

Отчет к лабораторной работе №2

Common information

discipline: Основы информационной безопасности

group: НПМбд-02-21

author: Бабина Ю. О.

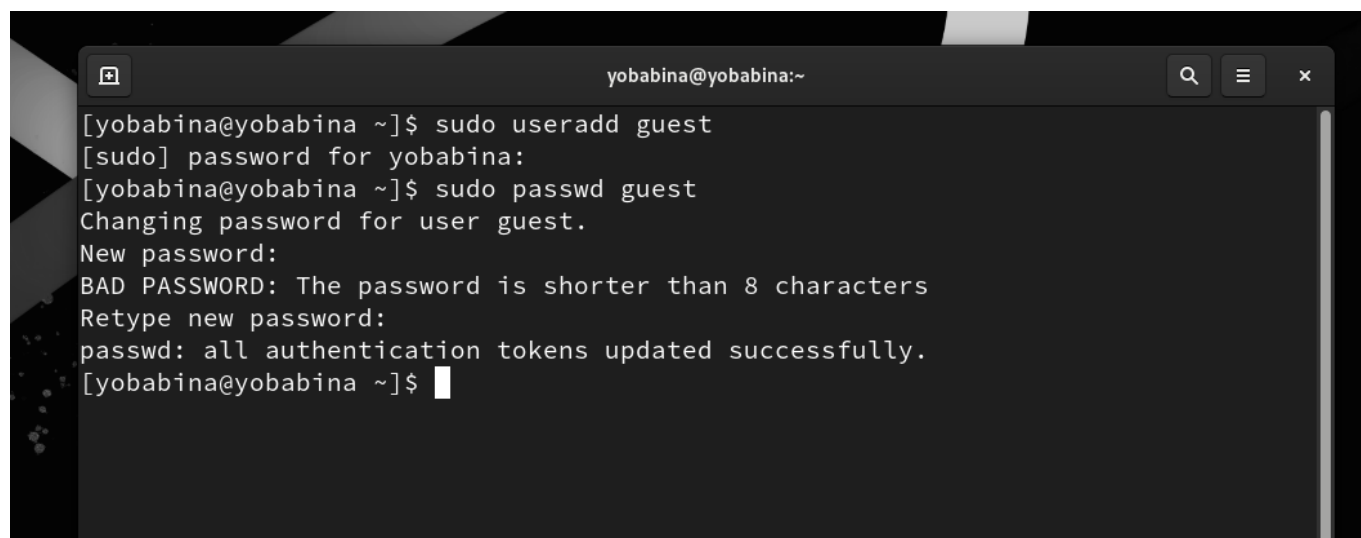
Цель работы

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 работы

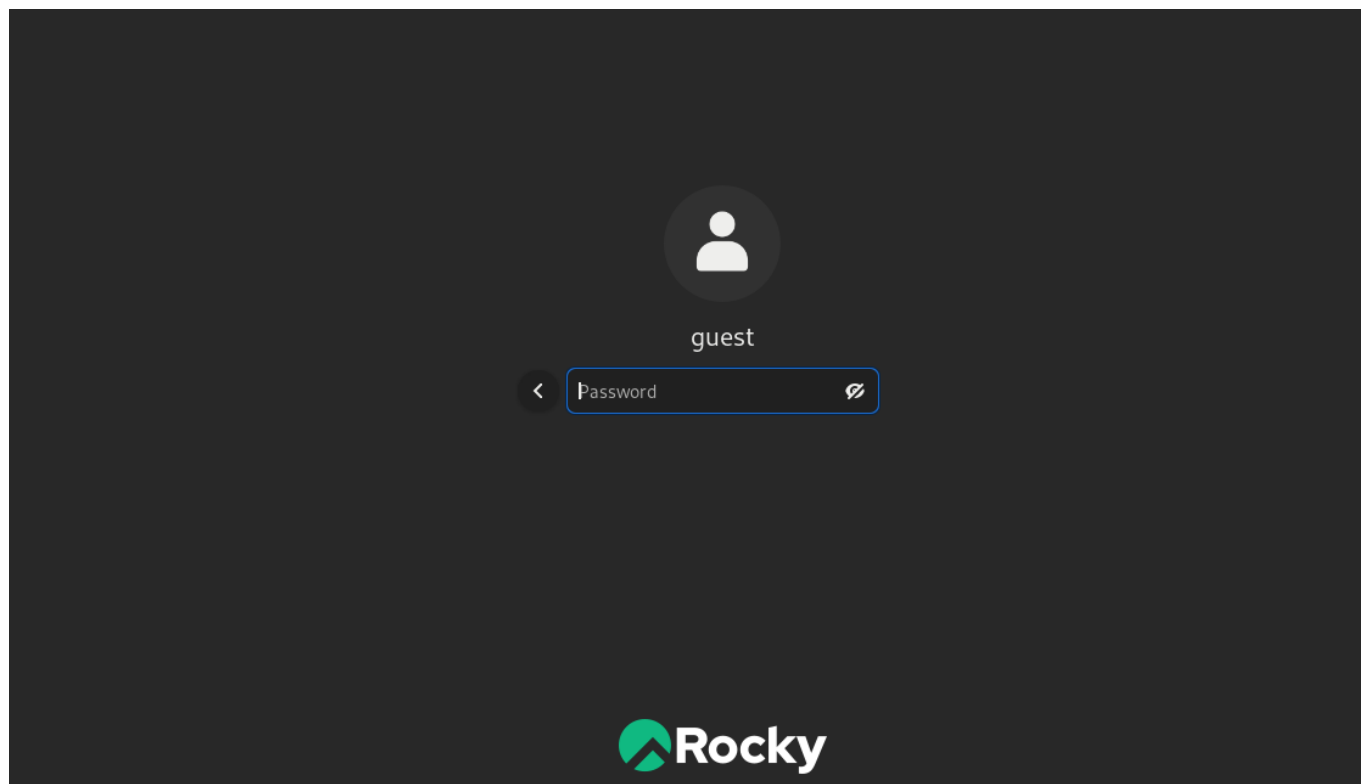
В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest при помощи команды "sudo useradd guest".

Затем зададим пароль для пользователя guest командой: "sudo passwd guest".



```
yobabina@yobabina:~  
[yobabina@yobabina ~]$ sudo useradd guest  
[sudo] password for yobabina:  
[yobabina@yobabina ~]$ sudo passwd guest  
Changing password for user guest.  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[yobabina@yobabina ~]$
```

Войдем в систему от имени пользователя guest:




Определим директорию, в которой мы находимся, командой "pwd". Данная директория является домашней для пользователя guest.

```
guest@yobabina:~  
[guest@yobabina ~]$ pwd  
/home/guest  
[guest@yobabina ~]$
```

Затем уточним имя нашего пользователя командой "whoami".

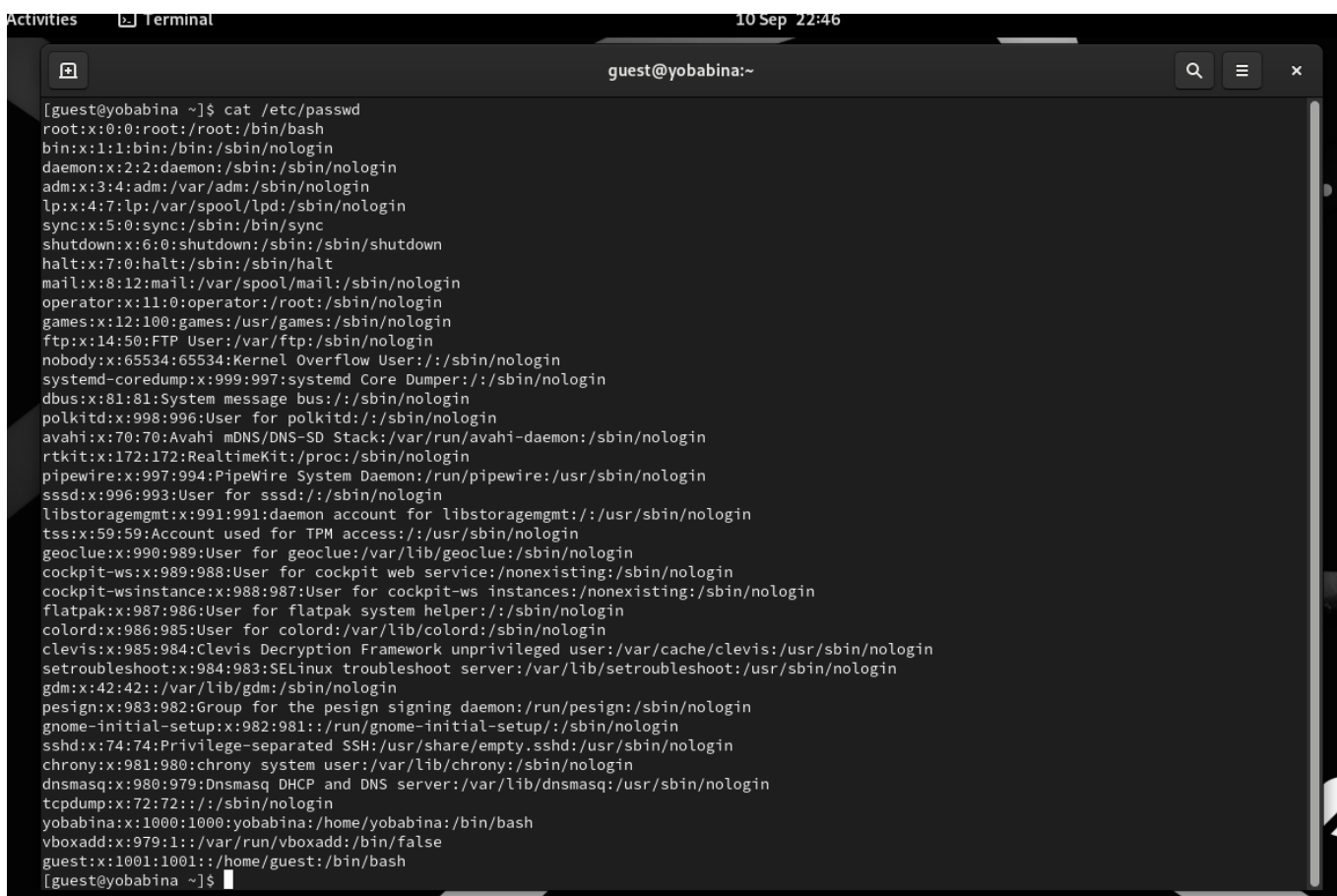
```
guest@yobabina:~  
[guest@yobabina ~]$ whoami  
guest  
[guest@yobabina ~]$
```

Уточним имя нашего пользователя, его группу, а также группы, куда входит пользователь, командой "id". Также сравним вывод "id" с выводом команды groups.



```
guest@yobabina:~$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@yobabina ~]$ groups
guest
[guest@yobabina ~]$
```

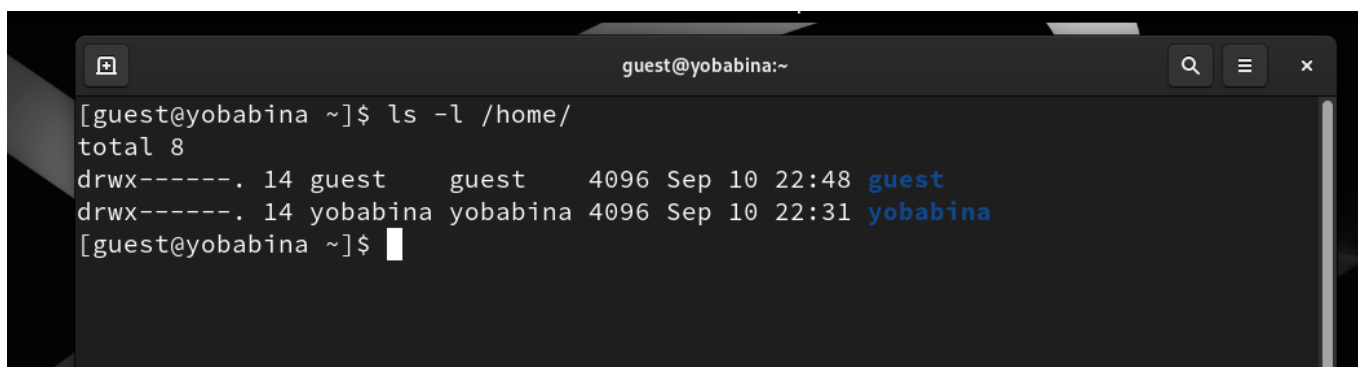
Просмотрим файл /etc/passwd командой "cat /etc/passwd".



```
10 Sep 22:46
guest@yobabina:~$ 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:65534:65534:Kernel Overflow User:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
polkitd:x:998:996:User for polkitd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:x:997:994:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
sssd:x:996:993:User for sssd:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:990:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:989:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:987:986:User for flatpak system helper:/sbin/nologin
colord:x:986:985:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:985:984:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:984:983:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:./var/lib/gdm:/sbin/nologin
design:x:983:982:Group for the design signing daemon:/run/design:/sbin/nologin
gnome-initial-setup:x:982:981:./run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:981:980:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:980:979:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:./sbin/nologin
yobabina:x:1000:1000:yobabina:/home/yobabina:/bin/bash
vboxadd:x:979:1:./var/run/vboxadd:/bin/false
guest:x:1001:1001:./home/guest:/bin/bash
[guest@yobabina ~]$
```

Как видно, id и gid пользователя guest совпадают с результатами выполнения команд id и groups.

Определим существующие в системе директории командой "ls -l /home/"



```
guest@yobabina:~$ ls -l /home/
total 8
drwx-----. 14 guest      guest      4096 Sep 10 22:48 guest
drwx-----. 14 yobabina  yobabina  4096 Sep 10 22:31 yobabina
[guest@yobabina ~]$
```

Нам удалось получить список поддиректорий директории. На все поддиректории установлены все права доступа - чтение, запись, выполнение.

Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: "lsattr /home".

```
guest@yobabina:~  
[guest@yobabina ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/yobabina  
----- /home/guest  
[guest@yobabina ~]$
```

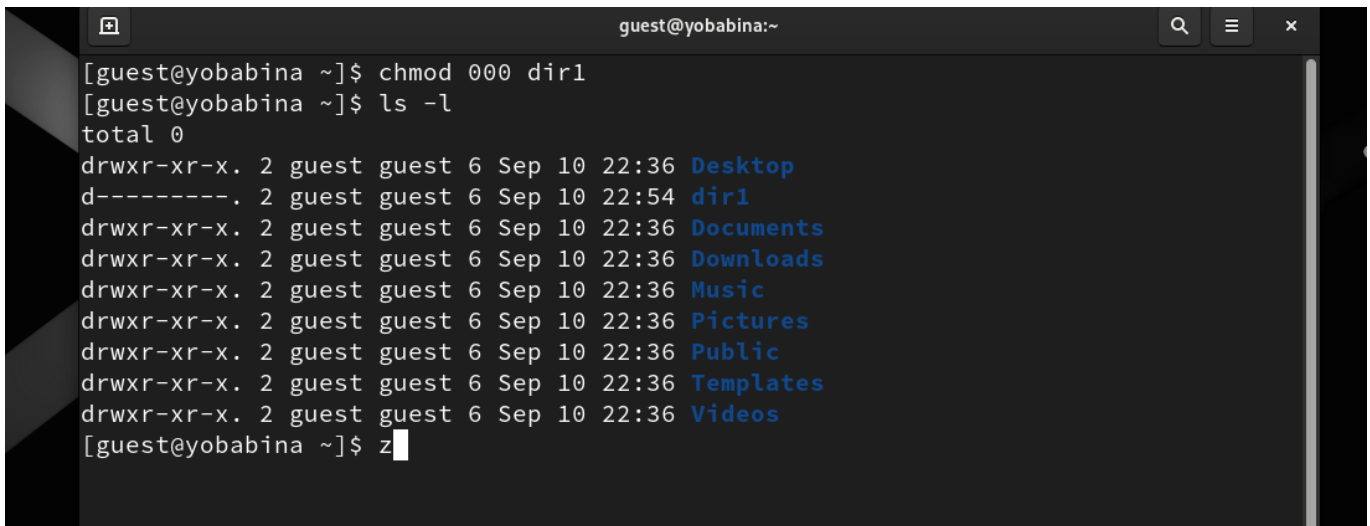
Итак, расширенные атрибуты директории увидеть не удалось.

Создадим в домашней директории поддиректорию dir1 командой "mkdir dir1". Определим командами "ls -l" и "lsattr", какие права доступа и расширенные атрибуты были выставлены на директорию dir1.

```
guest@yobabina:~  
[guest@yobabina ~]$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos  
[guest@yobabina ~]$ mkdir dir1  
[guest@yobabina ~]$ ls -l  
total 0  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Desktop  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:54 dir1  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Documents  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Downloads  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Music  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Pictures  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Public  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Templates  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Videos  
[guest@yobabina ~]$ lsattr  
----- ./Desktop  
----- ./Downloads  
----- ./Templates  
----- ./Public  
----- ./Documents  
----- ./Music  
----- ./Pictures  
----- ./Videos  
----- ./dir1  
[guest@yobabina ~]$ S
```

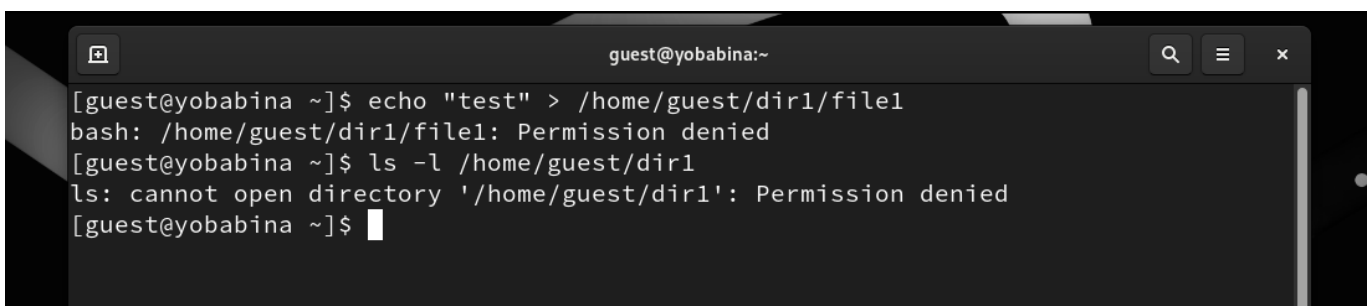
Отражает, захвачена ли клавиатура гостевой ОС:
⬇️ клавиатура не захвачена

Снимем с директории dir1 все атрибуты командой "chmod 000 dir1".



```
guest@yobabina:~  
[guest@yobabina ~]$ chmod 000 dir1  
[guest@yobabina ~]$ ls -l  
total 0  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Desktop  
d------. 2 guest guest 6 Sep 10 22:54 dir1  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Documents  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Downloads  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Music  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Pictures  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Public  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Templates  
drwxr-xr-x. 2 guest guest 6 Sep 10 22:36 Videos  
[guest@yobabina ~]$ z
```

Попытаемся создать в директории dir1 файл file1 командой: "echo "test" > /home/guest/dir1/file1".



```
guest@yobabina:~  
[guest@yobabina ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Permission denied  
[guest@yobabina ~]$ ls -l /home/guest/dir1  
ls: cannot open directory '/home/guest/dir1': Permission denied  
[guest@yobabina ~]$
```

Отказ в выполнении операции по созданию файла произошел ввиду снятия прав на все операции с пользователя guest.

Начнем заполнять таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет.

Для начала для пользователя guest установим права только на чтение dir1 и файла file1, после чего проделаем различные действия с файлом и директорией:



```
guest@yobabina:~  
[guest@yobabina ~]$ ls -l dir1  
total 0  
-rw-r--r--. 1 guest guest 0 Sep 10 23:05 file1  
[guest@yobabina ~]$ chmod 100 dir1  
[guest@yobabina ~]$ chmod 000 dir1/file1  
[guest@yobabina ~]$ touch dir1/file2  
touch: cannot touch 'dir1/file2': Permission denied  
[guest@yobabina ~]$ rm dir1/file1  
rm: remove write-protected regular empty file 'dir1/file1'? ^Z  
[1]+  Stopped                  rm dir1/file1  
[guest@yobabina ~]$ rm dir1/file1  
rm: remove write-protected regular empty file 'dir1/file1'?  
[guest@yobabina ~]$ ls -l dir1  
ls: cannot open directory 'dir1': Permission denied  
[guest@yobabina ~]$
```

В итоге получилась следующая таблица

директория	файл	оп. 1	оп. 2	оп. 3	оп. 4	оп. 5	оп. 6	оп. 7	оп. 8
000	000	-	-	-	-	-	-	-	-
100	000	-	-	-	-	+	-	-	-
200	000	-	-	-	-	-	-	-	-
300	000	+	+	-	-	+	-	+	-
400	000	-	-	-	-	-	+	-	-
500	000	-	-	-	-	+	+	-	-
600	000	-	-	-	-	-	+	-	-
700	000	+	+	-	-	+	+	+	-
000	100	-	-	-	-	-	-	-	-
100	100	-	-	-	-	+	-	-	-
200	100	-	-	-	-	-	-	-	-
300	100	+	+	-	-	+	-	+	-
400	100	-	-	-	-	-	+	-	-
500	100	-	-	-	-	+	+	-	-
600	100	-	-	-	-	-	+	-	-
700	100	+	+	-	-	+	+	+	-
000	200	-	-	-	-	-	-	-	-
100	200	-	-	+	-	+	-	-	-
200	200	-	-	-	-	-	-	-	-
300	200	+	+	+	-	+	-	+	-
400	200	-	-	-	-	-	+	-	-
500	200	-	-	+	-	+	+	-	-
600	200	-	-	-	-	-	+	-	-
700	200	+	+	+	-	+	+	+	-
000	300	-	-	-	-	-	-	-	-
100	300	-	-	+	-	+	-	-	-
200	300	-	-	-	-	-	-	-	-
300	300	+	+	-	+	+	-	+	-
400	300	-	-	-	-	-	+	-	-

директория	файл	оп. 1	оп. 2	оп. 3	оп. 4	оп. 5	оп. 6	оп. 7	оп. 8
500	300	-	-	+	-	+	+	-	-
600	300	-	-	-	-	-	+	-	-
700	300	+	+	+	-	+	+	+	-
000	400	-	-	-	-	-	-	-	-
100	400	-	-	-	+	+	-	-	+
200	400	-	-	-	-	-	-	-	-
300	400	+	+	-	+	+	-	+	+
400	400	-	-	-	-	-	+	-	-
500	400	-	-	-	+	+	+	-	+
600	400	-	-	-	-	-	+	-	-
700	400	+	+	-	+	+	+	+	+
000	500	-	-	-	-	-	-	-	-
100	500	-	-	-	+	+	-	-	+
200	500	-	-	-	-	-	-	-	-
300	500	+	+	-	+	+	-	+	+
400	500	-	-	-	-	-	+	-	-
500	500	-	-	-	+	+	+	-	+
600	500	-	-	-	-	-	+	-	-
700	500	+	+	-	+	+	+	+	+
000	600	-	-	-	-	-	-	-	-
100	600	-	-	+	+	+	-	-	+
200	600	-	-	-	-	-	-	-	-
300	600	+	+	+	+	+	-	+	+
400	600	-	-	-	-	-	+	-	-
500	600	-	-	+	+	+	+	-	+
600	600	-	-	-	-	-	+	-	-
700	600	+	+	+	+	+	+	+	+
000	700	-	-	-	-	-	-	-	-
100	700	-	-	+	+	+	-	-	+
200	700	-	-	-	-	-	-	-	-

директория	файл	оп. 1	оп. 2	оп. 3	оп. 4	оп. 5	оп. 6	оп. 7	оп. 8
300	700	+	+	+	+	+	-	+	+
400	700	-	-	-	-	-	+	-	-
500	700	-	-	+	+	+	+	-	+
600	700	-	-	-	-	-	+	-	-
700	700	+	+	+	+	+	+	+	+

где

- директория - права доступа директории
- файл права доступа файла
- оп. 1 - создание файла
- оп. 2 - удаление файла
- оп. 3 - запись в файл
- оп. 4 - чтение файла
- оп. 5 - смена директории
- оп. 6 - просмотр файлов в директории
- оп. 7 - переименование файла
- оп. 8 - смена атрибутов файла

Теперь на основе таблицы выше заполним таблицу «Минимально необходимые права для выполнения операций внутри директории»:

Операция	Директория мин. права	Файл мин. права
оп. 1	300	000
оп. 2	300	000
оп. 3	100	400
оп. 4	100	200
оп. 5	300	000
оп. 6	300	000
оп. 7	300	000

где

- оп. 1 - создание файла
- оп. 2 - удаление файла
- оп. 3 - чтение файла
- оп. 4 - запись в файл
- оп. 5 - переименование файла
- оп. 6 - создание поддиректории
- оп. 7 - переименование файла
- оп. 8 - удаление поддиректории

Вывод

В рамках выполнения данной лабораторной работы я получила практические навыки работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

- https://docs.rockylinux.org/books/admin_guide/06-users/
- <https://habr.com/ru/articles/469667/>
- <https://linux-faq.ru/page/komanda-lsattr>