LDAP.	Добавить их в домен или изменить привилегии пользователя командой `user-ald-cap`. При указании опции `--fix` группы компьютеров удаляются из списка привилегий пользователя.
Проверка групп	
Группа имеет GID, который меньше, чем MINIMUM_GID.	Ошибка создания группы. Удалить группу и создать ее заново с правильным GID или изменить с помощью команды `group-mod.`.

Продолжение таблицы 46

Ошибки	Способы устранения
Группа содержит несуществующего пользователя.	Изменить состав группы с помощью команды `group-mod`. При указании опции `--fix` пользователь удаляется из группы.
Проверка администраторов	
Группа администраторов не найдена.	Критическая ошибка. Необходимо пересоздать домен.
Следующие bind-DN не найдены в группе администраторов:...	Добавить с помощью команд `ald-admin` недостающие члены или пересоздать домен. При указании опции `--fix` добавляются автоматически.
Сервис присутствует в группе администраторов, но не найден в базе данных.	Модифицировать группу администраторов или создать указанный сервис заново. При указании опции `--fix` сервис удаляется из группы администраторов.
Пользователь присутствует в группе администраторов, но не обладает привилегией администратора. Пользователь обладает привилегией администратора, но не присутствует в группе администраторов.	Установить правильные привилегии пользователя командой `user-ald-cap`. При указании опции `--fix` пользователь удаляется из группы администраторов или лишается привилегий.
Проверка сервисов	
Компьютер сервиса не найден в LDAP.	Если принципал не создан вручную для других целей, следует удалить сервис или ввести указанный компьютер в домен.
Проверка групп сервисов	
Группа сервисов содержит сервис с неверным именем. Группа сервисов содержит несуществующий сервис.	Изменить состав группы с помощью команды `sgroup-svc-rm`. При указании опции `--fix` сервис удаляется из группы.
Проверка доменных документов	
Неверная версия документа. Неверный путь к файлу.	Исправить свойства документа.
Файл не существует.	Удалить документ и создать заново.
Проверка доверенных доменов	
Доверенный домен области не найден. Inbound/Outbound TGT принципал не найден.	Удалить доверенный домен и создать заново.
Не удалось разыменовать KDC домена.	Проверить настройку системы разрешения имен и наличие связи с указанным севером. При необходимости удалить доверенный домен.
Проверка серверных заданий	

Окончание таблицы 46

Ошибки	Способы устранения
Параметр `task-history` должен быть числом > 2 и < 2000.	Установите корректное значение. При указании опции `--fix` устанавливается значение по умолчанию (100).
Количество завершенных заданий превышает параметр `task-history`.	Удалить задания вручную. При указании опции `--fix` выполняется ротация заданий.

6.11. Настройка сетевых служб

Ряд сетевых служб, таких как СУБД PostgreSQL, электронная почта, обработка гипертекстовых документов (web), система печати и др. для работы в ЕПП должны быть соответствующим образом настроены. Как правило, настройка заключается в обеспечении возможности использования этими службами сквозной аутентификации и получения необходимой информации из БД ALD.

Примечание. При выполнении настройки сетевых служб потребуется использование учетной записи привилегированного пользователя через механизм `sudo`. При снятии блокировки на интерактивный вход в систему для суперпользователя `root` не рекомендуется осуществлять переключение в режим суперпользователя командой `su`. Необходимо использовать команду:

```
# su -
```

ВНИМАНИЕ! Для обеспечения нормальной работы пользователя с сетевыми сервисами в ЕПП должны быть явно заданы диапазоны его мандатных уровней и категорий с помощью соответствующих утилит (см. 6.6), даже если ему не доступны уровни и категории выше 0.

Описание настройки некоторых сетевых сервисов приведены в следующих разделах:

– Система обмена сообщениями электронной почты — см. 13.4;

– Защищенный комплекс программ гипертекстовой обработки данных — см. 12.3;

– Защищенный комплекс программ печати и маркировки документов — см. 10.3;

– Защищенная система управления базами данных — (см. РУСБ.10015-01 95 01-2 «Операционная система специального назначения «Astra Linux Special Edition» Руководство администратора. Часть 2» раздел 1.4.2. Использование сквозной аутентификации в ЕПП);

7. ЗАЩИЩЕННАЯ ГРАФИЧЕСКАЯ ПОДСИСТЕМА

Защищенная графическая подсистема в составе ОС функционирует с использованием графического сервера Xorg.

По умолчанию в графическую подсистему встроена мандатная защита.

Для установки пакетов графической подсистемы следует в процессе работы программы установки ОС отметить в окне «Выбор программного обеспечения» строку «Рабочий стол Fly». В этом случае рабочий стол Fly установится с настройками по умолчанию, и в процессе загрузки установленной системы после окончания работы системного загрузчика произойдет переход к графическим программам «Вход в систему: сервер и GUI» (`fly-dm`, `fly-qdm`). После завершения процедуры аутентификации на экране монитора появится графический рабочий стол.

7.1. Конфигурирование менеджера окон и рабочего стола в зависимости от типа сессии

Выбор режима рабочего стола Fly выполняется в меню «Тип сессии» в окне графического вхоода в систему (утилита `fly-dm`). Предусмотрено несколько режимов, но администратор системы может добавить сколько угодно новых дополнительных. Для этого он должен добавить файл (файлы) типа `desktop` в `/usr/share/fly-dm/sessions` и создать соответствующие конфигурационные файлы для `fly-wm`.

При входе через `fly-dm` выставляется переменная `DESKTOP_SESSION=имя_режима` (она и в предыдущих версии ОС выставлялась как `fly`), например, `fly`, `fly-desktop`, `fly-tablet`, `fly-mobile` и т.д.). То есть эта переменная — это имя ярлыка сессии из `/usr/share/fly-dm/sessions` (но без расширения `.desktop`), которая указывает на тип сессии. Например:

`DESKTOP_SESSION=fly` — десктопный

`DESKTOP_SESSION=fly-tablet` — планшетный

`DESKTOP_SESSION=fly-mobile` — мобильный

Это имя сессии используется как суффикс для выбора конфигурационных файлов менеджера окон `fly-wm`. Т.е. к базовому имени конфигурационного файла добавляется «`.$DESKTOP_SESSION`».

Если тип сессии просто десктопный, т.е. `DESKTOP_SESSION=fly`, то конфигурационные файлы остаются как в предыдущих версиях ОС, т.е. без суффикса (для обратной совместимости).

Имеются конфигурационные файлы:

`apprc`

`apprc.fly-mini`

```
apprc.fly-mobile
apprc.fly-tablet
en.fly-wmrc
en.fly-wmrc.fly-mini
en.fly-wmrc.fly-mobile
en.fly-wmrc.fly-tablet
en.miscrc
en.miscrc.fly-mini
en.miscrc.fly-mobile
en.miscrc.fly-tablet
keyshortcutrc
keyshortcutrc.fly-mini
keyshortcutrc.fly-mobile
keyshortcutrc.fly-tablet
ru_RU.UTF-8.fly-wmrc
ru_RU.UTF-8.fly-wmrc.fly-mini
ru_RU.UTF-8.fly-wmrc.fly-mobile
ru_RU.UTF-8.fly-wmrc.fly-tablet
ru_RU.UTF-8.miscrc
ru_RU.UTF-8.miscrc.fly-mini
ru_RU.UTF-8.miscrc.fly-mobile
ru_RU.UTF-8.miscrc.fly-tablet
sessrc
sessrc.fly-mini
sessrc.fly-mobile
sessrc.fly-tablet
theme/default.themerc
theme/default.themerc.fly-mini
theme/default.themerc.fly-tablet
theme/default.themerc.fly-mobile
```

Есть также `/usr/share/fly-wm/fly-wmrc.mini`, этот конфигурационный файл служит для совместимости и включает все `*.fly-mini`. Из названий этих файлов и комментариев в файлах можно понять их назначение и особенности использования.

Если использовались файлы типа:

```
~/.fly/*rc
~/.fly/theme/*rc
/usr/share/fly-wm/*rc
/usr/share/fly-wm/theme/*rc
```

то необходимо переделать формирование имени конфигурационного файла. Например, это сделано в утилитах `fly-admin-theme`, `fly-admin-hotkeys`, `fly-admin-winprops` и др.

В ярлыках в полях `NotShowIn` и `OnlyShowIn` можно использовать имена типов сессий (`fly`, `fly-tablet`, `fly-mobile` и т.д.). Функция `FlyDesktopEntry::isDisplayable()` из `libflycore` изменена с учетом нахождения в сессии какого-либо типа (`$DESKTOP_SESSION`), также в `libflycore` добавлены:

```
const char * flySessionName()
const char * flySessionConfigSuffix()
```

Используя имена типов сессий в `NotShowIn` и `OnlyShowIn`, можно скрывать/показывать определенные ярлыки из меню «Пуск», панели задач или автозапуска (в зависимости от текущего режима).

Если у какой-либо Qt-программы есть сохраняемые/восстанавливаемые параметры «чувствительные» к типу сессии (планшет, десктоп и т.д.), то будет иметь такие параметры в отдельных экземплярах для каждого типа сессии, добавляя, например, суффиксы `$DESKTOP_SESSION` к именам параметров.

Таким образом, есть основной источник информации о типе сессии `$DESKTOP_SESSION` и к нему необходимо теперь «привязываться».

Также можно легко создавать новые типы сессий. Например, для «слабых» систем или удаленных терминалов можно создавать какой-нибудь вход типа `fly-light` и т.п.

7.2. Рабочий стол как часть экрана

В файлах `*themerc` (прежде всего в `~/.fly/theme/current.themerc`) можно задавать параметры `FlyDesktopWidth` и `FlyDesktopHeight`, которые определяют размер (в пикселях) рабочего стола на экране. Это может быть полезно, например, для:

– деления широкоформатного монитора на две части: с рабочим столом и свободной областью, куда можно перетаскивать окна;

– для задания области рабочего стола только на левом мониторе в двухмониторной конфигурации с Xinerama.

7.3. Удаленный вход по протоколу XDMCP

По умолчанию в системе удаленный вход по протоколу XDMCP запрещен. Чтобы его разрешить необходимо:

1) в файле `/etc/X11/fly-dm/Xaccess` `localhost` заменить на `*`;

2) в файле `/etc/X11/fly-dm/fly-dmrc` убедиться, что `Enable=true`:

```
...
[Xdmcp]
```

```
Enable=true
...
```

7.4. Решение возможных проблем с видеодрайвером Intel

Видеодрайвер для систем на базе процессоров Intel может в некоторых случаях устранять проблемы: от искажений на экране до падения X-сервера. В ряде случаев это может быть вызвано типом используемого ускорения графики. По умолчанию в драйвере включен тип ускорения SNA. Для использования более старого, медленного, но более стабильного UXA можно в `/usr/share/X11/xorg.conf.d` разместить файл `10-intel.conf`:

```
Section "Device"
Identifier "intel"
Driver "intel"
Option "AccelMethod" "sna"
EndSection
```

7.5. Автоматизация входа в систему

Для включения автоматизации входа пользователя в систему на разных разрешенных ему уровнях секретности, с последующим легким же переключением между такими входами необходимо в `/etc/init.d/fly-dm` перед запуском `fly-dm` выставить переменную:

```
...
export DM_LOGIN_AUTOMATION=1
...
```

Затем на рабочих столах пользователя можно создать такие, например, ярлыки:

Ярлык для запуска или перехода в сессию с меткой `0:0:0x0:0x0`

```
[Desktop Entry]
Name = session 0
Name[ru] = Сессия 0
Type = Application
NoDisplay = false
Exec = fly-dmctl maclogin user password 0:0:0x0:0x0
Icon = ledgreen
X-FLY-IconContext = Actions
Hidden = false
Terminal = false
StartupNotify = false
```

Ярлык для запуска или перехода в сессию с меткой `1:0:0x0:0x0`

```
[Desktop Entry]
Name = session 1
Name[ru] = Сессия 1
Type = Application
NoDisplay = false
Exec = /usr/bin/fly-dmctl maclogin user password 1:0:0x0:0x0
Icon = ledyellow
X-FLY-IconContext = Actions
Hidden = false
Terminal = false
StartupNotify = false
```

Ярлык для запуска или перехода в сессию с меткой `2:0:0x0:0x0`

```
[Desktop Entry]
Name = session 2
Name[ru] = Сессия 2
Type = Application
NoDisplay = false
Exec = fly-dmctl maclogin user password  2:0:0x0:0x0
Icon = ledred
X-FLY-IconContext = Actions
Hidden = false
Terminal = false
StartupNotify = false
```

С помощью ярлыков такого типа пользователь сможет максимально легко переключаться между сессиями с разными мандатными метками (они, естественно, должны быть ему предварительно разрешены администратором системы).

7.6. Рабочий стол Fly

В состав рабочего стола Fly входит оконный менеджер и большое количество графических утилит, которые могут быть использованы для администрирования ОС. Большинство из этих утилит представляет собой графические оболочки над соответствующими текстовыми утилитами командной строки.

Основные графические утилиты для настройки и администрирования системы приведены в таблице 47.

Таблица 47

Утилита	Назначение
`fly-admin-autostart` «Автозапуск»	Установки приложений, запускаемых автоматически при загрузке рабочего стола
`fly-admin-center` «Панель управления»	Централизованный доступ к графическим утилитам настройки и администрирования системы
`fly-admin-cron` «Планировщик задач»	Запуск программ в фоновом режиме в определенное время
`fly-admin-date` «Дата и время»	Настройка часового пояса даты и времени
`fly-admin-device-manager` «Менеджер устройств»	Настройка некоторых системных устройств
`fly-admin-dhcp` «Настройка DHCP-сервера»	Настройка сервера DHCP
`fly-admin-dm` «Настройка графического входа»	Настройка входа в систему
`fly-admin-env` «Переменные окружения»	Добавление, изменение и удаление переменных окружения
`fly-admin-fonts` «Менеджер шрифтов»	Просмотр и импорт системных шрифтов
`fly-admin-ftp` «FTP»	Настройка сервера FTP
`fly-admin-gamma` «Коррекция гаммы»	Установка цветового баланса монитора
`fly-admin-grub2` «Загрузчик GRUB2»	Инструмент настройки системного загрузчика GRUB2
`fly-admin-hotkeys` «Редактор горячих клавиш»	Редактор «горячих» клавиш рабочего стола
`fly-admin-int-check` «Проверка целостности системы»	Проверка целостности системы для рабочего стола Fly
`fly-admin-kiosk` «Киоск»	Управление ограничениями среды
`fly-admin-marker` «Редактор маркеров»	Настройка маркировки печати сопроводительной надписи секретных документов
`fly-admin-ntp` «Настройка NTP»	Настройка сервера времени NTP
`fly-admin-policykit-1` «Санкции PolicyKit»	Управление санкциями Policykit
`fly-admin-power` «Управление питанием»	Управление питанием
`fly-admin-printer` «Менеджер печати»	Настройка системы печати

Продолжение таблицы 47

Утилита	Назначение
`fly-admin-reflex` «Обработка подключения устройств»	Настройка реакций при подключении устройств
`fly-admin-runlevel` («Уровни запуска»)	Настройка уровней выполнения (запуска) сервисов ОС
`fly-admin-samba` «Общие папки Samba»	Управление общими папками Samba
`fly-admin-session` «Управление сессиями»	Настройки для сессий рабочего стола
`fly-admin-smc` «Управление политикой безопасности»	Управление локальной политикой безопасности и управление ЕПП. Позволяет управлять: пользователями, группами и настройками и атрибутами (мандатным разграничением доступа пользователя, параметрами протоколирования, привилегиями, политикой срока действия пароля, политикой блокировки); базами данных Parsec (аудитом, мандатными атрибутами и привилегиями); политикой создания пользователей; настройками безопасности (устанавливать параметры монтирования для очистки блоков памяти при их освобождении, настраивать очистку разделов страничного обмена при выключении системы); параметрами подключения внешних устройств (учитывать носители и управлять их принадлежностью, протоколированием и мандатными атрибутам
`fly-admin-ald` «Управление доменной политикой безопасности»	Управление политикой безопасности ЕПП (домена). Работает как и программа `fly-admin-smc` в режиме ЕПП. Выполняет те же действия, что и консольная утилита `ald-admin`
`fly-admin-service` «Консоль управления сервисами»	Статус и конфигурация служб, их запуск и остановка, автоматизированная настройка служб для функционирования с аутентификацией в режиме ЕПП и PAM
`fly-admin-theme` «Темы рабочего стола»	Оформление и поведение рабочего стола
`fly-admin-viewaudit` «Журнал безопасности»	Просмотр журнала расширенной системы протоколирования
`fly-admin-wicd` «Сетевые соединения»	Общесистемная настройка службы Wicd
`fly-admin-winprops` «Настройка параметров окон»	Настройка параметров окон
`fly-alternatives` «Системные альтернативы»	Управление системой альтернатив дистрибутивов, основанных на Debian
`fly-dialer` «Работа с модемом»	Настройка модема и установление соединения
`fly-menuedit` «Меню и ярлыки»	Редактирование основного меню, панели быстрого запуска и коллекций ярлыков

Окончание таблицы 47

Утилита	Назначение
`fly-mimeapps` «Приложения для типов файлов»	Сопоставление типов файлов и приложений (запускается с аргументом `--dialog`)
`fly-passwd` «Изменить пароль»	Смена пароля
`fly-randr` «Настройка монитора»	Переключение разрешений экрана с помощью расширения `X randr` и настройка энергосбережения
`fly-scan` «Сканеры»	Установка сканера и сканирование с сохранением изображения (запускается с аргументом `--noautoselect`)
`fly-su` «Подмена пользователя»	Выполнение команды от имени другого пользователя
`fly-xkbmap` «Раскладка клавиатуры»	Настройка раскладок клавиатуры

Описание утилит приведено в электронной справке.

7.7. Мандатное разграничение доступа

Мандатная защита, встроенная в рабочий стол Fly, позволяет администратору устанавливать отдельно для каждого пользователя разрешенный диапазон мандатных уровней и категорий. Для этой цели следует использовать графическую утилиту `fly-admin-smc`.

После того, как пользователь, для которого установлены возможные мандатные уровни и категории, отличные от нуля, войдет в систему, ему будет предложено установить конкретный мандатный уровень и конкретную категорию для данной сессии в пределах разрешенных диапазонов. Выбранные значения этих параметров можно будет проверить с помощью индикатора в виде кружка с числом внутри, расположенного в области уведомлений на панели задач в правом нижнем углу рабочего стола. Для получения информационного сообщения следует навести курсор на этот индикатор (рис. 2).

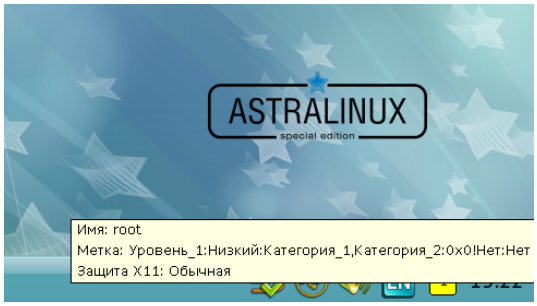


Рис. 2

8. УПРАВЛЕНИЕ ПРОГРАММНЫМИ ПАКЕТАМИ

В ОС используются программные пакеты (далее по тексту — пакеты) в формате «.deb». Для управления пакетами в режиме командной строки (или в эмуляторе терминала в графическом режиме) предназначены набор команд нижнего уровня dpkg и комплекс программ высокого уровня apt-get, apt-cache и aptitude. В графическом режиме управлять пакетами можно с помощью программы synaptic (универсальная графическая оболочка для apt).

По умолчанию обычный пользователь не имеет права использовать эти инструменты. Для всех операций с пакетами (за исключением некоторых случаев получения информации о пакетах) необходимы права суперпользователя, которые администратор может получить через механизм sudo.

Примечание. Права доступа к исполняемым файлам позволяют всем пользователям запускать их на выполнение, но удалять или модифицировать такие файлы может только суперпользователь. Обычно приложения устанавливаются в каталог с правами чтения всеми пользователями, но без права записи в него.

Средства управления пакетами обеспечивают возможность автоматизированной установки обновлений ОС.

8.1. Набор команд dpkg

Набор команд dpkg предназначен, в основном, для операций с пакетами на локальном уровне. С помощью команды dpkg и других команд этого набора можно устанавливать и удалять пакеты, собирать их из исходных текстов, получать информацию о конкретном пакете и об установленных в системе пакетах:

```
dpkg -i <полный_путь>/<полное_имя_пакета>
```

Если пакет (например, iptables_1.4.21-2_amd64.deb), который необходимо установить, помещен в рабочий каталог (например, /home/user1) или находится на смонтированном внешнем носителе, следует выполнить следующую команду:

```
dpkg -i /home/user1/iptables_1.4.21-2_amd64.deb
```

В случае, если неудовлетворенные зависимости пакета отсутствуют, он будет установлен. В случае нарушения зависимостей dpkg выдаст сообщение об ошибке, в котором будут перечислены все необходимые пакеты, которые следует установить, чтобы разрешить обязательные зависимости.

Для удаления ненужного пакета, но сохранения всех его файлов настройки, следует выполнить команду:

```
dpkg -r <значимая_часть_имени_пакета>
```

Для приведенного выше примера команда будет выглядеть следующим образом:

```
dpkg -r iptables
```

Для удаления пакета и очистки системы от всех его компонентов (в случае, если данный пакет не связан зависимостями с другими установленными пакетами) следует выполнить команду:

```
dpkg -P <значимая_часть_имени_пакета>
```

Если же удаляемый пакет зависит от других пакетов, последует сообщение об ошибке с перечнем зависимостей.

Следует отметить, что использование полного имени пакета регулируется для всех команд семейства `dpkg` простым правилом: для любых действий с уже установленным пакетом в командной строке применяется значимая часть имени, а во всех остальных случаях — полное имя.

Подробное описание команды приведено в `man dpkg`.

8.2. Комплекс программ apt

Комплекс программ `apt` предназначен, в основном, для управления всеми операциями с пакетами (в т. ч. автоматическим разрешением зависимостей) при наличии доступа к сетевым или локальным архивам (источникам) пакетов.

8.2.1. Настройка доступа к архивам пакетов

Информация о сетевых и локальных архивах пакетов для комплекса программ `apt` содержится в файле `/etc/apt/sources.list`. В этом файле находится список источников пакетов, который используется программами для определения местоположения архивов. Список источников разрабатывается для поддержки любого количества активных источников и различных видов этих источников. В данном файле перечисляется по одному источнику на строку, где источники следуют в порядке убывания их приоритета.

Описание файла `/etc/apt/sources.list` приведено в `man sources.list`.

Пример файла `sources.list`:

```
deb cdrom:[OS Astra Linux 1.3.39 smolensk - amd64 DVD]/ smolensk contrib
main non-free
deb ftp://192.168.32.1/astra/unstable/smolensk/mounted-iso-main smolensk
main contrib non-free
deb ftp://192.168.32.1/astra/unstable/smolensk/mounted-iso-devel smolensk devel
contrib non-free
```

При установке ОС с дистрибутива строка `deb cdrom...` автоматически записывается в этот список.

Включить эту строку в данный список можно также при помощи команды:

```
apt-cdrom add
```

DVD-диск с дистрибутивом ОС при этом должен находиться в устройстве чтения DVD-дисков (монтировать его не обязательно).

Строки, соответствующие источникам остальных типов, вносятся в файл при помощи любого редактора.

8.2.2. Установка и удаление пакетов

После установки ОС создается локальная БД о всех пакетах, которые находились на DVD-диске с дистрибутивом и архив установленных пакетов. Эта информация может выводиться в различной форме при помощи команды `apt-cache`. Например, команда:

```
apt-cache show iptables
```

выведет всю информацию, содержащуюся в описании пакета `iptables`.

Обновить содержимое локальной БД можно при помощи команды:

```
apt-get install update
```

Эту операцию необходимо выполнять при каждом изменении как списка источников пакетов, так и содержимого этих источников (например, при переходе к использованию обновленной версии ОС).

Полное обновление всех установленных в системе пакетов производится при помощи команды:

```
apt-get install upgrade
```

Обновление старой версии ОС до новой (без переустановки) производится при помощи команды:

```
apt-get install dist-upgrade
```

Установка отдельного пакета (если он отсутствовал в системе) производится при помощи команды:

```
apt-get install <значимая_часть_имени_пакета>
```

При этом будут исследованы и разрешены все обязательные зависимости и, при необходимости, установлены необходимые дополнительные пакеты.

Удаление пакета (с сохранением его файлов настройки) производится при помощи команды:

```
apt-get remove <значимая_часть_имени_пакета>
```

Если при этом необходимо полностью очистить систему от всех компонент удаляемого пакета, то применяется команда:

```
apt-get remove --purge <значимая_часть_имени_пакета>
```

Описание команд приведено в `man apt-cache` и `man apt-get`.

9. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ

Целью резервного копирования является обеспечение возможности восстановления с минимальными затратами труда и времени отдельных файлов или всей ФС в случае утери рабочей копии информации по какой-либо причине.

С точки зрения администратора системы, процесс резервного копирования должен быть как можно больше автоматизирован и требовать минимального участия.

Примечание. Резервное копирование — это процесс, влияющий на работоспособность системы. Резервное копирование и восстановление увеличивает текущую нагрузку на систему, что может вызывать замедление работы системы или недовольство пользователей. Кроме того, в зависимости от вида резервного копирования и восстановления, может требоваться монопольный доступ к системе или даже полная остановка ее работы.

В зависимости от имеющихся в распоряжении устройств для хранения резервных копий могут быть использованы различные носители информации: ленточные или дисковые накопители, различные отчуждаемые носители информации или специально выделенные разделы жесткого диска.

Для обеспечения надежного резервного копирования и восстановления в реальных системах как правило применяется четкое планирование указанных процессов, учитывающее все аспекты построения и функционирования системы (см. 9.2).

Для выполнения операций резервного копирования и восстановления объектов ФС с сохранением и восстановлением мандатных атрибутов и атрибутов аудита в ОС могут использоваться: комплекс программ Bacula (9.3), утилита копирования `rsync` (9.4) или утилита архивирования `tar` (4.2.1.1).

ВНИМАНИЕ! Работа с мандатными атрибутами и атрибутами аудита при использовании различных утилит создания резервных копий требует опций сохранения расширенных атрибутов (как правило вида `–xattrs`, возможно с указанием дополнительных параметров, например 9.4 и 9.5).

ВНИМАНИЕ! Для восстановления мандатных атрибутов файлов из резервных копий необходимо от имени учетной записи администратора выполнить команду:

```
sudo echo 1 > /parsecfs/unsecure_setxattr
```

ВНИМАНИЕ! Для восстановления мандатных атрибутов файлов из резервных копий процесс должен иметь PRASEC-привилегию `0x1000`. Привилегия может быть получена с использованием утилиты `execaps`:

```
sudo execaps –c 0x1000 tar .......
```

После восстановления из резервных копий файлов с мандатными атрибутами необходимо от имени учетной записи администратора выполнить команду:

```
sudo echo 0 > /parsecfs/unsecure_setxattr
```

9.1. Виды резервного копирования

Существуют следующие виды резервного копирования:

– полное резервное копирование — сохранение резервной копии всех файлов системы. Это процедура занимает много времени и требует большого количества носителей информации. Как правило, выполняется в тех случаях, когда не влияет на основную работу системы, или для создания базовой резервной копии данных. В дальнейшем может выполняться дифференциальное или инкрементное резервное копирование;

– дифференциальное резервное копирование — сохранение копий изменившихся с последнего полного резервного копирования файлов. Требования к объему хранения и времени создания копии уменьшаются, а восстановление выполняется быстро за счет прямой перезаписи файлов;

– инкрементное резервное копирование — сохранение изменений файлов с момента последнего инкрементного копирования. Требует минимального количества времени и места для создания копии, но усложняет последующее восстановление, поскольку требует последовательного восстановления всех инкрементных копий с момента последнего полного резервного копирования.

9.2. Планирование резервного копирования

Планирование резервного копирования заключается в рассмотрении и определении следующих вопросов:

– что именно и как часто должно архивироваться;

– какие виды резервного копирования и на какие носители должны применяться;

– как часто и каким образом будут восстанавливаться файлы при необходимости;

– каким образом пользователи могут запросить ранее сохраненные файлы.

Примечание. План резервного копирования должен периодически пересматриваться для отражения текущих изменений в системе, используемых технологиях или условиях функционирования.

9.2.1. Составление расписания резервного копирования

При составлении расписания резервного копирования определяется что, когда и на каком носителе должно сохраняться.

Должна существовать возможность восстановления любого файла в любой момент времени. Например, требуется восстановить файл не более, чем однодневной давности. Для этого может использоваться комбинация полного и обновляемого (дифференциального или инкрементного) резервного копирования. Полное резервное копирование позволяет сохранить копии всех файлов системы, обновляемое — только изменившиеся со време-

ни последнего архивирования. Обновляемое может иметь несколько уровней, например обновление по отношению к последней обновляемой резервной копии.

Для восстановления отдельных файлов при таком многоуровневом расписании может понадобиться полная резервная копия, если файл не изменялся в течение месяца; копия первого уровня, если файл не изменялся в течение недели; копия второго уровня при ежедневной работе с этим файлом. Такая схема несколько сложнее, однако требует меньших ежедневных затрат времени.

Примечание. Расписание резервного копирования должно быть доведено до пользователей.

9.2.2. Планирование восстановления системы

При составлении плана резервного копирования должен быть определен план действий на случай аварийной ситуации и то, как при необходимости может быть восстановлена система или отдельные файлы, где хранятся и насколько доступны носители с резервными копиями и не могут ли они потерять работоспособность при неполадках на компьютере.

Примечание. Следует проверять архивы резервных копий. Эта проверка может включать в себя чтение содержимого копии после сохранения или выборочную проверку файлов резервной копии.

9.3. Комплекс программ Bacula

Все действия выполняются от имени учетной записи администратора с использованием механизма `sudo`.

В примере использована следующая инфраструктура:

– выделенный сервер `bakula1.my.dom` с IP-адресом `11.11.11.21` (на нем будет функционировать `Director Daemon` — это главный сервер, осуществляющий резервное копирование);

– выделенный сервер `bakula2.my.dom` с IP-адресом `11.11.11.22` (на нем будет функционировать `Storage Daemon` — это машина, на которую будут размещаться резервные копии данных);

– персональный компьютер `bakula3.my.dom` с IP-адресом `11.11.11.23` (на нем будет функционировать `File Daemon` — это машина, с которой будут копироваться данные и на которую будут восстанавливаться резервные копии данных).

9.3.1. Подготовка инфраструктуры для управления системой резервного копирования

1) Установить `Postgresql-9.3` на сервер, где будет работать `Director Daemon`:

```
aptitude install postgresql-9.3
```

2) Установить pgadmin3 на сервер, где будет работать Director Daemon:

```
aptitude install pgadmin3
```

3) Предполагается, что на всех машинах изначально установлены все пакеты, касающиеся Bacula, из состава ОС. Через менеджер пакетов Synaptic по ключевому слову «bacula» необходимо установить все пакеты, кроме тех, где в названии фигурирует «-sqlite3».

При настройке Bacula появится интерфейс для настройки совместимости с БД, в качестве имени базы необходимо указать bacula и пароль bacula.

При настройке базы Bacula может произойти ошибка, на данном этапе необходимо ее игнорировать, база будет настроена позже.

Примечание. Далее в любом случае придется править созданную БД.

4) Подготовить БД для Bacula, для чего необходимо:

– в файле /etc/postgresql/9.3/main/postgresql.conf указать listen_addresses = '*';

– в файле /etc/postgresql/9.3/main/pg_hba.conf внести необходимые изменения, для простоты можно указать метод trust для всех соединений, удалить любую дополнительную конфигурацию после метода типа mod=;

– обязательно добавить host с IP-адресом, где будет работать bacula-dir. В случае если все демоны Bacula будут установлены на одну машину, указывать IP-адрес не обязательно, т.к. работа будет идти через localhost.

Пример файла pg_hba.conf:

```
local all postgres trust
local all all trust
host all all 127.0.0.1/32 trust
host all all 11.11.11.21/24 trust
```

– выполнить запуск БД:

```
pg_ctlcluster 9.3 main restart
```

– присвоить пароль postgres:

```
passwd postgres
```

– присвоить для Bacula пароль bacula:

```
passwd bacula
```

– создать пользователя БД для работы с Bacula (выполнять не от имени учетной записи администратора):

```
# psql template1 postgres
postgres=# CREATE ROLE bacula;
```

```
postgres=# ALTER USER bacula PASSWORD 'bacula';
postgres=# ALTER USER bacula LOGIN SUPERUSER CREATEDB CREATEROLE;
```

5) Создать БД bacula (выполнять не от имени учетной записи администратора):

– выполнить pgadmin3;

– указать имя template1, пользователя postgres, пароль postgres;

– в секции Роли входа добавить роль входа bacula. Создать БД bacula, владельцем назначить bacula.

6) На сервере bakula1.my.dom необходимо запустить скрипты, которые создадут все необходимые таблицы и привилегии:

– в скрипте /usr/share/bacula-director/make_postgresql_tables предварительно необходимо открыть скрипт на редактирование:

– в строке db_name указать имя -bacula;

– в строке psql после psql вписать -U bacula;

– в скрипте /usr/share/bacula-director/grant_postgresql_privileges предварительно необходимо открыть скрипт на редактирование:

– в строке db_user указать имя -bacula;

– в строке db_name указать имя -bacula;

– в строке db_password указать пароль bacula;

– в строке $bindir/psql после psql вписать -U bacula;

– сохранить изменения и выполнить скрипты:

```
make_postgresql_tables
grant_postgresql_privileges
```

7) На машине, где будет работать Storage Daemon, необходимо создать каталог /back, в котором будут храниться резервные копии данных и присвоить каталогу владельца bacula:

```
mkdir /back
chown -R bacula /back
```

8) На машине, где будет работать File Daemon, необходимо создать каталог /etc2, в который будут восстанавливаться данные из резервной копии:

```
mkdir /etc2
```

Если подготовительные настройки выполнены корректно, БД стартует без ошибок и скрипты выполнились без ошибок, то можно приступить к настройке Bacula.

9.3.2. Настройка Bacula

Подготовка Bacula к работе заключается в настройке каждого компонента в отдельности и последующей настройке их взаимодействия.

9.3.2.1. Настройка Director Daemon

Далее необходимо приступить к настройке Director Daemon в конфигурационном файле /etc/bacula/bacula-dir сервера bakula1.my.dom. В первую очередь необходимо определить основные параметры в секции Director. На начальном этапе важно установить параметры Name и Password. Name задает уникальное имя Director Daemon, а Password — пароль, который будет использоваться при соединениях BC с DD. Остальные параметры можно оставить в значениях по умолчанию.

```
Director { # define myself
Name = bacula-dir
DIRport = 9101 # where we listen for UA connections
QueryFile = "/etc/bacula/scripts/query.sql"
WorkingDirectory = "/var/lib/bacula"
PidDirectory = "/var/run/bacula"
Maximum Concurrent Jobs = 1
Password = "1" # Console password
Messages = Daemon
DirAddress = 11.11.11.21
}
```

Следующей группой параметров, которые необходимо определить, является секция Catalog. Здесь необходимо указать реквизиты доступа к БД, а также назначить уникальное имя данного Bacula Catalog с помощью параметра Name.

```
Catalog {
Name = MyCatalog
# Uncomment the following line if you want the dbi

PS. driver
# dbdriver = "dbi:sqlite3"; dbaddress = 127.0.0.1; dbport =
dbname = "bacula"; dbuser = "bacula"; dbpassword = "bacula"
DB Address = 11.11.11.21
}
```

Теперь необходимо определить SD, на который будет производиться передача данных для дальнейшей записи на устройство хранения. Storage Daemon настроен и готов к работе, необходимо определить реквизиты доступа к нему в секции Storage файла bacula-dir.conf. Основные параметры:

1) Параметр Name — уникальное имя, использующееся для адресации секции Storage в рамках файла bacula-dir.conf.

2) Параметры Device и MediaType дублируют одноименные параметры файла

bacula-sd.conf.

3) Параметр Password содержит пароль, который будет использоваться при подключении к Storage Daemon.

```
Storage {
Name = File
# Do not use "localhost" here
Address = 11.11.11.22 # N.B. Use a fully qualified name here
SDPort = 9103
Password = "1"
Device = FileStorage
Media Type = File
}
```

Секция Pool определяет набор носителей информации и параметры, определяющие то, как SD будет их обрабатывать. Каждый Pool взаимодействует с устройством хранения данных, и поэтому необходимо создать столько же пулов, сколько определено устройств хранения. Фактически если для каждого File Daemon вы определяете отдельное устройство, то для каждого FD необходимо определить и Pool. Основные параметры:

1) Параметр Name определяет уникальное имя пула.

2) Параметр Pool Type определяет тип, и для резервных копий должен быть установлен в значение Backup.

3) Параметр Maximum Volume Jobs рекомендуется установить в значение 1. Это будет означать, что в рамках одного носителя данных могут быть размещены резервные данные, полученные в ходе выполнения только одного задания. Носитель данных — это устройство, на которое непосредственно записываются данные (оптические диски, магнитные ленты). Если размер созданной резервной копии много меньше размера носителя, то имеет смысл сохранить на него и другие копии, которые будут создаваться в будущем. Но если говорится о файлах, то желательно придерживаться правила «один файл — одна копия», т.е. в одном файле Bacula должны храниться резервные данные, которые были сформированы в рамках выполнения одного задания. Для каждого последующего будут создаваться новые файлы.

4) Volume Retention — время, по прошествии которого данные о резервной копии, хранящейся на носителе, будут удалены из каталога. Для обеспечения работоспособности Bacula необходимо помнить о том, что информация обо всех зарезервированных файлах хранится в БД, по записи на каждый файл. Если резервируются тысячи файлов, то очень скоро БД станет огромной, что может затруднить работу Bacula. Поэтому очень важно своевременно очищать базу от устаревшей инфор-

мации. При этом сам носитель информации не будет очищен автоматически. Он будет промаркирован как устаревший, но всегда можно будет использовать его для восстановления данных в ручном режиме.

5) `Maximum Volumes` — максимальное количество носителей (в нашем случае файлов), доступных в данном пуле. Параметр `Recycle` указывает на необходимость повторного использования носителей, помеченных как устаревшие. При этом реальная перезапись носителя произойдет лишь в случае, когда свободных носителей не останется. Свободные носители определяются из параметра `Maximum Volumes`.

6) Параметр `AutoPrune` указывает на то, необходимо ли производить удаление устаревших записей из `Bacula Catalog` автоматически после завершения выполнения очередного задания.

7) Параметр `Label Format` определяет префикс, который будет использован Bacula для маркирования носителей информации, в нашем случае — для именования файлов.

8) Параметр `Storage` указывает на имя устройства хранения данных, указанного в параметре `Name` секции `Storage` файла `bacula-dir.conf`.

```
Pool {
Name = Default
Pool Type = Backup
Recycle = yes # Bacula can automatically recycle Volumes
AutoPrune = yes # Prune expired volumes
Volume Retention = 1 month # one year
Maximum Volume Jobs = 1
Maximum Volumes = 32
Storage = File
Label Format = "volume-"
}
```

Секция `FileSet` позволяет предопределить несколько наборов резервируемых файлов. Например, один набор для Windows, другой — для Linux или один для серверов, а другой — для рабочих станций. Параметр `Name` определяет уникальное имя набора.

Секция `Include` содержит пути к резервируемым файлам/каталогам, а `Exclude` — пути к файлам и каталогам, которые необходимо исключить из списка резервируемых. В секции `Include` возможна секция `Options`, в которой определяются параметры резервирования. Основные параметры:

1) Параметр `signature` указывает алгоритм вычисления контрольных сумм файлов.

2) Параметр `compression` указывает алгоритм компрессии файлов.

3) Параметр `recurse` указывает на необходимость рекурсивного резервирования, включая подкаталоги и файлы.

4) Параметр `File` указывает на каталог, который мы копируем.

5) Параметр `xattrsupport` указывает на возможность включения поддержки расширенных атрибутов, это обязательный параметр для работы с мандатными метками.

```
FileSet {
Name = "Catalog"
Include {
Options {
signature = MD5
compression = GZIP
# recurse = yes
aclsupport = yes
xattrsupport = yes
}
File = /etc
}
}
```

Все настройки связываются воедино с помощью секции `Job`, в которой дается задание планировщику по выполнению резервирования данных. Основные параметры:

1) Параметр `Type` указывает на тип задания. Типов существует несколько. Здесь достаточно указать `Backup`.

2) Параметр `Schedule` указывает на предопределенное расписание, согласно которому будет выполняться резервирование данных. Все расписания определены здесь же, в файле `bacula-dir.conf`.

3) Параметр `Where` указывает на каталог, в котором будут восстанавливаться данные из резервной копии.

4) Параметр `Write Bootstrap` указывает путь к файлу, в который будет записываться информация, с помощью которой данные могут быть восстановлены из резервной копии без наличия подключения к `Bacula Catalog`. Вместо `%n` будет подставлено значение параметра `Name`.

```
Schedule {
Name = "DailyCycle"
Run = Full daily at 16:10
# Run = Differential 2nd-5th sun at 23:05
```

```
        Run = Incremental mon-sat at 23:05
        }

        Job {
        Name = "RestoreFiles"
        Type = Restore
        Client= bacula-fd
        FileSet="Catalog"

        Storage = File
        Pool = Default
        Messages = Standard
        Where = /etc2
        }

        Job {
        Name = "BackupCilent1"
        Type = Backup
        Client = bacula-fd
        FileSet = "Catalog"
        Schedule = "DailyCycle"
        Messages = Standard
        Pool = Default
        Write Bootstrap = "/var/lib/bacula/Client1.bsr"
        Priority = 1
        }
```

Теперь необходимо указать параметры единственного Агента.

```
Client {
Name = bacula-fd
Address = 11.11.11.23
FDPort = 9102
Catalog = MyCatalog
Password = "1" # password for FileDaemon
File Retention = 30 days # 30 days
Job Retention = 6 months # six months
AutoPrune = yes # Prune expired Jobs/Files
}
```

Теперь необходимо закомментировать все остальные секции: Job, JobDefs, Client и Console, на данном этапе они не понадобятся. Трафик данных будет идти по тем портам, что указаны в конфигурационных файлах каждого из компонентов Bacula.

Далее необходимо настроить доступ к DD со стороны Bacula Console в файле /etc/bacula/bconsole.conf сервера bakula1.my.dom:

```
Director {
Name = bacula-dir
DIRport = 9101
address = 11.11.11.21
Password = "1"
}
```

На машине, где будет Director Daemon следует удалить пакеты bacula-sd и bacula-fd:

```
apt-get remove bacula-sd
apt-get remove bacula-fd
```

Конфигурационные файлы bacula-sd и bacula-fd в /etc/bacula следует либо переименовать, либо удалить. Сервисы bacula-sd и bacula-fd следует остановить:

```
/etc/init.d/bacula-sd stop
/etc/init.d/bacula-fd stop
```

9.3.2.2. Настройка Storage Daemon

Далее необходимо начать подготовку Storage Daemon, который будет отвечать за непосредственную работу с устройством хранения данных. Bacula поддерживает широкий спектр устройств, начиная от оптических дисков и заканчивая полнофункциональными ленточными библиотеками. В примере самый распространенный вариант — обычный жесткий диск с существующей файловой системой (например, ext3). Итак, на сервере bakula2.my.dom необходимо отредактировать файл /etc/bacula/bacula-sd.conf. В секции основных параметров — Storage необходимо определить параметр Name, который задает уникальное имя Storage Daemon. Остальные параметры можно оставить в значениях по умолчанию.

Секция Director необходима для указания уникального имени DD и пароля, с которым этот DD может подключаться к SD. Секций может быть несколько, что дает возможность использовать единый сервер хранения данных для нескольких систем резервирования. Все остальные секции Director, найденные в файле, необходимо закомментировать.

```
Storage { # definition of myself
Name = bacula-sd
SDPort = 9103 # Director's port
WorkingDirectory = "/var/lib/bacula"
```

```
Pid Directory = "/var/run/bacula"
Maximum Concurrent Jobs = 20
SDAddress = 11.11.11.22
}

Director {
Name = bacula-dir
Password = "1"
}
```

Но основные настройки, определяющие взаимодействие с устройствами хранения, находятся в секции `Device`. Ниже приведены параметры, необходимые для хранения резервных копий в рамках существующей ФС, подключенной в каталог `/back`:

1) Параметр `Name` определяет уникальное имя подключенного устройства. Если планируется создавать изолированные друг от друга резервные копии для каждого из `File Daemon`, то необходимо создать несколько секций `Device` с уникальными именами. В противном случае резервируемые файлы со всех `FD` будут размещаться в одном и том же файле, что может затруднить дальнейшее обслуживание системы.

2) Параметр `Media Type` определяет произвольное уникальное имя, которое будет использоваться Bacula при восстановлении данных. Согласно ему определяется устройство хранения, с которого будет производиться восстановление. Если резервные копии хранятся в файлах, то для каждой секции `Device` должен быть задан уникальный `Media Type`.

3) Параметр `Archive Device` указывает путь к файлу устройства в каталоге `/dev` или путь к каталогу, в котором будут размещаться резервные копии.

4) Параметр `Device Type` определяет тип устройства. Для размещения в существующей ФС указывается `File`.

5) Параметр `Random Access` указывает на возможность случайной (непоследовательной) адресации. Для файлов указывается `Yes`.

6) Параметр `RemovableMedia` указывает, возможно ли извлечение устройства хранения. Необходимо для ленточных устройств, приводов оптических дисков и т.д. Для файлов устанавливается в значение `No`. Параметр `LabelMedia` указывает на необходимость автоматического маркирования носителей информации.

```
Device {
Name = FileStorage
Media Type = File
Archive Device = /back
```

```
LabelMedia = yes; # lets Bacula label unlabeled media
Random Access = Yes;
AutomaticMount = yes; # when device opened, read it
RemovableMedia = no;
AlwaysOpen = no;
}
```

Для базовой настройки этого достаточно.

На машине, где будет Storage Daemon следует удалить пакет bacula-fd:

```
apt-get remove bacula-fd
```

Конфигурационный файл bacula-fd в /etc/bacula следует либо переименовать, либо удалить. Сервис bacula-fd следует остановить:

```
/etc/init.d/bacula-fd stop
```

9.3.2.3. Настройка File Daemon

Для настройки File Daemon на рабочей станции bakula3.my.dom используется файл /etc/bacula/bacula-fd, в котором для базовой настройки достаточно лишь определить параметры секции Director, где указывается пароль, который будет использовать DD при подключении к FD, а также секции FileDaemon, где указываются настройки FD. Все остальные секции Director, найденные в файле, необходимо закомментировать.

```
Director {
Name = bacula-dir
Password = "1"
}
```

В секции FileDaemon на данном этапе необходим только параметр Name, в котором указывается уникальное имя File Daemon:

```
FileDaemon { # this is me
Name = bacula-fd
FDport = 9102 # where we listen for the director
WorkingDirectory = /var/lib/bacula
Pid Directory = /var/run/bacula
Maximum Concurrent Jobs = 20
FDAddress = 11.11.11.23
}
```

На машине, где будет File Daemon следует удалить пакет bacula-sd:

```
apt-get remove bacula-sd
```

Конфигурационный файл bacula-sd в /etc/bacula следует либо переименовать, либо удалить.

Сервис bacula-sd следует остановить:

```
/etc/init.d/bacula-sd stop
```

Далее необходимо запустить все компоненты соответствующими командами, данными на соответствующих серверах:

```
/etc/init.d/bacula-director restart
/etc/init.d/bacula-sd restart
/etc/init.d/bacula-fd restart
```

После этого Bacula будет работать. Управление Bacula осуществляется через `bconsole`. Настройки каталогов, заданий, расписаний и прочие задаются в конфигурационных файлах.

9.3.2.4. Проверка Bacula

Для тестовой проверки необходимо:

– выполнить `bconsole`;

– выполнить `run`;

– выбрать `job 1`;

– войти в меню, набрав `mod`;

– выбрать `1` (Level);

– выбрать `1` (Full);

– подтвердить выполнение, набрав `yes`.

Будет создана резервная копия данных в каталоге `/back` на машине с `Storage Daemon`.

Для восстановления объектов ФС с установленными мандатными атрибутами необходимо запустить консоль управления `Bacula` с PARSEC-привилегией 0x1000, выполнив команду:

```
sudo execaps -c 0x1000 -- bconsole
```

Для восстановления данных из резервной копии необходимо:

– выполнить `restore`;

– выбрать пункт `12`;

– ввести номер `job id`;

– указать параметр маркировки `mark *`;

– подтвердить выполнение командой `done`.

Данные из резервной копии будут восстановлены в каталоге `/etc2` на машине с `File Daemon`.

Также управление Bacula возможно с помощью графической утилиты `bacula-console-qt`.

9.4. Утилита rsync

Утилита rsync предназначена для удаленного копирования (резервного копирования) или синхронизации файлов и каталогов, с минимальными затратами трафика.

Все действия выполняются от имени учетной записи администратора с использованием механизма sudo.

В таблице 48 приведены некоторые наиболее часто используемые опции команды rsync.

Таблица 48

Опция	Назначение
-v, --verbose	Подробный вывод
-z, --compress	Сжимать трафик
-r, --recursive	Выполнять копирование рекурсивно
-p, --perms	Сохранять дискретные права доступа
-t, --times	Сохранять время доступа к файлам
-g, --group	Сохранять группу
-o, --owner	Сохранять владельца
-A, --acls	Сохранять списки контроля доступа ACL (включает -p)
-X, --xattrs	Сохранять расширенные атрибуты (в том числе мандатные атрибуты)

Подробное описание команды приведено в man rsync.

Пример

Следующая команда сделает копию домашней директории на 192.168.0.1

```
sudo rsync -vzrptgoAX /home/ admin@192.168.0.1:/home_bak
```

В данном примере должна быть создана директория /home_bak на сервере и провешены на нее максимальные метки с ccnr.

ВНИМАНИЕ! Не рекомендуется использовать опцию -l для копирования символических ссылок при создании резервной копии домашних каталогов пользователей.

9.5. Утилита tar

Утилита tar (4.2.1.1) предназначена для архивирования файлов и каталогов.

Все действия выполняются от имени учетной записи администратора с использованием механизма sudo.

Подробное описание команды приведено в man tar.

Далее приведены примеры создания и восстановления резервных копий с использованием утилиты tar.

ВНИМАНИЕ! Предполагается, что уже создан пользователь user1, для которого

заданы мандатные атрибуты и пользователь уже выполнял вход в систему.

Создание администратором архива домашнего каталога пользователя может быть выполнено с помощью команды:

```
sudo tar --xattrs --acls -cvzf /opt/home.tgz /home/.pdp/user1
```

Опция `--xattrs` означает включение поддержки расширенных атрибутов. Опция `--acls` означает включение поддержки POSIX ACL. Опции `-cvzf` необходимы для создания архива (`create`), включения режима отображения обрабатываемых файлов (`verboze`), применения метода сжатия (`gzip`), указания файла (`file`) соответственно. Путь `/opt/home.tgz` задает место расположения созданного архива и его имя, путь `/home/.pdp/user1` определяет, что именно будет вложено в архив.

Восстановление выполняется с помощью команды:

```
sudo execaps -c 0x1000 -- tar --xattrs
    --xattrs-include=security.{PDPL,AUDIT,DEF_AUDIT}
    --acls -xvf /opt/home.tgz -C /opt/home2/
```

Опция `--xattrs-include=security.{PDPL,AUDIT,DEF_AUDIT}` определяет подключаемый шаблон восстановления расширенных атрибутов (мандатных атрибутов, атрибутов аудита и атрибутов аудита по умолчанию) для ключа `xattrs`. Опции `-xvf` необходимы для извлечения из архива (`extract`), включения режима отображения обрабатываемых файлов (`verboze`), указания файла (`file`) соответственно.

10. ЗАЩИЩЕННЫЙ КОМПЛЕКС ПРОГРАММ ПЕЧАТИ И МАРКИРОВКИ ДОКУМЕНТОВ

Одним из основных сервисов, предоставляемых ОС, является сервис печати, позволяющий осуществлять печать документов в соответствии с требованиями, предъявляемыми к защищенным ОС.

Защищенный комплекс программ печати и маркировки документов обеспечивает:

– управение заданиями, выдаваемыми на печать;

– выполнение команд администра печати;

– предоставление информации о состоянии принтеров локальным и удаленным программам;

– выдачу информационных сообщений пользователям.

Предварительная настойка защищенного комплекса программ печати и маркировки документов должна выполняться от имени учетной записи администратора с использованием механизма `sudo`. В дальнейшем ряд действий по администрированию CUPS (добавление и удаление принтеров, изменение политики для принтера, установка мандатных атрибутов для принтера) может выполняться от имени пользователя, входящего в группу администраторов печати, указанную в значении параметра `SystemGroup` в файле `/etc/cups/cups-files.conf` (по умолчанию `lpadmin`).

10.1. Устройство системы печати

В ОС используется система печати CUPS, которая:

– управляет заданиями на печать;

– исполняет административные команды;

– предоставляет информацию о состоянии принтеров локальным и удаленным программам;

– информирует пользователей, если это требуется.

Планировщик — это сервер, который управляет списком доступных принтеров и направляет задания на печать, как требуется, используя подходящие фильтры и выходные буферы (backends).

Файлами конфигурации являются:

– файл конфигурации сервера;

– файлы определения принтеров и классов;

– типы MIME и файлы правил преобразования;

– файлы описания PostScript-принтеров (PPD).

Конфигурационный файл сервера очень похож на файлы конфигурации web-сервера и определяет все свойства управления доступом.

Файлы описания принтеров и классов перечисляют доступные очереди печати и классы. Классы принтеров — наборы принтеров. Задания, посланные классу принтеров, направляются к первому доступному принтеру данного класса.

Очередь печати — механизм, который позволяет буферизовать и организовать задания, посылаемые на принтер. Необходимость организации такого механизма обуславливается тем, что принтер является медленно действующим устройством, и задания не могут быть распечатаны мгновенно. Очевидно, что в многопользовательской среде возникает конкуренция со стороны пользователей при доступе к принтерам, поэтому задания необходимо располагать в очереди. Для этого используется буферный каталог `/var/spool/cups/`.

Файлы типов MIME перечисляют поддерживаемые MIME-типы (`text/plain`, `application/postscript` и т. д.) и правила для автоматического обнаружения формата файла. Они используются сервером для определения поля `Content-Type` для GET- и HEAD-запросов и обработчиком запросов IPP, чтобы определить тип файла.

Правила преобразования MIME перечисляют доступные фильтры. Фильтры используются, когда задание направляется на печать, таким образом, приложение может послать файл удобного (для него) формата системе печати, которая затем преобразует документ в требуемый печатный формат. Каждый фильтр имеет относительную «стоимость», связанную с ним, и алгоритм фильтрования выбирает набор фильтров, который преобразует файл в требуемый формат с наименьшей общей «стоимостью».

Файлы PPD описывают возможности всех типов принтеров. Для каждого принтера имеется один PPD-файл. Файлы PPD для не-PostScript-принтеров определяют дополнительные фильтры посредством атрибута `cupsFilter` для поддержки драйверов принтеров.

В ОС стандартным языком описания страниц является язык PostScript. Большинство прикладных программ (редакторы, браузеры) генерируют программы печати на этом языке. Когда необходимо напечатать ASCII-текст, программа печати может быть ASCII-текстом. Имеется возможность управления размером шрифтов при печати ASCII-текста. Управляющая информация используется для контроля доступа пользователя к принтеру и аудита печати. Также имеется возможность печати изображений в форматах GIF, JPEG, PNG, TIFF и документов в формате PDF.

Фильтр — программа, которая читает из стандартного входного потока или из файла, если указано его имя. Все фильтры поддерживают общий набор опций, включающий имя принтера, идентификатор задания, имя пользователя, имя задания, число копий и опции задания. Весь вывод направляется в стандартный выходной поток.

Фильтры предоставлены для многих форматов файлов и включают, в частности, фильтры файлов изображения и растровые фильтры PostScript, которые поддерживают принтеры, не относящиеся к типу PostScript. Иногда несколько фильтров запускаются параллельно для получения требуемого формата на выходе.

Программа `backend` — это специальный фильтр, который отправляет печатаемые данные устройству или через сетевое соединение. В состав системы печати включены фильтры для поддержки устройств, подключаемых с помощью параллельного и последовательного интерфейсов, а также шины USB.

Клиентские программы используются для управления заданиями и сервером печати.

Управление заданиями включает:

– формирование;

– передачу серверу печати;

– мониторинг и управление заданиями в очереди на печать.

Управление сервером включает:

– запуск/остановку сервера печати;

– запрещение/разрешение постановки заданий в очередь;

– запрещение/разрешение вывода заданий на принтер.

Основные пользовательские настройки содержатся в файлах конфигурации `client.conf` и `~/.cups/lpoptions`.

В общем случае вывод данных на принтер происходит следующим образом:

1) программа формирует запрос на печать задания к серверу печати;

2) сервер печати принимает подлежащие печати данные, формирует в буферном каталоге файлы с содержимым задания и файлы описания задания, при этом задание попадает в соответствующую очередь печати;

3) сервер печати просматривает очереди печати для незанятых принтеров, находит в них задания и запускает конвейер процессов, состоящий из фильтров и заканчивающийся выходным буфером, информация из которого поступает в принтер посредством драйверов ОС;

4) контроль и мониторинг процесса печати выполняется с помощью программ `lpq`, `lpc`, `lprm`, `lpstat`, `lpmove`, `cancel`, а также с помощью графической утилиты `fly-admin-printer`.

Система печати ОС решает следующие задачи:

1) монопольная постановка задания в очередь на печать. Данная функция предполагает невозможность вывода документа на печать в обход системы печати;

2) маркировка каждого напечатанного листа. Каждый лист сопровождается автома-

тической маркировкой (учетными атрибутами документа).

ВНИМАНИЕ! Для обеспечения нормальной работы пользователя с сетевыми сервисами должны быть явно заданы диапазоны его мандатных уровней и категорий с помощью соответствующих утилит, даже если ему не доступны уровни и категории выше 0. Дополнительная информация приведена в пункте «Средства управления мандатными ПРД» документа РУСБ.10015-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1».

10.2. Настройка для работы с локальной базой безопасности

Для удаленного использования сервера печати от имени администратора через механизм `sudo` необходимо:

1) выполнить следующие команды:

```
cupsctl --remote-admin --remote-printers --remote-any
cupsctl ServerAlias=*
cupsctl DefaultAuthType=Basic
```

2) осуществить перезапуск сервера системы печати, выполнив команды:

```
service cups stop
service cups start
```

В файле конфигурации клиента `client.conf` должен быть задан один параметр `ServerName`, определяющий имя сервера печати, например:

```
ServerName computer.domain
```

10.3. Настройка для работы в ЕПП

Для работы системы печати в ЕПП необходимо выполнение следующих условий:

1) наличие в системах, на которых функционируют сервер и клиенты системы печати, установленного пакета клиента ALD — `ald-client`;

2) разрешение имен должно быть настроено таким образом, чтобы имя системы разрешалось, в первую очередь, как полное имя (например, `myserver.example.ru`);

3) клиент ALD должен быть настроен на используемый ALD домен (см. 6.6.3).

Для проведения операций по настройке ALD и администрированию Kerberos необходимо знание паролей администраторов ALD и Kerberos.

10.3.1. Сервер

Для обеспечения совместной работы сервера печати с ALD необходимо, чтобы сервер печати функционировал как сервис Kerberos. Выполнение данного условия требует наличия в БД Kerberos принципала для сервера печати, имя которого задается в формате:

```
servicename/hostname@realm
```

Для выполнения действий по управлению принтерами и очередями печати необходимо создать в ALD учетную запись группы администраторов печати, например, выполнив команду:

```
ald-admin group-add print_admins
```

ВНИМАНИЕ! Имя учетной записи для группы администраторов печати не должно совпадать с именами локальных групп на сервере печати.

Ряд действий по администрированию CUPS (добавление и удаление принтеров, изменение политики для принтера, установка мандатных атрибутов для принтера) может выполняться от имени пользователя, входящего в группу администраторов печати, указанную в значении параметра `SystemGroup` в файле `/etc/cups/cups-files.conf` (по умолчанию `print_admins`). Редактирование указанного файла должно выполняться от имени учетной записи администратора с использованием механизма `sudo`.

Создать в ALD учетную запись администратора печати и добавить ее в группу администратор печати ALD, например, выполнив команды:

```
ald-admin user-add ald_print_admin
ald-admin group-mod print_admins --add-users --user=ald_print_admin
```

Для обеспечения совместной работы сервера печати с ALD необходимо:

1) создать в БД ALD с помощью утилиты администрирования ALD принципала, соответствующего серверу печати. Принципал создается с автоматически сгенерированным случайным ключом:

```
ald-admin service-add ipp/server.my_domain
```

2) ввести созданного принципала в группу сервисов `mac`, используя следующую команду:

```
ald-admin sgroup-svc-add ipp/server.my_domain --sgroup=mac
```

3) создать файл ключа Kerberos для сервера печати с помощью утилиты администрирования ALD `ald-client`, используя следующую команду:

```
ald-client update-svc-keytab ipp/server.my_domain
```

4) от имени учетной записи администратора с использованием механизма `sudo` выполнить следующие команды:

```
cupsctl --remote-admin --remote-printers --remote-any
cupsctl ServerAlias=*
cupsctl DefaultPolicy=default
cupsctl MarkerUser=ipp
cupsctl ServerName=server.my_domain
cupsctl MacEnable=On
cupsctl DefaultAuthType=Negotiate
```

5) от имени учетной записи администратора с использованием механизма `sudo` в конфигурационном файле `/etc/cups/cupsd.conf` рекомендуется удалить следу-

ющие строки:

```
Port 631
Listen /var/run/cups/cups.sock
```

и вставить следующую строку:

```
Listen 0.0.0.0:631
```

6) осуществить перезапуск сервера системы печати, выполнив команды:

```
service cups stop
service cups start
```

Подробная информация по маркировке документов приведена в 10.4. Информация о печати нескольких копий документов с ненулевым мандатным уровнем приведена в 10.5.

Далее выполнить вход на сервере печати от имени учетной записи, входящей в группу ALD `print_admins`, и настроить принтеры. Настройка принтеров может быть выполнена с использованием утилиты `fly-admin-printer` (см. электронную справку). После запуска утилиты необходимо указать, что для выполнения привилегированных действий не используется учетная запись `root`, и затем выполнять действия по настройке.

Дополнительная информация по системе печати приведена в разделе 10.

10.3.2. Клиент

Общие условия, при которых обеспечивается совместное функционирование клиентов системы печати с ALD, см. в 10.3. Кроме того, сервер печати должен быть также настроен соответствующим образом (см. 10.3.1). Для настройки клиента системы печати необходимо:

1) создать конфигурационный файл `/etc/cups/client.conf`;

2) задать в конфигурационным файле `/etc/cups/client.conf` для параметра `ServerName` в качестве значения имя сервера системы печати, например, `server.my_domain`.

10.4. Маркировка документов

Маркировка печатных листов осуществляется «наложением» маркеров с учетными атрибутами документа, включающими:

– уровень конфиденциальности документа;
– номер экземпляра;
– количество листов в экземпляре;
– дату вывода документа на печать;
– номер каждого входящего документа;
– имя исполнителя;
– имя пользователя, производившего печать на станции печати.

Система печати является инвариантной по отношению к приложениям, которые обращаются к сервису печати. Это означает, что приложения, выводящие на печать, должны учитывать маркировку листов и оставлять для этого свободное место. В противном случае маркеры могут затереть фрагменты печатаемой информации.

В каталогах `/usr/share/cups/psmarker` и `/usr/share/cups/fonarik` хранятся файлы с настойками маркеров печати. Настройка элементов маркировки осуществляется редактированием следующих файлов:

– `/usr/share/cups/marker.template` — описание элементов маркера, проставляемых на первой, каждой, последней странице и на обороте последней страницы;

– `/usr/share/cups/psmarker/marker.defs` — описание положения элементов маркера на странице;

– `/usr/share/cups/fonarik/fonarik.defs` — описание положения элементов маркера на обороте последей страницы.

Для изменения положения маркера, проставляемого на первой, каждой и последней странице необходимо в файле `/usr/share/cups/psmarker/marker.defs` изменить значение параметра:

– `MarkerTopShift` — для верхнего элемента маркера;

– `MarkerBottomShift` — для нижнего элемента маркера;

– `MarkerLeftShift` — для левого элемента маркера;

– `MarkerRightShift` — для правого элемента маркера.

Для изменения положения маркера, проставляемого на обороте последней страницы, необходимо в файле `/usr/share/cups/fonarik/fonarik.defs` изменить значение параметра:

– `FonarikTopShift` — для верхнего элемента маркера;

– `FonarikBottomShift` — для нижнего элемента маркера;

– `FonarikLeftShift` — для левого элемента маркера;

– `FonarikRightShift` — для правого элемента маркера.

Любые изменения содержания и формата маркера страниц может производить только администратор через механизм `sudo`. Данная настройка может осуществляется с использованием графической утилиты `fly-admin-marker`.

Для выполнения маркировки должна быть создана группа `lpmac`.

Пользователь, от имени которого будут выполняться команды по маркировке, должен входить в группу `lpmac`.

Для печати документов с ненулевым мандатным контекстом необходимо соответствующим образом настроить принтер. Данная настройка осуществляется с использованием утилиты `fly-admin-printer`. В закладке «МАС» необходимо установить политику

parsec, а также допустимый диапазон мандатных уровней и категорий. Дополнительная информация об утилите fly-admin-printer приведена в электронной справке.

После отправки пользователем на печать документа с ненулевым мандатным контекстом в очереди сервера печати формируется задание.

Для печати документа необходимо выполнить его маркировку. Маркировка выполняется вызовом скрипта markjob, который требует наличия утилиты lpq, входящей в состав пакета cups-bsd.

В процессе выполнения скрипта markjob у пользователя запрашиваются следующие атрибуты маркера:

– mac-inv-num — инвентарный номер;

– mac-owner-phone — телефон исполнителя;

– mac-workplace-id — идентификатор рабочего места;

– mac-distribution — список рассылки.

При вводе списка рассылки адреса разделяются символом '^'. Если в значении списка рассылки используется пробел, то значение атрибута необходимо взять в кавычки целиком.

Примеры:

1. Выдается запрос на ввод списка рассылки

```
Enter mac-distribution - Distribution list, addresses separated by '^':
```

2. Вводится список рассылки

```
"В дело^В адрес"
```

После выполнения маркировки в очереди формируются два дополнительных задания, первое (с меньшим номером) представляет собой промаркированный документ, а второе (с большим номером) — маркировку, размещаемую на обороте последнего листа документа. Необходимо возобновить выполнение первого задания, что приведет к печати промаркированного документа. Затем на обороте последнего листа документа печатается маркировка посредством возобновления выполнения второго дополнительного задания.

При выполнении маркировки от имени пользователя, входящего в группу lpmac, возможно получение сообщения:

```
Невозможно выполнить запрос: запрещено
```

В данном случае необходимо выполнить команду id от имени пользователя, выполняющего маркировку, и повторно запустить скрипт маркировки markjob.

10.5. Печать нескольких экземпляров документа с ненулевым мандатным уровнем

Для печати нескольких экземпляров документа с ненулевым мандатным уровнем пользователь должен отправить на печать только одну копию документа.

Пользователь, осуществляющий маркировку, должен выполнить следующую последовательность действий:

1) получить номер задания для маркировки, выполнив команду:

```
lpq -a
```

2) задать число копий для печати, выполнив команду:

```
lpattr -j <номер_задания> -s copies=<число_копий>
```

3) произвести маркировку, выполнив скрипт `markjob`.

После выполнения маркировки в очереди формируются по два дополнительных задания для каждого экземпляра документа, располагаемых в очереди последовательно. Первое (с меньшим номером) представляет собой промаркированный экземпляр документа, а второе (с большим номером) — маркировку, размещаемую на обороте последнего листа экземпляра документа. Для печати экземпляра документа необходимо возобновить выполнение первого соответствующего ему задания, что приведет к печати промаркированного экземпляра документа. Затем на обороте последнего листа экземпляра документа печатается маркировка посредством возобновления выполнения второго соответствующего экземпляру документа дополнительного задания.

10.6. Установка и настройка принтера

Установку и настройку принтера следует производить после завершения установки и первоначальной настройки ОС.

10.6.1. Общие положения

При печати через локальный сервер печати данные сначала формируются на локальном сервере, как для любой другой задачи печати, после чего посылаются на принтер, подключенный к данному компьютеру.

Вся информация, необходимая для драйвера принтера (используемое физическое устройство, удаленный компьютер и принтер для удаленной печати), содержится в файлах `/etc/cups/printers.conf` и `/etc/cups/ppd/<имя_очереди>.ppd`.

Далее термин «принтер» в этом разделе используется для обозначения принтера, соответствующего одной записи в файле `/etc/cups/printers.conf`. Под термином «физический принтер» подразумевается устройство, с помощью которого производится печать на бумаге. В файле `/etc/cups/printers.conf` может быть несколько записей, описывающих один физический принтер различными способами.

10.6.2. Команды управления печатью

В систему печати ОС включены файлы, предоставляющие командный интерфейс пользователя в стиле BSD и System V (таблица 49).

Таблица 49

Файл	Описание
/usr/bin/lpr	Постановка заданий в очередь. Совместима с командой lpr системы печати BSD UNIX
/usr/bin/lp	Постановка заданий в очередь. Совместима с командой lp системы печати System V UNIX
/usr/bin/lpq	Просмотр очередей печати
/usr/sbin/lpc	Управление принтером. Является частичной реализацией команды lpc системы печати BSD UNIX
/usr/bin/lprm	Отмена заданий, поставленных в очередь на печать
/usr/sbin/cupsd	Сервер печати
/usr/sbin/lpadmin	Настройка принтеров и классов принтеров
/usr/sbin/lpmove	Перемещение задания в другую очередь
/usr/bin/fly-admin-printer	Настройка системы печати, установка и настройка принтеров, управление заданиями

Описание данных команд приведено на страницах руководства man.

CUPS предоставляет утилиты командной строки для отправления заданий и проверки состояния принтера. Команды lpstat и lpc status также показывают сетевые принтеры (принтер@сервер), когда разрешен обзор принтеров.

Команды администрирования System V предназначены для управления принтерами и классами. Средство администрирования (lpc) поддерживается только в режиме чтения для проверки текущего состояния очередей печати и планировщика.

С помощью команды lp выполняется передача задачи принтеру, т. е. задача ставится в очередь на печать. В результате выполнения этой команды файл передается серверу печати, который помещает его в каталог /var/spool/cups/.

Остановить работу сервиса печати можно с помощью команды:

```
service cups stop
```

Запустить сервис печати можно с помощью команды:

```
service cups start
```

10.6.2.1. lpq

Команда lpq предназначена для проверки очереди печати (используемой lpd) и вывода состояния заданий на печать, указанных при помощи номера задания либо системного идентификатора пользователя, которому принадлежит задание. Она выводит для каждого задания имя его владельца, текущий приоритет задания, номер задания и размер

задания в байтах, без параметров выводит состояние всех заданий в очереди.

10.6.2.2. lprm

Команда `lprm` предназначена для удаления задания из очереди печати. Для определения номера задания необходимо использовать команду `lpq`. Для того чтобы удалить задание, необходимо быть его владельцем или администратором печати.

Системные каталоги, определяющие работу системы печати ОС, также содержат файлы, которые не являются исполняемыми:

– `/etc/cups/printers.conf` — содержит описания принтеров в ОС;

– `/etc/cups/ppd/<имя_очереди>.ppd` — содержит описания возможностей принтера, которые используются при печати заданий и при настройке принтеров;

– `/var/log/cups/error_log` — поступает протокол работы принтера. В этом файле могут находиться сообщения об ошибках сервера печати или других программ системы печати;

– `/var/log/cups/access_log` — регистрируются все запросы к серверу печати;

– `/var/log/cups/page_log` — поступают сообщения, подтверждающие успешную обработку страниц задания фильтрами и принтером.

10.6.2.3. lpadmin

Настроить принтер в ОС можно также с помощью команды `lpadmin`.

Ее запуск с опцией `-p` — для добавления или модификации принтера:

```
/usr/sbin/lpadmin -p printer [опции]
```

Основные опции команды `lpadmin` приведены в таблице 50.

Таблица 50

Опция	Описание
`-c class`	Добавляет названный принтер к классу принтеров `class`. Если класс не существует, то он создается
`-m model`	Задает стандартный драйвер принтера, обычно файл `PPD`. Файлы `PPD` обычно хранятся в каталоге `/usr/share/cups/model/`. Список всех доступных моделей можно вывести командой `lpinfo` с опцией `-m`
`-r class`	Удаляет указанный принтер из класса `class`. Если в результате класс становится пустым, он удаляется
`-v device-uri`	Указывает адрес устройства для связи с принтером
`-D info`	Выдает текстовое описание принтера
`-E`	Разрешает использование принтера и включает прием заданий
`-L location`	Выводит расположение принтера
`-P ppd-file`	Указывает локальный файл `PPD` для драйвера принтера

Для данной команды существуют также опции по регулированию политики лимитов

и ограничений по использованию принтеров и политики доступа к принтерам.

Запуск команды `lpadmin` с опцией `-x` — для удаления принтера:

```
/usr/sbin/lpadmin -x printer
```

10.6.2.4. fly-admin-printer

Утилита `fly-admin-printer` предназначена для настройки печати в графическом режиме. Позволяет в режиме администратора печати устанавливать, настраивать и удалять принтеры и классы принтеров, а также настраивать сервер печати и управлять заданиями на печать. В режиме обычного пользователя позволяет устанавливать настройки печати и опции принтера, а также управлять заданиями на печать (удалять, приостанавливать, возобновлять печать и устанавливать отложенную печать). Для вызова привилегированных действий запрашивается авторизация. Подробную информацию по использованию утилиты `fly-admin-printer` см. в электронной справке.

Для установки драйверов принтеров производства Hewlett Packard рекомендуется использовать утилиту `hp-setup`.

10.7. Станция печати документов с маркировкой

Для печати документов с маркировкой используется web-приложение «Управление печатью», расположенное в deb-пакете `printcontrol-web`. Приложение предназначено для управления заданиями на печать и для маркировки документов, отправленных на печать. На каждый документ, отправленный на печать, может быть «наложен» маркер с учетными атрибутами и после этого выполнена печать нескольких экземпляров маркированного документа.

ВНИМАНИЕ! Для печати нескольких экземпляров документа с ненулевым мандатным уровнем пользователь должен отправить на печать только одну копию документа.

Для установки web-приложения «Управление печатью» необходимо выполнить следующие действия:

1) настроить систему печати согласно разделу 10;

2) настроить web-сервер Apache согласно разделу 12)

3) маркировка документов осуществляется от имени пользователя, входящего в группу `lpmac`, поэтому требуется создать группу (если не создана) `lpmac` и внести в нее пользователя, от имени которого будет проходить маркировка документов:

```
groupadd -g 900 lpmac
usermod -a -G lpmac "user"
```

где `user` — имя локального пользователя.

Для ЕПП:

```
ald-admin group-add lpmac --gid=2900 --user="user"
```

где `user` — имя доменного пользователя;

4) установить пакет `printcontrol-web` командой:

```
apt-get install printcontrol-web
```

5) при необходимости подключить модуль web-сервера Apache `php5` и перезапустить сервер:

```
a2enmod php5
/etc/init.d/apache2 restart
```

6) открыть окно браузера и перейти по адресу:

```
server/printcontrol/prog/printcontrol.php
```

где `server` — доменное имя web-сервера Apache.

10.7.1. Запуск Web-приложения «Управление печатью»

После запуска приложения запрашивается аутентификация администратора печати.

Главное окно программы (рис. 3) содержит панель «Управление печатью документов» с рабочей панелью внизу и ссылкой «Просмотр регистрации вывода документов на печать» (10.7.6) вверху справа.

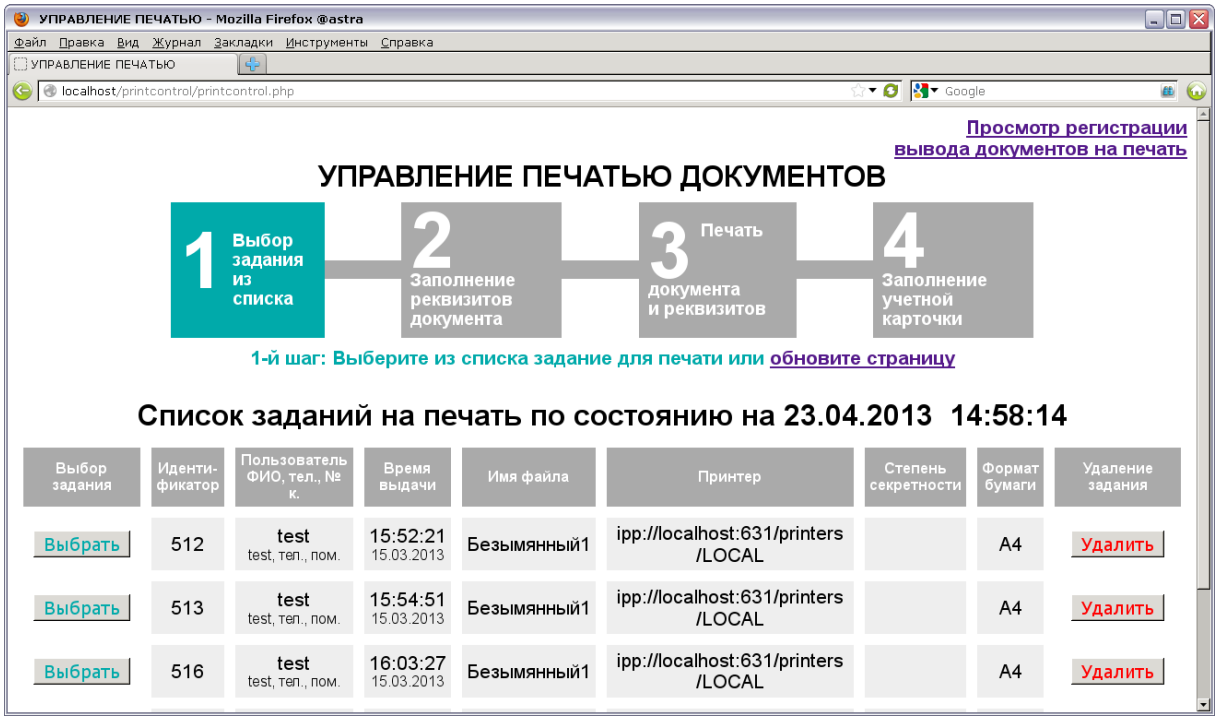


Рис. 3

На панели «Управление печатью документов» схематически в виде отдельных этапов (шагов) отображается порядок управления печатью документов. Этапы выполняются последовательно, начиная с первого (10.7.2). Текущий этап выполнения выделяется цветом, а под схематическим изображением этапов отображается порядковый номер текущего этапа и сопутствующий краткий комментарий. Переход на следующий этап управления осуществляется автоматически.

На рабочей панели внизу отображаются соответствующие этапу сопутствующая информация, параметры для установки и кнопки управления.

10.7.2. Этап 1: выбор задания из списка

На первом этапе выполняется установка элемента из списка заданий на печати.

На рабочей панели (см. рис. 3) в табличном виде отображается список заданий на печать по состоянию на указанную в заголовке таблицы дату и время. Список заданий обновляется каждые пять секунд. Если заданий на печать нет, то появляется сообщение «Заданий на печать нет» и производится автоматический запрос списка заданий на печать.

Для каждого элемента списка (задания) в столбцах таблицы отображаются сведения о задании: идентификатор задания, информация о пользователе, время выдачи, имя файла с документом, указатель ресурса принтера, уровень секретности, формат бумаги. Управляющие кнопки для каждого задания отображаются столбцах таблицы:

– «Выбор задания» – **[Выбрать]**, устанавливается задание на печать и происходит переход ко второму этапу (10.7.3);

– «Удалить» – **[Удалить]**, элемент списка удаляется.

10.7.3. Этап 2: заполнение реквизитов документа

На втором этапе установленный документ и реквизиты для его маркирования при печати отправляются на печать. Реквизиты документа устанавливаются в соответствии с требованиями секретного делопроизводства.

Рабочая панель (рис. 4) содержит:

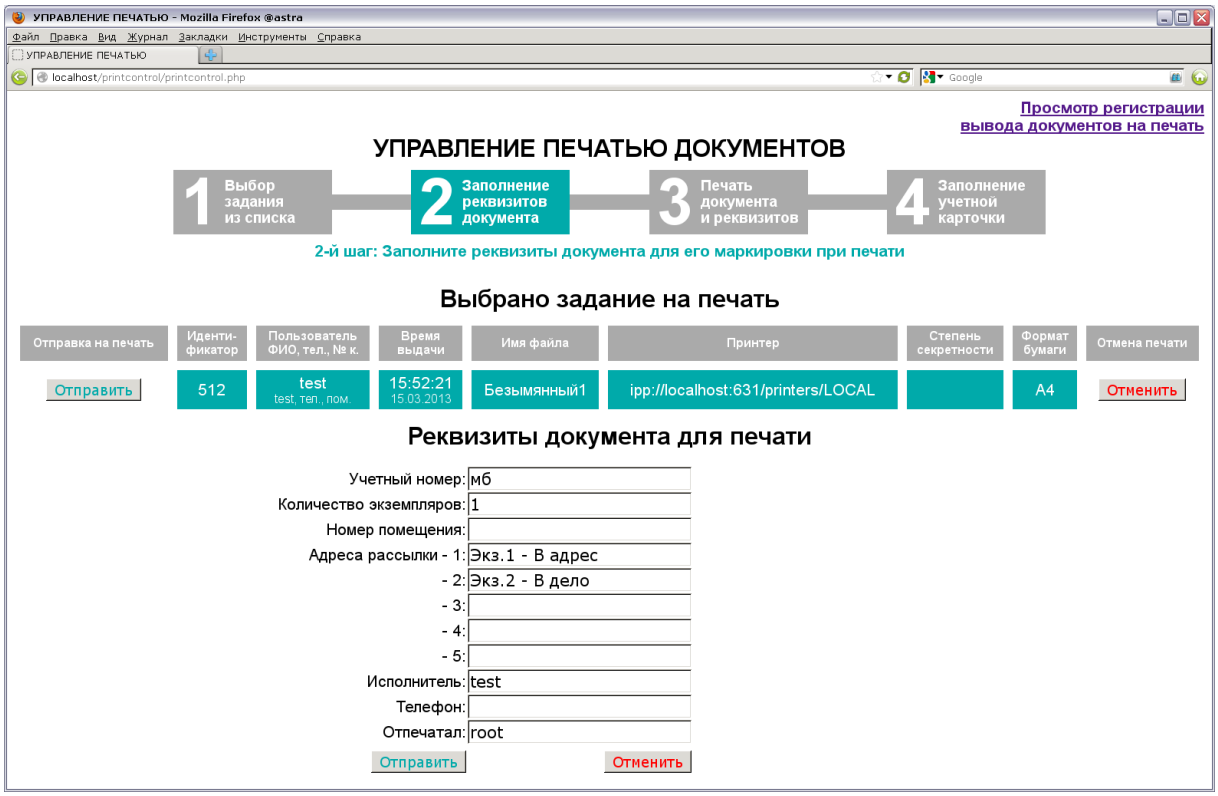


Рис. 4

– «Выбрано задание на печать» – в табличном виде отображаются сведения об установленном задании (см. 10.7.2) и управляющие кнопки в столбцах:

– «Отправить на печать» – **[Отправить]**, установленный документ и установленные реквизиты отправляются на печать и происходит переход к третьему этапу (10.7.4);

– «Отменить» – **[Отменить]**, установленные реквизиты отправляются на печать и происходит переход к третьему этапу(10.7.4);

– «Реквизиты документа для печати»:

– форма со строками ввода, в которых устанавливается:

– «Учетный номер» – учетный номер;

– «Количество экземпляров» – количество экземпляров;

– «Номер помещения» – номера помещения;

– «Адреса рассылки» – до 5 адресов рассылки;

– «Исполнитель» – имя исполнителя документа;

– «Телефон» – номер телефона;

– «Отпечатал» – имя исполнителя печати;

– управляющие кнопки:

– «Отправить на печать» – **[Отправить]**, установленный документ и установленные реквизиты отправляются на печать и происходит переход к третьему этапу (10.7.4) ;

– «Отмена печати» – **[Удалить]**, установленный документ отправляется на печать и происходит переход к третьему этапу (10.7.4).

10.7.4. Этап 3: печать документа и реквизитов

На третьем этапе выполняется выдача на печать установленного количества экземпляров документа и его реквизитов на оборотной стороне последнего листа.

Рабочая панель (рис. 5) содержит:

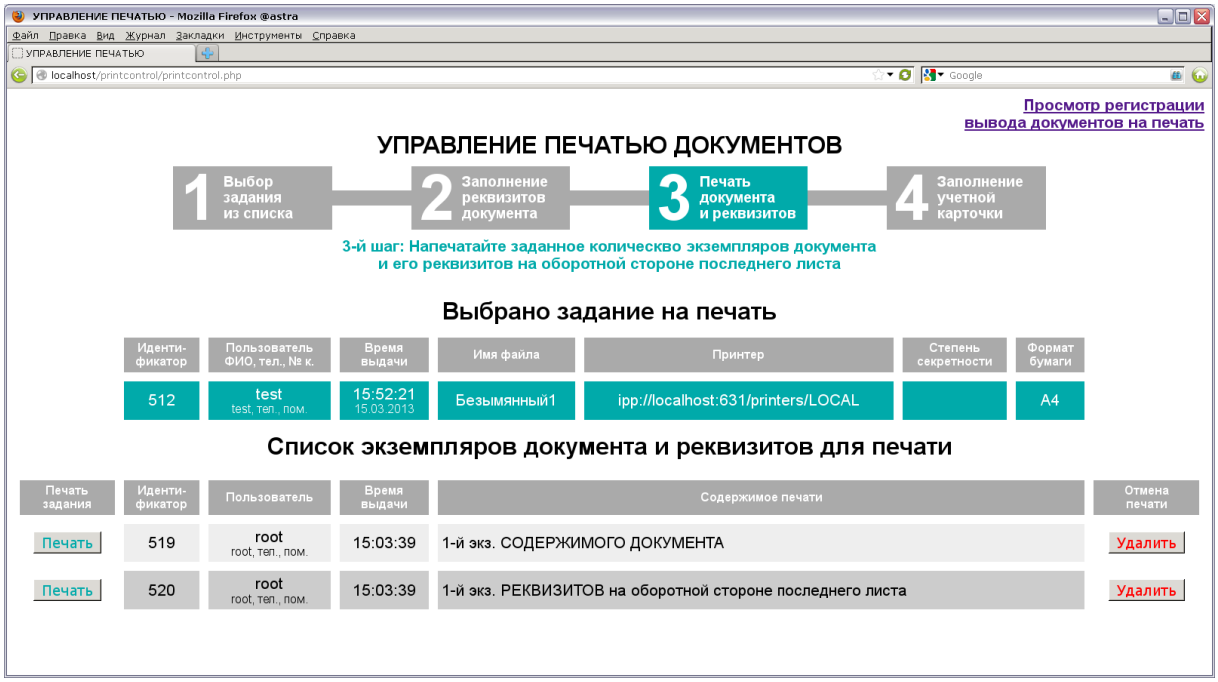


Рис. 5

– «Выбрано задание на печать» – в табличном виде отображается список сведений об установленном задании (см. 10.7.2);

– «Список экземпляров документа и реквизитов для печати» – в табличном виде отображается список экземпляров документа и реквизитов для печати. Для каждого элемента списка в столбцах таблицы отображаются сведения: идентификатор, информация о пользователе, время выдачи и содержимое печати (номер экземпляра документа или его реквизитов). Управляющие кнопки для каждого элемента отображаются столбцах таблицы:

– «Печать задания» – **[Печать]**, выдача на печать соответствующего экземпляра документа или его реквизитов, элемент удаляется из списка;

– «Отмена печати» – **[Удалить]**, элемент удаляется из списка.

После завершения обработки всех элементов списка происходит переход на четвертый этап (10.7.5).

10.7.5. Этап 4: заполнение учетной карточки

На четвертом этапе в соответствии с требованиями секретного делопроизводства заполняются поля учетной карточки документа.

Рабочая панель (рис. 6) содержит:

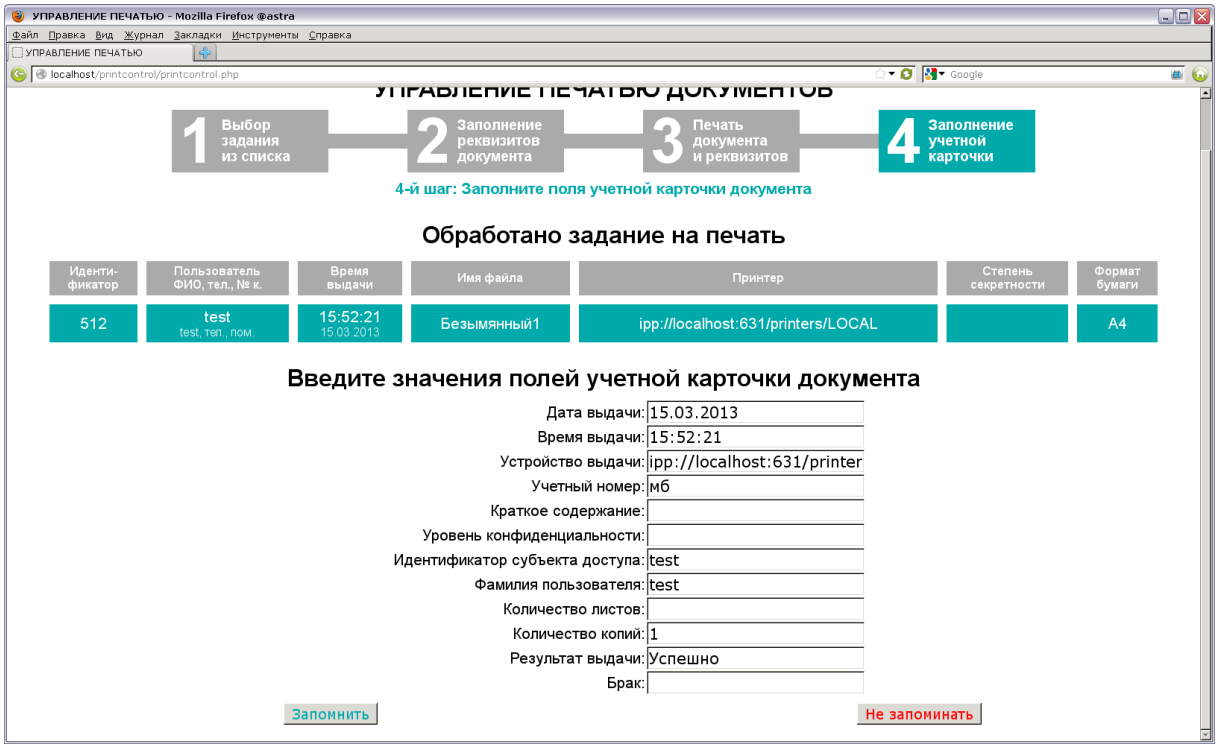


Рис. 6

– «Обработано задание на печать» – в табличном виде отображаются сведения об установленном задании (см. 10.7.2);

– «Введите значения полей учетной карточки документов»:

  – форма со строками ввода, в которых устанавливается:

    – «Дата выдачи» – дата выдачи;

    – «Время выдачи» – время выдачи;

    – «Устройство выдачи» – указатель ресурса принтера;

    – «Учетный номер» – учетный номер документа;

    – «Краткое содержание» – краткий комментарий;

    – «Уровень конфиденциальности» – степень секретности;

    – «Идентификатор субъекта доступа» – идентификатор субъекта доступа;

    – «Фамилия пользователя» – фамилия пользователя;

    – «Количество листов» – количество листов в документе;

    – «Количество копий» – количество экземпляров;

    – «Результат выдачи» – результат выдачи на печать;

    – «Брак» – метка брака;

  – управляющие кнопки:

    – **[Запомнить]** – учетная карточка сохраняется в файле регистрации вывода документов на печать, происходит переход на первый этап (10.7.2);

    – **[Не запоминать]** – происходит переход на первый этап (10.7.2).

10.7.6. Просмотр регистрации вывода документов на печать

Щелчком левой кнопки мыши на ссылке «Просмотр регистрации вывода документов на печать» открывается вкладка, (рис. 7) в которой отображаются записи из журнала регистрации вывода документов на печать.

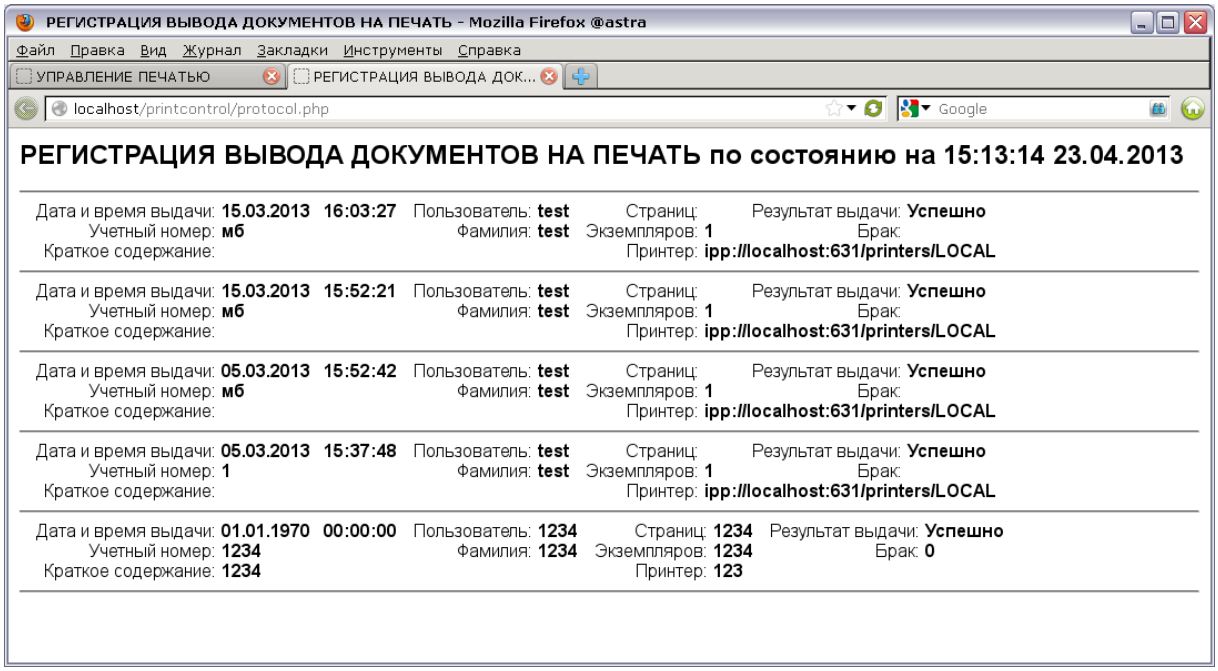


Рис. 7

Для каждого документа указывается дата и время выдачи на печать, учетный номер и краткое содержание, количество страниц и экземпляров для печати, результат выдачи на печать, а также учетное имя и фамилия пользователя и указатель ресурсов принтера.

11. ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

В качестве защищенной СУБД в составе ОС используется PostgreSQL, доработанная в соответствии с требованием интеграции с ОС в части мандатного разграничения доступа к информации.

Примечание. В текущей версии ОС представлены две версии защищенной СУБД (на базе версий СУБД PostgreSQL 9.2 и 9.4), отличающиеся в части реализации мандатного разграничения доступа к информации (см. РУСБ.10015-01 97 01-1).

СУБД PostgreSQL предназначена для создания и управления реляционными БД и предоставляет многопользовательский доступ к расположенным в них данным.

Данные в реляционной БД хранятся в отношениях (таблицах), состоящих из строк и столбцов. При этом единицей хранения и доступа к данным является строка, состоящая из полей, идентифицируемых именами столбцов. Кроме таблиц, существуют другие объекты БД (виды, процедуры и т. п.), которые предоставляют доступ к данным, хранящимся в таблицах.

В связи с большим объемом информации подробное описание работы с защищенной СУБД приведено в отдельном документе РУСБ.10015-01 95 01-2.

12. ЗАЩИЩЕННЫЙ КОМПЛЕКС ПРОГРАММ ГИПЕРТЕКСТОВОЙ ОБРАБОТКИ ДАННЫХ

Защищенный комплекс программ гипертекстовой обработки данных — это ПО, осуществляющее взаимодействие по HTTP-протоколу между сервером и браузерами: прием запросов, поиск указанных файлов и передача их содержимого, выполнение приложений на сервере и передача клиенту результатов их выполнения. Комплекс представлен web-севером Apache2 и браузером Firefox. Web-сервер Apache2, входящий в состав ОС, не допускает возможности анонимного использования ресурсов web-сервера и требует обязательной настройки авторизации пользователей.

ВНИМАНИЕ! Для обеспечения нормальной работы пользователя с сетевыми сервисами должны быть явно заданы диапазоны его мандатных уровней и категорий с помощью соответствующих утилит, даже если ему не доступны уровни и категории выше 0. Дополнительная информация приведена в пункте «Средства управления мандатыми ПРД» документа РУСБ.10015-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1».

12.1. Настройка сервера

После установки сервера необходимо установить пакет `libapache2-mod-auth-pam`. После этого сервер настроен и готов к приему запросов на всех сетевых интерфейсах на 80 порту. Если по каким-то причинам он не работоспособен, следует проверить минимально необходимые настройки сервера. В файле `/etc/apache2/ports.conf` должны быть указаны параметры:

```
NameVirtualHost *:80
Listen 80
```

В каталоге `/etc/apache2/sites-available` должны находиться файлы с настройками виртуальных хостов и как минимум один из них должен быть разрешен к использованию командой:

```
a2ensite config_filename
```

ВНИМАНИЕ! В команде необходимо использовать только имя файла (без указания полного пути).

Минимальное содержимое таких файлов с конфигурациями виртуальных хостов выглядит следующим образом:

```
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        ServerName server.domain.name
        DocumentRoot /path/to/root/dir/
        <Directory /path/to/root/dir/>
                Options Indexes FollowSymLinks MultiViews
```

```
            AllowOverride None
        </Directory>
        ErrorLog /var/log/apache2/error.log
        LogLevel warn
        CustomLog /var/log/apache2/access.log combined
</VirtualHost>
```

В случае когда web-сервер должен предоставлять пользователям доступ к объектам файловой системы с различными мандатными атрибутами, то на корневой каталог виртуального хоста (по умолчанию `/var/www`) и все его родительские каталоги должны быть установлены значения мандатных атрибутов не маньше максимальных атрибутов объектов к которым будет разграничиваться доступ. Кроме того на корневой каталог виртуального хоста (по умолчанию `/var/www`) должен быть установлен тип метки `ccnr`. Операция может быть выполнена с использованием утилиты `pdp-flbl` от имени учетной записи администратора через механизм `sudo`. Дополнительная информация приведена в разделе «Мандатное разграничение доступа» документа РУСБ.10015-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1».

После окончания правки конфигурационных файлов необходимо перезапустить сервер командой:

```
/etc/init.d/apache2 restart
```

12.2. Настройка авторизации

Настройку сквозной аутентификации и авторизации для сервера и клиента, работающих в рамках ЕПП, см. в 12.3. Если не настроена аутентификация через Kerberos, то для всех ресурсов должна использоваться аутентификация и авторизация через PAM, при этом будет использоваться пользовательская БД, прописанная в настройках ОС. Для выполнения аутентификации и авторизации через PAM должен быть установлен пакет `libapache2-mod-auth-pam` и выполнена следующая команда:

```
#a2enmod auth_pam
```

В конфигурационных файлах виртуальных хостов web-сервера Apache2 указать:

```
AuthPAM_Enabled on
AuthType Basic
AuthName "PAM authentication"
require valid-user
```

Логин и пароль пользователя будут передаваться от пользователя к серверу в открытом виде с использованием метода аутентификации Basic. Для корректного функционирования авторизации через PAM пользователю, от которого работает web-сервер (по умолчанию — `www-data`), необходимо выдать права на чтение информации из БД пользо-

вателей и сведений о мандатных метках:

```
#usermod -a -G shadow www-data
#setfacl -d -m u:www-data:r /etc/parsec/macdb
#setfacl -R -m u:www-data:r /etc/parsec/macdb
#setfacl -m u:www-data:rx /etc/parsec/macdb
```

Если установлен модуль web-сервера Apache2 `auth_kerb` из пакета `libapache2-mod-auth-kerb` для аутентификации через Kerberos (см. в 12.3), отключить его использование при помощи команды:

```
a2dismod auth_kerb
```

Сервер для PAM-аутентификации использует сценарий PAM, содержащийся в конфигурационном файле `/etc/pam.d/apache2`. PAM-сценарий включает `common-auth` и `common-account`. По умолчанию в ОС для фиксации числа неверных попыток входа пользователей применяется PAM-модуль `pam_tally`. Использование `pam_tally` в секции `auth` в файле `/etc/pam.d/common-auth` обеспечивает увеличение счетчика неверных попыток входа пользователя при начале процесса аутентификации. Для сброса счетчика неверных попыток входа пользователя после успешной аутентификации необходимо в сценарий PAM, содержащийся в конфигурационном файле `/etc/pam.d/apache2`, добавить использование `pam_tally` в секции `account`. PAM-сценарий для сервера будет иметь следующий вид:

```
@include common-auth
@include common-account
account required pam_tally.so
```

При использовании `pam_tally` необходимо разрешить пользователю `www-data` запись в `/var/log/faillog`, выполнив команду:

```
#setfacl -m u:www-data:rw /var/log/faillog
```

Выполнить перезапуск сервера:

```
#/etc/init.d/apache2 restart
```

12.3. Настройка для работы в ЕПП

Для обеспечения совместной работы web-сервера Apache2 с ALD необходимо:

1) наличие в системе, на которой функционирует web-сервер, установленного пакета клиента ALD — `ald-client`;

2) разрешение имен должно быть настроено таким образом, чтобы имя системы разрешалось, в первую очередь, как полное имя (например, `myserver.example.ru`);

3) клиент ALD должен быть настроен на используемый ALD домен (см. 6.6.3);

4) в системе должен быть установлен модуль web-сервера Apache2 `auth_kerb` из пакета `libapache2-mod-auth-kerb`.

Наличие модуля web-сервера Apache2 auth_kerb предоставляет возможность организации совместной работы с ALD с использованием для аутентификации пользователей посредством Kerberos метода GSSAPI.

Для проведения операций по настройке ALD и администрированию Kerberos необходимо знание паролей администраторов ALD и Kerberos.

Для обеспечения возможности работы web-сервера Apache2 с ALD необходимо:

1) отключить модуль аутентификации через PAM (12.2) web-сервера Apache2 auth_kerb при помощи команды:

```
a2dismod auth_pam
```

2) активировать модуль web-сервера Apache2 auth_kerb при помощи команды:

```
a2enmod auth_kerb
```

3) в конфигурационных файлах виртуальных хостов web-сервера Apache2 в секции <Directory>, для которой настраивается доступ пользователей ЕПП, указать:

```
AuthType Kerberos
KrbAuthRealms REALM
KrbServiceName HTTP/server.my_domain.org
Krb5Keytab /etc/apache2/keytab
KrbMethodNegotiate on
KrbMethodK5Passwd off
require valid-user
```

4) создать в БД ALD с помощью утилиты администрирования ALD принципала, соответствующего настраиваемому web-серверу Apache2. Принципал создается с автоматически сгенерированным случайным ключом:

```
ald-admin service-add HTTP/server.my_domain.org
```

5) ввести созданного принципала в группу сервисов mac, используя следующую команду:

```
ald-admin sgroup-svc-add HTTP/server.my_domain.org
--sgroup=mac
```

6) создать файл ключа Kerberos для web-сервера Apache2 с помощью утилиты администрирования ALD ald-client, используя следующую команду:

```
ald-client update-svc-keytab HTTP/server.my_domain.org
   --ktfile="/etc/apache2/keytab"
```

Полученный файл должен быть доступен web-серверу Apache2 по пути, указанному в конфигурационном параметре Krb5Keytab (в данном случае — /etc/apache2/keytab). Права доступа к этому файлу должны позволять читать его пользователю, от имени которого работает web-сервер Apache2 (как правило, владельцем файла назначается пользователь www-data);

7) сменить владельца, полученного на предыдущем шаге, файла keytab на поль-

зователя www-data, выполнив следующую команду:

```
chown www-data /etc/apache2/keytab
```

8) сделать файл /etc/apache2/keytab доступным на чтение для остальных пользователей:

```
chmod 644 /etc/apache2/keytab
```

9) перезапустить web-сервер Apache2, выполнив команду:

```
/etc/init.d/apache2 restart
```

Браузер пользователя должен поддерживать аутентификацию negotiate. В последних версиях браузера Konqueror данная поддержка присутствует автоматически. В браузере Mozilla Firefox в настройках, доступных по адресу about:config, необходимо указать: для каких серверов доступна аутентификация negotiate. Для выполнения данной настройки необходимо задать маски доменов или в общем случае http- и https-соединения в качестве значений параметра network.negotiate-auth.trusted-uris, вставив, например, значение http://, https://.

При необходимости обеспечения сквозной аутентификации из скриптов с другими службами, например, серверу postgresql, в конфигурационном файле виртуального хоста следует дополнительно указать:

```
KrbSaveCredentials on
```

А в браузере Mozilla Firefox в настройках задать значения, в качестве значений параметра параметра network.negotiate-auth.delegation-uris, маски доменов которым можно передавать данные для сквозной аутентификации. А в запускаемых скриптах выставить переменную окружения KRB5CCNAME. Например, для php это будет выглядеть так:

```
putenv("KRB5CCNAME=".$_SERVER['KRB5CCNAME']);
```

13. ЗАЩИЩЕННЫЙ КОМПЛЕКС ПРОГРАММ ЭЛЕКТРОННОЙ ПОЧТЫ

В качестве защищенного комплекса программ электронной почты используется сервер электронной почты, состоящий из агента передачи электронной почты Exim4, агента доставки электронной почты Dovecot и клиента электронной почты Thunderbird, доработанных для реализации следующих дополнительных функциональных возможностей:

– интеграции с ядром ОС и базовыми библиотеками для обеспечения разграничения доступа;

– реализации мандатного разграничения доступа к почтовым сообщениям;

– автоматической маркировки создаваемых почтовых сообщений, отражающих уровень их конфиденциальности;

– регистрации попыток доступа к почтовым сообщениям.

Агент передачи электронной почты использует протокол SMTP и обеспечивает решение следующих задач:

1) доставку исходящей почты от авторизованных клиентов до сервера, который является целевым для обработки почтового домена получателя;

2) прием и обработку почтовых сообщений доменов, для которых он является целевым;

3) передачу входящих почтовых сообщений для обработки агентом доставки электронной почты.

Агент доставки электронной почты предназначен для решения задач по обслуживанию почтового каталога и предоставления удаленного доступа к почтовому ящику по протоколу IMAP.

Клиент электронной почты — прикладное ПО, устанавливаемое на рабочем месте пользователя и предназначенное для получения, написания, отправки и хранения сообщений электронной почты пользователя.

13.1. Состав

Защищенный комплекс программ электронной почты состоит из следующих пакетов:

– `exim4-daemon-heavy` — агент передачи сообщений СЭП (MTA) Exim4. `exim4-daemon-ligth` не поддерживает работу с мандатными метками, отличными от `0:0`;

– `dovecot-imapd` — агент доставки сообщений СЭП (MDA) Dovecot. Работает только по протоколу IMAP, протокол POP3 отключен. Серверная часть СЭП в защищенном исполнении использует в качестве почтового хранилища MailDir (mailbox не поддерживает работу с мандатными метками, отличными от `0:0`);

– thunderbird — клиент СЭП (MUA) Mozilla Thunderbird.

13.2. Настройка серверной части

Настройки по умолчанию:

1) прием почты по протоколу SMTP, только от MUA из доменов relay-domens и из подсети;

2) отправка почты по протоколу SMTP в соответствии с DNS;

3) хранение локальной почты в MailDir в /var/mail/%u, где %u — локальная часть адресата;

4) выдача локальной почты по протоколу IMAP.

ВНИМАНИЕ! Для обеспечения нормальной работы пользователя с сетевыми сервисами должны быть явно заданы диапазоны его мандатных уровней и категорий с помощью соответствующих утилит, даже если ему не доступны уровни и категории выше 0. Дополнительная информация приведена в пункте «Средства управления мандатыми ПРД» документа РУСБ.10015-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1».

ВНИМАНИЕ! Редактирование конфигурационных файлов и выполнение команд по настройке необходимо выполнять от имени учетной записи администратора с использованием механизма sudo.

13.2.1. Настройка агента доставки сообщений

Настройка агента доставки сообщений СЭП (MDA) Dovecot осуществляется путем правки конфигурационного файла /etc/dovecot/dovecot.conf и конфигурационных файлов в каталоге /etc/dovecot/conf.d.

В файле /etc/dovecot/dovecot.conf необходимо задать список интерфейсов, с которых будут приниматься соединения, и установить протокол IMAP, например:

```
protocols = imap
listen =  192.168.2.55
```

Для настройки аутентификации с использованием PAM в конфигурационном файле /etc/dovecot/conf.d/10-auth.conf необходимо установить:

```
disable_plaintext_auth = no
auth_mechanisms = plain
```

Агент доставки сообщений СЭП (MDA) Dovecot для PAM-аутентификации использует сценарий PAM, содержащийся в конфигурационном файле /etc/pam.d/dovecot. PAM-сценарий для Dovecot включает common-auth и common-account. По умолчанию в ОС для фиксации числа неверных попыток входа пользователей применяется PAM-модуль pam_tally. Использование pam_tally в секции auth в файле /etc/pam.d/common-auth обеспечивает увеличение счетчика неверных попыток входа

пользователя при начале процесса аутентификации. Для сброса счетчика неверных попыток входа пользователя после успешной аутентификации в Dovecot необходимо в сценарий PAM, содержащийся в конфигурационном файле `/etc/pam.d/dovecot`, добавить использование `pam_tally` в секции `account`.PAM-сценарий для Dovecot будет иметь следующий вид:

```
@include common-auth
@include common-account
@include common-session
account required pam_tally.so
```

В случае когда SSL не будет использоваться в конфигурационном файле `/etc/dovecot/conf.d/10-ssl.conf`, необходимо установить:

```
ssl = no
```

Для настройки встроенного в MDA Dovecot сервера SASL, к которому будет обращаться MTA Exim4 для аутентификации пользователей с использованием PAM, в конфигурационном файле `/etc/dovecot/conf.d/10-master.conf` в секцию `service auth` необходимо добавить:

```
unix_listener auth-client {
mode = 0600
user = Debian-exim
}
```

Перезапустить MDA Dovecot, выполнив команду:

```
sudo service dovecot restart
```

13.2.2. Настройка агента передачи сообщений

Для настройки агента передачи сообщений СЭП (MTA) Exim4 требуется инициировать переконфигурирование пакета `exim4-config`, для этого выполнить в эмуляторе терминала команду:

```
sudo dpkg-reconfigure exim4-config
```

В появившемся окне настройки для указанных ниже параметров необходимо установить следующие значения:

– общий тип почтовой конфигурации: интернет-сайт; прием и отправка почты напрямую, используя SMTP;

– почтовое имя системы: `имя_домена`;

– IP-адреса, с которых следует ожидать входящие соединения: `IP-адрес_сервера` (например, `192.168.32.1`);

– другие места назначения, для которых должна приниматься почта: `имя_домена`;

– домены, для которых доступна релейная передача почты: оставить пустым;

– компьютеры, для которых доступна релейная передача почты: оставить пустым;

– сокращать количество DNS-запросов до минимума: Нет;

– метод доставки локальной почты: Maildir — формат в домашнем каталоге;

– разделить конфигурацию на маленькие файлы: Да.

Если возникла необходимость изменить расположение каталога /var/spool/exim4, убедиться, что каталог exim4, подкаталоги db input msglog, файлы db/retry db/retry.lockfileимеют метки безопасности 0:::EHOLE, если это не так, установить соответствующие метки на указанные каталоги и файлы командами:

```
sudo cd new_dir
sudo pdpl-file 0:::EHOLE . db input msglog db/retry db/retry.lockfile
```

Если возникла необходимость изменить расположение каталога хранилища локальной почты /var/mail, убедиться, что на новый каталог установлены права 1777, если это не так, установить командой:

```
sudo chmod 1777 new_dir
```

Для нормальной работы exim4-daemon-heavy необходимо в каталоге /var/mail удалить файл с именем пользователя созданного при установке системы.

В каталоге /etc/exim4/conf.d/auth необходимо создать файл с именем 05_dovecot_login и следующим содержимым:

```
dovecot_plain:
        driver = dovecot
        public_name = plain
        server_socket = /var/run/dovecot/auth-client
        server_set_id = $auth1
```

Для запрета отправки писем без аутентификации в конфигурационном файле /etc/exim4/conf.d/acl/30_exim4-config_check_rcpt в начало секции acl_check_rcpt добавить строки:

```
deny
    message = "Auth required"
    hosts = *:+relay_from_hosts
    !authenticated = *
```

Настройку сквозной авторизации для сервера и клиента, работающих в рамках ЕПП, см. 13.4.

Настроить автоматический запуск службы MTA Exim4, выполнив команду:

```
sudo chkconfig exim4 on
```

Перезапустить MTA Exim4, выполнив команду:

```
sudo service dovecot restart
```

13.3. Настройка клиентский части

Первичное создание для пользователя учетной записи СЭП в MUA Mozilla Thunderbird должно производиться в нулевом мандатном контексте (значение уровня — `0`, категорий — `нет`). Далее для каждого конкретного мандатного контекста (значение уровня и набор категорий) создание учетной записи необходимо повторить.

При создании учетной записи пользователя СЭП в MUA Mozilla Thunderbird необходимо выбрать тип используемого сервера входящей почты IMAP. При настройке учетной записи установить в параметрах сервера и параметрах сервера исходящей почты:

– защита соединения: `Нет`;

– использование метода аутентификации: `Обычный пароль`.

13.4. Настройка для работы в ЕПП

Для обеспечения совместной работы системы обмена сообщениями электронной почты (СЭП) с ALD предлагается использовать ее в следующем составе:

– агент передачи сообщений СЭП (MTA) — Exim4, установленный из пакета `exim4-daemon-heavy`;

– агент доставки сообщений СЭП (MDA) — Dovecot, установленный из пакета `dovecot-imapd`;

– пакет `dovecot-gssapi` поддержки GSSAPI-аутентификации для MDA Dovecot;

– клиент СЭП (MUA) — Mozilla Thunderbird, установленный из пакета `thunderbird`.

Предложенная конфигурация СЭП предоставляет возможность организации совместной работы с ALD с использованием для аутентификации пользователей посредством Kerberos метода GSSAPI на основе встроенного в Dovecot сервера SASL.

Для обеспечения совместной работы СЭП, состоящей из перечисленных выше средств, с ALD необходимо выполнение следующих условий:

1) наличие в системах, на которых функционируют MTA, MDA и MUA, установленного пакета клиента ALD — `ald-client`;

2) разрешение имен должно быть настроено таким образом, чтобы имя системы разрешалось, в первую очередь, как полное имя (например, `myserver.example.ru`);

3) клиент ALD должен быть настроен на используемый ALD домен (см. 6.6.3);

4) в процессе установки MTA Exim4 необходимо указать, что для хранения сообщений электронной почты должен быть использован формат `Maildir` в домашнем каталоге и конфигурация разделена на небольшие файлы.

Для проведения операций по настройке ALD и администрированию Kerberos необходимо знание паролей администраторов ALD и Kerberos.

13.4.1. Сервер

Для обеспечения работы сервера СЭП, включающего MDA Dovecot, установленный из пакета `dovecot-imapd` и настроенный (13.2.1), и MTA Exim4, установленный из пакета `exim4-daemon-heavy` и настроенный (13.2.2), необходимо:

1) создать в БД ALD с помощью утилиты администрирования ALD принципала, соответствующего установленному MDA Dovecot. Принципал создается с автоматически сгенерированным случайным ключом:

```
ald-admin service-add imap/server.my_domain.org
```

2) ввести созданного принципала в группу сервисов `mac`, используя следующую команду:

```
ald-admin sgroup-svc-add imap/server.my_domain.org --sgroup=mac
```

3) ввести созданного принципала в группу сервисов `mail`, используя следующую команду:

```
ald-admin sgroup-svc-add imap/server.my_domain.org --sgroup=mail
```

4) создать файл ключа Kerberos для MDA Dovecot с помощью утилиты администрирования ALD `ald-client`, используя следующую команду:

```
ald-client update-svc-keytab imap/server.my_domain.org
   --ktfile="/var/lib/dovecot/dovecot.keytab"
```

5) создать в БД Kerberos принципала, соответствующего установленному MTA Exim4. Принципал создается с автоматически сгенерированным случайным ключом:

```
ald-admin service-add smtp/server.my_domain.org
```

6) ввести созданного принципала в группу сервисов `mac`, используя следующую команду:

```
ald-admin sgroup-svc-add smtp/server.my_domain.org --sgroup=mac
```

7) ввести созданного принципала в группу сервисов `mail`, используя следующую команду:

```
ald-admin sgroup-svc-add smtp/server.my_domain.org --sgroup=mail
```

8) создать файл ключа Kerberos для MTA Exim4 с помощью утилиты администрирования ALD `ald-client`, используя следующую команду:

```
sudo ald-client update-svc-keytab smtp/server.my_domain.org
  --ktfile="/var/lib/dovecot/dovecot.keytab"
```

9) предоставить пользователю `dovecot` права на чтение файл ключа Kerberos, выполнив команды:

```
sudo setfacl –m u:dovecot:x /var/lib/dovecot
sudo setfacl –m u:dovecot:r /var/lib/dovecot/dovecot.keytab
```

10) в конфигурационном файле `/etc/dovecot/dovecot.conf` отключить использование протоколов POP3, установив:

```
protocols = imap
```

11) в конфигурационном файле /etc/dovecot/conf.d/10-auth.conf установить:

```
auth_krb5_keytab = /var/lib/dovecot/dovecot.keytab
```

12) для отключения передачи при аутентификации пароля открытым текстом в конфигурационном файле /etc/dovecot/conf.d/10-auth.conf установить:

```
disable_plaintext_auth = yes
```

13) для настройки аутентификации посредством Kerberos с использованием метода GSSAPI в конфигурационном файле /etc/dovecot/conf.d/10-auth.conf установить:

```
auth_mechanisms = gssapi
auth_gssapi_hostname = server.my_domain.org
```

14) перезапустить MDA Dovecote, выполнив команду:

```
sudo service dovecot restart
```

15) для настройки аутентификации пользователей в MTA Exim4 посредством Kerberos с использованием метода GSSAPI и встроенного в Dovecot сервера SASL создать конфигурационный файл /etc/exim4/conf.d/auth/33_exim4-dovecot-kerberos-ald со следующим содержимым:

```
dovecot_gssapi:
driver = dovecot
public_name = GSSAPI
  server_socket = /var/run/dovecot/auth-client
server_set_id = $auth1
```

Если раннее MTA Exmin4 был настроен для использования PAM-аутентификации, то необходимо в каталоге /etc/exim4/conf.d/auth удалить файл с именем 05_dovecot_login

16) для запрета отправки писем без аутентификации в конфигурационном файле /etc/exim4/conf.d/acl/30_exim4-config_check_rcpt в начало секции acl_check_rcpt добавить строки:

```
deny
    message = "Auth required"
    hosts = *:+relay_from_hosts
    !authenticated = *
```

17) перезапустить MTA Exim4, выполнив команду:

```
sudo /etc/init.d/exim4 reload
```

13.4.2. Клиент

Для обеспечения возможности работы MUA Mozilla Thunderbird с ЕПП необходимо создать учетную запись пользователя в ALD, например при помощи команды:

```
ald-admin user-add user1
```

Первичное создание для пользователя `user1` учетной записи СЭП в MUA Mozilla Thunderbird должно производится в нулевом мандатном контексте (значение уровня 0, категорий нет). Далее для каждого конкретного мандатного контекста (значение уровня и набор категорий) создание учетной записи необходимо повторить.

При создании учетной записи пользователя СЭП в MUA Mozilla Thunderbird необходимо выбрать тип используемого сервера входящей почты IMAP. При настройке учетной записи:

1) установить в параметре «Защита соединения» для сервера и сервера исходящей почты значение «Нет»;

2) установить в параметрах сервера и параметрах сервера исходящей почты использование метода аутентификации «Kerberos/GSSAPI».

14. СРЕДСТВА КОНТРОЛЯ ЦЕЛОСТНОСТИ

Для решения задач контроля целостности в ОС реализованы:

– средство подсчета контрольных сумм файлов и оптических носителей (14.1);

– средство подсчета контрольных сумм файлов в deb-пакетах (14.2;

– средство контроля соответствия дистрибутиву (14.3);

– средства регламентного контроля целостности (14.4);

– средства создания замкнутой программной среды (14.5).

14.1. Средство подсчета контрольных сумм файлов и оптических носителей

Для подсчета контрольных сумм файлов и оптических носителей в состав ОС включена утилита командной строки `gostsum`. Для вывода информации о ее синтаксисе необходимо выполнить команду:

```
gostsum -h
```

Синтаксис:

```
gostsum [КЛЮЧ]... [ФАЙЛ]
```

Опции приведены в таблице 51.

Таблица 51

Опция	Описание
`--gost-94`	Устанавливает, что будет использован алгоритм ГОСТ Р 34.11-94
`--gost-2012`	Устанавливает, что будет использован алгоритм ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит (по умолчанию)
`--gost-2012-512`	Устанавливает, что будет использован алгоритм ГОСТ Р 34.11-2012 с длиной хэш-кода 512 бит
`-b`	Устанавливает размер блоков, которыми будет считываться файл
`-o`	Задает имя файла для вывода контрольной суммы (по умолчанию — стандартный поток вывода)
`-d`	Задает имя файла устройства чтения оптических дисков (файла с образом оптического диска) для подсчета контрольной суммы
`-t`	Тестирование алгоритмов подсчета контрольных сумм
`-p`	Тестирование алгоритмов подсчета контрольных сумм в многопоточной среде
`-h [--help]`	показать эту справку и выйти

Далее приведен пример подсчета контрольной суммы оптического носителя:

```
gostsum -d /dev/cdrom
```

14.2. Средство подсчета контрольных сумм файлов в deb-пакетах

Для подсчета контрольных сумм файлов в deb-пакетах в состав ОС включена утилита командной строки `gostsum_from_deb`. Для вывода информации о синтаксисе утили-

ты gostsum_from_deb необходимо выполнить команду:

```
gostsum_from_deb -h
```

Синтаксис:

```
gostsum_from_deb [gostsum аргументы] [-d директория] [-p deb-пакет]
```

Опции приведены в таблице 52.

Таблица 52

Опция	Описание
--gost-94	Устанавливает, что будет использован алгоритм ГОСТ Р 34.11-94
--gost-2012	Устанавливает, что будет использован алгоритм ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит (по умолчанию)
--gost-2012-512	Устанавливает, что будет использован алгоритм ГОСТ Р 34.11-2012 с длиной хэш-кода 512 бит
gostsum arguments	Аргументы утилиты gostsum
-d директория	Задает имя каталога, содержащего deb-пакеты, для файлов в которых вычисляются контрольные суммы
-p deb-пакет	Задает имя deb-пакета, для файлов которого вычисляются контрольные суммы

14.3. Средство контроля соответствия дистрибутиву

Средство контроля соответствия дистрибутиву предоставляет возможность для контроля соответствия объектов ФС ОС дистрибутиву ОС. Для обеспечения контроля целостности объектов ФС ОС (в т. ч. СЗИ) в состав дистрибутива входит файл gostsums.txt со списком контрольных сумм по ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит для всех файлов, входящих в пакеты программ дистрибутива. Используя графическую утилиту fly-admin-int-check, можно провести вычисление контрольных сумм файлов системы и проверку соответствия полученных контрольных сумм файлов системы эталонным контрольным суммам. Более подробное описание утилиты см. в электронной справке.

14.4. Средства регламентного контроля целостности

Организация регламентного контроля целостности ОС, прикладного ПО и СЗИ обеспечивается набором программных средств на основе «Another File Integrity Checker». В указанном наборе реализована возможность для проведения периодического (с использованием системного планировщика заданий cron) вычисления контрольных сумм файлов и соответствующих им атрибутов расширенной подсистемы безопасности PARSEC (мандатных атрибутов и атрибутов расширенной подсистемы протоколирования) с последующим сравнением вычисленных значений с эталонными. В указанном наборе программных средств реализовано использование библиотеки libgost, обеспечивающей подсчет кон-

трольных сумм в соответствии с ГОСТ Р 34.11-94.

Эталонные значения контрольных сумм и атрибутов фалов хранятся в БД. База контрольных сумм и атрибутов может быть создана при помощи команды:

```
afick -i
```

Для вычисления контрольных сумм могут использоваться алгоритмы: MD5-Digest, SHA1 и ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит.

14.4.1. Настройка

Для настройки достаточно параметров, которые указаны в конфигурационном файле по умолчанию (`etc/afick.conf`). Кроме различных путей, например, к файлам БД:

```
database:=/var/lib/afick/afick
```

где содержится указание о том, какие файлы/каталоги подвергаются контролю целостности и с какими правилами.

Правило `PARSEC` выглядит следующим образом:

```
PARSEC = p+d+i+n+u+g+s+b+md5+m+e+t
```

где `p+d+i+n+u+g+s+b+md5+m` означает слежение за всеми стандартными атрибутами файла и использование хэш-функции MD5-Digest для слежения за целостностью содержимого файлов. `+e+t` означает контроль расширенных атрибутов: мандатной метки и флагов аудита, соответственно. Контроль ACL осуществляется при установке флага `+g`.

Правило `GOST` выглядит следующим образом:

```
GOST = p+d+i+n+u+g+s+b+gost+m+e+t
```

где `p+d+i+n+u+g+s+b+gost+m` означает слежение за всеми стандартными атрибутами файла и использование хэш-функции ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит для слежения за целостностью содержимого файлов. `+e+t` означает контроль расширенных атрибутов: мандатной метки и флагов аудита, соответственно. Контроль ACL осуществляется при установке флага `+g`.

Правило для каталогов:

```
DIR = p+i+n+u+g
```

Правило означает слежение за правами доступа, метаданными, количеством ссылок и другими стандартными атрибутами (подробнее см. `/etc/afick.conf`).

В файле конфигурации задаются пути к файлам и каталогам, контролируемых `afick`, например:

```
/boot            GOST
/bin        GOST
/etc/security    PARSEC
/etc/pam.d       PARSEC
/etc/fatab       PARSEC
/lib/modules     PARSEC
```

```
/lib64/security  PARSEC
/lib/security    PARSEC
/sbin            PARSEC
/usr/bin  PARSEC
/usr/lib  PARSEC
/usr/sbin        PARSEC
```

Кроме того, на выбор администратора представлен ряд дополнительных путей с правилами. Соответствующие строки помечены знаком комментария # и могут быть активированы снятием этого знака.

При запуске `afick` с параметром `-i`:

```
afick -i
```

будет создан файл `/var/lib/afick/afick`. Это и есть БД формата `ndbm`. Если посмотреть ее содержимое, то можно обнаружить набор строк, каждая из которых — имя файла и далее через пробел его атрибуты и сигнатуры.

БД защищается системой разграничения доступа.

При запуске `AFICK` автоматически установит ежедневное задание для `CRON`. Файл с заданием находится в `/etc/cron.daily/afick_cron`.

Параметр `report_url:=stdout` задает местоположение файла-отчета.

В конфигурационном файле есть простой язык макросов, который используется при определении переменных для заданий системного планировщика заданий `cron`.

14.5. Средства создания замкнутой программной среды

В ОС реализован механизм, обеспечивающий проверку неизменности и подлинности загружаемых исполняемых файлов формата ELF. Проверка производится на основе контрольных сумм файлов, вычисляемых в соответствии с ГОСТ Р 34.11-2012, и ЭЦП, реализованной в соответствии с ГОСТ Р 34.10-2012, которые внедрены в исполняемые файлы формата ELF в процессе сборки ОС. При этом сохраняется возможность проверки контрольных сумм, вычисляемых в соответствии с ГОСТ Р 34.11-94, и ЭЦП, реализованной в соответствии с ГОСТ Р 34.10-2001. Средства создания замкнутой программной среды предоставляют возможность внедрения цифровой подписи в исполняемые файлы формата ELF, входящие в состав устанавливаемого СПО (14.5.2).

В ОС реализован механизм, обеспечивающий проверку неизменности и подлинности файлов. Проверка производится на основе контрольных сумм, вычисляемых в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит, и ЭЦП, реализованной в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, которые внедряются в расширенные атрибуты файловой системы. Данный механизм предназначен для выявления фактов несанкционированного изменения исполняемых файлов и предотвращения их

открытия.

Механизм контроля целостности исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнение реализован в модуле ядра ОС `digsig_verif`, который является невыгружаемым модулем ядра Linux. Может функционировать в одном из следующих режимов:

1) исполняемым файлам и разделяемым библиотекам с неверной ЭЦП, а также без ЭЦП загрузка на исполнение запрещается (штатный режим функционирования);

2) исполняемым файлам и разделяемым библиотекам с неверной ЭЦП, а также без ЭЦП загрузка на исполнение разрешается, при этом выдается сообщение об ошибке проверки ЭЦП (режим для проверки ЭЦП в СПО);

3) ЭЦП при загрузке исполняемых файлов и разделяемых библиотек не проверяется (отладочный режим для тестирования СПО).

Механизм контроля целостности файлов при их открытии на основе ЭЦП в расширенных атрибутах файловой системы также реализован в модуле ядра ОС `digsig_verif` и может функционировать в одном из следующих режимов:

1) запрещается открытие файлов, поставленных на контроль, с неверной ЭЦП или без ЭЦП;

2) открытие файлов, поставленных на контроль, с неверной ЭЦП или без ЭЦП разрешается, при этом выдается сообщение об ошибке проверки ЭЦП (режим для проверки ЭЦП в расширенных атрибутах файловой системы);

3) ЭЦП при открытии файлов не проверяется.

14.5.1. Настройка модуля digsig_verif

Для изменения режима функционирования модуля `digsig_verif` необходимо отредактировать файл `/etc/digsig/digsig_initramfs.conf`.

Настройка режима функционирования механизма контроля целостности исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнение осуществляется следующим образом:

1) Для использования отладочного режима для тестирования СПО необходимо установить для параметра `DIGSIG_LOAD_KEYS` значение `0`:

```
DIGSIG_LOAD_KEYS=0
```

2) Для использования режима для проверки ЭЦП в СПО необходимо установить для параметра `DIGSIG_LOAD_KEYS` значение `1`:

```
DIGSIG_LOAD_KEYS=1
```

3) Для использования штатного режима функционирования необходимо установить следующие значения параметров:

```
DIGSIG_LOAD_KEYS=1
```

DIGSIG_ENFORCE=1

Каждый дополнительный ключ, использованный для подписывания СПО (14.5.2), необходимо скопировать в каталог /etc/digsig/keys/, например, с использованием команды:

```
cp /<каталог>/<файл ключа> /etc/digsig/keys/
```

В каталоге /etc/digsig/keys/ может располагаться иерархическая структура дополнительных ключей для контроля целостности исполняемых файлов и разделяемых библиотек формата ELF. В указанной структуре одни дополнительные ключи могут быть подписаны на других дополнительных ключах. При этом дополнительные ключи должны располагаться в подкаталогах таким образом, чтобы при их загрузке не нарушалась цепочка проверки подписей.

Пример

```
/etc/digsig/keys/key1.gpg - публичный ключ 1, подписанный
на первичном ключе ОАО <<НПО РусБИТех>>
/etc/digsig/keys/key2.gpg - публичный ключ 2, подписанный
на первичном ключе ОАО <<НПО РусБИТех>>
/etc/digsig/keys/key1/key1-1.gpg - публичный ключ, подписанный на ключе 1
/etc/digsig/keys/key1/key1-2.gpg - публичный ключ, подписанный на ключе 1
/etc/digsig/keys/key2/key2-1.gpg - публичный ключ, подписанный на ключе 2
/etc/digsig/keys/key2/key2-2.gpg - публичный ключ, подписанный на ключе 2
```

Для проверки использования дополнительных ключей для контроля целостности исполняемых файлов и разделяемых библиотек формата ELF (до перезагрузки ОС) можно от имени учетной записи администратора через механизм sudo выполнить команды:

```
cat /etc/digsig/key_for_signing.gpg > /sys/digsig/keys
cat /etc/digsig/keys/key1.gpg >> /sys/digsig/keys
cat /etc/digsig/keys/key2.gpg >> /sys/digsig/keys
cat /etc/digsig/keys/key1/key1-1.gpg >> /sys/digsig/keys
cat /etc/digsig/keys/key1/key1-2.gpg >> /sys/digsig/keys
cat /etc/digsig/keys/key2/key2-1.gpg >> /sys/digsig/keys
cat /etc/digsig/keys/key2/key2-2.gpg >> /sys/digsig/keys
```

ВНИМАНИЕ! При проверке ЭЦП в расширенных атрибутах файловой системы установка для параметра DIGSIG_ENFORCE значения 1 запрещает открытие поставленных на контроль файлов с неверной ЭЦП или без ЭЦП.

Настройка режима функционирования механизма контроля целостности файлов при их открытии на основе ЭЦП в расширенных атрибутах файловой системы осуществляется следующим образом:

1) Для включения механизма необходимо установить для параметра

DIGSIG_USE_XATTR значение 1:

```
DIGSIG_USE_XATTR=1
```

2) Для загрузки дополнительных ключей, используемых только при проверке ЭЦП в расширенных атрибутах файловой, системы необходимо установить для параметра DIGSIG_LOAD_XATTR_KEYS значение 1:

```
DIGSIG_LOAD_XATTR_KEYS=1
```

3) Для игнорирования дополнительных ключей, используемых только при проверке ЭЦП в расширенных атрибутах файловой, необходимо установить для параметра DIGSIG_IGNORE_XATTR_KEYS значение 1:

```
DIGSIG_IGNORE_XATTR_KEYS=1
```

4) Для настройки шаблонов имен, используемых при проверке ЭЦП в расширенных атрибутах ФС, необходимо в файле /etc/digsig/xattr_control задать их список. Каждая строка задает свой шаблон в виде маски полного пути. Например, следующий шаблон определяет, что будет проверяться ЭЦП всех файлов в каталоге /bin, имя которых начинается на lo:

```
\bin\lo
```

Каждый дополнительный ключ, использованный для подписывания файлов в расширенных атрибутах, необходимо скопировать в каталог /etc/digsig/xattr_keys/, например, с использованием команды:

```
cp /<каталог>/<файл ключа> /etc/digsig/xattr_keys/
```

В каталоге /etc/digsig/xattr_keys/ может располагаться иерархическая структура дополнительных ключей для контроля целостности файлов. В указанной структуре одни дополнительные ключи могут быть подписаны на других дополнительных ключах. При этом дополнительные ключи должны располагаться в подкаталогах таким образом, чтобы при их загрузке не нарушалась цепочка проверки подписей.

Пример

```
/etc/digsig/xattr_keys/key1.gpg – публичный ключ 1
/etc/digsig/xattr_keys/key2.gpg – публичный ключ 2
/etc/digsig/xattr_keys/key1/key1-1.gpg – публичный ключ, подписанный на ключе 1
/etc/digsig/xattr_keys/key1/key1-2.gpg – публичный ключ, подписанный на ключе 1
/etc/digsig/xattr_keys/key2/key2-1.gpg – публичный ключ, подписанный на ключе 2
/etc/digsig/xattr_keys/key2/key2-2.gpg – публичный ключ, подписанный на ключе 2
```

Для проверки использования дополнительных ключей для контроля целостности файлов (до перезагрузки ОС) можно от имени учетной записи администратора через механизм sudo выполнить команды:

```
cat /etc/digsig/xattr_keys/key1.gpg >> /sys/digsig/xattr_keys
cat /etc/digsig/xattr_keys/key2.gpg >> /sys/digsig/xattr_keys
cat /etc/digsig/xattr_keys/key1/key1-1.gpg >> /sys/digsig/xattr_keys
```

```
cat /etc/digsig/xattr_keys/key1/key1-2.gpg >> /sys/digsig/xattr_keys
cat /etc/digsig/xattr_keys/key2/key2-1.gpg >> /sys/digsig/xattr_keys
cat /etc/digsig/xattr_keys/key2/key2-2.gpg >> /sys/digsig/xattr_keys
```

Управление модулем digsig_verif осуществляется через интерфейс sysfs с использованием файлов:

– /sys/digsig/enforce — проверка и переключение режима работы;

– /sys/digsig/use_xattr — включить проверку ЭЦП в расширенных атрибутах ФС;

– /sys/digsig/keys — файл загрузки дополнительных ключей для проверки ЭЦП исполняемых файлов формата ELF и ЭЦП в расширенных атрибутах ФС;

– /sys/digsig/ignore_gost2001 — отключение проверки ЭЦП по ГОСТ Р 34.10-2001;

– /sys/digsig/ignore_xattr_keys — 1;

– /sys/digsig/xattr_control — список шаблонов имен, используемых при проверке ЭЦП в расширенных атрибутах ФС;

– /sys/digsig/xattr_keys — файл загрузки дополнительных ключей, используемых только при проверке ЭЦП в расширенных атрибутах ФС.

Проверка режима работы выполняется командой:

```
cat /sys/digsig/enforce
```

ВНИМАНИЕ! Для отключения проверки ЭЦП по ГОСТ Р 34.10-2001 необходимо в конфигурационном файле /etc/digsig/digsig_initramfs.conf установить следующее значение параметра:

```
DIGSIG_IGNORE_GOST2001=1
```

ВНИМАНИЕ! После внесения изменений в конфигурационный файл /etc/digsig/digsig_initramfs.conf и для загрузки модулем digsig_verif ключей после их размещения его в каталогах /etc/digsig/keys/ и /etc/digsig/xattr_keys/ необходимо от имени учетной записи администратора через механизм sudo выполнить команду:

```
sudo update-initramfs -u -k all
```

14.5.2. Подписывание

В модуле ядра digsig_verif реализован механизм, позволяющий использовать несколько ключей при подписывании файлов формата ELF.

Порядок использования ключей для digsig_verif: дополнительные ключи записываются в /sys/digsig/keys или /sys/digsig/xattr_keys в иерархической последовательности цепочек подписей.

Все дополнительные ключи должны быть подписаны главным ключом или другим

дополнительным ключом, подпись которого может быть проверена (за исключением первого ключа в каталоге /sys/digsig/xattr_keys).

Подписывание пакетов должно осуществляться на инструментальном компьютере под управлением ОС. Для выполнения подписывания необходимо, чтобы в инструментальной среде были установлены следующие пакеты: bsign, binutils, gzip, lzma, bzip2, gnupg.

Подписывание пакетов должно осуществляться от имени администратора через механизм sudo. Закрытый ключ для подписывания должен быть импортирован в набор его ключей командой:

```
gpg --import key_for_signing.key
gpg: ключ 078AC4F1: секретный ключ импортирован
gpg: ключ 078AC4F1: открытый ключ "CCT RusBITech (Key for signing)
      <mail@rusbitech.ru>" импортирован
gpg: Всего обработано: 1
gpg:                  импортировано: 1
gpg:     прочитано секретных ключей: 1
gpg: импортировано секретных ключей: 1
```

Для подписывания пакетов может быть использован скрипт, текст которого представлен ниже. Скрипт должен запускаться от имени пользователя root. В качестве первого аргумента должен быть указан полный путь до каталога, содержащего пакеты, которые необходимо подписать. В качестве второго аргумента должен быть указан каталог, в который будут помещаться подписанные пакеты.

```
#!/bin/bash

DIR_BIN=$1
DIR_SIGNED=$2

TMP_DIR=$DIR_SIGNED/tmp$$

if [ -z $DIR_BIN ] ; then
echo "Specify original directory as first argument."
exit 1
fi

if [ -z $DIR_SIGNED ] ; then
echo "Specify destination directory as second argument."
exit 1
fi
```

```
if [ ! -e $DIR_BIN ] ; then
echo "Original directory $DIR_BIN doesn’t exist."
exit 1
fi

list_of_packages=‘find $DIR_BIN -type f -name "*.deb"‘
list_of_udebs=‘find $DIR_BIN -type f -name "*.udeb"‘
#echo $list_of_packages

for i in $list_of_packages ; do
pack_name=‘echo $i | awk ’{sub(/^.+\//,"",$0) ; a=$0; print a}’‘
mkdir -p $TMP_DIR/{control,data}
cp $i $TMP_DIR
pushd $TMP_DIR
ar x $pack_name

# Definig archives type
data_arch_type=‘ls data.tar* | cut -d’.’ -f3‘
control_arch_type=‘ls control.tar* | cut -d’.’ -f3‘
popd

# Unpack data archive
pushd $TMP_DIR/data
case $data_arch_type in
gz)
tar --same-permissions --same-owner -xzf ../data.tar.gz
;;
bz2)
tar --same-permissions --same-owner -xjf ../data.tar.bz2
;;
lzma)
tar --same-permissions --same-owner --lzma -xf ../data.tar.lzma
;;
esac
popd

# Unpack control archive
```

```
pushd $TMP_DIR/control
case $control_arch_type in
gz)
tar --same-permissions --same-owner -xzf ../control.tar.gz
;;
bz2)
tar --same-permissions --same-owner -xjf ../control.tar.bz2
;;
lzma) \item пользователь подписывает утилитой \verb|bsign| на данном ключе произво

tar --same-permissions --same-owner --lzma -xf ../control.tar.lzma
;;
esac
popd

# Sign files
pushd $TMP_DIR/data
for file in `find . -type f` ; do
oldstat=`stat -c %a $file`
bsign -s --pgoptions "--default-key=A42E56D6" $file
bsign -V $file | grep -v "not ELF64"
bsign -w $file | grep -v "not ELF64"
newstat=`stat -c %a $file`
[$newstat!=$oldstat] && echo "BSIGN_CHMOD_ERROR in $file" >> ${SIGN_LOG} 2>&1
done
popd

# Counting md5sums
pushd $TMP_DIR/control
if [ -e ./md5sums ] ; then
filenames=`cat md5sums | awk -F'  ' '{print $2}'`
popd
pushd $TMP_DIR/data
for j in $filenames
do
echo `md5sum $j` >> $TMP_DIR/control/md5sums.new
done
sed -e 's/\ /\ \ /g' $TMP_DIR/control/md5sums.new >
```

```
$TMP_DIR/control/md5sums.new_mod
popd
mv -f $TMP_DIR/control/md5sums.new_mod $TMP_DIR/control/md5sums
rm -f $TMP_DIR/control/md5sums.new
fi

# Packing back in deb
pushd $TMP_DIR/data
case $data_arch_type in
gz)
tar --same-permissions --same-owner -czf ../data.tar.gz .
;;
bz2)
tar --same-permissions --same-owner -cjf ../data.tar.bz2 .
;;
lzma)
tar --same-permissions --same-owner --lzma -cf ../data.tar.lzma .
;;
esac
popd

pushd $TMP_DIR/control
case $control_arch_type in
gz)
tar --same-permissions --same-owner -czvf ../control.tar.gz .
;;
bz2)
tar --same-permissions --same-owner -cjvf ../control.tar.bz2 .
;;
lzma)
tar --same-permissions --same-owner --lzma -cvf ../control.tar.lzma .
;;
esac
popd
pushd $TMP_DIR
ar rcs $TMP_DIR/$pack_name debian-binary control.tar.$control_arch_type
    data.tar.$data_arch_type
cp $pack_name  $DIR_SIGNED/
```

```
popd
rm -rf $TMP_DIR
done

for j in $list_of_udebs ; do
    cp $j $DIR_SIGNED
done
```

Для корректной работы скрипта в строке:

```
bsign -s --pgoptions "--default-key=A42E56D6" $file
```

следует указать идентификатор ключа (слово A42E56D6), с помощью которого необходимо подписать пакет. Идентификатор ключа можно получить, используя команду:

```
gpg --list-keys
```

Далее приведен пример вывода команды gpg --list-keys:

```
/root/.gnupg/pubring.gpg
------------------------
pub    256E/A42E56D6 2010-06-16
uid                  CCT NPO RusBITech (Key for signing) <mail@rusbitech.ru>
```

Пример вызова скрипта для подписывания исполняемых модулей формата ELF, находящихся в каталоге /tmp/orig_packs, с помещением результатов подписывания в каталог /tmp/signed_packs:

```
sign.sh /tmp/orig_packs /tmp/signed_packs
```

Дополнительный ключ пользователя копируется в каталог /etc/digsig/keys/.

Для проверки правильности ЭЦП файла формата ELF используется утилита bsign:

```
keys@debian:~$ bsign -w test_elf
```

Подписанный файл формата ELF может выполняться:

```
keys@debian:~$ ./test_elf
hello world!
keys@debian:~$
```

Дополнительный ключ пользователя для проверки ЭЦП в расширенных атрибутах файла копируется в каталог /etc/digsig/xattr_keys/.

Для внедрения ЭЦП в расширенные атрибуты файла пользователь подписывает утилитой bsign на данном ключе произвольный файл:

```
keys@debian:~$ bsign --sign --xattr test_elf
```

15. СРЕДСТВА ЦЕНТРАЛИЗОВАННОГО ПРОТОКОЛИРОВАНИЯ

Для решения задач централизованного сбора и анализа журналов протоколирования (журналов аудита) в ОС реализованы:

– сервер — пакет `ossec-hids-server` (15.1);
– агент — пакет `ossec-hids-agent` (15.2);
– графический интерфейс — пакет `ossec-web` (15.3);
– настройка для бездисковых станций `ossec-cnt` (15.4).

15.1. Сервер

Сервер системы централизованного протоколирования предназначен для решения задач сбора и анализа информации о протоколируемых событиях посредством выполнения соответствующих процессов системных сервисов `ossec-logcollector`, `ossec-remoted` и `ossec-analisisd`.

15.1.1. Установка

Установка сервера системы централизованного протоколирования осуществляется от имени администратора через механизм `sudo` из пакета `ossec-hids-server` с использованием пакетного менеджера `aptitude` или посредством выполнения команды:

```
apt-get install ossec-hids-server
```

ВНИМАНИЕ! Не следует устанавливать пакет `ossec-hids-agent` на сервере системы централизованного протоколирования. Пакет `ossec-hids-server` включает компоненты агента.

15.1.2. Настройка

Настройка сервера системы централизованного протоколирования осуществляется от имени администратора через механизм `sudo` посредством редактирования конфигурационного файла `/var/ossec/etc/ossec.conf`.

Добавление клиентов, обрабатываемых сервером, осуществляется утилитой `manage_agents`, находящейся в каталоге `/var/ossec/bin/`. В интерактивном режиме указываются имя, IP-адрес и ID для каждого клиента. В нем же производится импортирование ключей клиентов, которые необходимы для настройки клиентов.

После выполнения всех этих действий необходимо перезапустить сервер:

```
/etc/init.d/ossec-hids-server restart
```

15.2. Агент

15.2.1. Установка

Установка агента системы централизованного протоколирования осуществляется от имени администратора через механизм `sudo` из пакета `ossec-hids-agent` с использо-

ванием пакетного менеджера aptitude или посредством выполнения команды:

```
apt-get install ossec-hids-agent
```

ВНИМАНИЕ! Не следует устанавливать пакет ossec-hids-agent на сервере системы централизованного протоколирования. Пакет ossec-hids-server включает компоненты агента.

15.2.2. Настройка

Настройка агента системы централизованного протоколирования осуществляется от имени администратора через механизм sudo посредством редактирования конфигурационного файла /var/ossec/etc/ossec.conf. В этом файле необходимо изменить параметр <server-ip> на соответствующий серверу:

```
<server-ip>x.x.x.x</server-ip>
```

Также в этом файле указываются файлы, за которыми будет следить агент. В установку входит пример конфигурационного файла /var/ossec/etc/ossec.conf.default

Для слежения за логами PARSEC необходимо раскомментировать в файле /var/ossec/etc/ossec.conf вызов /var/ossec/bin/parseclog.sh

С помощью утилиты manage_agents, находящейся в каталоге /var/ossec/bin/, импортировать соответствующий клиенту ключ с сервера.

После выполнения настройки перезапустить агента:

```
/etc/init.d/ossec-hids-agent restart
```

15.3. Графический интерфейс

15.3.1. Установка и настройка

Установка должна производиться на той же вычислительной системе, где установлен сервер системы. Так же должен быть установлен и настроен сервер Apache2 с поддержкой PHP.

Установка графического интерфейса системы централизованного протоколирования осуществляется от имени администратора через механизм sudo из пакета ossec-web с использованием пакетного менеджера aptitude или посредством выполнения команды:

```
apt-get install ossec-web
```

Перезапустить сервис incron:

```
service incron restart
```

После установки необходимо добавить в группу ossec пользователей, которые будут следить за событиями:

```
usermod -a -G ossec user
```

В случае если система настроена для работы в рамках ЕПП для пользователей, которые будут следить за событиями, можно использовать ACL, например:

```
setfacl -R u:ald-user:rx /var/www/ossec/
```

```
setfacl -d -m u:ald-user:rwx /var/www/ossec/data
setfacl -d -m u:ald-user:rwx /var/www/ossec/arch
```

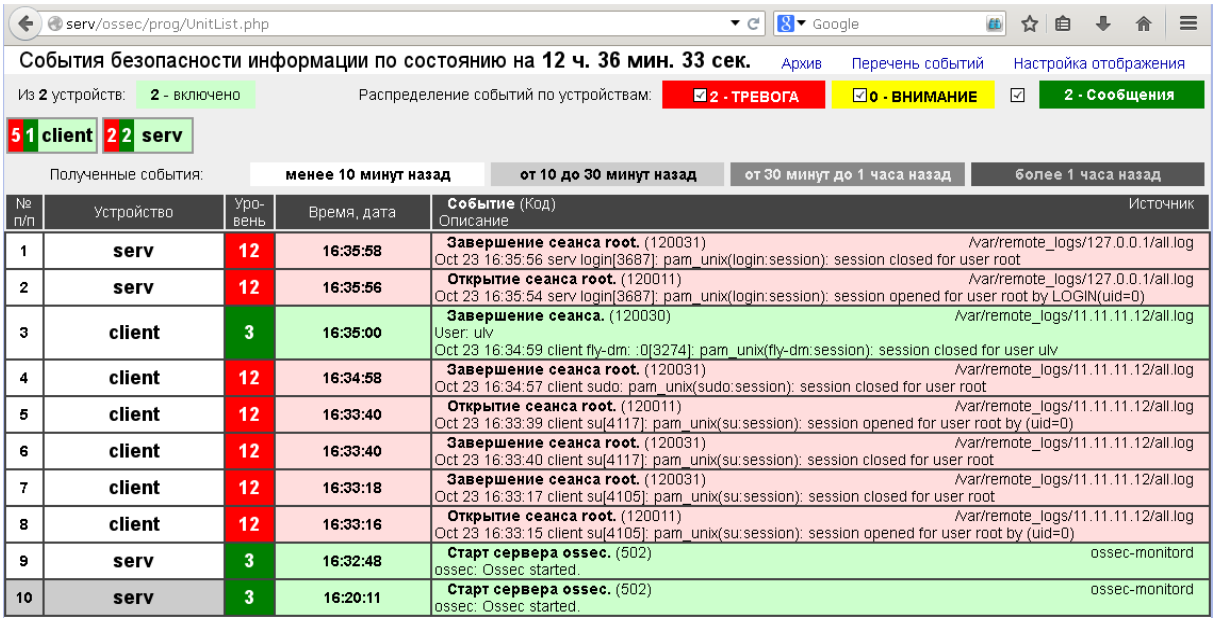
либо создать в ЕПП для них отдельную группу и добавить ACL для этой группы.

В файлах `/etc/php5/apache2/php.ini` и `/etc/php5/cli/php.ini` в секцию `[Date]` нужно добавить параметр `date.timzone <зона>`. Системную временную зону можно посмотреть в файле `/etc/timzone`. Например, `Europe/Moscow`.

После этого доступ к графическому интерфейсу может быть осуществлен из браузера по адресу: `http://servername/ossec/prog/UnitList.php`, при этом, в зависимости от настроек сервера может потребоваться авторизация от имени пользователя, имеющего доступ к системе.

15.3.2. Описание графического интерфейса

После запуска открывается главное окно программы (см. рис. 8), на котором отображаются: список клиентов, с которых собирается мониторинг, обновляющийся список приходящих сообщений с клиентов, настройки фильтра отображения сообщений и расшифровка подсветки информации



№ п/п	Устройство	Уро-вень	Время, дата	Событие (Код) Описание	Источник
1	serv	12	16:35:58	**Завершение сеанса root.** (120031) Oct 23 16:35:56 serv login[3687]: pam_unix(login:session): session closed for user root	/var/remote_logs/127.0.0.1/all.log
2	serv	12	16:35:56	**Открытие сеанса root.** (120011) Oct 23 16:35:54 serv login[3687]: pam_unix(login:session): session opened for user root by LOGIN(uid=0)	/var/remote_logs/127.0.0.1/all.log
3	client	3	16:35:00	**Завершение сеанса.** (120030) User: ulv Oct 23 16:34:59 client fly-dm: :0[3274]: pam_unix(fly-dm:session): session closed for user ulv	/var/remote_logs/11.11.11.12/all.log
4	client	12	16:34:58	**Завершение сеанса root.** (120031) Oct 23 16:34:57 client sudo: pam_unix(sudo:session): session closed for user root	/var/remote_logs/11.11.11.12/all.log
5	client	12	16:33:40	**Открытие сеанса root.** (120011) Oct 23 16:33:39 client su[4117]: pam_unix(su:session): session opened for user root by (uid=0)	/var/remote_logs/11.11.11.12/all.log
6	client	12	16:33:40	**Завершение сеанса root.** (120031) Oct 23 16:33:40 client su[4117]: pam_unix(su:session): session closed for user root	/var/remote_logs/11.11.11.12/all.log
7	client	12	16:33:18	**Завершение сеанса root.** (120031) Oct 23 16:33:17 client su[4105]: pam_unix(su:session): session closed for user root	/var/remote_logs/11.11.11.12/all.log
8	client	12	16:33:16	**Открытие сеанса root.** (120011) Oct 23 16:33:15 client su[4105]: pam_unix(su:session): session opened for user root by (uid=0)	/var/remote_logs/11.11.11.12/all.log
9	serv	3	16:32:48	**Старт сервера ossec.** (502) ossec: Ossec started.	ossec-monitord
10	serv	3	16:20:11	**Старт сервера ossec.** (502) ossec: Ossec started.	ossec-monitord

Рис. 8

При нажатии в списке на имя клиентской машины, в новой вкладке открывается окно (см. рис. 9), содержащее сообщения, относящиеся к данному агенту. По умолчанию однотипные сообщения группируются и указывается только их количество. Отключить группировку для просмотра всех сообщений можно сняв галочку в левом верхнем углу.

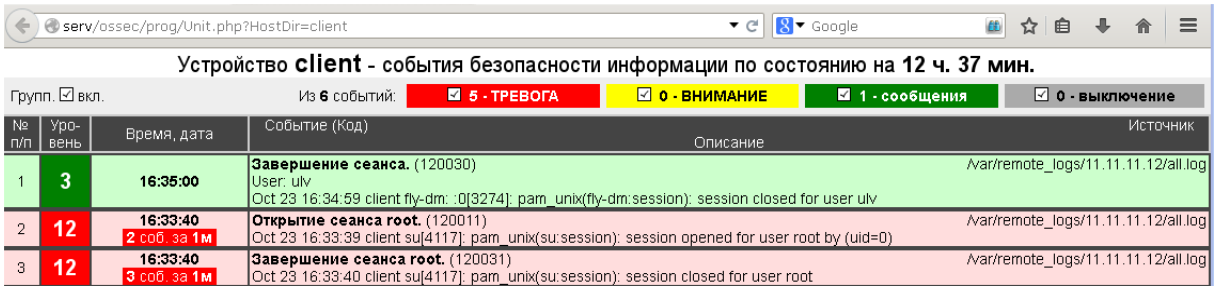


Рис. 9

Нажатие в главном окне на ссылку «Архив», открывает в новой вкладке окно (см. рис. 10) на котором можно выбрать интересующие сообщения с конкретных клиентских устройств.

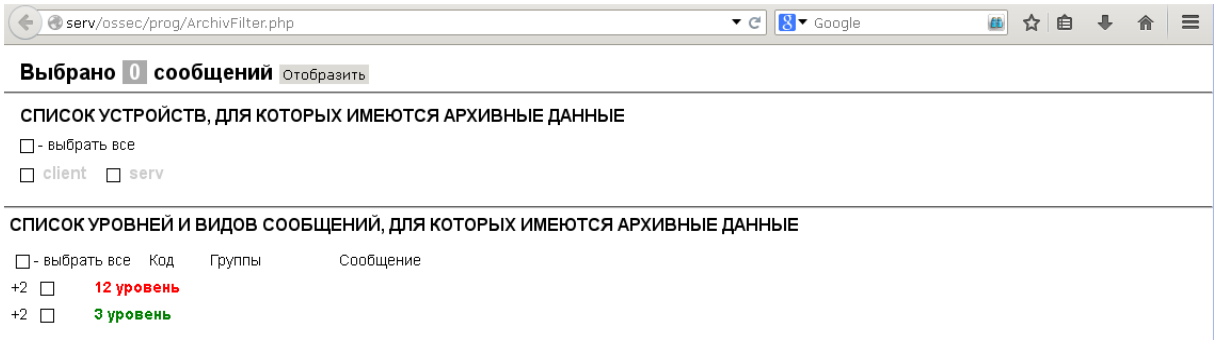


Рис. 10

Нажатие в главном окне на ссылку «Перечень событий» выводит в новой вкладке список всех правил (см. рис. 11), которые обрабатываются системой, с указанием в каком конфигурационном файле описано данное событие.

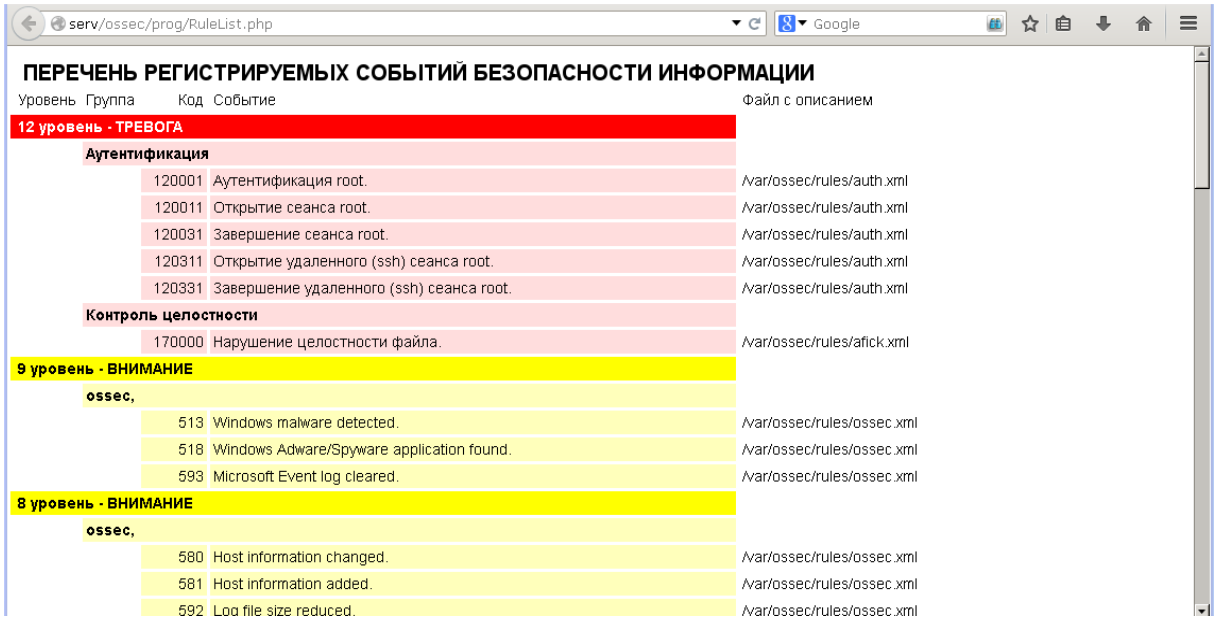


Рис. 11

Нажатие в главном окне на ссылку «Настройка отображения», выводит в новой вкладке окно (см. рис. 12) в котором возможно выбрать и убрать из отображения сооб-

щения для конкретных клиентов за конкретный период времени. При нажатии на кнопку **[Снять с отображения]** выбранные сообщения больше не отображаются в главном окне. При этом сами сообщения не удаляются и доступны для просмотра в архиве.

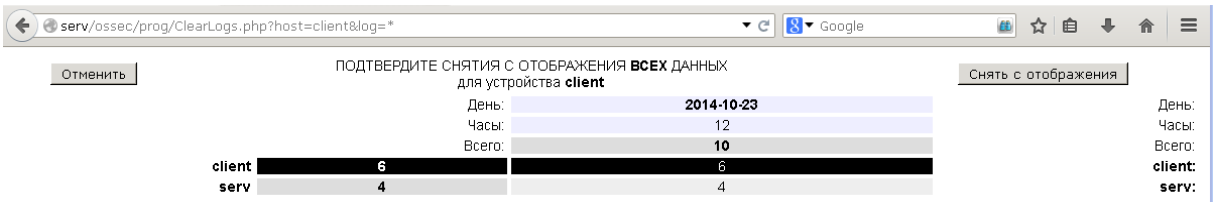


Рис. 12

15.4. Настройка сбора журналов без использования агентов

Могут возникать случаи когда ограничена возможность хранения логов на клиентах и необходимо настраивать их перенаправление на сервер, например с использованием `rsyslog`. Далее приведена последовательность действий для такой настройки.

15.4.1. Настройки на сервере

Создать каталог для хранения логов с агентов и дать доступ для группы `ossec`:

```
mkdir /var/remote_logs
setfacl -d -m g:ossec:rwx /var/remote_logs/
setfacl -R -m g:ossec:rwx /var/remote_logs/
```

Скопировать настройки для `rsyslog` и для запуска демона `syslog`

```
cp /var/ossec/etc/10-ossec-syslog.conf /etc/rsyslog.d/
```

Перезапустить сервис `rsyslog`:

```
service rsyslog restart
```

Расскоментировать в файле `/var/ossec/etc/ossec.conf` строки:

```
<localfile>
<log_format>syslog</log_format>
<location>/var/remote_logs/*/all.log</location>
</localfile>
```

После выполнения всех этих действий необходимо перезапустить сервер:

```
/etc/init.d/ossec-hids-server restart
```

15.4.2. Настройка на клиентах

Добавить в `/etc/rsyslog.conf` строки:

```
echo '*.* @SERVER' >> /etc/rsyslog.conf
echo '$SystemLogRateLimitInterval 2' >> /etc/rsyslog.conf
echo '$SystemLogRateLimitBurst 50000' >> /etc/rsyslog.conf
```

где `SERVER` это полное доменное имя сервера.

Перезапустить сервис `rsyslog`:

```
service rsyslog restart
```

Раскомментировать в файле `/var/ossec/etc/ossec.conf` вызов `/var/ossec/bin/check_running_audit_send.sh`.

После выполнения настройки перезапустить агента:

```
/etc/init.d/ossec-hids-agent restart
```

16. СРЕДСТВА РАЗГРАНИЧЕНИЯ ДОСТУПА К ПОДКЛЮЧАЕМЫМ УСТРОЙСТВАМ

В ОС с использованием генерации правил менеджера устройств udev осуществляется разграничение доступа к символьным и блочным устройствам, для которых в каталоге /dev создаются файлы устройств. При разграничении доступа к устройствам типа видеокарт, сетевых карт и т.д. данный метод не используется.

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

– средства разграничения доступа к устройствам на основе правил udev (16.1);

– средства регистрации устройств (16.2).

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

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

16.1. Разграничение доступа к устройствам на основе генерации правил udev

Разграничение доступа к устройствам на основе генерации правил менеджера устройств udev осуществляется для символьных и блочных устройств посредством автоматической генерации правил. Генерация осуществляется с использованием базы учета устройств, ведущейся в локальной системе (файл /etc/parsec/devices.cfg) или в ALD (см. раздел 6).

Разграничение доступа к устройству осуществляется на основе соответствующего правила для менеджера устройств udev, которое хранится в файле в каталоге /etc/udev/rules.d. Для устройств, учитываемых в локальной базе (см. 16.2), генерация правила осуществляется при сохранении информации об устройстве с использованием утилиты fly-admin-smc. Для устройств, учитываемых в базе ALD (см. 16.2), генерация правил осуществляется PAM-модулем pam_ald при входе пользователя в систему. При этом правила генерируются для всех устройств, учтенных в базе ALD, вне зависимости от имени пользователя, осуществляющего вход в систему, и наименования хоста, на котором выполняется вход.

Далее приведен пример правила для съемного USB-накопителя.

Пример

```
ENV{ID_SERIAL}=="JetFlash_TS256MJF120_OYLIXNA6-0:0", OWNER="user",
```

```
GROUP="users" PDPL="3:0:f:0!:"
```

В примере для съемного USB-накопителя с серийным номером JetFlash_TS256MJF120_OYLIXNA6-0:0 разрешено его использование владельцу устройства: пользователю user и пользователям, входящим в группу users. Для устройства установлены мандатные атрибуты: уровень конфиденциальности — 3, уровень целостности — 0, категории — f, роли и административные роли отсутствуют.

При монтировании блочных устройств используется утилита mount, модифицированная для монтирования устройства владельцем или пользователем, входящим в группу, с использованием регулярных выражений. В процессе монтирования от имени пользователя ожидается два параметра: конкретное наименование файла устройства и конкретное наименование точки монтирования. При этом монтирование ФС съемных накопителей от имени пользователя (в т. ч. с использованием графической утилиты fly-fm) осуществляется в каталог, создаваемый в подкаталоге media домашнего каталога пользователя. Для предоставления локальным пользователям возможности монтирования ФС съемных накопителей необходимо наличие в файле /etc/fstab следующей записи:

```
/dev/s*  /home/*/media/*  auto owner,group,noauto,noexec,iocharset=utf8,
defaults 0 0
```

Для предоставления пользователям ALD (см. раздел 6) возможности монтирования ФС съемных накопителей необходимо наличие в файле /etc/fstab следующей записи:

```
/dev/s* /ald_home/*/media/* auto owner,group,noauto,noexec,iocharset=utf8,
defaults 0 0
```

Для одновременного предоставления локальным пользователям и пользователям ALD (см. раздел 6) возможности монтирования ФС съемных накопителей необходимо наличие в файле /etc/fstab следующей записи:

```
/dev/s*  /*home/*/media/* auto owner,group,noauto,noexec,iocharset=utf8,
defaults 0 0
```

По умолчанию для монтирования различных ФС, содержащихся в учтенных разделах на блочных устройствах USB-накопителей, в файл /etc/fstab включены следующие записи:

```
/dev/*fat  /*home/*/media/*  auto  owner,group,noauto,nodev,noexec,
iocharset=utf8,defaults  0  0

/dev/*ntfs*  /*home/*/media/*  auto  owner,group,noauto,nodev,noexec,
iocharset=utf8,defaults  0  0

/dev/sd*ext*  /*home/*/media/*  auto  owner,group,noauto,nodev,noexec,
defaults  0  0
```

По умолчанию для монтирования различных ФС, содержащихся на учтенных

компакт- и DVD-дисках, в файл /etc/fstab включены следующие записи:

```
/dev/*udf  /*home/*/media/*  udf  owner,group,nodev,noexec,noauto,
defaults  0  0

/dev/*iso9660  /*home/*/media/*  iso9660  owner,group,nodev,noexec,noauto,
defaults  0  0
```

По умолчанию монтирование ФС, содержащихся в неучтенных разделах на блочных устройствах USB-накопителей, разрешено пользователям, входящим в группу floppy. В данном случае монтирование будет осуществляться в соответствии со следующей записью из файла /etc/fstab:

```
/dev/sd*  /*home/*/media/*  auto  owner,group,noauto,nodev,noexec,
iocharset=utf8,defaults  0  0
```

Использование указанной записи невозможно для ФС Ext*, поскольку для них не поддерживается опция монтирования iocharset=utf8.

Для монтирования пользователями ФС, содержащихся на неучтенных компакт- и DVD-дисках, в конец файла /etc/fstab необходимо включить следующую запись:

```
/dev/sr*  /*home/*/media/*  udf,iso9660  user,noauto  0  0
```

При монтировании ФС, поддерживающей атрибуты UNIX и расширенные атрибуты, права доступа на файл учтенного устройства не будут совпадать с правами доступа в ФС. Использование мандатных атрибутов будет ограничено атрибутами, установленными для файла устройства.

16.2. Регистрация устройств

Регистрация устройств в локальной базе учета устройств осуществляется с использованием графической утилиты управления политикой безопасности fly-admin-smc.

Регистрация устройств в базе учета устройств ALD (см. раздел 6) осуществляется с использованием графической утилиты управления политикой безопасности fly-admin-smc (fly-admin-ald) или утилиты командной строки ald-admin.

Устройства идентифицируются на основе атрибутов менеджера устройств udev. В большинстве случаев достаточно использовать серийный номер ID_SERIAL. В случае когда использование для идентификации устройства серийного номера невозможно, необходимо выбрать один или несколько других атрибутов, обеспечивающих идентификацию устройства.

Для предоставления пользователям доступа к устройствам (USB-накопители, сканеры, оптические носители) из контекста мандатного сеанса необходимо выполнить следующее действия:

1) запустить от имени администратора через механизм sudo утилиту управления

политикой безопасности `fly-admin-smc` (см. электронную справку). Выбрать в дереве объектов в боковой панели «Устройства и правила – Устройства»;

2) нажать кнопку **[Создать новый элемент]** на панели инструментов. Дождаться появления графического окна и подключить устройство следующим способом:

– подключить USB-накопитель к USB-порту компьютера;

– подключить кабель USB-сканера в USB-порт компьютера;

– вставить оптический носитель в устройство чтения CD/DVD-дисков.

3) в появившемся перечне выбрать устройство, далее открыть его «Свойства». В списке свойств устройства должны быть отмечены строки следующего вида:

– для USB-накопителей (отмечено по умолчанию):

`ID_SERIAL Значение`

– для сканеров (отмечено по умолчанию):

`ID_SERIAL Значение`

`PRODUCT Значение`

– для оптических носителей (отмечено по умолчанию):

`ID_SERIAL Значение`

Позволяет идентифицировать устройства, на которых будет осуществляться работа с оптическими носителями.

`ID_FS_LABEL Значение`

Позволяет идентифировать оптический носитель.

При необходимости можно выбрать другие свойства.

4) добавить устройство, нажав кнопку **[Да]**;

5) в поле `Наименование` указать наименование устройства;

6) во вкладке `Общие` необходимо выбрать пользователя, группу (владельца устройства) и задать права доступа для пользователя, группы и всех остальных;

7) указать мандатный уровень, для этого во вкладке `МРД` выбрать мандатный уровень, далее необходимо указать набор мандатных категорий;

8) назначить параметры регистрации событий, связанных с устройством, для этого во вкладке `Аудит` необходимо выбрать событие и результат (`Успех`, `Отказ`), подлежащие регистрации;

9) назначить дополнительные наборы правил для устройства из списка правил, созданных во вкладке боковой панели «Устройства и правила – Правила» (в данной вкладке создается набор правил для менеджера устройств `udev` (см. 16.1);

10) применить изменения, нажав кнопку **[Применить изменения]** на панели инструментов.

После переподключения устройства владелец устройства или пользователи из

группы смогут монтировать устройство, и на точку монтирования будут устанавливаться указанные мандатный уровень и категории.

ВНИМАНИЕ! Учет разделов съемных накопителей, содержащих файловую систему NTFS и другие файловые системы, монтируемые с использованием технологии FUSE (Filesystem in Userspace — файловая система в пользовательском пространстве), должен осуществляется только с нулевым мандатным уровнем и без категорий. Пользователя, который должен работать с подобным разделом, необходимо включить в локальную группу fuse.

17. ПОДДЕРЖКА СРЕДСТВ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Повышение надежности аутентификации возможно путем применения многофакторной аутентификации, т.е. аутентификации, в процессе которой используются аутентификационные факторы нескольких типов.

К факторам, которые могут быть использованы относятся:

– ввод пароля или PIN-кода;

– ввод одноразовых паролей (скрэтч-карты);

– предоставление физического устройства или носителя, содержащего аутентификационную информацию (смарт-карта, USB-токен, и т.п.);

– предоставление биометрической информации (отпечатки пальцев, изображение сетчатки глаза и т.п.).

На практике, в большинстве случаев используется двухфакторная аутентификация на основе ввода пароля с одновременным предоставлением пользователем физического устройства или носителя, содержащего дополнительную аутентификационную информацию. Дополнительной аутентификационной информацией в этом случае зачастую является размещенный на устройстве сертификат пользователя.

Для обеспечения двухфакторной аутентификации с помощью внешнего носителя используются следующие средства и технологии:

– PKCS (Public-Key Cryptography Standard) — группа стандартов криптографии с открытым ключом, в частности стандарты PKCS-11, PKCS-12, PKCS-15, относящиеся к работе с криптографическими токенами.

– X.509 — стандарт, определяющий форматы данных и процедуры распределения открытых ключей с помощью сертификатов с цифровыми подписями, которые предоставляются сертификационными органами (CA).

– OpenSC — набор программных утилит и библиотек работы с носителями аутентификационной информации пользователя (смарт-карты, USB-токены), содержащие функции аутентификации, шифрования и цифровой подписи. Поддерживает стандарты PKCS-11, PKCS-15.

– OpenCT — набор драйверов устройств работы с носителями аутентификационной информации (устаревшее).

– OpenSSL — программное средство для работы с криптографическим протоколом SSL/TLS. Позволяет создавать ключи RSA, DH, DSA и сертификаты X.509, подписывать их, формировать файлы сертификатов CSR и CRT. Также имеется возможность шифрования данных и тестирования SSL/TLS соединений.

– PC/SC — набор спецификаций для доступа к смарт-картам;

– PKINIT (Public Key Cryptography for Initial Authentication in Kerberos) — стандарт использования криптографии с открытым ключом в качестве фактора аутентификации в протоколе аутентификации Kerberos (см. 6.4).

Двухфакторная аутентификация может применятся как в случае использования локальной аутентификации, так и в случае использования ЕПП.

17.1. Аутентификация с открытым ключом (Инфраструктура открытых ключей)

При доступе к ресурсам информационных систем часто используются криптографические механизмы, основанные на ассиметричных алгоритмах шифрования и сертификатах открытого ключа. Применение указанных механизмов в информационных системах обеспечивается инфраструкторой открытых ключей (PKI — Public Key Infrastructure), которая включает в себя набор аппаратных и программных средств, политик и процедур создания, управления, распространения, использования и отзыва цифровых сертификатов.

В основе PKI лежит использование криптографической системы с открытым ключом и несколько основных принципов:

– закрытый ключ известен только его владельцу;

– удостоверяющий центр создает сертификат открытого ключа, таким образом удостоверяя этот ключ;

– никто не доверяет друг другу, но все доверяют удостоверяющему центру;

– удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом.

Аутентификация на основе ключей использует два ключа, один «открытый» (публичный ключ), который доступен каждому и второй «закрытый» (секретный ключ), который доступен только владельцу. В процессе аутентификации используются криптографические алгоритмы с открытым ключом для проверки подлинности пользователя. При этом секретный ключ находится непосредственно у пользователя, а открытый ключ по защищенным каналам связи передается в те системы, которые должны с его помощью проверять подлинность пользователя.

В качестве электронного представления ключей используются цифровые сертификаты. Сертификат является удостоверением принадлежности открытого ключа. Цифровой сертификат устанавливает и гарантирует соответствие между открытым ключом и его владельцем. Сертификаты выдаются специальными уполномоченными организациями — удостоверяющими центрами (УЦ) сертификации. Сертификаты могут быть использованы не только для аутентификации, но и для предоставления избирательных прав доступа, в том числе и права подписи других сертификатов.

В рамках изолированной информационной системы средством выработки и подписывания цифровых сертификатов могут быть использованы различные программные средства, например `openssl`. В этом случае такое средство может выступать в роли локального удостоверяющего центра для создания ключевых пар и сертификатов клиентов и серверов системы.

17.2. Состав средств поддержки двухфакторной аутентификации

В состав ОС входят необходимые программные инструменты и библиотеки, реализующие перечисленные средства и технологии. Сведение о содержащих их программных пакетах приведены в таблице 53.

Таблица 53

Наименование	Описание
`opensc`	Набор программных утилит и библиотек OpenSC
`pcscd`	Служба доступа к смарт-картам через PC/SC
`libpcsclite1`	Библиотека доступа к смарт-картам через PC/SC
`openct`	Набор драйверов устройств работы с носителями аутентификационной информации (OpenCT)
`libopenct1`	Библиотека драйверов устройств работы с носителями аутентификационной информации (OpenCT)
`libccid`	PC/SC драйвер для CCID совместимых USB устройств работы с носителями аутентификационной информации
`openssl`	Программное средство генерации ключей и сертификатов OpenSSL
`libengine-pkcs11-openssl`	Расширение OpenSSL для поддержки модулей PKCS-11
`libp11`	Библиотека поддержки PKCS-11
`libpam-p11`	Подгружаемый модуль аутентификации с помощью смарт-карт PKCS-11
`libpam-pkcs11`	Полнофункциональный подгружаемый модуль аутентификации с помощью смарт-карт PKCS-11
`krb5-pkinit`	Расширение MIT Kerberos V5 для поддержки PKINIT

Более подробное описание см. в руководстве `man`.

ВНИМАНИЕ! Перед использованием средств двухфакторной аутентификации должны быть установлены перечисленные пакеты. Из последних трех пакетов должны быть выбраны именно те, которые будут применяться для организации локального входа пользователя (`libpam-p11` или `libpam-pkcs11`) или доменного входа пользователя в случае использования ЕПП (`krb5-pkinit`).

17.3. Управление сертификатами

Для обеспечения аутентификации с открытым ключом в информационной системе необходимо иметь набор ключевых пар и сертификатов ресурсов сети (серверов или служб) и ее клиентов (пользователей). Формирование и подписывание сертификатов выполняется с помощью удостоверяющего центра информационной системы. Процедура получения необходимого набора сертификатов заключается в следующем:

1) формируются ключи и корневой сертификат удостоверяющего центра;
2) для каждого сервера или клиента генерируется ключевая пара;
3) на основе полученной ключевой пары формируется заявка (запрос) на сертификат;
4) с помощью УЦ по заявке выписывается сертификат;
5) полученная ключевая пара и сертификат сохраняются в соответствующие места системы.

Примечание. Генерация ключевых пар и формирование заявок может выполнятся как программными средствами, так и с помощью аппаратно-программных возможностей устройств аутентификации.

ВНИМАНИЕ! В отличие от генерации ключевых пар и формирования заявок, которые, как правило, выполняются на рабочем месте клиента, выписывание сертификатов должно производится по месту расположения УЦ.

17.3.1. Создание корневого сертификата CA

Корневой сертификат является сертификатом самого удостоверяющего центра и используется для подписи и удостоверения подлинности других сертификатов. Является самоподписанным.

Генерация ключевой пары удостоверяющего центра и создания его самоподписанного сертификата с помощью `openssl` выполняется следующим образом (используется ключ RSA длиной 2048 бит):

```
openssl genrsa -out cakey.pem 2048
openssl req -key cakey.pem -new -x509 -out cacert.pem
```

ВНИМАНИЕ! Корневой сертификат является наиболее секретным элементом инфраструктуры открытых ключей и должен быть надежно защищен.

17.3.2. Генерация ключевых пар

Генерация ключевой пары может выполнятся с помощью `openssl` (используется ключ RSA длиной 2048 бит):

```
openssl genrsa -out key.pem 2048
```

При наличии соответствующего устройства или носителя генерация ключевой пары должна быть выполнена с использованием PKCS утилит:

```
pkcs15-init --generate-key rsa/2048 --auth-id 02 --id 45
```

При этом указывается уникальный идентификатор сертификата `id` и запрашивается PIN-код пользователя-владельца токена.

17.3.3. Создание заявки на сертификат

Для полученных с помощью `openssl` ключей заявка на сертификат создается следующим образом:

```
openssl req -new -out client.req -key key.pem
```

При этом указывается полученный ранее файл ключей `key.pem`.

В случае использования устройств PKCS-11 создание заявки на сертификат требует дополнительного взаимодействия `openssl` с устройством. После запуска `openssl`:

```
openssl
```

необходимо подгрузить модуль поддержки PKCS-11:

```
OpenSSL> engine dynamic -pre SO_PATH:/usr/lib/ssl/engines/engine_pkcs11.so
 -pre ID:pkcs11 -pre LIST_ADD:1 -pre LOAD -pre MODULE_PATH:opensc-pkcs11.so
(dynamic) Dynamic engine loading support
[Success]: SO_PATH:/usr/lib/ssl/engines/engine_pkcs11.so
[Success]: ID:pkcs11
[Success]: LIST_ADD:1
[Success]: LOAD
Loaded: (pkcs11) pkcs11 engine
```

Затем выполнить команду создания заявки на сертификат:

```
OpenSSL> req -engine pkcs11 -new -key 1:45 -keyform engine -out client.req
 -subj "/C=RU/ST=Moscow/L=Moscow/O=Aktiv/OU=dev/CN=testuser/
 emailAddress=testuser@mail.com"
engine "pkcs11" set.
PKCS#11 token PIN:
OpenSSL>
```

При этом указывается уникальный идентификатор сертификата и запрашивается PIN-код владельца токена. Для привязки к субъекту информационной системы указывается его полное имя.

Примечание. Опция `-key 1:45` является указанием слота смарт-карты и идентификатора в виде slot:id.

Примечание. Способ формирования и задания полного имени клиента засисит от реализации конкретной информационной системы. Зачастую для этого используется DN (Distinguish Name) пользователя в системе.

Полученный запрос сохраняется в файле `client.req`.

17.3.4. Выписывание сертификата

Полученная ранее заявка на сертификат должна быть передана в УЦ для выписывания сертификата.

При выписывании сертификата могут быть использованы специальный файлы расширений OpenSSL, в которых указываются дополнительные используемые поля сертификатов. Например, в случае использования PKINIT, конфигурация задается файлом `pkinit_extensions` (см.17.5.5), в котором указаны дополнительные поля сертификатов, используемых в Kerberos:

– Extended Key Usage (EKU) — идентификатор (OID), говорящий о том, как планируется использовать сертификат;

– otherName — поле, задающее принципала Kerberos, для которого выписывается сертификат.

ВНИМАНИЕ! Перед выписыванием сертификата может потребоваться указание субъекта, для которого выполняется подпись с помощью параметров окружения, например:

```
export REALM=AKTIV-TEST.RU
export CLIENT=testuser
```

Выписывание сертификата выполняется следующей командой `openssl`:

```
openssl x509 -req -in client.req -CAkey cakey.pem -CA cacert.pem
 -out client.pem -CAcreateserial
```

При этом для формирования подписи задается корневой сертификат.

Примечание. Опция `-CAcreateserial` служит для создания серийного номера нового сертификата. Нужно только первый раз, затем используется опция `-CAserial cacert.srl` для увеличения этого номера.

При использовании файлов расширений указываются дополнительные опции, например:

```
openssl x509 -req -in client.req -CAkey cakey.pem -CA cacert.pem -CAcreateserial
 -extensions client_cert -extfile pkinit_extensions -out client.pem
```

Примечание. Использование PKINIT и формирование сертификатов в ЕПП рассматривается далее в разделе 17.5.

После получения готового сертификата он сохраняется на токене и в дальнейшем может быть считан с него для размещения в списках доверенных сертификатов.

17.3.5. Проверка сертификата

Проверка сертификата может быть выполнена командой `verify` утилиты `openssl`:

```
openssl verify -CAfile cacert.pem client.pem
```

При этом необходимо указать корневой сертификат.

17.3.6. Сохранение сертификата на токене

Сохранение сертификата на смарт-карте PKCS-11 выполняется с помощью PKCS утилит:

```
pkcs15-init --store-certificate client.pem --auth-id 02 --id 45 --format pem
```

При этом также указывается уникальный идентификатор сертификата `id` и запрашивается PIN-код пользователя-владельца.

17.4. Настройка локального входа

Для организации локального входа пользователей с помощью смарт-карт PKCS-11 могут быть использованы следующие подгружаемые модули аутентификации:

– Pam_p11 (`libpam-p11`) — подгружаемый модуль аутентификации с помощью смарт-карт PKCS-11;

– PKCS#11 (`libpam-pkcs11`) — полнофункциональный подгружаемый модуль аутентификации с помощью смарт-карт PKCS-11.

17.4.1. Использование модуля аутентификации Pam_p11

Пакет подгружаемого модуля аутентификации Pam_p11 `libpam-p11` содержит в своем составе два модуля аутентификации:

– `pam_p11_openssh` — подгружаемый модуль аутентификации пользователя с помощью файла ключей `openssh`, расположенного в `~/.ssh/authorized_keys`;

– `pam_p11_opensc` — подгружаемый модуль аутентификации пользователя с помощью списка доверенных сертификатов пользователя, расположенного в `~/.eid/authorized_certificates`.

Для использования аутентификации с помощью смарт-карт PKCS-11 в секции `auth` соответствующего сценария аутентификации в каталоге `/etc/pam.d` необходимо указать использование модуля и его параметры. Например в общем сценарии аутентификации `/etc/pam.d/common_auth` возможно следующее указание:

```
# here are the per-package modules (the "Primary" block)
auth [success=ignore default=die] pam_tally.so per_user deny=10
auth [success=2 default=ignore]   pam_p11_opensc.so \
                                   /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so
auth [success=1 default=ignore]   pam_unix.so nullok_secure try_first_pass
```

Здесь в первую очередь указано использование модуля аутентификации `pam_p11_opensc`. В качестве параметра задается путь к библиотеке `opensc-pkcs11.so`. Если аутентификация с помощью устройства PKCS-11 не была успешно произведена или устройство не было подключено, указано применение стандартной процедуры аутентификации Linux.

ВНИМАНИЕ! Для задания принудительного использования аутентификации с помощью смарт-карт в сценарии аутентификации не должно быть указано иных модулей аутентификации кроме `pam_p11_opensc.so`. В этом случае, если аутентификация с помощью устройства PKCS-11 не была успешно произведена или устройство не было подключено, вход в систему будет невозможен.

Должны быть сформированы все необходимые сертификаты и подготовлены персональные носители аутентификационной информации.

Для возможности входа пользователя необходимо сохранить сертификат с его персонального носителя (смарт-карты) в списке доверенных сертификатов. Список доверенных сертификатов пользователя располагается в файле `authorized_certificates`, расположенном в подкаталоге `~/.eid` его домашнего каталога:

```
mkdir ~/.eid
chmod 0755 ~/.eid
pkcs15-tool -r 45 > ~/.eid/authorized_certificates
chmod 0644 ~/.eid/authorized_certificates
```

При этом указывается уникальный идентификатор сертификата (в примере — `45`) и запрашивается PIN-код владельца токена.

После выполненных действий, данный пользователь может осуществлять локальный вход с помощью смарт-карты, содержащей сохраненный сертификат.

17.4.2. Использование модуля аутентификации PKCS#11

Пакет подгружаемого модуля аутентификации PKCS#11 `libpam-pkcs11` содержит в своем составе модуль аутентификации `pam_pkcs11` и набор модулей отображения полей сертификата в имя пользователя системы:

- `subject` — отображение поля `Subject` сертификата в имя пользователя;
- `pwent` — отображение поля `CN` в поля `login` или `gecos` результата `getpwent()`;
- `ldap` — отображение поля `Subject` сертификата в учетную запись LDAP;
- `opensc` — с помощью списка доверенных сертификатов пользователя, расположенного в `~/.eid/authorized_certificates`;
- `openssh` — с помощью файла ключей `openssh`, расположенного в `~/.ssh/authorized_keys`;
- `mail` — сравнение полей `email` сертификата;
- `ms` — использование расширения Microsoft Universal Principal Name;
- `krb` — сравнение с именем принципала Kerberos;
- `cn` — сравнение поля `CN`;
- `uid` — сравнение уникальных идентификаторов;
- `digest` — отображение цифровой подписи сертификата в имя пользователя;

– generic — настраиваемое отображение содержимого сертификата;

– null — обработка неаутентифицированных пользователей (NULL, nobody);

Модуль отображения отвечает за извлечение соответствующего поля сертификата и сравнение полученного значения с различными видами идентификационной информации. При этом для большинства модулей могут быть использованы соответствующие файлы отображения.

Для проведения процедуры аутентификации может быть указана цепочка используемых модулей отображения. При этом модуль null должен быть указан последним.

Для настройки модуля используется конфигурационный файл pam_pkcs11.conf, который по умолчанию должен быть расположен в каталоге /etc/pam_pkcs11. В этом же каталоге по умолчанию должны располагаться и файлы отображения для модулей отображения.

Конфигурационный файл pam_pkcs11.conf позволяет задать параметры модуля аутентификации, способ работы с устройством PKCS-11, способы проверки сертификата и используемые модули отображения. Для каждого из модулей отображения или работы с устройством PKCS-11 в конфигурационном файле предусмотрены свои секции параметров.

ВНИМАНИЕ! Перед использованием модуля аутентификации должен быть создан каталог /etc/pam_pkcs11, в который должен быть создан и соответствующим образом настроен файл pam_pkcs11.conf из шаблона /usr/share/doc/libpam_pkcs11/examples/pam_pkcs11.conf.example.

Для использования аутентификации с помощью смарт-карт PKCS-11 в секции auth соответствующего сценария аутентификации в каталоге /etc/pam.d необходимо указать использование модуля и его параметры. Например в общем сценарии аутентификации /etc/pam.d/common_auth возможно следующее указание:

```
# here are the per-package modules (the "Primary" block)
auth [success=ignore default=die] pam_tally.so per_user deny=10
auth [success=2 default=ignore]   pam_pkcs11.so
auth [success=1 default=ignore]   pam_unix.so nullok_secure try_first_pass
```

Здесь в первую очередь указано использование модуля аутентификации pam_pkcs11. Если аутентификация с помощью устройства PKCS-11 не была успешно произведена или устройство не было подключено, указано применение стандартной процедуры аутентификации Linux.

ВНИМАНИЕ! Для задания принудительного использования аутентификации с помощью смарт-карт в сценарии аутентификации не должно быть указано иных модулей аутентификации кроме pam_pkcs11.so. В этом случае, если аутентификация с помощью

устройства PKCS-11 не была успешно произведена или устройство не было подключено, вход в систему будет невозможен.

Должны быть сформированы все необходимые сертификаты и подготовлены персональные носители аутентификационной информации.

17.4.2.1. Настройка доступа к устройству PKCS-11

Для использования различных вариантов реализации модулей взаимодействия с устройствами PKCS-11 в конфигурационном файле предусмотрен параметр `use_pkcs11_module`, значением которого должно являться имя раздела конфигурационного файла, описывающего параметры конкретного модуля взаимодействия с устройствами PKCS-11.

Одним из вариантов является стандартный модуль `opensc`. Для его использования необходимо задать следующие параметры:

```
use_pkcs11_module = opensc
pkcs11_module opensc {
  module = /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so;
  description = "OpenSC PKCS#11 module";
  slot_description = "none";
  ca_dir = /etc/pam_pkcs11/cacerts/cacert.pem;
  cert_policy = ca,signature;
  token_type = "Smart card";
}
```

В качестве параметров задается путь к библиотеке PKCS-11, путь к корневому сертификату и способ проверки сертификата пользователя.

Описание параметров и их возможных значений приведено в шаблоне конфигурационного файла. Также в шаблоне присутствуют примеры использования других модулей взаимодействия с устройствами PKCS-11.

17.4.2.2. Настройка аутентификации по списку доверенных сертификатов

Аутентификации по списку доверенных сертификатов (аналогично применяемой в модуле аутентификации Pam_p11 17.4.1) реализуется модулем отображения `opensc`. Для его использования необходимо задать следующие параметры:

```
use_mappers = opensc
mapper opensc {
  debug = false;
  module = /lib/pam_pkcs11/opensc_mapper.so
}
```

Для возможности входа пользователя необходимо сохранить сертификат с его персонального носителя (смарт-карты) в списке доверенных сертификатов. Список доверен-

ных сертификатов пользователя располагается в файле authorized_certificates, расположенном в подкаталоге ~/.eid его домашнего каталога:

```
mkdir ~/.eid
chmod 0755 ~/.eid
pkcs15-tool -r 45 > ~/.eid/authorized_certificates
chmod 0644 ~/.eid/authorized_certificates
```

При этом указывается уникальный идентификатор сертификата (в примере — 45) и запрашивается PIN-код владельца токена.

После выполненных действий, данный пользователь может осуществлять локальный вход с помощью смарт-карты, содержащей сохраненный сертификат.

17.4.2.3. Настройка аутентификации по полям сертификата

Рассмотрим аутентификацию по полям сертификата на примере использования поля Subject.

Аутентификация по полю Subject сертификата реализуется модулем отображения subject. При проведении аутентификации из сертификата извлекается поле subject, по значению которого из файла отображения /etc/pam_pkcs11/subject_mapping выбирается имя пользователя.

Для использования модуля отображения subject необходимо задать следующие параметры:

```
use_mappers = subject
mapper subject {
  debug = false;
  module = internal;
  ignorecase = false;
  mapfile = file:///etc/pam_pkcs11/subject_mapping;
}
```

Файл отображения /etc/pam_pkcs11/subject_mapping имеет следующий вид:

```
# Mapping file for Certificate Subject
# format: Certificate Subject -> login
#
/C=RU/ST=Moscow/L=Moscow/O=RBT/CN=testuser -> testuser
```

Аналогичным образом настраивается использование и других модулей отображения (mail, cn и др.).

17.5. Настройка доменного входа (ЕПП)

При использовании ЕПП для аутентификации пользователей применяется доверенная аутентификация Kerberos (см. 6.4). По умолчанию аутентификации производится по паролю пользователя. В тоже время существует стандарт использования криптогра-

фии с открытым ключом в качестве фактора аутентификации в протоколе аутентификации Kerberos PKINIT (Public Key Cryptography for Initial Authentication in Kerberos). Это позволяет применять сертификаты, и следовательно устройства PKCS-11 для аутентификации по Kerberos.

Для используемого варианта Kerberos (MIT Kerberos V5) возможности PKINIT реализуются пакетом расширения `krb5-pkinit`. При этом для проведения аутентификации используется подгружаемый модуль аутентификации `libpam-krb5`.

ВНИМАНИЕ! Перед настройкой доменного входа с помощью сертификатов с устройств PKCS-11 должны быть выполнены следующие условия:

1) установлена и соответствующим образом настроена служба Astra Linux Directory (см. 6.6);
2) настроен домен ЕПП, созданы необходимые пользователи;
3) на компьютеры домена установлен пакет расширения `krb5-pkinit`;
4) получен или создан корневой сертификат CA (см.17.3.1).

17.5.1. Создание ключа и сертификата контролера домена KDC

Создание ключа и сертификата контролера домена KDC выполняется согласно ранее описанному алгоритму (разделы 17.3.2, 17.3.3, 17.3.4) следующим образом:

1) создается ключевая пара KDC:

```
openssl genrsa -out kdckey.pem 2048
```

2) создается заявка на сертификат:

```
openssl req -new -out kdc.req -key kdckey.pem
```

При этом в поле `CN` указывается имя домена.

3) выписывается сертификат:

```
export REALM=<домен>
export CLIENT=<имя сервера>
openssl x509 -req -in kdc.req -CAkey cakey.pem -CA cacert.pem
 -out kdc.pem -extfile pkinit_extensions -extensions kdc_cert
 -CAcreateserial
```

Для выписывания сертификата необходимо наличие файла `pkinit_extensions` (см.17.5.5) и заданных заранее значений переменных окружения `REALM` и `CLIENT`. В качестве клиента в этом случае выступает имя сервера домена.

Примечание. Опция `-CAcreateserial` служит для создания серийного номера нового сертификата. Нужно только первый раз, затем используется опция `-CAserial cacert.srl` для увеличения этого номера.

17.5.2. Создание ключей и сертификатов пользователей ЕПП

Создание ключей и сертификатов пользователей ЕПП выполняется согласно ранее описанному алгоритму (разделы 17.3.2, 17.3.3, 17.3.4).

ВНИМАНИЕ! Все операции по генерации ключей и формированию заявок на сертификаты должны выполняться с использованием персональных носителей аутентификационной информации пользователей.

Выписывание сертификата выполняется следующим образом:

```
export REALM=<домен>
export CLIENT=<имя пользователя>
openssl x509 -req -in client.req -CAkey cakey.pem -CA cacert.pem
 -extensions client_cert -extfile pkinit_extensions -out client.pem
```

Для выписывания сертификата необходимо наличие файла `pkinit_extensions` (см.17.5.5) и заданных заранее значений переменных окружения `REALM` и `CLIENT`. В качестве клиента в этом случае выступает имя пользователя домена.

17.5.3. Настройка сервера ЕПП

Полученные ранее ключи и сертификаты контролера домена KDC должны быть помещены в каталог `/var/lib/krb5kdc/`:

– `kdckey.pem` — секретный ключ KDC;

– `kdc.pem` — сертификат KDC;

– `cacert.pem` — корневой сертификат.

В конфигурационном файле сервера Kerberos `/etc/krb5kdc/kdc.conf` должны быть указаны пути к используемым ключам и сертификатам:

```
[kdcdefaults]
    kdc_tcp_ports = 88
    pkinit_identity = FILE:/var/lib/krb5kdc/kdc.pem,/var/lib/krb5kdc/kdckey.pem
    pkinit_anchors = FILE:/var/lib/krb5kdc/cacert.pem
```

Так же для вновь создаваемых пользователей домена необходимо включить флаг `preauth` в соответствующей секции конфигурационного файла `/etc/krb5kdc/kdc.conf`, например:

```
[realms]
    TEST.RU = {
      ...
      default_principal_flags = +preauth
}
```

ВНИМАНИЕ! Kerberos принципалы пользователей домена должны иметь флаг `requires_preauth`.

После завершения настроек службы Kerberos должны быть перезапущены.

ВНИМАНИЕ! Для сохранения настроек при переинициализации домена указанные изменения должны быть внесены и в шаблон конфигурационного файла `/etc/ald/config-templates/kdc.conf`.

17.5.4. Настройка рабочих мест

На компьютерах домена, где предполагается использовать аутентификацию с помощью устройств PKCS-11, должен быть создан каталог `/etc/krb5/`, в котором необходимо разместить корневой сертификат `cacert.pem` и при необходимости сертификаты пользователей.

Также в конфигурационном файле `/etc/krb5.conf` должны быть указаны пути к корневому сертификату УЦ и модулю взаимодействия PKCS-11:

```
[libdefaults]
    default_realm = TEST.RU
    pkinit_anchors = FILE:/etc/krb5/cacert.pem
    pkinit_identities = PKCS11:/usr/lib/x86_64-linux-gnu/opensc-pkcs11.so
```

ВНИМАНИЕ! Для сохранения настроек при переинициализации домена указанные изменения должны быть внесены и в шаблон конфигурационного файла `/etc/ald/config-templates/krb5.conf`.

Для реализации аутентификации Kerberos используется модуль аутентификации `pam_krb5.so`, расположенный в пакете `libpam-krb5`.

При использовании PKINIT существует возможность указания дополнительных параметров модуля аутентификации `pam_krb5.so` в файле `/etc/pam.d/common-auth` в строке относящейся к `pam_krb5.so`:

– `try_pkinit` — режим при котором осуществляется попытка аутентификации с помощью устройтсв PKCS-11, в случае провала попытки предоставляется возможность входа с помощью Kerberos пароля пользователя;

– `use_pkinit` — режим при котором требуется аутентификация с помощью устройтсв PKCS-11, в случае провала процесс входа прерывается;

– `pkinit_prompt` — вывод приглашения для подключения устройства PKCS-11 перед выполнением попытки входа.

Более подробное описание см. в руководстве `man`.

17.5.5. Пример `pkinit_extensions`

При выписывании сертификата как правило используются специальные файлы расширений OpenSSL, в которых указываются дополнительные используемые поля сертификатов. Например, в случае использования PKINIT, конфигурация задается файлом `pkinit_extensions`, в котором указаны дополнительные поля сертификатов, используемых в Kerberos:

– Extended Key Usage (EKU) — идентификатор (OID), говорящий о том, как планируется использовать сертификат;

– otherName — поле, задающее принципала Kerberos, для которого выписывается сертификат.

Пример файла `pkinit_extensions`:

```
[ kdc_cert ]
basicConstraints=CA:FALSE

# Here are some examples of the usage of nsCertType. If it is omitted
keyUsage = nonRepudiation, digitalSignature, keyEncipherment, keyAgreement

#Pkinit EKU
extendedKeyUsage = 1.3.6.1.5.2.3.5

subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer

# Copy subject details

issuerAltName=issuer:copy

# Add id-pkinit-san (pkinit subjectAlternativeName)
subjectAltName=otherName:1.3.6.1.5.2.2;SEQUENCE:kdc_princ_name

[kdc_princ_name]
realm = EXP:0, GeneralString:${ENV::REALM}
principal_name = EXP:1, SEQUENCE:kdc_principal_seq

[kdc_principal_seq]
name_type = EXP:0, INTEGER:1
name_string = EXP:1, SEQUENCE:kdc_principals

[kdc_principals]
princ1 = GeneralString:krbtgt
princ2 = GeneralString:${ENV::REALM}

[ client_cert ]

# These extensions are added when 'ca' signs a request.

basicConstraints=CA:FALSE
```

```
keyUsage = digitalSignature, keyEncipherment, keyAgreement

extendedKeyUsage = 1.3.6.1.5.2.3.4
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer


subjectAltName=otherName:1.3.6.1.5.2.2;SEQUENCE:princ_name


# Copy subject details

issuerAltName=issuer:copy

[princ_name]
realm = EXP:0, GeneralString:${ENV::REALM}
principal_name = EXP:1, SEQUENCE:principal_seq

[principal_seq]
name_type = EXP:0, INTEGER:1
name_string = EXP:1, SEQUENCE:principals

[principals]
princ1 = GeneralString:${ENV::CLIENT}
```

17.6. Применение Rutoken ECP

Электронный идентификатор Rutoken — это компактное устройство в виде USB-брелока, которое служит для авторизации пользователя в сети или на локальном компьютере, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам, а также надежного хранения персональных данных.

Операции с токеном осуществляются путем выполнения команд PKCS утилит командной сроки (вида `pkcs15-*` и `pkcs11-*`).

ВНИМАНИЕ! Для функционирования Rutoken ECP необходимы следующие программные пакеты: `libccid`, `pcscd`, `libpcsclite1`.

17.6.1. Инициализация токена

Для инициализации токена необходимо выполнить следующую последовательность действий:

```
pkcs15-init --erase-card
pkcs15-init --create-pkcs15 --so-pin "87654321" --so-puk ""
pkcs15-init --store-pin --label "User PIN" --auth-id 02 --pin "12345678"
```

```
--puk "" --so-pin "87654321" --finalize
```

Первая команда выполняет полное стирание носителя. Вторая форматирует носитель в соответствии с PKCS-15 с заданием PIN-кода администратора, а последняя формирует PIN-код пользователя-владельца носителя, который будет использоваться впоследствии для подтверждения операций с носителем.

17.6.2. Создание сертификата на токене

Получение готового токена пользователя производится в соответствии с описанным ранее алгоритмом с помощью утилит PKCS и утилиты `openssl`:

1) генерируется ключевая пара пользователя (17.3.2);
2) создается заявка на сертификат (17.3.3);
3) выписыватеся сертификат (17.3.4);
4) полученный сертификат сохраняется на токене (17.3.6).

ВНИМАНИЕ! При работе с токеном следует учитывать слот, к которому подключено устройство и идентификатор пользователя, которому принадлежит токен.

18. СООБЩЕНИЯ АДМИНИСТРАТОРУ

При возникновении проблем в процессе функционирования ОС появляются диагностические сообщения трех типов: информационные, предупреждающие и сообщения об ошибках (примеры приведены в таблицах 54– 56, соответственно). Администратор должен проанализировать диагностические сообщения и принять меры по устранению появившихся проблем.

Таблица 54 – Информационные сообщения

Сообщение ОС	Что означает сообщение	Файл
`Setting hostname to <>`	Установка имени хоста <>	`hostname`
`Setting domainname to <>`	Установка имени домена как <>	`hostname`
`Statistics dump initiated`	Вывод статистики запущен	`named`
`Query logging is now on`	Регистрация очередей включена	`named`
`Query logging is now off`	Регистрация очередей выключена	`named`
`Unknown host`	Неизвестный хост	`dnsquery`
`Non reloadable zone`	Не перезагружаемая зона	`named`
`Reconfig initiated`	Переконфигурирование запущено	`named`
`Zone not found`	Зона не найдена	`named`

Таблица 55 – Предупреждающие сообщения

Сообщение ОС	Что означает сообщение	Действия по устранению проблемы	Файл
`<>: You can't change the DNS domain name with this command`	Неверное использование команды	Использовать соответствующую команду	`hostname`
`Could not find any active network interfaces`	Активные сетевые интерфейсы не найдены	Активировать сетевой интерфейс	`sendmail`
`You must be root to change the host name`	Недостаточно прав для изменения имени хоста	Обратиться к администратору	`dnsdomainname`

Таблица 56 – Сообщения об ошибках

Сообщение ОС	Что означает сообщение	Действия по устранению проблемы	Файл
`Unknown server error`	Неизвестная ошибка сервера	Изменить права доступа	`dnsquery`
`Resolver internal error`	Внутренняя ошибка резольвера	Изменить права доступа	`dnsquery`

Окончание таблицы 56

Сообщение ОС	Что означает сообщение	Действия по устранению проблемы	Файл
`Superblock last mount time (значение времени) is in the future`	Неверная установка времени	См. 18.1	См. 18.1

18.1. Неверная установка времени

Если в BIOS Setup установить время на будущую дату, загрузиться в ОС, а потом установить верное текущее время, или сразу выставить в BIOS Setup время «из прошлого», то возможна циклическая перезагрузка компьютера.

Во время загрузки ОС, когда на экране появляется заставка с мерцающей надписью «Astra Linux Special Edition», необходимо нажать клавишу **<Esc>**. Если среди сообщений есть, например:

```
/dev/sda1: Superblock last mount time (Wed Feb 15 12:41:05 2017,
            now = Mon Feb 15 12:45:37 2016) is in the future.
```

то проблема связана с неверной установкой времени.

Для ее решения необходимо зайти в меню настройки BIOS или UEFI и проверить настройки системного времени. Если системное время установлено на некоторое время в прошлом, то возможно это связано с аппаратной неисправностью компьютера (отказ батарейки часов реального времени). В этом случае необходимо заменить батарейку реального времени так, как это описано в инструкции к техническому средству и установить системные часы на текущее время.

Если системное время в меню настроек BIOS или UEFI установлено верно, но циклические перезагрузки продолжаются, то неисправность может быть связана с неверным переводом времени на будущую дату и обратно. В этом случае необходимо установить системное время на какой-нибудь момент в будущем (позже того момента, который упоминался в сообщении об ошибке при загрузке), загрузить ОС и выполнить следующие действия:

1) Создать файл `/etc/ef2fsck.conf` с содержимым:

```
[options]
broken_system_clock = true
```

2) Создать файл `/etc/initramfs-tools/hooks/e2fsck-conf.sh` с содержимым:

```
#!/bin/sh
```

```
PREREQ=""
prereqs()
{
   echo "$PREREQ"
}

case $1 in
prereqs)
   prereqs
   exit 0
   ;;
esac

. /usr/share/initramfs-tools/hook-functions
CONFFILE=/etc/e2fsck.conf
CONFDIR=`dirname "$CONFFILE"`
if [ -f "$CONFFILE" ]
then
   mkdir -p ${DESTDIR}${CONFDIR}
   cp $CONFFILE ${DESTDIR}${CONFDIR}
fi
```

3) Запустить команду:

```
sudo update-initramfs -u
```

4) Далее необходимо перезагрузить ОС и установить системное время в текущее.

ПРИЛОЖЕНИЕ А
(справочное)

ПЕРЕЧЕНЬ ПАКЕТОВ ОС

А.1. БАЗОВАЯ СИСТЕМА

acpi
acpi-support-base
acpid
adduser
apt
apt-utils
apt-xapian-index
aptitude
aptitude-common
astra-extra
astra-safepolicy
base-files
base-passwd
bash
bsdmainutils
bsdutils
busybox
bzip2
console-setup
console-setup-linux
coreutils
cpio
cracklib-runtime
cron
dash
debconf
debconf-i18n
debconf-utils
debian-archive-keyring
debianutils
diffutils
dmidecode
dmsetup
dpkg
e2fslibs:amd64
e2fsprogs
eject
emdebian-archive-keyring
ept-cache
expect
expect-dev
file
findutils
fontconfig
fontconfig-config
fonts-dejavu-core
gawk
gcc-4.7-base:amd64
gettext-base
gnupg
gpgv
grep
groff-base
grub-common
grub-pc
grub-pc-bin
grub2-common
gzip
hostname
ifupdown

info
init-system-helpers
initramfs-tools
initscripts
insserv
install-info
installation-report
iproute
iptables
iputils-ping
isc-dhcp-client
isc-dhcp-common
kbd
keyboard-configuration
klibc-utils
kmod
laptop-detect
libacl1:amd64
libapt-inst1.5:amd64
libapt-pkg4.12:amd64
libasprintf0c2:amd64
libatk1.0-0:amd64
libatk1.0-data
libattr1:amd64
libaudit-common
libaudit1:amd64
libavahi-client3:amd64
libavahi-common-data:amd64
libavahi-common3:amd64
libblkid1:amd64
libboost-iostreams1.49.0
libboost-iostreams1.55.0:amd64
libbz2-1.0:amd64
libc-bin
libc6:amd64
libcairo2:amd64
libcap2:amd64
libclass-isa-perl
libcomerr2:amd64
libcrack2:amd64
libcups2:amd64
libcwidget3
libdatrie1:amd64
libdb5.1:amd64
libdbus-1-3:amd64
libdevmapper1.02.1:amd64
libdrm2:amd64
libegl1-mesa:amd64
libept1.4.12
libexpat1:amd64
libffi5:amd64
libfontconfig1:amd64
libfreetype6:amd64
libfuse2:amd64
libgbm1:amd64
libgcc1:amd64
libgcrypt11:amd64
libgdbm3:amd64
libgdk-pixbuf2.0-0:amd64
libgdk-pixbuf2.0-common
libgl1-mesa-glx:amd64
libglapi-mesa:amd64
libglib2.0-0:amd64
libgnutls26:amd64
libgost
libgpg-error0:amd64
libgssapi-krb5-2:amd64
libgtk2.0-0:amd64
libgtk2.0-common
libident
libidn11:amd64
libjasper1:amd64

libjbig0:amd64
libjpeg8:amd64
libk5crypto3:amd64
libkeyutils1:amd64
libklibc
libkmod2:amd64
libkrb5-3:amd64
libkrb5support0:amd64
liblocale-gettext-perl
liblzma5:amd64
libmagic1:amd64
libmount1
libncurses5:amd64
libncursesw5:amd64
libnewt0.52
libnfnetlink0
libnih-dbus1
libnih1
libp11-kit0:amd64
libpam-cracklib:amd64
libpam-modules:amd64
libpam-modules-bin
libpam-runtime
libpam0g:amd64
libpango1.0-0:amd64
libparsec-aud2
libparsec-base2
libparsec-cap2
libpci3:amd64
libpcre3:amd64
libpdp
libpipeline1:amd64
libpixman-1-0:amd64
libpng12-0:amd64
libpopt0:amd64
libprocps0:amd64
libreadline6:amd64
libselinux1:amd64
libsemanage-common
libsemanage1:amd64
libsepol1:amd64
libsigc++-1.2-5c2
libsigc++-2.0-0c2a:amd64
libsigsegv2
libslang2:amd64
libsqlite3-0:amd64
libss2:amd64
libssl1.0.0:amd64
libstdc++6:amd64
libswitch-perl
libsysfs2:amd64
libtasn1-3:amd64
libtext-charwidth-perl
libtext-iconv-perl
libtext-wrapi18n-perl
libthai-data
libthai0:amd64
libtiff5:amd64
libtinfo5:amd64
libudev0:amd64
libusb-0.1-4:amd64
libusb-1.0-0:amd64
libustr-1.0-1:amd64
libuuid1:amd64
libwayland-client0:amd64
libwayland-server0:amd64
libx11-6:amd64
libx11-data
libx11-xcb1:amd64
libx86-1:amd64
libxapian22
libxau6:amd64

libxcb-dri2-0:amd64
libxcb-dri3-0:amd64
libxcb-glx0:amd64
libxcb-present0:amd64
libxcb-randr0:amd64
libxcb-render0:amd64
libxcb-shape0:amd64
libxcb-shm0:amd64
libxcb-sync1:amd64
libxcb-xfixes0:amd64
libxcb1:amd64
libxcomposite1:amd64
libxcursor1:amd64
libxdamage1:amd64
libxdmcp6:amd64
libxext6:amd64
libxfixes3:amd64
libxft2:amd64
libxi6:amd64
libxinerama1:amd64
libxml2:amd64
libxrandr2:amd64
libxrender1:amd64
libxshmfence1:amd64
libxtables10
libxxf86vm1:amd64
linux-image-4.2-generic
linux-image-4.2.0-23-generic
locales
login
logrotate
lsb-base
makedev
man-db
manpages
mawk
mime-support
module-init-tools
mount
mountall
multiarch-support
nano
ncurses-base
ncurses-bin
net-tools
netbase
os-prober
passwd
pciutils
perl
perl-base
perl-modules
plymouth
plymouth-drm
plymouth-themes
plymouth-x11
procps
python
python-apt
python-apt-common
python-chardet
python-debian
python-minimal
python-support
python-xapian
python2.7
python2.7-minimal
readline-common
rsyslog
sed
sensible-utils
shared-mime-info

sudo
sysv-rc
sysvinit
sysvinit-utils
tar
tasksel
tasksel-data
tcl8.5
tcl8.5-dev
traceroute
ttf-dejavu-core
tzdata
ubuntu-keyring
ucf
udev
usbutils
util-linux
v86d
vim-common
vim-tiny
wamerican
wget
whiptail
xkb-data
xz-utils
zlib1g:amd64

А.2. БАЗОВЫЕ СРЕДСТВА

acpi
acpi-support
acpi-support-base
acpid
adduser
afick
anacron
apt
apt-doc
apt-transport-https
apt-utils
apt-xapian-index
aptitude
aptitude-common
aspell
aspell-en
aspell-ru
astra-extra
astra-safepolicy
atftp
avahi-autoipd
base-files
base-passwd
bash
bc
bluetooth
bluez
bsdmainutils
bsdutils
bsign
busybox
bzip2
chkconfig
console-setup
console-setup-linux
coreutils
cpio
cpp
cpp-4.7
cracklib-runtime
crda
cron
cups
cups-bsd
cups-client
cups-common
cups-filters
cups-ppdc
dash
dbus
debconf
debconf-i18n
debconf-utils
debian-archive-keyring
debianutils
dictionaries-common
diffutils
dmidecode
dmsetup
dosfstools
dpkg
dvd+rw-tools
e2fslibs:amd64
e2fsprogs
eject
emdebian-archive-keyring
ept-cache
exim4-base

exim4-config
exim4-daemon-light
expect
expect-dev
fakeroot
file
findutils
fontconfig
fontconfig-config
fonts-dejavu-core
fonts-freefont-ttf
foomatic-db
fuse
gawk
gcc-4.7-base:amd64
genisoimage
gettext
gettext-base
ghostscript
gir1.2-glib-2.0
gnupg
gostsum
gpgv
gpm
grep
groff-base
growisofs
grub-common
grub-pc
grub-pc-bin
grub2-common
gsfonts
gutenprint-locales
gzip
hostname
ia32-libs
ifupdown
info
init-system-helpers
initramfs-tools
initscripts
insserv
install-info
installation-report
iproute
iptables
iputils-ping
irussian
isc-dhcp-client
isc-dhcp-common
ispell
kbd
keyboard-configuration
klibc-utils
kmod
laptop-detect
less
lib32asound2
lib32bz2-1.0
lib32gcc1
lib32ncurses5
lib32stdc++6
lib32tinfo5
lib32v4l-0
lib32z1
libacl1:amd64
libapt-inst1.5:amd64
libapt-pkg-doc
libapt-pkg4.12:amd64
libasound2:amd64
libaspell15
libasprintf0c2:amd64

libatk1.0-0:amd64
libatk1.0-data
libattr1:amd64
libaudit-common
libaudit1:amd64
libavahi-client3:amd64
libavahi-common-data:amd64
libavahi-common3:amd64
libblkid1:amd64
libboost-iostreams1.49.0
libboost-iostreams1.55.0:amd64
libbsd0:amd64
libbz2-1.0:amd64
libc-bin
libc6:amd64
libc6-i386
libcairo2:amd64
libcap-ng0
libcap2:amd64
libclass-isa-perl
libcomerr2:amd64
libconfig++9:amd64
libcrack2:amd64
libcroco3:amd64
libcups2:amd64
libcupscgi1:amd64
libcupsfilters1:amd64
libcupsimage2:amd64
libcupsmime1:amd64
libcupsppdc1:amd64
libcurl3-gnutls:amd64
libcwidget3
libdaemon0
libdatrie1:amd64
libdb5.1:amd64
libdbus-1-3:amd64
libdbus-glib-1-2:amd64
libdevmapper1.02.1:amd64
libdrm2:amd64
libedit2:amd64
libegl1-mesa:amd64
libept1.4.12
libevdev2
libexpat1:amd64
libffi5:amd64
libfile-copy-recursive-perl
libfontconfig1:amd64
libfontembed1:amd64
libfreetype6:amd64
libfuse2:amd64
libgbm1:amd64
libgcc1:amd64
libgcrypt11:amd64
libgdbm3:amd64
libgdk-pixbuf2.0-0:amd64
libgdk-pixbuf2.0-common
libgettextpo0:amd64
libgirepository-1.0-1
libgl1-mesa-glx:amd64
libglapi-mesa:amd64
libglib2.0-0:amd64
libgmp10:amd64
libgnutls26:amd64
libgomp1:amd64
libgost
libgpg-error0:amd64
libgpm2:amd64
libgraphite2-2.0.0
libgs9
libgs9-common
libgssapi-krb5-2:amd64
libgtk2.0-0:amd64

libgtk2.0-common
libgutenprint2
libharfbuzz0b:amd64
libice6:amd64
libicu52:amd64
libident
libidn11:amd64
libijs-0.35
libinput10:amd64
libipc-signal-perl
libiw30:amd64
libjasper1:amd64
libjbig0:amd64
libjbig2dec0
libjpeg8:amd64
libk5crypto3:amd64
libkeyutils1:amd64
libklibc
libkmod2:amd64
libkrb5-3:amd64
libkrb5support0:amd64
liblcms2-2:amd64
libldap-2.4-2:amd64
liblocale-gettext-perl
liblockfile-bin
liblockfile1:amd64
liblzma5:amd64
libmagic1:amd64
libmime-types-perl
libmount1
libmpc2:amd64
libmpfr4:amd64
libmtdev1:amd64
libnatspec0
libncurses5:amd64
libncursesw5:amd64
libnewt0.52
libnfnetlink0
libnih-dbus1
libnih1
libnl-3-200:amd64
libnl-genl-3-200:amd64
libopenjpeg2:amd64
libopts25
libp11-kit0:amd64
libpam-cracklib:amd64
libpam-modules:amd64
libpam-modules-bin
libpam-runtime
libpam0g:amd64
libpango1.0-0:amd64
libpaper1:amd64
libparsec-aud-db-legacy2
libparsec-aud2
libparsec-base2
libparsec-cap-db-legacy2
libparsec-cap2
libparsec-iss2
libparsec-log2
libparsec-mac-db-legacy2
libparsec-mac2
libparsec-mic2
libpci3:amd64
libpcre3:amd64
libpcsclite1:amd64
libpdac++
libpdp
libperl5.14
libpipeline1:amd64
libpixman-1-0:amd64
libpng12-0:amd64
libpoppler44:amd64

libpopt0:amd64
libproc-waitstat-perl
libprocps0:amd64
libproxy1:amd64
libqpdf13:amd64
libqt5core5a:amd64
libqt5dbus5:amd64
libqt5gui5:amd64
libqt5network5:amd64
libqt5widgets5:amd64
libqt5xcbqpa5:amd64
libreadline5:amd64
libreadline6:amd64
librtmp0:amd64
libsasl2-2:amd64
libselinux1:amd64
libsemanage-common
libsemanage1:amd64
libsensors4:amd64
libsepol1:amd64
libsigc++-1.2-5c2
libsigc++-2.0-0c2a:amd64
libsigsegv2
libslang2:amd64
libslp1
libsm6:amd64
libsnmp-base
libsnmp15
libsqlite3-0:amd64
libss2:amd64
libssh2-1:amd64
libssl1.0.0:amd64
libstdc++6:amd64
libswitch-perl
libsysfs2:amd64
libsystemd-login0:amd64
libtasn1-3:amd64
libtext-charwidth-perl
libtext-iconv-perl
libtext-wrapi18n-perl
libthai-data
libthai0:amd64
libtiff5:amd64
libtinfo5:amd64
libudev0:amd64
libunistring0:amd64
libusb-0.1-4:amd64
libusb-1.0-0:amd64
libustr-1.0-1:amd64
libuuid1:amd64
libv4l-0:amd64
libv4lconvert0:amd64
libwayland-client0:amd64
libwayland-server0:amd64
libwrap0:amd64
libx11-6:amd64
libx11-data
libx11-xcb1:amd64
libx86-1:amd64
libxapian22
libxau6:amd64
libxaw7:amd64
libxcb-dri2-0:amd64
libxcb-dri3-0:amd64
libxcb-glx0:amd64
libxcb-icccm4:amd64
libxcb-image0:amd64
libxcb-keysyms1:amd64
libxcb-present0:amd64
libxcb-randr0:amd64
libxcb-render-util0:amd64
libxcb-render0:amd64

libxcb-shape0:amd64
libxcb-shm0:amd64
libxcb-sync1:amd64
libxcb-util0:amd64
libxcb-xfixes0:amd64
libxcb-xinerama0:amd64
libxcb-xkb1:amd64
libxcb1:amd64
libxcomposite1:amd64
libxcursor1:amd64
libxdamage1:amd64
libxdmcp6:amd64
libxext6:amd64
libxfixes3:amd64
libxft2:amd64
libxi6:amd64
libxinerama1:amd64
libxkbcommon-x11-0:amd64
libxkbcommon0:amd64
libxml2:amd64
libxmu6:amd64
libxmuu1:amd64
libxpm4:amd64
libxrandr2:amd64
libxrender1:amd64
libxshmfence1:amd64
libxt6:amd64
libxtables10
libxxf86vm1:amd64
linux-astra-modules
linux-astra-modules-4.2.0-23-generic
linux-astra-modules-4.2.0-23-pax
linux-astra-modules-common
linux-astra-modules-generic
linux-astra-modules-pax
linux-doc
linux-firmware
linux-image-4.2-generic
linux-image-4.2.0-23-generic
linux-image-4.2.0-23-pax
linux-image-extra-4.2.0-23-generic
linux-image-pax
locales
lockfile-progs
logcheck
login
logrotate
logtail
lsb-base
lsb-release
lsof
makedev
man-db
manpages
manpages-ru
mawk
mc
mc-data
mime-construct
mime-support
module-init-tools
mount
mountall
mueller7-dict
multiarch-support
myspell-ru
nano
ncurses-base
ncurses-bin
net-tools
netbase
ntfs-3g

ntp
openprinting-ppds
openssh-client
openssl
os-prober
p7zip-full
p7zip-rar
parsec
parsec-aud
parsec-base
parsec-cap
parsec-cups
parsec-iss
parsec-log
parsec-mac
parsec-tests
parsec-tools
passwd
pciutils
pcmciautils
pdp
perl
perl-base
perl-modules
perl-tk
plymouth
plymouth-drm
plymouth-themes
plymouth-x11
pm-utils
poppler-data
poppler-utils
powermgmt-base
powertop
printer-driver-gutenprint
procps
psmisc
python
python-apt
python-apt-common
python-chardet
python-dbus
python-dbus-dev
python-debian
python-gi
python-gobject
python-gobject-2
python-minimal
python-support
python-wicd
python-xapian
python2.7
python2.7-minimal
python3
python3-minimal
python3.2
python3.2-minimal
readline-common
rsh-client
rsyslog
sed
sensible-utils
shared-mime-info
slptool
snmp
ssl-cert
sudo
sysv-rc
sysvinit
sysvinit-utils
tar
tasksel

tasksel-data
tcl8.5
tcl8.5-dev
traceroute
ttf-dejavu-core
tzdata
ubuntu-keyring
ucf
udev
ufw
unrar
unzip
update-inetd
usbutils
userinfo
util-linux
util-linux-locales
v86d
vim
vim-common
vim-doc
vim-runtime
vim-tiny
wamerican
wget
whiptail
wicd
wicd-cli
wicd-daemon
wireless-regdb
wireless-tools
wpasupplicant
x11-common
x11-xserver-utils
xkb-data
xz-utils
zlib1g:amd64

А.3. РАБОЧИЙ СТОЛ FLY

acl
acpi
acpi-support
acpi-support-base
acpid
adduser
afick
alsa-base
alsa-utils
anacron
apt
apt-doc
apt-transport-https
apt-utils
apt-xapian-index
aptitude
aptitude-common
asciidoc
aspell
aspell-en
aspell-ru
astra-extra
astra-safepolicy
at-spi2-core
at-spi2-doc
atftp
avahi-autoipd
avahi-daemon
base-files
base-passwd
bash
bc
bind9-host
bluetooth
bluez
brasero
brasero-cdrkit
brasero-common
browser-plugin-gnash
bsdmainutils
bsdutils
bsign
busybox
bzip2
chkconfig
compton
connman
console-setup
console-setup-linux
consolekit
coreutils
cpio
cpp
cpp-4.7
cracklib-runtime
crda
cron
cups
cups-bsd
cups-client
cups-common
cups-filters
cups-pk-helper
cups-ppdc
curlftpfs
dash
dbus
dbus-x11

dconf-gsettings-backend:amd64
dconf-service
debconf
debconf-i18n
debconf-utils
debian-archive-keyring
debianutils
desktop-base
desktop-file-utils
dictionaries-common
diffutils
dmidecode
dmsetup
dosfstools
dpkg
dvd+rw-tools
e2fslibs:amd64
e2fsprogs
easypaint
eject
emdebian-archive-keyring
ept-cache
exim4-base
exim4-config
exim4-daemon-light
expect
expect-dev
fakeroot
file
findutils
fly-admin-autostart
fly-admin-center
fly-admin-cron
fly-admin-date
fly-admin-device-manager
fly-admin-dm
fly-admin-env
fly-admin-fonts
fly-admin-gamma
fly-admin-gmc
fly-admin-grub2
fly-admin-int-check
fly-admin-local
fly-admin-local-se
fly-admin-marker
fly-admin-power
fly-admin-printer
fly-admin-printer-mac
fly-admin-reflex
fly-admin-runlevel
fly-admin-service
fly-admin-viewaudit
fly-admin-wicd
fly-admin-winprops
fly-admin-wm
fly-all-main
fly-all-optional
fly-all-qml
fly-alternatives
fly-calc
fly-contacts
fly-data
fly-dialer
fly-dm
fly-doc
fly-fm
fly-fm-audit
fly-fm-bsign
fly-fm-libs
fly-fm-mac
fly-fontconfig-settings
fly-hexedit

fly-image
fly-jobviewer
fly-kiosk
fly-launcher
fly-mac-dialog
fly-mail
fly-notes
fly-passwd
fly-phone-db-client
fly-phone-dbus
fly-phone-webbrowser
fly-phone-widgets
fly-photocamera
fly-plastique-style
fly-policykit-1
fly-print-monitor
fly-qdm
fly-qml-components
fly-qml-dialer
fly-randr
fly-record
fly-reflex
fly-reflex-service
fly-run
fly-run-sumac
fly-scan
fly-secretsservice
fly-shutdown-dialog
fly-sms
fly-snapshot
fly-start-panel
fly-su
fly-system-monitor
fly-system-monitor-mac-plugin
fly-term
fly-videocamera
fly-vkbd
fly-winprops-service
fly-wm
fly-xkbmap
flyqt5platformtheme
flyui-utils
fontconfig
fontconfig-config
fonts-croscore
fonts-crosextra-carlito
fonts-dejavu-core
fonts-freefont-ttf
fonts-liberation
fonts-pt
fonts-pt-mono
fonts-pt-sans
fonts-pt-serif
fonts-wine-tahoma
foomatic-db
foomatic-filters
freeglut3:amd64
freetype2-demos
fuse
gawk
gcc-4.7-base:amd64
genisoimage
gettext
gettext-base
ghostscript
gir1.2-atspi-2.0
gir1.2-glib-2.0
glib-networking:amd64
glib-networking-common
glib-networking-services
gmc-common
gmc-miscellaneous

gmc-miscellaneous-se
gnash
gnash-common
gnome-icon-theme
gnupg
goldendict
gostsum
gparted
gpgv
gpm
grep
groff-base
growisofs
grub-common
grub-pc
grub-pc-bin
grub2-common
gsettings-desktop-schemas
gsfonts
gstreamer0.10-alsa:amd64
gstreamer0.10-plugins-base:amd64
gstreamer0.10-plugins-good:amd64
gutenprint-locales
guvcview
gvfs:amd64
gvfs-common
gvfs-daemons
gvfs-libs:amd64
gzip
hicolor-icon-theme
hostname
hpijs-ppds
hplip
hplip-data
hplip-gui
ia32-libs
ifupdown
iio-sensor-proxy
imagemagick-common
info
init-system-helpers
initramfs-tools
initscripts
inotify-tools
input-utils
insserv
install-info
installation-report
iproute
iptables
iputils-ping
irussian
isc-dhcp-client
isc-dhcp-common
iso-codes
ispell
juffed
kbd
keyboard-configuration
klibc-utils
kmod
laptop-detect
less
lesstif2:amd64
lib32asound2
lib32bz2-1.0
lib32gcc1
lib32ncurses5
lib32stdc++6
lib32tinfo5
lib32v4l-0
lib32z1

liba52-0.7.4
libaa1:amd64
libacl1:amd64
libao-common
libao4
libapt-inst1.5:amd64
libapt-pkg-doc
libapt-pkg4.12:amd64
libarchive13:amd64
libasound2:amd64
libaspell15
libasprintf0c2:amd64
libass4:amd64
libasyncns0:amd64
libatasmart4:amd64
libatk-adaptor:amd64
libatk-adaptor-data
libatk-bridge2.0-0:amd64
libatk1.0-0:amd64
libatk1.0-data
libatkmm-1.6-1
libatspi2.0-0:amd64
libattr1:amd64
libaudio2:amd64
libaudit-common
libaudit1:amd64
libavahi-client3:amd64
libavahi-common-data:amd64
libavahi-common3:amd64
libavahi-core7:amd64
libavc1394-0:amd64
libavcodec55:amd64
libavformat55:amd64
libavresample1:amd64
libavutil53:amd64
libbind9-80
libblkid1:amd64
libbluray1:amd64
libboost-chrono1.55.0:amd64
libboost-iostreams1.49.0
libboost-iostreams1.55.0:amd64
libboost-program-options1.55.0:amd64
libboost-system1.55.0:amd64
libboost-thread1.55.0:amd64
libbrasero-media3-1
libbsd0:amd64
libburn4
libbz2-1.0:amd64
libc-ares2:amd64
libc-bin
libc6:amd64
libc6-i386
libcaca0:amd64
libcairo-gobject2:amd64
libcairo2:amd64
libcairomm-1.0-1
libcanberra-gtk3-0:amd64
libcanberra0:amd64
libcap-ng0
libcap2:amd64
libcddb2
libcdio13
libcdparanoia0
libchromaprint0:amd64
libck-connector0:amd64
libclass-isa-perl
libcolord1:amd64
libcomerr2:amd64
libconfig++9:amd64
libconfig9:amd64
libconnman-qt
libcrack2:amd64

libcroco3:amd64
libcrypto++9
libcrystalhd3:amd64
libcups2:amd64
libcupscgi1:amd64
libcupsfilters1:amd64
libcupsimage2:amd64
libcupsmime1:amd64
libcupsppdc1:amd64
libcurl3-gnutls:amd64
libcwidget3
libdaemon0
libdatrie1:amd64
libdb5.1:amd64
libdbus-1-3:amd64
libdbus-glib-1-2:amd64
libdc1394-22:amd64
libdca0
libdconf0:amd64
libdevmapper-event1.02.1:amd64
libdevmapper1.02.1:amd64
libdirectfb-1.2-9:amd64
libdjvulibre-text
libdjvulibre21
libdmx1:amd64
libdns88
libdrm-intel1:amd64
libdrm-nouveau2:amd64
libdrm-radeon1:amd64
libdrm2:amd64
libdv4:amd64
libdvbpsi7
libdvdnav4:amd64
libdvdread4:amd64
libebml3:amd64
libedit2:amd64
libegl1-mesa:amd64
libelf1
libenca0
libenchant1c2a
libepoxy0
libept1.4.12
libevdev2
libexif12:amd64
libexiv2-12
libexpat1:amd64
libfaac0:amd64
libfaad2:amd64
libfam0
libffi5:amd64
libfile-copy-recursive-perl
libflac8:amd64
libfly-admin-printer
libfly-system-monitor
libflyauth
libflycore
libflydbus
libflydevices
libflydevices-icons
libflyfiledialog2
libflyintegration1
libflyjobs2
libflyjpeg1
libflypty2
libflyscan2
libflysecrets
libflysu2
libflythumbnails2
libflyui2
libflyuiaux2
libflyuiextra2
libflyuinet2

libfontconfig1:amd64
libfontembed1:amd64
libfontenc1:amd64
libfreerdp1:amd64
libfreetype6:amd64
libfribidi0:amd64
libfs6:amd64
libfuse2:amd64
libgail-3-0:amd64
libgail-common:amd64
libgail18:amd64
libgbm1:amd64
libgcc1:amd64
libgcrypt11:amd64
libgd2-xpm:amd64
libgdbm3:amd64
libgdk-pixbuf2.0-0:amd64
libgdk-pixbuf2.0-common
libgdu0
libgeoclue0:amd64
libgeoip1
libgettextpo0:amd64
libgif4
libgirepository-1.0-1
libgl1-mesa-dri:amd64
libgl1-mesa-glx:amd64
libglapi-mesa:amd64
libgle3
libgles1-mesa:amd64
libgles2-mesa:amd64
libglew1.10:amd64
libglib2.0-0:amd64
libglibmm-2.4-1c2a:amd64
libglu1-mesa:amd64
libglw1-mesa:amd64
libgmime-2.6-0
libgmp10:amd64
libgnome-keyring-common
libgnome-keyring0:amd64
libgnutls26:amd64
libgomp1:amd64
libgost
libgpg-error0:amd64
libgpgme11
libgphoto2-6:amd64
libgphoto2-port12:amd64
libgpm2:amd64
libgraphite2-2.0.0
libgs9
libgs9-common
libgsasl7
libgsm1:amd64
libgssapi-krb5-2:amd64
libgstreamer-plugins-base0.10-0:amd64
libgstreamer0.10-0:amd64
libgtk-3-0:amd64
libgtk-3-bin
libgtk-3-common
libgtk2.0-0:amd64
libgtk2.0-common
libgtkglext1
libgtkmm-2.4-1c2a
libgtop2-7
libgtop2-common
libgudev-1.0-0:amd64
libgutenprint2
libguvcview-1.1-1:amd64
libharfbuzz0b:amd64
libhogweed2:amd64
libhpmud0
libhunspell-1.3-0:amd64
libhyphen0

libice6:amd64
libicu52:amd64
libid3tag0
libident
libidn11:amd64
libiec61883-0
libieee1284-3:amd64
libijs-0.35
libilmbase6
libimlib2:amd64
libimobiledevice2
libinotifytools0
libinput10:amd64
libipc-signal-perl
libisc84
libiscсc80
libisccfg82
libiso9660-8
libisofs6
libiw30:amd64
libjack-jackd2-0:amd64
libjasper1:amd64
libjavascriptcoregtk-3.0-0
libjbig0:amd64
libjbig2dec0
libjemalloc1
libjpeg8:amd64
libjson0:amd64
libjte1
libk5crypto3:amd64
libkate1
libkeyutils1:amd64
libkf5config-bin
libkf5config-data
libkf5configcore5:amd64
libkf5coreaddons-data
libkf5coreaddons5:amd64
libkf5idletime5:amd64
libkf5itemviews-data
libkf5itemviews5:amd64
libkf5solid5:amd64
libkf5solid5-data
libkf5windowsystem-data
libkf5windowsystem5:amd64
libklibc
libkmod2:amd64
libkrb5-3:amd64
libkrb5support0:amd64
liblcms1:amd64
liblcms2-2:amd64
libldap-2.4-2:amd64
liblircclient0
libllvm3.4:amd64
liblocale-gettext-perl
liblockfile-bin
liblockfile1:amd64
liblqr-1-0:amd64
libltdl7:amd64
liblua5.1-0:amd64
liblua5.2-0:amd64
liblvm2app2.2:amd64
liblwres80
liblzma5:amd64
liblzo2-2:amd64
libmacdetect
libmad0
libmagic1:amd64
libmagick++5:amd64
libmagickcore5:amd64
libmagickwand5:amd64
libmatroska5:amd64
libmime-types-perl

libmng1:amd64
libmodplug1
libmount1
libmp3lame0:amd64
libmpc2:amd64
libmpcdec6:amd64
libmpeg2-4
libmpfr4:amd64
libmtdev1:amd64
libmtp-common
libmtp-runtime
libmtp9:amd64
libnatspec0
libnautilus-extension1a
libncurses5:amd64
libncursesw5:amd64
libnettle4:amd64
libnewt0.52
libnfnetlink0
libnih-dbus1
libnih1
libnl-3-200:amd64
libnl-genl-3-200:amd64
libnotify-bin
libnotify4:amd64
libntlm0
libnuma1
libogg0:amd64
libopencv-calib3d2.4:amd64
libopencv-contrib2.4:amd64
libopencv-core2.4:amd64
libopencv-features2d2.4:amd64
libopencv-flann2.4:amd64
libopencv-gpu2.4:amd64
libopencv-highgui2.4:amd64
libopencv-imgproc2.4:amd64
libopencv-legacy2.4:amd64
libopencv-ml2.4:amd64
libopencv-objdetect2.4:amd64
libopencv-ocl2.4:amd64
libopencv-photo2.4:amd64
libopencv-stitching2.4:amd64
libopencv-superres2.4:amd64
libopencv-ts2.4:amd64
libopencv-video2.4:amd64
libopencv-videostab2.4:amd64
libopenexr6
libopenjpeg2:amd64
libopts25
libopus0:amd64
liborc-0.4-0:amd64
libosmesa6:amd64
libp11-kit0:amd64
libpam-cracklib:amd64
libpam-modules:amd64
libpam-modules-bin
libpam-runtime
libpam0g:amd64
libpango1.0-0:amd64
libpangomm-1.4-1
libpaper1:amd64
libparsec-aud-db-legacy2
libparsec-aud-qt5-1
libparsec-aud2
libparsec-base2
libparsec-cap-db-legacy2
libparsec-cap2
libparsec-common-qt5-1
libparsec-iss2
libparsec-log2
libparsec-mac-db-legacy2
libparsec-mac-qt5-1

libparsec-mac2
libparsec-mic2
libparted-fs-resize0:amd64
libparted2:amd64
libpcap0.8:amd64
libpci3:amd64
libpciaccess0:amd64
libpcre3:amd64
libpcsclite1:amd64
libpdac++
libpdp
libperl5.14
libphonon4:amd64
libphonon4qt5-4:amd64
libpipeline1:amd64
libpixman-1-0:amd64
libplist1
libpng12-0:amd64
libpolkit-agent-1-0:amd64
libpolkit-backend-1-0:amd64
libpolkit-gobject-1-0:amd64
libpolkit-qt5-1-1
libpoppler-qt5-1:amd64
libpoppler44:amd64
libpopt0:amd64
libportaudio2:amd64
libpostproc52
libproc-waitstat-perl
libprocps0:amd64
libproxy-tools
libproxy1:amd64
libpth20
libpulse-mainloop-glib0:amd64
libpulse0:amd64
libpython2.7
libqaccessibilityclient
libqca-qt5-2:amd64
libqca-qt5-2-plugins:amd64
libqgsttools-p1:amd64
libqimageblitz5
libqofono-qt5-0:amd64
libqpdf13:amd64
libqsane1
libqt4-dbus:amd64
libqt4-declarative:amd64
libqt4-designer:amd64
libqt4-help:amd64
libqt4-network:amd64
libqt4-opengl:amd64
libqt4-script:amd64
libqt4-scripttools:amd64
libqt4-sql:amd64
libqt4-svg:amd64
libqt4-test:amd64
libqt4-xml:amd64
libqt4-xmlpatterns:amd64
libqt5clucene5:amd64
libqt5concurrent5:amd64
libqt5core5a:amd64
libqt5dbus5:amd64
libqt5declarative5:amd64
libqt5designer5:amd64
libqt5gui5:amd64
libqt5help5:amd64
libqt5lockedfile5
libqt5multimedia5:amd64
libqt5multimedia5-plugins:amd64
libqt5multimediaquick-p5:amd64
libqt5multimediawidgets5:amd64
libqt5network5:amd64
libqt5opengl5:amd64
libqt5printsupport5:amd64

libqt5qml5:amd64
libqt5quick5:amd64
libqt5quickparticles5:amd64
libqt5scintilla2-11
libqt5scintilla2-l10n
libqt5script5:amd64
libqt5sensors5:amd64
libqt5serialport5:amd64
libqt5singleapplication5
libqt5singlecoreapplication5
libqt5sql5:amd64
libqt5sql5-sqlite:amd64
libqt5svg5:amd64
libqt5webkit5:amd64
libqt5widgets5:amd64
libqt5x11extras5:amd64
libqt5xcbqpa5:amd64
libqt5xml5:amd64
libqt5xmlpatterns5:amd64
libqtassistantclient4:amd64
libqtcore4:amd64
libqtdbus4:amd64
libqtgui4:amd64
libqtwebkit4:amd64
libqudev0
libquvi-scripts
libquvi7:amd64
libraw1394-11:amd64
libreadline5:amd64
libreadline6:amd64
libresid-builder0c2a
librsvg2-2:amd64
librsvg2-common:amd64
librtmp0:amd64
libsamplerate0:amd64
libsane:amd64
libsane-common
libsane-hpaio
libsasl2-2:amd64
libschroedinger-1.0-0:amd64
libsdl-image1.2:amd64
libsdl1.2debian:amd64
libselinux1:amd64
libsemanage-common
libsemanage1:amd64
libsensors4:amd64
libsepol1:amd64
libsgutils2-2
libshine3:amd64
libshout3:amd64
libsidplay2
libsigc++-1.2-5c2
libsigc++-2.0-0c2a:amd64
libsigsegv2
libslang2:amd64
libslidingstackedwidget
libslp1
libsm6:amd64
libsmbclient:amd64
libsndfile1:amd64
libsnmp-base
libsnmp15
libsoup-gnome2.4-1:amd64
libsoup2.4-1:amd64
libspectre1:amd64
libspeex1:amd64
libspeexdsp1:amd64
libsqlite3-0:amd64
libss2:amd64
libssh2-1:amd64
libssl1.0.0:amd64
libstdc++6:amd64

libswitch-perl
libswscale2:amd64
libsysfs2:amd64
libsystemd-login0:amd64
libtag1-vanilla:amd64
libtag1c2a:amd64
libtalloc2:amd64
libtasn1-3:amd64
libtbb2
libtdb1:amd64
libtext-charwidth-perl
libtext-iconv-perl
libtext-wrapi18n-perl
libthai-data
libthai0:amd64
libtheora0:amd64
libtiff5:amd64
libtinfo5:amd64
libtotem-plparser17
libts-0.0-0:amd64
libtwolame0
libudev0:amd64
libuniconf4.6
libunistring0:amd64
libupnp6
libupower-glib1:amd64
libusb-0.1-4:amd64
libusb-1.0-0:amd64
libusbmuxd1
libustr-1.0-1:amd64
libutempter0
libuuid1:amd64
libv4l-0:amd64
libv4lconvert0:amd64
libva-drm1:amd64
libva-x11-1:amd64
libva1:amd64
libvcdinfo0
libvisual-0.4-0:amd64
libvlc5
libvlccore8
libvmime0
libvncserver0:amd64
libvorbis0a:amd64
libvorbisenc2:amd64
libvorbisfile3:amd64
libvpx1:amd64
libvte-common
libvte9
libwavpack1:amd64
libwayland-client0:amd64
libwayland-server0:amd64
libwbclient0:amd64
libwebkitgtk-3.0-0
libwebkitgtk-3.0-common
libwebp5:amd64
libwrap0:amd64
libwvstreams4.6-base
libwvstreams4.6-extras
libx11-6:amd64
libx11-data
libx11-xcb1:amd64
libx264-142:amd64
libx265-68:amd64
libx86-1:amd64
libxapian22
libxatracker2:amd64
libxau6:amd64
libxaw7:amd64
libxcb-composite0:amd64
libxcb-damage0:amd64
libxcb-dpms0:amd64

libxcb-dri2-0:amd64
libxcb-dri3-0:amd64
libxcb-glx0:amd64
libxcb-icccm4:amd64
libxcb-image0:amd64
libxcb-keysyms1:amd64
libxcb-present0:amd64
libxcb-randr0:amd64
libxcb-record0:amd64
libxcb-render-util0:amd64
libxcb-render0:amd64
libxcb-res0:amd64
libxcb-screensaver0:amd64
libxcb-shape0:amd64
libxcb-shm0:amd64
libxcb-sync1:amd64
libxcb-util0:amd64
libxcb-xevie0:amd64
libxcb-xf86dri0:amd64
libxcb-xfixes0:amd64
libxcb-xinerama0:amd64
libxcb-xkb1:amd64
libxcb-xparsec:amd64
libxcb-xprint0:amd64
libxcb-xtest0:amd64
libxcb-xv0:amd64
libxcb-xvmc0:amd64
libxcb1:amd64
libxcomposite1:amd64
libxcursor1:amd64
libxdamage1:amd64
libxdmcp6:amd64
libxext6:amd64
libxfixes3:amd64
libxfont1:amd64
libxft2:amd64
libxi6:amd64
libxinerama1:amd64
libxkbcommon-x11-0:amd64
libxkbcommon0:amd64
libxkbfile1:amd64
libxml2:amd64
libxmu6:amd64
libxmuu1:amd64
libxosd2
libxp6:amd64
libxpm4:amd64
libxrandr2:amd64
libxrender1:amd64
libxres1:amd64
libxshmfence1:amd64
libxslt1.1:amd64
libxss1:amd64
libxt6:amd64
libxtables10
libxtst6:amd64
libxv1:amd64
libxvidcore4:amd64
libxvmc1
libxxf86dga1:amd64
libxxf86vm1:amd64
libyelp0
libzvbi-common
libzvbi0:amd64
linux-astra-modules
linux-astra-modules-4.2.0-23-generic
linux-astra-modules-4.2.0-23-pax
linux-astra-modules-common
linux-astra-modules-generic
linux-astra-modules-pax
linux-doc
linux-firmware

linux-image-4.2-generic
linux-image-4.2.0-23-generic
linux-image-4.2.0-23-pax
linux-image-extra-4.2.0-23-generic
linux-image-pax
locales
lockfile-progs
logcheck
login
logrotate
logtail
lsb-base
lsb-release
lsof
makedev
man-db
manpages
manpages-ru
mawk
mc
mc-data
menu
mesa-utils
mime-construct
mime-support
module-init-tools
mount
mountall
msttcorefonts
mtdev-tools
mueller7-dict
multiarch-support
myspell-en-us
myspell-ru
nano
ncurses-base
ncurses-bin
net-tools
netbase
nettle-bin
ntfs-3g
ntp
ntpdate
ofono
openprinting-ppds
openssh-client
openssl
os-prober
p7zip-full
p7zip-rar
parsec
parsec-aud
parsec-base
parsec-cap
parsec-cups
parsec-iss
parsec-log
parsec-mac
parsec-tests
parsec-tools
passwd
patch
pciutils
pcmciautils
pdp
perl
perl-base
perl-modules
perl-tk
phonon-backend-gstreamer:amd64
phonon-backend-gstreamer-common:amd64
phonon4qt5-backend-gstreamer:amd64

plymouth
plymouth-drm
plymouth-themes
plymouth-x11
pm-utils
policykit-1
poppler-data
poppler-utils
powermgmt-base
powertop
ppp
printer-driver-gutenprint
printer-driver-hpcups
printer-driver-hpijs
printer-driver-postscript-hp
procps
psmisc
python
python-apt
python-apt-common
python-chardet
python-dbus
python-dbus-dev
python-debian
python-gi
python-gobject
python-gobject-2
python-imaging
python-minimal
python-pexpect
python-pyatspi
python-pyatspi2
python-qt4
python-qt4-dbus
python-reportlab
python-selinux
python-sip
python-support
python-wicd
python-xapian
python-xcbgen
python2.7
python2.7-minimal
python3
python3-all
python3-gi
python3-minimal
python3-pyatspi
python3-pyatspi2
python3-rbtconfig
python3.2
python3.2-minimal
qasmixer
qastools-common
qbat
qml-module-qt-labs-folderlistmodel:amd64
qml-module-qtgraphicaleffects:amd64
qml-module-qtmultimedia:amd64
qml-module-qtquick-controls:amd64
qml-module-qtquick-layouts:amd64
qml-module-qtquick-particles2:amd64
qml-module-qtquick-window2:amd64
qml-module-qtquick2:amd64
qml-module-qtsensors:amd64
qml-module-qtwebkit:amd64
qpat
qpdfview
qpdfview-djvu-plugin
qpdfview-ps-plugin
qpdfview-translations
qt-at-spi:amd64
qt-at-spi-doc

qt4-qtconfig
qt5-assistant
qt5-style-plugins
qtchooser
qtcore4-l10n
qtdeclarative5-ofono0.2:amd64
qtnotifydaemon
qttranslations5-l10n
qtvirtualkeyboard
rbtconfig-scripts
readline-common
rsh-client
rsyslog
samba-common
samba-common-bin
sed
selinux-utils
sensible-utils
sepol-utils
shared-mime-info
slptool
smbclient
smbnetfs
smolensk-security
snmp
sound-theme-freedesktop
speedcrunch
sshfs
ssl-cert
stardict-dicts-en-ru
stardict-dicts-ru-en
sudo
swfdec-mozilla
synaptic
sysv-rc
sysvinit
sysvinit-utils
tar
tasksel
tasksel-data
tcl8.5
tcl8.5-dev
traceroute
tsconf
ttf-dejavu-core
tzdata
ubuntu-keyring
ucf
udev
udisks
ufw
unrar
unzip
update-inetd
upower
usbmuxd
usbutils
userinfo
util-linux
util-linux-locales
v86d
vim
vim-common
vim-doc
vim-runtime
vim-tiny
vlc
vlc-astra
vlc-data
vlc-nox
vlc-tablet-plugin
vorbis-tools

wamerican
wget
whiptail
wicd
wicd-cli
wicd-daemon
wireless-regdb
wireless-tools
wodim
wpasupplicant
wvdial
x11-apps
x11-common
x11-session-utils
x11-utils
x11-xkb-utils
x11-xserver-utils
xarchiver
xauth
xbacklight
xbase-clients
xbitmaps
xcb-proto
xdg-user-dirs
xdg-utils
xdmx
xdmx-tools
xfonts-100dpi
xfonts-75dpi
xfonts-base
xfonts-bolkhov-75dpi
xfonts-bolkhov-isocyr-75dpi
xfonts-bolkhov-isocyr-misc
xfonts-bolkhov-misc
xfonts-encodings
xfonts-terminus
xfonts-terminus-oblique
xfonts-utils
xinit
xinput
xkb-data
xkbset
xnest
xorg
xorg-all-main
xorg-docs
xorg-docs-core
xorg-sgml-doctools
xosd-bin
xpmutils
xserver-common
xserver-xephyr
xserver-xorg
xserver-xorg-core
xserver-xorg-input-acecad
xserver-xorg-input-aiptek
xserver-xorg-input-all
xserver-xorg-input-evdev
xserver-xorg-input-mouse
xserver-xorg-input-synaptics
xserver-xorg-input-vmmouse
xserver-xorg-input-wacom
xserver-xorg-video-all
xserver-xorg-video-ati
xserver-xorg-video-fbdev
xserver-xorg-video-intel
xserver-xorg-video-mach64
xserver-xorg-video-nouveau
xserver-xorg-video-r128
xserver-xorg-video-radeon
xserver-xorg-video-vesa
xserver-xorg-video-vmware

xterm
xutils
xvfb
xz-utils
yelp
yelp-xsl
zlib1g:amd64

А.4. СРЕДСТВА РАБОТЫ В СЕТИ

acpi
acpi-support
acpi-support-base
acpid
adduser
afick
anacron
apt
apt-doc
apt-transport-https
apt-utils
apt-xapian-index
aptitude
aptitude-common
aspell
aspell-en
aspell-ru
astra-extra
astra-safepolicy
atftp
avahi-autoipd
base-files
base-passwd
bash
bc
bluetooth
bluez
browser-plugin-grabanddrag
browser-plugin-zoompage
bsdmainutils
bsdutils
bsign
busybox
bzip2
chkconfig
console-setup
console-setup-linux
coreutils
cpio
cpp
cpp-4.7
cracklib-runtime
crda
cron
cups
cups-bsd
cups-client
cups-common
cups-filters
cups-ppdc
dash
dbus
debconf
debconf-i18n
debconf-utils
debian-archive-keyring
debianutils
dictionaries-common
diffutils
dmidecode
dmsetup
dosfstools
dpkg
dvd+rw-tools
e2fslibs:amd64
e2fsprogs
eject
emdebian-archive-keyring

ept-cache
exim4-base
exim4-config
exim4-daemon-light
expect
expect-dev
fakeroot
file
findutils
firefox
firefox-astra
firefox-locale-ru
fontconfig
fontconfig-config
fonts-dejavu-core
fonts-freefont-ttf
foomatic-db
fuse
gawk
gcc-4.7-base:amd64
genisoimage
gettext
gettext-base
ghostscript
gir1.2-glib-2.0
gnupg
gostsum
gpgv
gpm
grep
groff-base
growisofs
grub-common
grub-pc
grub-pc-bin
grub2-common
gsfonts
gutenprint-locales
gzip
hostname
ia32-libs
ifupdown
info
init-system-helpers
initramfs-tools
initscripts
insserv
install-info
installation-report
iproute
iptables
iputils-ping
irussian
isc-dhcp-client
isc-dhcp-common
ispell
kbd
keyboard-configuration
klibc-utils
kmod
laptop-detect
less
lib32asound2
lib32bz2-1.0
lib32gcc1
lib32ncurses5
lib32stdc++6
lib32tinfo5
lib32v4l-0
lib32z1
libacl1:amd64
libapt-inst1.5:amd64

libapt-pkg-doc
libapt-pkg4.12:amd64
libasound2:amd64
libaspell15
libasprintf0c2:amd64
libatk1.0-0:amd64
libatk1.0-data
libattr1:amd64
libaudio2:amd64
libaudit-common
libaudit1:amd64
libavahi-client3:amd64
libavahi-common-data:amd64
libavahi-common3:amd64
libblkid1:amd64
libboost-iostreams1.49.0
libboost-iostreams1.55.0:amd64
libbsd0:amd64
libbz2-1.0:amd64
libc-bin
libc6:amd64
libc6-i386
libcairo2:amd64
libcap-ng0
libcap2:amd64
libclass-isa-perl
libcomerr2:amd64
libconfig++9:amd64
libcrack2:amd64
libcroco3:amd64
libcups2:amd64
libcupscgi1:amd64
libcupsfilters1:amd64
libcupsimage2:amd64
libcupsmime1:amd64
libcupsppdc1:amd64
libcurl3-gnutls:amd64
libcwidget3
libdaemon0
libdatrie1:amd64
libdb5.1:amd64
libdbus-1-3:amd64
libdbus-glib-1-2:amd64
libdevmapper1.02.1:amd64
libdrm2:amd64
libedit2:amd64
libegl1-mesa:amd64
libenchant1c2a
libept1.4.12
libevdev2
libexpat1:amd64
libffi5:amd64
libfile-copy-recursive-perl
libfontconfig1:amd64
libfontembed1:amd64
libfreetype6:amd64
libfuse2:amd64
libgbm1:amd64
libgcc1:amd64
libgcrypt11:amd64
libgdbm3:amd64
libgdk-pixbuf2.0-0:amd64
libgdk-pixbuf2.0-common
libgettextpo0:amd64
libgirepository-1.0-1
libgl1-mesa-glx:amd64
libglapi-mesa:amd64
libglib2.0-0:amd64
libgmp10:amd64
libgnutls26:amd64
libgomp1:amd64
libgost

libgpg-error0:amd64
libgpm2:amd64
libgraphite2-2.0.0
libgs9
libgs9-common
libgssapi-krb5-2:amd64
libgtk2.0-0:amd64
libgtk2.0-common
libgutenprint2
libharfbuzz0b:amd64
libhunspell-1.3-0:amd64
libice6:amd64
libicu52:amd64
libident
libidn11:amd64
libijs-0.35
libinput10:amd64
libipc-signal-perl
libiw30:amd64
libjasper1:amd64
libjbig0:amd64
libjbig2dec0
libjpeg8:amd64
libk5crypto3:amd64
libkeyutils1:amd64
libklibc
libkmod2:amd64
libkrb5-3:amd64
libkrb5support0:amd64
liblcms1:amd64
liblcms2-2:amd64
libldap-2.4-2:amd64
liblocale-gettext-perl
liblockfile-bin
liblockfile1:amd64
liblzma5:amd64
libmagic1:amd64
libmime-types-perl
libmng1:amd64
libmount1
libmpc2:amd64
libmpfr4:amd64
libmtdev1:amd64
libnatspec0
libncurses5:amd64
libncursesw5:amd64
libnewt0.52
libnfnetlink0
libnih-dbus1
libnih1
libnl-3-200:amd64
libnl-genl-3-200:amd64
libopenjpeg2:amd64
libopts25
libp11-kit0:amd64
libpam-cracklib:amd64
libpam-modules:amd64
libpam-modules-bin
libpam-runtime
libpam0g:amd64
libpango1.0-0:amd64
libpaper1:amd64
libparsec-aud-db-legacy2
libparsec-aud2
libparsec-base2
libparsec-cap-db-legacy2
libparsec-cap2
libparsec-iss2
libparsec-log2
libparsec-mac-db-legacy2
libparsec-mac2
libparsec-mic2

libpci3:amd64
libpcre3:amd64
libpcsclite1:amd64
libpdac++
libpdp
libperl5.14
libpipeline1:amd64
libpixman-1-0:amd64
libpng12-0:amd64
libpoppler44:amd64
libpopt0:amd64
libproc-waitstat-perl
libprocps0:amd64
libproxy1:amd64
libqca2:amd64
libqca2-plugin-ossl:amd64
libqca2-plugins:amd64
libqpdf13:amd64
libqt4-dbus:amd64
libqt4-declarative:amd64
libqt4-designer:amd64
libqt4-network:amd64
libqt4-qt3support:amd64
libqt4-script:amd64
libqt4-sql:amd64
libqt4-xml:amd64
libqt4-xmlpatterns:amd64
libqt5core5a:amd64
libqt5dbus5:amd64
libqt5gui5:amd64
libqt5network5:amd64
libqt5widgets5:amd64
libqt5xcbqpa5:amd64
libqtcore4:amd64
libqtdbus4:amd64
libqtgui4:amd64
libreadline5:amd64
libreadline6:amd64
librtmp0:amd64
libsasl2-2:amd64
libselinux1:amd64
libsemanage-common
libsemanage1:amd64
libsensors4:amd64
libsepol1:amd64
libsigc++-1.2-5c2
libsigc++-2.0-0c2a:amd64
libsigsegv2
libslang2:amd64
libslp1
libsm6:amd64
libsnmp-base
libsnmp15
libsqlite3-0:amd64
libss2:amd64
libssh2-1:amd64
libssl1.0.0:amd64
libstartup-notification0
libstdc++6:amd64
libswitch-perl
libsysfs2:amd64
libsystemd-login0:amd64
libtasn1-3:amd64
libtext-charwidth-perl
libtext-iconv-perl
libtext-wrapi18n-perl
libthai-data
libthai0:amd64
libtiff5:amd64
libtinfo5:amd64
libudev0:amd64
libunistring0:amd64

libusb-0.1-4:amd64
libusb-1.0-0:amd64
libustr-1.0-1:amd64
libuuid1:amd64
libv4l-0:amd64
libv4lconvert0:amd64
libwayland-client0:amd64
libwayland-server0:amd64
libwrap0:amd64
libx11-6:amd64
libx11-data
libx11-xcb1:amd64
libx86-1:amd64
libxapian22
libxau6:amd64
libxaw7:amd64
libxcb-dri2-0:amd64
libxcb-dri3-0:amd64
libxcb-glx0:amd64
libxcb-icccm4:amd64
libxcb-image0:amd64
libxcb-keysyms1:amd64
libxcb-present0:amd64
libxcb-randr0:amd64
libxcb-render-util0:amd64
libxcb-render0:amd64
libxcb-shape0:amd64
libxcb-shm0:amd64
libxcb-sync1:amd64
libxcb-util0:amd64
libxcb-xfixes0:amd64
libxcb-xinerama0:amd64
libxcb-xkb1:amd64
libxcb1:amd64
libxcomposite1:amd64
libxcursor1:amd64
libxdamage1:amd64
libxdmcp6:amd64
libxext6:amd64
libxfixes3:amd64
libxft2:amd64
libxi6:amd64
libxinerama1:amd64
libxkbcommon-x11-0:amd64
libxkbcommon0:amd64
libxml2:amd64
libxmu6:amd64
libxmuu1:amd64
libxpm4:amd64
libxrandr2:amd64
libxrender1:amd64
libxshmfence1:amd64
libxss1:amd64
libxt6:amd64
libxtables10
libxxf86vm1:amd64
linux-astra-modules
linux-astra-modules-4.2.0-23-generic
linux-astra-modules-4.2.0-23-pax
linux-astra-modules-common
linux-astra-modules-generic
linux-astra-modules-pax
linux-doc
linux-firmware
linux-image-4.2-generic
linux-image-4.2.0-23-generic
linux-image-4.2.0-23-pax
linux-image-extra-4.2.0-23-generic
linux-image-pax
locales
lockfile-progs
logcheck

login
logrotate
logtail
lsb-base
lsb-release
lsof
makedev
man-db
manpages
manpages-ru
mawk
mc
mc-data
mime-construct
mime-support
module-init-tools
mount
mountall
mueller7-dict
multiarch-support
myspell-ru
nano
ncurses-base
ncurses-bin
net-tools
netbase
ntfs-3g
ntp
openprinting-ppds
openssh-client
openssl
os-prober
p7zip-full
p7zip-rar
parsec
parsec-aud
parsec-base
parsec-cap
parsec-cups
parsec-iss
parsec-log
parsec-mac
parsec-tests
parsec-tools
passwd
pciutils
pcmciautils
pdp
perl
perl-base
perl-modules
perl-tk
plymouth
plymouth-drm
plymouth-themes
plymouth-x11
pm-utils
poppler-data
poppler-utils
powermgmt-base
powertop
printer-driver-gutenprint
procps
psi
psi-translations
psmisc
python
python-apt
python-apt-common
python-chardet
python-dbus
python-dbus-dev

python-debian
python-gi
python-gobject
python-gobject-2
python-minimal
python-support
python-wicd
python-xapian
python2.7
python2.7-minimal
python3
python3-minimal
python3.2
python3.2-minimal
qtcore4-l10n
readline-common
rsh-client
rsyslog
sed
sensible-utils
shared-mime-info
slptool
snmp
ssl-cert
sudo
sysv-rc
sysvinit
sysvinit-utils
tar
tasksel
tasksel-data
tcl8.5
tcl8.5-dev
thunderbird
thunderbird-addon-firetray
thunderbird-locale-ru
traceroute
ttf-dejavu-core
tzdata
ubuntu-keyring
ucf
udev
ufw
unrar
unzip
update-inetd
usbutils
userinfo
util-linux
util-linux-locales
v86d
vim
vim-common
vim-doc
vim-runtime
vim-tiny
wamerican
wget
whiptail
wicd
wicd-cli
wicd-daemon
wireless-regdb
wireless-tools
wpasupplicant
x11-common
x11-xserver-utils
xkb-data
xz-utils
zlib1g:amd64

А.5. ОФИСНЫЕ СРЕДСТВА

acpi
acpi-support-base
acpid
adduser
apt
apt-utils
apt-xapian-index
aptitude
aptitude-common
astra-extra
astra-safepolicy
base-files
base-passwd
bash
bsdmainutils
bsdutils
busybox
bzip2
coinor-libcoinmp1:amd64
console-setup
console-setup-linux
coreutils
cpio
cracklib-runtime
cron
dash
debconf
debconf-i18n
debconf-utils
debian-archive-keyring
debianutils
dictionaries-common
diffutils
dmidecode
dmsetup
dpkg
e2fslibs:amd64
e2fsprogs
eject
emdebian-archive-keyring
ept-cache
expect
expect-dev
file
findutils
fontconfig
fontconfig-config
fonts-dejavu
fonts-dejavu-core
fonts-dejavu-extra
fonts-opensymbol
fonts-sil-gentium-basic
gawk
gcc-4.7-base:amd64
gettext-base
gnupg
goldendict
gpgv
grep
groff-base
grub-common
grub-pc
grub-pc-bin
grub2-common
gzip
hostname
ifupdown
info

init-system-helpers
initramfs-tools
initscripts
insserv
install-info
installation-report
iproute
iptables
iputils-ping
isc-dhcp-client
isc-dhcp-common
iso-codes
kbd
keyboard-configuration
klibc-utils
kmod
laptop-detect
libabw-0.1-1
libacl1:amd64
libao-common
libao4
libapt-inst1.5:amd64
libapt-pkg4.12:amd64
libasprintf0c2:amd64
libatk1.0-0:amd64
libatk1.0-data
libattr1:amd64
libaudit-common
libaudit1:amd64
libavahi-client3:amd64
libavahi-common-data:amd64
libavahi-common3:amd64
libavcodec55:amd64
libavformat55:amd64
libavutil53:amd64
libblkid1:amd64
libboost-date-time1.55.0:amd64
libboost-iostreams1.49.0
libboost-iostreams1.55.0:amd64
libboost-system1.55.0:amd64
libbz2-1.0:amd64
libc-bin
libc6:amd64
libcairo2:amd64
libcap2:amd64
libcdr-0.1-1
libclass-isa-perl
libclucene-contribs1v5:amd64
libclucene-core1v5:amd64
libcmis-0.5-5v5
libcolamd2.7.1
libcomerr2:amd64
libcrack2:amd64
libcups2:amd64
libcurl3-gnutls:amd64
libcwidget3
libdatrie1:amd64
libdb5.1:amd64
libdbus-1-3:amd64
libdbus-glib-1-2:amd64
libdevmapper1.02.1:amd64
libdrm2:amd64
libe-book-0.1-1
libegl1-mesa:amd64
libeot0
libept1.4.12
libetonyek-0.1-1
libevdev2
libexpat1:amd64
libexttextcat-data
libexttextcat0
libfaac0:amd64

libffi5:amd64
libfontconfig1:amd64
libfontenc1:amd64
libfreehand-0.1-1
libfreetype6:amd64
libfuse2:amd64
libgbm1:amd64
libgcc1:amd64
libgcrypt11:amd64
libgdbm3:amd64
libgdk-pixbuf2.0-0:amd64
libgdk-pixbuf2.0-common
libgl1-mesa-glx:amd64
libglapi-mesa:amd64
libglew1.10:amd64
libglib2.0-0:amd64
libgltf-0.0-0v5
libglu1-mesa:amd64
libgmp10:amd64
libgnutls26:amd64
libgost
libgpg-error0:amd64
libgraphite2-2.0.0
libgsm1:amd64
libgssapi-krb5-2:amd64
libgstreamer-plugins-base0.10-0:amd64
libgstreamer0.10-0:amd64
libgtk2.0-0:amd64
libgtk2.0-common
libharfbuzz-icu0:amd64
libharfbuzz0b:amd64
libhunspell-1.3-0:amd64
libhyphen0
libice6:amd64
libicu52:amd64
libident
libidn11:amd64
libinput10:amd64
libjasper1:amd64
libjbig0:amd64
libjpeg8:amd64
libk5crypto3:amd64
libkeyutils1:amd64
libklibc
libkmod2:amd64
libkrb5-3:amd64
libkrb5support0:amd64
liblangtag-common
liblangtag1
liblcms2-2:amd64
libldap-2.4-2:amd64
liblocale-gettext-perl
libltdl7:amd64
liblzma5:amd64
liblzo2-2:amd64
libmagic1:amd64
libmhash2
libmount1
libmp3lame0:amd64
libmspub-0.1-1
libmtdev1:amd64
libmwaw-0.3-3
libmythes-1.2-0
libncurses5:amd64
libncursesw5:amd64
libneon27-gnutls
libnewt0.52
libnfnetlink0
libnih-dbus1
libnih1
libnspr4:amd64
libnss3:amd64

libodfgen-0.1-1
libogg0:amd64
libopenjpeg2:amd64
libopus0:amd64
liborc-0.4-0:amd64
liborcus-0.10-0v5
libp11-kit0:amd64
libpagemaker-0.0-0
libpam-cracklib:amd64
libpam-modules:amd64
libpam-modules-bin
libpam-runtime
libpam0g:amd64
libpango1.0-0:amd64
libparsec-aud2
libparsec-base2
libparsec-cap2
libpci3:amd64
libpcre3:amd64
libpdp
libpipeline1:amd64
libpixman-1-0:amd64
libpng12-0:amd64
libpoppler44:amd64
libpopt0:amd64
libprocps0:amd64
libproxy-tools
libproxy1:amd64
libpython2.7
libqt5clucene5:amd64
libqt5core5a:amd64
libqt5dbus5:amd64
libqt5gui5:amd64
libqt5help5:amd64
libqt5network5:amd64
libqt5opengl5:amd64
libqt5printsupport5:amd64
libqt5qml5:amd64
libqt5quick5:amd64
libqt5sql5:amd64
libqt5svg5:amd64
libqt5webkit5:amd64
libqt5widgets5:amd64
libqt5x11extras5:amd64
libqt5xcbqpa5:amd64
libqt5xml5:amd64
libraptor2-0:amd64
librasqal3:amd64
librdf0:amd64
libreadline6:amd64
libreoffice
libreoffice-astra
libreoffice-avmedia-backend-vlc
libreoffice-base
libreoffice-base-core
libreoffice-base-drivers
libreoffice-calc
libreoffice-common
libreoffice-core
libreoffice-draw
libreoffice-gtk
libreoffice-help-ru
libreoffice-impress
libreoffice-l10n-ru
libreoffice-math
libreoffice-pdfimport
libreoffice-style-galaxy
libreoffice-writer
librevenge-0.0-0
librtmp0:amd64
libsasl2-2:amd64
libschroedinger-1.0-0:amd64

libselinux1:amd64
libsemanage-common
libsemanage1:amd64
libsepol1:amd64
libsigc++-1.2-5c2
libsigc++-2.0-0c2a:amd64
libsigsegv2
libslang2:amd64
libsm6:amd64
libspeex1:amd64
libsqlite3-0:amd64
libss2:amd64
libssh2-1:amd64
libssl1.0.0:amd64
libstdc++6:amd64
libswitch-perl
libsysfs2:amd64
libtasn1-3:amd64
libtext-charwidth-perl
libtext-iconv-perl
libtext-wrapi18n-perl
libthai-data
libthai0:amd64
libtheora0:amd64
libtiff5:amd64
libtinfo5:amd64
libudev0:amd64
libusb-0.1-4:amd64
libusb-1.0-0:amd64
libustr-1.0-1:amd64
libuuid1:amd64
libva1:amd64
libvisio-0.1-1
libvlc5
libvlccore8
libvorbis0a:amd64
libvorbisenc2:amd64
libvorbisfile3:amd64
libvpx1:amd64
libwayland-client0:amd64
libwayland-server0:amd64
libwebp5:amd64
libwpd-0.10-10
libwpg-0.3-3
libwps-0.4-4
libx11-6:amd64
libx11-data
libx11-xcb1:amd64
libx264-142:amd64
libx86-1:amd64
libxapian22
libxau6:amd64
libxcb-dri2-0:amd64
libxcb-dri3-0:amd64
libxcb-glx0:amd64
libxcb-icccm4:amd64
libxcb-image0:amd64
libxcb-keysyms1:amd64
libxcb-present0:amd64
libxcb-randr0:amd64
libxcb-render-util0:amd64
libxcb-render0:amd64
libxcb-shape0:amd64
libxcb-shm0:amd64
libxcb-sync1:amd64
libxcb-util0:amd64
libxcb-xfixes0:amd64
libxcb-xinerama0:amd64
libxcb-xkb1:amd64
libxcb1:amd64
libxcomposite1:amd64
libxcursor1:amd64

libxdamage1:amd64
libxdmcp6:amd64
libxext6:amd64
libxfixes3:amd64
libxfont1:amd64
libxft2:amd64
libxi6:amd64
libxinerama1:amd64
libxkbcommon-x11-0:amd64
libxkbcommon0:amd64
libxml2:amd64
libxmu6:amd64
libxrandr2:amd64
libxrender1:amd64
libxshmfence1:amd64
libxslt1.1:amd64
libxt6:amd64
libxtables10
libxtst6:amd64
libxvidcore4:amd64
libxxf86vm1:amd64
libyajl2
linux-image-4.2-generic
linux-image-4.2.0-23-generic
locales
login
logrotate
lp-solve
lsb-base
makedev
man-db
manpages
mawk
mime-support
module-init-tools
mount
mountall
msttcorefonts
multiarch-support
nano
ncurses-base
ncurses-bin
net-tools
netbase
os-prober
passwd
pciutils
perl
perl-base
perl-modules
plymouth
plymouth-drm
plymouth-themes
plymouth-x11
procps
python
python-apt
python-apt-common
python-chardet
python-debian
python-minimal
python-support
python-uno
python-xapian
python2.7
python2.7-minimal
readline-common
rsyslog
sed
sensible-utils
shared-mime-info
sudo

sysv-rc
sysvinit
sysvinit-utils
tar
tasksel
tasksel-data
tcl8.5
tcl8.5-dev
traceroute
ttf-dejavu-core
tzdata
ubuntu-keyring
ucf
udev
uno-libs3
ure
usbutils
util-linux
v86d
vim-common
vim-tiny
vlc-data
wamerican
wget
whiptail
x11-common
xfonts-encodings
xfonts-utils
xkb-data
xz-utils
zlib1g:amd64

А.6. СЕТЕВЫЕ СЕРВИСЫ

acl
acpi
acpi-support-base
acpid
adduser
apache2
apache2-mpm-prefork
apache2-utils
apache2.2-bin
apache2.2-common
apt
apt-utils
apt-xapian-index
aptitude
aptitude-common
astra-extra
astra-safepolicy
base-files
base-passwd
bash
bc
bcrelay
bind9
bind9-doc
bind9-host
bind9utils
bsdmainutils
bsdutils
busybox
bzip2
console-setup
console-setup-linux
consolekit
coreutils
cpio
cracklib-runtime
cron
cups
cups-client
cups-common
cups-filters
cups-ppdc
cvs
dash
dbus
debconf
debconf-i18n
debconf-utils
debian-archive-keyring
debianutils
diffutils
dmidecode
dmsetup
dnsutils
dpkg
e2fslibs:amd64
e2fsprogs
eject
emdebian-archive-keyring
ept-cache
exim4
exim4-base
exim4-config
exim4-daemon-light
expect
expect-dev
file
findutils

fontconfig
fontconfig-config
fonts-dejavu-core
fonts-freefont-ttf
foomatic-filters
gawk
gcc-4.7-base:amd64
gettext-base
ghostscript
gnupg
gpgv
grep
groff-base
grub-common
grub-pc
grub-pc-bin
grub2-common
gsfonts
gzip
hostname
hpijs-ppds
hplip
hplip-data
ifupdown
info
init-system-helpers
initramfs-tools
initscripts
insserv
install-info
installation-report
iproute
iptables
iputils-ping
isc-dhcp-client
isc-dhcp-common
kbd
keyboard-configuration
klibc-utils
kmod
laptop-detect
libacl1:amd64
libapr1
libaprutil1
libaprutil1-dbd-sqlite3
libaprutil1-ldap
libapt-inst1.5:amd64
libapt-pkg4.12:amd64
libasprintf0c2:amd64
libatk1.0-0:amd64
libatk1.0-data
libattr1:amd64
libaudit-common
libaudit1:amd64
libavahi-client3:amd64
libavahi-common-data:amd64
libavahi-common3:amd64
libbind9-80
libblkid1:amd64
libboost-iostreams1.49.0
libboost-iostreams1.55.0:amd64
libbsd0:amd64
libbz2-1.0:amd64
libc-bin
libc6:amd64
libcairo2:amd64
libcap2:amd64
libck-connector0:amd64
libclass-isa-perl
libcomerr2:amd64
libcrack2:amd64
libcups2:amd64

libcupscgi1:amd64
libcupsfilters1:amd64
libcupsimage2:amd64
libcupsmime1:amd64
libcupsppdc1:amd64
libcwidget3
libdatrie1:amd64
libdb5.1:amd64
libdbus-1-3:amd64
libdbus-glib-1-2:amd64
libdevmapper1.02.1:amd64
libdns88
libdrm2:amd64
libedit2:amd64
libegl1-mesa:amd64
libept1.4.12
libevent-2.0-5:amd64
libexif12:amd64
libexpat1:amd64
libffi5:amd64
libfile-copy-recursive-perl
libfontconfig1:amd64
libfontembed1:amd64
libfreetype6:amd64
libfuse2:amd64
libgbm1:amd64
libgcc1:amd64
libgcrypt11:amd64
libgd2-xpm:amd64
libgdbm3:amd64
libgdk-pixbuf2.0-0:amd64
libgdk-pixbuf2.0-common
libgeoip1
libgl1-mesa-glx:amd64
libglapi-mesa:amd64
libglib2.0-0:amd64
libgnutls26:amd64
libgost
libgpg-error0:amd64
libgpgme11
libgphoto2-6:amd64
libgphoto2-port12:amd64
libgs9
libgs9-common
libgssapi-krb5-2:amd64
libgssglue1:amd64
libgtk2.0-0:amd64
libgtk2.0-common
libgutenprint2
libhpmud0
libident
libidn11:amd64
libieee1284-3:amd64
libijs-0.35
libisc84
libisccc80
libisccfg82
libjasper1:amd64
libjbig0:amd64
libjbig2dec0
libjpeg8:amd64
libk5crypto3:amd64
libkeyutils1:amd64
libklibc
libkmod2:amd64
libkrb5-3:amd64
libkrb5support0:amd64
liblcms1:amd64
liblcms2-2:amd64
libldap-2.4-2:amd64
liblocale-gettext-perl
libltdl7:amd64

liblwres80
liblzma5:amd64
liblzo2-2:amd64
libmagic1:amd64
libmount1
libncurses5:amd64
libncursesw5:amd64
libnewt0.52
libnfnetlink0
libnfsidmap2:amd64
libnih-dbus1
libnih1
libopenjpeg2:amd64
libp11-kit0:amd64
libpam-cracklib:amd64
libpam-modules:amd64
libpam-modules-bin
libpam-runtime
libpam0g:amd64
libpango1.0-0:amd64
libpaper1:amd64
libparsec-aud2
libparsec-base2
libparsec-cap2
libparsec-mac2
libpcap0.8:amd64
libpci3:amd64
libpcre3:amd64
libpdp
libperl5.14
libpipeline1:amd64
libpixman-1-0:amd64
libpkcs11-helper1:amd64
libpng12-0:amd64
libpolkit-agent-1-0:amd64
libpolkit-backend-1-0:amd64
libpolkit-gobject-1-0:amd64
libpoppler44:amd64
libpopt0:amd64
libprocps0:amd64
libpth20
libqpdf13:amd64
libreadline6:amd64
libsane:amd64
libsane-common
libsane-hpaio
libsasl2-2:amd64
libselinux1:amd64
libsemanage-common
libsemanage1:amd64
libsensors4:amd64
libsepol1:amd64
libsigc++-1.2-5c2
libsigc++-2.0-0c2a:amd64
libsigsegv2
libslang2:amd64
libslp1
libsnmp-base
libsnmp15
libsqlite3-0:amd64
libss2:amd64
libssl1.0.0:amd64
libstdc++6:amd64
libswitch-perl
libsysfs2:amd64
libsystemd-login0:amd64
libtalloc2:amd64
libtasn1-3:amd64
libtdb1:amd64
libtext-charwidth-perl
libtext-iconv-perl
libtext-wrapi18n-perl

libthai-data
libthai0:amd64
libtiff5:amd64
libtinfo5:amd64
libtirpc1:amd64
libtokyocabinet9:amd64
libudev0:amd64
libusb-0.1-4:amd64
libusb-1.0-0:amd64
libustr-1.0-1:amd64
libuuid1:amd64
libwayland-client0:amd64
libwayland-server0:amd64
libwbclient0:amd64
libwrap0:amd64
libx11-6:amd64
libx11-data
libx11-xcb1:amd64
libx86-1:amd64
libxapian22
libxau6:amd64
libxcb-dri2-0:amd64
libxcb-dri3-0:amd64
libxcb-glx0:amd64
libxcb-present0:amd64
libxcb-randr0:amd64
libxcb-render0:amd64
libxcb-shape0:amd64
libxcb-shm0:amd64
libxcb-sync1:amd64
libxcb-xfixes0:amd64
libxcb1:amd64
libxcomposite1:amd64
libxcursor1:amd64
libxdamage1:amd64
libxdmcp6:amd64
libxext6:amd64
libxfixes3:amd64
libxft2:amd64
libxi6:amd64
libxinerama1:amd64
libxml2:amd64
libxpm4:amd64
libxrandr2:amd64
libxrender1:amd64
libxshmfence1:amd64
libxtables10
libxxf86vm1:amd64
linux-image-4.2-generic
linux-image-4.2.0-23-generic
locales
login
logrotate
lsb-base
lwresd
makedev
man-db
manpages
mawk
mime-support
module-init-tools
mount
mountall
multiarch-support
mutt
nano
ncurses-base
ncurses-bin
net-tools
netbase
nfs-common
nfs-kernel-server

openbsd-inetd
openprinting-ppds
openssh-client
openssh-server
openssl
openvpn
os-prober
passwd
pciutils
perl
perl-base
perl-modules
plymouth
plymouth-drm
plymouth-themes
plymouth-x11
policykit-1
poppler-data
poppler-utils
ppp
pptpd
printer-driver-gutenprint
printer-driver-hpcups
printer-driver-hpijs
printer-driver-postscript-hp
procmail
procps
python
python-apt
python-apt-common
python-chardet
python-dbus
python-dbus-dev
python-debian
python-gobject-2
python-imaging
python-minimal
python-pexpect
python-reportlab
python-support
python-xapian
python2.7
python2.7-minimal
python3
python3-minimal
python3.2
python3.2-minimal
readline-common
rpcbind
rsyslog
samba
samba-common
samba-common-bin
samba-doc
sed
sensible-utils
shared-mime-info
slpd
smbclient
snmpd
squid
squid-common
squid-langpack
ssl-cert
sudo
swat
sysv-rc
sysvinit
sysvinit-utils
tar
tasksel
tasksel-data

tcl8.5
tcl8.5-dev
tcpd
tftpd
traceroute
ttf-dejavu-core
tzdata
ubuntu-keyring
ucf
udev
update-inetd
usbutils
util-linux
v86d
vim-common
vim-tiny
wamerican
wget
whiptail
winbind
xkb-data
xz-utils
zlib1g:amd64

А.7. СУБД

acpi
acpi-support-base
acpid
adduser
apt
apt-utils
apt-xapian-index
aptitude
aptitude-common
astra-extra
astra-safepolicy
base-files
base-passwd
bash
bsdmainutils
bsdutils
busybox
bzip2
console-setup
console-setup-linux
coreutils
cpio
cracklib-runtime
cron
dash
debconf
debconf-i18n
debconf-utils
debian-archive-keyring
debianutils
diffutils
dmidecode
dmsetup
dpkg
e2fslibs:amd64
e2fsprogs
eject
emdebian-archive-keyring
ept-cache
expect
expect-dev
file
findutils
fontconfig
fontconfig-config
fonts-dejavu-core
gawk
gcc-4.7-base:amd64
gettext-base
gnupg
gpgv
grep
groff-base
grub-common
grub-pc
grub-pc-bin
grub2-common
gzip
hostname
ifupdown
info
init-system-helpers
initramfs-tools
initscripts
insserv
install-info
installation-report
iproute

iptables
iputils-ping
isc-dhcp-client
isc-dhcp-common
kbd
keyboard-configuration
klibc-utils
kmod
laptop-detect
libacl1:amd64
libapt-inst1.5:amd64
libapt-pkg4.12:amd64
libasprintf0c2:amd64
libatk1.0-0:amd64
libatk1.0-data
libattr1:amd64
libaudit-common
libaudit1:amd64
libavahi-client3:amd64
libavahi-common-data:amd64
libavahi-common3:amd64
libblkid1:amd64
libboost-iostreams1.49.0
libboost-iostreams1.55.0:amd64
libbsd0:amd64
libbz2-1.0:amd64
libc-bin
libc6:amd64
libcairo2:amd64
libcap2:amd64
libclass-isa-perl
libcomerr2:amd64
libcrack2:amd64
libcups2:amd64
libcwidget3
libdatrie1:amd64
libdb5.1:amd64
libdbus-1-3:amd64
libdevmapper1.02.1:amd64
libdrm2:amd64
libedit2:amd64
libegl1-mesa:amd64
libept1.4.12
libexpat1:amd64
libffi5:amd64
libfontconfig1:amd64
libfreetype6:amd64
libfuse2:amd64
libgbm1:amd64
libgcc1:amd64
libgcrypt11:amd64
libgdbm3:amd64
libgdk-pixbuf2.0-0:amd64
libgdk-pixbuf2.0-common
libgl1-mesa-glx:amd64
libglapi-mesa:amd64
libglib2.0-0:amd64
libgnutls26:amd64
libgost
libgpg-error0:amd64
libgssapi-krb5-2:amd64
libgtk2.0-0:amd64
libgtk2.0-common
libident
libidn11:amd64
libjasper1:amd64
libjbig0:amd64
libjpeg8:amd64
libk5crypto3:amd64
libkeyutils1:amd64
libklibc
libkmod2:amd64

libkrb5-3:amd64
libkrb5support0:amd64
libldap-2.4-2:amd64
liblocale-gettext-perl
liblzma5:amd64
libmagic1:amd64
libmount1
libncurses5:amd64
libncursesw5:amd64
libnewt0.52
libnfnetlink0
libnih-dbus1
libnih1
libp11-kit0:amd64
libpam-cracklib:amd64
libpam-modules:amd64
libpam-modules-bin
libpam-runtime
libpam0g:amd64
libpango1.0-0:amd64
libparsec-aud2
libparsec-base2
libparsec-cap2
libparsec-log2
libpci3:amd64
libpcre3:amd64
libpdp
libpipeline1:amd64
libpixman-1-0:amd64
libpng12-0:amd64
libpopt0:amd64
libpq5:amd64
libprocps0:amd64
libreadline6:amd64
libsasl2-2:amd64
libselinux1:amd64
libsemanage-common
libsemanage1:amd64
libsepol1:amd64
libsigc++-1.2-5c2
libsigc++-2.0-0c2a:amd64
libsigsegv2
libslang2:amd64
libsqlite3-0:amd64
libss2:amd64
libssl1.0.0:amd64
libstdc++6:amd64
libswitch-perl
libsysfs2:amd64
libtasn1-3:amd64
libtext-charwidth-perl
libtext-iconv-perl
libtext-wrapi18n-perl
libthai-data
libthai0:amd64
libtiff5:amd64
libtinfo5:amd64
libudev0:amd64
libusb-0.1-4:amd64
libusb-1.0-0:amd64
libustr-1.0-1:amd64
libuuid1:amd64
libwayland-client0:amd64
libwayland-server0:amd64
libx11-6:amd64
libx11-data
libx11-xcb1:amd64
libx86-1:amd64
libxapian22
libxau6:amd64
libxcb-dri2-0:amd64
libxcb-dri3-0:amd64

libxcb-glx0:amd64
libxcb-present0:amd64
libxcb-randr0:amd64
libxcb-render0:amd64
libxcb-shape0:amd64
libxcb-shm0:amd64
libxcb-sync1:amd64
libxcb-xfixes0:amd64
libxcb1:amd64
libxcomposite1:amd64
libxcursor1:amd64
libxdamage1:amd64
libxdmcp6:amd64
libxext6:amd64
libxfixes3:amd64
libxft2:amd64
libxi6:amd64
libxinerama1:amd64
libxml2:amd64
libxrandr2:amd64
libxrender1:amd64
libxshmfence1:amd64
libxtables10
libxxf86vm1:amd64
linux-astra-modules-4.2.0-23-pax
linux-astra-modules-common
linux-image-4.2-generic
linux-image-4.2.0-23-generic
linux-image-4.2.0-23-pax
locales
login
logrotate
lsb-base
makedev
man-db
manpages
mawk
mime-support
module-init-tools
mount
mountall
multiarch-support
nano
ncurses-base
ncurses-bin
net-tools
netbase
openssl
os-prober
parsec-base
parsec-cap
passwd
pciutils
perl
perl-base
perl-modules
plymouth
plymouth-drm
plymouth-themes
plymouth-x11
postgresql
postgresql-9.4
postgresql-astra
postgresql-client
postgresql-client-9.4
postgresql-client-common
postgresql-common
procps
python
python-apt
python-apt-common
python-chardet

python-debian
python-minimal
python-support
python-xapian
python2.7
python2.7-minimal
readline-common
rsyslog
sed
sensible-utils
shared-mime-info
ssl-cert
sudo
sysv-rc
sysvinit
sysvinit-utils
tar
tasksel
tasksel-data
tcl8.5
tcl8.5-dev
traceroute
ttf-dejavu-core
tzdata
ubuntu-keyring
ucf
udev
usbutils
util-linux
v86d
vim-common
vim-tiny
wamerican
wget
whiptail
xkb-data
xz-utils
zlib1g:amd64

А.8. СРЕДСТВА МУЛЬТИМЕДИА

acpi
acpi-support-base
acpid
adduser
apt
apt-utils
apt-xapian-index
aptitude
aptitude-common
astra-extra
astra-safepolicy
base-files
base-passwd
bash
bsdmainutils
bsdutils
busybox
bzip2
coinor-libcoinmp1:amd64
console-setup
console-setup-linux
coreutils
cpio
cracklib-runtime
cron
dash
debconf
debconf-i18n
debconf-utils
debian-archive-keyring
debianutils
dictionaries-common
diffutils
dmidecode
dmsetup
dpkg
e2fslibs:amd64
e2fsprogs
eject
emdebian-archive-keyring
ept-cache
expect
expect-dev
file
findutils
fontconfig
fontconfig-config
fonts-dejavu
fonts-dejavu-core
fonts-dejavu-extra
fonts-opensymbol
fonts-sil-gentium-basic
gawk
gcc-4.7-base:amd64
gettext-base
gnupg
goldendict
gpgv
grep
groff-base
grub-common
grub-pc
grub-pc-bin
grub2-common
gzip
hostname
ifupdown
info

init-system-helpers
initramfs-tools
initscripts
insserv
install-info
installation-report
iproute
iptables
iputils-ping
isc-dhcp-client
isc-dhcp-common
iso-codes
kbd
keyboard-configuration
klibc-utils
kmod
laptop-detect
libabw-0.1-1
libacl1:amd64
libao-common
libao4
libapt-inst1.5:amd64
libapt-pkg4.12:amd64
libasprintf0c2:amd64
libatk1.0-0:amd64
libatk1.0-data
libattr1:amd64
libaudit-common
libaudit1:amd64
libavahi-client3:amd64
libavahi-common-data:amd64
libavahi-common3:amd64
libavcodec55:amd64
libavformat55:amd64
libavutil53:amd64
libblkid1:amd64
libboost-date-time1.55.0:amd64
libboost-iostreams1.49.0
libboost-iostreams1.55.0:amd64
libboost-system1.55.0:amd64
libbz2-1.0:amd64
libc-bin
libc6:amd64
libcairo2:amd64
libcap2:amd64
libcdr-0.1-1
libclass-isa-perl
libclucene-contribs1v5:amd64
libclucene-core1v5:amd64
libcmis-0.5-5v5
libcolamd2.7.1
libcomerr2:amd64
libcrack2:amd64
libcups2:amd64
libcurl3-gnutls:amd64
libcwidget3
libdatrie1:amd64
libdb5.1:amd64
libdbus-1-3:amd64
libdbus-glib-1-2:amd64
libdevmapper1.02.1:amd64
libdrm2:amd64
libe-book-0.1-1
libegl1-mesa:amd64
libeot0
libept1.4.12
libetonyek-0.1-1
libevdev2
libexpat1:amd64
libexttextcat-data
libexttextcat0
libfaac0:amd64

libffi5:amd64
libfontconfig1:amd64
libfontenc1:amd64
libfreehand-0.1-1
libfreetype6:amd64
libfuse2:amd64
libgbm1:amd64
libgcc1:amd64
libgcrypt11:amd64
libgdbm3:amd64
libgdk-pixbuf2.0-0:amd64
libgdk-pixbuf2.0-common
libgl1-mesa-glx:amd64
libglapi-mesa:amd64
libglew1.10:amd64
libglib2.0-0:amd64
libgltf-0.0-0v5
libglu1-mesa:amd64
libgmp10:amd64
libgnutls26:amd64
libgost
libgpg-error0:amd64
libgraphite2-2.0.0
libgsm1:amd64
libgssapi-krb5-2:amd64
libgstreamer-plugins-base0.10-0:amd64
libgstreamer0.10-0:amd64
libgtk2.0-0:amd64
libgtk2.0-common
libharfbuzz-icu0:amd64
libharfbuzz0b:amd64
libhunspell-1.3-0:amd64
libhyphen0
libice6:amd64
libicu52:amd64
libident
libidn11:amd64
libinput10:amd64
libjasper1:amd64
libjbig0:amd64
libjpeg8:amd64
libk5crypto3:amd64
libkeyutils1:amd64
libklibc
libkmod2:amd64
libkrb5-3:amd64
libkrb5support0:amd64
liblangtag-common
liblangtag1
liblcms2-2:amd64
libldap-2.4-2:amd64
liblocale-gettext-perl
libltdl7:amd64
liblzma5:amd64
liblzo2-2:amd64
libmagic1:amd64
libmhash2
libmount1
libmp3lame0:amd64
libmspub-0.1-1
libmtdev1:amd64
libmwaw-0.3-3
libmythes-1.2-0
libncurses5:amd64
libncursesw5:amd64
libneon27-gnutls
libnewt0.52
libnfnetlink0
libnih-dbus1
libnih1
libnspr4:amd64
libnss3:amd64

libodfgen-0.1-1
libogg0:amd64
libopenjpeg2:amd64
libopus0:amd64
liborc-0.4-0:amd64
liborcus-0.10-0v5
libp11-kit0:amd64
libpagemaker-0.0-0
libpam-cracklib:amd64
libpam-modules:amd64
libpam-modules-bin
libpam-runtime
libpam0g:amd64
libpango1.0-0:amd64
libparsec-aud2
libparsec-base2
libparsec-cap2
libpci3:amd64
libpcre3:amd64
libpdp
libpipeline1:amd64
libpixman-1-0:amd64
libpng12-0:amd64
libpoppler44:amd64
libpopt0:amd64
libprocps0:amd64
libproxy-tools
libproxy1:amd64
libpython2.7
libqt5clucene5:amd64
libqt5core5a:amd64
libqt5dbus5:amd64
libqt5gui5:amd64
libqt5help5:amd64
libqt5network5:amd64
libqt5opengl5:amd64
libqt5printsupport5:amd64
libqt5qml5:amd64
libqt5quick5:amd64
libqt5sql5:amd64
libqt5svg5:amd64
libqt5webkit5:amd64
libqt5widgets5:amd64
libqt5x11extras5:amd64
libqt5xcbqpa5:amd64
libqt5xml5:amd64
libraptor2-0:amd64
librasqal3:amd64
librdf0:amd64
libreadline6:amd64
libreoffice
libreoffice-astra
libreoffice-avmedia-backend-vlc
libreoffice-base
libreoffice-base-core
libreoffice-base-drivers
libreoffice-calc
libreoffice-common
libreoffice-core
libreoffice-draw
libreoffice-gtk
libreoffice-help-ru
libreoffice-impress
libreoffice-l10n-ru
libreoffice-math
libreoffice-pdfimport
libreoffice-style-galaxy
libreoffice-writer
librevenge-0.0-0
librtmp0:amd64
libsasl2-2:amd64
libschroedinger-1.0-0:amd64

libselinux1:amd64
libsemanage-common
libsemanage1:amd64
libsepol1:amd64
libsigc++-1.2-5c2
libsigc++-2.0-0c2a:amd64
libsigsegv2
libslang2:amd64
libsm6:amd64
libspeex1:amd64
libsqlite3-0:amd64
libss2:amd64
libssh2-1:amd64
libssl1.0.0:amd64
libstdc++6:amd64
libswitch-perl
libsysfs2:amd64
libtasn1-3:amd64
libtext-charwidth-perl
libtext-iconv-perl
libtext-wrapi18n-perl
libthai-data
libthai0:amd64
libtheora0:amd64
libtiff5:amd64
libtinfo5:amd64
libudev0:amd64
libusb-0.1-4:amd64
libusb-1.0-0:amd64
libustr-1.0-1:amd64
libuuid1:amd64
libva1:amd64
libvisio-0.1-1
libvlc5
libvlccore8
libvorbis0a:amd64
libvorbisenc2:amd64
libvorbisfile3:amd64
libvpx1:amd64
libwayland-client0:amd64
libwayland-server0:amd64
libwebp5:amd64
libwpd-0.10-10
libwpg-0.3-3
libwps-0.4-4
libx11-6:amd64
libx11-data
libx11-xcb1:amd64
libx264-142:amd64
libx86-1:amd64
libxapian22
libxau6:amd64
libxcb-dri2-0:amd64
libxcb-dri3-0:amd64
libxcb-glx0:amd64
libxcb-icccm4:amd64
libxcb-image0:amd64
libxcb-keysyms1:amd64
libxcb-present0:amd64
libxcb-randr0:amd64
libxcb-render-util0:amd64
libxcb-render0:amd64
libxcb-shape0:amd64
libxcb-shm0:amd64
libxcb-sync1:amd64
libxcb-util0:amd64
libxcb-xfixes0:amd64
libxcb-xinerama0:amd64
libxcb-xkb1:amd64
libxcb1:amd64
libxcomposite1:amd64
libxcursor1:amd64

libxdamage1:amd64
libxdmcp6:amd64
libxext6:amd64
libxfixes3:amd64
libxfont1:amd64
libxft2:amd64
libxi6:amd64
libxinerama1:amd64
libxkbcommon-x11-0:amd64
libxkbcommon0:amd64
libxml2:amd64
libxmu6:amd64
libxrandr2:amd64
libxrender1:amd64
libxshmfence1:amd64
libxslt1.1:amd64
libxt6:amd64
libxtables10
libxtst6:amd64
libxvidcore4:amd64
libxxf86vm1:amd64
libyajl2
linux-image-4.2-generic
linux-image-4.2.0-23-generic
locales
login
logrotate
lp-solve
lsb-base
makedev
man-db
manpages
mawk
mime-support
module-init-tools
mount
mountall
msttcorefonts
multiarch-support
nano
ncurses-base
ncurses-bin
net-tools
netbase
os-prober
passwd
pciutils
perl
perl-base
perl-modules
plymouth
plymouth-drm
plymouth-themes
plymouth-x11
procps
python
python-apt
python-apt-common
python-chardet
python-debian
python-minimal
python-support
python-uno
python-xapian
python2.7
python2.7-minimal
readline-common
rsyslog
sed
sensible-utils
shared-mime-info
sudo

sysv-rc
sysvinit
sysvinit-utils
tar
tasksel
tasksel-data
tcl8.5
tcl8.5-dev
traceroute
ttf-dejavu-core
tzdata
ubuntu-keyring
ucf
udev
uno-libs3
ure
usbutils
util-linux
v86d
vim-common
vim-tiny
vlc-data
wamerican
wget
whiptail
x11-common
xfonts-encodings
xfonts-utils
xkb-data
xz-utils
zlib1g:amd64

А.9. РЕЖИМ КИОСКА

acl
acpi
acpi-support-base
acpid
adduser
apt
apt-utils
apt-xapian-index
aptitude
aptitude-common
astra-extra
astra-safepolicy
base-files
base-passwd
bash
bsdmainutils
bsdutils
busybox
bzip2
console-setup
console-setup-linux
coreutils
cpio
cracklib-runtime
cron
dash
debconf
debconf-i18n
debconf-utils
debian-archive-keyring
debianutils
diffutils
dmidecode
dmsetup
dpkg
e2fslibs:amd64
e2fsprogs
eject
emdebian-archive-keyring
ept-cache
expect
expect-dev
file
findutils
fontconfig
fontconfig-config
fonts-dejavu-core
gawk
gcc-4.7-base:amd64
gettext-base
gnupg
gpgv
grep
groff-base
grub-common
grub-pc
grub-pc-bin
grub2-common
gzip
hostname
ifupdown
info
init-system-helpers
initramfs-tools
initscripts
insserv
install-info
installation-report

iproute
iptables
iputils-ping
isc-dhcp-client
isc-dhcp-common
kbd
keyboard-configuration
klibc-utils
kmod
laptop-detect
libacl1:amd64
libapt-inst1.5:amd64
libapt-pkg4.12:amd64
libasprintf0c2:amd64
libatk1.0-0:amd64
libatk1.0-data
libattr1:amd64
libaudit-common
libaudit1:amd64
libavahi-client3:amd64
libavahi-common-data:amd64
libavahi-common3:amd64
libblkid1:amd64
libboost-iostreams1.49.0
libboost-iostreams1.55.0:amd64
libbz2-1.0:amd64
libc-bin
libc6:amd64
libcairo2:amd64
libcap2:amd64
libclass-isa-perl
libcomerr2:amd64
libcrack2:amd64
libcups2:amd64
libcwidget3
libdatrie1:amd64
libdb5.1:amd64
libdbus-1-3:amd64
libdevmapper1.02.1:amd64
libdrm2:amd64
libegl1-mesa:amd64
libept1.4.12
libexpat1:amd64
libffi5:amd64
libfontconfig1:amd64
libfreetype6:amd64
libfuse2:amd64
libgbm1:amd64
libgcc1:amd64
libgcrypt11:amd64
libgdbm3:amd64
libgdk-pixbuf2.0-0:amd64
libgdk-pixbuf2.0-common
libgl1-mesa-glx:amd64
libglapi-mesa:amd64
libglib2.0-0:amd64
libgnutls26:amd64
libgost
libgpg-error0:amd64
libgssapi-krb5-2:amd64
libgtk2.0-0:amd64
libgtk2.0-common
libident
libidn11:amd64
libjasper1:amd64
libjbig0:amd64
libjpeg8:amd64
libk5crypto3:amd64
libkeyutils1:amd64
libklibc
libkmod2:amd64
libkrb5-3:amd64

libkrb5support0:amd64
liblocale-gettext-perl
liblzma5:amd64
libmagic1:amd64
libmount1
libncurses5:amd64
libncursesw5:amd64
libnewt0.52
libnfnetlink0
libnih-dbus1
libnih1
libp11-kit0:amd64
libpam-cracklib:amd64
libpam-modules:amd64
libpam-modules-bin
libpam-runtime
libpam0g:amd64
libpango1.0-0:amd64
libparsec-aud2
libparsec-base2
libparsec-cap2
libparsec-log2
libpci3:amd64
libpcre3:amd64
libpdp
libpipeline1:amd64
libpixman-1-0:amd64
libpng12-0:amd64
libpopt0:amd64
libprocps0:amd64
libreadline6:amd64
libselinux1:amd64
libsemanage-common
libsemanage1:amd64
libsepol1:amd64
libsigc++-1.2-5c2
libsigc++-2.0-0c2a:amd64
libsigsegv2
libslang2:amd64
libsqlite3-0:amd64
libss2:amd64
libssl1.0.0:amd64
libstdc++6:amd64
libswitch-perl
libsysfs2:amd64
libtasn1-3:amd64
libtext-charwidth-perl
libtext-iconv-perl
libtext-wrapi18n-perl
libthai-data
libthai0:amd64
libtiff5:amd64
libtinfo5:amd64
libudev0:amd64
libusb-0.1-4:amd64
libusb-1.0-0:amd64
libustr-1.0-1:amd64
libuuid1:amd64
libwayland-client0:amd64
libwayland-server0:amd64
libx11-6:amd64
libx11-data
libx11-xcb1:amd64
libx86-1:amd64
libxapian22
libxau6:amd64
libxcb-dri2-0:amd64
libxcb-dri3-0:amd64
libxcb-glx0:amd64
libxcb-present0:amd64
libxcb-randr0:amd64
libxcb-render0:amd64

libxcb-shape0:amd64
libxcb-shm0:amd64
libxcb-sync1:amd64
libxcb-xfixes0:amd64
libxcb1:amd64
libxcomposite1:amd64
libxcursor1:amd64
libxdamage1:amd64
libxdmcp6:amd64
libxext6:amd64
libxfixes3:amd64
libxft2:amd64
libxi6:amd64
libxinerama1:amd64
libxml2:amd64
libxrandr2:amd64
libxrender1:amd64
libxshmfence1:amd64
libxtables10
libxxf86vm1:amd64
linux-astra-modules-4.2.0-23-pax
linux-astra-modules-common
linux-image-4.2-generic
linux-image-4.2.0-23-generic
linux-image-4.2.0-23-pax
locales
login
logrotate
lsb-base
makedev
man-db
manpages
mawk
mime-support
module-init-tools
mount
mountall
multiarch-support
nano
ncurses-base
ncurses-bin
net-tools
netbase
os-prober
parsec-aud
parsec-base
parsec-cap
parsec-kiosk
parsec-log
passwd
pciutils
perl
perl-base
perl-modules
plymouth
plymouth-drm
plymouth-themes
plymouth-x11
procps
python
python-apt
python-apt-common
python-chardet
python-debian
python-minimal
python-support
python-xapian
python2.7
python2.7-minimal
readline-common
rsyslog
sed

sensible-utils
shared-mime-info
sudo
sysv-rc
sysvinit
sysvinit-utils
tar
tasksel
tasksel-data
tcl8.5
tcl8.5-dev
traceroute
ttf-dejavu-core
tzdata
ubuntu-keyring
ucf
udev
usbutils
util-linux
v86d
vim-common
vim-tiny
wamerican
wget
whiptail
xkb-data
xz-utils
zlib1g:amd64

А.10. СЛУЖБА ALD

А.10.1. Серверная часть ALD

acpi
acpi-support-base
acpid
adduser
ald-admin
ald-admin-common
ald-admin-parsec
ald-client
ald-client-common
ald-client-fs
ald-client-parsec
ald-server-common
ald-server-dc
ald-server-parsec
apt
apt-utils
apt-xapian-index
aptitude
aptitude-common
astra-extra
astra-safepolicy
base-files
base-passwd
bash
bind9-host
bsdmainutils
bsdutils
busybox
bzip2
cifs-utils
console-setup
console-setup-linux
coreutils
cpio
cracklib-runtime
cron
dash
debconf
debconf-i18n
debconf-utils
debian-archive-keyring
debianutils
diffutils
dmidecode
dmsetup
dpkg
e2fslibs:amd64
e2fsprogs
eject
emdebian-archive-keyring
ept-cache
expect
expect-dev
file
findutils
fontconfig
fontconfig-config
fonts-dejavu-core
gawk
gcc-4.7-base:amd64
gettext-base
gnupg
gpgv
grep

groff-base
grub-common
grub-pc
grub-pc-bin
grub2-common
gzip
hostname
ifupdown
info
init-system-helpers
initramfs-tools
initscripts
insserv
install-info
installation-report
iproute
iptables
iputils-ping
isc-dhcp-client
isc-dhcp-common
kbd
keyboard-configuration
keyutils
klibc-utils
kmod
krb5-admin-server
krb5-config
krb5-kdc
krb5-user
laptop-detect
libacl1:amd64
libapt-inst1.5:amd64
libapt-pkg4.12:amd64
libasprintf0c2:amd64
libatk1.0-0:amd64
libatk1.0-data
libattr1:amd64
libaudit-common
libaudit1:amd64
libavahi-client3:amd64
libavahi-common-data:amd64
libavahi-common3:amd64
libbind9-80
libblkid1:amd64
libboost-iostreams1.49.0
libboost-iostreams1.55.0:amd64
libbz2-1.0:amd64
libc-bin
libc6:amd64
libcairo2:amd64
libcap-ng0
libcap2:amd64
libclass-isa-perl
libcomerr2:amd64
libconfig++9:amd64
libcrack2:amd64
libcups2:amd64
libcwidget3
libdatrie1:amd64
libdb5.1:amd64
libdbus-1-3:amd64
libdevmapper1.02.1:amd64
libdns88
libdrm2:amd64
libegl1-mesa:amd64
libept1.4.12
libev4
libevent-2.0-5:amd64
libexpat1:amd64
libffi5:amd64
libfile-copy-recursive-perl
libfontconfig1:amd64

libfreetype6:amd64
libfuse2:amd64
libgbm1:amd64
libgcc1:amd64
libgcrypt11:amd64
libgdbm3:amd64
libgdk-pixbuf2.0-0:amd64
libgdk-pixbuf2.0-common
libgeoip1
libgl1-mesa-glx:amd64
libglapi-mesa:amd64
libglib2.0-0:amd64
libgnutls26:amd64
libgost
libgpg-error0:amd64
libgssapi-krb5-2:amd64
libgssglue1:amd64
libgssrpc4:amd64
libgtk2.0-0:amd64
libgtk2.0-common
libident
libidn11:amd64
libisc84
libiscсc80
libisccfg82
libjasper1:amd64
libjbig0:amd64
libjpeg8:amd64
libk5crypto3:amd64
libkadm5clnt-mit9:amd64
libkadm5srv-mit9:amd64
libkdb5-7:amd64
libkeyutils1:amd64
libklibc
libkmod2:amd64
libkrb5-3:amd64
libkrb5support0:amd64
libldap-2.4-2:amd64
liblocale-gettext-perl
libltdl7:amd64
liblwres80
liblzma5:amd64
libmagic1:amd64
libmount1
libncurses5:amd64
libncursesw5:amd64
libnewt0.52
libnfnetlink0
libnfsidmap2:amd64
libnih-dbus1
libnih1
libnss-ldapd:amd64
libodbc1:amd64
libp11-kit0:amd64
libpam-cracklib:amd64
libpam-krb5:amd64
libpam-modules:amd64
libpam-modules-bin
libpam-runtime
libpam0g:amd64
libpango1.0-0:amd64
libparsec-aud-db-ald2
libparsec-aud-db-ldap2
libparsec-aud2
libparsec-base2
libparsec-cap-db-ald2
libparsec-cap-db-ldap2
libparsec-cap2
libparsec-db-ldap2
libparsec-mac-db-ald2
libparsec-mac-db-ldap2
libparsec-mac2

libparsec-mic-db-ald2
libparsec-mic-db-ldap2
libparsec-mic2
libpci3:amd64
libpcre3:amd64
libpdac++
libpdp
libperl5.14
libpipeline1:amd64
libpixman-1-0:amd64
libpng12-0:amd64
libpopt0:amd64
libprocps0:amd64
libreadline6:amd64
libsasl2-2:amd64
libsasl2-modules:amd64
libsasl2-modules-gssapi-mit:amd64
libselinux1:amd64
libsemanage-common
libsemanage1:amd64
libsepol1:amd64
libsigc++-1.2-5c2
libsigc++-2.0-0c2a:amd64
libsigsegv2
libslang2:amd64
libslp1
libsocket++1
libsqlite3-0:amd64
libss2:amd64
libssl1.0.0:amd64
libstdc++6:amd64
libswitch-perl
libsysfs2:amd64
libtalloc2:amd64
libtar0
libtasn1-3:amd64
libtdb1:amd64
libtext-charwidth-perl
libtext-iconv-perl
libtext-wrapi18n-perl
libthai-data
libthai0:amd64
libtiff5:amd64
libtinfo5:amd64
libtirpc1:amd64
libudev0:amd64
libusb-0.1-4:amd64
libusb-1.0-0:amd64
libustr-1.0-1:amd64
libuuid1:amd64
libverto-libev1:amd64
libverto1:amd64
libwayland-client0:amd64
libwayland-server0:amd64
libwbclient0:amd64
libwrap0:amd64
libx11-6:amd64
libx11-data
libx11-xcb1:amd64
libx86-1:amd64
libxapian22
libxau6:amd64
libxcb-dri2-0:amd64
libxcb-dri3-0:amd64
libxcb-glx0:amd64
libxcb-present0:amd64
libxcb-randr0:amd64
libxcb-render0:amd64
libxcb-shape0:amd64
libxcb-shm0:amd64
libxcb-sync1:amd64
libxcb-xfixes0:amd64

libxcb1:amd64
libxcomposite1:amd64
libxcursor1:amd64
libxdamage1:amd64
libxdmcp6:amd64
libxext6:amd64
libxfixes3:amd64
libxft2:amd64
libxi6:amd64
libxinerama1:amd64
libxml2:amd64
libxrandr2:amd64
libxrender1:amd64
libxshmfence1:amd64
libxtables10
libxxf86vm1:amd64
linux-astra-modules-4.2.0-23-pax
linux-astra-modules-common
linux-image-4.2-generic
linux-image-4.2.0-23-generic
linux-image-4.2.0-23-pax
locales
login
logrotate
lsb-base
makedev
man-db
manpages
mawk
mime-support
module-init-tools
mount
mountall
multiarch-support
nano
ncurses-base
ncurses-bin
net-tools
netbase
nfs-common
nfs-kernel-server
nscd
nslcd
openbsd-inetd
os-prober
parsec-base
passwd
pciutils
perl
perl-base
perl-modules
plymouth
plymouth-drm
plymouth-themes
plymouth-x11
procps
psmisc
python
python-apt
python-apt-common
python-chardet
python-debian
python-minimal
python-support
python-xapian
python2.7
python2.7-minimal
readline-common
rpcbind
rsyslog
samba
samba-common

sed
sensible-utils
shared-mime-info
slapd
sudo
sysv-rc
sysvinit
sysvinit-utils
tar
tasksel
tasksel-data
tcl8.5
tcl8.5-dev
tcpd
traceroute
ttf-dejavu-core
tzdata
ubuntu-keyring
ucf
udev
update-inetd
usbutils
util-linux
v86d
vim-common
vim-tiny
wamerican
wget
whiptail
xkb-data
xz-utils
zlib1g:amd64

A.10.2. Клиентская часть ALD

acpi
acpi-support-base
acpid
adduser
ald-client
ald-client-common
ald-client-parsec
apt
apt-utils
apt-xapian-index
aptitude
aptitude-common
astra-extra
astra-safepolicy
base-files
base-passwd
bash
bind9-host
bsdmainutils
bsdutils
busybox
bzip2
cifs-utils
console-setup
console-setup-linux
coreutils
cpio
cracklib-runtime
cron
dash
debconf
debconf-i18n
debconf-utils
debian-archive-keyring

debianutils
diffutils
dmidecode
dmsetup
dpkg
e2fslibs:amd64
e2fsprogs
eject
emdebian-archive-keyring
ept-cache
expect
expect-dev
file
findutils
fontconfig
fontconfig-config
fonts-dejavu-core
gawk
gcc-4.7-base:amd64
gettext-base
gnupg
gpgv
grep
groff-base
grub-common
grub-pc
grub-pc-bin
grub2-common
gzip
hostname
ifupdown
info
init-system-helpers
initramfs-tools
initscripts
insserv
install-info
installation-report
iproute
iptables
iputils-ping
isc-dhcp-client
isc-dhcp-common
kbd
keyboard-configuration
keyutils
klibc-utils
kmod
krb5-config
krb5-user
laptop-detect
libacl1:amd64
libapt-inst1.5:amd64
libapt-pkg4.12:amd64
libasprintf0c2:amd64
libatk1.0-0:amd64
libatk1.0-data
libattr1:amd64
libaudit-common
libaudit1:amd64
libavahi-client3:amd64
libavahi-common-data:amd64
libavahi-common3:amd64
libbind9-80
libblkid1:amd64
libboost-iostreams1.49.0
libboost-iostreams1.55.0:amd64
libbz2-1.0:amd64
libc-bin
libc6:amd64
libcairo2:amd64
libcap-ng0

libcap2:amd64
libclass-isa-perl
libcomerr2:amd64
libconfig++9:amd64
libcrack2:amd64
libcups2:amd64
libcwidget3
libdatrie1:amd64
libdb5.1:amd64
libdbus-1-3:amd64
libdevmapper1.02.1:amd64
libdns88
libdrm2:amd64
libegl1-mesa:amd64
libept1.4.12
libevent-2.0-5:amd64
libexpat1:amd64
libffi5:amd64
libfontconfig1:amd64
libfreetype6:amd64
libfuse2:amd64
libgbm1:amd64
libgcc1:amd64
libgcrypt11:amd64
libgdbm3:amd64
libgdk-pixbuf2.0-0:amd64
libgdk-pixbuf2.0-common
libgeoip1
libgl1-mesa-glx:amd64
libglapi-mesa:amd64
libglib2.0-0:amd64
libgnutls26:amd64
libgost
libgpg-error0:amd64
libgssapi-krb5-2:amd64
libgssglue1:amd64
libgssrpc4:amd64
libgtk2.0-0:amd64
libgtk2.0-common
libident
libidn11:amd64
libisc84
libisccc80
libisccfg82
libjasper1:amd64
libjbig0:amd64
libjpeg8:amd64
libk5crypto3:amd64
libkadm5clnt-mit9:amd64
libkadm5srv-mit9:amd64
libkdb5-7:amd64
libkeyutils1:amd64
libklibc
libkmod2:amd64
libkrb5-3:amd64
libkrb5support0:amd64
libldap-2.4-2:amd64
liblocale-gettext-perl
liblwres80
liblzma5:amd64
libmagic1:amd64
libmount1
libncurses5:amd64
libncursesw5:amd64
libnewt0.52
libnfnetlink0
libnfsidmap2:amd64
libnih-dbus1
libnih1
libnss-ldapd:amd64
libp11-kit0:amd64
libpam-cracklib:amd64

libpam-krb5:amd64
libpam-modules:amd64
libpam-modules-bin
libpam-runtime
libpam0g:amd64
libpango1.0-0:amd64
libparsec-aud-db-ald2
libparsec-aud-db-ldap2
libparsec-aud2
libparsec-base2
libparsec-cap-db-ald2
libparsec-cap-db-ldap2
libparsec-cap2
libparsec-db-ldap2
libparsec-mac-db-ald2
libparsec-mac-db-ldap2
libparsec-mac2
libparsec-mic-db-ald2
libparsec-mic-db-ldap2
libparsec-mic2
libpci3:amd64
libpcre3:amd64
libpdac++
libpdp
libpipeline1:amd64
libpixman-1-0:amd64
libpng12-0:amd64
libpopt0:amd64
libprocps0:amd64
libreadline6:amd64
libsasl2-2:amd64
libsasl2-modules:amd64
libsasl2-modules-gssapi-mit:amd64
libselinux1:amd64
libsemanage-common
libsemanage1:amd64
libsepol1:amd64
libsigc++-1.2-5c2
libsigc++-2.0-0c2a:amd64
libsigsegv2
libslang2:amd64
libsocket++1
libsqlite3-0:amd64
libss2:amd64
libssl1.0.0:amd64
libstdc++6:amd64
libswitch-perl
libsysfs2:amd64
libtalloc2:amd64
libtar0
libtasn1-3:amd64
libtext-charwidth-perl
libtext-iconv-perl
libtext-wrapi18n-perl
libthai-data
libthai0:amd64
libtiff5:amd64
libtinfo5:amd64
libtirpc1:amd64
libudev0:amd64
libusb-0.1-4:amd64
libusb-1.0-0:amd64
libustr-1.0-1:amd64
libuuid1:amd64
libwayland-client0:amd64
libwayland-server0:amd64
libwbclient0:amd64
libwrap0:amd64
libx11-6:amd64
libx11-data
libx11-xcb1:amd64
libx86-1:amd64

libxapian22
libxau6:amd64
libxcb-dri2-0:amd64
libxcb-dri3-0:amd64
libxcb-glx0:amd64
libxcb-present0:amd64
libxcb-randr0:amd64
libxcb-render0:amd64
libxcb-shape0:amd64
libxcb-shm0:amd64
libxcb-sync1:amd64
libxcb-xfixes0:amd64
libxcb1:amd64
libxcomposite1:amd64
libxcursor1:amd64
libxdamage1:amd64
libxdmcp6:amd64
libxext6:amd64
libxfixes3:amd64
libxft2:amd64
libxi6:amd64
libxinerama1:amd64
libxml2:amd64
libxrandr2:amd64
libxrender1:amd64
libxshmfence1:amd64
libxtables10
libxxf86vm1:amd64
linux-astra-modules-4.2.0-23-pax
linux-astra-modules-common
linux-image-4.2-generic
linux-image-4.2.0-23-generic
linux-image-4.2.0-23-pax
locales
login
logrotate
lsb-base
makedev
man-db
manpages
mawk
mime-support
module-init-tools
mount
mountall
multiarch-support
nano
ncurses-base
ncurses-bin
net-tools
netbase
nfs-common
nscd
nslcd
os-prober
parsec-base
passwd
pciutils
perl
perl-base
perl-modules
plymouth
plymouth-drm
plymouth-themes
plymouth-x11
procps
python
python-apt
python-apt-common
python-chardet
python-debian
python-minimal

python-support
python-xapian
python2.7
python2.7-minimal
readline-common
rpcbind
rsyslog
samba-common
sed
sensible-utils
shared-mime-info
sudo
sysv-rc
sysvinit
sysvinit-utils
tar
tasksel
tasksel-data
tcl8.5
tcl8.5-dev
traceroute
ttf-dejavu-core
tzdata
ubuntu-keyring
ucf
udev
usbutils
util-linux
v86d
vim-common
vim-tiny
wamerican
wget
whiptail
xkb-data
xz-utils
zlib1g:amd64

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД — база данных
ЕПП — единое пространство пользователей
КСЗ — комплекс средств защиты
ЛВС — локальная вычислительная сеть
НСД — несанкционированный доступ
ОЗУ — оперативное запоминающее устройство
ОС — операционная система
ПО — программное обеспечение
СЗИ — средства защиты информации
СЗФС — сетевая защищенная файловая система
СПО — специальное программное обеспечение
СУБД — система управления базами данных
СЭП — система обмена сообщениями электронной почты
ФС — файловая система

ACL — Access Control List (список контроля доступа)
ALD — Astra Linux Directory (единое пространство пользователей)
ARP — Address Resolution Protocol (протокол разрешения адресов)
BOOTP — Bootstrap Protocol (простой протокол динамической конфигурации хоста)
BSD — Berkeley Software Distribution (программное изделие Калифорнийского университета)
CIFS — Common Internet File System (общий протокол доступа к файлам Интернет)
DHCP — Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста)
DIB — Directory Information Base (информационная база каталога)
DIT — Directory Information Tree (информационное дерево каталога)
DN — Distinguished Name (уникальное имя)
DNS — Domain Name System (служба доменных имен)
FTP — File Transfer Protocol (протокол передачи файлов)
GID — Group Identifier (идентификатор группы)
HBA — Host-based Authentication (аутентификация на основе адресов узлов сети)
HTTP — HyperText Transfer Protocol (протокол передачи гипертекстовых файлов)
ICMP — Internet Control Message Protocol (протокол управляющих сообщений в сети Интернет)

IDE — Integrated Drive Electronics (встроенный интерфейс накопителей)

IMAP — Internet Message Access Protocol (протокол доступа к сообщениям в сети Интернет)

IP — Internet Protocol (протокол Интернет)

IPC — InterProcess Communication (межпроцессное взаимодействие)

KDC — Key Distribution Center (центр распределения ключей)

LDAP — Lightweight Directory Access Protocol (легковесный протокол доступа к сервисам каталогов)

LPR — Line Printer Remote (удаленный линейный принтер)

LVM — Logical Volume Manager (менеджер логических томов)

MAC — Mandatory Access Control (мандатное управление доступом)

MDA — Mail Delivery Agent (агент доставки электронной почты)

MTA — Mail Transfer Agent (агент пересылки сообщений)

MTU — Maximum Transfer Unit (максимальная единица передачи)

MUA — Mail User Agent (клиент электронной почты)

NFS — Network File System (сетевая файловая система)

NIS — Network Information Service (сетевая информационная служба)

NSS — Name Service Switch (диспетчер службы имен)

NTP — Network Time Protocol (сетевой протокол времени)

PAM — Pluggable Authentication Modules (подгружаемые аутентификационные модули)

POP3 — Post Office Protocol Version 3 (почтовый протокол, версия 3)

RFC — Request For Comments (общее название технических стандартов сети Интернет)

SASL — Simple Authentication and Security Layer (простая аутентификация и слой безопасности)

SCSI — Small Computer System Interface (системный интерфейс малых компьютеров)

SMB — Session Message Block (блок сессионных сообщений)

SQL — Structured Query Language (язык структурированных запросов)

SSH — Secure Shell Protocol (протокол передачи информации в зашифрованном виде)

SSL — Secure Sockets Layer (протокол защищенных сокетов)

TCP — Transmission Control Protocol (протокол передачи данных)

TOS — Type of Service (тип сервиса)

TTL — Time To Live (время жизни IP-пакета)

UDP — User Datagram Protocol (протокол пользовательских дейтаграмм)

UID — User Identifier (идентификатор пользователя)

UTC — Universal Time Coordinated (универсальное скоординированное время)

VFS — Virtual File System (виртуальная файловая система)

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопрово-дительного докум. и дата	Подп.	Дата
	изменен-ных	заменен-ных	новых	аннулиро-ванных					