ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION» РУСБ.10015-01

Руководство администратора. Часть 1

Оперативное обновление 1.8.3

Бюллетень № 2025-0811SE18

Листов 85

2025

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

В настоящем документе приведены кумулятивные изменения в документ РУСБ.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1» из комплектности изделия РУСБ.10015-01 «Операционная система специального назначения «Astra Linux Special Edition» (далее по тексту — ОС).

При настройке и эксплуатации ОС с установленным оперативным обновлением согласно бюллетеню № 2025-0811SE18 рекомендуется руководствоваться документом РУСБ.10015-01 95 01-1 совместно с настоящим документом.

Документ предназначен для администраторов ОС и сети.

2. ПЕРЕЧЕНЬ ИЗМЕНЕНИЙ

2.1. Пункт «2.5.2. Автоматическое обновление»

2.1.1. В пункте 2.5.2 после таблицы 4 добавить следующий текст:

Если доступно очередное обновление ОС, то будет установлен статус `stopped-for-major` и показано уведомление о возможности установки очередного обновления ОС. Результаты работы службы заносятся в журнал `/var/log/astra-update-service/service.log`.

2.1.2. В пункте 2.5.2 в таблице 5 заменить последнюю строку следующими строками:

Таблица 5

Настройка	Описание
`Use_sources_list_d`	Проверка наличия обновлений в репозиториях, указанных в файлах в `/etc/apt/sources.list.d/`. Данная настройка позволяет использовать службу `astra-update-service` для обновления стороннего ПО, установленного в системе. Возможные значения: 1) `0` — используются только репозитории, указанные в `/etc/apt/sources.list` (обновления ОС, значение по умолчанию); 2) `1` — используются репозитории, указанные в `/etc/apt/sources.list` и репозитории, указанные в файлах в `/etc/apt/sources.list.d/` (обновления стороннего ПО). **ВНИМАНИЕ!** Данный параметр игнорируется, если в конфигурационном файле указан параметр `Extra_repos_policy` с любым из возможных значений
`Extra_repos_policy`	Проверка наличия обновлений в дополнительных репозиториях, указанных в значении параметра `Extra_repos`. Возможные значения: 1) `0` — используются только дополнительные репозитории без репозиториев, указанных в `/etc/apt/sources.list` (значение по умолчанию, если параметр указан без значения); 2) `1` — используются дополнительные репозитории и репозитории, указанные в `/etc/apt/sources.list`. **ВНИМАНИЕ!** При использовании данного параметра игнорируется значение параметра `Use_sources_list_d`. Чтобы дополнительно использовать репозитории из `/etc/apt/sources.list.d/`, нужно указать пути к их файлам в значении параметра `Extra_repos`
`Extra_repos`	Список путей к файлам с дополнительными репозиториями. Список указывается в виде строки в кавычках, пути в строке разделяются запятыми

2.2. Пункт «2.5.3. Пользовательские сценарии»

Ввести новый пункт 2.5.3:

В процессе обновления возможно выполнение пользовательских сценариев, например для проведения дополнительных проверок перед обновлением ОС или для обновления стороннего ПО, установленного вручную.

Процесс обновления ОС архитектурно поделен на следующие стадии:

1) блок проверок перед переводом ОС в режим обновления;
2) блок проверок перед обновлением ОС;
3) обновление ОС;
4) откат обновления (при наличии выполненного снимка состояния ОС).

На каждой из перечисленных стадий может выполняться одно или несколько действий, задаваемых пользовательским сценарием. Каждое действие может выполняться перед началом стадии или после ее окончания.

Пользовательские сценарии размещаются в каталоге `/usr/share/astra-update-service/scripts/`. Порядок запуска сценариев определяется алфавитным порядком имен их файлов.

Каждый сценарий должен иметь возможность запуска с параметром `config` для вывода основной информации о сценарии.

Результатом запуска сценария с указанным параметром должен быть вывод в `stdout` следующей основной информации о сценарии:

1) уникальный строковый идентификатор сценария;
2) список уникальных идентификаторов стадий обновления, на которых должен запускаться сценарий, перечисляемых через запятую:
   а) `ready` — стадия проверок перед переводом ОС в режим обновления;
   б) `activated` — стадия проверок перед обновлением ОС;
   в) `upgrade` — стадия обновления ОС;
   г) `rollback` — стадия отката обновления;

   Если для сценария не задано ни одного идентификатора стадии или стадии с заданными идентификаторами не существуют, то сценарий не будет выполнен;
3) порядок выполнения на стадии:
   а) `pre` — перед выполнением стадии;
   б) `post` — после выполнения стадии.

Формат вывода конфигурации:

```
id: <уникальный_ID_сценария/плагина>
stage: <уникальный_ID_стадии_обновления>,...
substage: pre
```

Если в выводе отсутствует любой из вышеперечисленных параметров или какой-то из них некорректен, то сценарий не будет запущен.

Пример

Запуск сценария `verification_script`:

```
verification_script config
```

Вывод команды:

```
id: Condition verification script
stage: activated
substage: post
```

При запуске без параметров сценарий должен выполнять свой основной код. В процессе выполнения сценария может выводиться в `stdout` следующая информация:

1) произвольное сообщение, регистрируемое в системном журнале;
2) предупреждения;
3) ошибки.

Сценарий может иметь код возврата. Если он ненулевой, то считается, что действие из сценария вернуло ошибку.

Результаты выполнения сценария должны выводиться в следующем формате:

```
message: <произвольное сообщение>
warning: <предупреждение>
error: <ошибка>
```

Если вывод сценария пуст или не соответствует данному формату ни в одной выведенной строке, но код возврата при этом равен нулю, то действие считается полностью успешно выполненным.

Также в сценарий может быть передана информация о результатах выполнения предыдущей стадии обновления ОС. Данная возможность предусматривается для обработки возврата на предыдущие стадии. Для получения данной информации сценарий должен иметь возможность запуска с параметром `prev <идентификатор_стадии>`. Требования к выводу сценария при запуске с данными параметрами такие же, как при его запуске без параметров.

2.3. Подраздел «6.6. Настройка SSH»

Текст между заголовком подраздела 6.6 и подзаголовком начиная со второго абзаца перенести в новый пункт 6.6.3 с соответствующим изменением нумерации последующих пунктов.

2.4. Пункт «6.6.3. Настройки безопасности»

Текст между заголовком подраздела 6.6 и подзаголовком начиная со второго абзаца перенести в новый пункт 6.6.3 с соответствующим изменением нумерации последующих пунктов и изложить в следующей редакции:

В поставляемую в составе дистрибутива версию пакета `ssh` встроены алгоритмы защитного преобразования по ГОСТ Р 34.12-2015 («Кузнечик») в режиме гаммирования (Counter, CTR) по ГОСТ Р 34.13-2015 и имитовставки с длиной хеш-кода 256 бит на основе ГОСТ Р 34.11-2012. Эти алгоритмы используются по умолчанию, их использование не требует специальной настройки.

Для вывода полного списка поддерживаемых алгоритмов выполнить следующие команды:

- вывести список поддерживаемых алгоритмов защитного преобразования:

```
ssh -Q cipher
```

- вывести список поддерживаемых алгоритмов выработки имитовставки:

```
ssh -Q mac
```

Наборы используемых алгоритмов защитного преобразования и выработки имитовставки указываются в конфигурационном файле клиента `/etc/ssh/ssh_config` в качестве значений параметров `Ciphers` и `MACs` соответственно. Если значения данных параметров не указаны или их строки закомментированы, то используются следующие алгоритмы в порядке уменьшения их приоритета:

1) защитное преобразование: `grasshopper-ctr128` («Кузнечик» по ГОСТ Р 34.12-2015), `chacha20-poly1305@openssh.com`, `aes128-ctr`, `aes192-ctr`, `aes256-ctr`, `aes128-gcm@openssh.com`, `aes256-gcm@openssh.com`, `grasshopper-cbc`;

2) имитовставка: `hmac-gost2012-256-etm` (по ГОСТ Р 34.11-2012), `umac-64-etm@openssh.com`, `umac-128-etm@openssh.com`, `hmac-sha2-256-etm@openssh.com`, `hmac-sha2-512-etm@openssh.com`, `hmac-sha1-etm@openssh.com`, `umac-64@openssh.com`, `umac-128@openssh.com`, `hmac-sha2-256`, `hmac-sha2-512`, `hmac-sha1`.

Для вывода списка текущих используемых алгоритмов в порядке уменьшения их приоритета выполнить следующие команды:

- вывести список используемых алгоритмов защитного преобразования:

```
sudo sshd -T | grep ciphers
```

- вывести список используемых алгоритмов выработки имитовставки:

```
sudo sshd -T | grep macs
```

Для указания других алгоритмов следует в конфигурационном файле сервера `/etc/ssh/sshd_config` раскомментировать строки с параметрами `Ciphers` и `MACs` и в качестве значений параметров указать через запятую нужные алгоритмы защитного преобразования и имитовставки соответственно в порядке уменьшения приоритета их выполнения.

Пример

```
Ciphers grasshopper-ctr128,chacha20-poly1305@openssh.com,aes128-ctr,\
   aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
MACs hmac-gost2012-256-etm,umac-128-etm@openssh.com,hmac-sha2-256-\
   etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.\
   com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
```

ВНИМАНИЕ! В целях безопасности не рекомендуется использовать слабые и устаревшие алгоритмы, такие как алгоритмы на основе CBC, RC4, MD5 и алгоритмы с длиной ключа менее 128 бит.

Если компьютер, выступающий в роли сервера SSH, не предполагается использовать для обеспечения работы каких-либо сетевых приложений, то рекомендуется дополнительно отключить передачу меток времени по протоколу TCP (TCP Timestamps). Данные служебные метки используются для расчета времени приема-передачи, максимального времени ожидания и других нужд сетевого протокола. Также с их помощью возможно узнать принадлежность сетевой службы конкретному серверу и время работы сервера с момента последнего запуска. Подобная информация может быть использована для определения набора обновлений безопасности, установленных на сервере, и поиска уязвимостей. Для отключения TCP Timestamps необходимо добавить в конфигурационный файл `/etc/sysctl.conf` следующую строку:

```
net.ipv4.tcp_timestamps = 0
```

Дополнительная информация по применению `ssh` доступна на официальном сайте разработчика `wiki.astralinux.ru`.

2.5. Подпункт «6.10.2.1. Параметры инструмента командной строки»

В подпункте 6.10.2.1 в таблице 33 описание параметра `cipher` изложить в редакции:

Таблица 33

Параметр	Описание
`cipher <метод>`	Метод защитного преобразования данных. Поддерживаются следующие методы защитного преобразования: - `kuznyechik-cbc` — алгоритм «Кузнечик», используется по умолчанию; - `AES-256-GCM` — рекомендован для применения в системах общего назначения; - `AES-256-CBC` — допустим для применения в системах общего назначения; - `AES-128-CBC` — используется для совместимости со старыми системами, к применению не рекомендуется

2.6. Подпункт «6.10.2.6. Настройка клиента»

В подпункте 6.10.2.6 пункт 2д) перечисления изложить в редакции:

2) в скопированном файле конфигурации внести следующие исправления:
   д) для параметра `cipher` указать метод защитного преобразования данных, используемый службой. Используемый метод защитного преобразования можно узнать на сервере OpenVPN с помощью инструмента командной строки `astra-openvpn-server`:

   ```
   sudo astra-openvpn-server get cipher
   ```

   Защитному преобразованию по алгоритму «Кузнечик» в режиме простой замены с зацеплением соответствует значение `kuznyechik-cbc`;

2.7. Подпункт «6.10.3.2. Настройка службы»

В подпункте 6.10.3.2 пункты 4) и 4а) перечисления изложить в редакции:

4) «Метод защитного преобразования» — выбор метода защитного преобразования:
   а) `kuznyechik-cbc` — алгоритм «Кузнечик», выбран по умолчанию;

2.8. Пункт «8.2.3. Предварительная настройка контроллера домена»

В пункте 8.2.3 изложить второй абзац в следующей редакции:

ВНИМАНИЕ! При развертывании домена FreeIPA на контроллере домена создается веб-сервер Apache2 для размещения веб-интерфейса FreeIPA. Работа домена FreeIPA осуществляется только при отключенном режиме `AstraMode` данного веб-сервера (описание режима приведено в 11.2). Данный режим автоматически отключается инструментом установки сервера FreeIPA `astra-freeipa-server` и графической утилитой `fly-admin-freeipa-server`. Описание настройки веб-сервера Apache2 в разделе 11 не относится к веб-серверу на контроллере домена.

2.9. Пункт «8.2.13. Настройка веб-сервера Apache2 для работы в домене FreeIPA»

Текст между заголовком пункта 8.2.13 и подпунктом 8.2.13.1 исключить, перенести подпункты в раздел 11 в виде подразделов с заменой подраздела 11.4, созданием подразделов 11.5, 11.6, и соответствующим изменением нумерации последующих подразделов. Изменить нумерацию последующих пунктов подраздела 8.2.

2.10. Подпункт «8.2.14.3. Добавление доменной службы»

Ввести новый подпункт 8.2.14.3 с соответствующим изменением нумерации следующих подпунктов:

Для добавления новой доменной службы необходимо:

1) в разделе «Идентификация» перейти во вкладку «Службы»;

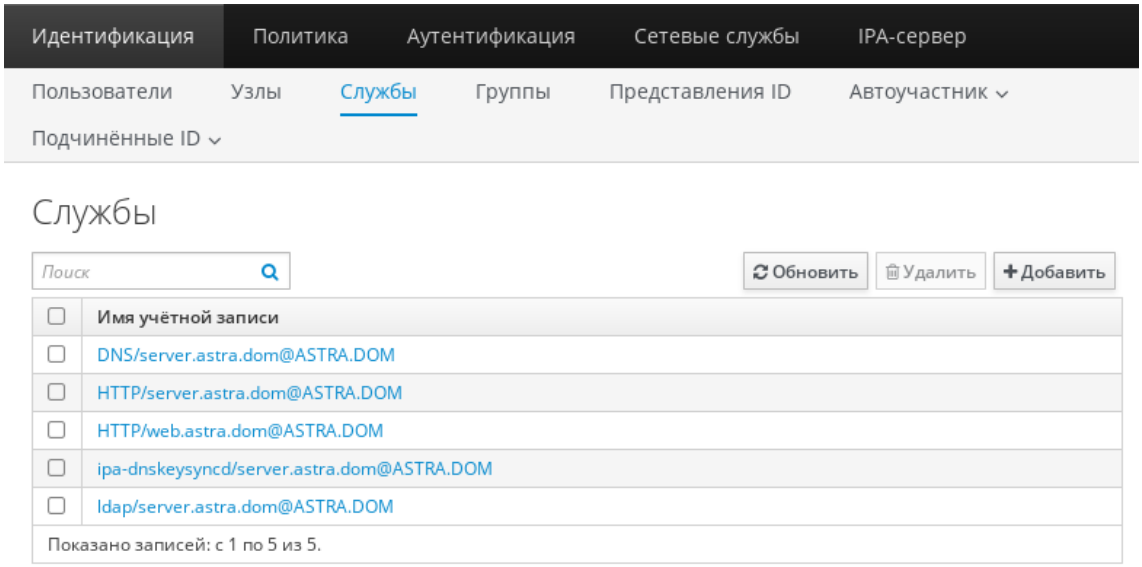

Рис. 6

2) нажать **[Добавить]**;

3) в открывшемся окне «Добавить службу» выбрать из выпадающих списков «Служба» и «Имя узла» тип службы и компьютер, на котором она будет работать;

4) для принудительной установки имени учетной записи службы, если для ее узла отсутствует запись в DNS, установить флаг «Принудительно»;

5) если узел для размещения службы недоступен или ещё не создан, то установить флаг «Пропустить проверку узла»;

6) для завершения добавления службы нажать **[Добавить]**. Для добавления службы и открытия окна для добавления еще одной службы нажать **[Добавить и добавить еще]**. Для добавления службы и последующего изменения ее параметров нажать **[Добавить и изменить]**. Для отмены изменений и закрытия окна нажать **[Отменить]**.

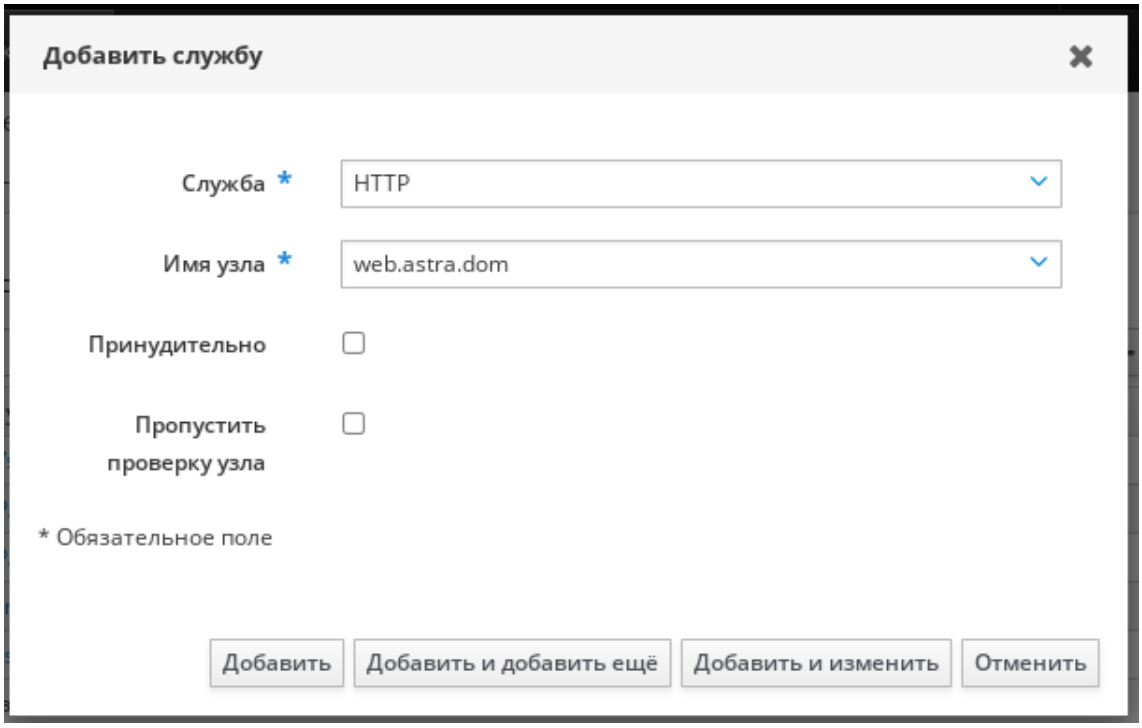

Рис. 7

2.11. Пункт «10.1.4. Docker swarm»

Ввести новый пункт 10.1.4 с соответствующим изменением нумерации последующих пунктов:

10.1.4. Docker swarm

Docker позволяет выполнять некоторые функции оркестратора контейнеров и создавать простые кластеры, состоящие из узлов, на которых запускаются контейнеры. При этом Docker не является полноценной системой оркестрации, так как не обеспечивает контроль доступа по сети, не позволяет планировать выполнение служебных задач и работать с группами контейнеров. Для управления кластерами используется механизм `docker swarm`.

Синтаксис команды:

```
docker swarm <действие> [параметры]
```

Список основных действий команды `docker swarm` приведен в таблице 50.

Таблица 50

Действие	Описание
`init`	Инициализировать кластер
`join`	Присоединить узел к кластеру в качестве рабочего или управляющего
`join-token`	Получить токен безопасности для присоединения узла к кластеру
`leave`	Вывести рабочий узел из кластера
`update`	Применить параметры кластера после их изменения

Полный список действий и параметров команды `docker swarm` приведен в официальной документации Docker.

Для разграничения доступа к кластерам и их ресурсам используются роли. Назначение ролей осуществляется добавлением пользователей в группы, приведенные в таблице 51. Группы создаются автоматически при установке Docker.

Таблица 51

Роль	Группа	Описание
Администратор кластера	`swarm-cluster-admin`	Управляет всем кластером с возможностью создания кластера и подключения нового узла к управляющему узлу кластера. Пользователям из группы доступны все возможности `docker swarm`
Администратор сервиса	`swarm-service-admin`	Управление сервисами кластера
Администратор рабочего узла	`swarm-cluster-node-admin`	Управление рабочим узлом, просмотр состояния узла, подключение узла к существующему кластеру
Наблюдатель	`swarm-observer`	Просмотр состояния кластера без внесения изменений

Управление доступа к кластерам по умолчанию включено. Для его отключения следует в файле `/etc/docker/daemon.json` изменить значение параметра `swarm-rules-enabled` на `false` (см. 10.3.2.4 и 10.3.3).

2.12. Пункт «10.2.6. Управление группами контейнеров»

В пункте 10.2.6 изменить заголовок.

2.13. Подраздел «10.3. Сканирование образов контейнеров на уязвимости»

Ввести новый подраздел 10.3:

10.3. Сканирование образов контейнеров на уязвимости

Программное обеспечение Docker и Podman обеспечивает сканирование образов контейнеров на уязвимости. Сканирование может выполняться:

- при создании образов;
- при запуске контейнеров на основе образов;
- периодически с заданным периодом выполнения.

Система сканирования представлена пакетами `openscap-scanner` и `oval-db`, устанавливаемыми автоматически при установке Docker или Podman. При необходимости пакеты могут быть установлены отдельно.

Информация об уязвимостях, подверженных им объектах и методах выявления уязвимостей содержится в файлах oval-описаний в формате XML. Актуальные версии описаний устанавливаются автоматически вместе с пакетом `oval-db` и могут автоматически обновляться (см. 10.3.2.2).

Oval-описания содержатся в отдельных файлах для каждого уровня угрозы (критический, высокий, средний, низкий, отсутствует) и группируются по имени и версии операционной системы образа в каталогах `/usr/share/oval/db/<имя>/<версия>`.

Имя и идентификатор версии (код релиза ОС) операционной системы образа содержатся внутри образа в файле `/etc/os-release` в значениях параметров `ID` и `VERSION_ID` соответственно.

Пример

```
PRETTY_NAME="Astra Linux"
NAME="Astra Linux"
ID=astra
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://astralinux.ru"
SUPPORT_URL="https://astralinux.ru/support"
LOGO=astra
VERSION_ID=1.8_x86-64
VERSION_CODENAME=1.8_x86-64
VARIANT_ID=se
```

10.3.1 Базовое использование

После установки пакетов система сканирования уязвимостей готова к работе со следующими настройками по умолчанию:

1) включено сканирование при создании образов;
2) включено сканирование при запуске контейнеров на основе образов;
3) включено периодическое сканирование образов с периодом 168 часов (7 суток);
4) для Docker дополнительно включено применение swarm-правил: проверка пользователя, работающего с Docker, на членство в группах в соответствии с ролями (см. 10.1.4).

Сканирование контейнеров при запуске выполняется в следующих случаях:

- образ контейнера ранее не сканировался;
- образ контейнера был изменен;
- с момента предыдущего сканирования прошло более 48 часов.

10.3.2 Инструмент oval-db

Для работы с oval-описаниями и изменения параметров сканирования используется инструмент командной строки `oval-db`.

Синтаксис команды:

```
sudo oval-db <действие> [параметры]
```

Действия инструмента приведены в таблице 52.

Таблица 52

Действие	Описание
`auto-update`	Включить или отключить автоматическое обновление oval-описаний
`config`	Запустить графический конфигуратор `oval-db`
`history`	Вывести историю сканирований на уязвимости
`list`	Вывести список загруженных файлов oval-описаний
`load`	Загрузить файл oval-описания из XML-файла
`restore`	Восстановить файл oval-описания из резервной копии
`remove`	Удалить загруженный файл oval-описания
`status`	Вывести состояние службы `oval-dbd`
`update`	Принудительно обновить oval-описания
`vul-info`	Вывести информацию о конкретной уязвимости
`help [действие]`	Вывести справку по указанному действию. Если действие не указано, то вывести общую справку по инструменту

10.3.2.1 Действия с файлами oval-описаний

Для вывода списка загруженных файлов oval-описаний используется действие `list`.

Синтаксис команды:

```
sudo oval-db list [параметры]
```

Параметры команды приведены в таблице 53.

Таблица 53

Параметр	Описание
`-b, --backup-include`	Включить в список каталоги с резервными копиями предыдущих версий файлов oval-описаний
`-c, --check`	Включить в список результаты проверки контрольных сумм загруженных файлов oval-описаний
`-h, --help`	Вывести справку и выйти

Пример

```
sudo oval-db list-b
```

Вывод команды:

```
astra:1.7_x86-64; Critical: 239, High: 312, Low: 2221, Medium: 16574
astra:1.7_x86-64 (Backup); High: 306, Low: 128, Medium: 2393, None: 548
astra:1.8_x86-64; Critical: 4, High: 206, Low: 8, Medium: 97, None: 7
astra:1.8_x86-64 (Backup); Critical: 11, High: 206, Low: 8, Medium: 97
ubuntu:24.04; Medium: 16574, Critical: 239, High: 312, Low: 2221
```

Для ручного добавления файлов oval-описаний используется действие `load`.

Синтаксис команды:

```
sudo oval-db load [параметры]
```

Параметры команды приведены в таблице 54.

Таблица 54

Параметр	Описание
`-f, --filepath <путь>`	Путь к загружаемому файлу oval-описания. Обязательный параметр

Продолжение таблицы 54

Параметр	Описание
`-o, --os <имя>`	Имя операционной системы, для которой загружается oval-описание. Обязательный параметр
`-v, --version <идентификатор>`	Идентификатор версии операционной системы (код релиза ОС), для которой загружается oval-описание. Обязательный параметр
`-h, --help`	Вывести справку и выйти

Пример

```
sudo oval-db load -f /tmp/oval.xml -o astra -v 1.7_x86-64
```

При добавлении новой версии ранее добавленных файлов старые файлы перемещаются в подкаталог `backup`.

Для восстановления старой версии файлов из резервной копии в подкаталоге `backup` используется действие `restore`.

Синтаксис команды:

```
sudo oval-db restore [параметры]
```

Параметры команды приведены в таблице 55.

Таблица 55

Параметр	Описание
`-o, --os <имя>`	Имя операционной системы, для которой восстанавливается oval-описание. Обязательный параметр
`-v, --version <идентификатор>`	Идентификатор версии операционной системы (код релиза ОС), для которой восстанавливается oval-описание. Обязательный параметр
`-h, --help`	Вывести справку и выйти

Для удаления добавленных oval-описаний используется действие `remove`.

Синтаксис команды:

```
sudo oval-db remove [параметры]
```

Параметры команды приведены в таблице 56.

Таблица 56

Параметр	Описание
`-o, --os <имя>`	Имя операционной системы, для которой удаляется oval-описание. Обязательный параметр
`-v, --version <идентификатор>`	Идентификатор версии операционной системы (код релиза ОС), для которой удаляется oval-описание. Обязательный параметр
`-h, --help`	Вывести справку и выйти

10.3.2.2 Обновление oval-описаний

Инструмент `oval-db` поддерживает автоматическое и ручное обновление oval-описаний для образов на основе ОС. Oval-описания для других операционных систем обновляются путем ручного добавления новых версий файлов (см. 10.3.2.1).

Автоматическое обновление oval-описаний по умолчанию отключено. Для управления автоматическим обновлением используется действие `auto-update`.

Синтаксис команды:

```
sudo oval-db auto-update [параметры]
```

Параметры команды приведены в таблице 57.

Таблица 57

Параметр	Описание
`-e, --enable`	Включить автоматическое обновление oval-описаний
`-e=false`	Отключить автоматическое обновление oval-описаний
`-h, --help`	Вывести справку и выйти

Для ручного обновления oval-описаний используется действие `update`.

Синтаксис команды:

```
sudo oval-db update [параметры]
```

Параметры команды приведены в таблице 58.

Таблица 58

Параметр	Описание
-v, --version <код_релиза_ОС>	Очередное обновление ОС, для которого будут обновлены oval-описания. Обязательный параметр. Чтобы обновить oval-описания для всех очередных обновлений ОС, следует указать значение all
-h, --help	Вывести справку и выйти

10.3.2.3 Вывод описаний уязвимостей

Инструмент oval-db позволяет выводить справочную информацию по конкретным уязвимостям с помощью действия vul-info.

Синтаксис команды:

```
sudo oval-db vul-info [параметры]
```

Параметры команды приведены в таблице 59.

Таблица 59

Параметр	Описание
-i <идентификатор>	Идентификатор уязвимости. Обязательный параметр
-o, --os <имя>	Имя операционной системы, к которой относится уязвимость. Обязательный параметр
-v, --version <идентификатор>	Идентификатор версии операционной системы (код релиза ОС), к которой относится уязвимость. Обязательный параметр
-x, --xml	Вывести информацию в XML-формате
-h, --help	Вывести справку и выйти

Пример

Вывести описание уязвимости в ОС очередного обновления 1.8:

```
sudo oval-db vul-info -i \
     oval:astra:def:101849418303406667215420926023021 1 \
     -o astra -v 1.8_x86-64
```

10.3.2.4 Графический конфигуратор системы сканирования уязвимостей

Графический конфигуратор позволяет настроить параметры сканирования и обнаружения уязвимостей для систем контейнеризации Docker и Podman.

Для запуска графического конфигуратора выполнить команду:

```
sudo oval-db config
```

Навигация в графическом интерфейсе производится с помощью мыши или клавиатуры. Используемые клавиши и их действия приведены в таблице 60.

Таблица 60

Клавиша	Описание
<←> или **<→>**	Переход между вкладками
<Enter>	Подтверждение действия
<Tab>	Переход к следующему параметру
<↑>	Переход к выбору шаблона настроек
<Q>	Выход без сохранения изменений

Интерфейс графического конфигуратора приведен на рис. 8.

Рис. 8

В графическом конфигураторе возможно выбрать один из предустановленных шаблонов настроек. Доступны шаблоны шести уровней безопасности, шаблон отключения всех функций сканирования и поиска уязвимостей, а также пользовательский шаблон. Пользовательский шаблон выбирается автоматически при изменении любых параметров.

Шаблоны настроек и их состав приведены в таблице 61.

Таблица 61

Имя шаблона	Сканирование на уязвимости при создании образа	Сканирование на уязвимости при запуске контейнера	Периодическое сканирование на уязвимости	Использование swarm-правил	Запуск контейнеров без oval-описаний	Сканирование контейнера на уязвимости / Запрет запуска при обнаружении уязвимостей				
						Уровень критичности				
						нет	низкий	средний	высокий	критический
Level 1	Да	Да	Да 7 дней	Да	Нет	Да / Да	Да / Да	Да / Да	Да / Да	Да / Да

Продолжение таблицы 61

Имя шаблона	Сканирование на уязвимости при создании образа	Сканирование на уязвимости при запуске контейнера	Периодическое сканирование на уязвимости	Использование swarm-правил	Запуск контейнеров без oval-описаний	Сканирование контейнера на уязвимости / Запрет запуска при обнаружении уязвимостей				
						Уровень критичности				
						нет	низкий	средний	высокий	критический
Level 2	Да	Да	Да 7 дней	Да	Да	Да / Да	Да / Да	Да / Да	Да / Да	Да / Да
Level 3	Да	Да	Да 7 дней	Да	Да	Да / Нет	Да / Нет	Да / Да	Да / Да	Да / Да
Level 4	Да	Да	Да 7 дней	Да	Да	Нет / Нет	Да / Нет	Да / Нет	Да / Да	Да / Да
Level 5	Да	Да	Да 7 дней	Да	Да	Нет / Нет	Нет / Нет	Да / Нет	Да / Да	Да / Да
Level 6	Да	Да	Да 14 дней	Да	Да	Нет / Нет	Нет / Нет	Нет / Нет	Да / Нет	Да / Нет
None	Нет	Нет	Нет	Нет	Да	Нет / Нет	Нет / Нет	Нет / Нет	Нет / Нет	Нет / Нет

10.3.3 Конфигурационные файлы системы сканирования уязвимостей

Настройки системы сканирования уязвимостей хранятся в формате JSON в следующих конфигурационных файлах:

- `/etc/podman.json` — параметры сканирования для системы контейнеризации Podman;
- `/etc/docker/daemon.json` — параметры сканирования для системы контейнеризации Docker;
- `/usr/share/oval/conf/podman.json` — параметры поиска уязвимостей при использовании Podman;
- `/usr/share/oval/conf/docker.json` — параметры поиска уязвимостей при использовании Docker;
- `/usr/share/oval/conf/daemon.json` — параметры службы `oval-dbd`.

При отсутствии какого-либо файла применяются настройки по умолчанию.

Параметры сканирования образов и контейнеров содержатся в конфигурационных файлах Docker и Podman — `/etc/docker/daemon.json` и `/etc/podman.json` соответственно. Для обоих систем контейнеризации используются одинаковые параметры, за исключением параметра `swarm-rules-enabled`. После установки системы сканирования уязвимостей в

файлы добавляются следующие настройки по умолчанию. Комментарии в файле начинаются с символа «#».

```
{
   # Включение или отключение сканирования при создании образов
   "scan-on-image-create": true,

   # Включение или отключение сканирования при запуске контейнеров из образов
   "scan-on-container-start": true,

   # Включение или отключение swarm-правил (только для /etc/docker/daemon.json)
   "swarm-rules-enabled": true,

   # Период сканирования образов в часах
   "periodic-scan-time-in-hours": 168
}
```

Параметры поиска уязвимостей при использовании Docker и Podman содержатся в конфигурационных файлах `oval-db` — `/usr/share/oval/conf/docker.json` и `/usr/share/oval/conf/podman.json` соответственно. Для обоих систем контейнеризации используются одинаковые параметры. После установки системы сканирования уязвимостей файлы имеют следующее содержимое, соответствующее настройкам по умолчанию. Комментарии в файле начинаются с символа «#».

```
{

   # система контейнеризации (docker или podman)
   "engine": "docker",

   # управление запуском контейнеров без oval-описаний (true - разрешено, false - \
      запрещено)
   "allow-run-wo-oval-file": true,

   # параметры для различных уровней критичности уязвимостей
   "levels": {
      "critical": {

         # обнаружение уязвимостей данного уровня критичности (true - включено, \
            false - отключено)
         "enabled": true,

         # запрет запуска контейнеров с обнаруженными уязвимостями (true - запуск \
            запрещен, false - запуск разрешен)
         "drop": true
      },
      "high": {
         "enabled": true,
         "drop": true
```

```
      },
      "medium": {
         "enabled": true,
         "drop": true
      },
      "low": {
         "enabled": true,
         "drop": true
      },
      "none": {
         "enabled": true,
         "drop": true
      }
   }
}
```

Параметры службы `oval-dbd` содержатся в файле `/usr/share/oval/conf/daemon.json`. После установки системы сканирования уязвимостей файл имеет следующее содержимое, соответствующее настройкам по умолчанию. Комментарии в файле начинаются с символа «#».

```
{
  # Параметры базы данных уязвимостей
  "Database": {

    # Путь к базе данных с результатами сканирования
    "Path": "/usr/share/oval/history/scan_results.db",

    # Срок устаревания результатов сканирования (в часах)
    "ExpireTime": 48
  },

  # Параметры автоматического обновления oval-описаний для образов на основе Astra \
     Linux
  "Update": {

    # Автоматическая проверка наличия обновлений oval-описаний
    "Auto": true,

    # URL сервера, с которого будет выполняться обновление
    "ManifestUrl": "https://dl.astralinux.ru/artifactory/al-oval/oval_meta.json",

    # Временный каталог для размещения загружаемых файлов
    "TmpDir": "/tmp/oval_temp/",

    # Интервал проверки обновлений oval-описаний (в часах)
    "Interval": 24,

    # URL каталога с файлами oval-описаний на сервере
```

```
   "FoldersForVersionsUrl": "https://dl.astralinux.ru/astra/oval/"
  }
}
```

10.3.4 Обновление oval-описаний в закрытом контуре

10.3.4.1 Настройка сервера обновления oval-описаний

При необходимости возможно создать локальный сервер для обновления oval-описаний уязвимостей ОС с доступом по протоколам HTTP/HTTPS или FTP. На сервере должен присутствовать каталог с oval-описаниями, все элементы которого должны быть доступны для загрузки.

Пример

Вариант структуры каталога с oval-описаниями на сервере.

```
oval/
| 1.7_x86-64/
|    |--- oval-definitions-alse-1.7.xml
|    |--- oval-definitions-alse-1.7.xml.md5
|    |--- oval-definitions-alse-1.7.xml.sha1
|    |--- oval-definitions-alse-1.7.xml.sha256
| 1.8_x86-64/
|    |---...
| 4.7_arm/
|    |---...
|--- oval_meta.json
|--- oval_meta.json.md5
|--- oval_meta.json.sha1
|--- oval_meta.json.sha256
...
```

Oval-описания хранятся в файлах формата XML и размещаются для удобства в отдельных каталогах для каждого очередного обновления и архитектуры ОС. Файлы форматов MD5, SHA1 и SHA256 размещаются в тех же каталогах и содержат контрольные суммы одноименных файлов. Файл `oval_meta.json` содержит ссылки на все доступные oval-описания и значения их контрольных сумм.

Пример

Файл `oval_meta.json`. Комментарии в файле начинаются с символа «#».

```
{
# Массив процессорных архитектур ОС
"platforms": [
   {
      # Процессорная ахитектура ОС
      "platform": "x86-64",

      # Массив очередных обновлений ОС в рамках процессорной архитектуры
      "targets": [

         {
            # Очередное обновление ОС (обязательный элемент)
            "target": "1.8_x86-64",

            # URL файла oval-описания (обязательный элемент)
            "url": "http://server.astra.dom/oval/1.8_x86-64/oval-definitions-\
               alse-1.8.xml",

            # Контрольная сумма файла oval-описания по MD5 (обязательный \
               элемент)
            "md5": "ccf88d2c64764db8fdd3ded3f5cfd54f",

            # Контрольные суммы файла oval-описания по SHA256 и ГОСТ
            "sha256sum": "58\
               f8075bbf40fb822de9a2cacc91067c8055ed8e05449f58997e3c50cf93371b\
               ",
            "gost": "\
               ad35297e12241c12574d6abc9edae6004bd7e9eb97a8daba2b93fdd2ed76bc27\
               ",

            # Дата добавления файла oval-описания на сервер
            "uploaded": "21-05-2025 14:54:10.513"
         },
         {
            "target": "1.7_x86-64",
            "url": "http://server.astra.dom/oval/1.7_x86-64/oval-definitions-\
               alse-1.7.xml",
            "md5": "b1d7fbd7de8d4b5554d18cf4168224a0",
            "sha256sum": "783709\
               c6a0ad9b8f610c05be2e86e45e69538b0c573f3e654279ce2379640e37",
            "gost": "\
               af9f17dfcffa95b5a3ac85f9da834dde07ef8434b7a6d9ac59de581eab990c45\
               ",
            "uploaded": "19-05-2025 14:38:41.976"
         }
      ]
   }
   {
      "platform": "arm",
      "targets": [
```

```
            {
               "target": "4.7_arm",
               "url": "https://dl.astralinux.ru/astra/oval/4.7_arm/oval-\
                  definitions-alse-4.7.xml",
               "md5": "1534df4ecb76014aec8da1d090948e3b",
               "sha256sum": "\
                  bed2619a835e6afc31171f29c1a0b659d7124604fa03e8cc5a9c3dadd3c474f5\
                  ",
               "gost": "7\
                  ee2703817bfbf13ff242b5bb55daccf554dfc7c30a0bc4cdc20854e70bd6423\
                  ",
               "uploaded": "02-06-2025 16:28:37.169"
            }
         ]
      }
]
}
```


Обновление файлов oval-описаний на сервере в закрытом контуре выполняется вручную:

1) получить актуальные версии oval-описаний на компьютере с установленным пакетом `oval-db` и доступом в Интернет:

а) для получения актуальных версий всех oval-описаний для ОС выполнить команду:

```
sudo oval-db update -v all
```

б) для получения актуальных версий oval-описаний для определенного очередного обновления ОС выполнить команду:

```
sudo oval-db update -v <кодовое_имя_ОС>
```

где кодовое имя ОС — это значение параметра `VERSION_ID` в файле `/etc/os-release`;

Пример

```
sudo oval-db update -v 1.8_x86-64
```

2) после завершения обновления перенести содержимое каталога `/usr/share/oval/db/astra/` в такой же каталог на сервере обновления и убедиться, что права доступа к файлам и подкаталогам такие же, как на исходном компьютере.

10.3.4.2 Настройка клиента для обновления oval-описаний

Настройки обновления oval-описаний на клиентском компьютере содержатся в файле `/usr/share/oval/conf/daemon.json` (см. 10.3.3). Данный файл по умолчанию отсут-

ствует и создается при включении автоматического обновления oval-описаний (см. 10.3.2.2). Для указания сервера обновлений следует изменить значения следующих параметров:

1) `ManifestUrl` — указать URL или путь к файлу `oval_meta.json` на сервере обновлений;

2) `FoldersForVersionsUrl` — указать URL каталога с oval-описаниями на сервере обновлений.

Пример

Файл `/usr/share/oval/conf/daemon.json`.

```
{
  "Database": {
    "Path": "/usr/share/oval/history/scan_results.db",
    "ExpireTime": 48
  },
  "Update": {
    "Auto": true,
    "ManifestUrl": "http://server.astra.dom/oval/oval_meta.json",
    "TmpDir": "/tmp/oval_temp/",
    "Interval": 24,
    "FoldersForVersionsUrl": "http://server.astra.dom/oval/"
  }
}
```

2.14. Подраздел «11.1. Установка и настройка веб-сервера Apache2»

2.14.1. В подразделе 11.1 изменить заголовок и изложить первый абзац в следующей редакции:

Для развертывания веб-сервера Apache2 требуется установить пакет `apache2` на компьютер, который будет использовать в качестве веб-сервера. Установка выполняется командой:

```
sudo apt install apache2
```

После установки веб-сервер Apache2 будет готов к приему запросов на всех сетевых интерфейсах на 80 порту.

2.14.2. В подразделе 11.1 изложить предпоследний абзац в следующей редакции:

Дополнительные настройки веб-сервера для предоставления пользователям доступа к страницам и другому содержимому веб-сайтов с ненулевыми классификационными метками приведены в 11.6.

2.15. Подраздел «11.3. Настройка аутентификации через PAM»

Изменить заголовок подраздела 11.3.

2.16. Подраздел «11.4. Настройка веб-сервера Apache2 для работы в домене FreeIPA»

Изложить подраздел 11.4 в следующей редакции:

При работе в составе домена FreeIPA веб-сервер Apache2 может использоваться для аутентификации пользователей с использованием Kerberos, в том числе для сквозной аутентификации в приложениях.

Для обеспечения работы веб-сервера Apache2 в составе домена FreeIPA требуется:

1) развернутый домен FreeIPA, например `astra.dom` (см. 8.2.3, 8.2.4 и 8.2.5);
2) отдельный компьютер для размещения веб-сервера Apache2, удовлетворяющий следующим требованиям:
   а) компьютер с веб-сервером должен быть введен в домен FreeIPA в соответствии с 8.2.6;
   б) разрешение имен должно быть настроено таким образом, чтобы имя компьютера с веб-сервером разрешалось как полное доменное имя (FQDN), например `web.astra.dom`;
   в) компьютеру с веб-сервером должен быть назначен статический IP-адрес.

В качестве дополнительной меры безопасности возможно настроить использование защищенных SSL-соединений между веб-сервером и его клиентами (см. 11.5).

Для настройки аутентификации Kerberos требуется дополнительно установить на веб-сервере модуль аутентификации `auth-gssapi`. Установка выполняется командой:

```
sudo apt install libapache2-mod-auth-gssapi
```

Активация модуля происходит автоматически при установке.

Если в ОС установлен в соответствии с 11.3 модуль веб-сервера Apache2 `authnz_pam` для аутентификации через PAM, то его следует отключить при помощи команды:

```
sudo a2dismod authnz_pam
```

Если модуль `auth_gssapi` был ранее отключен, то для его активации выполнить команду:

```
sudo a2enmod auth_gssapi
```

ВНИМАНИЕ! При установке на компьютер веб-сервера Apache2 по умолчанию включается режим `AstraMode` для работы с ненулевыми классификационными метками (см. 11.2). Для работы аутентификации Kerberos в данном режиме следует в конфигурационном файле `/etc/apache2/apache2.conf` добавить (раскомментировать) параметр `IncludeRealm` со значением `on`.

ВНИМАНИЕ! При включенном режиме `AstraMode` доменным пользователям, проходящим аутентификацию, должны быть явно заданы классификационные метки (диапазоны уровней конфиденциальности и категорий конфиденциальности) с помощью соответствующих утилит, даже если этим пользователям недоступны уровни и категории выше 0. Дополнительная информация приведена в документе РУСБ.10015-01 97 01-1.

Развернутый веб-сервер необходимо зарегистрировать в качестве доменной службы одним из следующих способов:

1) в веб-интерфейсе администратора FreeIPA (см. 8.2.14.3);

2) с помощью инструмента командной строки `ipa`. Для этого необходимо на контроллере домена или компьютере веб-сервера выполнить следующее:

   а) получить билет Kerberos администратора домена:

```
kinit admin
```

   б) зарегистрировать доменную службу:

```
ipa service-add HTTP/<полное_доменное_имя_хоста_веб-сервера>
```

П р и м е р

```
ipa service-add HTTP/web.astra.dom
```

Для аутентификации пользователей на веб-сервере необходимо загрузить с контроллера домена на компьютер веб-сервера таблицу ключей для зарегистрированной службы, выполнив на компьютере веб-сервера следующее:

1) получить билет Kerberos администратора домена для пользователя `root` (необходимо для последующего использования билета с механизмом `sudo`):

```
sudo kinit admin
```

2) получить с контроллера домена таблицу ключей Kerberos и сохранить ее в файл:

```
sudo ipa-getkeytab -p HTTP/<полное_доменное_имя_хоста_веб-сервера> -k \
     <путь_к_сохраняемому_файлу_таблицы>
```

Пример

```
sudo ipa-getkeytab -p HTTP/web.astra.dom -k /etc/apache2/keytab
```

Примечание. Получить таблицу ключей с помощью `ipa-getkeytab` можно на контроллере домена. В этом случае полученную таблицу необходимо скопировать на компьютер веб-сервера;

3) изменить владельца полученной таблицы ключей на служебную учетную запись `www-data` и установить права доступа:

```
sudo chown www-data <путь_к_таблице_ключей>
sudo chmod 600 <путь_к_таблице_ключей>
```

На компьютере веб-сервера создать конфигурационный файл с параметрами аутентификации Kerberos, например `/etc/apache2/conf-available/kerberos-auth.conf`, в котором указать путь к сохраненной таблице ключей. Файл должен содержать следующие строки:

```
<Directory /var/www>
# тип аутентификации
AuthType GSSAPI
# Подсказка с информацией о ресурсе (выводится при запросе пароля)
AuthName "Astra Kerberos protected area"
GssapiCredStore keytab:<путь_к_таблице_ключей>
# Включить 3 нижних параметра, если нужно кешировать сессии
#GssapiUseSessions On
#Session On
#SessionCookieName myapp_web_gssapi_session path=/my_url;httponly;secure;
Require valid-user
</Directory>
```

Созданный конфигурационный файл необходимо указать с помощью директивы `Include` в конфигурационных файлах веб-сайтов, размещаемых в каталоге `/etc/apache2/sites-available/`. Путь к файлу аутентификации указывается относительно каталога `/etc/apache2/`.

Пример

```
Include conf-available/kerberos-auth.conf
```

Чтобы использовать аутентификацию на веб-сайте, созданном по умолчанию при установке Apache2 (`http://<полное_доменное_имя_хоста_веб-сервера>/`),

следует указать файл аутентификации в его конфигурационном файле /etc/apache2/sites-available/000-default.conf.

Для создания веб-сайта, например http://web.astra.dom/authorized/, требующего аутентификацию Kerberos, необходимо выполнить следующее:

1) создать конфигурационный файл веб-сайта /etc/apache2/sites-available/authorized.conf и указать в нем ранее созданный файл аутентификации /etc/apache2/conf-available/kerberos-auth.conf:

```
<VirtualHost *:80>
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
Include conf-available/kerberos-auth.conf
</VirtualHost>
```

2) активировать созданный конфигурационный файл веб-сайта:

```
sudo a2ensite authorized
```

3) создать каталог /var/www/html/authorized для файлов веб-сайта;

4) создать файл /var/www/html/authorized/index.html с заглавной страницей.

Пример

```
<html>
<body>
<div style="width: 100%; font-size: 40px; font-weight: bold; text-\
   align: center;">
Тестовая страница для проверки аутентификации Kerberos.
Если вы видите этот текст, то аутентификация выполнена успешно.
</div>
</body>
</html>
```

5) для корректного отображения кириллицы в тексте страниц веб-сайта добавить в конфигурационный файл /etc/apache2/apache2.conf строку:

```
AddDefaultCharset UTF-8
```

6) обновить конфигурацию веб-сервера:

```
sudo systemctl reload apache2
```

Для аутентификации на веб-сервере необходимо на компьютере, с которого осуществляется доступ к веб-серверу, получить билет Kerberos:

1) если используемый компьютер входит в домен:
   а) при работе от имени доменного пользователя билет выдается автоматически при входе в сессию. Для просмотра выданных билетов выполнить команду:

   ```
   klist
   ```

   б) при работе от имени локального пользователя получить билет Kerberos на имя доменного пользователя:

   ```
   kinit <имя_пользователя_домена>
   ```

2) если используемый компьютер не входит в домен:
   а) установить клиент Kerberos:

   ```
   sudo apt install krb5-user
   ```

   б) указать в качестве DNS-сервера адрес контроллера домена FreeIPA (см. 8.2.6.1);
   в) получить билет Kerberos на имя доменного пользователя:

   ```
   kinit <имя_пользователя_домена>
   ```

Для проверки аутентификации через консоль следует загрузить заглавную страницу веб-сайта:

```
curl --negotiate -u : http://<полное_доменное_имя_хоста_веб-сервера>/authorized/
```

В случае успешной аутентификации доменного пользователя по билету Kerberos будет получен доступ к заглавной странице сайта и команда выведет содержимое созданного файла `/var/www/html/authorized/index.html`.

Для работы аутентификации Kerberos при использовании веб-браузера данный браузер должен поддерживать метод аутентификации `negotiate`. Для включения метода `negotiate` и проверки аутентификации в веб-браузере Mozilla Firefox выполнить следующее:

1) в адресной строке веб-браузера ввести:

   ```
   about:config
   ```

2) ввести в строке поиска параметр `network.negotiate-auth.trusted-uris` и нажать «Изменить»;

3) задать маски доменов, для которых будет использоваться аутентификация `negotiate`. В общем случае в качестве значения можно указать `http://`, `https://`;

4) нажать «Сохранить»;

5) ввести в адресной строке:

```
http://<полное_доменное_имя_хоста_веб-сервера>/authorized/
```

В случае успешной аутентификации пользователя по билету Kerberos будет отображена заглавная страница сайта `/var/www/html/authorized/index.html`.

Если необходимо обеспечить сквозную аутентификацию из сценариев при работе с другими службами, например с сервером СУБД, то в веб-браузере Mozilla Firefox для параметра `network.negotiate-auth.delegation-uris` следует задать маски доменов, которым можно передавать данные для сквозной аутентификации. При этом в запускаемых сценариях следует выставить переменную окружения `KRB5CCNAME`.

Пример

Установка переменной для сценариев на языке PHP:

```
putenv("KRB5CCNAME=" . $_SERVER['KRB5CCNAME']);
```

2.17. Подраздел «11.6. Настройка веб-сервера Apache2 для работы с данными ограниченного доступа»

Изменить заголовок подраздела 11.6 и изложить его в следующей редакции:

Разграничение доступа к содержимому веб-сайтов на веб-сервере Apache2 осуществляется за счет мандатного управления доступом при включенном параметре `AstraMode` (см. 11.2).

Доступ пользователя к содержимому веб-сайта определяется сопоставлением классификационных меток файлов веб-сервера с классификационной меткой пользователя. Файлы с ненулевыми классификационными метками доступны только из сессии пользователя с соответствующей классификационной меткой. Если классификационная метка пользователя ниже метки файла или несравнима с ней, то файл будет недоступен и веб-сервер вернет ошибку «404».

Перед назначением классификационных меток каталогу и файлам веб-сайта необходимо назначить каталогам веб-сервера `/var/www/` и `/var/www/html/` максимальные классификационные метки, с которыми планируется работать, а также дополнительный атрибут `ccnr`:

```
sudo pdpl-file -u <уровень_конфиденциальности>::\
```

```
     <категории_конфиденциальности>:ccnr /var/www
sudo pdpl-file -u <уровень_конфиденциальности>::
     <категории_конфиденциальности>:ccnr /var/www/html
```

Если каталогу веб-сайта назначается классификационная метка с дополнительным атрибутом `ccnr`, то файлы и подкаталоги в нем могут иметь различные классификационные метки (в том числе нулевые), но не выше метки каталога. Это позволяет создать заглавную страницу с нулевой классификационной меткой, видимую всем пользователям, и ограничить доступ к другому содержимому.

Пример

Назначить каталогу веб-сайта `/restricted` второй уровень конфиденциальности, все возможные категории конфиденциальности и атрибут `ccnr`, а файлу `secret.html` — первый уровень и категорию `Категория_1` (категория должна быть определена в системе):

```
sudo pdpl-file -u 2::-1:ccnr /var/www/html/restricted
sudo pdpl-file -u 1::Категория_1 /var/www/html/restricted/secret.html
```

Если каталогу веб-сайта назначается классификационная метка без атрибута `ccnr`, то все файлы и подкаталоги в нем могут иметь только такую же классификационную метку. Доступ ко всему содержимому веб-сайта будет возможен только из сессии пользователя с классификационной меткой не ниже назначенной.

Примечание. Если назначить классификационную метку без атрибута `ccnr` каталогу веб-сайта по умолчанию `/var/www/html/`, то на веб-сервере будет возможно создавать другие веб-сайты только с такой же классификационной меткой.

Для ограничения доступа к создаваемому новому веб-сайту с использованием единой классификационной метки для всего его содержимого необходимо создать каталог веб-сайта и назначить ему требуемую классификационную метку:

```
sudo pdpl-file -u <уровень_конфиденциальности>::\
     <категории_конфиденциальности> /var/www/html/<каталог_веб-сайта>
```

Пример

Создать каталог веб-сайта `/secret` и назначить ему третий уровень конфиденциальности:

```
sudo mkdir /var/www/html/secret
sudo pdpl-file -u 3 /var/www/html/secret
```

Если требуется ограничить доступ с использованием единой классификационной метки к веб-сайту с уже имеющимся содержимым, то необходимо:

1) назначить каталогу веб-сайта и всему его содержимому требуемую классификационную метку и атрибут `ccnr` (нужен для рекурсивного изменения меток):

```
sudo pdpl-file -R -u <уровень_конфиденциальности>::\
     <категории_конфиденциальности>:ccnr /var/www/html/<каталог_веб-сайта>
```

2) снять атрибут `ccnr` с каталогов и подкаталогов веб-сайта:

```
sudo pdpl-file -R -s <уровень_конфиденциальности>:::ccnr\
     /var/www/html/<каталог_веб-сайта>
```

Пример

Назначить веб-сайту `/secret` второй уровень конфиденциальности и категорию `Категория_2` (категория должна быть определена в системе) без атрибута `ccnr`:

```
sudo pdpl-file -R -u 2::Категория_2:ccnr /var/www/html/secret
sudo pdpl-file -R -s 2:::ccnr /var/www/html/secret
```

Для применения изменений необходимо перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

Дополнительная информация по мандатному управлению доступом приведена в документе РУСБ.10015-01 97 01-1.

2.18. Подраздел «12.6. Рабочий стол Fly»

В подразделе 12.6 из таблицы 50 исключить следующую строку:

Таблица 50

Параметр	Описание
`fly-admin-dhcp` «Настройка DHCP-сервера»	Настройка сервера DHCP

2.19. Подраздел «14.2. Установка комплекса программ печати»

В подразделе 14.2 изложить последний абзац в следующей редакции:

В случае необходимости возможно вручную установить защищенный комплекс программ печати и маркировки документов, выполнив команду:

```
sudo apt install parsec-cups fly-admin-printer-mac fly-admin-marker fly-print-station
```

2.20. Подраздел «14.3. Настройка комплекса программ печати»

Изложить текст между заголовком подраздела 14.3 и пунктом 14.3.1 в следующей редакции:

Настройка защищенного комплекса программ печати и маркировки документов (сервер печати CUPS) выполняется редактированием конфигурационных файлов `/etc/cups/cupsd.conf` и `/etc/cups/cups-files.conf`. Копии конфигурационных файлов, устанавливаемые вместе с пакетом, размещаются в `/usr/share/cups` (файлы `cupsd.conf.default` и `cups-files.conf.default`), данные файлы могут использоваться при необходимости восстановить комплекс программ печати и маркировки документов в исходное состояние.

Настройка сервера печати CUPS также может выполняться следующими способами:

1) графической утилитой `fly-admin-printer`;
2) через веб-интерфейс по адресу:

```
localhost:631/admin
```

3) инструментом командной строки `cupsctl`. Запуск инструмента возможен:
   а) от имени пользователя `root` с использованием механизма `sudo`:

   ```
   sudo cupsctl [параметры]
   ```

   б) от имени пользователя, входящего в группы с правами администрирования сервера печати CUPS, командой:

   ```
   /usr/sbin/cupsctl [параметры]
   ```

Группы пользователей с правами администрирования сервера печати CUPS указаны в качестве значения параметра `SystemGroup` в файле `/etc/cups/cups-files.conf`. По умолчанию в этот список включены группы `root` и `lpadmin`. Если удалить группу `root` из значения параметра `SystemGroup`, то инструмент командной строки `cupsctl`, запущенный на компьютере сервера печати с использованием механизма `sudo`, будет возвращать ошибку доступа.

Основные пользовательские настройки содержатся в конфигурационных файлах `/etc/cups/client.conf` и `/home/<имя_пользователя>/.cups/lpoptions`.

2.21. Пункт «14.3.1. Настройка сервера печати с локальной аутентификацией»

Изменить заголовок пункта 14.3.1 и изложить его следующей редакции:

Чтобы сервер печати мог удаленно принимать задания и команды, необходимо разрешить совместный доступ к принтерам, выполнив команду:

```
sudo cupsctl --share-printers
```

При необходимости принимать задания печати с любых адресов, а не только из подсети сервера печати, следует выполнить команду:

```
sudo cupsctl --remote-any
```

Администрирование сервера печати CUPS по умолчанию разрешено только локально. Для включения удаленного администрирования выполнить команду:

```
sudo cupsctl --remote-admin
```

По умолчанию сервер печати использует политику доступа, которая позволяет не прошедшим аутентификацию пользователям добавлять принтеры и отправлять задания на печать. Для разрешения доступа к серверу печати и принтерам только аутентифицированным пользователям необходимо применить встроенную политику доступа `authenticated`:

```
sudo cupsctl DefaultPolicy=authenticated
```

Для применения изменений перезагрузить сервер печати:

```
sudo systemctl restart cups
```

2.22. Пункт «14.3.2. Настройка сервера печати для работы в ЕПП»

Изменить заголовок пункта 14.3.2 и изложить его в следующей редакции:

Для работы системы печати в ЕПП компьютер сервера печати CUPS должен быть введен в домен в соответствии с 8.2.6.

Для авторизации на сервере печати и выполнения действий по управлению принтерами и очередями печати следует создать в FreeIPA учетную запись администратора печати и предоставить ей права на сервере печати одним из следующих способов:

- добавить учетную запись администратора печати в локальную группу администраторов печати lpadmin:

```
sudo gpasswd –a <доменное_имя_учетной_записи> lpadmin
```

Пример

```
sudo gpasswd –a print_admin@ASTRA.DOM lpadmin
```

- указать в значении параметра SystemGroup в файле /etc/cups/cups-files.conf первичную группу администратора печати, совпадающую с его доменным именем:

```
SystemGroup root lpadmin <полное_имя_первичной_группы>
```

Пример

```
SystemGroup root lpadmin print_admin@ASTRA.DOM
```

- добавить учетную запись администратора печати в доменную группу и указать эту группу в значении параметра SystemGroup в файле /etc/cups/cups-files.conf:

```
SystemGroup root lpadmin <полное_имя_доменной_группы>
```

Пример

```
SystemGroup root lpadmin printer_admins@ASTRA.DOM
```

Все члены указанной доменной группы получат права на управление сервером печати.

Для доступа пользователей к серверу печати через веб-интерфейс необходима HTTP-служба, зарегистрированная для компьютера сервера печати в домене FreeIPA. Если сервер печати развернут на контроллере домена, то данная служба уже была создана автоматически при создании домена. Если сервер печати развернут на отдельном компьютере в составе домена, то для регистрации службы необходимо на сервере печати выполнить следующее:

1) получить билет Kerberos администратора домена для пользователя root (необходимо для последующего использования билета с механизмом sudo):

```
sudo kinit admin
```

2) зарегистрировать доменную службу HTTP:

```
sudo ipa service-add HTTP/<полное_имя_хоста_сервера_печати>
```

Пример

```
sudo ipa service-add HTTP/cups.astra.dom
```

3) получить с контроллера домена таблицу ключей Kerberos и сохранить ее в файл:

```
sudo ipa-getkeytab -p HTTP/<полное_имя_хоста_сервера_печати> -k \
     /etc/krb5.keytab
```

Пример

```
sudo ipa-getkeytab -p HTTP/cups.astra.dom -k /etc/krb5.keytab
```

Если сервер печати развернут на контроллере домена, то доменную службу создавать и регистрировать не нужно. Для получения копии существующих ключей доменной службы HTTP выполнить следующее:

1) получить билет Kerberos администратора домена для пользователя `root` (необходимо для последующего использования билета с механизмом `sudo`):

```
sudo kinit admin
```

2) разрешить группе администраторов домена получение таблицы ключей:

```
sudo ipa service-allow-retrieve-keytab \
     HTTP/<полное_имя_контроллера_домена> --groups=admins
```

3) получить копию таблицы ключей:

```
sudo ipa-getkeytab -p \
     HTTP/<полное_имя_контроллера_домена> -k /etc/krb5.keytab -r
```

4) вернуть изначальное состояние доступа к таблице ключей:

```
sudo ipa service-disallow-retrieve-keytab \
     HTTP/<полное_имя_контроллера_домена> --groups=admins
```

Для проверки добавления ключей выполнить команду:

```
sudo klist -kte /etc/krb5.keytab
```

Корректный вывод команды:

```
Keytab name: FILE:/etc/krb5.keytab
```

```
KVNO Timestamp Principal
---- ------------------ --------------------------------------------------------
  1 26.06.2025 14:22:30 host/cups.astra.dom@ASTRA.DOM (aes256-cts-hmac-sha384-192)
  1 26.06.2025 14:22:30 host/cups.astra.dom@ASTRA.DOM (aes128-cts-hmac-sha256-128)
  1 26.06.2025 14:22:30 host/cups.astra.dom@ASTRA.DOM (aes256-cts-hmac-sha1-96)
  1 26.06.2025 14:22:30 host/cups.astra.dom@ASTRA.DOM (aes128-cts-hmac-sha1-96)
  1 26.06.2025 14:39:01 HTTP/cups.astra.dom@ASTRA.DOM (aes256-cts-hmac-sha384-192)
  1 26.06.2025 14:39:01 HTTP/cups.astra.dom@ASTRA.DOM (aes128-cts-hmac-sha256-128)
  1 26.06.2025 14:39:01 HTTP/cups.astra.dom@ASTRA.DOM (aes256-cts-hmac-sha1-96)
  1 26.06.2025 14:39:01 HTTP/cups.astra.dom@ASTRA.DOM (aes128-cts-hmac-sha1-96)
```

Для дальнейшей настройки сервера печати выполнить следующее:

1) выбрать метод `Negotiate` в качестве способа аутентификации по умолчанию:

```
sudo cupsctl DefaultAuthType=Negotiate
```

2) указать имя хоста сервера печати:

```
sudo cupsctl ServerName=<полное_имя_хоста_сервера_печати>
```

3) включить поддержку мандатного управления доступом:

```
sudo cupsctl MacEnable=On
```

4) перезапустить службу сервера печати, выполнив команду:

```
sudo systemctl restart cups
```

ВНИМАНИЕ! В конфигурационном файле защищенного сервера печати `/etc/cups/cupsd.conf` не допускается установка значения `None` параметра `DefaultAuthType` (отключение аутентификации)и внесение изменений в параметры политики PARSEC, не соответствующих эксплуатационной документации.

По умолчанию локальные пользователи сервера печати, входящие в группу `lpadmin`, не проходят аутентификацию Kerberos при доступе к серверу печати, так как локальное соединение с сервером выполняется через сокет (механизм `SO_PEERCRED`). Для переключения локальных пользователей на сетевое соединение с аутентификацией Kerberos необходимо:

1) создать на сервере печати файл `/etc/cups/client.conf`, содержащий строку:

```
ServerName <полное_имя_хоста_сервера_печати>
```

2) сделать данный файл доступным на чтение всем пользователям:

```
sudo chmod +r /etc/cups/client.conf
```

При настроенном удаленном администрировании (см. 14.3.1) сервер печати по умолчанию принимает только обращения, содержащие в HTTP-заголовке полное сетевое имя его хоста.

При необходимости возможно настроить доступ к серверу печати с помощью одного или нескольких сетевых псевдонимов (псевдоним должен разрешаться в IP-адрес службой DNS). Для указания псевдонима выполнить команду:

```
sudo cupsctl ServerAlias=<псевдоним_сервера_печати>
```

Пример

Указать псевдоним `printserver` для доступа к серверу печати по адресу `http://printserver:631`:

```
sudo cupsctl ServerAlias=printserver
```

Указать несколько псевдонимов возможно через пробел в значении параметра `ServerAlias` в конфигурационном файле `/etc/cups/cupsd.conf`. Если в качестве псевдонима указать символ «*», то будут разрешены обращения по любым псевдонимам.

Если удаленное администрирование отключено, то единственным разрешенным псевдонимом является `localhost`.

Настройка браузера Mozilla Firefox для использования аутентификации Kerberos описана в 11.4.

Настройка принтеров может быть выполнена с использованием графической утилиты `fly-admin-printer` (см. электронную справку).

2.23. Пункт «14.3.3. Настройка клиентов сервера печати»

Ввести новый пункт 14.3.3 с соответствующим изменением нумерации следующих пунктов:

Основные компоненты клиентской части защищенного комплекса программ печати и маркировки документов устанавливаются автоматически при установке ОС.

В случае необходимости возможно вручную установить клиентскую часть комплекса, выполнив команду:

```
sudo apt install parsec-cups-client fly-admin-printer-mac
```

На компьютеры, с которых будет выполняться маркировка документов (см. 14.5), дополнительно установить следующие пакеты:

```
fly-print-station fly-admin-marker
```

Для работы клиента с сервером печати необходимо:

1) создать на компьютере клиента файл `/etc/cups/client.conf`, содержащий строку:

```
ServerName <полное_имя_хоста_сервера_печати>
```

Пример

```
ServerName cups.astra.dom
```

2) сделать данный файл доступным на чтение всем пользователям:

```
sudo chmod +r /etc/cups/client.conf
```

Если сервер печати настроен для работы в ЕПП (см. 14.3.2), то компьютер клиента должен быть введен в домен в соответствии с 8.2.8.

2.24. Подраздел «18.3. Комплекс программ Bacula»

Подраздел 18.3 изложить в следующей редакции:

Bacula — это сетевая клиент-серверная система резервного копирования и восстановления данных. Благодаря модульной архитектуре ее можно масштабировать до больших сетей, состоящих из сотен компьютеров.

Bacula состоит из следующих основных компонентов:

- Bacula Director — диспетчер. Это центральная программа, координирующая все выполняемые операции. Функционирует в фоновом режиме;
- Bacula Console — консоль Bacula. Она позволяет администратору взаимодействовать с центральной программой;
- Bacula File — клиентская программа (клиент), которая устанавливается на каждый обслуживаемый компьютер;
- Bacula Storage — хранилище данных. Программа, взаимодействующая с физическими или логическими носителями для копирования и восстановления данных;
- Bacula Catalog — программа, отвечающая за индексирование и организацию базы резервных данных.

Bacula обеспечивает сохранение расширенных атрибутов каталогов и файлов, а также их последующее восстановление при необходимости (см. РУСБ.10015-01 97 01-1).

Порядок использования Bacula описан на примере системы со следующей инфраструктурой:

- выделенный сервер для функционирования Bacula Director — главный сервер, осуществляющий резервное копирование;

- выделенный сервер для функционирования Bacula Storage — рабочая станция, на которой будут размещаться резервные копии данных;

- персональный компьютер для функционирования Bacula File — рабочая станция, с которой будут копироваться данные и на которую будут восстанавливаться резервные копии данных.

18.3.1. Настройка СУБД для Bacula

Для хранения каталога резервных копий используется СУБД. Настройку СУБД необходимо выполнить до запуска компонентов Bacula.

Для настройки необходимо выполнить следующие действия:

1) установить СУБД на сервер, где будет работать Bacula Director:

```
sudo apt install postgresql-<версия>
```

2) через менеджер пакетов Synaptic по ключевому слову «bacula» необходимо установить все пакеты, кроме тех, где в названии фигурирует «-sqlite3». При установке Bacula в появившемся окне настройки совместимости с БД снять флаг автоматической настройки и нажать **[Далее]**;

3) подготовить СУБД для работы с Bacula, выполнив следующие действия:

а) в файле `/etc/postgresql/<версия>/<кластер>/postgresql.conf` для прослушивания всех IP-адресов указать:

```
listen_addresses = '*'
```

б) в файле `/etc/postgresql/<версия>/<кластер>/pg_hba.conf` добавить узел Bacula Director с IP-адресом `11.11.11.21` и указать метод аутентификации `trust` для всех соединений:

```
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
```

ВНИМАНИЕ! Метод аутентификации `trust` рекомендуется использовать только в доверенной сети;

в) выполнить перезапуск СУБД:

```
sudo pg_ctlcluster <версия> <кластер> restart
```

г) присвоить пароль для пользователя `postgres` командой:

```
sudo passwd postgres
```

на запрос системы ввести пароль для пользователя `postgres`;

д) присвоить пароль для пользователя bacula командой:

```
sudo passwd bacula
```

на запрос системы ввести пароль для пользователя bacula;

е) запустить интерактивный терминал psql и подключиться к предустановленной БД template1 от имени пользователя postgres:

```
psql template1 postgres
```

ж) создать пользователя bacula и назначить для него пароль, а также предоставить данному пользователю административные права:

```
CREATE ROLE bacula;
ALTER USER bacula PASSWORD '<пароль_СУБД-пользователя_bacula>';
ALTER USER bacula LOGIN SUPERUSER CREATEDB CREATEROLE;
```

з) выйти из интерактивного терминала psql:

```
\q
```

4) запустить интерактивный терминал psql и подключиться к БД postgres через порт подключения, по умолчанию порт 5432:

```
psql postgres -p 5432 -U postgres
```

затем выполнить команды:

а) создать БД с именем bacula-db, задать для БД кодировку и классификацию символов, а также указать шаблон создаваемой БД:

```
CREATE DATABASE bacula-db WITH ENCODING = 'SQL_ASCII'
LC_COLLATE = 'C' LC_CTYPE = 'C' TEMPLATE = 'template0';
```

б) назначить владельцем БД bacula-db пользователя bacula:

```
ALTER DATABASE bacula-db OWNER TO bacula;
```

в) выйти из интерфейса управления psql:

```
\q
```

5) на сервере Bacula Director отредактировать сценарий создания таблиц /usr/share/bacula-director/make_postgresql_tables:

а) в строке db_name указать имя БД bacula-db:

```
db_name=bacula-db
```

б) в строке psql указать IP-адрес Bacula Director и порт подключения 5432:

```
psql -U bacula -h 11.11.11.21 -p 5432 -f - -d ${db_name}
$* <<END-OF-DATA
```

6) на сервере Bacula Director отредактировать сценарий назначения привилегий /usr/share/bacula-director/grant_postgresql_privileges:

а) в строке db_user указать имя СУБД-пользователя bacula:

```
db_user=bacula
```

б) в строке db_name указать имя БД bacula-db:

```
db_name=bacula-db
```

в) в строке db_password указать пароль СУБД-пользователя bacula:

```
db_password=<пароль_СУБД-пользователя_bacula>
```

г) в строке $bindir/psql указать СУБД-пользователя bacula, IP-адрес Bacula Director и порт подключения 5432:

```
$bindir/psql -U bacula -h 11.11.11.21 -p 5432 -f - -d
${db_name} $* <<END-OF-DATA
```

7) для корректного функционирования отредактированных сценариев:

а) предоставить пользователю postgres право чтения БД меток безопасности локальных пользователей:

```
sudo usermod -a -G shadow postgres
sudo setfacl -d -m u:postgres:r /etc/parsec/macdb /etc/parsec/capdb
sudo setfacl -R -m u:postgres:r /etc/parsec/macdb /etc/parsec/capdb
sudo setfacl -m u:postgres:rx /etc/parsec/macdb /etc/parsec/capdb
```

б) назначить метку безопасности пользователю bacula (нулевую классификационную метку, категорию целостности не назначать):

```
sudo pdpl-user bacula -l 0:0
```

Подробное описание инструмента pdpl-user приведено на справочной странице man pdpl-user;

8) выполнить сценарии для создания таблиц и назначения привилегий пользователю bacula:

```
sudo /usr/share/bacula-director/make_postgresql_tables
sudo /usr/share/bacula-director/grant_postgresql_privileges
```

При успешном создании таблиц будет выведено следующее сообщение:

```
Creation of Bacula PostgreSQL tables succeeded.
```

При успешном назначении привилегий будет выведено следующее сообщение:

```
Privileges for user bacula granted on database bacula-db.
```

18.3.2. Настройка Bacula

Для функционирования системы резервного копирования и восстановления данных необходимо настроить следующие компоненты Bacula в конфигурационных файлах:

- `/etc/bacula/bacula-dir.conf` — настройка Bacula Director;
- `/etc/bacula/bacula-sd.conf` — настройка Bacula Storage;
- `/etc/bacula/bacula-fd.conf` — настройка Bacula File;
- `/etc/bacula/bconsole.conf` — настройка Bacula Console.

Описание основных секций конфигурационных файлов и задаваемых в них параметрах приведены в таблице 58.

Таблица 58

Параметр	Описание
`Director`	Параметры конфигурации диспетчера Bacula Director. Указывается имя, пароль и IP-адрес диспетчера, а также настройки взаимодействия с другими компонентами
`JobDefs`	Шаблон задания для резервного копирования или восстановления данных. Задаются типовые параметры, которые могут быть использованы для конкретных заданий
`Job`	Параметры конкретного задания резервного копирования или восстановления данных
`Schedule`	Расписание запуска заданий
`FileSet`	Определяются каталоги и файлы, включаемые в резервную копию, а также задаются параметры их обработки, такие как алгоритмы вычисления контрольных сумм и сжатия файлов, сохранения прав доступа и т.п.
`Client`	Параметры конфигурации клиента Bacula File, с которого будет выполняться копирование данных. Указывается имя, пароль и IP-адрес клиента, а также настройки взаимодействия с другими компонентами
`Storage`	Параметры конфигурации хранилища Bacula Storage. Указывается имя, IP-адрес хранилища, максимальное количество одновременно выполняемых заданий и другие параметры
`Catalog`	Параметры подключения к базе данных, в которой хранится информация о резервных копиях
`Messages`	Настройка уведомлений о результатах выполнения заданий. Позволяет задать куда будут направляться уведомления (например, на диспетчер) и что в них будет фиксироваться (например, сведения об ошибках, предупреждениях или успешных и неуспешных действиях)
`Pool`	Настройка группы томов хранилища Bacula Storage для упорядоченного хранения резервных копий по типу данных или сроку их хранения
`Device`	Параметры устройств хранения информации. Указывается физический путь к устройству хранения, является ли носитель информации съемным и другие параметры
`Autochanger`	Настройка автосменщика носителей информации. Осуществляет виртуальную группировку устройств хранения информации для обращения к ним как к единому целому

Подробное описание всех параметров и возможных для них значений приведены в официальной документации системы резервного копирования Bacula.

При корректировке конфигурационных файлов следует задавать в секциях уникальные имена для параметра `Name`, а неиспользуемые параметры и секции рекомендуется оставить со значениями по умолчанию.

18.3.2.1. Настройка Bacula Director

Настройка Bacula Director осуществляется на сервере с IP-адресом `11.11.11.21` в конфигурационном файле `/etc/bacula/bacula-dir.conf`:

1) в секции `Director` задать значения параметров `Name`, `Password` и `DirAddress`, остальные параметры оставить со значениями по умолчанию:

```
Director {

Name = bacula-dir # имя Bacula Director

DIRport = 9101 # прослушиваемый порт

QueryFile = "/etc/bacula/scripts/query.sql" # путь к сценарию,
# содержащему SQL-запросы для работы с Bacula Catalog

WorkingDirectory = "/var/lib/bacula" # каталог, в котором хранятся
# статус-файлы Bacula Director

PidDirectory = "/run/bacula" # pid-файл службы Bacula Director

Maximum Concurrent Jobs = 1 # максимальное количество выполняемых
# заданий (не рекомендуется одновременно запускать более одного задания)

Password = "<пароль_bacula-dir>" # пароль Bacula Director

Messages = Daemon # конфигурация уведомлений из секции Messages

DirAddress = 11.11.11.21 # IP-адрес Bacula Director

}
```

2) в секции `JobDefs` задать значения параметров для шаблонного задания, параметры которого могут быть использованы другими заданиями:

```
JobDefs {

Name = "DefaultJob" # имя задания
```

```
Type = Backup # тип задания (Backup, Restore и т.д.)

Level = Incremental # уровень резервного копирования
# (Full, Incremental, Differential и т.д.)

Client =bacula-fd # имя Bacula File, заданное в bacula-fd.conf

FileSet = "Full Set" # имя набора файлов из секции FileSet

Schedule = "WeeklyCycle" # имя расписания из секции Schedule

Storage = bacula-sd # имя Bacula Storage, заданное в bacula-sd.conf

Messages = Standard # конфигурация уведомлений о выполняемых заданиях
# из секции Messages (Standard, ErrorsOnly и т.д.)

Pool = File # имя пула (группы томов) из секции Pool для записей
# резервного копирования

SpoolAttributes = yes # включена буферизация атрибутов файлов

Priority = 10 # приоритет выполнения задания
# от 1 (максимальный) до 1000 (минимальный)

Write Bootstrap = "/var/lib/bacula/%c.bsr" # файл, в котором хранится
# информация откуда извлекать данные при восстановлении

}
```

3) в секции `Storage` для настройки подключения к хранилищу Bacula Storage задать следующие значения параметров:

```
Storage {

Name = bacula-sd # имя Bacula Storage

Address = 11.11.11.22 # IP-адрес Bacula Storage

SDPort = 9103 # порт подключения

Password = "<пароль_bacula-sd>" # пароль Bacula Storage

Device = Autochanger1 # имя устройства хранения, указанное
# в файле bacula-sd.conf

Media Type = File1 # имя, которое будет использовано Bacula для
```

```
# восстановления данных

Maximum Concurrent Jobs = 1 # максимальное количество выполняемых
# заданий (не рекомендуется одновременно запускать более одного задания)

}
```

4) в секции Job, которая используется для настройки заданий резервирования файлов клиента, задать следующие параметры:

```
Job {

Name = "BackupClient1" # имя задания

JobDefs = "DefaultJob" # имя шаблонного задания

}
```

5) в секции Job, которая используется для настройки заданий резервирования файлов Bacula Catalog, задать следующие параметры:

```
Job {

Name = "BackupCatalog" # имя задания

JobDefs = "DefaultJob" # имя шаблонного задания

Level = Full # уровень резервного копирования

FileSet="Catalog" # имя для набора восстанавливаемых файлов
# из секции FileSet

Schedule = "WeeklyCycleAfterBackup" # имя расписания запуска задания
# из секции Schedule

Write Bootstrap = "/var/lib/bacula/%n.bsr" # файл с информацией откуда
# извлекать данные при восстановлении

}
```

6) в секции Job, которая используется для настройки заданий восстановления файлов клиента, задать следующие параметры:

```
Job {

Name = "RestoreFiles" # имя задания

Type = Restore # тип задания (резервирование, восстановление и т.д.)
```

```
Client=bacula-fd # имя Bacula File, заданное в bacula-fd.conf

FileSet="Full Set" # имя набора восстанавливаемых файлов
# из секции FileSet

Storage = bacula-sd # имя Bacula Storage, заданное в bacula-sd.conf

Pool = File # имя пула (группы томов) Bacula Storage, где находится
# резервная копия файлов/каталогов клиента

Messages = Standard # тип уведомлений о выполняемых заданиях

Where = /restore # путь восстановления на клиенте

}
```

7) в секции FileSet, которая используется для настройки наборов файлов и параметров для клиента, задать следующие параметры:

```
FileSet {

Name = "Full Set" # имя набора файлов

Include { # секция, содержащая пути к резервируемым файлам/каталогам

Options { # секция, определяющая параметры резервирования
# файлов/каталогов

signature = MD5 # алгоритм вычисления контрольных сумм файлов

compression = GZIP # алгоритм сжатия файлов

recurse = yes # необходимость рекурсивного резервирования

aclsupport = yes # необходимость сохранения прав, назначенным файлам
# и каталогам (например, назначенным с помощью setfacl)

xattrsupport = yes # указывает на возможность включения
# поддержки расширенных атрибутов
# (обязательный параметр для работы с метками безопасности)

}

File = /home # путь к файлам/каталогам, которые должны быть включены
# в список резервируемых
```

```
}

Exclude { # секция содержит пути к файлам/каталогам, которые необходимо
# исключить из списка резервируемых

File = /tmp

}

}
```

8) в секции `Schedule`, которая используется для настройки расписания обработки файлов при выполнении заданий клиента, задать следующие параметры:

```
Schedule {

Name = "WeeklyCycle" # имя расписания

Run = Full 1st sun at 23:05 # тип, периодичность и время запуска
# полного резервного копирования

Run = Differential 2nd-5th sun at 23:05 # тип, периодичность и время
# запуска дифференциального резервного копирования

Run = Incremental mon-sat at 23:05 # тип, периодичность и время запуска
# инкрементального резервного копирования

}
```

9) в секции `Schedule`, которая используется для настройки расписания обработки файлов при выполнении заданий для Bacula Catalog, задать следующие параметры:

```
Schedule {

Name = "WeeklyCycleAfterBackup" # имя расписания

Run = Full sun-sat at 23:10 # тип, периодичность и время запуска
# полного резервного копирования

}
```

10) в секции `FileSet`, которая используется для настройки наборов файлов и параметров для Bacula Catalog, задать следующие параметры:

```
FileSet {

Name = "Catalog" # имя Bacula Catalog
```

```
Include { # секция, содержащая пути к резервируемым файлам/каталогам

Options { # секция, определяющая параметры резервирования
# файлов/каталогов

signature = MD5 # алгоритм вычисления контрольных сумм файлов

compression = GZIP # алгоритм сжатия файлов

recurse = yes # необходимость рекурсивного резервирования

aclsupport = yes # необходимость сохранения прав, назначенным файлам
# и каталогам (например, назначенным с помощью setfacl)

xattrsupport = yes # указывает на возможность включения поддержки
# расширенных атрибутов
# (обязательный параметр для работы с метками безопасности)

}

File = "/var/lib/bacula/bacula.sql" # путь к файлам/каталогам, которые
# должны быть включены в список резервируемых

}

}
```

11) в секции `Client` для настройки клиента необходимо задать следующие параметры:

```
Client {

Name = bacula-fd # имя Bacula File

Address = 11.11.11.23 # IP-адрес Bacula File

FDPort = 9102 # порт прослушивания

Catalog = BaculaCatalog # имя Bacula Catalog, заданное в секции Catalog
# для параметра Name

Password = "<пароль_bacula-fd>" # пароль Bacula File

File Retention = 60 days # период, в течении которого информация
# о файлах хранится в БД
```

```
Job Retention = 6 months # период, в течении которого информация
# о заданиях хранится в БД

AutoPrune = yes # автоматическое удаление из БД записей о заданиях
# и файлах, срок хранения которых истек в соответствии с периодами
# параметров File Retention и Job Retention

}
```

12) в секции `Catalog` указать параметры доступа к БД, а также назначить уникальное имя данного Bacula Catalog:

```
Catalog {

Name = BaculaCatalog # имя Bacula Catalog

dbaddress = 11.11.11.21 # адрес сервера СУБД

dbport = 5432 # порт подключения на сервере

dbname = bacula-db # имя БД на сервере СУБД

dbuser = bacula # имя СУБД-пользователя

dbpassword = <пароль_СУБД-пользователя_bacula>

}
```

13) в секции `Pool`, которая используется для файлов, указать параметры группы томов хранилища Bacula Storage:

```
Pool {

Name = File # имя пула, указывается в заданиях резервного копирования

Pool Type = Backup # тип пула (например, Backup, Copy или Cloned)

Recycle = yes # возможность автоматической очистки или перезаписи тома
# пула

Volume Retention = 365 days # период, в течение которого информация
# о заданиях и файлах хранится в БД

AutoPrune = yes # автоматическое удаление из БД записей о заданиях
# и файлах, срок хранения которых истек в соответствии с периодом
# параметра Volume Retention
```

```
Maximum Volume Bytes = 50G # максимальный объем тома в пуле

Maximum Volumes = 100 # максимальное количество томов в пуле

Label Format = "Vol-" # начальные символы имен томов пула

}
```

Далее следует установить права на чтение и запись пользователю `bacula` и назначить его владельцем конфигурационного файла `bacula-dir.conf`:

```
sudo chmod 644 /etc/bacula/bacula-dir.conf
sudo chown root:bacula /etc/bacula/bacula-dir.conf
```

Чтобы настроить доступ к Bacula Console необходимо:

1) отредактировать конфигурационный файл `/etc/bacula/bconsole.conf`:

```
Director {

Name = bacula-dir # имя Bacula Director, заданное в bacula-dir.conf

DIRport = 9101 # прослушиваемый порт

address = 11.11.11.21 # IP-адрес Bacula Director

Password = "<пароль_bacula-dir>" # пароль Bacula Director

}
```

2) перезапустить Bacula Director командой:

```
sudo systemctl restart bacula-director
```

18.3.2.2. Настройка Bacula Storage

Bacula Storage отвечает за непосредственную работу с устройством хранения данных. Bacula поддерживает широкий спектр устройств от оптических дисков до ленточных библиотек. В описываемой конфигурации используется следующий вариант — жесткий диск с файловой системой ext3.

Настройка Bacula Storage осуществляется на сервере с IP-адресом `11.11.11.22` в конфигурационном файле `/etc/bacula/bacula-sd.conf`, для этого необходимо:

1) указать основные параметры хранилища:

```
Storage {

Name = bacula-sd # имя Bacula Storage

SDPort = 9103 # прослушиваемый порт

WorkingDirectory = "/var/lib/bacula" # каталог, в котором хранятся
# статус-файлы Bacula Storage

Pid Directory = "/run/bacula" # pid-файл службы Bacula

Maximum Concurrent Jobs = 1 # максимальное количество выполняемых
# заданий (не рекомендуется одновременно запускать более одного задания)

SDAddress = 11.11.11.22 # IP-адрес Bacula Storage

}
```

2) для подключения диспетчера к хранилищу указать следующие параметры:

```
Director {

Name = bacula-dir # имя Bacula Director, которому разрешено
# подключаться к Bacula Storage

Password = "<пароль_bacula-sd>" # пароль Bacula Storage

}
```

3) для настройки автосменщика носителей информации (виртуальной группировки устройств хранения, входящих в одну библиотеку, и обращения к ним как к единому целому) настроить параметры в секции `Autochanger`:

```
Autochanger {

Name = Autochanger1 # имя автосменщика

Device = FileChgr1-Dev1, FileChgr1-Dev2 # имена устройств хранения,
# относящихся к автосменщику

Changer Command = "" # при виртуальной группировки устройств хранения
# значение не требуется

Changer Device = /dev/null # значение при использовании виртуальной
# группировки устройств хранения

}
```

4) для устройств хранения FileChgr1-Dev1 и FileChgr1-Dev2 создать соответственно каталоги files1 и files2, назначить владельцем пользователя bacula и предоставить ему полный доступ:

```
sudo mkdir -p /backups/files1/
sudo chmod 755 /backups/files1/
sudo chown bacula:bacula /backups/files1/

sudo mkdir -p /backups/files2/
sudo chmod 755 /backups/files2/
sudo chown bacula:bacula /backups/files2/
```

5) в конфигурационном файле /etc/bacula/bacula-sd.conf задать параметры устройств хранения FileChgr1-Dev1 и FileChgr1-Dev2, а также настроить уведомления для хранилища:

```
Device {

Name = FileChgr1-Dev1 # имя устройства хранения

Media Type = File1 # логический тип носителя

Archive Device = /backups/files1 # путь к каталогу, в котором будут
# размещаться резервные копии

LabelMedia = yes # автоматическая разметка новых томов

Random Access = Yes # возможность доступа к данным в непоследовательном
# (произвольном) порядке

AutomaticMount = yes # поддержка автоматического монтирования

RemovableMedia = no # физическое извлечение устройства хранения
# (при наличии устройства)

AlwaysOpen = no # состояние открытия устройства хранения
# (yes - устройство открыто всегда, no - устройство открывается
# при выполнении задания)

Maximum Concurrent Jobs = 1 # максимальное количество выполняемых
# заданий (не рекомендуется одновременно запускать более одного задания)

}

Device {
```

```
Name = FileChgr1-Dev2 # имя устройства хранения

Media Type = File1 # логический тип носителя

Archive Device = /backups/files2 # путь к каталогу, в котором будут
# размещаться резервные копии

LabelMedia = yes # автоматическая разметка новых томов

Random Access = Yes # возможность доступа к данным в непоследовательном
# (произвольном) порядке

AutomaticMount = yes # поддержка автоматического монтирования

RemovableMedia = no # физическое извлечение устройства хранения
# (при наличии устройства)

AlwaysOpen = no # состояние открытия устройства хранения
# (yes - устройство открыто всегда, no - устройство открывается при
# выполнении задания)

Maximum Concurrent Jobs = 1 # максимальное количество выполняемых
# заданий (не рекомендуется одновременно запускать более одного задания)

}

Messages {

Name = Standard # имя шаблона уведомлений для заданий

director = bacula-dir = all # все уведомления будут направлены
# на Bacula Director

}
```

6) установить права на чтение и запись пользователю `bacula` и назначить его владельцем конфигурационного файла `bacula-sd.conf`:

```
sudo chmod 644 /etc/bacula/bacula-sd.conf
sudo chown root:bacula /etc/bacula/bacula-sd.conf
```

7) перезапустить Bacula Storage командой:

```
sudo systemctl restart bacula-sd
```

18.3.2.3. Настройка Bacula File

Настройка Bacula File (клиента) осуществляется на рабочей станции с IP-адресом 11.11.11.23 в конфигурационном файле /etc/bacula/bacula-fd.conf, для этого необходимо:

1) в секции Director настроить возможность подключения диспетчера к клиенту:

```
Director {

Name = bacula-dir # имя Bacula Director, которому разрешено
подключаться к Bacula File

Password = "<пароль_bacula-fd>" # пароль Bacula File

}
```

2) в секции FileDaemon указать основные параметры клиента:

```
FileDaemon {

Name = bacula-fd # имя Bacula File

FDport = 9102 # прослушиваемый порт

WorkingDirectory = /var/lib/bacula # каталог, в котором хранятся
# статус-файлы Bacula File

Pid Directory = /run/bacula # pid-файл службы Bacula File

Maximum Concurrent Jobs = 1 # максимальное количество выполняемых
# заданий (не рекомендуется одновременно запускать более одного задания)

Plugin Directory = /usr/lib/bacula # каталог хранения подключаемых
# расширений для дополнительной функциональности
# (например, использование внешних сценариев)

FDAddress = 11.11.11.23 # IP-адрес Bacula File

}
```

3) в секции Messages для настройки уведомлений клиента установить следующие параметры:

```
Messages {

Name = Standard # имя шаблона уведомлений для заданий

director = bacula-dir = all # все уведомления будут направлены
```

```
# на Bacula Director

}
```

4) установить права на чтение и запись пользователю `bacula` и назначить его владельцем конфигурационного файла `bacula-fd.conf`:

```
sudo chmod 644 /etc/bacula/bacula-fd.conf
sudo chown root:bacula /etc/bacula/bacula-fd.conf
```

5) перезапустить Bacula File командой:

```
sudo systemctl restart bacula-fd
```

18.3.2.4. Проверка работоспособности Bacula

Для проверки работоспособности компонентов Bacula необходимо:

1) на сервере Bacula Director с IP-адресом `11.11.11.21` выполнить команду для входа в консоль:

```
sudo bconsole
```

2) при корректной настройке всех компонентов будет открыта консоль Bacula. Для вывода диалогового сообщения с возможностью проверки статуса одного или всех компонентов необходимо ввести следующую команду:

```
status
```

3) ввести цифру от 1 до 6, где:
   - 1 — статус Bacula Director;
   - 2 — статус Bacula Storage;
   - 3 — статус Bacula Client;
   - 4 — статус связи компонентов Bacula;
   - 6 — статус всех компонентов;

4) выход из консоли осуществляется следующей командой:

```
exit
```

18.3.2.5. Резервное копирование данных

Для создания резервной копии необходимо:

1) на сервере Bacula Director с IP-адресом `11.11.11.21` выполнить команду для входа в консоль:

```
sudo bconsole
```

2) в консоли выполнить команду для запуска задания резервного копирования:

```
run
```

3) в отобразившемся меню выбрать задание, нажав необходимую цифру на клавиатуре (например, «1»):

```
Select Job resource (1-3): 1
```

4) после вывода списка параметров задания необходимо указать вариант продолжения работы (`yes` — выполнить задание, `no` — отменить задание, `mod` — изменить параметры задания):

```
OK to run? (yes/mod/no): yes
```

5) для проверки уведомления о выполнении задания ввести команду:

```
messages
```

В случае успешного выполнения задания будет выведено сообщение со строкой:

```
Termination: Backup OK
```

18.3.2.6. Восстановление данных из резервной копии

Для восстановление данных из резервной копии необходимо:

1) на сервере Bacula Director с IP-адресом `11.11.11.21` выполнить команду для входа в консоль:

```
sudo bconsole
```

2) в консоли выполнить команду для инициализации восстановления данных и выбора режима восстановления:

```
restore
```

3) в отобразившемся меню выбрать пункт `3` для ввода задания:

```
Select item: (1-13): 3
```

4) ввести идентификатор нужного задания или несколько идентификаторов нужных заданий, разделенных запятой:

```
Enter JobId(s), comma separated to restore: 10,11,12
```

5) указать параметр маркировки и определить, что необходимо восстановить. Например, для восстановления всех файлов в задании:

```
mark *
```

6) подтвердить выполнение командой:

```
done
```

7) после вывода информации о файлах, выбранных для восстановления, необходимо указать вариант продолжения работы (`yes` — выполнить задание, `no` — отменить задание, `mod` — изменить параметры задания):

```
OK to run? (yes/mod/no): yes
```

8) для проверки уведомления о восстановлении данных ввести команду:

```
messages
```

В случае успешного восстановления данных будет выведено сообщение со строкой:

```
Termination: Restore OK
```

Данные из резервной копии будут восстановлены в каталоге `/restore` на рабочей станции с Bacula File.

Также управление Bacula возможно с помощью графической утилиты `bacula-console-qt`.

2.25. Раздел «19. Контроль подключаемых устройств»

Раздел 19 изложить в следующей редакции:

В состав ОС входит средство контроля подключения устройств (СКПУ). Механизм работы СКПУ основан на правилах `udev`. Подробное описание правил `udev` приведено на справочной странице `man udev`.

СКПУ обеспечивает контроль подключения к шине USB различных устройств (сканеры, съемные накопители, видеокамеры и т.п.). Для таких устройств в СКПУ можно подготовить следующие типы правил:

1) блокирующее — устанавливает запрет на использование устройства;
2) разрешающее — устанавливает разрешение на использование устройства;
3) назначающее правило — устанавливает разрешение на использование устройства и назначает права доступа, правила регистрации событий и метку безопасности. Назначающие правила можно подготовить только для следующих типов устройств:
   - носители информации или устройства для их считывания (flash-накопители, SD-карты, внешние HDD/SSD, floppy-привод, оптический привод и т.д.);
   - устройства, для взаимодействия с которыми используется протокол MTP (цифровые фотокамеры, смартфоны, электронные книги и т.д.);
   - аудиоустройства (микрофоны, колонки, переходники USB/Jack и т.д.);
   - видеоустройства (веб-камеры, адаптеры видеозахвата и т.д.).

В СКПУ можно подготовить блокирующие и разрешающие правила для группы устройств определенного типа. Для многосоставных устройств, в которых объединены устройства различных типов (например, веб-камера с интегрированным микрофоном), можно включить режим усиленной блокировки (см. 19.4.4).

В ОС каждому разделу съемного накопителя соответствует отдельный файл устройства. При этом не допускается создавать отдельные правила для съемного накопителя и для

его раздела. Если на съемном накопителе находится несколько разделов, то правило СКПУ будет применено ко всем разделам на этом накопителе. При подготовке съемного накопителя к использованию в ОС рекомендуется руководствоваться принципом «одно устройство — один дисковый раздел».

Для управления правилами и непосредственно механизмом работы СКПУ используется инструмент командной строки `pdac-adm`. С помощью этого инструмента можно:

1) вывести перечень подключенных устройств и их статус, а также идентификационные параметры. Кроме того, можно вывести правила классификации, по которым определяется тип устройства (подробнее см. 19.1);
2) добавить, изменить или удалить правило СКПУ (см. 19.2);
3) запустить генерацию правил `udev` на основе правил СКПУ (см. 19.3);
4) выключить или включить СКПУ, а также управлять режимами его работы (см. 19.4).

19.1. Информация об устройствах и их типах

19.1.1. Идентификационные параметры устройств

При создании правил используются следующие идентификационные параметры устройств:

1) `serial` — серийный номер;
2) `model` — идентификатор модели;
3) `vendor` — идентификатор производителя;
4) `dev` — путь к файлу устройства, который размещен в каталоге `/dev/`. Используется для удобства добавления правил СКПУ. При сохранении правила будет автоматически заменен на серийный номер устройства.

Примечание. Определить значения идентификационных параметров устройств, которые подключены в ОС, можно с помощью инструмента `pdac-adm` (см. 19.1.2).

Для указания типа устройств применяется идентификационный параметр `type`, который принимает одно из следующих значений:

1) `storage` — носители информации, устройства для их считывания;
2) `printer` — принтеры, сканеры, МФУ;
3) `security_cardreader` — устройства безопасности, считыватели карт, токены;
4) `image_mtp` — устройства, для взаимодействия с которыми используется протокол MTP;
5) `audio` — аудиоустройства;
6) `video` — видеоустройства;
7) `communication` — устройства связи (LAN-адаптеры, WIFI-антенны и т.д.);
8) `hub` — хабы, переходники;

9) `hid` — интерфейсные устройства (клавиатуры, мыши, беспроводные ресиверы, MIDI-клавиатуры и т.д.);

10) `other` — прочие устройства (персональные медицинские устройства, микроконтроллеры и другие специфические устройства).

В СКПУ можно подготовить блокирующие и разрешающие правила для группы устройств одного типа.

Также в СКПУ применяется идентификационный параметр `bus`, для которого обязательно нужно указать значение `usb`. Этот параметр используется для подготовки блокирующего или разрешающего правила для шины USB.

При подключении устройства в ОС производится автоматическое определение его типа и наименование шины подключения. Для этого используются специальные правила классификации. Изменение этих правил не предусмотрено.

Для просмотра правил классификации выполнить команду:

```
sudo pdac-adm classification [параметры]
```

Описание параметров приведено в таблице 61.

Таблица 61

Параметр	Описание
`types`	Вывести правила классификации, по которым определяется тип устройства. При выполнении команды без параметров `types` и `buses` будет выведен перечень всех правил классификации
`buses`	Вывести правило классификации, по которому определяется наименование шины подключения. При выполнении команды без параметров `types` и `buses` будет выведен перечень всех правил классификации
`-H`, `--no-headers`	При выводе не отображать заголовки столбцов
`-J`, `--json`	Выводить информацию в формате JSON

19.1.2. Вывод информации об устройствах

Для вывода информации об устройствах, которые подключены в ОС, выполнить команду:

```
sudo pdac-adm devices [параметры]
```

Описание параметров приведено в таблице 62.

Таблица 62

Параметр	Описание
`tree`	Вывести перечень устройств в соответствии с порядком их подключения. При выполнении команды без параметра `tree` будет выведен перечень, в котором устройства сгруппированы по типам и шинам, к которым эти устройства подключены. Примечание. Одновременное использование параметров `tree` и `-e` не допускается
`-a`, `--all`	Дополнительно вывести информацию о всех составных частях устройств, для которых в СКПУ можно подготовить правила. Например, если у USB-накопителя `/dev/sdb` имеется раздел `/dev/sdb1`, то также будет выведена информация об этом разделе
`-H`, `--no-headers`	При выводе не отображать заголовки столбцов
`-J`, `--json`	Выводить информацию в формате JSON
`-V`, `--verbose`	Выводить подробную информацию

Примечание. Для действия `devices` допускается любой из вариантов укороченной записи: `device`, `devic`, `devi` или `dev`.

При выполнении команды без параметра `tree` будет выведена таблица, состоящая из следующих столбцов:

1) `BUS/TYPE/DEVICE` — наименование шины, типа устройств или экземпляра устройства;

2) `STATUS` — статус устройства, установленный в соответствии с правилами udev. Может принимать одно из следующих значений:

   а) `allowed` — использование устройства разрешено;

   б) `blocked` — использование устройства запрещено;

3) `INHERITED` — порядок присвоения статуса. Может принимать одно из следующих значений:

   а) `by bus` — статус был унаследован от шины;

   б) `by type` — статус был унаследован от типа устройств;

   в) `by rule` — статус установлен в соответствии с правилом;

4) `IDENTIFICATION` — значения идентификационных параметров.

При выполнении команды с параметром `tree` в таблице после столбца `INHERITED` будут дополнительно выведены следующие столбцы:

1) `TYPE` — тип устройства;

2) `BUS` — наименование шины, к которой подключено устройство.

Примечание. Будут выведены только устройства, для которых был автоматически определен их тип по правилам классификации (см. 19.1.1)

.

Примеры:

1. Пример вывода команды без параметра `tree`:

```
BUS/TYPE/DEVICE                                          STATUS  INHERITED
IDENTIFICATION
Устройства интерфейса USB (usb)                          allowed
bus=usb
Носители информации (storage)                            allowed
bus=usb,type=storage
JetFlash (Transcend Information, Inc.)                   allowed
serial=06ZC7LCZYRBQNCDY,vendor=8564,model=1000,dev=/dev/bus/usb/001~
Устройства безопасности, считыватели карт (security_~ allowed
bus=usb,type=security_cardreader
58200 (Broadcom Corp.)                                   allowed
serial=0123456789ABCD,vendor=0a5c,model=5842,dev=/dev/bus/usb/001/0~
Видеоустройства (video)                                  allowed
bus=usb,type=video
Integrated_Webcam_HD (Microdia)                          allowed
serial=CN0XYXJ28LG0028JAFM3A00_Integrated_Webcam_HD,vendor=0c45,mod~
Хабы, переходники (hub)                                  allowed
bus=usb,type=hub
2.0 root hub (Linux Foundation)                          allowed
serial=0000:00:0d.0,vendor=1d6b,model=0002,dev=/dev/bus/usb/003/001
3.0 root hub (Linux Foundation)                          allowed
serial=0000:00:0d.0,vendor=1d6b,model=0003,dev=/dev/bus/usb/004/001
4-Port_USB_3.0_Hub (Realtek Semiconductor Corp.)         allowed
serial=Generic_4-Port_USB_3.0_Hub,vendor=0bda,model=0423,dev=/dev/~
2.0 root hub (Linux Foundation)                          allowed
serial=0000:00:14.0,vendor=1d6b,model=0002,dev=/dev/bus/usb/001/001
4-Port_USB_2.0_Hub (Realtek Semiconductor Corp.)         allowed
serial=Generic_4-Port_USB_2.0_Hub,vendor=0bda,model=5423,dev=/dev/~
3.0 root hub (Linux Foundation)                          allowed
serial=0000:00:14.0,vendor=1d6b,model=0003,dev=/dev/bus/usb/002/001
2.0 root hub (Linux Foundation)                          allowed
serial=vhci_hcd.0,vendor=1d6b,model=0002,dev=/dev/bus/usb/005/001
3.0 root hub (Linux Foundation)                          allowed
serial=vhci_hcd.0,vendor=1d6b,model=0003,dev=/dev/bus/usb/006/001
Интерфейсные устройства (hid)                            allowed
```

```
bus=usb,type=hid
Unifying Receiver (Logitech, Inc.)                    allowed
serial=Logitech_USB_Receiver,vendor=046d,model=c534,dev=/dev/bus/~
Прочие устройства (other)                               allowed
bus=usb,type=other
D-Link_DWA-160_Xtreme_N_Dual_Band_USB_Adapter_rev.~ allowed
serial=20130629,vendor=2001,model=3c21,dev=/dev/bus/usb/001/009
```

2. Пример вывода команды с параметром `tree`:

```
BUS/TYPE/DEVICE                                          STATUS  INHERITED
TYPE           BUS  IDENTIFICATION
2.0 root hub (Linux Foundation)                          allowed
hub            usb  serial=0000:00:0d.0,vendor=1d6b,model=0002,de~
3.0 root hub (Linux Foundation)                          allowed
hub            usb  serial=0000:00:0d.0,vendor=1d6b,model=0003,de~
4-Port_USB_3.0_Hub (Realtek Semiconductor Corp.)     allowed
hub            usb  serial=Generic_4-Port_USB_3.0_Hub,vendor=0bda~
2.0 root hub (Linux Foundation)                          allowed
hub            usb  serial=0000:00:14.0,vendor=1d6b,model=0002,de~
58200 (Broadcom Corp.)                                   allowed
security_card~ usb  serial=0123456789ABCD,vendor=0a5c,model=5842,~
Integrated_Webcam_HD (Microdia)                          allowed
video          usb  serial=CN0XYXJ28LG0028JAFM3A00_Integrated_Web~
4-Port_USB_2.0_Hub (Realtek Semiconductor Corp.)     allowed
hub            usb  serial=Generic_4-Port_USB_2.0_Hub,vendor=0bda~
JetFlash (Transcend Information, Inc.)               allowed
storage        usb  serial=06ZC7LCZYRBQNCDY,vendor=8564,model=100~
Unifying Receiver (Logitech, Inc.)                   allowed
hid            usb  serial=Logitech_USB_Receiver,vendor=046d,mode~
D-Link_DWA-160_Xtreme_N_Dual_Band_USB_Adapter_rev.C~ allowed
other          usb  serial=20130629,vendor=2001,model=3c21,dev=/d~
3.0 root hub (Linux Foundation)                          allowed
hub            usb  serial=0000:00:14.0,vendor=1d6b,model=0003,de~
2.0 root hub (Linux Foundation)                          allowed
hub            usb  serial=vhci_hcd.0,vendor=1d6b,model=0002,dev=~
3.0 root hub (Linux Foundation)                          allowed
hub            usb  serial=vhci_hcd.0,vendor=1d6b,model=0003,dev=~
```

19.2. Управление правилами СКПУ

19.2.1. Наследование и приоритет правил

В СКПУ установлена следующая иерархия объектов контроля (сущностей, для которых можно подготовить правило):

1) шина, к которой может быть подключено устройство;
2) тип устройства;
3) экземпляр устройства.

Правила наследуются сверху вниз в соответствии с иерархией. При этом чем ниже ступень иерархии, тем выше приоритет применения правила.

Пример

Для запрета использовать любые носители информации, кроме одного разрешенного USB-накопителя, требуется добавить одно блокирующее правило для устройств типа `storage` и одно разрешающее правило для конкретного экземпляра USB-накопителя.

19.2.2. Синтаксис правила СКПУ

В СКПУ можно подготовить правила только для тех устройств, для которых может быть автоматически определен их тип по правилам классификации (см. 19.1.1).

Используется следующий синтаксис правил:

```
[параметры_правила],<тип_правила>,<идентификационные_параметры>,
[параметры_доступа]
```

где `[параметры_правила]` — дополнительные параметры правила, которые перечисляются через запятую в формате `<параметр>=<значение>`. Для правила могут быть заданы значения следующих параметров:

1) `name` — наименование правила. Если параметр не указан, то правилу будет присвоено наименование вида `<тип_устройства>_<идентификационные_параметры>_<тип_правила>`.
Примечание. Если в правиле указаны идентификационные параметры конкретного экземпляра устройства, то вместо префикса <тип_устройства> используется условное наименование `device`;

2) `active` — флаг применимости (активности). Может принимать одно из следующих значений:

а) `true` — правило активно, т.е. правило будет применено при подключении устройства;

б) `false` — правило не активно, т.е. правило не будет применено при подключении устройства. Если параметр не указан, то параметру будет присвоено значение `true`;

3) desc — описание правила. Если параметр не задан, то у правила не будет описания;

<тип_правила> — тип правила, может принимать одно из следующих значений:

1) allow — разрешающее или назначающее. Для назначающего правила необходимо дополнительно задать [параметры_доступа];

2) block — блокирующее;

<идентификационные_параметры> — идентификационные параметры (см. 19.1.1), которые перечисляются через запятую в формате <параметр>=<значение>;

[параметры_доступа] — параметры доступа для устройства, которые необходимо указать в назначающем правиле. Параметры доступа перечисляются через запятую в формате <параметр>=<значение>. Допускается не задавать значения для всех параметров доступа. В этом случае будут установлены значения по умолчанию. В набор включены следующие параметры доступа:

1) owner — имя пользователя, который будет назначен пользователем-владельцем. Значение по умолчанию root;

2) group — наименование группы пользователей, которая будет назначена группой-владельцем. Значение по умолчанию root;

3) mode — набор прав доступа (в формате строки из трех восьмеричных цифр). Значение по умолчанию 660;

4) audit — флаги аудита. Значение по умолчанию 0x0:0x0;

5) pdpl — метка безопасности. Значение по умолчанию 0:0:0x0:0x0!.

ВНИМАНИЕ! Параметры доступа назначаются комплексно. Если в правиле СКПУ указан хотя бы один параметр доступа, то для остальных параметров будут заданы значения, установленные по умолчанию в СКПУ.

Примечания:

1. Назначающие правила можно подготовить только для следующих типов устройств:

а) storage (носители информации, устройства для их считывания);

б) image_mtp (устройства, для взаимодействия с которыми используется протокол MTP);

в) audio (аудиоустройства);

г) video (видеоустройства).

2. Если [параметры_доступа] в правиле не заданы, то монтирование ФС блочных устройств будет выполняться по правилам, которые описаны в 19.6.

3. Мандатное управление доступом к устройствам реализуется только на уровне защищенности «Смоленск» при включенном мандатном управлении доступом. В правилах, применяемых на уровне защищенности, отличном от «Смоленск», в метке безопасности должен быть задан нулевой уровень конфиденциальности и должны отсутствовать категории конфиденциальности.

Примеры:

1. Разрешающее правило для устройства с идентификатором производителя `152d` и идентификатором модели `0580`:

```
allow,vendor=152d,model=0580
```

2. Назначающее правило для USB-накопителя с серийным номером `DD564198838FA`:

```
allow,serial=DD564198838FA,owner=astra
```

В представленном примере при подключении в ОС устройству будут назначены следующие значения параметров доступа:

а) пользователь-владелец `astra`;

б) группа-владелец `root` (значение по умолчанию);

в) набор прав доступа `660` (значение по умолчанию);

г) флаги аудита `0x0:0x0` (значение по умолчанию);

д) метка безопасности `0:0:0x0:0x0!` (значение по умолчанию).

3. Правило с наименованием `dev_2` и описанием «`flashdisk-2`», разрешающее использование устройства, для которого был создан файл `/dev/sdb1`:

```
name=dev_2,desc="flashdisk-2",allow,dev=/dev/sdb1
```

Примечание. В процессе сохранения этого правила идентификационный параметр `dev` будет автоматически заменен на `serial`.

19.2.3. Добавление правила СКПУ

Для добавления нового правила применяется следующая команда:

```
sudo pdac-adm rules add <правило>
```

где <правило> — правило подключения устройства (см. 19.2.2).

Примечание. Для действия rules допускается любой из вариантов укороченной записи: rule или rul.

ВНИМАНИЕ! Запрещается создавать несколько правил, в которых указаны одни и те же идентификационные параметры.

19.2.4. Просмотр правил СКПУ

Для просмотра правил СКПУ применяется следующая команда:

```
sudo pdac-adm rules
```

Примечание. Для действия rules допускается любой из вариантов укороченной записи: rule или rul.

Будет выведена таблица, состоящая из следующих столбцов:

1) TYPE — тип правила (см. 19.2.2);

2) ACTIVE — флаг применимости (активности), может принимать одно из следующих значений:

   а) yes — правило активно, т.е. правило будет применено при подключении устройства;

   б) no — правило не активно, т.е. правило не будет применено при подключении устройства;

3) NAME — наименование правила;

4) EXPRESSIONS — идентификационные параметры устройства (см. 19.1.1), которые перечислены через запятую в формате <параметр>==<значение>;

5) ASSIGNATIONS — параметры доступа (см. 19.2.2), которые перечислены через запятую в формате <параметр>==<значение>;

6) DESCRIPTION — описание правила.

Пример

Вывод после выполнения команды:

```
TYPE  ACTIVE   NAME              EXPRESSIONS
ASSIGNATIONS     DESCRIPTION
allow yes      device_152d_05~   vendor==152d,model==0580
allow yes      device_DD56419~   serial==DD564198838FA
pdpl=0:0:0x0:0x0!,audit=0x0:0x0,rights=astra,root~
allow yes      dev_2             serial==E5B92A75EAE94DB4
```

```
flashdisk-2
```

Правила СКПУ хранятся в файле `/etc/parsec/PDAC/devices.cfg`.

Примечание. Если в правиле заданы значения параметров доступа, то в файле `/etc/parsec/PDAC/devices.cfg` для параметра `type` (тип правила) будет указано значение `by_rule` (назначающее правило).

Пример

Содержание файла /etc/parsec/PDAC/devices.cfg:

```
device_152d_0580_allow :
{
type = "allow";
enabled = true;
description = "";
expressions = ( "vendor==152d", "model==0580" );
};
device_DD564198838FA_allow :
{
type = "by_rule";
enabled = true;
description = "";
expressions = ( "serial==DD564198838FA" );
user = "astra";
group = "root";
mode = "660";
pdpl = "0:0:0x0:0x0!";
audit = "0x0:0x0";
};
dev_2 :
{
type = "allow";
enabled = true;
description = "flashdisk-2";
expressions = ( "serial==E5B92A75EAE94DB4" );
};
```

19.2.5. Изменение правила СКПУ

Допускается изменить значения параметров правила, а также добавить, изменить и удалить параметры доступа.

ВНИМАНИЕ! Изменение наименование правила и идентификационных параметров устройства не предусмотрено. Вместо этого необходимо удалить правило, а затем создать новое.

Для изменения имеющегося правила применяется следующая команда:

```
sudo pdac-adm rules modify <имя_правила> [тип_правила],[параметры_правила],
[параметры_доступа]
```

где <имя_правила> — наименование правила. Если при добавлении правила не было задано его наименование, то по умолчанию правилу было присвоено наименование вида <тип_устройства>_<идентификационные_параметры>_<тип_правила>
Примечание. Если в правиле указаны идентификационные параметры конкретного экземпляра устройства, то вместо префикса <тип_устройства> используется условное наименование device;

[тип_правила] — тип, который требуется назначить правилу.
ВНИМАНИЕ! При изменении типа правила его наименование не меняется. Например, если для разрешающего правила device_DD564198838FA_allow заменить его тип на блокирующее, то в наименовании этого правила по-прежнему будет суффикс allow;

[параметры_правила] — новые значения параметров правила (флаг применимости и описание). Параметры доступа перечисляются через запятую в формате <параметр>=<значение>. Указываются только те параметры доступа, значения которых требуется изменить;

[параметры_доступа] — новые значения параметров доступа. Параметры доступа перечисляются через запятую в формате <параметр>=<значение>. Указываются только те параметры доступа, значения которых требуется изменить. Если для какого-то параметра требуется установить значение по умолчанию, то для такого параметра необходимо задать пустое значение.

Примечания:

1. Для действия rules допускается любой из вариантов укороченной записи: rule или rul.
2. Для ключа modify допускается любой из вариантов укороченной записи: modif, modi или mod.

Если при подготовке правила не были указаны параметры доступа, то их можно добавить.

ВНИМАНИЕ! Параметры доступа назначаются комплексно. Если в правиле СКПУ указан хотя бы один параметр доступа, то для остальных параметров будут заданы значения, установленные по умолчанию в СКПУ (см. 19.2.2).

Пример

В правило dev_2 добавить параметры доступа:

1) пользователь-владелец astra;
2) группа-владелец astra;
3) набор прав доступа 770;
4) флаги аудита 0x0:0x0 (значение по умолчанию);
5) метка безопасности 0:0:0x0:0x0! (значение по умолчанию).

Команда изменения правила:

```
sudo pdac-adm rules modify dev_2 owner=astra,mode=770,group=astra
```

Т.к. для параметров audit и pdpl необходимо задать значения, которые используются по умолчанию, то в команде они не указаны.

Если в правиле нужно изменить параметры доступа, то в команде следует указать один или несколько параметров с новыми значениями. Если параметр не указан в команде, то он останется без изменений.

Примеры:

1. В правиле dev_2 изменить флаги аудита и метку безопасности:

```
sudo pdac-adm rules modify dev_2 audit=0x21:0x21,pdpl=1:0:0x0:0x0!
```

2. В правиле dev_2 задать следующие значения параметров доступа:
   а) пользователь-владелец flashowner;
   б) группа-владелец users;
   в) набор прав доступа 640;
   г) флаги аудита 0xa1:0x21;
   д) метка безопасности 1:0:0x2:0x0!.

Команда изменения правила:

```
sudo pdac-adm rules modify dev_2 owner=flashowner,group=users,mode=640,\
audit=0xa1:0x21,pdpl=1:0:0x2:0x0!
```

Если в правиле для каких-либо параметров доступа нужно установить значение по умолчанию, то для этих параметров, но не для всех одновременно, задать пустые значения.

Примеры:

1. В правиле dev_2 для группы-владельца установить значение по умолчанию (root):

```
sudo pdac-adm rules modify dev_2 group=
```

2. В правиле dev_2 установить значения по умолчанию для флагов аудита (0x0:0x0) и метки безопасности (0:0:0x0:0x0!):

```
sudo pdac-adm rules modify dev_2 audit=,pdpl=
```

Если в правиле нужно удалить все параметры доступа, то для всех параметров доступа одновременно задать пустые значения.

Пример

В правиле dev_2 удалить все параметры доступа:

```
sudo pdac-adm rules modify dev_2 owner=,group=,mode=,audit=,pdpl=
```

Примечание. Если в правиле не заданы параметры доступа, то монтирование ФС блочных устройств будет выполняться по правилам, которые описаны в 19.6.

Правило можно временно выключить (деактивировать). В этом случае правило не будет применено при подключении устройства.

Пример

Временно выключить правило dev_2 и изменить его описание:

```
sudo pdac-adm rules modify dev_2 active=false,desc="временно выключено"
```

19.2.6. Удаление правил СКПУ

19.2.6.1. Удаление правила с заданным наименованием

Для удаления правила СКПУ применяется следующая команда:

```
sudo pdac-adm rules delete <имя_правила>
```

где <имя_правила> — наименование правила. Если при добавлении правила не было задано его наименование, то по умолчанию правилу было присвоено наименование вида <тип_устройства>_<идентификационные_параметры>_<тип_правила>

Примечание. Если в правиле указаны идентификационные параметры конкретного экземпляра устройства, то вместо префикса <тип_устройства> используется условное наименование device.

Примечания:

1. Для действия rules допускается любой из вариантов укороченной записи: rule или rul.
2. Для ключа delete допускается любой из вариантов укороченной записи: delet, dele или del.

Пример

Удалить правило с наименованием dev_2:

```
sudo pdac-adm rules delete dev_2
```

19.2.6.2. Удаление правила с заданными значениями параметров

В СКПУ можно удалить правило, в котором один или несколько параметров имеют указанные значения. Для этого применяется команда:

```
sudo pdac-adm rules delete <параметр>=<значение>[,<параметр>=<значение>]
```

Примечания:

1. Для действия rules допускается любой из вариантов укороченной записи: rule или rul.
2. Для ключа delete допускается любой из вариантов укороченной записи: delet, dele или del.

Пример

Удалить правило для устройства с серийным номером 234567890126:

```
sudo pdac-adm rules delete serial=234567890126
```

С помощью этой команды можно удалить только одно правило. Если указанные значения параметров содержатся в нескольких правилах, то в выводе команды будет отображено предупреждение и список правил, который соответствует указанным параметрам:

```
pdac-adm: deleting multiple rules is prohibited: <перчень_правил>
```

В случае если требуется одновременно удалить нескольких правил, то в команде необходимо указать параметр `--force` или `-f`. Рекомендуется предварительно выполнить команду без этого параметра, чтобы просмотреть перечень правил, которые будут удалены.

Пример

Удалить все активные правила, в которых пользователем-владельцем назначается `astra`:

```
sudo pdac-adm rules delete active=true,user=astra --force
```

19.3. Применение правил в ОС

Чтобы правила СКПУ начали применяться в ОС, необходимо на их основе сгенерировать правила `udev`. Генерацию правил `udev` требуется выполнять после любых действий с правилами в СКПУ — создание, удаление или изменение.

Для генерации правил `udev` на основе правил СКПУ выполнить команду:

```
sudo pdac-adm commit
```

или

```
sudo pdac-adm generate
```

Если к компьютеру были подключены какие-либо устройства, то для применения сгенерированных правил требуется переподключить эти устройства или выполнить команду:

```
sudo udevadm trigger
```

Также правила будут применены после перезагрузки ОС.

19.4. Управление СКПУ

С помощью инструмента `pdac-adm` можно:

1) включить или выключить СКПУ (см. 19.4.1);

2) включить или выключить регистрацию событий, связанных с контролем подключения устройств (см. 19.4.2);

3) включить или выключить режим защиты критически важных устройств (см. 19.4.3);

4) включить или выключить режим усиленной блокировки многосоставных устройств (см. 19.4.4).

Для вывода справки инструмента `pdac-adm` выполнить команду:

```
sudo pdac-adm --help
```

Примечание. Для параметра `-help` допускается укороченная запись `-h`.

Для вывода информации о версии инструмента pdac-adm выполнить команду:

```
sudo pdac-adm --version
```

Примечание. Для параметра `-version` допускается укороченная запись `-v`.

19.4.1. Включение и выключение СКПУ

По умолчанию СКПУ включено. При этом при подключении устройств применяются системные правила `udev`, созданные при установке пакета `systemd`, или пользовательские правила `udev`, подготовленные с помощью других средств.

Для включения и выключения СКПУ используется следующая команда:

```
sudo pdac-adm state [enable|disable]
```

или

```
sudo pdac-adm status [enable|disable]
```

Выполнение команды без указания параметра отображает текущее состояние СКПУ. Описание параметров приведено в таблице 63.

Таблица 63

Параметр	Описание
`disable`	Выключить СКПУ. При этом правила `udev` , сгенерированные на основе правил СКПУ, будут удалены. Но файл с правилами СКПУ `/etc/parsec/PDAC/devices.cfg` сохранится
`enable`	Включить СКПУ. При этом на основе имеющихся правил СКПУ будут сгенерированы правила `udev`

Для вступления изменений в силу требуется перезагрузка ОС.

19.4.2. Включение и выключение регистрации событий

С помощью инструмента `pdac-adm` можно включить или выключить регистрацию событий, связанных с контролем подключения устройств (регистрация результатов применения блокирующих, разрешающих или назначающих правил при подключении устройств).

По умолчанию регистрация событий выключена

Для включения и выключения регистрации событий используется команда:

```
sudo pdac-adm audit [enable|disable]
```

где параметр `enable` используется для включения регистрации событий;
параметр `disable` используется для выключения регистрации событий.

Изменения будут применены сразу.

Выполнение команды без параметра отображает текущее состояние регистрации событий.

19.4.3. Режим защиты от блокировки критически важных устройств

Режим защиты от блокировки критически важных устройств предотвращает случайную блокировку устройств ввода (клавиатура, мышь и т.д.).

При включении этого режима игнорируются имеющиеся блокирующие правила для устройств типа `hub` и `hid`. Кроме того, устанавливается запрет на изменение или удаление этих правил. Также для устройств типа `hub` и `hid` игнорируется наследование блокирующего правила шины подключения устройств.

Режим защиты от блокировки критически важных устройств включен по умолчанию. Для выключения и включения этого режима используется команда:

```
sudo pdac-adm protect-critical-devices [enable|disable]
```

где параметр `enable` используется для включения режима защиты от блокировки критически важных устройств;
параметр `disable` используется для выключения режима защиты от блокировки критически важных устройств.

Изменения будут применены сразу.

Выполнение команды без параметра отображает текущее состояние режима защиты от блокировки критически важных устройств.

19.4.4. Режим усиленной блокировки многосоставных устройств

Режим усиленной блокировки многосоставных устройств обеспечивает блокировку устройств, в которых объединены устройства различных типов, например веб-камера с интегрированным микрофоном.

При включении этого режима многосоставное устройство будет заблокировано, если имеется блокирующее правило для хотя бы одного из типов устройств в его составе. Например, использование веб-камеры с интегрированным микрофоном будет запрещено, даже если имеется разрешающее правило для устройств типа `video`, но при этом также имеется блокирующее правило для устройств типа `audio`.

Режим усиленной блокировки многосоставных устройств по умолчанию выключен. Для включения и выключения этого режима используется команда:

```
sudo pdac-adm force-deny [enable|disable]
```

где параметр `enable` используется для включения режима усиленной блокировки многосоставных устройств;
параметр `disable` используется для выключения режима усиленной блокировки многосоставных устройств.

Изменения будут применены сразу.

Выполнение команды без параметра отображает текущее состояние режима усиленной блокировки многосоставных устройств.

19.5. Управление подключением устройств с помощью графической утилиты

Контроль подключения устройств также можно настроить с использованием модуля «Устройства и правила» графической утилиты `astra-systemsettings` («Параметры системы»), описание модуля приведено в электронной справке. Для вызова модуля можно использовать команду:

```
astra-systemsettings astra_kcm_devices_and_rules
```

19.6. Монтирование съемных накопителей

Для того, чтобы устройство могло быть примонтировано, на нем должна быть размечена файловая система (устройство должно быть отформатировано).

Для монтирования ФС блочных устройств в командной строке используется инструмент `mount`, который позволяет:

- монтировать ФС произвольных блочных устройств в произвольные точки монтирования. Выполнение такого монтирования доступно только администраторам;

- непривилегированным пользователям из системной группы `floppy` монтировать ФС оптических дисков в каталог `/media/cdrom0`. Правило монтирования задано в файле `/etc/fstab`;

- непривилегированным пользователям из системной группы `floppy` монтировать ФС определенных типов в каталог `/run/user/<UID>/media/<UUID_монтируемой_ФС>/`. Список типов ФС задан в файле `/etc/fstab.pdac`.

Примечание. Пользователям из системной группы `cdrom` разрешено выполнять операции чтения и записи в ФС оптических дисков, но не разрешено монтировать эти ФС.

В команде монтирования с использованием инструмента `mount` необходимо указать наименование файла устройства и наименование точки монтирования. Остальные параметры монтирования выбираются из файлов `/etc/fstab` и `/etc/fstab.pdac`.

Для монтирования различных типов ФС разделов USB-накопителей в файл `/etc/fstab.pdac` включены следующие записи:

```
/dev/*fat       /run/user/*/media/*  auto    pdac,noauto,nodev,defaults  0 0
/dev/*ntfs*     /run/user/*/media/*  auto    pdac,noauto,nodev,iocharset=utf8,\
defaults  0 0
/dev/sd*ext*    /run/user/*/media/*  auto    pdac,nodev,noauto,defaults  0 0
/dev/sd*iso9660 /run/user/*/media/*  iso9660 pdac,nodev,noexec,noauto,\
defaults  0 0
/dev/sd*        /run/user/*/media/*  auto    owner,group,nodev,noexec,noauto,\
iocharset=utf8,defaults  0 0
```

Для монтирования различных типов ФС оптических дисков в файл `/etc/fstab.pdac` включены следующие записи:

```
/dev/s*udf       /run/user/*/media/*  udf      pdac,nodev,noexec,noauto,\
defaults  0 0
/dev/sr*iso9660  /run/user/*/media/*  iso9660  pdac,nodev,noexec,noauto,\
defaults  0 0
```

Для монтирования ФС оптических дисков в каталог `/media/cdrom0/` включена следующая строка в файл `/etc/fstab`:

```
/dev/sr0    /media/cdrom0   udf,iso9660   user,noauto 0 0
```

Эта запись необходима для корректной работы инструмента `apt` при установке пакетов с оптического диска. При этом остается возможность монтировать любой оптический диск в каталог `/media/cdrom0`. Если для установки пакетов оптические диски не используются, то эту строку рекомендуется удалить.

Примечание. Установить запрет на монтирование ФС пользователями из системной группы `floppy` можно с помощью инструмента `astra-mount-lock` (см. РУСБ.10015-01 97 01-1).

Для непривилегированных пользователей из системной группы `floppy` доступно полуавтоматическое монтирование в графической среде (в утилите `fly-fm` «Менеджер файлов» или с помощью инструмента `fly-reflex-service` из окружения рабочего стола, см. электронную справку).

19.7. Безопасная эксплуатация ОС при подключении съемных накопителей

При обработке в системе конфиденциальной информации рекомендуется настраивать и контролировать использование съемных накопителей. Способы контроля подключения устройств:

- редактирование файла `/etc/fstab.pdac`;
- ограничение доступа с помощью назначающих правил;
- исключение пользователей из групп `floppy` и `cdrom`;
- применение блокирующего правила для устройств типа `storage`;
- включение запрета на монтирование съемных накопителей пользователями из группы `floppy` с помощью инструмента `astra-mount-lock` (см. РУСБ.10015-01 97 01-1).

При размещении конфиденциальной информации на съемных накопителях с твердотельными носителями информации (SSD, Flash) следует учитывать их технические особенности. Механизм очистки освобождаемых блоков ФС не может гарантировать полное удаление конфиденциальной информации, записанной на такой накопитель.

Кроме того, наличие физического доступа к любому устройству хранения информации позволяет прочитать с него все записанные данные, независимо от наличия и содержания меток безопасности. При использовании съемных накопителей для хранения конфиденциальной информации должны быть выполнены следующие требования:

- ограничен физический доступ к съемным накопителям;
- применено защитное преобразование информации, которая хранится на съемном накопителе.

19.8. Использование устройств в ненулевой сессии

По умолчанию всем подключаемым устройствам присваивается нулевая метка безопасности. В ненулевой сессии (на уровне конфиденциальности, отличном от 0) можно использовать устройство, для которого задано назначающее правило. Назначающее правило для локальных пользователей необходимо подготовить в СКПУ (см. 19.2) или с использованием модуля «Устройства и правила» графической утилиты «Параметры системы» (см. электронную справку). Назначающее правило для пользователей домена FreeIPA необходимо подготовить в веб-интерфейсе контроллера домена (см. 19.9). При этом в правиле должны быть указаны значения следующих параметров доступа:

- пользователи, которым разрешено использование устройства;
- метка безопасности устройства.

Устройство можно использовать (например, монтировать с правами на чтение, запись и выполнение) на том уровне конфиденциальности сессии пользователя, который задан в правиле для этого устройства. В сессии пользователя, уровень конфиденциальности которой выше заданного в правиле, устройство можно использовать только с правами на чтение.

Для USB-накопителей правила мандатного управления доступом применяется к дисковыми разделам. Если на USB-накопителе находится несколько разделов, то метка безопасности, заданная в назначающем правиле, будет назначена всем разделам.

ФС ext2, ext3, ext4 и XFS обеспечивают хранение расширенных атрибутов файловых объектов. В расширенных атрибутах может быть размещена информация о владельцах и правах доступа, а также метка безопасности файлового объекта.

Раздел USB-накопителя с ФС, поддерживающей расширенные атрибуты файловых объектов, следует подготовить для использования на ненулевом уровне конфиденциальности. Для этого назначить его корневой ФС уровень конфиденциальности, который задан в правиле для этого USB-накопителя (или будет задан), а также назначить пользователя-владельца и группу-владельца. Чтобы подготовить раздел USB-накопителя, необходимо:

1) примонтировать ФС раздела USB-накопителя. Каталог монтирования должен располагаться внутри каталога, имеющего атрибут `ccnr` и уровень конфиденциальности не ниже уровня, который требуется назначить USB-накопителю. В ОС монтирование устройства по умолчанию осуществляется в каталог `/run/user/<UID>/media/<UUID_монтируемой_ФС>/` (каталог `/run/` имеет максимальный в ОС уровень конфиденциальности и атрибут `ccnr`);

2) назначить каталогу монтирования уровень конфиденциальности, который задан в правиле для этого USB-накопителя (или будет задан):

```
sudo pdpl-file <уровень> /run/<каталог_монтирования>
```

3) назначить для каталога монтирования пользователя-владельца и группу-владельца:

```
sudo chown -R <имя_пользователя>:<имя_группы> /run/<каталог_монтирования>
```

4) размонтировать устройство.

ВНИМАНИЕ! В случае если включен мандатный контроль целостности, то действия по подготовке раздела USB-накопителя должны осуществляться от имени администратора с высокой меткой целостности.

19.9. Контроль подключения устройств в домене FreeIPA

На компьютерах, входящих в домен FreeIPA, также можно ограничить доступ к устройству. Для этого следует создать назначающее правило в веб-интерфейсе контроллера домена.

Устройства идентифицируются на основе выражений сопоставления, которые применяются в правилах `udev`. В большинстве случаев достаточно использовать серийный номер (атрибут `ID_SERIAL`). Если использование серийного номера невозможно, необходимо указать один или несколько других атрибутов устройства (идентификатор модели, идентификатор производителя и т.п).

Для создания назначающего правила необходимо:

1) получить значение идентификационного параметра (атрибута), который используется в правилах `udev`. Для этого:
   а) подключить устройство к компьютеру;
   б) вывести перечень атрибутов подключенного устройства:

```
sudo udevadm info --query=property --name=/dev/<файл_устройства>
```

Пример

Атрибуты USB-накопителя:

```
DEVPATH=/devices/pci0000:00/0000:00:14.0/usb3/3-3/3-3:1.0/\
host0/target0:0:0/0:0:0:0/block/sda
DEVNAME=/dev/sda
DEVTYPE=disk
DISKSEQ=14
MAJOR=8
MINOR=0
SUBSYSTEM=block
USEC_INITIALIZED=33632934153
ID_BUS=usb
ID_MODEL=USB_DISK_2.0
ID_MODEL_ENC=USB\x20DISK\x202.0\x20\x20\x20\x20
ID_MODEL_ID=4100
ID_SERIAL=_USB_DISK_2.0_070A38235B908E23-0:0
ID_SERIAL_SHORT=070A38235B908E23
```

```
ID_VENDOR_ENC=\x20\x20\x20\x20\x20\x20\x20\x20
ID_VENDOR_ID=13fe
ID_REVISION=PMAP
ID_TYPE=disk
ID_INSTANCE=0:0
```

в) зафиксировать значение требуемого атрибута устройства (например, `ID_SERIAL` — серийный номер);

2) в веб-интерфейсе контроллера домена FreeIPA создать назначающее правило. Для этого:

а) открыть вкладку «Политика»;

б) из выпадающего списка «Политика PARSEC» выбрать «Учтенные устройства»;

в) на открывшейся странице «Учтенные устройства» нажать **[Добавить]**;

г) в открывшемся окне «Добавить» подготовить правило:

- задать условное наименование устройства;
- указать пользователя-владельца и группу-владельца.

ВНИМАНИЕ! В качестве группы-владельца не допускается указывать служебную доменную группу `ipausers`. Для использования в назначающих правилах рекомендуется создать отдельные доменные группы;

- в строке «Атрибуты устройства» нажать **[Добавить]** и в открывшемся поле ввода вставить выражение сопоставления устройства в формате правил `udev`.

Пример

Выражение сопоставления устройства по серийному номеру:

```
ENV{ID_SERIAL}=="_USB_DISK_2.0_070A38235B908E23-0:0"
```

- установить флаг «Правила учета включены»;
- нажать **[Добавить и изменить]**;

д) на открывшейся странице «Учтенное устройство: <наименование>» изменить (если необходимо) значения параметров доступа:

- во вкладке «Параметры» — набор прав доступа и уровень конфиденциальности;
- во вкладке «Категории конфиденциальности устройств» — набор категорий конфиденциальности;
- во вкладке «Маска аудита успеха» — флаги успешных событий;
- во вкладке «Маска аудита отказа» — флаги неуспешных событий.

По умолчанию установлены следующие значения параметров доступа:

- набор прав доступа: 640;

- флаги аудита: 0x0:0x0;
- метка безопасности: 0:0:0x0:0x0!;

е) на странице «Учтенное устройство: <наименование>» во вкладке «Параметры» нажать **[Сохранить]**.

На компьютерах, входящих в домен FreeIPA, генерация правил `udev` осуществляется службой `sssd` при входе в сессию пользователя домена.

Если к компьютеру были подключены какие-либо устройства, то для применения созданных или измененных правил доступа к устройствам требуется переподключить эти устройства или выполнить команду:

```
sudo udevadm trigger
```

Также правила будут применены после перезагрузки ОС.

После применения правил пользователь-владелец или пользователи из группы-владельца, указанные в правиле, смогут монтировать ФС дисковых разделов USB-накопителя.

Устройство, для которого создано назначающее правило, можно использовать в ненулевой сессии (на уровне конфиденциальности, отличном от 0). Для этого в веб-интерфейсе управления доменом FreeIPA необходимо назначить ему соответствующий уровень конфиденциальности:

1) открыть вкладку «Политика»;
2) из выпадающего списка «Политика PARSEC» выбрать «Учтенное устройства»;
3) на открывшейся странице «Учтенное устройства» выбрать устройство;
4) на открывшейся странице «Учтенное устройство: <наименование>»:
   а) во вкладке «Параметры» из выпадающего списка «Уровень конфиденциальности устройства» выбрать нужный уровень конфиденциальности;
   б) нажать **[Сохранить]**.

Порядок использования устройств в ненулевой сессии описан в 19.8.

19.10. Блокировка USB-устройств в режиме «Мобильный»

Блокировка USB-устройств в режиме «Мобильный» осуществляется с помощью утилиты USBGuard. Утилита позволяет создавать правила для управления блокировкой подключаемых устройств.

Настройка работы USBGuard осуществляется в конфигурационном файле `/etc/usbguard/usbguard-daemon.conf`.

Для управления блокировкой USB-устройств в графическом интерфейсе реализован модуль KCM. Доступ к модулю ограничивается политикой Polkit.

Администратор при подключении USB-устройства настраивает доступ к нему, создавая правила. Если при включенной службе блокировки USB-устройств будет подключено USB-устройство, для которого отсутствует правило, то данное устройство будет заблокировано. Порядок использования модуля KCM для блокировки USB-устройств описан в электронной справке («Документация — Графический интерфейс — Режим «Мобильный»).