

Информационная безопасность

Л.3. Дискреционное разграничение прав в Linux. Два пользователя

Ширяев Кирилл Владимирович

2022

Содержание

Цель работы	1
Ход работы.....	1
Новый пользователь.....	1
Добавление в группу	2
Два пользователя	3
Текущая директория	3
Группы пользователей	4
Файл /etc/group.....	4
Регистрация в группе	5
Права для группы.....	5
Снятие атрибутов.....	6
Таблицы.....	6
Вывод.....	8

Цель работы

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

Ход работы

Новый пользователь

В установленной операционной системе создали учётную запись пользователя guest2 (используя учётную запись администратора) с помощью команды `useradd guest`

Задали пароль для пользователя guest2 (используя учётную запись администратора) с помощью команды `passwd guest`

```
Обзор Терминал Вт, 22 февраля 12:28 en2
kvshiryaev@kvshiryaev:~
Файл Правка Вид Поиск Терминал Справка
[kvshiryaev@kvshiryaev ~]$ useradd guest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[kvshiryaev@kvshiryaev ~]$ su root
Пароль:
[root@kvshiryaev kvshiryaev]# useradd giest
[root@kvshiryaev kvshiryaev]# useradd guest
[root@kvshiryaev kvshiryaev]# passwd guest
Изменение пароля пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля :
Извините, но пароли не совпадают.
passwd: ошибка при операциях с маркером проверки подлинности
[root@kvshiryaev kvshiryaev]# passwd guest
Изменение пароля пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - не содержит достаточног
о числа РАЗЛИЧНЫХ символов
Повторите ввод нового пароля :
[root@kvshiryaev kvshiryaev]# passwd guest
Изменение пароля пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - не содержит достаточног
```

Figure 1: Новый пользователь

Добавление в группу

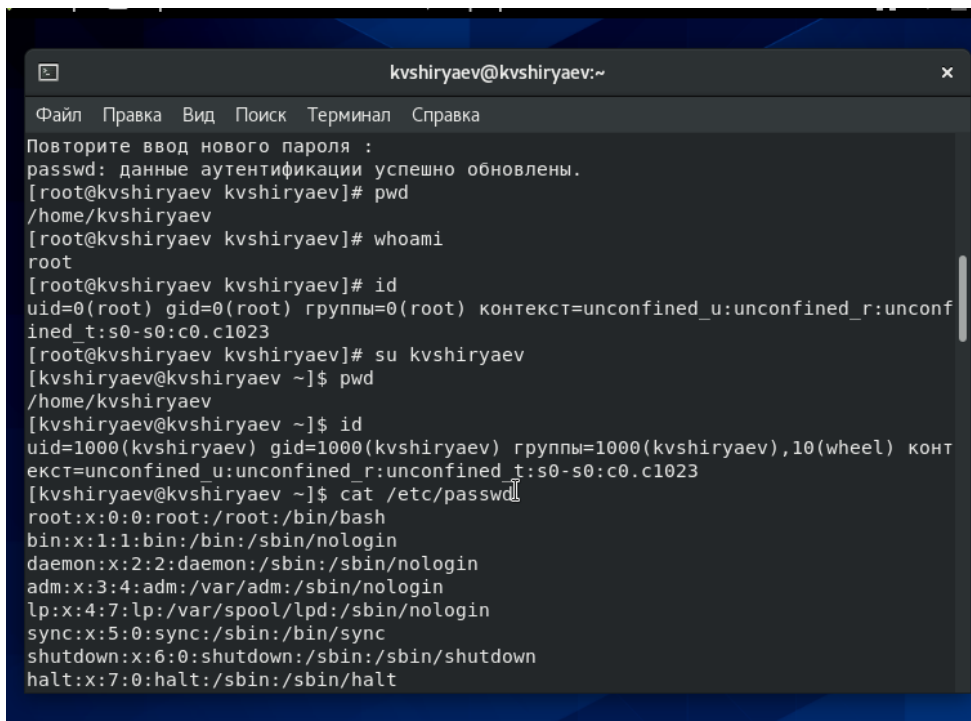
Добавили пользователя guest2 в группу guest с помощью команды `groupadd -a guest2 guest`

```
kvshiryaev@kvshiryaev:~
Файл Правка Вид Поиск Терминал Справка
Изменение пароля пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - не содержит достаточног
о числа РАЗЛИЧНЫХ символов
Повторите ввод нового пароля :
[root@kvshiryaev kvshiryaev]# passwd guest
Изменение пароля пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - слишком простой
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@kvshiryaev kvshiryaev]# pwd
/home/kvshiryaev
[root@kvshiryaev kvshiryaev]# whoami
root
[root@kvshiryaev kvshiryaev]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconf
ined_t:s0-s0:c0.c1023
[root@kvshiryaev kvshiryaev]# su kvshiryaev
[kvshiryaev@kvshiryaev ~]$ pwd
/home/kvshiryaev
[kvshiryaev@kvshiryaev ~]$ id
uid=1000(kvshiryaev) gid=1000(kvshiryaev) группы=1000(kvshiryaev),10(wheel) конт
екст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Figure 2: Добавление в группу

Два пользователя

Осуществили вход в систему от двух пользователей на двух разных консолях (вкладках): guest на первой консоли и guest2 на второй консоли

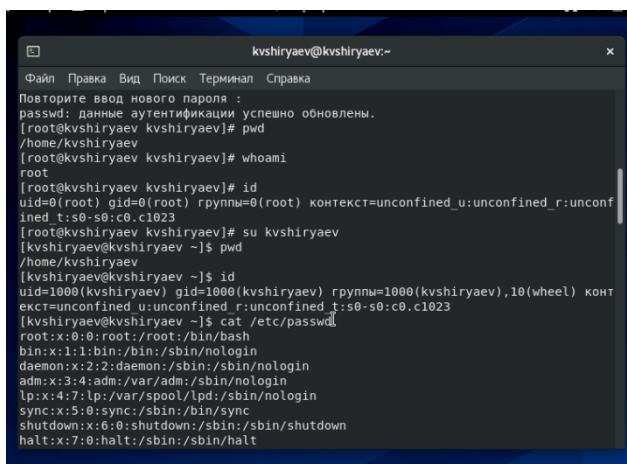


```
kvshiryaev@kvshiryaev:~  
Файл Правка Вид Поиск Терминал Справка  
Повторите ввод нового пароля :  
passwd: данные аутентификации успешно обновлены.  
[root@kvshiryaev kvshiryaev]# pwd  
/home/kvshiryaev  
[root@kvshiryaev kvshiryaev]# whoami  
root  
[root@kvshiryaev kvshiryaev]# id  
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[root@kvshiryaev kvshiryaev]# su kvshiryaev  
[kvshiryaev@kvshiryaev ~]$ pwd  
/home/kvshiryaev  
[kvshiryaev@kvshiryaev ~]$ id  
uid=1000(kvshiryaev) gid=1000(kvshiryaev) группы=1000(kvshiryaev),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[kvshiryaev@kvshiryaev ~]$ 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
```

Figure 3: Два пользователя

Текущая директория

Для обоих пользователей командой `pwd` определили директорию, в которой находились. Сравнили её с приглашениями командной строки и получили идентичные значения



```
kvshiryaev@kvshiryaev:~  
Файл Правка Вид Поиск Терминал Справка  
Повторите ввод нового пароля :  
passwd: данные аутентификации успешно обновлены.  
[root@kvshiryaev kvshiryaev]# pwd  
/home/kvshiryaev  
[root@kvshiryaev kvshiryaev]# whoami  
root  
[root@kvshiryaev kvshiryaev]# id  
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[root@kvshiryaev kvshiryaev]# su kvshiryaev  
[kvshiryaev@kvshiryaev ~]$ pwd  
/home/kvshiryaev  
[kvshiryaev@kvshiryaev ~]$ id  
uid=1000(kvshiryaev) gid=1000(kvshiryaev) группы=1000(kvshiryaev),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[kvshiryaev@kvshiryaev ~]$ 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
```

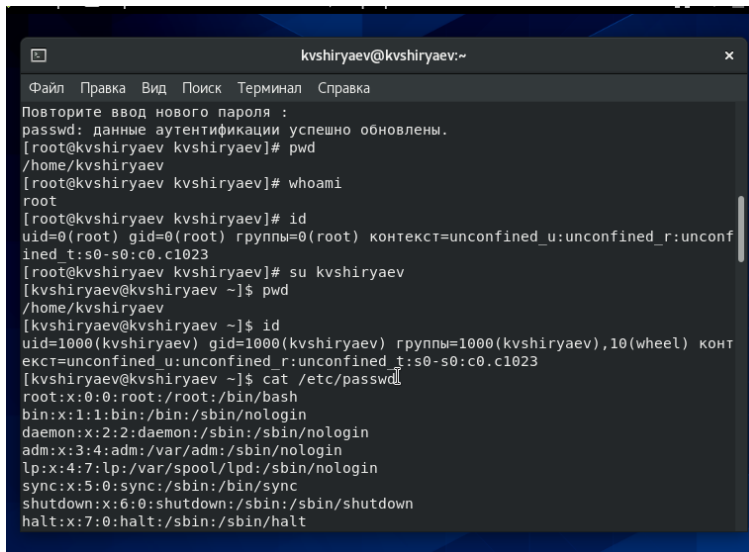
Figure 4: Текущая директория

Группы пользователей

Уточнили имя пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам.

Определили командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`.

Сравнили вывод команды `groups` с выводом команд `id -Gn` и `id -G`.



```
kvshiryaev@kvshiryaev:~  
Файл Правка Вид Поиск Терминал Справка  
Повторите ввод нового пароля :  
passwd: данные аутентификации успешно обновлены.  
[root@kvshiryaev kvshiryaev]# pwd  
/home/kvshiryaev  
[root@kvshiryaev kvshiryaev]# whoami  
root  
[root@kvshiryaev kvshiryaev]# id  
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[root@kvshiryaev kvshiryaev]# su kvshiryaev  
[kvshiryaev@kvshiryaev ~]$ pwd  
/home/kvshiryaev  
[kvshiryaev@kvshiryaev ~]$ id  
uid=1000(kvshiryaev) gid=1000(kvshiryaev) группы=1000(kvshiryaev),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[kvshiryaev@kvshiryaev ~]$ 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
```

Figure 5: Группы пользователей

Файл /etc/group

Сравнили полученную информацию с содержимым файла `/etc/group`, посмотрели файл командой `cat /etc/group`

```
kvshiryaev@kvshiryaev:~  
Файл Правка Вид Поиск Терминал Справка  
:/sbin/nologin  
gnome-initial-setup:x:975:975::/run/gnome-initial-setup:/sbin/nologin  
pesign:x:974:974:Group for the pesign signing daemon:/var/run/pesign:/sbin/nologin  
tcpdump:x:72:72::/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin  
kvshiryaev:x:1000:1000:kvshiryaev:/home/kvshiryaev:/bin/bash  
giest:x:1001:1001:~/home/giest:/bin/bash  
guest:x:1002:1002:~/home/guest:/bin/bash  
[kvshiryaev@kvshiryaev ~]$ ls -l /home/  
итого 4  
drwx-----. 3 giest      giest      78 фев 22 12:17 giest  
drwx-----. 3 guest      guest      78 фев 22 12:17 guest  
drwx-----. 15 kvshiryaev kvshiryaev 4096 фев 22 12:16 kvshiryaev  
[kvshiryaev@kvshiryaev ~]$ lsattr /home  
----- /home/kvshiryaev  
lsattr: Отказано в доступе While reading flags on /home/giest  
lsattr: Отказано в доступе While reading flags on /home/guest  
[kvshiryaev@kvshiryaev ~]$ cd ..  
[kvshiryaev@kvshiryaev home]$ cd kvshiryaev  
[kvshiryaev@kvshiryaev ~]$ mkdir dir1  
[kvshiryaev@kvshiryaev ~]$ ls -l lsattr  
ls: невозможно получить доступ к 'lsattr': Нет такого файла или каталога  
[kvshiryaev@kvshiryaev ~]$ ls -l
```

Figure 6: Файл /etc/group

Регистрация в группе

От имени пользователя guest2 выполнили регистрацию пользователя guest2 в группе guest командой `newgrp guest`

```
kvshiryaev@kvshiryaev:~  
Файл Правка Вид Поиск Терминал Справка  
[kvshiryaev@kvshiryaev ~]$ ls -l /home/  
итого 4  
drwx-----. 3 giest      giest      78 фев 22 12:17 giest  
drwx-----. 3 guest      guest      78 фев 22 12:17 guest  
drwx-----. 15 kvshiryaev kvshiryaev 4096 фев 22 12:16 kvshiryaev  
[kvshiryaev@kvshiryaev ~]$ lsattr /home  
----- /home/kvshiryaev  
lsattr: Отказано в доступе While reading flags on /home/giest  
lsattr: Отказано в доступе While reading flags on /home/guest  
[kvshiryaev@kvshiryaev ~]$ cd ..  
[kvshiryaev@kvshiryaev home]$ cd kvshiryaev  
[kvshiryaev@kvshiryaev ~]$ mkdir dir1  
[kvshiryaev@kvshiryaev ~]$ ls -l lsattr  
ls: невозможно получить доступ к 'lsattr': Нет такого файла или каталога  
[kvshiryaev@kvshiryaev ~]$ ls -l  
итого 8  
drwxrwxr-x. 2 kvshiryaev kvshiryaev 6 фев 22 12:25 dir1  
drwxr-xr-x. 2 kvshiryaev kvshiryaev 6 фев 22 11:48 Видео  
drwxr-xr-x. 2 kvshiryaev kvshiryaev 6 фев 22 11:48 Документы  
drwxr-xr-x. 2 kvshiryaev kvshiryaev 6 фев 22 11:48 Загрузки  
drwxr-xr-x. 2 kvshiryaev kvshiryaev 68 фев 22 12:14 Изображения  
drwxr-xr-x. 2 kvshiryaev kvshiryaev 6 фев 22 11:48 Музыка  
drwxr-xr-x. 2 kvshiryaev kvshiryaev 6 фев 22 11:48 Общедоступные  
drwxr-xr-x. 2 kvshiryaev kvshiryaev 6 фев 22 11:48 Рабочий стол
```

Figure 7: Регистрация в группе

Права для группы

От имени пользователя guest изменили права директории /home/guest, разрешив все действия для пользователей группы, применили команду `chmod g+rw /home/guest`

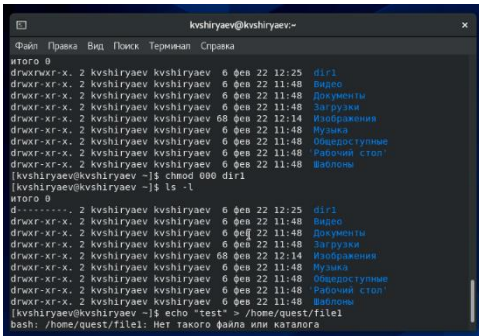


Figure 8: Права для группы

Снятие атрибутов

От имени пользователя guest сняли с директории /home/guest/dir1 все атрибуты командой `chmod 000 dir1`, проверили правильность снятия атрибутов

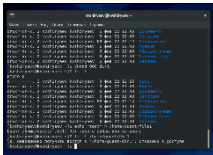


Figure 9: Снятие атрибутов

Таблицы

Меняя атрибуты у директории `dir1` и файла `file1` от имени пользователя `guest` и делая проверку от пользователя `guest2`, заполнили таблицу, определив опытным путём, какие операции разрешены, а какие нет.

На основании заполненной таблицы определили те или иные минимально необходимые права для выполнения пользователем `guest2` операций внутри директории `dir1` и заполнили вторую таблицу.

Установленные права и разрешённые действия для групп:

Права директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
d----- (000)	----- (000)	-	-	-	-	-	-	-	-
d-----x--- (010)	----- (000)	-	-	-	-	+	-	-	+
d----w---- (020)	----- (000)	-	-	-	-	-	-	-	-
d----wx--- (030)	----- (000)	+	+	-	-	+	-	+	+
d---r----- (040)	----- (000)	-	-	-	-	-	+	-	-
d---r-x--- (050)	----- (000)	-	-	-	-	+	+	-	+
d---rw---- (060)	----- (000)	-	-	-	-	-	+	-	-
d---rwx--- (070)	----- (000)	+	+	-	-	+	+	+	+
d-----x--- (010)	-----x--- (010)	-	-	-	-	-	-	-	-
d-----x--- (010)	-----x--- (010)	-	-	-	-	+	-	-	+
d----w---- (020)	-----x--- (010)	-	-	-	-	-	-	-	-

d-----wx----	(030)	-----x----	(010)	+	+	-	-	+	-	+	+
d---r-----	(040)	-----x----	(010)	-	-	-	-	-	+	-	-
d---r-x----	(050)	-----x----	(010)	-	-	-	-	+	+	-	+
d---rw----	(060)	-----x----	(010)	-	-	-	-	-	+	-	-
d---rwx----	(070)	-----x----	(010)	+	+	-	-	+	+	+	+
d-----w----	(000)	-----w----	(020)	-	-	-	-	-	-	-	-
d-----x----	(010)	-----w----	(020)	-	-	+	-	+	-	-	+
d---w----	(020)	-----w----	(020)	-	-	-	-	-	-	-	-
d---wx----	(030)	-----w----	(020)	+	+	+	-	+	-	+	+
d---r-----	(040)	-----w----	(020)	-	-	-	-	-	+	-	-
d---r-x----	(050)	-----w----	(020)	-	-	+	-	+	+	-	+
d---rw----	(060)	-----w----	(020)	-	-	-	-	-	+	-	-
d---rwx----	(070)	-----w----	(020)	+	+	+	-	+	+	+	+
d-----wx----	(000)	-----wx----	(030)	-	-	-	-	-	-	-	-
d-----x----	(010)	-----wx----	(030)	-	-	+	-	+	-	-	+
d---w----	(020)	-----wx----	(030)	-	-	-	-	-	-	-	-
d---wx----	(030)	-----wx----	(030)	+	+	+	-	+	-	+	+
d---r-----	(040)	-----wx----	(030)	-	-	-	-	-	+	-	-
d---r-x----	(050)	-----wx----	(030)	-	-	+	-	+	+	-	+
d---rw----	(060)	-----wx----	(030)	-	-	-	-	-	+	-	-
d---rwx----	(070)	-----wx----	(030)	+	+	+	-	+	+	+	+
d-----r-----	(040)	----r-----	(040)	-	-	-	-	-	-	-	-
d-----x----	(010)	----r-----	(040)	-	-	-	+	+	-	-	+
d---w----	(020)	----r-----	(040)	-	-	-	-	-	-	-	-
d---wx----	(030)	----r-----	(040)	+	+	-	+	+	-	+	+
d---r-----	(040)	----r-----	(040)	-	-	-	-	-	+	-	-
d---r-x----	(050)	----r-----	(040)	-	-	-	+	+	+	-	+
d---rw----	(060)	----r-----	(040)	-	-	-	-	-	+	-	-
d---rwx----	(070)	----r-----	(040)	+	+	-	+	+	+	+	+
d-----r-x----	(050)	----r-x----	(050)	-	-	-	-	-	-	-	-
d-----x----	(010)	----r-x----	(050)	-	-	-	+	+	-	-	+
d---w----	(020)	----r-x----	(050)	-	-	-	-	-	-	-	-
d---wx----	(030)	----r-x----	(050)	+	+	-	+	+	-	+	+
d---r-----	(040)	----r-x----	(050)	-	-	-	-	-	+	-	-
d---r-x----	(050)	----r-x----	(050)	-	-	-	+	+	+	-	+
d---rw----	(060)	----r-x----	(050)	-	-	-	-	-	+	-	-
d---rwx----	(070)	----r-x----	(050)	+	+	-	+	+	+	+	+
d-----rw----	(060)	----rw----	(060)	-	-	-	-	-	-	-	-

d-----x--- (010)	----rw---- (060)	-	-	+	+	+	-	-	+
d----w---- (020)	----rw---- (060)	-	-	-	-	-	-	-	-
d----wx--- (030)	----rw---- (060)	+	+	+	+	+	-	+	+
d---r----- (040)	----rw---- (060)	-	-	-	-	-	+	-	-
d---r-x--- (050)	----rw---- (060)	-	-	+	+	+	+	-	+
d---rw---- (060)	----rw---- (060)	-	-	-	-	-	+	-	-
d---rwx--- (070)	----rw---- (060)	+	+	+	+	+	+	+	+
d----- (000)	----rwx--- (070)	-	-	-	-	-	-	-	-
d-----x--- (010)	----rwx--- (070)	-	-	+	+	+	-	-	+
d----w---- (020)	----rwx--- (070)	-	-	-	-	-	-	-	-
d----wx--- (030)	----rwx--- (070)	+	+	+	+	+	-	+	+
d---r----- (040)	----rwx--- (070)	-	-	-	-	-	+	-	-
d---r-x--- (050)	----rwx--- (070)	-	-	+	+	+	+	-	+
d---rw---- (060)	----rwx--- (070)	-	-	-	-	-	+	-	-
d---rwx--- (070)	----rwx--- (070)	+	+	+	+	+	+	+	+

Минимальные права для совершения операций:

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d----wx--- (030)	----- (000)
Удаление файла	d----wx--- (030)	----- (000)
Чтение файла	d-----x--- (010)	----r----- (040)
Запись в файл	d-----x--- (010)	-----w---- (020)
Переименование файла	d----wx--- (030)	----- (000)
Создание поддиректории	d----wx--- (030)	----- (000)
Удаление поддиректории	d----wx--- (030)	----- (000)

Вывод

В ходе лабораторной работы получили практические навыки работы в консоли с атрибутами файлов для групп пользователей