Отчёт по лабораторной работе 6

Мандатное разграничение прав в Linux

Максимова Ксения НБИбд-02-18

Содержание

[Цель работы 1](#_Toc88865119)

[Задание 1](#_Toc88865120)

[Теоретическое введение 1](#_Toc88865121)

[Выполнение лабораторной работы 2](#_Toc88865122)

[Выводы 16](#_Toc88865123)

[Список литературы 16](#_Toc88865124)

# Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Задание

Установить веб-сервер Apache и проверить на нем работу SELinx.

# Теоретическое введение

SELinux (Security-Enhanced Linux) — реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа[[1]](https://ru.wikipedia.org/wiki/SELinux). В SELinux права доступа определяются самой системой при помощи специально определенных политик. Политики работают на уровне системных вызовов и применяются самим ядром (но можно реализовать и на уровне приложения). SELinux действует после классической модели безопасности Linux. Иными словами, через SELinux нельзя разрешить то, что запрещено через права доступа пользователей или групп. Политики описываются при помощи специального гибкого языка описания правил доступа[[1]](https://ru.wikipedia.org/wiki/SELinux).

Основные понятия [[1]](https://ru.wikipedia.org/wiki/SELinux)

1. Домен — это некоторый набор действий, которые может производить один процесс. Главным образом это действия, необходимые процессу для выполнения определенной задачи.
2. Роль — это совокупность нескольких доменов.
3. Контекст безопасности — это совокупность всех атрибутов, которые связаны с объектами и субъектами.
4. Политика безопасности — это набор заданных правил, который регулирует взаимодействие ролей, доменов.

Security Enhanced Linux может работать различными способами[[2]](https://itsecforu.ru/2019/07/25/%F0%9F%9B%A1%EF%B8%8F-%D1%80%D0%B5%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F-%D0%BC%D0%B0%D0%BD%D0%B4%D0%B0%D1%82%D0%BD%D0%BE%D0%B3%D0%BE-%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8F-%D0%B4/):

* Enforcing: SELinux запрещает доступ на основе правил политики SELinux, набора руководящих принципов, которые управляют механизмом безопасности.
* Permissive: SELinux не запрещает доступ, но в журнале регистрируются отказы для действий, которые были бы запрещены при запуске в принудительном режиме.
* Disabled: Полное отключение системы принудительного контроля доступа

SELinux предоставляет следующие модели управления доступом[[3]](https://habr.com/ru/company/kingservers/blog/209644/):

1. Type Enforcement (TE): основной механизм контроля доступа, используемый в целевых политиках. Позволяет детально, на самом низком уровне управлять разрешениями. Самый гибкий, но и самый трудоемкий для системного администратора механизм.
2. Role-Based Access Control (RBAC): в этой модели права доступа реализуются в качестве ролей. Ролью называется разрешения на выполнение определенных действий одним или несколькими элементами системы над другими частями системы. По-сути, RBAC является дальнейшим развитием TE.
3. Multi-Level Security (MLS): многоуровневая модель безопасности, в которой всем объектам системы присваивается определенный уровень доступа. Разрешение или запрет доступа определяется только соотношением этих уровней.

# Выполнение лабораторной работы

1. Убедитесь, что SELinux работает в режиме enforcing политики targeted.

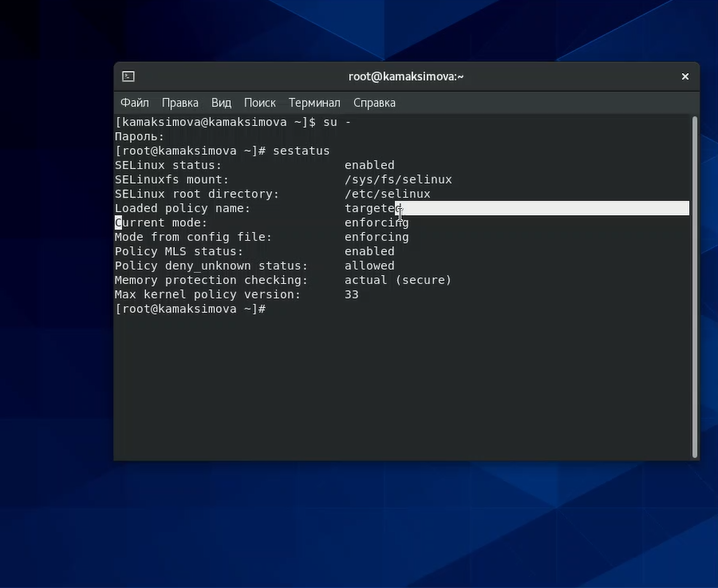


Рис 1.Режиме enforcing

[Рисунок 1](image/1.png)

1. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает.

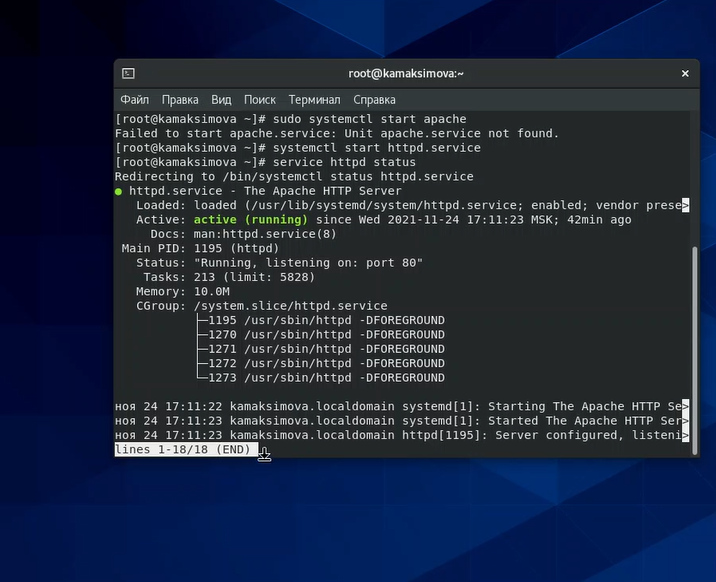


Рис 2.Проверка

[Рисунок 2](image/2.png)

1. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности.

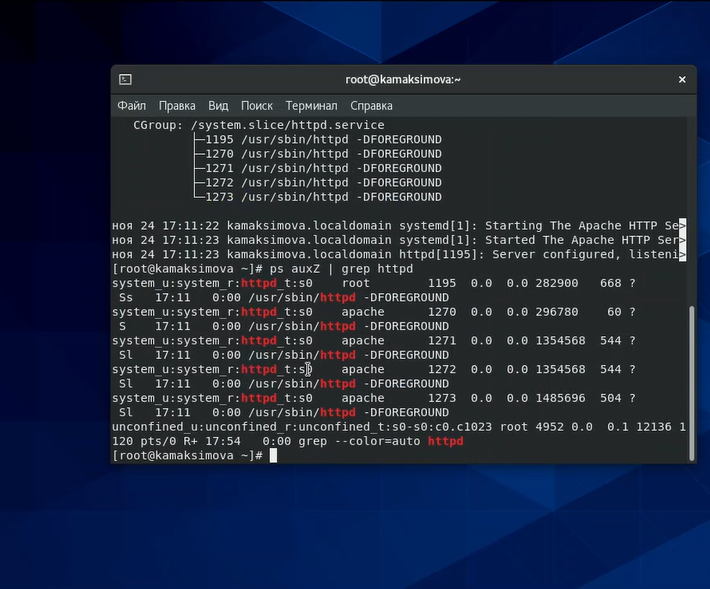


Рис 3.Список процессов

[Рисунок 3](image/3.png)

1. Посмотрите текущее состояние переключателей SELinux для Apache

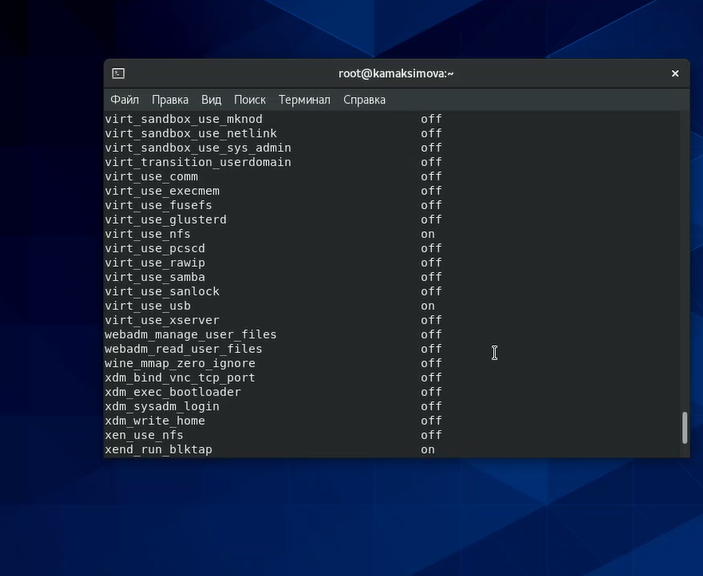


Рис 4.Текущее состояние

[Рисунок 4](image/4.png)

Многие из них находятся в положении «off».

1. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов.

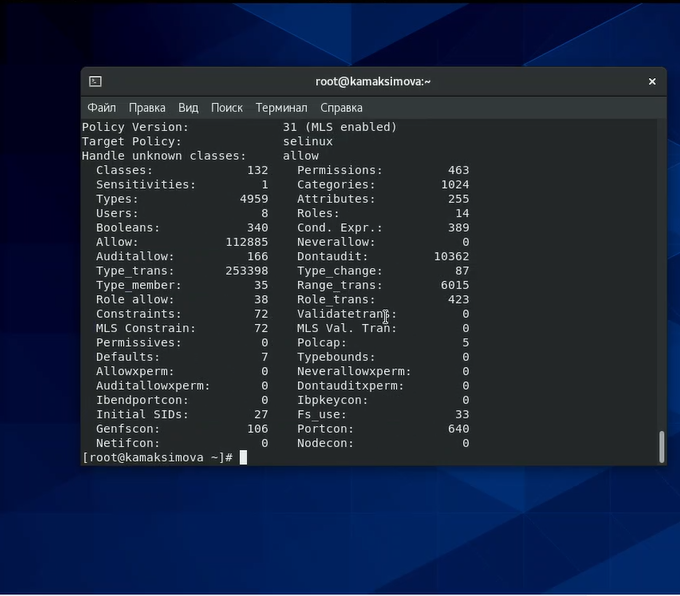


Рис 5.Статистика

[Рисунок 5](image/5.png)

1. Определите тип файлов и поддиректорий, находящихся в директории “/var/www”.

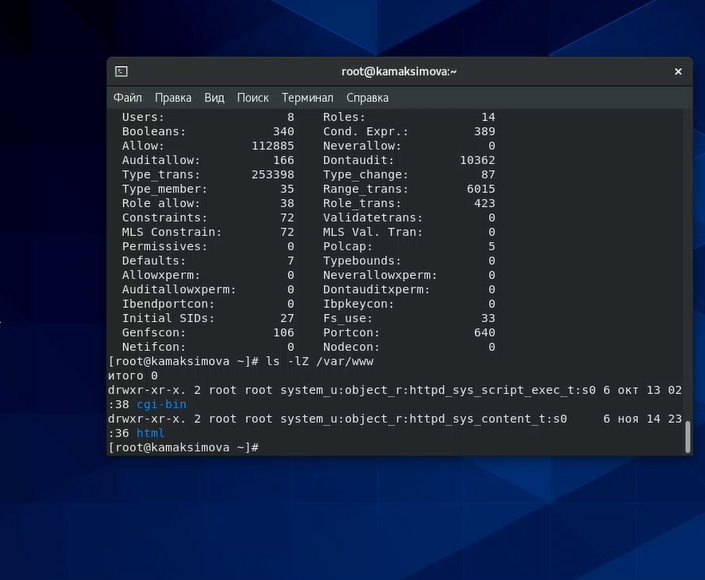


Рис 6.Директория “/var/www”

[Рисунок 6](image/6.png)

1. Определите тип файлов, находящихся в директории “/var/www/html”

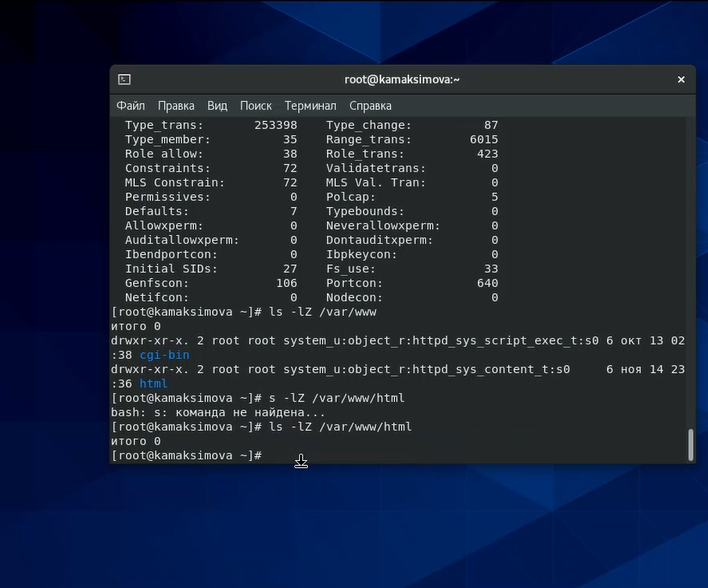


Рис 7.Директория “/var/www/html”

[Рисунок 7](image/7.png)

1. Определите круг пользователей, которым разрешено создание файлов в директории “/var/www/html”

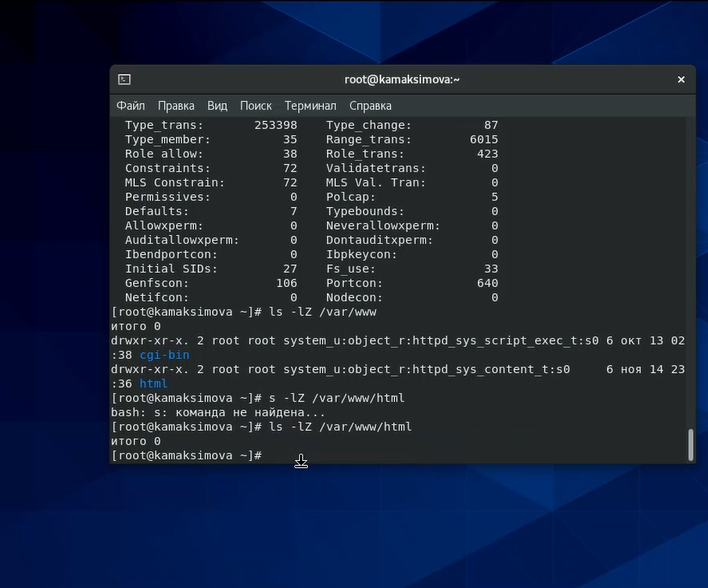


Рис 7.Директория “/var/www/html”

[Рисунок 7](image/7.png)

1. Создайте от имени суперпользователя html-файл

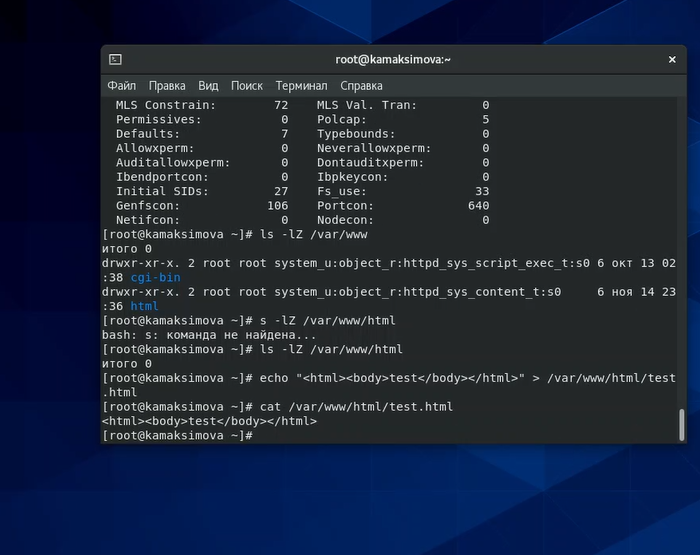


Рис 8.html-файл

[Рисунок 8](image/8.png)

1. Проверьте контекст созданного вами файла.

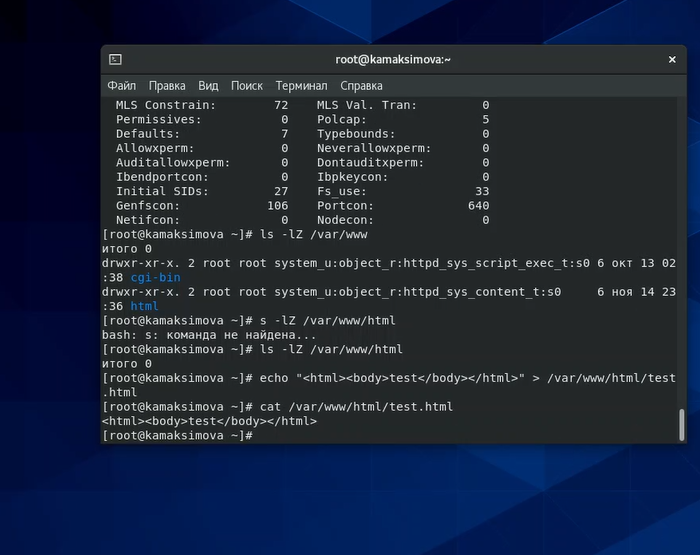


Рис 8.html-файл

[Рисунок 8](image/8.png)

1. Обратитесь к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”

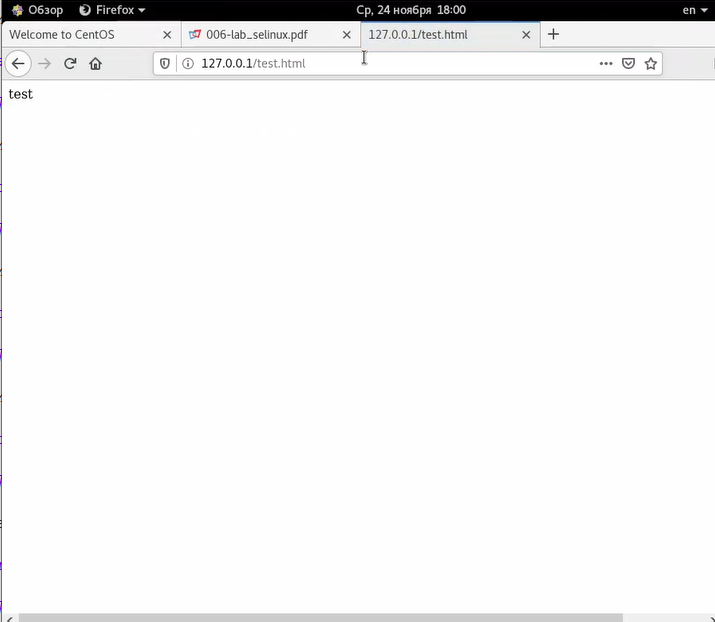


Рис 9.Файл

[Рисунок 9](image/9.png)

1. Изучите справку man httpd\_selinux и выясните, какие контексты файлов определены для httpd.

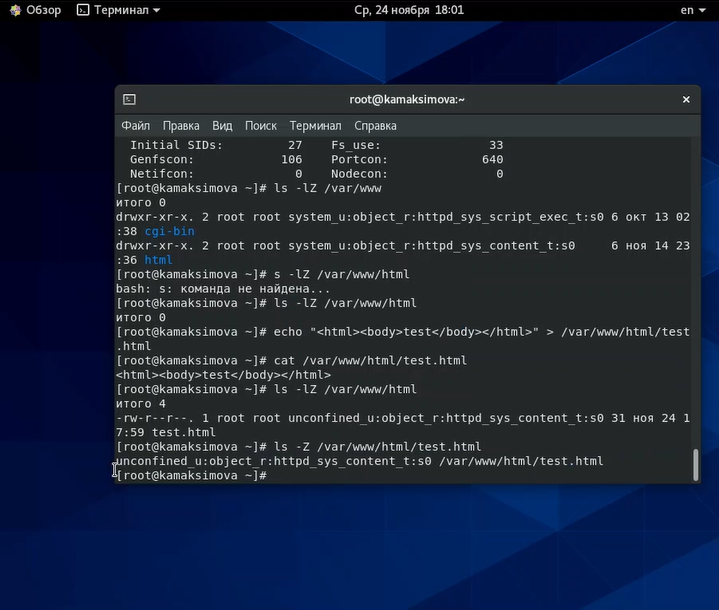


Рис 10.Контексты файлов

[Рисунок 10](image/10.png)

1. Измените контекст файла “/var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba\_share\_t

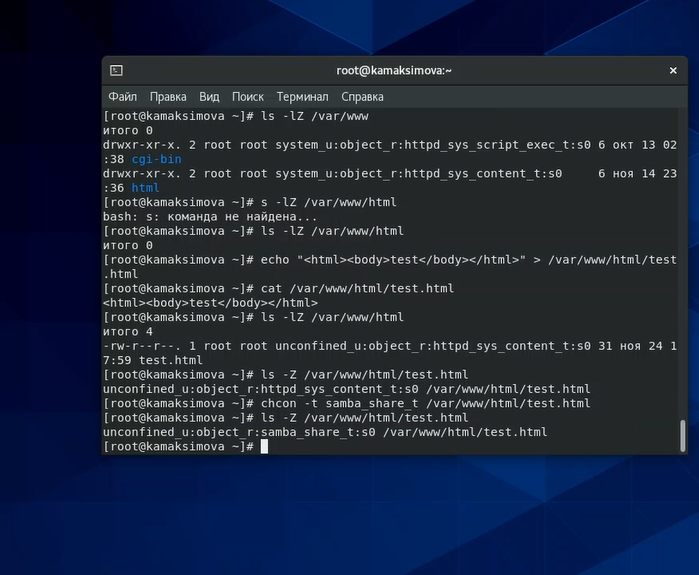


Рис 11.Изменение контекста файла

[Рисунок 11](image/11.png)

1. Попробуйте ещё раз получить доступ к файлу через веб-сервер.

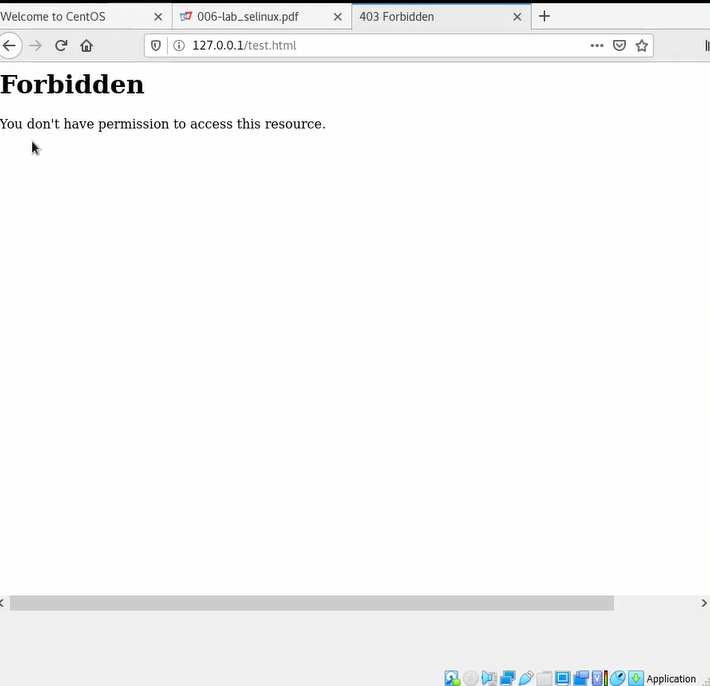


Рис 12.Изменение контекста файла

[Рисунок 12](image/12.png)

1. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю?

# Выводы

Получены практические навыки администрирования ОС Linux, а так же получено практическое знакомство с технологией SELinux совместно с веб-сервером Apache.

# Список литературы

[1. SELinux](https://ru.wikipedia.org/wiki/SELinux)

[2. Реализация мандатного контроля доступа с помощью SELinux или AppArmor в Linux](https://itsecforu.ru/2019/07/25/%F0%9F%9B%A1%EF%B8%8F-%D1%80%D0%B5%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F-%D0%BC%D0%B0%D0%BD%D0%B4%D0%B0%D1%82%D0%BD%D0%BE%D0%B3%D0%BE-%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8F-%D0%B4/)

[3. SELinux – описание и особенности работы с системой](https://habr.com/ru/company/kingservers/blog/209644/)