

Отчет к лабораторной работе №2

Common information

discipline: Основы информационной безопасности group: НПМбд-02-21

author: Ермолаев А.М.

Цель работы

Получить практический навык работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

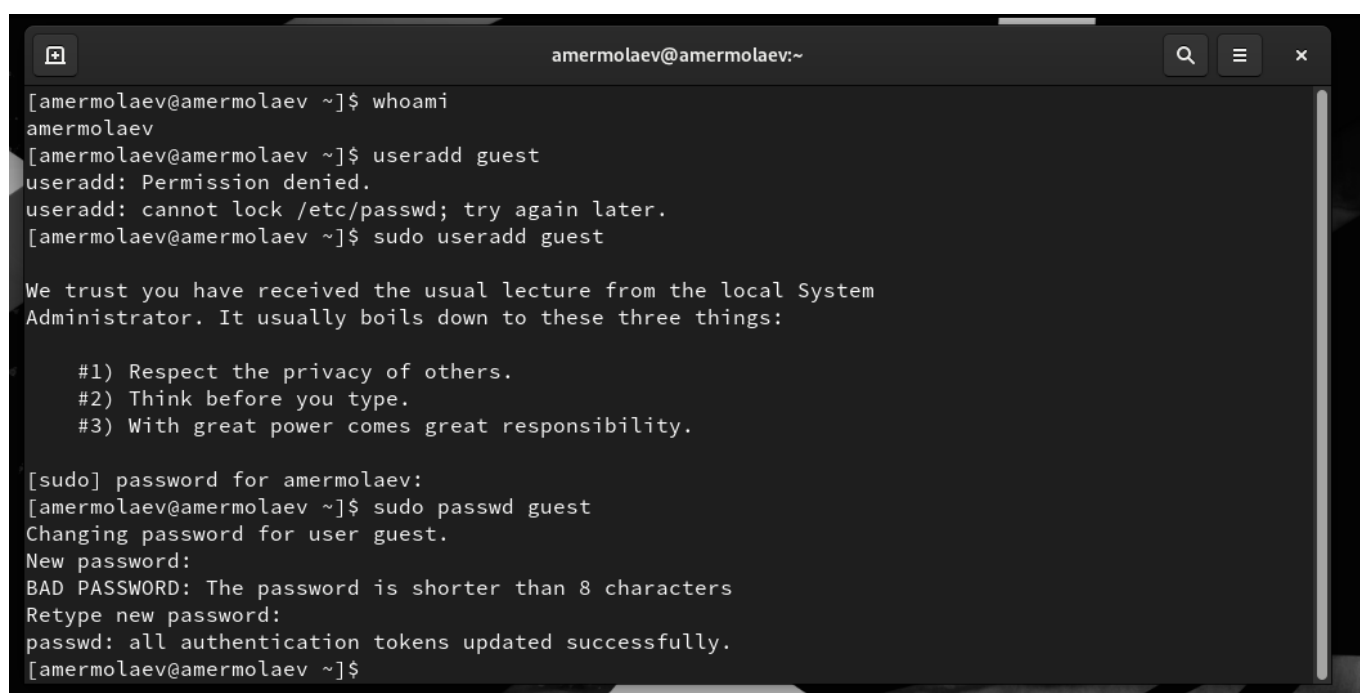
Выполнение работы

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

```
passwd guest.
```



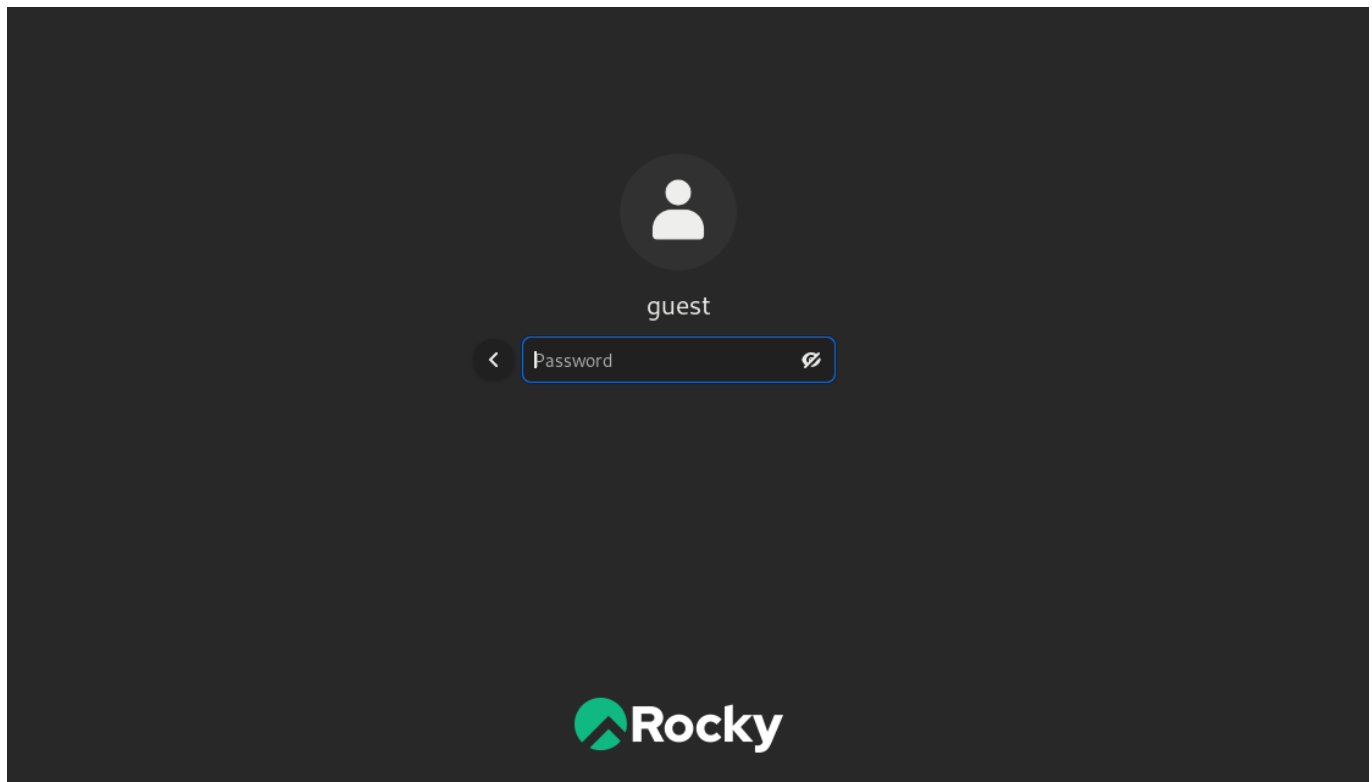
```
amermolaev@amermolaev:~$ whoami
amermolaev
[amermolaev@amermolaev ~]$ useradd guest
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
[amermolaev@amermolaev ~]$ sudo useradd guest

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 amermolaev:
[amermolaev@amermolaev ~]$ 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.
[amermolaev@amermolaev ~]$
```

Войдите в систему от имени пользователя guest:

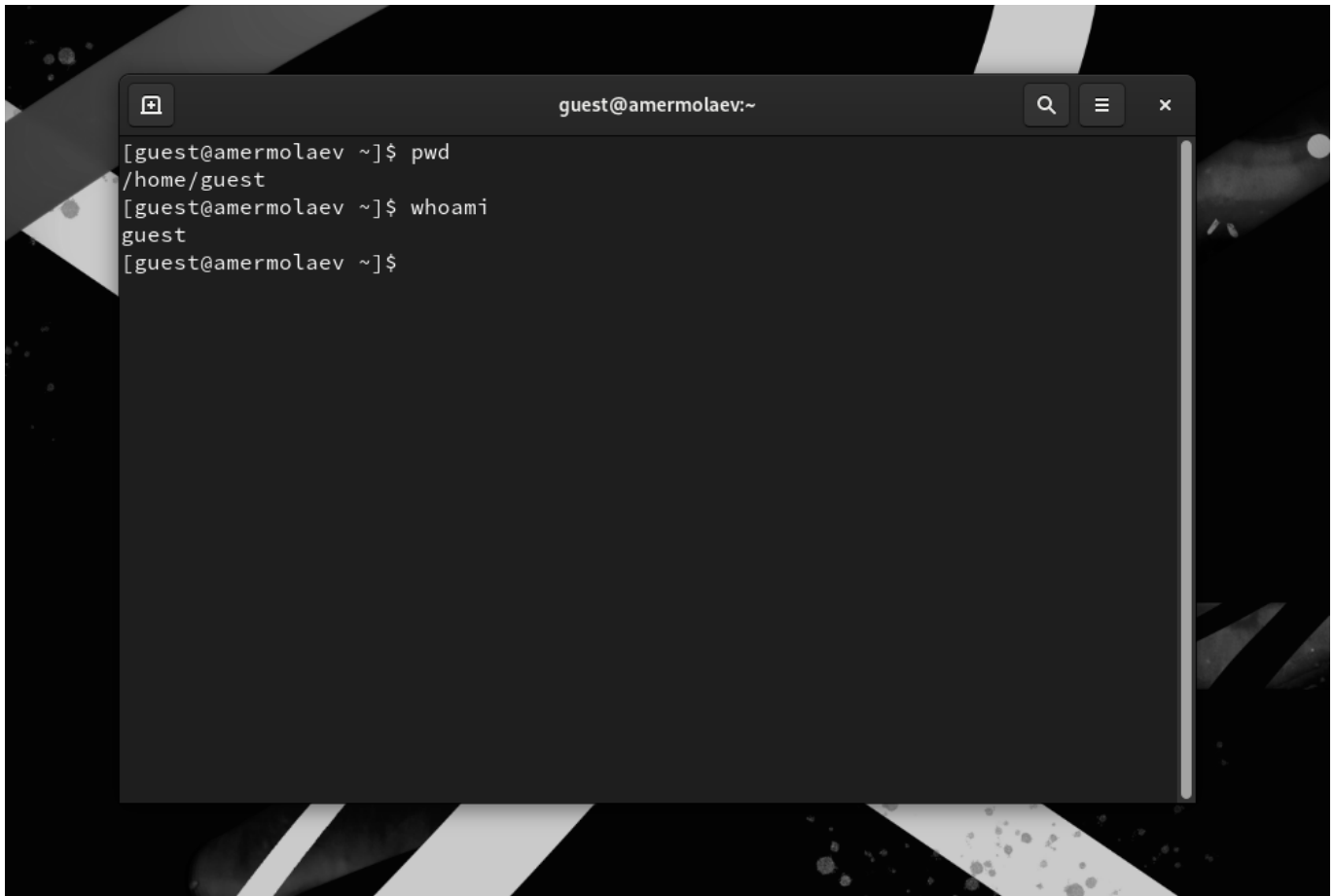


Определим директорию, в которой вы находитесь, командой

```
pwd
```

Действительно, данная директория является домашней для пользователя guest. Также уточним имя вашего пользователя командой

```
whoami
```

A terminal window titled 'guest@amermolaev:~' with search, menu, and close buttons. It shows the execution of 'pwd' resulting in '/home/guest' and 'whoami' resulting in 'guest'.

```
guest@amermolaev ~]$ pwd
/home/guest
guest@amermolaev ~]$ whoami
guest
guest@amermolaev ~]$
```

Уточним имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой

```
id
```

Сравним вывод команды с выводом команды

```
groups
```

A terminal window titled 'guest@amermolaev:~' with search, menu, and close buttons. It shows the output of 'id' and 'groups' commands.

```
[guest@amermolaev ~]$ id
uid=1002(guest) gid=1002(guest) groups=1002(guest) context=unconfined_u:unconfined
_r:unconfined_t:s0-s0:c0.c1023
[guest@amermolaev ~]$ groups
guest
[guest@amermolaev ~]$
```

Теперь посмотрим файл `/etc/passwd` командой

```
cat /etc/passwd
```

```
10 Sep 00:50
guest@amermolaev:~
[guest@amermolaev ~]$ 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
alexermolaev:x:1000:1000:Alex Ermolaev:/home/alexermolaev:/bin/bash
amermolaev:x:1001:1001:/home/amermolaev:/bin/bash
vboxadd:x:979:1:/var/run/vboxadd:/bin/false
guest:x:1002:1002:/home/guest:/bin/bash
[guest@amermolaev ~]$ S
```

Для более удобного поиска воспользуемся командой cat в связке с командой grep:

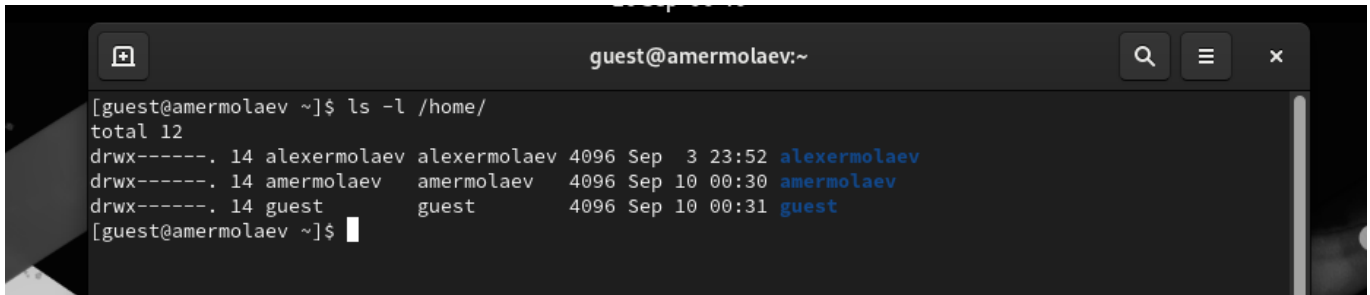
```
cat /etc/passwd | grep guest
```

```
10 Sep 00:55
guest@amermolaev:~
[guest@amermolaev ~]$ cat /etc/passwd | grep guest
guest:x:1002:1002:/home/guest:/bin/bash
[guest@amermolaev ~]$
```

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

Определим существующие в системе директории командой

```
ls -l /home/
```

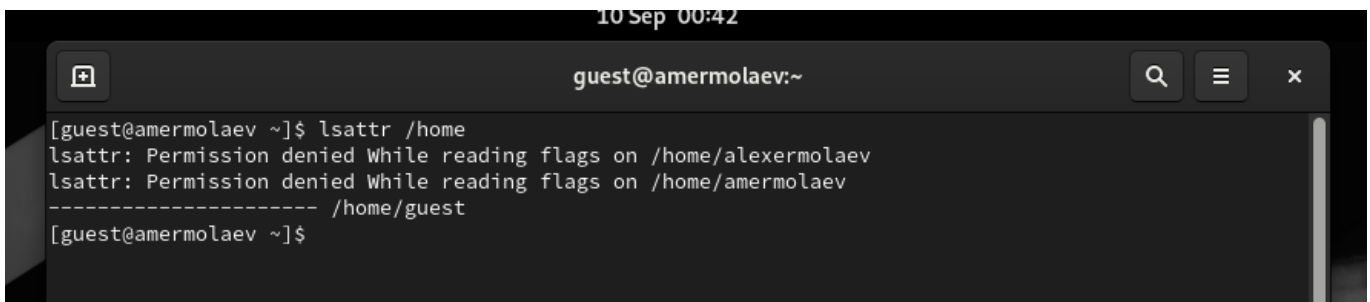


```
guest@amermolaev:~  
[guest@amermolaev ~]$ ls -l /home/  
total 12  
drwx-----. 14 alexermolaev alexermolaev 4096 Sep  3 23:52 alexermolaev  
drwx-----. 14 amermolaev amermolaev 4096 Sep 10 00:30 amermolaev  
drwx-----. 14 guest guest 4096 Sep 10 00:31 guest  
[guest@amermolaev ~]$
```

Список поддиректорий директории получить удалось. На все поддиректории установлены все права доступа - чтение (read), запись (write), выполнение (execute).

Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой

```
lsattr /home
```



```
10 Sep 00:42  
guest@amermolaev:~  
[guest@amermolaev ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/alexermolaev  
lsattr: Permission denied While reading flags on /home/amermolaev  
----- /home/guest  
[guest@amermolaev ~]$
```

Расширенные атрибуты директории увидеть не удалось.

Создадим в домашней директории поддиректорию dir1 командой

```
mkdir dir1
```

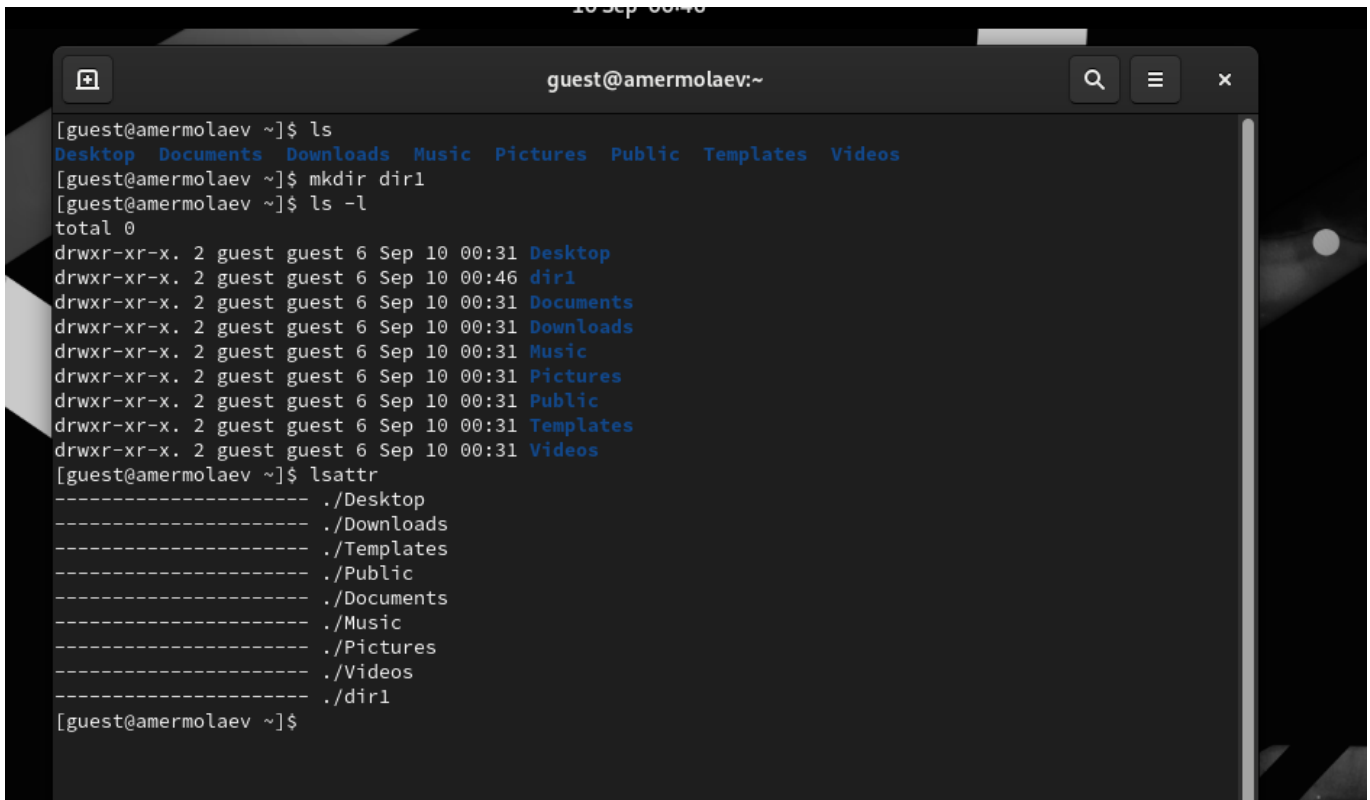
Определим командами

```
ls -l
```

и

```
lsattr
```

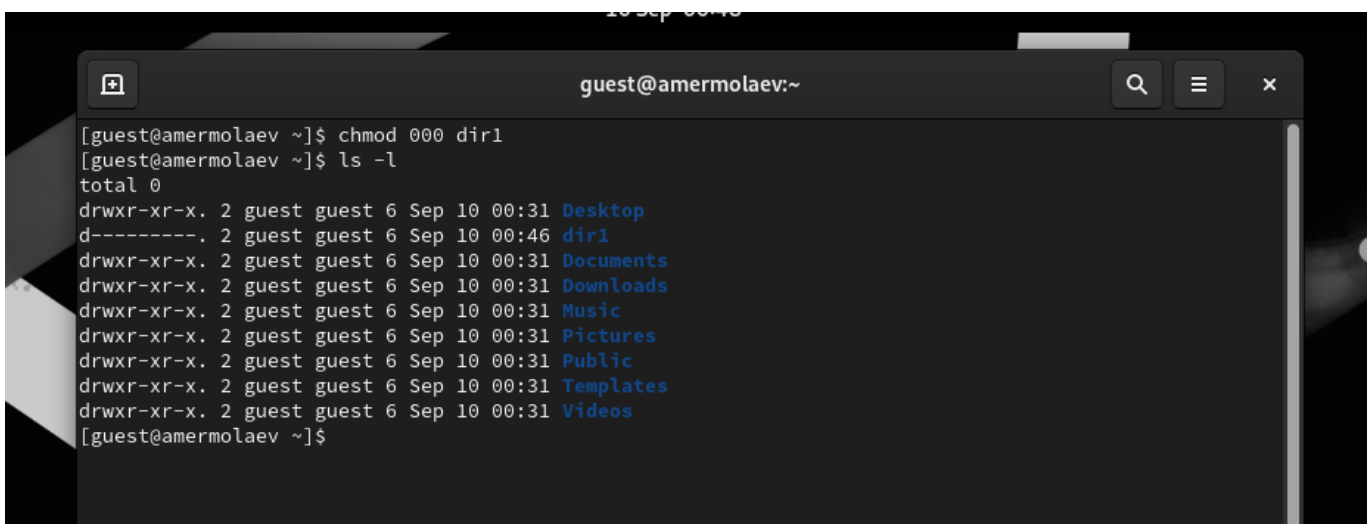
какие права доступа и расширенные атрибуты были выставлены на директорию dir1.

A terminal window titled 'guest@amermolaev:~' with search, menu, and close buttons. The user runs 'ls' showing standard Linux directories. Then 'mkdir dir1' is executed. Finally, 'ls -l' is run, showing a new directory 'dir1' with permissions 'drwxr-xr-x' and ownership '2 guest guest', created on Sep 10 at 00:46.

```
[guest@amermolaev ~]$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
[guest@amermolaev ~]$ mkdir dir1
[guest@amermolaev ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Desktop
drwxr-xr-x. 2 guest guest 6 Sep 10 00:46 dir1
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Documents
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Music
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Public
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Templates
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Videos
[guest@amermolaev ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@amermolaev ~]$
```

Снимем с директории dir1 все атрибуты командой

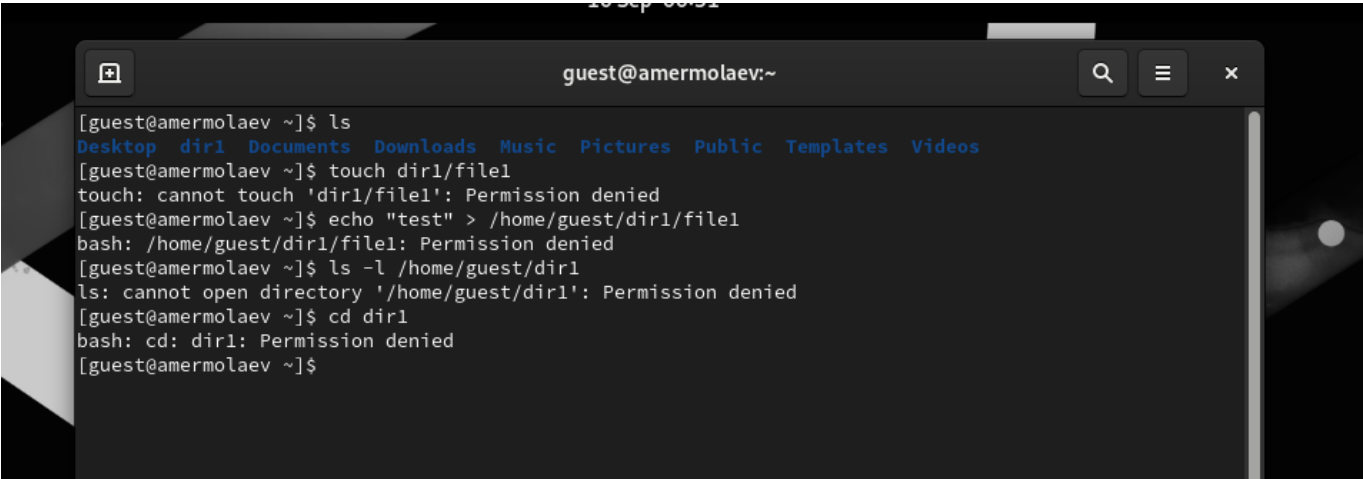
```
chmod 000 dir1
```

The same terminal window as before. The user runs 'chmod 000 dir1'. Then 'ls -l' is run again. The 'dir1' entry now shows permissions 'd-----' instead of 'drwxr-xr-x', indicating that all permissions have been removed.

```
[guest@amermolaev ~]$ chmod 000 dir1
[guest@amermolaev ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Desktop
d----- 2 guest guest 6 Sep 10 00:46 dir1
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Documents
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Music
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Public
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Templates
drwxr-xr-x. 2 guest guest 6 Sep 10 00:31 Videos
[guest@amermolaev ~]$
```

Попытаемся создать в директории dir1 файл file1 командой

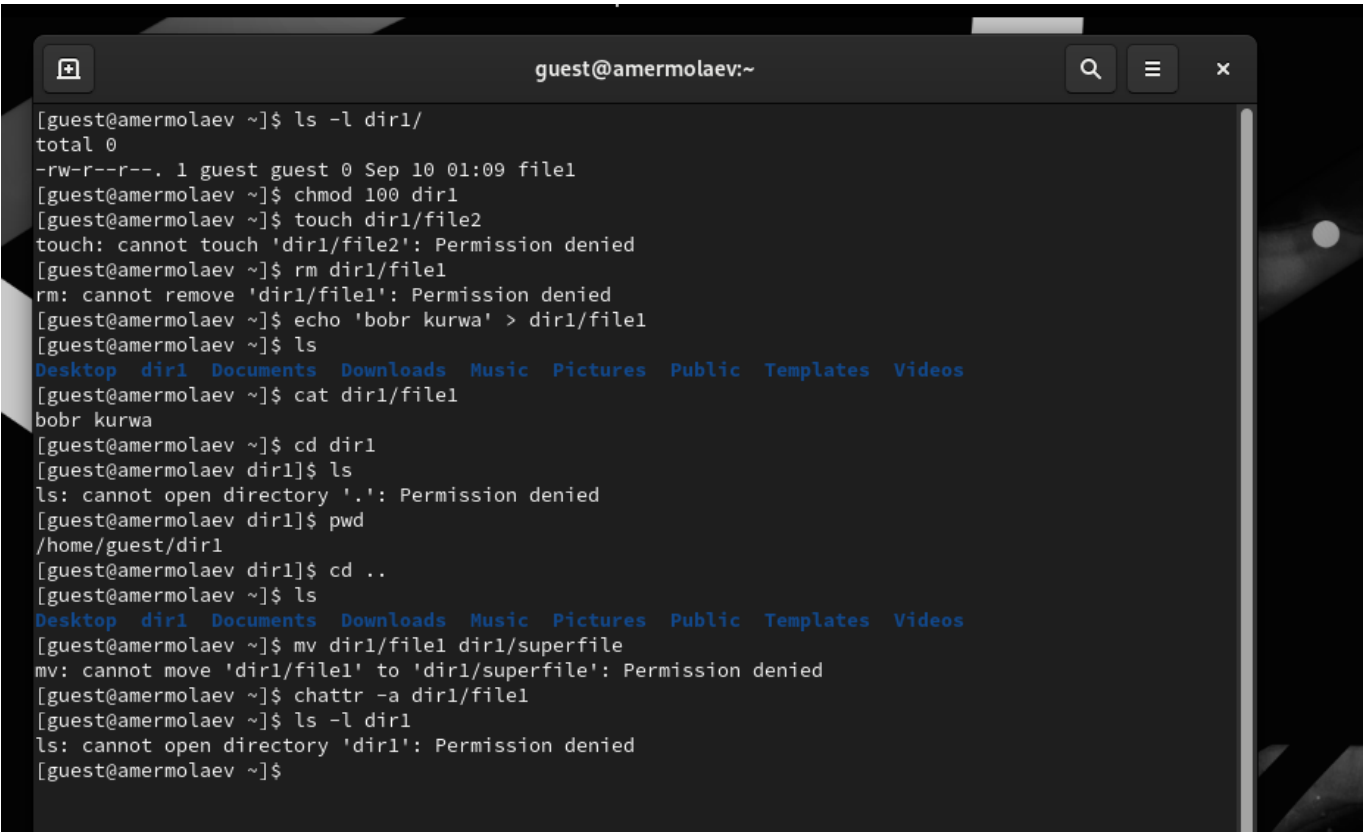
```
echo "test" > /home/guest/dir1/file1
```



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 установим для пользователя guest праыва только на чтения для директории dir1 и файла file1, после чего проделаем различные действия с файлом и директорией:



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	-	-	-	-	+	-	-	-

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

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

директория	файл	оп. 1	оп. 2	оп. 3	оп. 4	оп. 5	оп. 6	оп. 7	оп. 8
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 мы можем заполнить 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 работы я получил практический навык работы в консоли с атрибутами файлов, закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

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