

Отчет по лабораторной работе № 2. Дискреционное разграничение прав в Linux. Основные атрибуты

дисциплина: Информационная безопасность

Смирнова Мария Александровна

Содержание

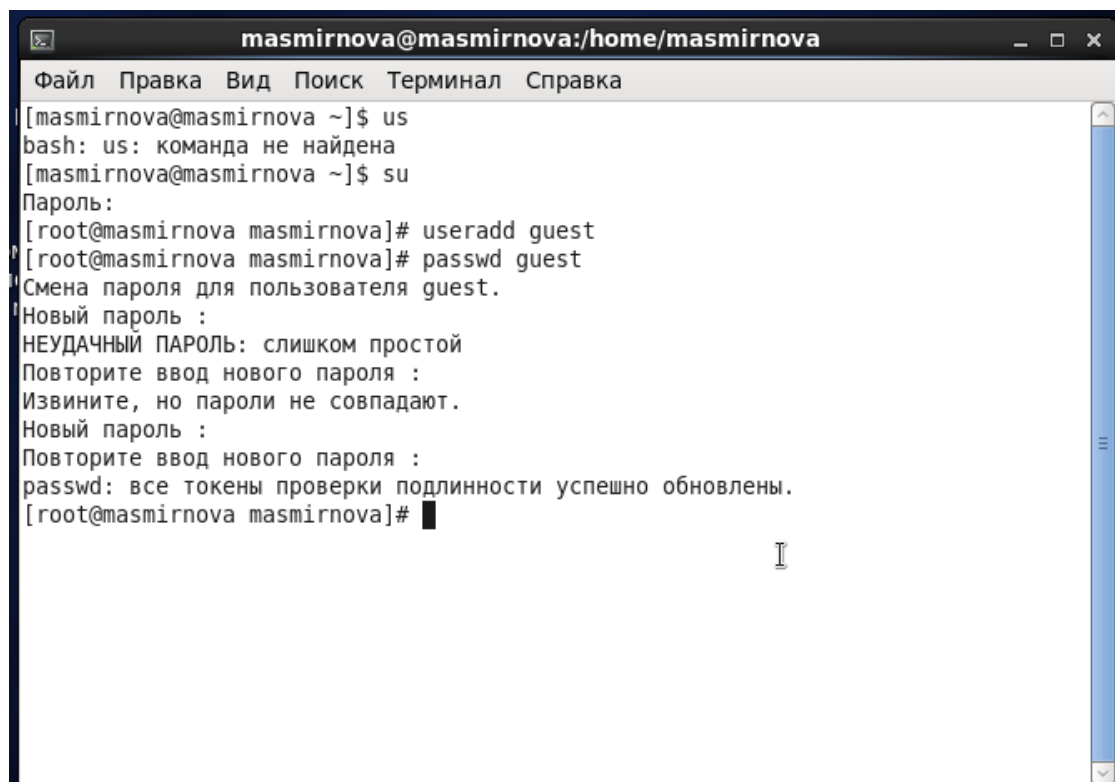
Цель работы	1
Выполнение лабораторной работы.....	1
Выводы	14

Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Выполнение лабораторной работы

1. Используя учетную запись администратора, создадим нового пользователя guest (useradd guest) и зададим ему пароль (passwd guest) (рис. -@fig:001).

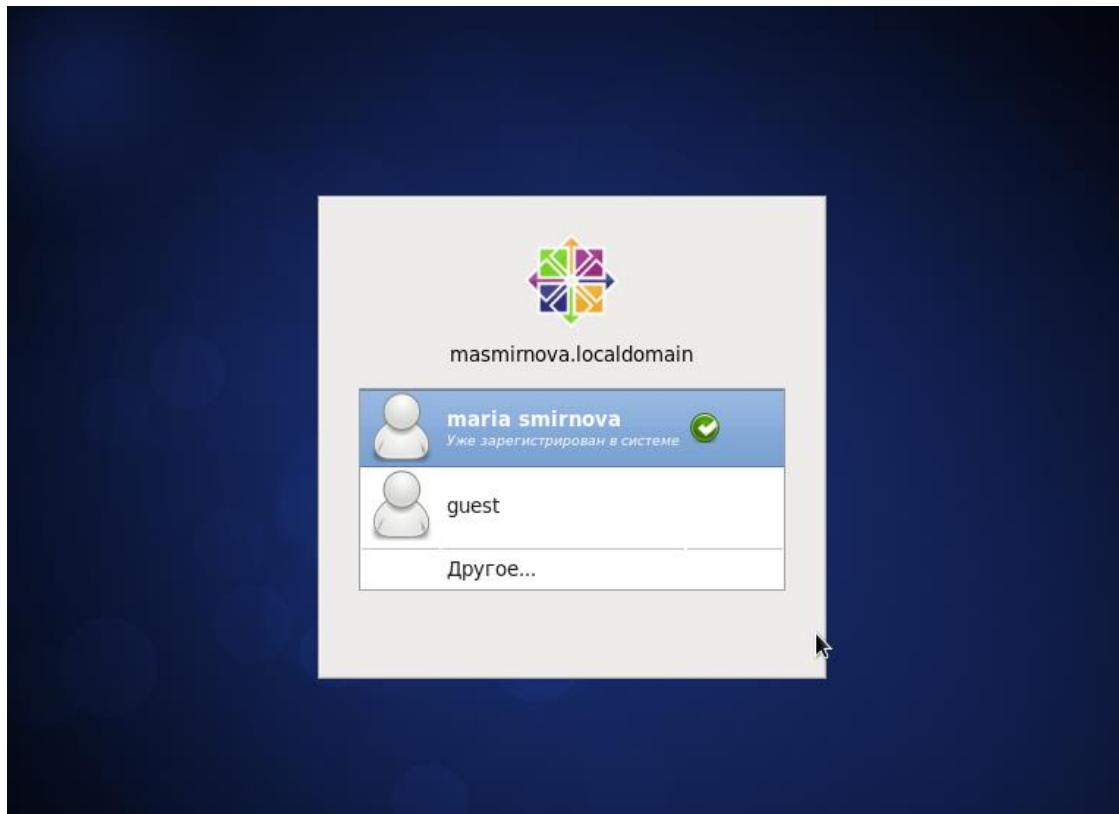


The image shows a terminal window titled "masmirnova@masmirnova:/home/masmirnova". The window has a menu bar with "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The terminal content shows the following sequence of commands and outputs:

```
[masmirnova@masmirnova ~]$ us
bash: us: команда не найдена
[masmirnova@masmirnova ~]$ su
Пароль:
[root@masmirnova masmirnova]# useradd guest
[root@masmirnova masmirnova]# passwd guest
Смена пароля для пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой
Повторите ввод нового пароля :
Извините, но пароли не совпадают.
Новый пароль :
Повторите ввод нового пароля :
passwd: все токены проверки подлинности успешно обновлены.
[root@masmirnova masmirnova]#
```

Добавление нового пользователя

2. Войдем в систему от имени пользователя guest (рис. -@fig:002).



Вход в систему

3. С помощью команды `pwd` убедимся, что мы находимся в домашней директории. Уточним имя пользователя - `guest` - с помощью команды `whoami`. Посмотрим на группы, в которые входит пользователь командой `id`. Значения `uid` и `gid` равны 501. Вывод команды `id` совпадает с выводом команды `groups` (рис. -@fig:003).

```
guest@masmirnova:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@masmirnova ~]$ pwd  
/home/guest  
[guest@masmirnova ~]$ whoiam  
bash: whoiam: команда не найдена  
[guest@masmirnova ~]$ whoami  
guest  
[guest@masmirnova ~]$ id  
uid=501(guest) gid=501(guest) группы=501(guest) контекст=unconfined_u:unconfined_r:unconfined_t  
:s0-s0:c0.c1023  
[guest@masmirnova ~]$ groups  
guest  
[guest@masmirnova ~]$
```

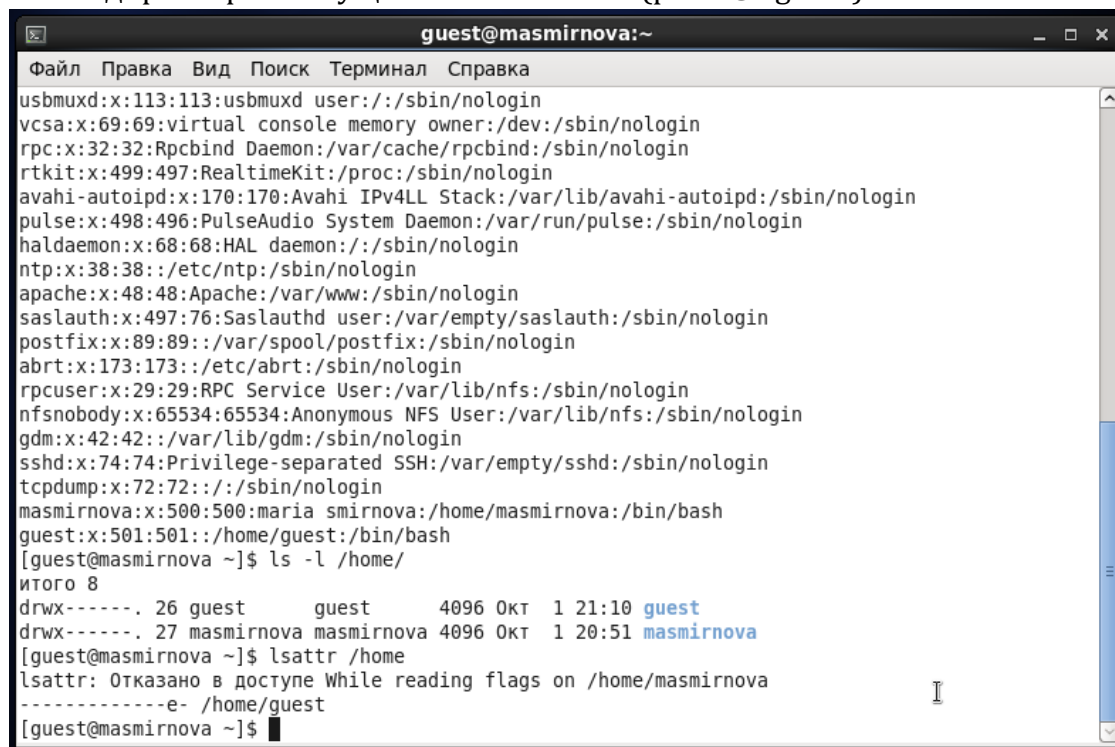
Сведения о пользователе

4. Просмотрим файл `/etc/passwd`. Uid и gid пользователя совпадают с полученными ранее (рис. -@fig:004).

```
guest@masmirnova:~  
Файл Правка Вид Поиск Терминал Справка  
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin  
games:x:12:100:games:/usr/games:/sbin/nologin  
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
nobody:x:99:99:Nobody:./:/sbin/nologin  
dbus:x:81:81:System message bus:./:/sbin/nologin  
usbmuxd:x:113:113:usbmuxd user:./:/sbin/nologin  
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin  
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin  
rtkit:x:499:497:RealtimeKit:/proc:/sbin/nologin  
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin  
pulse:x:498:496:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
haldaemon:x:68:68:HAL daemon:./:/sbin/nologin  
ntp:x:38:38:./etc/ntp:/sbin/nologin  
apache:x:48:48:Apache:/var/www:/sbin/nologin  
saslauth:x:497:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin  
postfix:x:89:89:./var/spool/postfix:/sbin/nologin  
abrt:x:173:173:./etc/abrt:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin  
gdm:x:42:42:./var/lib/gdm:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin  
tcpdump:x:72:72:./:/sbin/nologin  
masmirnova:x:500:500:masmirnova:/home/masmirnova:/bin/bash  
guest:x:501:501:./home/guest:/bin/bash  
[guest@masmirnova ~]$
```

Файл `/etc/passwd`

5. Посмотрим директории в системе. Нам удалось получить список директорий пользователей masmirnova и guest. У них есть права юзера на чтение, изменение и запуск. Проверим какие расширенные атрибуты установлены на поддиректориях. Нам удалось увидеть расширенные атрибуты только директории текущего пользователя (рис. -@fig:005).



```
guest@masmirnova:~  
Файл Правка Вид Поиск Терминал Справка  
usbmuxd:x:113:113:usbmuxd user:/sbin/nologin  
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin  
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin  
rtkit:x:499:497:RealtimeKit:/proc:/sbin/nologin  
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin  
pulse:x:498:496:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
haldaemon:x:68:68:HAL daemon:/sbin/nologin  
ntp:x:38:38::/etc/ntp:/sbin/nologin  
apache:x:48:48:Apache:/var/www:/sbin/nologin  
sasauth:x:497:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin  
postfix:x:89:89::/var/spool/postfix:/sbin/nologin  
abrt:x:173:173::/etc/abrt:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin  
gdm:x:42:42::/var/lib/gdm:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
tcpdump:x:72:72::/sbin/nologin  
masmirnova:x:500:500:masmirnova:/home/masmirnova:/bin/bash  
guest:x:501:501::/home/guest:/bin/bash  
[guest@masmirnova ~]$ ls -l /home/  
итого 8  
drwx-----. 26 guest      guest      4096 Окт  1 21:10 guest  
drwx-----. 27 masmirnova masmirnova 4096 Окт  1 20:51 masmirnova  
[guest@masmirnova ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/masmirnova  
-----e- /home/guest  
[guest@masmirnova ~]$
```

Права и расширенные атрибуты

6. Создадим в домашней директории поддиректорию dir1. Посмотрим на права доступа у каталога dir1 - чтение и запуск для всех пользователей и изменения для всех, кроме остальных пользователей. Командой lsattr посмотрим на расширенные атрибуты (рис. -@fig:006)

```
guest@masmirnova:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@masmirnova ~]$ ls -l dir1/  
итого 0  
[guest@masmirnova ~]$ lsattr dir1  
[guest@masmirnova ~]$ ls  
dir1 Видео Документы Загрузки Картинки Музыка Общедоступные Рабочий стол Шаблоны  
[guest@masmirnova ~]$ ls -l  
итого 36  
drwxrwxr-x. 2 guest guest 4096 Окт 1 21:16 dir1  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Видео  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Документы  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Загрузки  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Картинки  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Музыка  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Общедоступные  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Рабочий стол  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Шаблоны  
[guest@masmirnova ~]$ lsattr  
-----e- ./Рабочий стол  
-----e- ./dir1  
-----e- ./Картинки  
-----e- ./Шаблоны  
-----e- ./Общедоступные  
-----e- ./Документы  
-----e- ./Музыка  
-----e- ./Видео  
-----e- ./Загрузки  
[guest@masmirnova ~]$
```

Директория /home/dir1

7. Снимем с директории все атрибуты командой `chmod`. Проверим, что все права сняты. Попробуем создать в ней файл и увидим, что мы получили отказ из-за отсутствия прав доступа. Видим, что файл не создан. (рис. -@fig:007)

```
guest@masmirnova:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@masmirnova ~]$ chmod 000 dir1  
[guest@masmirnova ~]$ ls -l  
итого 36  
d----- . 2 guest guest 4096 Окт 1 21:16 dir1  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Видео  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Документы  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Загрузки  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Картинки  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Музыка  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Общедоступные  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Рабочий стол  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Шаблоны  
[guest@masmirnova ~]$ lsattr  
-----e- ./Рабочий стол  
lsattr: Отказано в доступе While reading flags on ./dir1  
-----e- ./Картинки  
-----e- ./Шаблоны  
-----e- ./Общедоступные  
-----e- ./Документы  
-----e- ./Музыка  
-----e- ./Видео  
-----e- ./Загрузки  
[guest@masmirnova ~]$ echo "test1" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@masmirnova ~]$ ls -l /home/guest/dir1  
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе  
[guest@masmirnova ~]$
```

Снятие прав у директории

8. Вернем директории необходимые права и убедимся, что теперь файл создался (рис. -@fig:008)

```
guest@masmirnova:~  
Файл Правка Вид Поиск Терминал Справка  
-----e- ./Загрузки  
[guest@masmirnova ~]$ echo "test1" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@masmirnova ~]$ ls -l /home/guest/dir1  
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе  
[guest@masmirnova ~]$ chmod 600 dir1  
[guest@masmirnova ~]$ echo "test1" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@masmirnova ~]$ ls -l  
итого 36  
drw----- . 2 guest guest 4096 Окт 1 21:16 dir1  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Видео  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Документы  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Загрузки  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Картинки  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Музыка  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Общедоступные  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Рабочий стол  
drwxr-xr-x. 2 guest guest 4096 Окт 1 21:10 Шаблоны  
[guest@masmirnova ~]$ cd dir1  
bash: cd: dir1: Отказано в доступе  
[guest@masmirnova ~]$ chmod 700 dir1  
[guest@masmirnova ~]$ echo "test1" > /home/guest/dir1/file1  
[guest@masmirnova ~]$ cd dir1  
[guest@masmirnova dir1]$ ls  
file1  
[guest@masmirnova dir1]$
```

Возвращение прав директории

9. Заполним таблицу “Установленные права” опытным путем (рис. -@fig:009, -@fig:010, -@fig:011,-@fig:012, -@fig:013, -@fig:014, -@fig:015).

Права директории	Права файла	Создания файла	Удаление файла	Запись в файл
000	000	-	-	-
000	100	-	-	-
000	200	-	-	-
000	300	-	-	-
000	400	-	-	-
000	500	-	-	-
000	600	-	-	-
000	700	-	-	-
100	000	-	-	-
100	100	-	-	-
100	200	-	-	+
100	300	-	-	+
100	400	-	-	-
100	500	-	-	-
100	600	-	-	+
100	700	-	-	+
200	000	-	-	-
200	100	-	-	-
200	200	-	-	-
200	300	-	-	-
200	400	-	-	-
200	500	-	-	-
200	600	-	-	-
200	700	-	-	-
300	000	+	+	-
300	100	+	+	-
300	200	+	+	+
300	300	+	+	+
300	400	+	+	-
300	500	+	+	-
300	600	+	+	+
300	700	+	+	+
400	000	-	-	-
400	100	-	-	-

Установленные права

Чтение файла	Смена директории	Просмотр файлов	Переименование файла
--------------	------------------	-----------------	----------------------

-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-
-	+	-	-
-	+	-	-
-	+	-	-
-	+	-	-
+	+	-	-
+	+	-	-
+	+	-	-
+	+	-	-
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-
-	+	-	+
-	+	-	+
-	+	-	+
-	+	-	+
+	+	-	+
+	+	-	+
+	+	-	+
+	+	-	+
-	-	+	-
-	-	+	-

Установленные права

Смена атрибутов файла

-

-

-

-

-

-

-

-

+

+

+

+

+

+

+

+

-

-

-

-

-

-

-

Установленные права

Права директории	Права файла	Создания файла	Удаление файла	Запись в файл
400	200	-	-	-
400	300	-	-	-
400	400	-	-	-
400	500	-	-	-
400	600	-	-	-
400	700	-	-	-
500	000	-	-	-
500	100	-	-	-
500	200	-	-	+
500	300	-	-	+
500	400	-	-	-
500	500	-	-	-
500	600	-	-	+
500	700	-	-	+
600	000	-	-	-
600	100	-	-	-
600	200	-	-	-
600	300	-	-	-
600	400	-	-	-
600	500	-	-	-
600	600	-	-	-
600	700	-	-	-
700	000	+	+	-
700	100	+	+	-
700	200	+	+	+
700	300	+	+	+
700	400	+	+	-
700	500	+	+	-
700	600	+	+	+
700	700	+	+	+

Установленные права

Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла
-	-	+	-
-	-	+	-
-	-	+	-
-	-	+	-
-	-	+	-
-	-	+	-
-	+	+	-
-	+	+	-
-	+	+	-
-	+	+	-
+	+	+	-
+	+	+	-
+	+	+	-
+	+	+	-
-	-	+	-
-	-	+	-
-	-	+	-
-	-	+	-
-	-	+	-
-	-	+	-
-	-	+	-
-	-	+	-
-	+	+	+
-	+	+	+
-	+	+	+
-	+	+	+
+	+	+	+
+	+	+	+
+	+	+	+
+	+	+	+

Установленные права

Смена атрибутов файла

-

-

-

-

-

-

+

+

+

+

+

+

+

+

-

-

-

-

-

-

-

Установленные права

10. Заполним таблицу “Минимальные права для совершения операций” (рис. - @fig:016).

Операция	Минимальные права на директорию	Минимальные права на файл
Создание фа	300	000
Удаление фа	300	000
Чтение файл:	100	400
Запись в файл	100	200
Переименова	300	000
Создание под	300	000
Удаление под	300	000

Минимальные права для совершения операций

Выводы

В процессе выполнения лабораторной работы мы получили практические навыки работы в консоли с атрибутами файлов, закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.