

Лабораторная работа №6

Мандатное разграничение прав в Linux

Кувшинова Ксения Олеговна¹

14.10.2022, Moscow

¹RUDN University, Moscow, Russian Federation

Целью данной лабораторной работы является развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Установили веб-сервер Apache. (fig. 1)

```
[root@kokuvshinova kokuvshinova]# yum install httpd
Rocky Linux 9 - BaseOS                               7.1 kB/s | 3.6 kB      00:00
Rocky Linux 9 - BaseOS                               1.7 MB/s | 1.7 MB      00:00
Rocky Linux 9 - AppStream                             6.9 kB/s | 3.6 kB      00:00
Rocky Linux 9 - AppStream                             3.2 MB/s | 6.0 MB      00:01
Rocky Linux 9 - Extras                               5.5 kB/s | 2.9 kB      00:00
Зависимости разрешены.
=====
Пакет                Архитектура Версия                Репозиторий    Размер
=====
Установка:
  httpd              x86_64      2.4.51-7.el9_0        appstream      1.4 M
Установка зависимостей:
```

Figure 1: Установка веб-сервера Apache

Подготовка лабораторного стенда

В конфигурационном файле `/etc/httpd/httpd.conf` задали параметр `ServerName`. (fig. 2)

```
[root@kokuvshinova kokuvshinova]# cd /etc/httpd  
[root@kokuvshinova httpd]# echo "ServerName test.ru" >> httpd.conf
```

Figure 2: Установка параметра `ServerName`

Отключаем пакетный фильтр. (fig. 3)

```
[root@kokuvshinova httpd]# iptables -F  
[root@kokuvshinova httpd]# iptables -P INPUT ACCEPT  
[root@kokuvshinova httpd]# iptables -P OUTPUT ACCEPT
```

Figure 3: Отключение пакетного фильтра

Выполнение лабораторной работы

Входим в систему с полученными учётными данными. Проверили, что SELinux работает в режиме enforcing политики targeted. (fig. 4)

```
[root@kokuvshinova ~]# cd  
[root@kokuvshinova ~]# getenforce  
Enforcing  
[root@kokuvshinova ~]# sestatus  
SELinux status:                enabled  
SELinuxfs mount:               /sys/fs/selinux  
SELinux root directory:        /etc/selinux  
Loaded policy name:             targeted  
Current mode:                   enforcing  
Mode from config file:          enforcing  
Policy MLS status:              enabled  
Policy deny_unknown status:     allowed  
Memory protection checking:     actual (secure)  
Max kernel policy version:      33  
[root@kokuvshinova ~]#
```

Figure 4: Выполнение команд getenforce и sestatus

Выполнение лабораторной работы

Запустили веб-сервер и обратились к нему (fig. 5)

```
[root@kokuvshinova etc]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@kokuvshinova etc]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-10-10 17:09:27 MSK; 10s ago
     Docs: man:httpd.service(8)
  Main PID: 39619 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/>>
    Tasks: 213 (limit: 12210)
   Memory: 26.2M
      CPU: 95ms
   CGroup: /system.slice/httpd.service
           └─39619 /usr/sbin/httpd -DFOREGROUND
             └─39620 /usr/sbin/httpd -DFOREGROUND
               └─39624 /usr/sbin/httpd -DFOREGROUND
                 └─39625 /usr/sbin/httpd -DFOREGROUND
                   └─39626 /usr/sbin/httpd -DFOREGROUND

окт 10 17:09:27 kokuvshinova.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 10 17:09:27 kokuvshinova.localdomain systemd[1]: Started The Apache HTTP Server.
окт 10 17:09:27 kokuvshinova.localdomain httpd[39619]: Server configured, listening on:
[root@kokuvshinova etc]#
```

Figure 5: Выполнение команд service httpd start и status

Выполнение лабораторной работы

Найшли веб-сервер Apache в списке процессов. Контекст безопасности - `unconfined_u:unconfined_r:unconfined_t`. (fig. 6)

```
[root@kokuvshinova ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0  root      39619  0.0  0.5  20248 11704 ?        Ss   17:09
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  39620  0.0  0.3  21572  7444 ?        S    17:09
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  39624  0.0  0.5 1079376 11100 ?        Sl   17:09
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  39625  0.0  0.6 1210512 13148 ?        Sl   17:09
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  39626  0.0  0.5 1079376 11100 ?        Sl   17:09
0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 40041 0.0  0.1 221692 2292 pts/0 S
+ 17:30  0:00 grep --color=auto httpd
```

Figure 6: Выполнение команды `ps auxZ | grep httpd`

Выполнение лабораторной работы

Посмотрели текущее состояние переключателей SELinux для Apache.
(fig. 7)

```
[root@kokuvshinova ~]# sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
httpd_can_connect_ldap off
httpd_can_connect_mythtv off
httpd_can_connect_zabbix off
httpd_can_manage_courier_spool off
httpd_can_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
httpd_graceful_shutdown off
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssi_exec off
```


Выполнение лабораторной работы

Посмотрели статистику по политике. Определили, что множество пользователей = 8; ролей = 14; типов = 5002. (fig. 8)

```
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:                  133      Permissions:              454
Sensitivities:            1        Categories:              1024
Types:                    5002     Attributes:               254
Users:                    8         Roles:                    14
Booleans:                 347      Cond. Expr.:             381
Allow:                    63996    Neverallow:               0
Auditallow:               168      Dontaudit:               8417
Type_trans:               258486   Type_change:              87
Type_member:              35       Range_trans:             5960
Role_allow:               38       Role_trans:              420
Constraints:              72       Validatetrans:           0
MLS Constrain:            72       MLS Val. Tran:           0
Permissives:              0        Polcap:                  5
Defaults:                 7        Typebounds:              0
Allowxperm:               0        Neverallowxperm:         0
Auditallowxperm:          0        Dontauditxperm:          0
```

Определили тип файлов и поддиректорий, находящихся в директории /var/www. (fig. 9)

```
[root@kokuvshinova ~]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 16 15:10 html
[root@kokuvshinova ~]#
```

Figure 9: Выполнение команды `ls -lZ /var/www`

Необходимо было определить тип файлов, находящихся в директории /var/www/html. Но в данной директории файлов не обнаружилось. (fig. 10)

A terminal window with a black background and white text. The prompt is [root@kokuvshinova ~]#. The command entered is ls -lZ /var/www/html. The output shown is Итого 0. There is some faint, illegible text visible in the background of the terminal window.

```
[root@kokuvshinova ~]# ls -lZ /var/www/html
Итого 0
```

Figure 10: Выполнение команды `ls -lZ /var/www/html`

Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html. (fig. 11)

```
[root@kokuvshinova ~]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 16 15:10 html
[root@kokuvshinova ~]#
```

Figure 11: Выполнение команды `ls -lZ /var/www`

Создали от имени суперпользователя html-файл
/var/www/html/test.html следующего содержания: (fig. 12)

A screenshot of a code editor window. The title bar at the top shows 'test.html' and the path '/var/www/html'. Below the title bar, there is a toolbar with a button labeled 'Открыть' (Open) and a plus icon. The main area of the editor contains three lines of HTML code:

```
1 <html>  
2 <body> test </body>  
3 </html>
```

Figure 12: Содержимое файла test.html

Проверили контекст созданного файла - httpd_sys_content_t. (fig. 13)

```
[root@kokuvshinova ~]# ls -lZ /var/www/html/test.html  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 35 окт 10 17:37 /var/www/html/test.html  
[root@kokuvshinova ~]#
```

Figure 13: Контекст файла test.html

Выполнение лабораторной работы

Обратились к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html` и убедились, что файл был успешно отображён. (fig. 14)

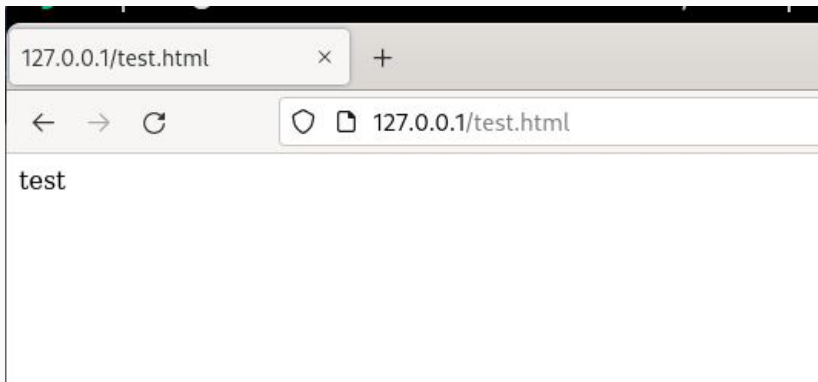


Figure 14: Обращение к файлу test.html через веб-сервер

Изменили контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`(fig. 15)

```
[root@kokuvshinova ~]# chcon -t samba_share_t /var/www/html/test.html
[root@kokuvshinova ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@kokuvshinova ~]#
```

Figure 15: Изменение контекста файла `/var/www/html/test.html`

Пробуем ещё раз получить доступ к файлу через веб-сервер. (fig. 16)

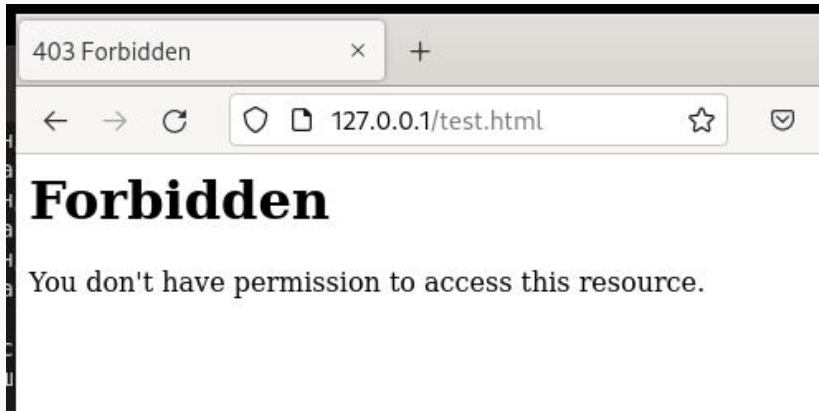


Figure 16: Обращение к файлу test.html через веб-сервер после изменения контекста

Выполнение лабораторной работы

Проанализируем ситуацию. Просмотрим log-файлы веб-сервера Apache и системный лог-файл. В системе оказались запущенны процессы `setroubleshootd` и `audtd`. (fig. 17)

```
iroot@kokushinova ~]# ls -l /var/www/html/test.html
-rw-r--r-- 1 root root 35 oct 10 17:37 /var/www/html/test.html
iroot@kokushinova ~]# tail /var/log/messages
Oct 10 17:43:03 kokushinova setroubleshoot[40846]: SELinux запечатлел /usr/sbin/httpd доступ getattr к файлу /var/www/html/test.html.#012#012*****
Модуль restorecon предупреждает (точность 92.2) *****#012#012Если вы хотите исправить метку STARGETзнак PATH по умолчанию должен
быть httpd_sys_content_t#012#012вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для досту
па к родительскому каталогу, и в этом случае пожалуйста, соответствующим образом измените следующую команду.#012#012catna#012#012$ /sbin/restorecon -v /v
ar/www/html/test.html#012#012***** Модуль public content предупреждает (точность 7.83) *****#012#012Если вы хотите лечить test.html
как ожидаемый контент#012#012вам необходимо изменить метку test.html с public content_t на public content_rw_t.#012#012catna#012#012$ semanage fcontext -a
-t public content_t /var/www/html/test.html.#012#012$ restorecon -v /var/www/html/test.html.#012#012***** Модуль catchall предупреждает (точность 1.41
) *****#012#012Если вы считаете, что httpd должен быть разрешено getattr доступ к test.html file по умолчанию.#012#012$ recomen
дуется создать отчет об анализе.#012#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012#012catna#012#012$ разрешить этот доступ сейчас, вы
полнив:#012#012$ ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012#012$ semodule -X 300 -i my-httpd.pp#012
Oct 10 17:43:03 kokushinova setroubleshoot[40846]: SELinux запечатлел /usr/sbin/httpd доступ getattr к файлу /var/www/html/test.html. Две выполнения
теск сообщения SELinux: sealert -i d6b233c3-d9b8-408f-8900-5340b72246c2
Oct 10 17:43:03 kokushinova setroubleshoot[40846]: SELinux запечатлел /usr/sbin/httpd доступ getattr к файлу /var/www/html/test.html.#012#012*****
Модуль restorecon предупреждает (точность 92.2) *****#012#012Если вы хотите исправить метку STARGETзнак PATH по умолчанию должен
быть httpd_sys_content_t#012#012вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для досту
па к родительскому каталогу, и в этом случае пожалуйста, соответствующим образом измените следующую команду.#012#012catna#012#012$ /sbin/restorecon -v /v
ar/www/html/test.html#012#012***** Модуль public content предупреждает (точность 7.83) *****#012#012Если вы хотите лечить test.html
как ожидаемый контент#012#012вам необходимо изменить метку test.html с public content_t на public content_rw_t.#012#012catna#012#012$ semanage fcontext -a
-t public content_t /var/www/html/test.html.#012#012$ restorecon -v /var/www/html/test.html.#012#012***** Модуль catchall предупреждает (точность 1.41
) *****#012#012Если вы считаете, что httpd должен быть разрешено getattr доступ к test.html file по умолчанию.#012#012$ recomen
дуется создать отчет об анализе.#012#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012#012catna#012#012$ разрешить этот доступ сейчас, вы
полнив:#012#012$ ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012#012$ semodule -X 300 -i my-httpd.pp#012
Oct 10 17:43:13 kokushinova systemd[1]: dbus-1.10-org.fedoraproject.SetroubleshootPrivileged@0.service: Main process exited, code=killed, status=
14/ALRM
Oct 10 17:43:13 kokushinova systemd[1]: dbus-1.10-org.fedoraproject.SetroubleshootPrivileged@0.service: Failed with result 'signal'.
Oct 10 17:43:13 kokushinova systemd[1]: dbus-1.10-org.fedoraproject.Setroubleshoot@0.service: Consumed 2.230s CPU time.
Oct 10 17:43:13 kokushinova systemd[1]: dbus-1.10-org.fedoraproject.Setroubleshoot@0.service: Main process exited, code=killed, status=14/ALRM
Oct 10 17:43:13 kokushinova systemd[1]: dbus-1.10-org.fedoraproject.Setroubleshoot@0.service: Failed with result 'signal'.
Oct 10 17:43:13 kokushinova systemd[1]: dbus-1.10-org.fedoraproject.Setroubleshoot@0.service: Consumed 1.670s CPU time.
iroot@kokushinova ~]#
```

Figure 17: Вывод команд `ls -l /var/www/html/test.html` и `tail /var/log/messages`

Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле `/etc/httpd/httpd.conf` заменяем строчку на `Listen 81`. (fig. 18)



```
44 # page for more information.
45 #
46 #Listen 12.34.56.78:80
47 Listen 81
48
49 #
50 # Dynamic Shared Object (DSO) Support
51 #
52 # To be able to use the functionality of a module which was built as a
```

Figure 18: Запуск веб-сервера Apache на прослушивание TCP-порта 81

Выполним перезапуск веб-сервера Apache. Проанализируем лог-файлы.(fig. 19)

```
[root@kokuvshinova conf]# systemctl restart httpd
[root@kokuvshinova conf]# tail -n1 /var/log/messages
Oct 10 17:50:15 kokuvshinova httpd[41216]: Server configured, listening on: port 81
[root@kokuvshinova conf]# tail -n3 /var/log/httpd/error_log
```

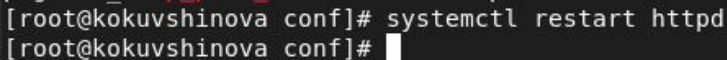
Figure 19: Перезапуск веб-сервера Apache

Определим 81 порт tcp. После этого проверим список портов. (fig. 20)

```
[root@kokuvshinova conf]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@kokuvshinova conf]# semanage port -l | grep http_port_t
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
```

Figure 20: Проверка установления 81 порта tcp

Попробуем запустить веб-сервер Apache ещё раз. (fig. 21)

A terminal window with a black background and white text. The prompt is [root@kokuvshinova conf]#. The command systemctl restart httpd has been entered. The prompt is now [root@kokuvshinova conf]# followed by a white cursor block.

```
[root@kokuvshinova conf]# systemctl restart httpd  
[root@kokuvshinova conf]#
```

Figure 21: Перезапуск веб-сервера Apache

Вернули контекст `httpd_sys_content__t` к файлу
`/var/www/html/test.html`.(fig. 22)

```
[root@kokuvshinova conf]# systemctl restart httpd
[root@kokuvshinova conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@kokuvshinova conf]# ls -Z /var/www/
cgi-bin/ html/
[root@kokuvshinova conf]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@kokuvshinova conf]#
```

Figure 22: Возвращение контекста `httpd_sys_content__t` к файлу `test.html`

Выполнение лабораторной работы

После этого пробуем получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. (fig. 23)

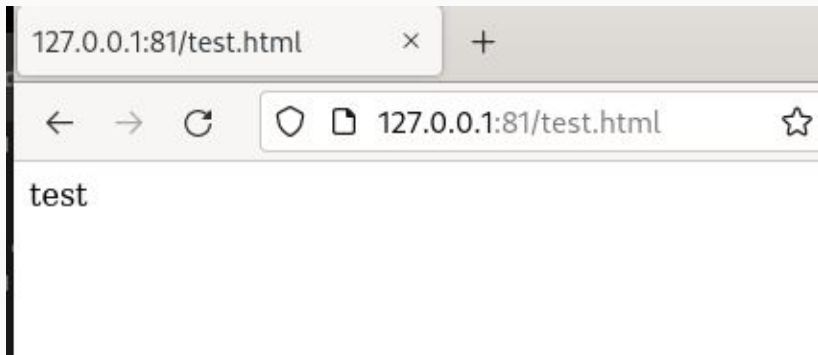
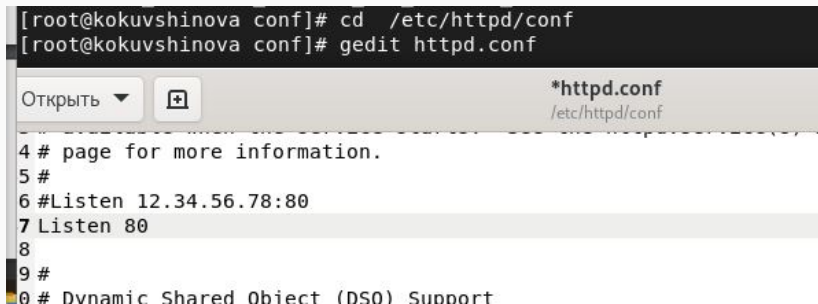


Figure 23: Обращение к файлу test.html через веб-сервер

Выполнение лабораторной работы

Исправим обратно конфигурационный файл apache, вернув Listen 80.
(fig. 24)



The image shows a terminal window at the top with the following commands:

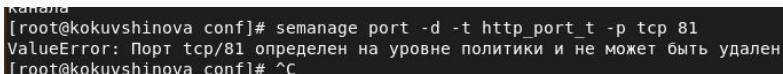
```
[root@kokuvshinova conf]# cd /etc/httpd/conf
[root@kokuvshinova conf]# gedit httpd.conf
```

Below the terminal is a window of the gedit text editor. The title bar shows "Открыть" (Open) and a file icon. The file name is "*httpd.conf" and the path is "/etc/httpd/conf". The editor content shows the following lines:

```
4 # page for more information.
5 #
6 #Listen 12.34.56.78:80
7 Listen 80
8
9 #
10 # Dynamic Shared Object (DSO) Support
```

Figure 24: Исправление конфигурационного файла apache

Удалим привязку http_port_t к 81 порту. (fig. 25)



```
kanala  
[root@kokuvshinova conf]# semanage port -d -t http_port_t -p tcp 81  
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален  
[root@kokuvshinova conf]# ^C
```

Figure 25: Удаление привязки http_port_t к 81 порту

Удалим файл /var/www/html/test.html. (fig. 26)



```
[root@kokuvshinova conf]# rm /var/www/html/test.html  
rm: удалить обычный файл '/var/www/html/test.html'? y
```

Figure 26: Удаление файла test.html

В ходе выполнения лабораторной работы мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux¹. Проверили работу SELinux на практике совместно с веб-сервером Apache.

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Мандатное разграничение прав в Linux [Текст] / Кулябов Д. С., Королькова А. В., Геворкян М. Н. - Москва: - 5 с. [^1]: Мандатное разграничение прав в Linux.
2. Справочник 70 основных команд Linux: полное описание с примерами (<https://eternalhost.net/blog/sozдание-saytov/osnovnye-komandy-linux>)