

## **Лабораторная работа N° 2**

Информационная безопасность

Леон Фернандо Хосе Фернандо | НПМбд02-20

## Содержание

1 Цель работы .....	2
2 Теоретическое введение.....	2
3 Выполнение лабораторной работы.....	3
4 Выводы .....	12
5 Список Литературы.....	13

## 1 Цель работы

Приобретение практического опыта в управлении атрибутами файлов с помощью консоли, а также углубление теоретического понимания дискреционного контроля доступа в современных системах с открытым исходным кодом, особенно в тех, которые построены на операционной системе Linux.

## 2 Теоретическое введение

Операционная система Linux предлагает множество надежных функций безопасности, но одной из наиболее важных является система прав доступа к файлам. На ранних стадиях разработки каждый файл был наделен тремя параметрами доступа. Вот они:

- Чтение - Разрешение на чтение позволяет получить доступ к содержимому файла, но не разрешает запись. Для каталогов это позволяет выводить список файлов и подкаталогов, содержащихся внутри.
- Запись - Затем разрешение "Запись" дает возможность создавать новые данные в файле, редактировать существующие данные, создавать новые файлы и изменять как файлы, так и каталоги.
- Выполнение - невозможно запустить программу, если у нее нет флага выполнения. Этот атрибут установлен для всех программ и скриптов, и именно с помощью этого флага система определяет, что файл должен выполняться как программа.

Каждый файл имеет три категории пользователей, для которых могут быть настроены различные комбинации прав доступа:

- Владелец - набор разрешений для владельца файла, пользователя, который его создал или в настоящее время назначен его владельцем. Как правило, владелец обладает полными правами, включая чтение, запись и выполнение.
- Группа - любая группа пользователей, существующая в системе и связанная с файлом. Однако, как правило, это только одна группа, часто группа владельца, хотя файлу можно назначить другую группу.
- Другие - все пользователи, кроме владельца и пользователей, принадлежащих к группе файла.

Команды, которые могут понадобиться при работе с правами доступа:

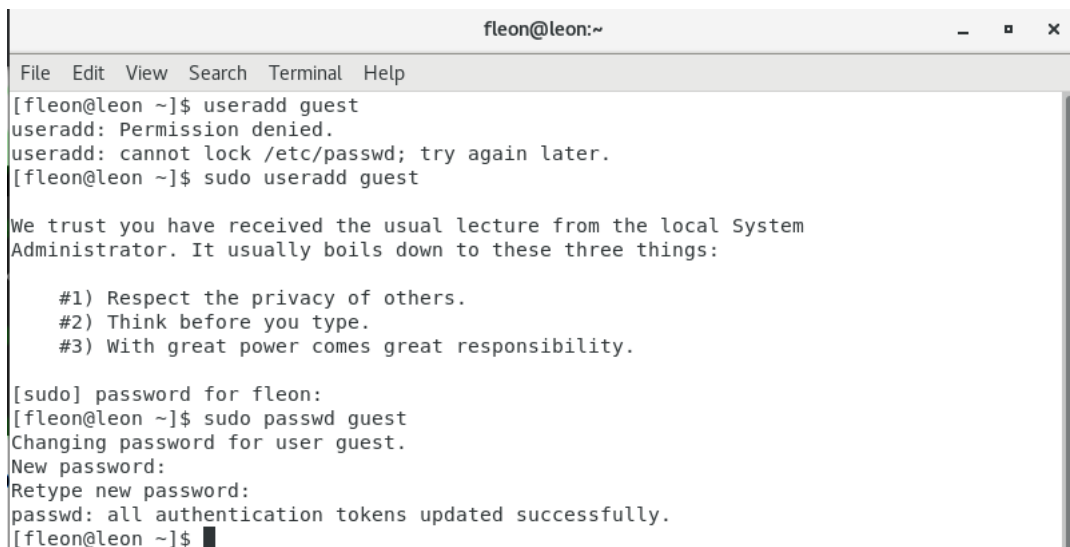
- “ls -l” - для просмотра прав доступа к файлам и каталогам
- “chmod категория действие флаг файл или каталог” - для изменения прав доступа к файлам и каталогам (категорию действие и флаг можно заменить на набор из трех цифр от 0 до 7)

Значения флагов прав:

- — - нет никаких прав
- -x - разрешено только выполнение файла, как программы, но не изменение и не чтение
- -w- - разрешена только запись и изменение файла
- -wx - разрешено изменение и выполнение, но в случае с каталогом, невозможно посмотреть его содержимое
- r- - права только на чтение
- r-x - только чтение и выполнение, без права на запись
- rw- - права на чтение и запись, но без выполнения
- rwx - все права

### 3 Выполнение лабораторной работы

В ранее проведенной лабораторной работе операционная система установила учетную запись пользователя для "гостя" с помощью команды "sudo useradd guest" и установила пароль для этого пользователя с помощью команды "sudo passwd guest".



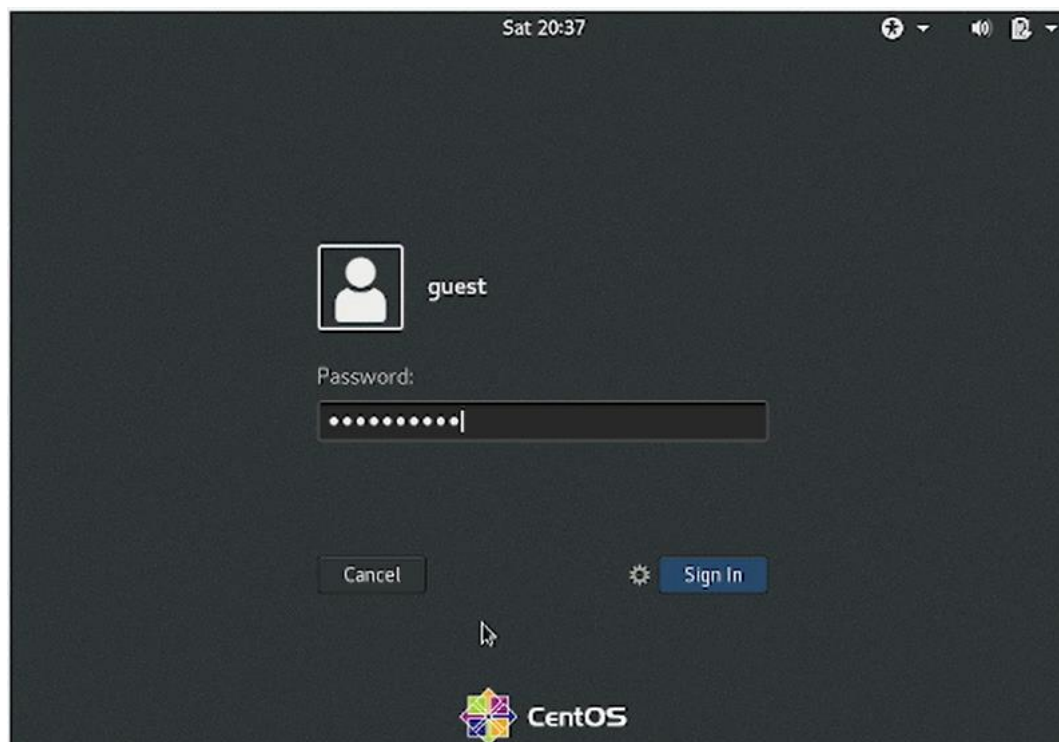
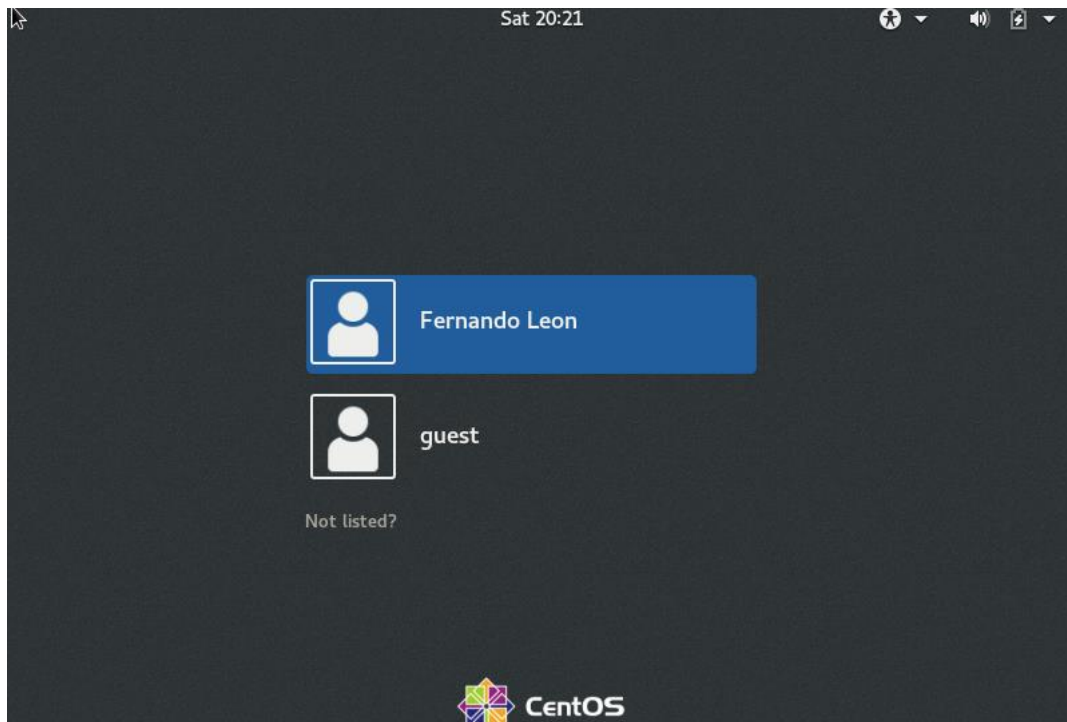
```
fleon@leon:~
File Edit View Search Terminal Help
[fleon@leon ~]$ useradd guest
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
[fleon@leon ~]$ sudo useradd guest

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for fleon:
[fleon@leon ~]$ sudo passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[fleon@leon ~]$
```

Вошел в систему от имени пользователя 'guest'



Используя команду "pwd", я определил, что нахожусь в каталоге /home/guest, который также является моим домашним каталогом. Это соответствует командной строке.

Я подтвердил свое имя пользователя с помощью команды "whoami" и получил вывод: 'guest'.

С помощью команды "id" я идентифицировал свое имя пользователя как "гость" с uid = 1001 (гость) и gid = 1001 (гость). Затем я сравнил эту информацию с выводом команды "группы", которая отображала "гость". Мой пользователь принадлежит только к одной группе, которая состоит из самого пользователя, поэтому выходные данные команд "id" и

"groups" совпадают. Данные, отображаемые в командной строке, совпадают с полученной информацией.

Затем я просмотрел файл /etc/passwd, используя команду "cat /etc/passwd".

```
guest@leon:~  
File Edit View Search Terminal Help  
[guest@leon ~]$ pwd  
/home/guest  
[guest@leon ~]$ whoami  
guest  
[guest@leon ~]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@leon ~]$ groups  
guest  
[guest@leon ~]$ /etc/passwd  
bash: /etc/passwd: Permission denied  
[guest@leon ~]$ cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
bin:x:1:1:bin:/bin:/sbin/nologin  
daemon:x:2:2:daemon:/sbin:/sbin/nologin  
adm:x:3:4:adm:/var/adm:/sbin/nologin  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
sync:x:5:0:sync:/sbin:/bin/sync  
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
halt:x:7:0:halt:/sbin:/sbin/halt  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin  
games:x:12:100:games:/usr/games:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
nobody:x:99:99:Nobody:/:/sbin/nologin  
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
```

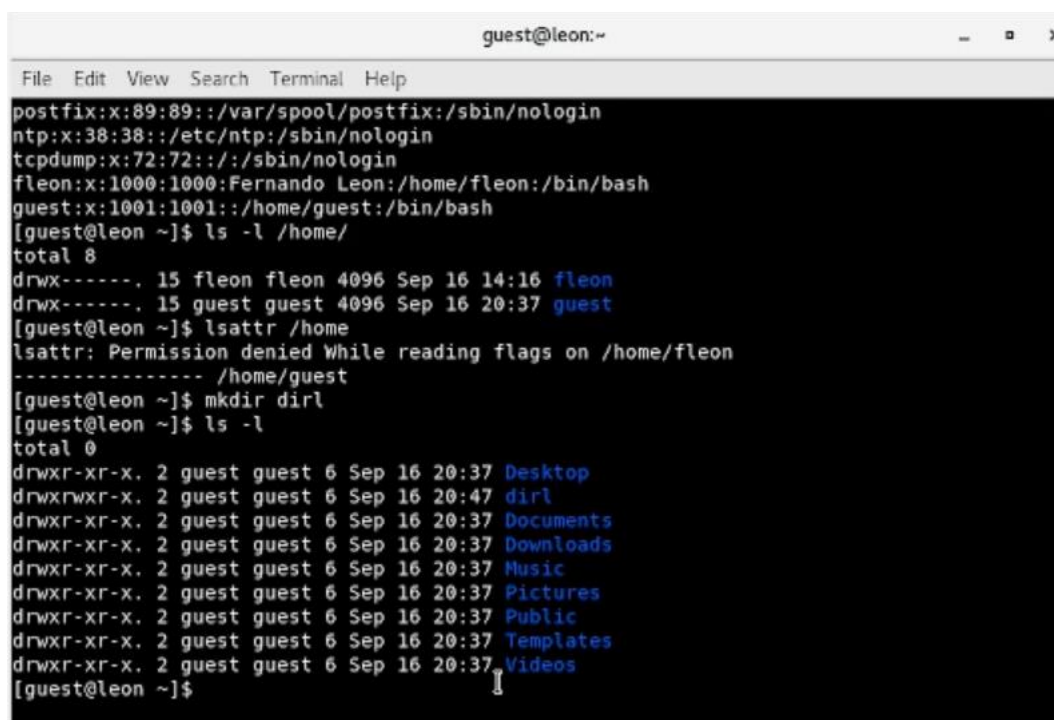
Я нашел свою учетную запись пользователя в самом конце файла /etc/passwd. uid равен 1001, а gid равен 1001, что соответствует информации, которую мы получили ранее.

```
guest@leon:~  
File Edit View Search Terminal Help  
abrt:x:173:173:/:etc/abrt:/sbin/nologin  
setroubleshoot:x:994:991:/:var/lib/setroubleshoot:/sbin/nologin  
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin  
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
radvd:x:75:75:radvd user:/:/sbin/nologin  
chrony:x:993:988:/:var/lib/chrony:/sbin/nologin  
unbound:x:992:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin  
qemu:x:107:107:qemu user:/:/sbin/nologin  
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/:/sbin/nologin  
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin  
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin  
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/nologin  
gdm:x:42:42:/:var/lib/gdm:/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  
gnome-initial-setup:x:989:983:/:run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin  
postfix:x:89:89:/:var/spool/postfix:/sbin/nologin  
ntp:x:38:38:/:etc/ntp:/sbin/nologin  
tcpdump:x:72:72:/:/sbin/nologin  
fleon:x:1000:1000:Fernando Leon:/home/fleon:/bin/bash  
guest:x:1001:1001:/:home/guest:/bin/bash  
[guest@leon ~]$
```

Я просмотрел каталоги в системе, используя команду "ls -l /home/". Мне удалось получить список подкаталогов в каталоге /home. Эти каталоги имеют разрешения на чтение, запись и выполнение, установленные для пользователя (для группы и других пользователей разрешения на доступ не установлены).

Я также проверил наличие расширенных атрибутов, установленных в подкаталогах, расположенных в каталоге /home, используя команду "lsattr /home". Я мог наблюдать только расширенные атрибуты в каталоге, связанном с учетной записью пользователя, которую я в данный момент использую в системе.

Я создал подкаталог с именем "dir1" в моем домашнем каталоге, используя команду "mkdir dir1". Затем я проверил установленные на нем права доступа и расширенные атрибуты. Разрешения следующие: чтение, запись и выполнение доступны для пользователя и группы, в то время как для других предоставляются только разрешения на чтение и выполнение. Для этого каталога не заданы расширенные атрибуты.



```
guest@leon:~  
File Edit View Search Terminal Help  
postfix:x:89:89::/var/spool/postfix:/sbin/nologin  
ntp:x:38:38::/etc/ntp:/sbin/nologin  
tcpdump:x:72:72::/sbin/nologin  
fleon:x:1000:1000:Fernando Leon:/home/fleon:/bin/bash  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@leon ~]$ ls -l /home/  
total 8  
drwx-----, 15 fleon fleon 4096 Sep 16 14:16 fleon  
drwx-----, 15 guest guest 4096 Sep 16 20:37 guest  
[guest@leon ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/fleon  
----- /home/guest  
[guest@leon ~]$ mkdir dir1  
[guest@leon ~]$ ls -l  
total 0  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Desktop  
drwxrwxr-x. 2 guest guest 6 Sep 16 20:47 dir1  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Documents  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Downloads  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Music  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Pictures  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Public  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Templates  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Videos  
[guest@leon ~]$
```

Я удалил все атрибуты из каталога "dir1" с помощью команды "chmod 000 dir1" и проверил его статус с помощью команды "ls -l". Действительно, все атрибуты были удалены.

Я попытался создать файл с именем "file1" в каталоге "dir1", используя команду "echo 'test' > /home/guest/dir1/file1". Однако эта операция завершилась неудачей, поскольку мы ранее удалили доступ на запись в каталог. Следовательно, файл не был создан. Изначально я даже не мог открыть каталог с помощью команды "ls -l /home/guest/dir1" по той же причине. Чтобы устранить это, я изменил права доступа, снова использовал команду, а затем смог просмотреть содержимое каталога, подтвердив, что файл не был создан



```
guest@leon:~  
File Edit View Search Terminal Help  
[guest@leon ~]$ chmod 000 dirl  
[guest@leon ~]$ ls -l  
total 0  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Desktop  
d-----, 2 guest guest 6 Sep 16 20:47 dirl  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Documents  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Downloads  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Music  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Pictures  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Public  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Templates  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Videos  
[guest@leon ~]$ echo "test" > /home/guest/dirl  
bash: /home/guest/dirl: Is a directory  
[guest@leon ~]$ ls -l /home/guest/dirl  
ls: cannot open directory /home/guest/dirl: Permission denied  
[guest@leon ~]$ chmod 700 di
```

```
guest@leon:~  
File Edit View Search Terminal Help  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Templates  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Videos  
[guest@leon ~]$ echo "test" > /home/guest/dirl  
bash: /home/guest/dirl: Is a directory  
[guest@leon ~]$ ls -l /home/guest/dirl  
ls: cannot open directory /home/guest/dirl: Permission denied  
[guest@leon ~]$ chmod 700 dirl  
[guest@leon ~]$ ls -l  
total 0  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Desktop  
drwx-----, 2 guest guest 6 Sep 16 20:47 dirl  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Documents  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Downloads  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Music  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Pictures  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Public  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Templates  
drwxr-xr-x. 2 guest guest 6 Sep 16 20:37 Videos  
[guest@leon ~]$ ls -l /home/guest/dirl  
total 0  
[guest@leon ~]$ cd dirl  
[guest@leon dirl]$ ls  
[guest@leon dirl]$ cd ../  
[guest@leon ~]$ chmod 000 dirl  
[guest@leon ~]$
```

Заполним таблицу «Установленные права и разрешённые действия» 3.1.

Создание файла: "echo"test" > /home/guest/dir1/file2"

Удаление файла: "rm -r /home/guest/dir1/file1"

Запись в файл: "echo"textnew" > /home/guest/dir1/file1"

Чтение файла: "cat /home/guest/dir1/file1"

Смена директории: "cd dir1"

Просмотр файлов в директории: "ls dir1"

Переименование файла: “mv /home/guest/dir1/file1 filenew”

Смена атрибутов файла: “chattr -a /home/guest/dir1/file1”

В случае успеха будет записывать +, в случае ошибки доступа будем записывать -.  
Соберём данные в таблицу 1.

Установленные права и разрешённые действия

Права директ ории	Пра ва фай ла	Созда ние файла	Удале ние файла	Зап ись в фай л	Чтен ие фай ла	Смена директ ории	Просмо тр файлов в директ ории	Переимено вание файла	Смена атрибу тов файла
d (000)	(00 0)	-	-	-	-	-	-	-	-
d -x (100)	(00 0)	-	-	-	-	+	-	-	-
d -w- (200)	(00 0)	-	-	-	-	-	-	-	-
d -wx (300)	(00 0)	+	+	-	-	+	-	+	-
d r- (400)	(00 0)	-	-	-	-	-	+	-	-
d r-x (500)	(00 0)	-	-	-	-	+	+	-	-
d rw- (600)	(00 0)	-	-	-	-	-	+	-	-
d rwx (700)	(00 0)	+	+	-	-	+	+	+	-
d (000)	-x (10 0)	-	-	-	-	-	-	-	-
d -x (100)	-x (10 0)	-	-	-	-	+	-	-	-
d -w- (200)	-x (10 0)	-	-	-	-	-	-	-	-
d -wx (300)	-x (10 0)	+	+	-	-	+	-	+	-



d r- (400)	-x (10 0)	-	-	-	-	-	+	-	-
d r-x (500)	-x (10 0)	-	-	-	-	+	+	-	-
d rw- (600)	-x (10 0)	-	-	-	-	-	+	-	-
d rwx (700)	-x (10 0)	+	+	-	-	+	+	+	-
d (000)	-w- (20 0)	-	-	-	-	-	-	-	-
d -x (100)	-w- (20 0)	-	-	+	-	+	-	-	-
d -w- (200)	-w- (20 0)	-	-	-	-	-	-	-	-
d -wx (300)	-w- (20 0)	+	+	+	-	+	-	+	-
d r- (400)	-w- (20 0)	-	-	-	-	-	+	-	-
d r-x (500)	-w- (20 0)	-	-	+	-	+	+	-	-
d rw- (600)	-w- (20 0)	-	-	-	-	-	+	-	-
d rwx (700)	-w- (20 0)	+	+	+	-	+	+	+	-
d (000)	-wx (30 0)	-	-	-	-	-	-	-	-
d -x (100)	-wx (30 0)	-	-	+	-	+	-	-	-
d -w- (200)	-wx (30 0)	-	-	-	-	-	-	-	-

d -wx (300)	-wx (30 0)	+	+	+	-	+	-	+	-
d r- (400)	-wx (30 0)	-	-	-	-	-	+	-	-
d r-x (500)	-wx (30 0)	-	-	+	-	+	+	-	-
d rw- (600)	-wx (30 0)	-	-	-	-	-	+	-	-
d rwx (700)	-wx (30 0)	+	+	+	-	+	+	+	-
d (000)	r- (40 0)	-	-	-	-	-	-	-	-
d -x (100)	r- (40 0)	-	-	-	+	+	-	-	+
d -w- (200)	r- (40 0)	-	-	-	-	-	-	-	-
d -wx (300)	r- (40 0)	+	+	-	+	+	-	+	+
d r- (400)	r- (40 0)	-	-	-	-	-	+	-	-
d r-x (500)	r- (40 0)	-	-	-	+	+	+	-	+
d rw- (600)	r- (40 0)	-	-	-	-	-	+	-	-
d rwx (700)	r- (40 0)	+	+	-	+	+	+	+	+
d (000)	r-x (50 0)	-	-	-	-	-	-	-	-
d -x (100)	r-x (50 0)	-	-	-	+	+	-	-	+

d -w- (200)	r-x (50 0)	-	-	-	-	-	-	-	-
d -wx (300)	r-x (50 0)	+	+	-	+	+	-	+	+
d r- (400)	r-x (50 0)	-	-	-	-	-	+	-	-
d r-x (500)	r-x (50 0)	-	-	-	+	+	+	-	+
d rw- (600)	r-x (50 0)	-	-	-	-	-	+	-	-
d rwx (700)	r-x (50 0)	+	+	-	+	+	+	+	+
d (000)	rw- (60 0)	-	-	-	-	-	-	-	-
d -x (100)	rw- (60 0)	-	-	+	+	+	-	-	+
d -w- (200)	rw- (60 0)	-	-	-	-	-	-	-	-
d -wx (300)	rw- (60 0)	+	+	+	+	+	-	+	+
d r- (400)	rw- (60 0)	-	-	-	-	-	+	-	-
d r-x (500)	rw- (60 0)	-	-	+	+	+	+	-	+
d rw- (600)	rw- (60 0)	-	-	-	-	-	+	-	-
d rwx (700)	rw- (60 0)	+	+	+	+	+	+	+	+
d (000)	rw- (70 0)	-	-	-	-	-	-	-	-

d -x (100)	rwX (70 0)	-	-	+	+	+	-	-	+
d -w- (200)	rwX (70 0)	-	-	-	-	-	-	-	-
d -wx (300)	rwX (70 0)	+	+	+	+	+	-	+	+
d r- (400)	rwX (70 0)	-	-	-	-	-	+	-	-
d r-x (500)	rwX (70 0)	-	-	+	+	+	+	-	+
d rw- (600)	rwX (70 0)	-	-	-	-	-	+	-	-
d rwX (700)	rwX (70 0)	+	+	+	+	+	+	+	+

На основании этой таблицы создадим другую, в которой опишем минимальные требования на права и директорию для выполнения тех или иных действий. Внесём проанализированные данные в таблицу.

#### *Минимальные права для совершения операций*

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d -wx (300)	— (000)
Удаление файла	d -wx (300)	— (000)
Чтение файла	d -x (100)	r- (400)
Запись в файл	d -x (100)	-w- (200)
Переименование файла	d -wx (300)	— (000)
Создание поддиректории	d -wx (300)	— (000)
Удаление поддиректории	d -wx (300)	— (000)

## 4 Выводы

В ходе этой лабораторной работы я приобрел практические навыки работы с атрибутами файлов в консоли. Я также укрепил свое теоретическое понимание дискреционного контроля доступа в современных системах с открытым исходным кодом, основанных на операционной системе Linux.

## 5 Список Литературы

1. Права доступа к файлам в Linux [Электронный ресурс]. 2019. URL: <https://losst.ru/prava-dostupa-k-fajlam-v-linux>.
2. Запечников С. В. и др. Информационная безопасность открытых систем. Том 1. — М.: Горячая линия -Телеком, 2006
3. Практические аспекты сетевой безопасности. Сетевая безопасность. Межсетевые экраны. (В. Иванов, МГУ)