Отчёт по лабораторной работе №9

Управление SELinux

Наурузова Айшат Магометовна

Содержание

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

# 2 Ход выполнения

# 3 Ход выполнения

## 3.1 Управление режимами SELinux

После входа в систему были получены административные права с помощью команды:

su -

Для проверки текущего состояния SELinux использовалась команда:

sestatus -v

На экран была выведена подробная информация о политике безопасности:

* **SELinux status:** enabled — SELinux активен.
* **SELinuxfs mount:** /sys/fs/selinux — каталог, где смонтирована файловая система SELinux.
* **SELinux root directory:** /etc/selinux — основной путь для конфигурационных файлов.
* **Loaded policy name:** targeted — используется целевая политика (targeted policy).
* **Current mode:** enforcing — система работает в режиме принудительного контроля доступа.
* **Mode from config file:** enforcing — то же значение прописано в конфигурационном файле.
* **Policy MLS status:** enabled — включена многоуровневая защита (Multi-Level Security).
* **Policy deny\_unknown status:** allowed — неизвестные объекты разрешены.
* **Max kernel policy version:** 33 — версия политики ядра Linux.

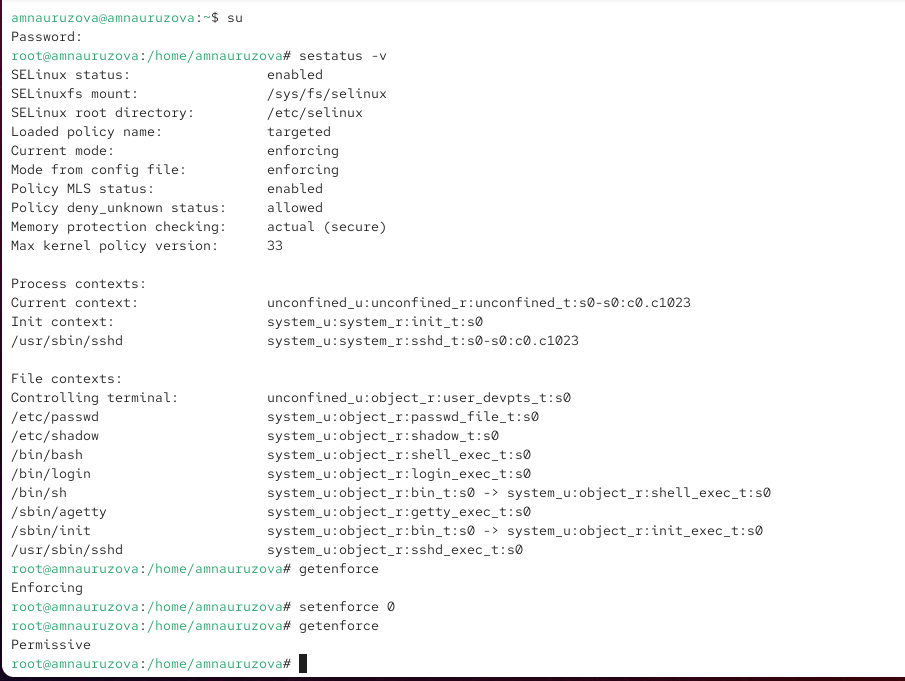


Рис. 1: Просмотр состояния SELinux

Для просмотра текущего режима работы SELinux введена команда:

getenforce

Результат — **Enforcing**, что подтверждает активный режим безопасности.

Далее режим был изменён на разрешающий (Permissive):

setenforce 0

После повторной проверки (getenforce) статус изменился на **Permissive**, что означает: SELinux теперь не блокирует действия, но записывает предупреждения.

Затем в конфигурационном файле /etc/sysconfig/selinux с помощью текстового редактора **nano** было изменено значение параметра:

SELINUX=disabled

и сохранены изменения.

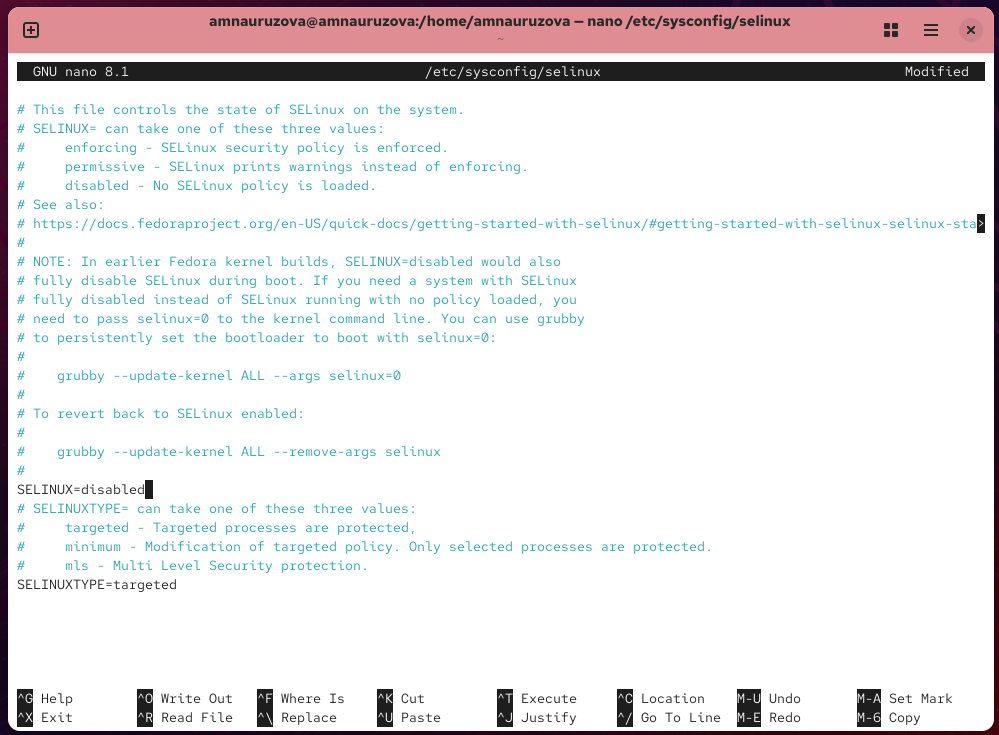


Рис. 2: Отключение SELinux в конфигурационном файле

После перезагрузки системы и повторного входа под пользователем **root** команда getenforce показала:

Disabled

Попытка принудительно включить SELinux (setenforce 1) завершилась сообщением:

setenforce: SELinux is disabled

Это означает, что при отключённом состоянии невозможно изменить режим без перезапуска системы.

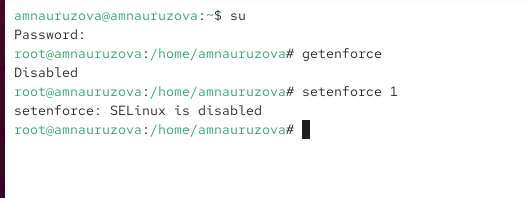


Рис. 3: SELinux отключён, попытка включения невозможна

Для повторного включения SELinux в файл /etc/sysconfig/selinux было возвращено значение:

SELINUX=enforcing

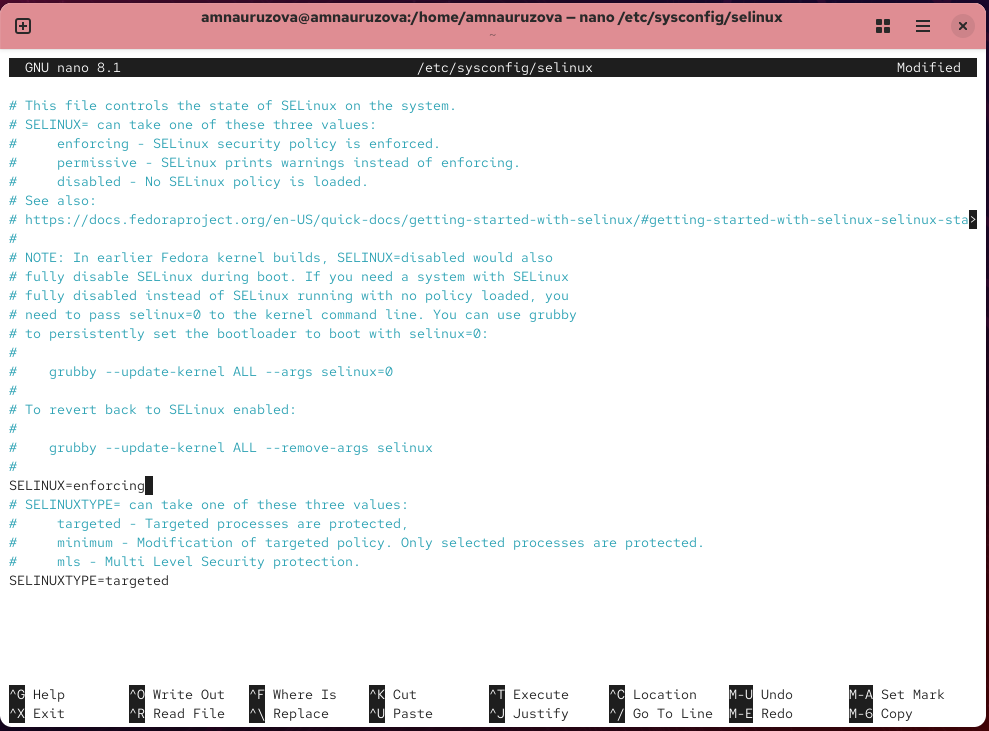


Рис. 4: Включение SELinux обратно в enforcing-режиме

После перезагрузки система начала автоматическое восстановление меток SELinux, что подтверждают сообщения службы **selinux-autorelabel.service**:

***Warning — SELinux targeted policy relabel is required.***  
***Relabeling could take a very long time, depending on system size and speed.***

Процесс завершился корректно.

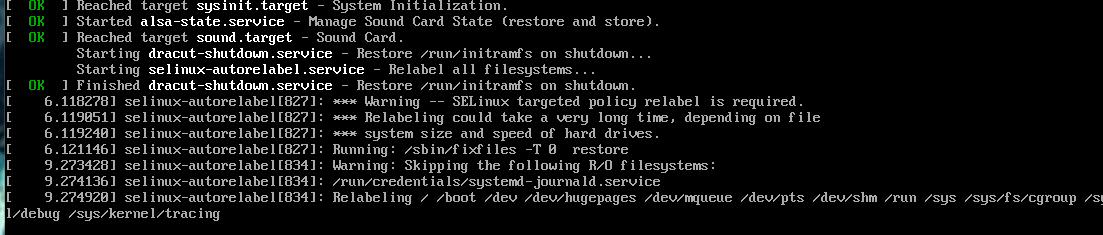


Рис. 5: Автоматическое восстановление контекста SELinux при перезагрузке

Повторная проверка состояния SELinux (sestatus -v) показала, что система снова работает в режиме **Enforcing** и политика безопасности применяется корректно.

## 3.2 Использование restorecon для восстановления контекста безопасности

После входа с правами администратора была просмотрена метка контекста файла /etc/hosts:

ls -Z /etc/hosts

Результат показал тип контекста **net\_conf\_t** — это корректная метка для сетевых конфигурационных файлов.

Далее файл был скопирован в домашний каталог:

cp /etc/hosts ~/

Повторная проверка (ls -Z ~/hosts) показала, что у новой копии контекст изменился на **admin\_home\_t**, поскольку копирование в домашний каталог создаёт файл с меткой, соответствующей окружению пользователя.

После этого файл был перемещён обратно в каталог /etc:

mv ~/hosts /etc

Теперь /etc/hosts имел контекст **admin\_home\_t**, что некорректно для данного пути.

Для восстановления правильной метки был применён инструмент **restorecon**:

restorecon -v /etc/hosts

Результат вывода подтвердил изменение контекста обратно на **net\_conf\_t**:

Relabeled /etc/hosts from unconfined\_u:object\_r:admin\_home\_t:s0 to unconfined\_u:object\_r:net\_conf\_t:s0



Рис. 6: Восстановление контекста файла /etc/hosts

Для массового восстановления контекстов безопасности на всей файловой системе была выполнена команда:

touch /.autorelabel

и произведена перезагрузка системы.

Во время запуска служба **selinux-autorelabel.service** автоматически провела полную перемаркировку файлов, о чём свидетельствуют соответствующие сообщения:

***Warning — SELinux targeted policy relabel is required.***  
***Relabeling could take a very long time…***

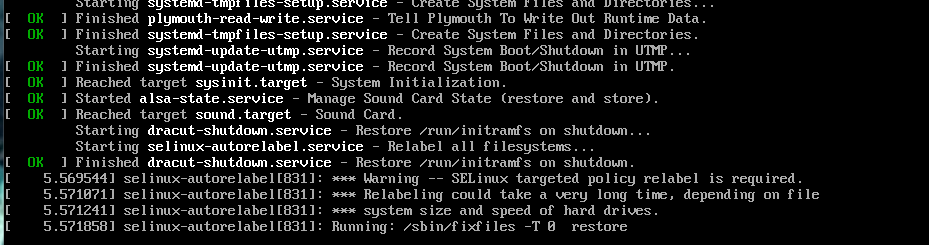


Рис. 7: Автоматическое перемаркирование файловой системы

После завершения загрузки SELinux функционировал в штатном режиме, а все контексты безопасности были восстановлены.

## 3.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

После получения административных прав было установлено необходимое программное обеспечение для работы веб-сервера Apache и текстового браузера Lynx:

dnf -y install httpd  
dnf -y install lynx

Далее был создан новый каталог, который будет использоваться как корневая директория веб-сервера:

mkdir /web

Внутри каталога /web создан файл index.html с содержимым:

Welcome to my web server

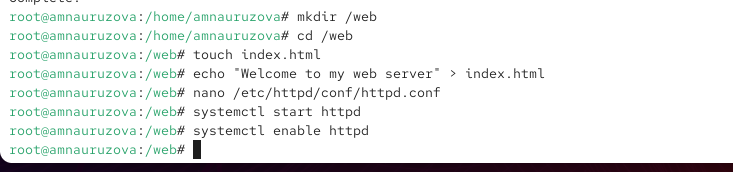


Рис. 8: Создание каталога и файла index.html

В конфигурационном файле /etc/httpd/conf/httpd.conf были внесены изменения.  
Закомментирована строка по умолчанию:

#DocumentRoot "/var/www/html"

и добавлена новая:

DocumentRoot "/web"

Также был добавлен новый раздел, определяющий разрешения для каталога /web:

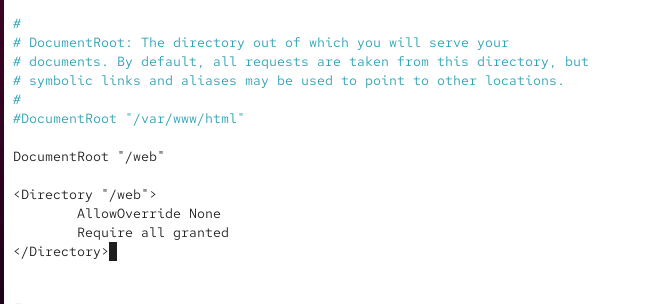


Рис. 9: Изменение конфигурации Apache

После сохранения изменений службы были запущены и добавлены в автозагрузку:

systemctl start httpd  
systemctl enable httpd

При первом обращении к веб-серверу через текстовый браузер Lynx по адресу http://localhost отобразилась стандартная тестовая страница Rocky Linux, а не созданный файл index.html.

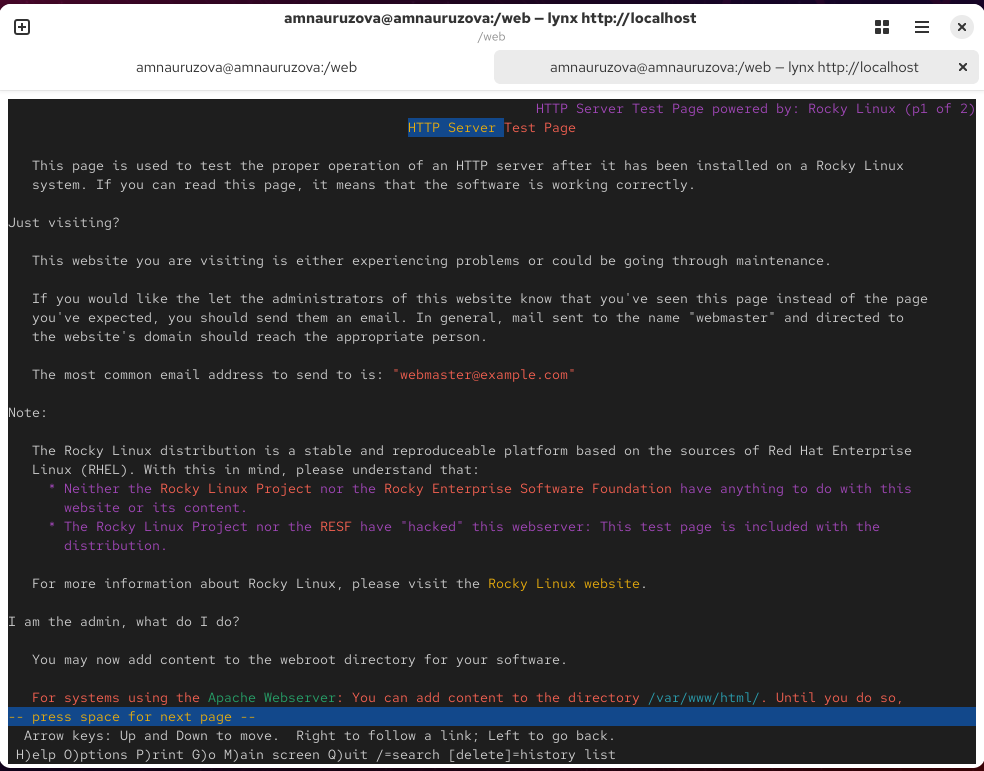


Рис. 10: Стандартная страница Apache

Это произошло из-за несоответствия контекста безопасности SELinux для нового каталога /web.  
Для исправления был добавлен правильный контекст безопасности с помощью команды:

semanage fcontext -a -t httpd\_sys\_content\_t "/web(/.\*)?"

После этого был выполнен пересмотр меток контекста:

restorecon -R -v /web

Результат показал изменение контекста:  
- /web и index.html были перемаркированы на **httpd\_sys\_content\_t**, что позволяет Apache читать эти файлы.

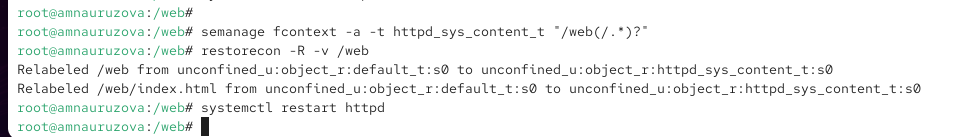


Рис. 11: Применение контекста безопасности SELinux

После перезапуска службы Apache (systemctl restart httpd) при повторном обращении через Lynx появилась пользовательская веб-страница с текстом:

**Welcome to my web server**

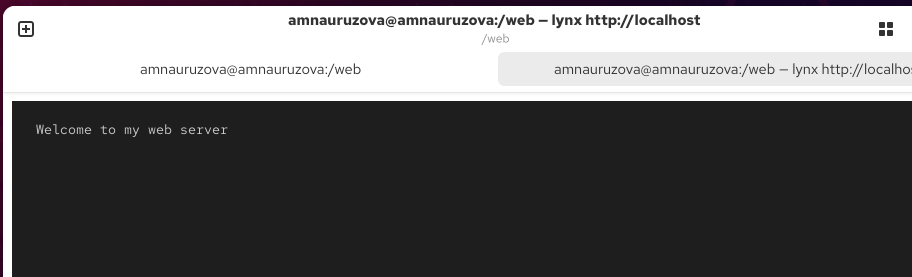


Рис. 12: Корректное отображение пользовательской страницы

## 3.4 Работа с переключателями SELinux

Для исследования работы SELinux-переключателей была выполнена команда:

getsebool -a | grep ftp

Результат показал, что переключатель **ftpd\_anon\_write** имеет значение **off**, то есть запись для анонимных пользователей через FTP отключена.

Далее просмотрен список переключателей SELinux с описанием для службы ftpd\_anon:

semanage boolean -l | grep ftpd\_anon

Вывод подтвердил, что параметр ftpd\_anon\_write отвечает за разрешение записи анонимных пользователей FTP и по умолчанию отключён.

Затем переключатель был активирован временно (до перезагрузки системы):

setsebool ftpd\_anon\_write on

Проверка (getsebool ftpd\_anon\_write) показала, что текущее значение стало **on**.  
Однако при просмотре с помощью semanage boolean -l постоянное значение оставалось **off**, то есть изменение не сохраняется после перезагрузки.

Для сохранения параметра в постоянной конфигурации была выполнена команда:

setsebool -P ftpd\_anon\_write on

Теперь проверка показала, что оба значения (временное и постоянное) равны **on**.

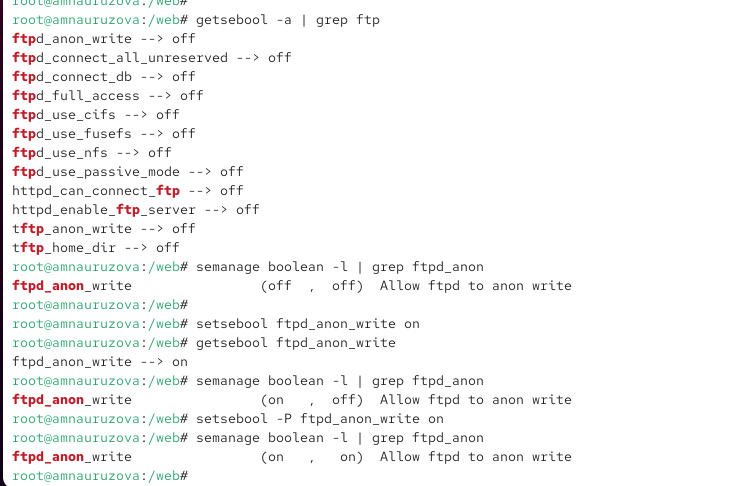


Рис. 13: Работа с переключателями SELinux для службы FTP

# 4 Контрольные вопросы

**1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?**  
Для временного перевода SELinux в разрешающий режим используется команда:  
setenforce 0  
Эта команда переключает режим с **Enforcing** (принудительный) на **Permissive** (разрешающий) до следующей перезагрузки системы.

**2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?**  
Чтобы просмотреть полный список всех переключателей SELinux, применяется команда:  
getsebool -a  
Она выводит текущее состояние (включено или выключено) для всех булевых параметров SELinux.

**3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?**  
Для удобного чтения и анализа сообщений SELinux в журнале аудита используется пакет:  
setroubleshoot  
Он предоставляет понятные уведомления и расшифровки ошибок SELinux через системный журнал.

**4. Какие команды вам нужно выполнить, чтобы применить тип контекста httpd\_sys\_content\_t к каталогу /web?**  
Для назначения правильного контекста безопасности веб-каталогу выполняются следующие команды:  
1. Добавление нового контекста:  
semanage fcontext -a -t httpd\_sys\_content\_t "/web(/.\*)?"  
2. Применение контекста ко всем файлам и подкаталогам:  
restorecon -R -v /web

**5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?**  
Для полного отключения SELinux необходимо отредактировать конфигурационный файл:  
/etc/sysconfig/selinux  
В нём нужно изменить строку:  
SELINUX=disabled

**6. Где SELinux регистрирует все свои сообщения?**  
Все события SELinux записываются в системный журнал по пути:  
/var/log/audit/audit.log  
В этом файле содержатся подробные записи обо всех действиях, заблокированных или разрешённых политикой SELinux.

**7. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию?**  
Чтобы получить список типов контекстов и булевых параметров, относящихся к службе FTP, используется команда:  
semanage boolean -l | grep ftp  
Она выводит доступные параметры и их текущее состояние (включено или выключено).

**8. Ваш сервис работает не так, как ожидалось, и вы хотите узнать, связано ли это с SELinux или чем-то ещё. Какой самый простой способ узнать?**  
Самый простой способ временно проверить влияние SELinux — перевести его в разрешающий режим командой:  
setenforce 0  
Если после этого служба заработала корректно, значит, проблема связана с политикой SELinux.  
После проверки рекомендуется вернуть систему в прежний режим:  
setenforce 1

# 5 Заключение

В ходе работы были изучены режимы SELinux, выполнена настройка контекстов безопасности для веб-сервера и FTP-службы, а также освоены основные инструменты администрирования и диагностики SELinux.