

Лабораторная работа №3

Основы информационной безопасности

Тойчубекова Асель Нурлановна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	20
6	Список литературы	21

Список иллюстраций

4.1	Создание пользователя guest2	9
4.2	Вход на двух разных консолях	10
4.3	Директория, в которой мы находимся	10
4.4	Группы, в которые входят пользователи	10
4.5	Название и идентификатор	10
4.6	Содержимое файла /etc/group	11
4.7	Регистрация guest2 и изменение прав директории	11
4.8	Изменение прав доступа dir1	12
4.9	Действия при правах: dir1=010,file1=030	13
4.10	Действия при правах: dir1=020,file1=030	13
4.11	Действия при правах: dir1=030,file1=030	14
4.12	Действия при правах: dir1=040,file1=030	14
4.13	Действия при правах: dir1=050,file1=030	14
4.14	Действия при правах: dir1=060,file1=030	15
4.15	Действия при правах: dir1=070,file1=030	15

Список таблиц

4.1	Установленные права и разрешённые действия	16
4.2	Минимальные права для совершения операций	19

1 Цель работы

Целью данной лабораторной работы является получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

2 Задание

- Выполнить порядок выполнения лабораторной работы
- Заполнить 2 таблицы, проверив действия на права доступа

3 Теоретическое введение

Дискреционное разграничение прав в Linux: основные атрибуты

В современных операционных системах критически важно обеспечить надежную защиту данных и контроль доступа к ресурсам. Одним из базовых механизмов безопасности в Linux является дискреционное управление доступом (Discretionary Access Control, DAC). Эта модель основана на том, что права доступа к файлам и каталогам определяются их владельцем, который может передавать или ограничивать доступ другим пользователям.

Основным инструментом DAC в Linux является система разрешений файловой системы (file permissions), которая управляет правами на чтение (read), запись (write) и выполнение (execute) для владельца файла, группы пользователей и всех остальных. Помимо классической схемы прав (rwx), Linux поддерживает специальные атрибуты, такие как SUID, SGID и sticky bit, а также списки расширенных прав доступа (ACLs), которые позволяют более гибко управлять доступом.

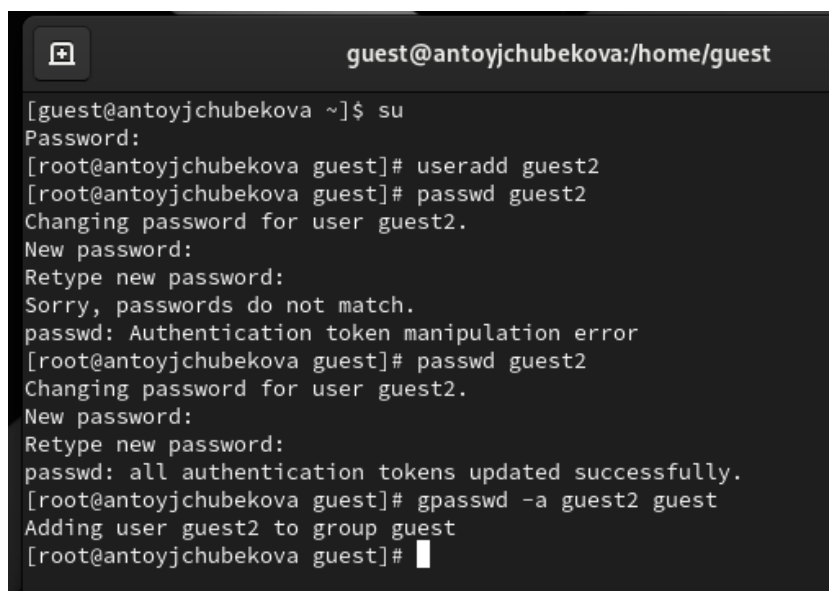
Хотя дискреционная модель удобна и широко применяется, она имеет уязвимости, связанные с человеческим фактором. Например, владелец файла может случайно предоставить доступ нежелательным пользователям, что создает риск утечки данных. Поэтому в современных системах безопасности Linux дополнительно используются механизмы обязательного контроля доступа (Mandatory Access Control, MAC), такие как SELinux и AppArmor, которые обеспечивают более строгие ограничения на уровне системы.

Таким образом, дискреционное разграничение прав в Linux является фундаментальным механизмом контроля доступа, который обеспечивает гибкость в

управлении ресурсами, но требует внимательной настройки и дополнения более строгими методами защиты.

4 Выполнение лабораторной работы

На прошлой лабораторной работе мы создали пользователя `guest`, заходим в систему под пользователем `guest`. Создаем пользователя `guest2` и зададим пароль, командой `passwd guest2`. Добавим пользователя `guest2` в группу `guest`, командой `gpasswd -a guest2 guest`. (рис. 4.1).



```
guest@antoychubekova:/home/guest
[guest@antoychubekova ~]$ su
Password:
[root@antoychubekova guest]# useradd guest2
[root@antoychubekova guest]# passwd guest2
Changing password for user guest2.
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
[root@antoychubekova guest]# passwd guest2
Changing password for user guest2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@antoychubekova guest]# gpasswd -a guest2 guest
Adding user guest2 to group guest
[root@antoychubekova guest]#
```

Рис. 4.1: Создание пользователя `guest2`

Осуществим вход в систему от двух пользователей на двух разных консолях: `guest` на первой консоли и `guest2` на второй консоли, для этого используем команду `su`. (рис. 4.2).

```
guest@antoychubekova:/home/guest
[guest@antoychubekova ~]$ su
Password:
[root@antoychubekova guest]# useradd guest2
[root@antoychubekova guest]# passwd guest2
Changing password for user guest2.
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
[root@antoychubekova guest]# passwd guest2
Changing password for user guest2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@antoychubekova guest]# gpasswd -a guest2 guest
Adding user guest2 to group guest
[root@antoychubekova guest]#

guest2@antoychubekova:/home/guest
[guest@antoychubekova ~]$ su guest2
Password:
[guest2@antoychubekova guest]$
```

Рис. 4.2: Вход на двух разных консолях

Для обоих пользователей командой `pwd` определим директорию, в которой мы находимся. Мы видим, что вывод совпадает с приглашениями командной строки. (рис. 4.3).

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

guest2@antoychubekova:/home/guest
[guest@antoychubekova ~]$ su guest2
Password:
[guest2@antoychubekova guest]$ pwd
/home/guest
[guest2@antoychubekova guest]$
```

Рис. 4.3: Директория, в которой мы находимся

Определим командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`. Мы видим, что `guest` входит в группу `guest`. А `guest2` в группы `guest` и `guest2`. (рис. 4.4).

```
guest@antoychubekova:~
[guest@antoychubekova ~]$ groups guest
guest : guest

guest2@antoychubekova:/home/guest
[guest2@antoychubekova guest]$ groups guest2
guest2 : guest2 guest
```

Рис. 4.4: Группы, в которые входят пользователи

Сравним вывод команды `groups` с выводом команд `id -Gn` (выводит название групп) и `id -G` (выводит идентификатор групп). Мы видим, что вывод команды `groups` и `id -Gn` совпадают и показывают название групп, в которые входит пользователь. А `id -Gn` выводит их идентификатор. (рис. 4.5).

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

guest2@antoychubekova:/home/guest
[guest2@antoychubekova guest]$ groups
guest2 guest
[guest2@antoychubekova guest]$ id -Gn
guest2 guest
[guest2@antoychubekova guest]$ id -G
1002 1001
[guest2@antoychubekova guest]$ id
uid=1002(guest2) gid=1002(guest2) groups=1002(guest2),1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@antoychubekova guest]$
```

Рис. 4.5: Название и идентификатор

Сравним полученную информацию с содержимым файла /etc/group. Мы видим, что и название групп и их идентификаторы совпадают с выводами предыдущих команд. (рис. 4.6).

```
tcpdump:x:72:
antoyjchubekova:x:1000:
vboxsf:x:978:
vboxdrmpc:x:977:
guest:x:1001:guest2
guest2:x:1002:
[guest@antoyjchubekova ~]$
```

Рис. 4.6: Содержимое файла /etc/group

От имени пользователя guest2 выполним регистрацию пользователя guest2 в группе guest командой newgrp guest. А также от имени пользователя guest измените права директории /home/guest, разрешив все действия для пользователей группы, используя команду chmod g+rx /home/guest. (рис. 4.7).

```
[guest@antoyjchubekova ~]$ chmod g+rx /home/guest
[guest@antoyjchubekova ~]$
[guest2@antoyjchubekova guest]$ newgrp guest
[guest2@antoyjchubekova guest]$
```

Рис. 4.7: Регистрация guest2 и изменение прав директории

От имени пользователя guest снимем с директории /home/guest/dir1 все атрибуты командой chmod 000 dir1 и проверим правильность снятия прав. Мы видим, что все было выполнено корректно. (рис. 4.8).

```

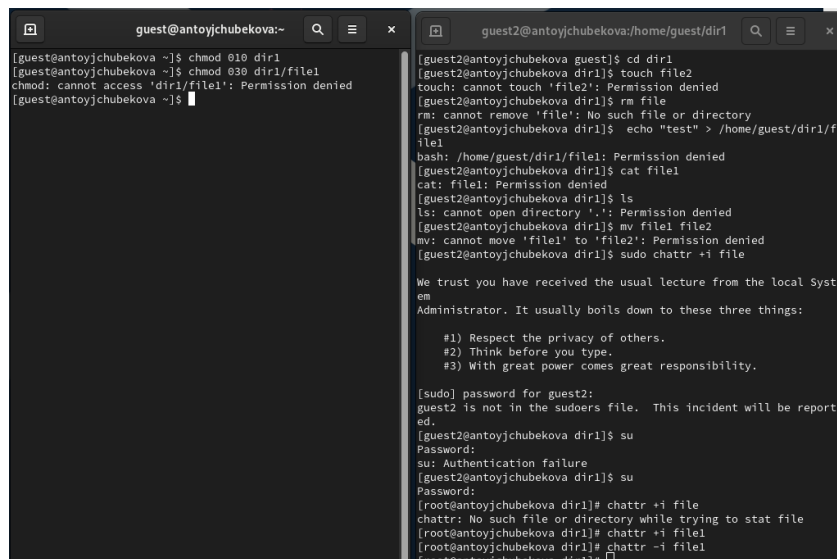
[guest@antoyjchubekova ~]$ chmod 000 dir1
chmod: cannot access 'dir1': No such file or directory
[guest@antoyjchubekova ~]$ ls
Desktop  Documents  Music      Public      Videos
dir1     Downloads  Pictures    Templates
[guest@antoyjchubekova ~]$ chmod 000 dir1
[guest@antoyjchubekova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest  6 Feb 27 07:45 Desktop
d------. 3 guest guest 31 Feb 27 11:13 dir1
drwxr-xr-x. 2 guest guest  6 Feb 27 07:45 Documents
drwxr-xr-x. 2 guest guest  6 Feb 27 07:45 Downloads
drwxr-xr-x. 2 guest guest  6 Feb 27 07:45 Music
drwxr-xr-x. 2 guest guest  6 Feb 27 07:45 Pictures
drwxr-xr-x. 2 guest guest  6 Feb 27 07:45 Public
drwxr-xr-x. 2 guest guest  6 Feb 27 07:45 Templates
drwxr-xr-x. 2 guest guest  6 Feb 27 07:45 Videos
[guest@antoyjchubekova ~]$

```

Рис. 4.8: Изменение прав доступа dir1

Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполним таблицу “Установленные права и разрешённые действия для групп”, определив опытным путём, какие операции разрешены, а какие нет.

На примере прав доступа dir1(000,010,020,030,040,050,060,070) и прав доступа file1(030) посмотрим какие действия разрешены при разных прав доступа директории и файла. Для начала посмотрим разрешенные действия, если права доступа следующие, dir1=010,file1=030. (рис. 4.9).



```
guest@antoychubekova:~$ chmod 010 dir1
[guest@antoychubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoychubekova ~]$

[guest2@antoychubekova guest]$ cd dir1
[guest2@antoychubekova dir1]$ touch file2
touch: cannot touch 'file2': Permission denied
[guest2@antoychubekova dir1]$ rm file
rm: cannot remove 'file': No such file or directory
[guest2@antoychubekova dir1]$ echo "test" > /home/guest/dir1/f
ile1
bash: /home/guest/dir1/file1: Permission denied
[guest2@antoychubekova dir1]$ cat file1
cat: file1: Permission denied
[guest2@antoychubekova dir1]$ ls
ls: cannot open directory '.': Permission denied
[guest2@antoychubekova dir1]$ mv file1 file2
mv: cannot move 'file1' to 'file2': Permission denied
[guest2@antoychubekova dir1]$ sudo chattr +i file

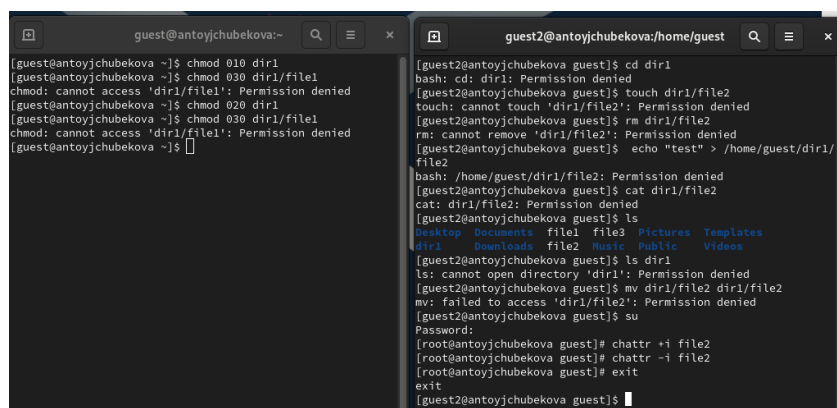
We trust you have received the usual lecture from the local Syst
em
Administrator. It usually boils down to these three things:

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

[sudo] password for guest2:
guest2 is not in the sudoers file. This incident will be report
ed.
[guest2@antoychubekova dir1]$ su
Password:
su: Authentication failure
[guest2@antoychubekova dir1]$ su
Password:
[root@antoychubekova dir1]# chattr +i file
chattr: No such file or directory while trying to stat file
[root@antoychubekova dir1]# chattr +i file1
[root@antoychubekova dir1]# chattr -i file1
[root@antoychubekova dir1]#
```

Рис. 4.9: Действия при правах: dir1=010,file1=030

Разрешенные действия, если права доступа следующие, dir1=020,file1=030.
(рис. 4.10).



```
guest@antoychubekova:~$ chmod 010 dir1
[guest@antoychubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoychubekova ~]$ chmod 020 dir1
[guest@antoychubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoychubekova ~]$

[guest2@antoychubekova guest]$ cd dir1
bash: cd: dir1: Permission denied
[guest2@antoychubekova guest]$ touch dir1/file2
touch: cannot touch 'dir1/file2': Permission denied
[guest2@antoychubekova guest]$ rm dir1/file2
rm: cannot remove 'dir1/file2': Permission denied
[guest2@antoychubekova guest]$ echo "test" > /home/guest/dir1/
file2
bash: /home/guest/dir1/file2: Permission denied
[guest2@antoychubekova guest]$ cat dir1/file2
cat: dir1/file2: Permission denied
[guest2@antoychubekova guest]$ ls
Desktop  Documents  file1  file3  Pictures  Templates
dir1     Downloads  file2  Music  Public    Videos
[guest2@antoychubekova guest]$ ls dir1
ls: cannot open directory 'dir1': Permission denied
[guest2@antoychubekova guest]$ mv dir1/file2 dir1/file2
mv: failed to access 'dir1/file2': Permission denied
[guest2@antoychubekova guest]$ su
Password:
[root@antoychubekova guest]# chattr +i file2
[root@antoychubekova guest]# chattr -i file2
[root@antoychubekova guest]# exit
exit
[guest2@antoychubekova guest]$
```

Рис. 4.10: Действия при правах: dir1=020,file1=030

Разрешенные действия, если права доступа следующие, dir1=030,file1=030.
(рис. 4.11).

```
guest@antoyjchubekova:~$ chmod 010 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 020 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 030 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$

guest2@antoyjchubekova:/home/guest/dir1$ cd dir1
[guest2@antoyjchubekova dir1]$ touch file1
[guest2@antoyjchubekova dir1]$ rm file1
[guest2@antoyjchubekova dir1]$ echo "test" > /home/guest/dir1/f
ile2
bash: /home/guest/dir1/file2: Permission denied
[guest2@antoyjchubekova dir1]$ cat file2
[guest2@antoyjchubekova dir1]$ cat file1
cat: file1: No such file or directory
[guest2@antoyjchubekova dir1]$ ls
ls: cannot open directory '.': Permission denied
[guest2@antoyjchubekova dir1]$ mv file2 file1
[guest2@antoyjchubekova dir1]$ su
Password:
[root@antoyjchubekova dir1]# chattr +i file1
[root@antoyjchubekova dir1]# chattr -i file1
[root@antoyjchubekova dir1]# exit
exit
[guest2@antoyjchubekova dir1]$
```

Рис. 4.11: Действия при правах: dir1=030,file1=030

Разрешенные действия, если права доступа следующие, dir1=040,file1=030.
(рис. 4.12).

```
guest@antoyjchubekova:~$ chmod 010 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 020 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 030 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 040 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ pwd
/home/guest
[guest@antoyjchubekova ~]$

guest2@antoyjchubekova:/home/guest$ cd dir1
bash: cd: dir1: Permission denied
[guest2@antoyjchubekova guest]$ touch dir1/file2
touch: cannot touch 'dir1/file2': Permission denied
[guest2@antoyjchubekova guest]$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
[guest2@antoyjchubekova guest]$ echo "test" > /home/guest/dir1/f
ile2
bash: /home/guest/dir1/file2: Permission denied
[guest2@antoyjchubekova guest]$ cat dir1/file1
cat: dir1/file1: Permission denied
[guest2@antoyjchubekova guest]$ ls
Desktop  Documents  file1  file3  Pictures  Templates
dir1     Downloads  file2  Music  Public    Videos
[guest2@antoyjchubekova guest]$ ls dir1
ls: cannot access 'dir1/dir2': Permission denied
ls: cannot access 'dir1/file1': Permission denied
dir2  file1
[guest2@antoyjchubekova guest]$ mv dir1/file1 dir1/file2
mv: failed to access 'dir1/file2': Permission denied
[guest2@antoyjchubekova guest]$ su
Password:
[root@antoyjchubekova guest]# chattr +i file1
[root@antoyjchubekova guest]# chattr -i file1
[root@antoyjchubekova guest]# exit
exit
[guest2@antoyjchubekova guest]$
```

Рис. 4.12: Действия при правах: dir1=040,file1=030

Разрешенные действия, если права доступа следующие, dir1=050,file1=030.
(рис. 4.13).

```
guest@antoyjchubekova:~$ chmod 010 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 020 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 030 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 030 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 040 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 050 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ pwd
/home/guest
[guest@antoyjchubekova ~]$

guest2@antoyjchubekova:/home/guest$ cd dir1
[guest2@antoyjchubekova guest]$ touch file2
touch: cannot touch 'file2': Permission denied
[guest2@antoyjchubekova dir1]$ rm file1
rm: remove write-protected regular empty file 'file1'? y
rm: cannot remove 'file1': Permission denied
[guest2@antoyjchubekova dir1]$ echo "test" > /home/guest/dir1/f
ile1
bash: /home/guest/dir1/file1: Permission denied
[guest2@antoyjchubekova dir1]$ cat file1
[guest2@antoyjchubekova dir1]$ ls
dir2  file1
[guest2@antoyjchubekova dir1]$ mv file1 file2
mv: cannot move 'file1' to 'file2': Permission denied
[guest2@antoyjchubekova dir1]$ su
Password:
[root@antoyjchubekova dir1]# chattr +i file1
[root@antoyjchubekova dir1]# chattr -i file1
[root@antoyjchubekova dir1]# exit
exit
[guest2@antoyjchubekova dir1]$ cd ..
[guest2@antoyjchubekova guest]$
```

Рис. 4.13: Действия при правах: dir1=050,file1=030

Разрешенные действия, если права доступа следующие, dir1=060,file1=030.
(рис. 4.14).

```

[guest@antoyjchubekova ~]$ chmod 010 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 020 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 030 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 040 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ pwd
/home/guest
[guest@antoyjchubekova ~]$ chmod 050 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 060 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$

[guest2@antoyjchubekova /home/guest]$ cd dir1
bash: cd: dir1: Permission denied
[guest2@antoyjchubekova guest]$ touch dir1/file2
touch: cannot touch 'dir1/file2': Permission denied
[guest2@antoyjchubekova guest]$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
[guest2@antoyjchubekova guest]$ cat dir1/file1
cat: dir1/file1: Permission denied
[guest2@antoyjchubekova guest]$ echo "test" > /home/guest/dir1/
file2
bash: /home/guest/dir1/file2: Permission denied
[guest2@antoyjchubekova guest]$ mv file1 file2
[guest2@antoyjchubekova guest]$ mv dir1/file1 dir1/file2
mv: failed to access 'dir1/file2': Permission denied
[guest2@antoyjchubekova guest]$ su
Password:
[root@antoyjchubekova guest]# cd dir1
[root@antoyjchubekova dir1]# chattr +i file1
[root@antoyjchubekova dir1]# chattr -i file1
[root@antoyjchubekova dir1]# exit
exit
[guest2@antoyjchubekova guest]$
  
```

Рис. 4.14: Действия при правах: dir1=060,file1=030

Разрешенные действия, если права доступа следующие, dir1=070,file1=030.
(рис. 4.15).

```

[guest@antoyjchubekova ~]$ chmod 050 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 060 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 070 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 770 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: changing permissions of 'dir1/file1': Operation not permitted
[guest@antoyjchubekova ~]$ chmod 777 dir1
[guest@antoyjchubekova ~]$ chmod 030 dir1/file1
chmod: changing permissions of 'dir1/file1': Operation not permitted
[guest@antoyjchubekova ~]$ cd dir1
[guest@antoyjchubekova dir1]$ chmod 030 file1
chmod: changing permissions of 'file1': Operation not permitted
[guest@antoyjchubekova dir1]$ ls
dir2  file1
[guest@antoyjchubekova dir1]$ sudo chmod 030 file1
[sudo] password for guest:
guest is not in the sudoers file. This incident will be reported.
[guest@antoyjchubekova dir1]$ su chmod 030 file1
su: user chmod does not exist or the user entry does not contain all the required fields
[guest@antoyjchubekova dir1]$ su
Password:
[root@antoyjchubekova dir1]# chmod 030 file1
[root@antoyjchubekova dir1]# exit
exit
[guest@antoyjchubekova dir1]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Feb 27 11:13 dir2
-----wx---. 1 root root 0 Mar 15 06:14 file1
[guest@antoyjchubekova dir1]$

[guest2@antoyjchubekova /home/guest/dir1]$ cd dir1
[guest2@antoyjchubekova dir1]$ touch file2
[guest2@antoyjchubekova dir1]$ rm file1
rm: remove write-protected regular empty file 'file1'? y
[guest2@antoyjchubekova dir1]$ echo "test" > /home/guest/dir1/
file1
[guest2@antoyjchubekova dir1]$ cat file1
test
[guest2@antoyjchubekova dir1]$ ls
dir2  file1  file2
[guest2@antoyjchubekova dir1]$ mv file1 file1
mv: 'file1' and 'file1' are the same file
[guest2@antoyjchubekova dir1]$ mv file1 file3
[guest2@antoyjchubekova dir1]$ mv file3 file1
[guest2@antoyjchubekova dir1]$ su
Password:
[root@antoyjchubekova dir1]# chattr +i file1
[root@antoyjchubekova dir1]# chattr -i file1
[root@antoyjchubekova dir1]# exit
exit
[guest2@antoyjchubekova dir1]$
  
```

Рис. 4.15: Действия при правах: dir1=070,file1=030

Исходя из этих результатов заполним таблицу “Установленные права и разрешённые действия” 4.1

Таблица 4.1: Установленные права и разрешённые действия

Пра- ва ди- ректо- рии	Со- Пра- ва фай- ла	Уда- зда- ние фай- ла	ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
000	000	-	-	-	-	-	-	-	-
010	000	-	-	-	-	+	-	-	+
020	000	-	-	-	-	-	-	-	-
030	000	+	+	-	-	+	-	+	+
040	000	-	-	-	-	-	+	-	-
050	000	-	-	-	-	+	+	-	+
060	000	-	-	-	-	-	-	-	-
070	000	+	+	-	-	+	+	+	+
000	010	-	-	-	-	-	-	-	-
010	010	-	-	-	-	+	-	-	+
020	010	-	-	-	-	-	-	-	-
030	010	+	+	-	-	+	-	+	+
040	010	-	-	-	-	-	+	-	-
050	010	-	-	-	-	+	+	-	+
060	010	-	-	-	-	-	-	-	-
070	010	+	+	-	-	+	+	+	+
000	020	-	-	-	-	-	-	-	-
010	020	-	-	+	-	+	-	-	+
020	020	-	-	-	-	-	-	-	-
030	020	+	+	+	-	+	-	+	+
040	020	-	-	-	-	-	+	-	-
050	020	-	-	+	-	+	+	-	+

Пра- ва ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
060	020	-	-	-	-	-	+	-	-
070	020	+	+	+	-	+	-	-	-
000	030	-	-	-	-	-	-	-	-
010	030	-	-	+	-	+	-	-	+
020	030	-	-	-	-	-	-	-	-
030	030	+	+	+	-	+	-	+	+
040	030	-	-	-	-	-	+	-	-
050	030	-	-	+	-	+	+	-	+
060	030	-	-	-	-	-	+	-	-
070	030	+	+	+	-	+	+	+	+
000	040	-	-	-	-	-	-	-	-
010	040	-	-	-	+	+	-	-	+
020	040	-	-	-	-	-	-	-	-
030	040	+	+	-	+	+	-	+	+
040	040	-	-	-	-	-	+	-	-
050	040	-	-	-	+	+	+	-	+
060	040	-	-	-	-	-	+	-	-
070	040	+	+	-	+	+	+	+	-
000	050	-	-	-	-	-	-	-	-
010	050	-	-	-	+	+	-	-	+
020	050	-	-	-	-	-	-	-	-
030	050	+	+	-	+	+	-	+	+
040	050	-	-	-	-	-	+	-	-
050	050	-	-	-	+	+	+	-	+

Пра- ва ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
060	050	-	-	-	-	-	+	-	-
070	050	+	+	-	+	+	+	+	+
000	060	-	-	-	-	-	-	-	-
010	060	-	-	+	+	+	-	-	+
020	060	-	-	-	-	-	-	-	-
030	060	+	+	+	+	+	-	+	+
040	060	-	-	-	-	-	+	-	-
050	060	-	-	+	+	+	+	-	+
060	060	-	-	-	-	-	+	-	-
070	060	+	+	+	+	+	+	+	+
000	070	-	-	-	-	-	-	-	-
010	070	-	-	+	+	+	-	-	+
020	070	-	-	-	-	-	-	-	-
030	070	+	+	+	+	+	-	+	+
040	070	-	-	-	-	-	+	-	-
050	070	-	-	+	+	+	+	-	+
060	070	-	-	-	-	-	+	-	-
070	070	+	+	+	+	+	+	+	+

Далее на основе заполненной таблицы определим те или иные минимально необходимые права для выполнения операций внутри директории dir1. Опишем это в таблице “Минимальные права для совершения операций” 4.2

Таблица 4.2: Минимальные права для совершения операций

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	030	000
Удаление файла	030	000
Чтение файла	010	040
Запись в файл	010	020
Переименование файла	030	000
Создание поддиректории	030	000
Удаление поддиректории	030	000

5 Выводы

В ходе выполнения лабораторной работы я получила практические навыки работы в консоли с атрибутами файлов для групп пользователей.

6 Список литературы

- <https://esystem.rudn.ru/course/view.php?id=21200>