

Шаблон отчёта по лабораторной работе

№9

Управление SELinux

Кхари Жекка Кализая Арсе

Содержание

1 Цель работы	6
2 Задание	7
3 Выполнение лабораторной работы	8
3.1 управление режимами SELinux	8
3.2 Использование restorecon для восстановления контекста безопасности	14
3.3 настройка контекста безопасности для нестандартного расположения файлов веб-сервера	17
3.4 Работа с переключателями SELinux	25
4 Выводы	30
Список литературы	31

Список иллюстраций

3.1 терминал	8
3.2 статус службы SELinux	9
3.3 режим работы SELinux	9
3.4 изменение режима работы	10
3.5 новая строка в файле selinux	10
3.6 перезагрузка системы	11
3.7 терминал	11
3.8 статус SELinux	12
3.9 режим работы SELinux	12
3.10 установка файла selinux	13
3.11 перезагрузка системы	13
3.12 Название	14
3.13 контекст безопасности	14
3.14 копирование файла hosts	15
3.15 контекст файла	15
3.16 перезапись файла hosts	16
3.17 исправление контекста файла hosts	16
3.18 проверка контекста	17
3.19 создание файла для исправления контекста безопасности	17
3.20 терминал	18
3.21 установка httpd	18
3.22 установка lynx	19
3.23 создание каталога web	19
3.24 файл index.html	20
3.25 добавление строки в файле index.html	20
3.26 изменение строк	21
3.27 запуск службы и веба-сервера	22
3.28 текстовой браузер lynx	22
3.29 закрытие браузера	23
3.30 semanage	23
3.31 восстановление контекста безопасности	24
3.32 текстовой браузер	24
3.33 lynx http://localhost	25
3.34 getsebool	25
3.35 список переключателей	26
3.36 изменение текущего значения переключателя	26
3.37 список переключателей с пояснением	27

3.38 изменить постоянное значение переключателя	27
3.39 список переключателей	28

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux

2 Задание

1. Продемонстрируйте навыки по управлению режимами SELinux (см. раздел 9.4.1).
2. Продемонстрируйте навыки по восстановлению контекста безопасности SELinux (см. раздел 9.4.2).
3. Настройте контекст безопасности для нестандартного расположения файлов веб- службы (см. раздел 9.4.3).
4. Продемонстрируйте навыки работы с переключателями SELinux (см. раздел 9.4.4)

3 Выполнение лабораторной работы

3.1 Управление режимами SELinux

Сначала этой лабораторной работы я открыл терминал под пользователя root как обычно (рис. 3.1).

```
su -
```

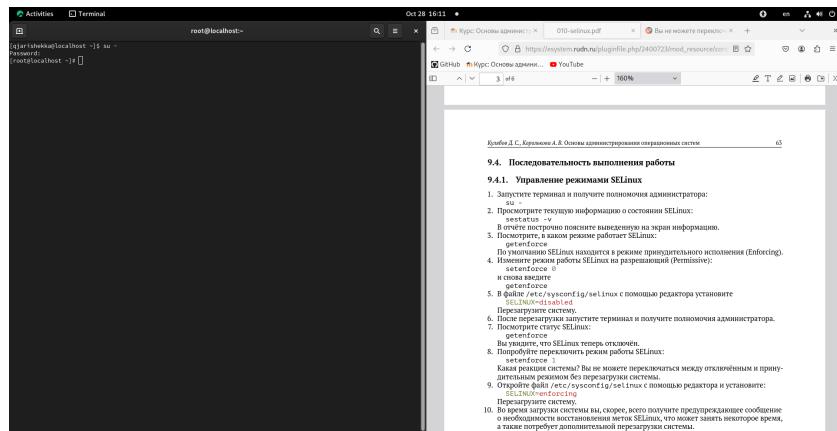


Рис. 3.1: терминал

Потом я смотрел статус службы SELinux (рис. 3.2).

```
sestatus -v
```

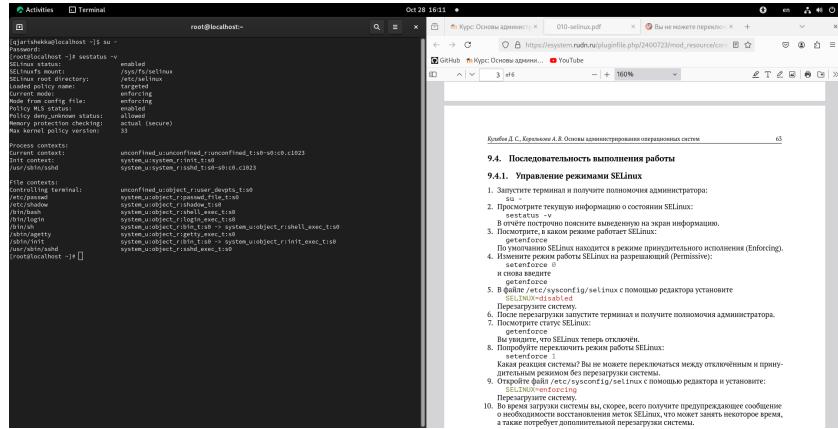


Рис. 3.2: статус службы SELinux

там я смог смотреть статус, место монтирования, место расположения загрузки на полиса, текущий режим и версию

Потом я выполнил команду чтобы только смотреть на каком режиме работает SELinux (рис. 3.3).

`getenforce`

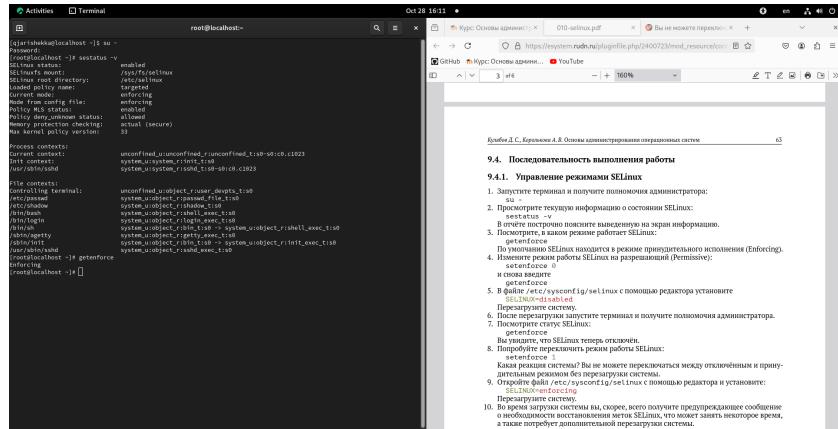


Рис. 3.3: режим работы SELinux

Потом я изменил режим работы SELinux на разрешающий и снова я смотрел режим работы (рис. 3.4).

`setenforce 0`

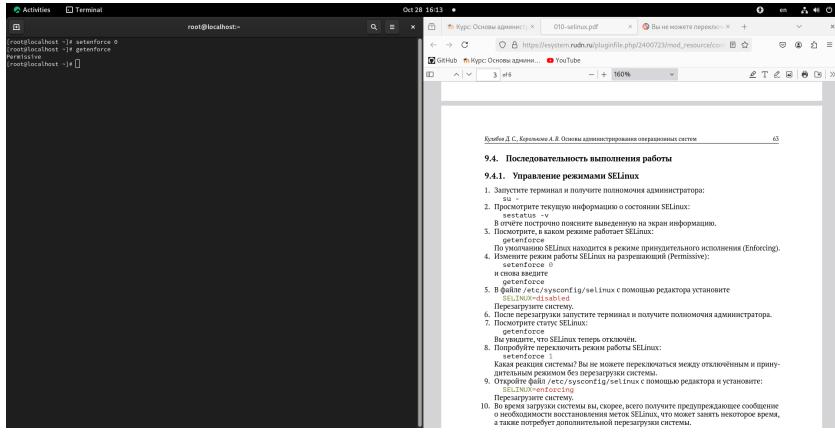


Рис. 3.4: изменение режима работы

Затем я добавил строку в файле /etc/sysconfig/selinux с помощью редактора vim (рис. 3.5).

SELINUX=disabled

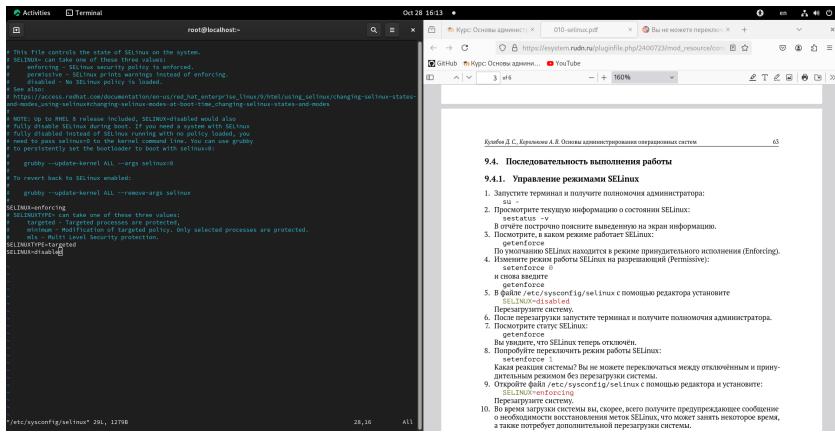


Рис. 3.5: новая строка в файле selinux

Дальше я перезагрузил ОС (рис. 3.6).

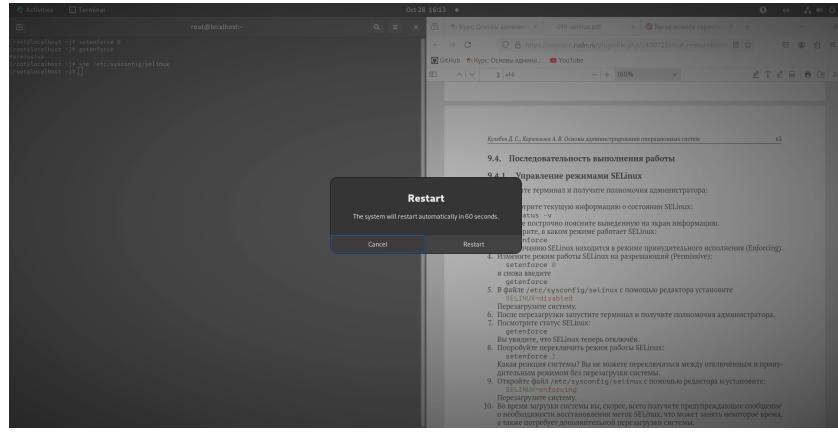


Рис. 3.6: перезагрузка системы

Потом я еще раз открыл терминал под пользователя root (рис. 3.7).

su -

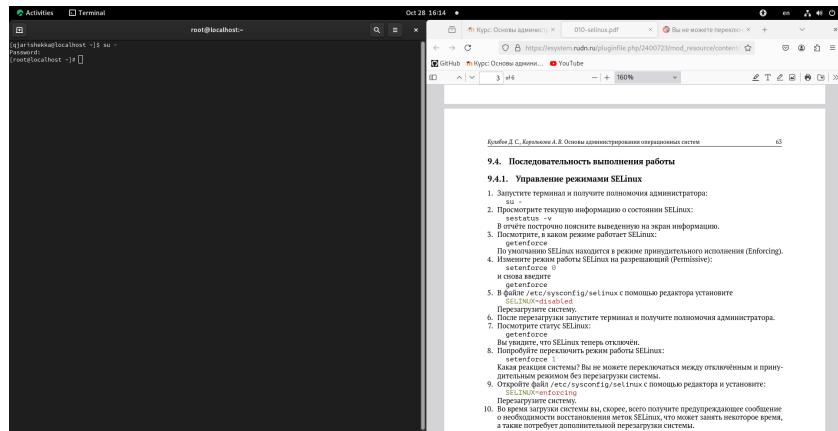


Рис. 3.7: терминал

Затем я посмотрел статус SELinux (рис. 3.8).

getenforce

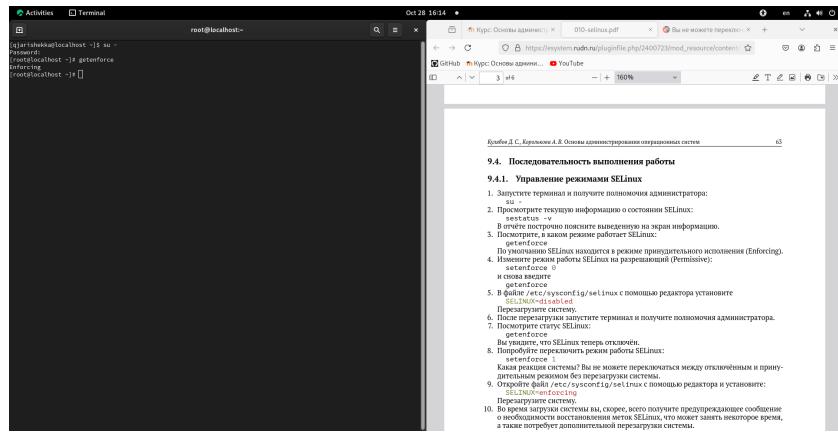


Рис. 3.8: статус SELinux

Потом я переключил режим работы SELinux (рис. 3.9).

`setenforce 1`

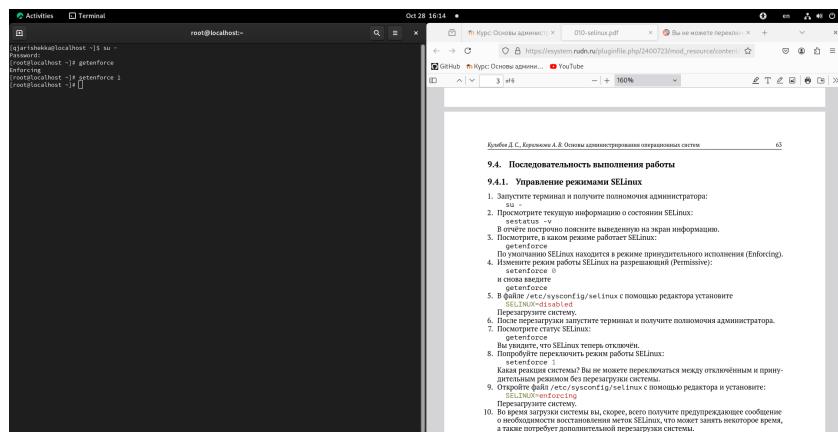


Рис. 3.9: режим работы SELinux

Потом я открыл файл /etc/sysconfig/selinux с помощью редактора vim и изменил строку (рис. 3.10).

```
vim /etc/sysconfig/selinux
SELINUX=enforcing
```

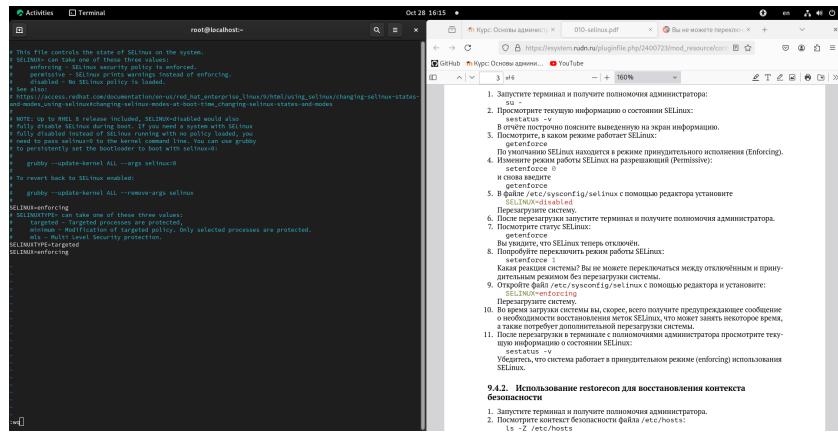


Рис. 3.10: установка файла selinux

Потом я еще раз перезагрузил систему (рис. 3.11).

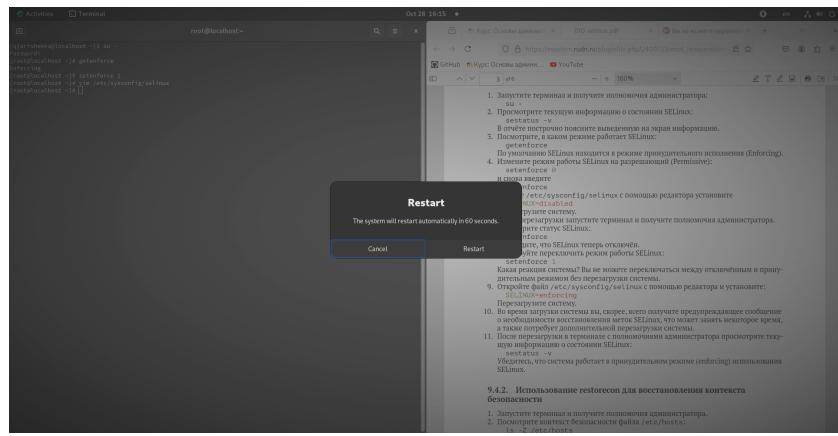


Рис. 3.11: перезагрузка системы

После перезагрузки я еще раз открыл терминал с полномочиями администратора и выполнил команду `sestatus` чтобы получил информацию о состоянии SELinux (рис. 3.12).

```
su -
password
sestatus -v
```

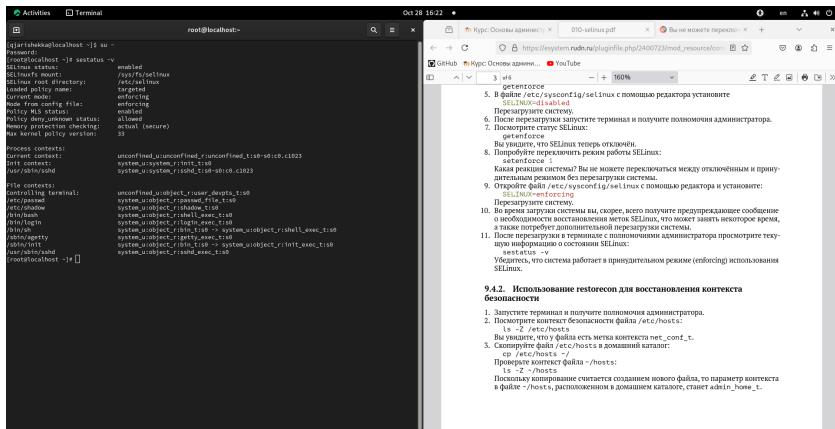


Рис. 3.12: Название

3.2 Использование restorecon для восстановления контекста безопасности

Еще раз в терминале под пользователем root я выполнил команду ls чтобы смотреть контекст безопасности файла /etc/hosts (рис. 3.13).

```
ls -Z /etc/hosts
```

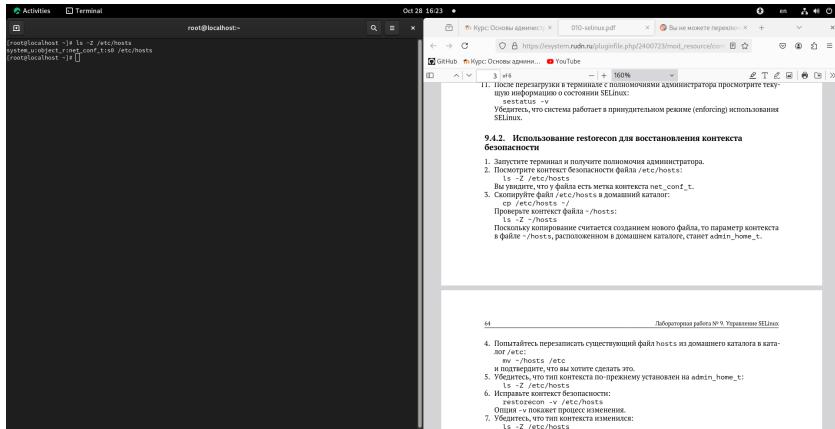


Рис. 3.13: контекст безопасности

и там я увидел что у файла есть метка контекста `net_conf_t`

Потом я скопировал то же файл в домашний каталог (рис. 3.14).

```
cp /etc/hosts ~/
```

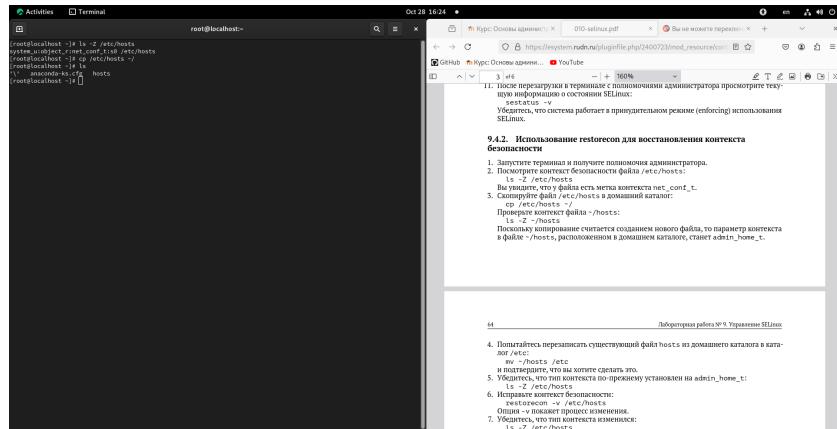


Рис. 3.14: копирование файла hosts

далше я проверил контекст файла (рис. 3.15).

```
ls -Z ~/hosts
```

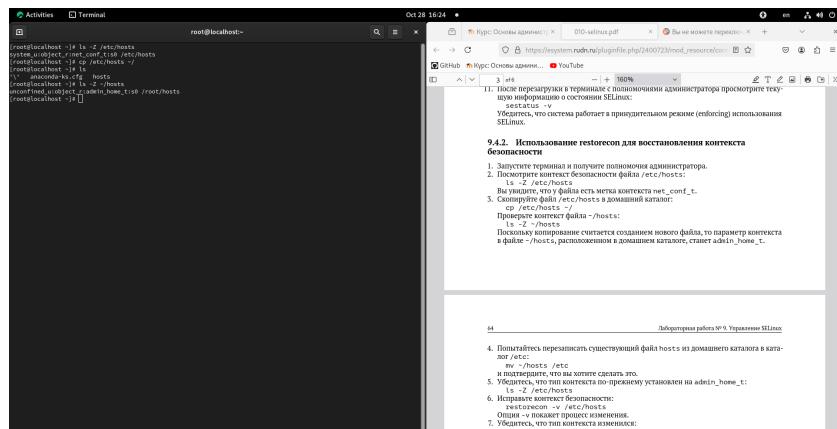


Рис. 3.15: контекст файла

там я смог увидет что контекст файла изменился. это произошло потому что файл скопирован в другой каталог(домашний каталог) и станет admin_home_t

Потом я перезаписал существующий файл hosts из домашнего каталога в каталог /etc (рис. 3.16).

```
mv ~hosts /etc  
yes
```

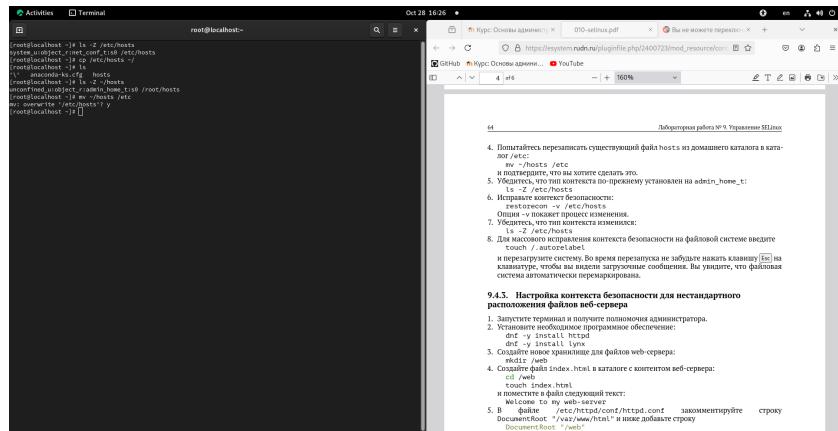


Рис. 3.16: перезапись файла hosts

Дальше я проверил тип контекста файла и он изменился на admin_home_t.

Чтобы исправить его я выполнил команду restorecon (рис. 3.17).

```
restorecon -v /etc/hosts
```

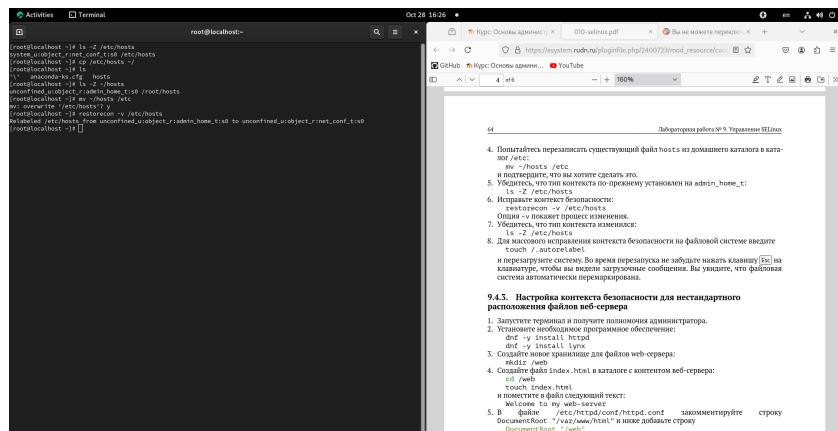


Рис. 3.17: исправление контекста файла hosts

И еще раз проверил его (рис. 3.18).

```
ls -Z /etc/hosts
```

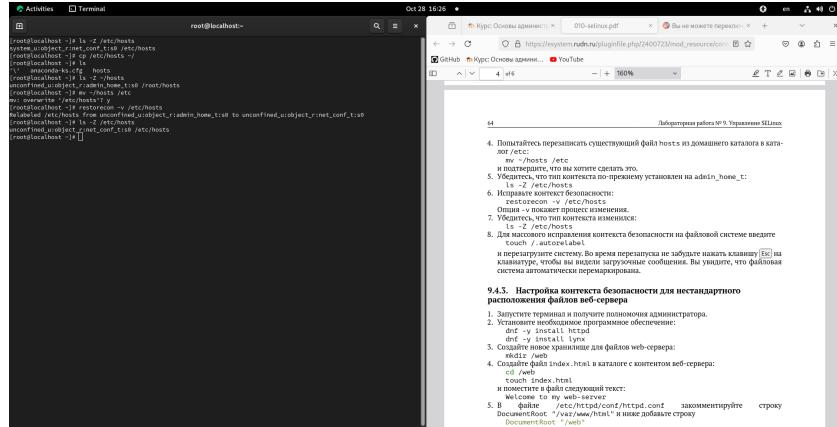


Рис. 3.18: проверка контекста

Потом для массового исправления контекста безопасности на файловой системе я выполнил создал файл `/.autorelabel` и перезагрузил систему (рис. 3.19).

```
touch /.autorelabel
```

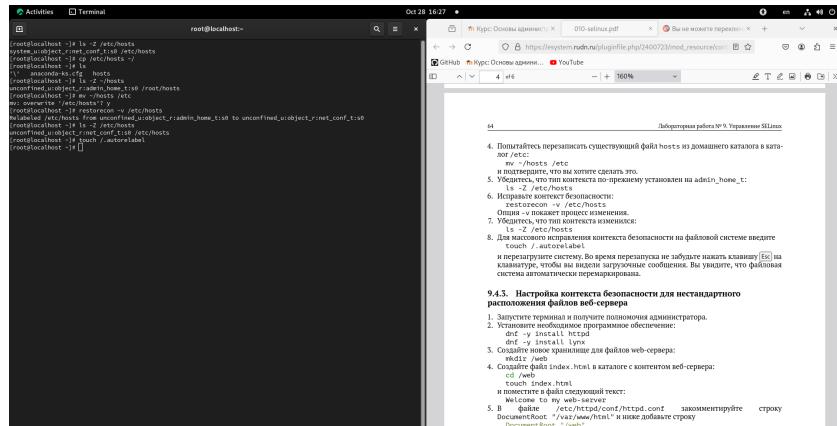


Рис. 3.19: создание файла для исправления контекста безопасности

3.3 настройка контекста безопасности для нестандартного расположения файлов веб-сервера

я еще раз открыл терминал и получил полномочия администратора (рис. 3.20).

SU -

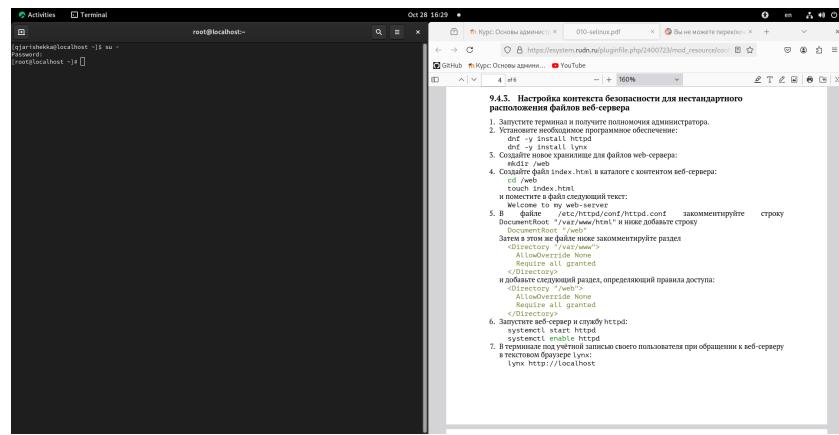


Рис. 3.20: терминал

Потом я установил два программного обеспечения (рис. 3.21) и (рис. 3.22).

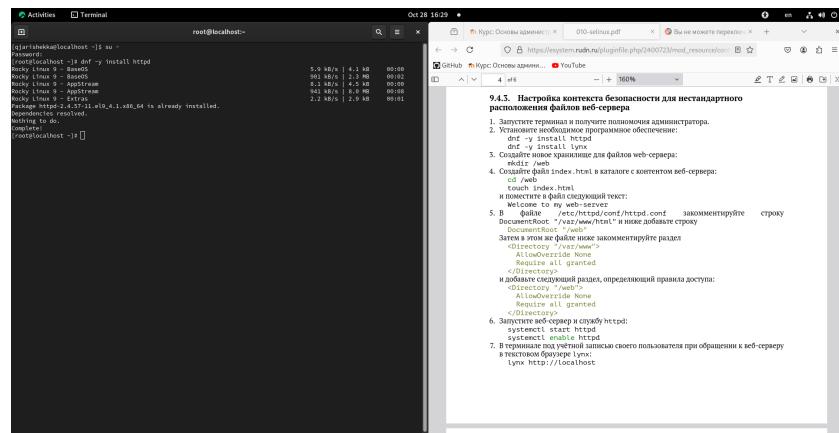


Рис. 3.21: установка httpd

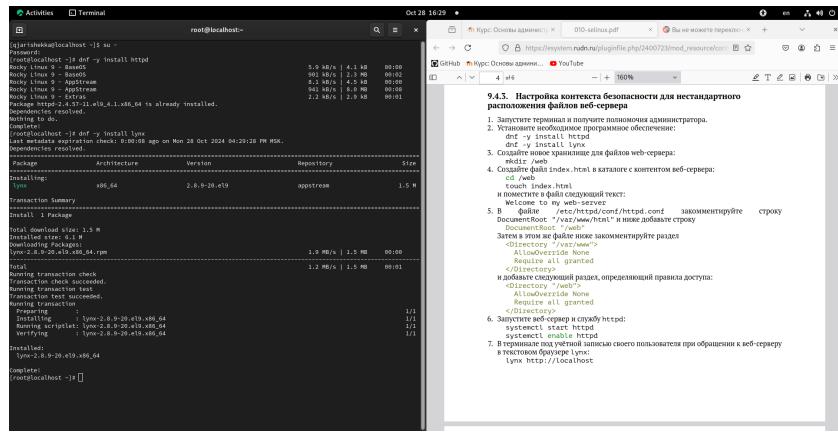


Рис. 3.22: установка lynx

Дальше я создал новое хранилище для файлов web-сервера (рис. 3.23).

```
mkdir /web
```

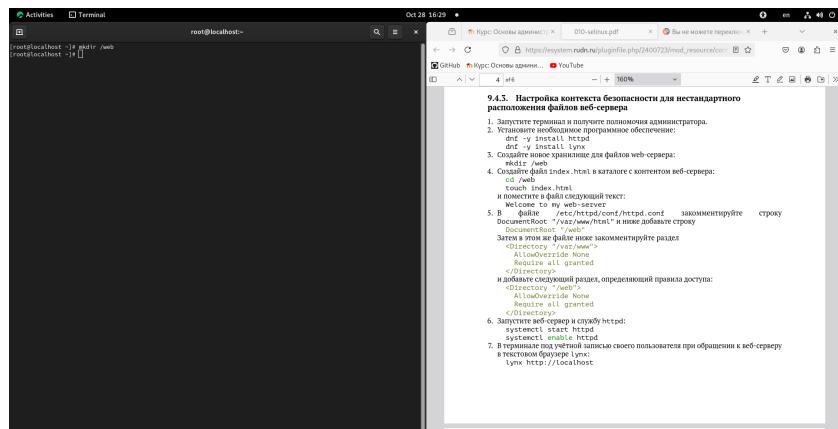


Рис. 3.23: создание каталога web

Потом я создал файл index.html и расположил его в каталоге web (рис. 3.24).

```
touch /web/index.html
```

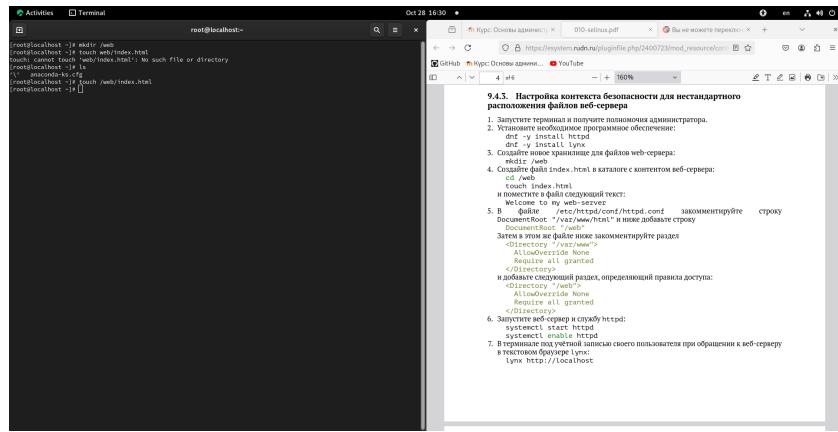


Рис. 3.24: файл index.html

Затем я добавил строку (рис. 3.25).

```
vim /web/index.html
```

Welcome to my web-server

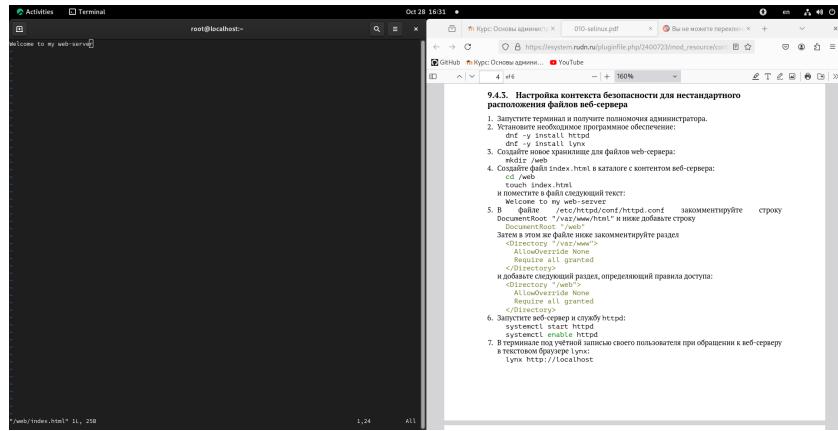


Рис. 3.25: добавление строки в файле index.html

Потом в файле /etc/httpd/conf/httpd.conf я изменил строки (рис. 3.26).

```
vim /etc/httpd/conf/httpd.conf
```

```
#DocumentRoot "/var/www/html"
```

```
#<Directory "/var/www">
#AllowOverride None
#Require all granted
#</Directory>
```

на

```
DocumentRoot "/web"
```

```
<Directory "/web">
AllowOverride None
Require all granted
</Directory>
```

:wq

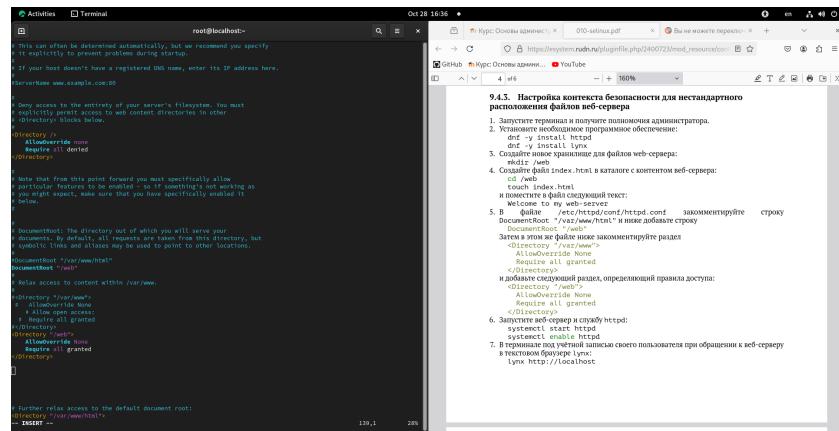


Рис. 3.26: изменение строк

Потом я запустил веб-сервер и службу httpd (рис. 3.27).

```
systemctl start httpd
systemctl enable httpd
```

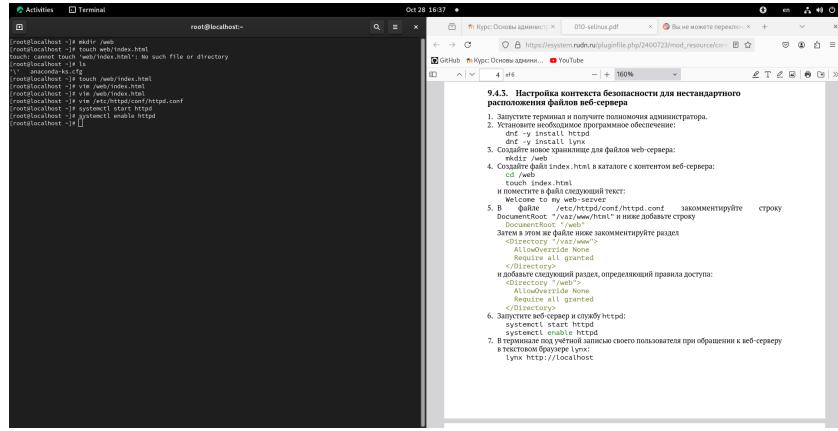


Рис. 3.27: запуск службы и веба-сервера

Затем в терминале я выполнил команду для запуск текстовой браузер lynx (рис. 3.28).

`lynx http://localhost`

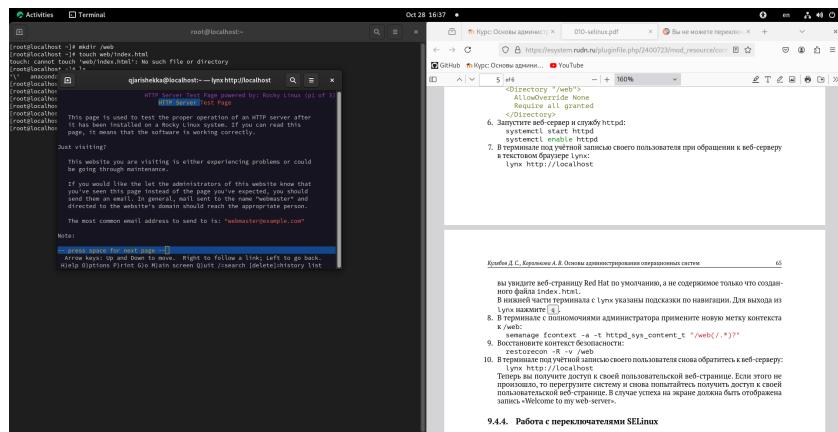


Рис. 3.28: текстовой браузер lynx

Но у меня не права доступа на сайт, поэтому я только закрыл браузер нажимая клавишу q и y (рис. 3.29).

q
y

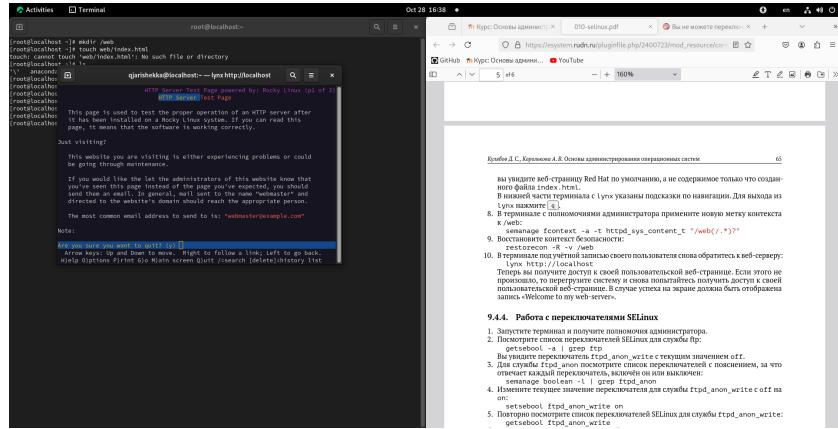


Рис. 3.29: закрытие браузера

Тогда я в терминале выполнил команду semanage чтобы изменить метку контекста каталога web (рис. 3.30).

```
semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
```

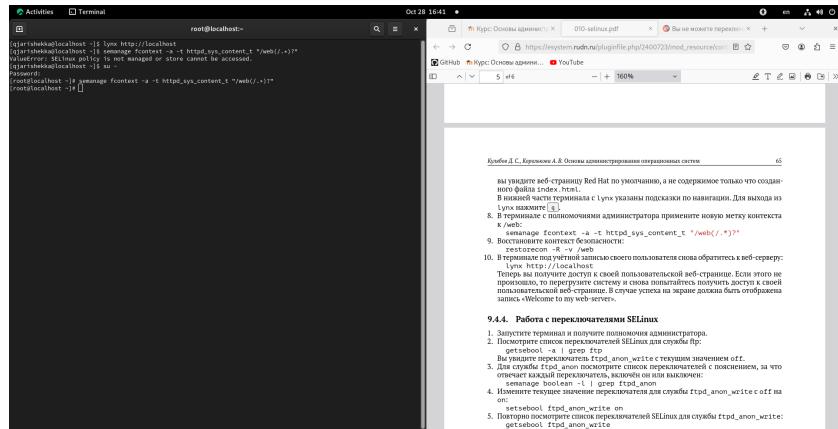


Рис. 3.30: semanage

и восстановил контекста безопасности (рис. 3.31).

```
restorecon -R -v /web
```

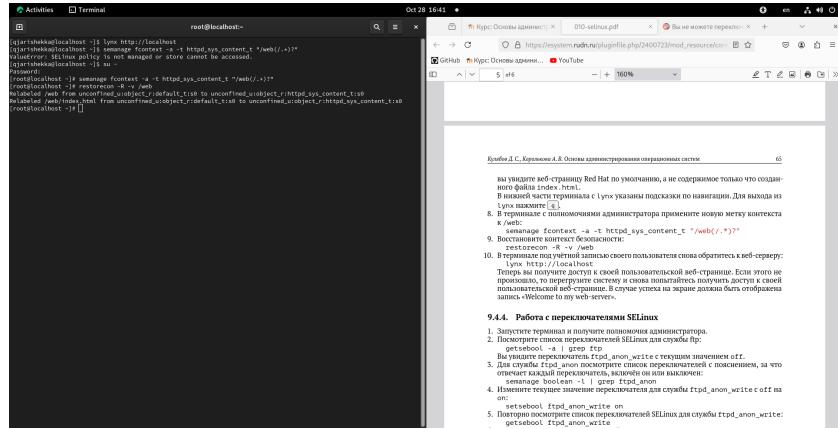


Рис. 3.31: восстановление контекста безопасности

И еще раз выполнил команду для запуска текстового браузера (рис. 3.32).

`lynx http://localhost`

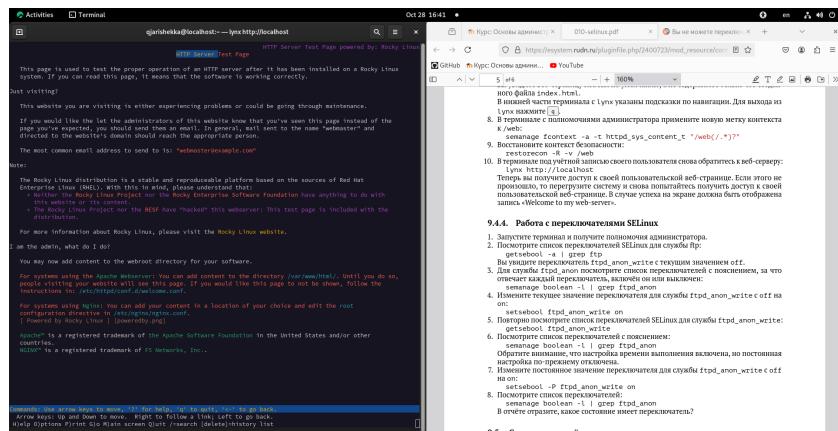


Рис. 3.32: текстовой браузер

у меня еще нет права доступа но после перезагрузки системы я снова выполнил ту же команду (рис. 3.33).

перезагрузка

`lynx http://localhost`

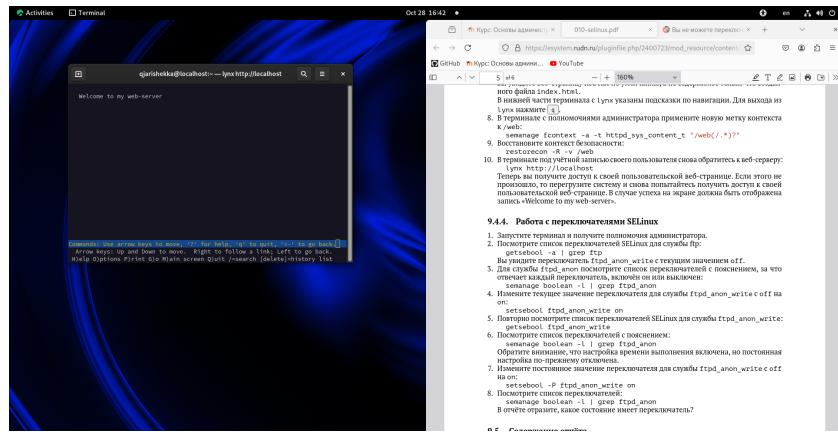


Рис. 3.33: lynx http://localhost

и там я смог смотреть то что я написал в файле index.html

3.4 Работа с переключателями SELinux

Еще раз в терминале под пользователем root я выполнил команду getsebool чтобы получить список переключателей SELinux для службы ftp (рис. 3.34).

`getsebool -a | grepftp`

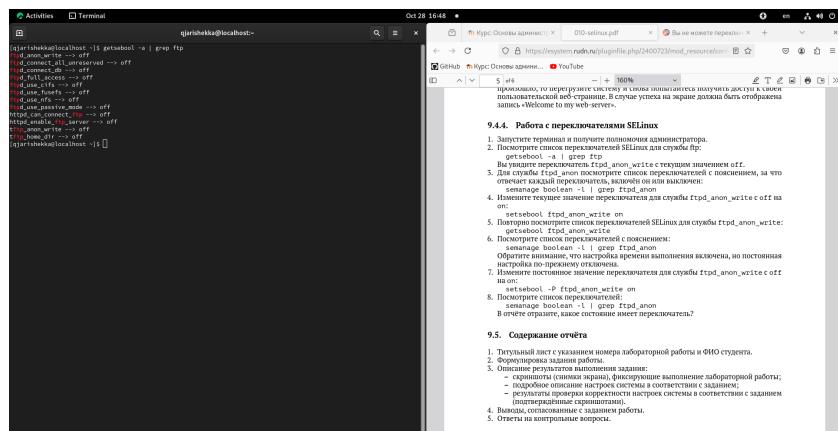


Рис. 3.34: getsebool

там у всех переключателей есть значение off

Потом я смотрел другой список переключателей чтобы смотреть за что отвечают и включён или выключен (рис. 3.35).

```
semanage boolean -l | grep ftpd_anon
```

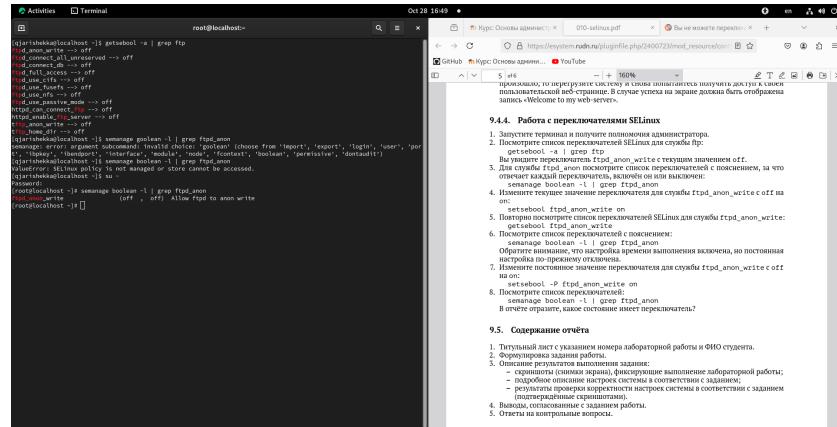


Рис. 3.35: список переключателей

дальше я изменил текущее значение для службы `ftpd_anon_write` с `off` на `on` (рис. 3.36).

```
setsebool ftpd_anon_write
```

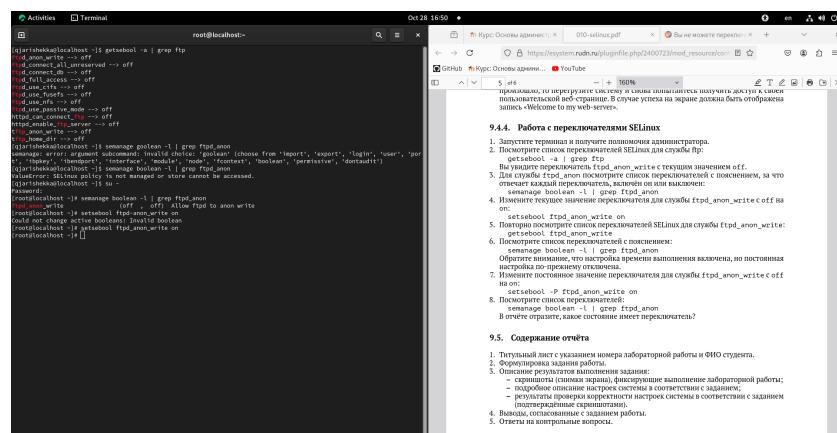


Рис. 3.36: изменение текущего значения переключателя

и еще раз смотрел список переключателей с пояснением (рис. 3.37).

```
semanage boolean -l | grep ftpd_anon
```

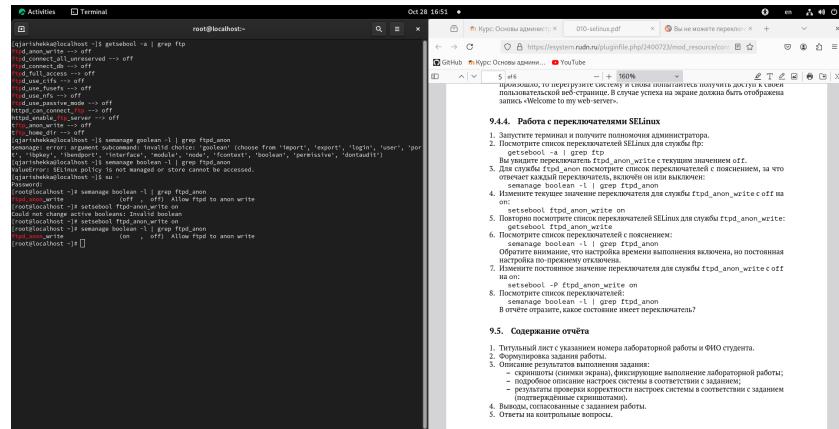


Рис. 3.37: список переключателей с пояснением

и там появилась та же служба, которую я изменил её значение. но настройка времени выполнения включена и постоянная настройка по-прежнему отключена.

чтобы исправить постоянное значение переключателя для службы `ftpd_anon_write` я использовал другую опцию (рис. 3.38).

```
setsebool -P ftpd_anon_write on
```

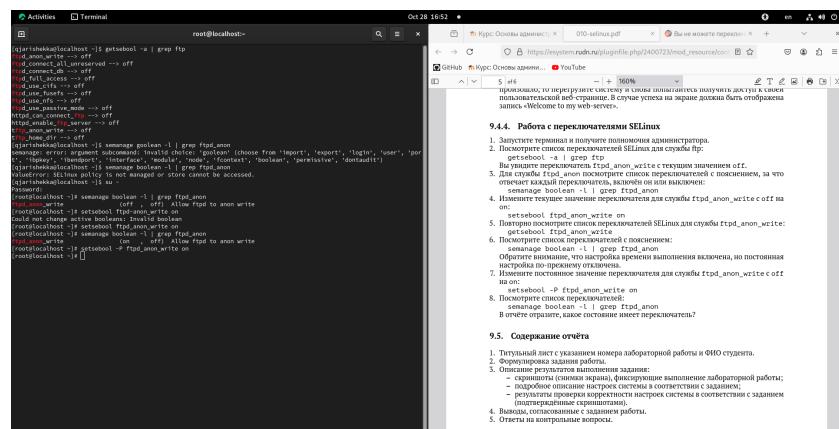


Рис. 3.38: изменить постоянное значение переключателя

и еще раз посмотрел список переключателей (рис. 3.39).

```
semanage boolean -l | grep ftpd_anon
```

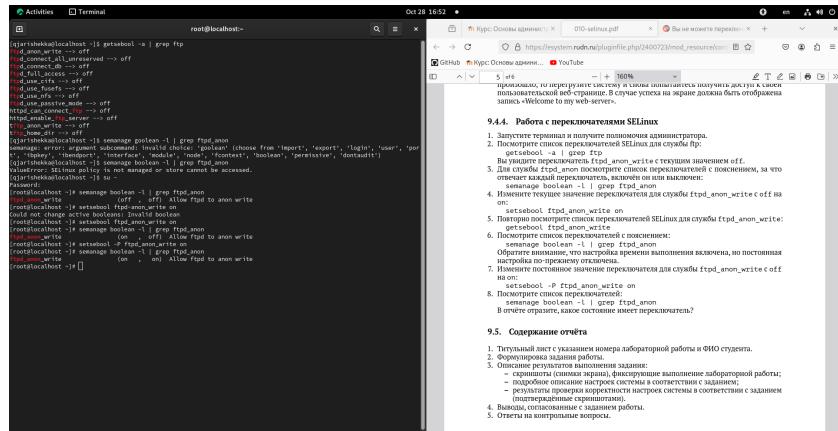


Рис. 3.39: список переключателей

Контрольные вопросы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?
2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?
3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?
4. Какие команды вам нужно выполнить, чтобы применить тип контекста httpd_sys_content_t к каталогу /web?
5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?
6. Где SELinux регистрирует все свои сообщения?
7. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию?

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?

4 Выводы

на эту лабораторную работу я смотрел работу контекстом безопасности и политиками SELinux, как они разрешают нас на ядер Linux и также как настройть его, также я смотрел переключатели SELinux и как изменить их значения

Список литературы