

Лабораторная работа №3

Дискреционное разграничение прав в Linux. Два пользователя

Роман Владимирович Иванов

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	18
5	Список литературы	19

Список иллюстраций

3.1	Создание учетной записи guest	7
3.2	Задание пароля для учетной записи	7
3.3	Создание учетной записи guest2	8
3.4	Добавление пользователя guest2 в группу guest	8
3.5	Вход в систему для двух пользователей	8
3.6	Определение текущей директории	9
3.7	Уточнение имени пользователей	9
3.8	Уточнение имени пользователей	10
3.9	Уточнение имени пользователей	10
3.10	Сравнение полученной информации (часть 1)	11
3.11	Сравнение полученной информации (часть 2)	11
3.12	Регистрация пользователя guest2 в группе guest	12
3.13	Изменение прав директории	12
3.14	Снятие всех атрибутов с директории	13

Список таблиц

3.1	Установленные права и разрешенные действия для групп	13
3.2	Минимальные права для совершения операций от имени пользователей, входящих в группу	17

1 Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

2 Задание

1. Создать учетные записи `guest` и `guest2`.
2. Войти от имени двух пользователей в две разные консоли и выполнить ряд команд.
3. Заполнить таблицу “Установленные права и разрешенные действия для групп”
4. Заполнить таблицу “Минимальные права для совершения операций от имени пользователей, входящих в группу”

3 Выполнение лабораторной работы

1. В установленной операционной системе создал учётную запись пользователя `guest` (использовал учётную запись администратора) (рис - @fig:001). Для этого использовал команду `user add guess`

```
[rvivanov@rvivanov Рабочий стол]$ su
Пароль:
[root@rvivanov Рабочий стол]# useradd guest
```

Рис. 3.1: Создание учетной записи `guest`

Задал пароль для пользователя `guest` (использовал учётную запись администратора) (рис - @fig:002). Для этого использовал команду `passwd guest`

```
[root@rvivanov Рабочий стол]# passwd guest
Смена пароля для пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой
НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой
Повторите ввод нового пароля :
passwd: все токены проверки подлинности успешно обновлены
```

Рис. 3.2: Задание пароля для учетной записи

Аналогично создал второго пользователя `guest2` (рис - @fig:003).

```
[root@rvivanov Рабочий стол]# useradd guest2
[root@rvivanov Рабочий стол]# passwd guest2
Смена пароля для пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой
НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой
Повторите ввод нового пароля :
passwd: все токены проверки подлинности успешно обновлены.
```

Рис. 3.3: Создание учетной записи guest2

Добавил пользователя guest2 в группу guest (рис -@fig:004):

```
[root@rvivanov Рабочий стол]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
```

Рис. 3.4: Добавление пользователя guest2 в группу guest

2. Вошел в систему от двух пользователей на двух разных консолях (рис -@fig:005).

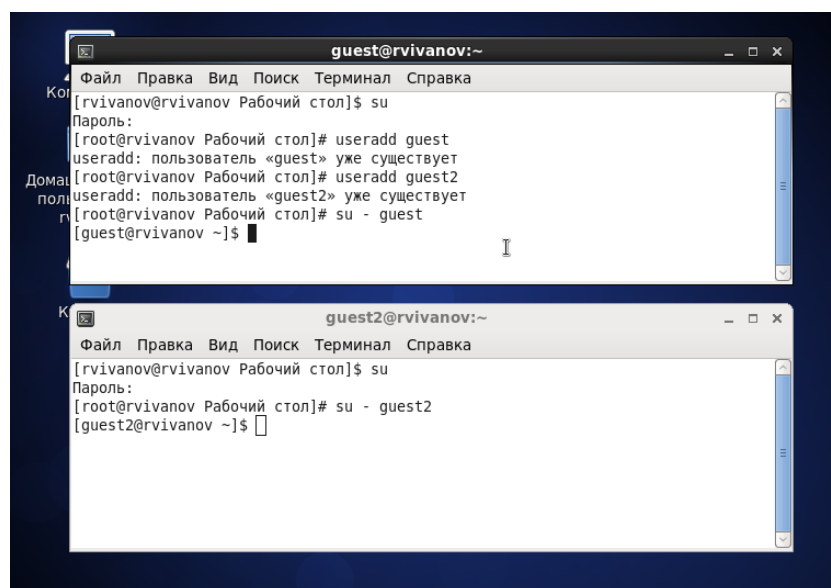


Рис. 3.5: Вход в систему для двух пользователей

Для обоих пользователей командой `pwd` определил директории, в которых я нахожусь. Они совпадают с приглашением командной строки (рис -@fig:006).

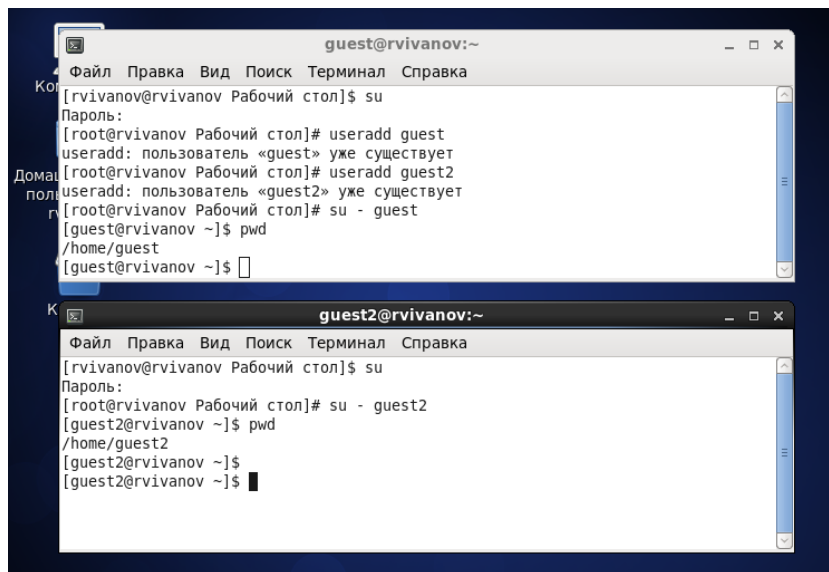


Рис. 3.6: Определение текущей директории

Уточнил имена своих пользователей командой `whoami` (рис -@fig:007), их группы, кто входит в них и к каким группам принадлежат они сами, а также определил командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2` (рис -@fig:008).

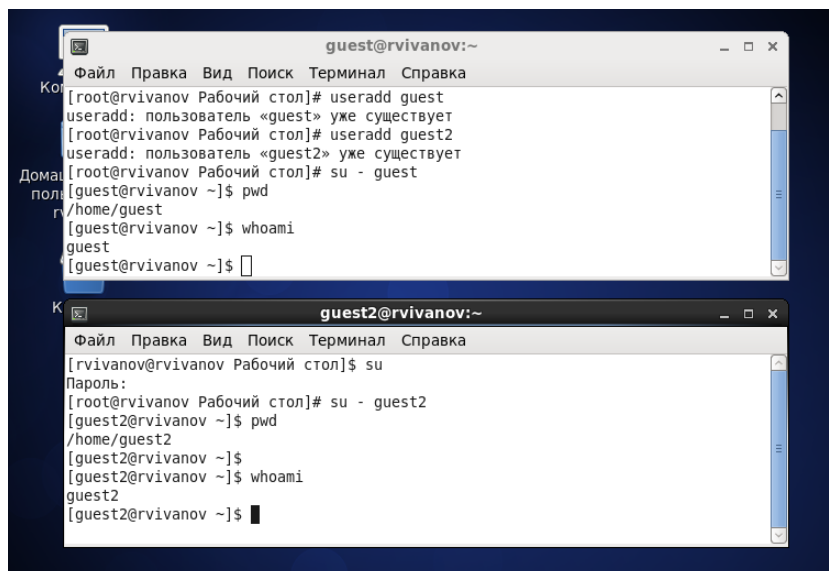


Рис. 3.7: Уточнение имени пользователей

The image shows two terminal windows. The top window is titled 'guest@rvivanov:~' and contains the following commands and output:

```
[guest@rvivanov ~]$ gpasswd -a guest2 guest
gpasswd: доступ запрещен.
[guest@rvivanov ~]$ id
uid=501(guest) gid=501(guest) rгруппы=501(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@rvivanov ~]$ groups guest
guest : guest
[guest@rvivanov ~]$ groups guest2
guest2 : guest2 guest
[guest@rvivanov ~]$
```

The bottom window is titled 'guest2@rvivanov:~' and contains the following commands and output:

```
[guest2@rvivanov ~]$
[guest2@rvivanov ~]$ whoami
guest2
[guest2@rvivanov ~]$ id
uid=502(guest2) gid=502(guest2) rгруппы=502(guest2),501(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@rvivanov ~]$ id
uid=502(guest2) gid=502(guest2) rгруппы=502(guest2),501(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@rvivanov ~]$
```

Рис. 3.8: Уточнение имени пользователей

Сравнил вывод команды `groups` с выводом команд `id -Gn` и `id -G` (рис - @fig:009). Группы совпадают, однако при выводе команд `id -Gn` и `id -G` объемнее.

The image shows two terminal windows. The top window is titled 'guest@rvivanov:~' and contains the following commands and output:

```
[guest@rvivanov ~]$ id
r:unconfined t:s0-s0:c0.c1023
[guest@rvivanov ~]$ groups guest
guest : guest
[guest@rvivanov ~]$ groups guest2
guest2 : guest2 guest
[guest@rvivanov ~]$ id -Gn
guest
[guest@rvivanov ~]$ id -G
501
[guest@rvivanov ~]$
```

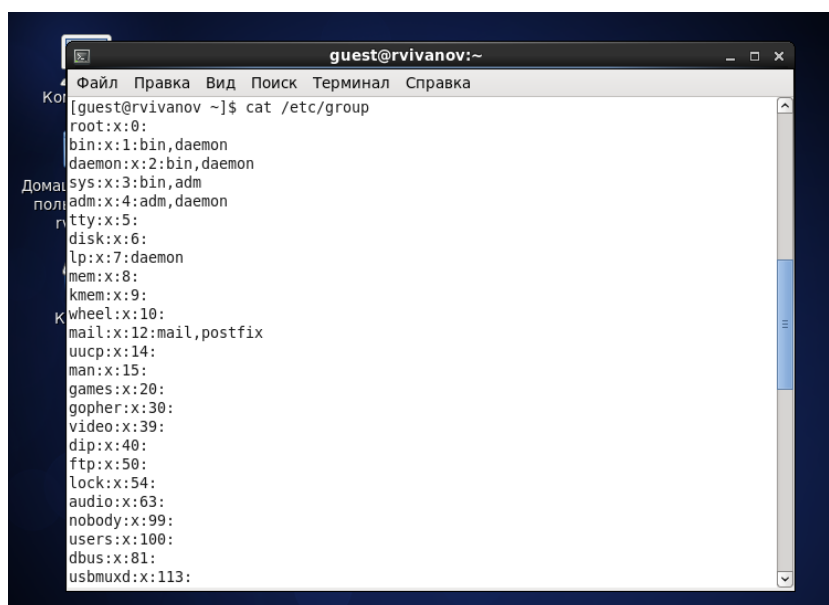
The bottom window is titled 'guest2@rvivanov:~' and contains the following commands and output:

```
[guest2@rvivanov ~]$ id
uid=502(guest2) gid=502(guest2) rгруппы=502(guest2),501(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@rvivanov ~]$ id
uid=502(guest2) gid=502(guest2) rгруппы=502(guest2),501(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@rvivanov ~]$ id -gn
guest2
[guest2@rvivanov ~]$ id -G
502 501
[guest2@rvivanov ~]$
```

Рис. 3.9: Уточнение имени пользователей

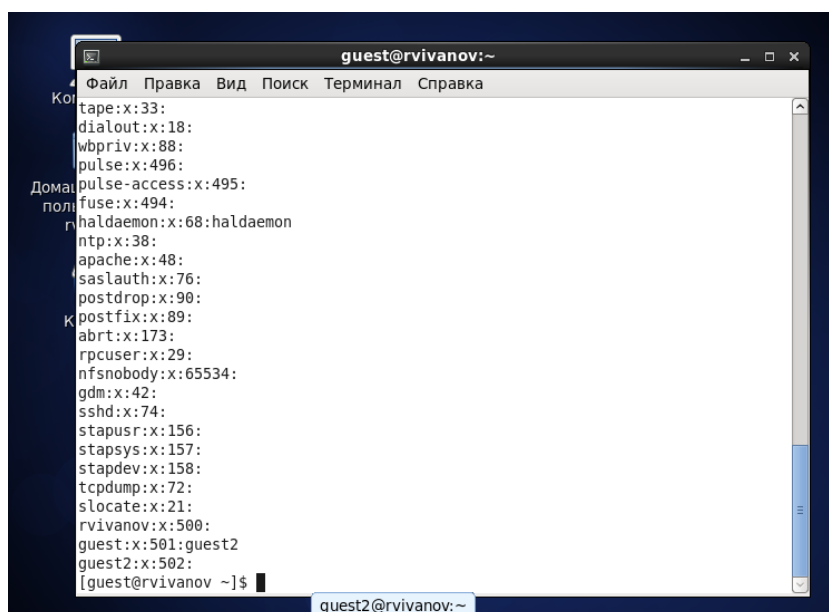
Сравнил полученную информацию с содержимым файла `/etc/group`. Про-

смотрел файл командой `cat /etc/group` (рис -@fig:010, рис -@fig:011)



```
guest@rvivanov:~  
[guest@rvivanov ~]$ cat /etc/group  
root:x:0:  
bin:x:1:bin,daemon  
daemon:x:2:bin,daemon  
sys:x:3:bin,adm  
adm:x:4:adm,daemon  
tty:x:5:  
disk:x:6:  
lp:x:7:daemon  
mem:x:8:  
kmem:x:9:  
wheel:x:10:  
mail:x:12:mail,postfix  
uucp:x:14:  
man:x:15:  
games:x:20:  
gopher:x:30:  
video:x:39:  
dip:x:40:  
ftp:x:50:  
lock:x:54:  
audio:x:63:  
nobody:x:99:  
users:x:100:  
dbus:x:81:  
usbmuxd:x:113:
```

Рис. 3.10: Сравнение полученной информации (часть 1)

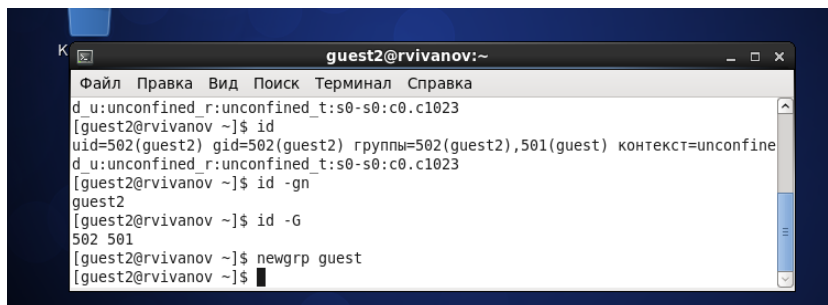


```
guest@rvivanov:~  
[guest@rvivanov ~]$ cat /etc/group  
tape:x:33:  
dialout:x:18:  
wbpriv:x:88:  
pulse:x:496:  
pulse-access:x:495:  
fuse:x:494:  
haldaemon:x:68:haldaemon  
ntp:x:38:  
apache:x:48:  
sasauth:x:76:  
postdrop:x:90:  
postfix:x:89:  
abrt:x:173:  
rpcuser:x:29:  
nfsnobody:x:65534:  
gdm:x:42:  
sshd:x:74:  
stapusr:x:156:  
stapusr:x:157:  
stapdev:x:158:  
tcpdump:x:72:  
slocate:x:21:  
rvivanov:x:500:  
guest:x:501:guest2  
guest2:x:502:  
[guest@rvivanov ~]$
```

Рис. 3.11: Сравнение полученной информации (часть 2)

Как видно из рисунка, информация об имени пользователя совпадает с полученной ранее информацией.

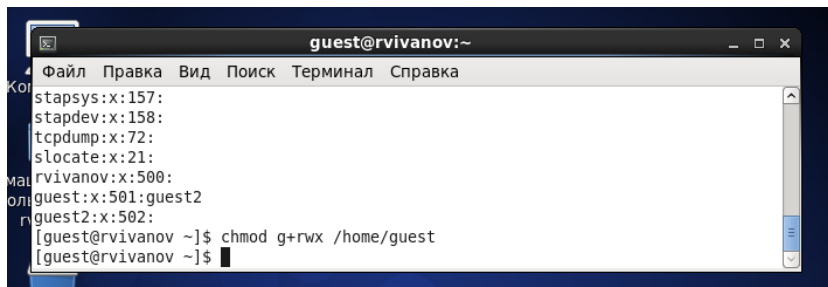
От имени пользователя guest2 выполнил регистрацию пользователя guest2 в группе guest командой `newgrp guest` (рис -@fig:012)



```
guest2@rvivanov:~  
Файл Правка Вид Поиск Терминал Справка  
d u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest2@rvivanov ~]$ id  
uid=502(guest2) gid=502(guest2) группы=502(guest2),501(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
d u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest2@rvivanov ~]$ id -gn  
guest2  
[guest2@rvivanov ~]$ id -G  
502 501  
[guest2@rvivanov ~]$ newgrp guest  
[guest2@rvivanov ~]$
```

Рис. 3.12: Регистрация пользователя guest2 в группе guest

От имени пользователя guest изменил права директории `/home/guest`, разрешив все действия для пользователей группы, командой `chmod g+rxw /home/guest` (рис -@fig:013)



```
guest@rvivanov:~  
Файл Правка Вид Поиск Терминал Справка  
stapsys:x:157:  
stapdev:x:158:  
tcpdump:x:72:  
slocate:x:21:  
rvivanov:x:500:  
guest:x:501:guest2  
guest2:x:502:  
[guest@rvivanov ~]$ chmod g+rxw /home/guest  
[guest@rvivanov ~]$
```

Рис. 3.13: Изменение прав директории

От имени пользователя guest снял с директории `/home/guest/dir1` все атрибуты командой `chmod 000 dir1`. Проверил это действие с помощью команды `ls -l` (рис -@fig:014)

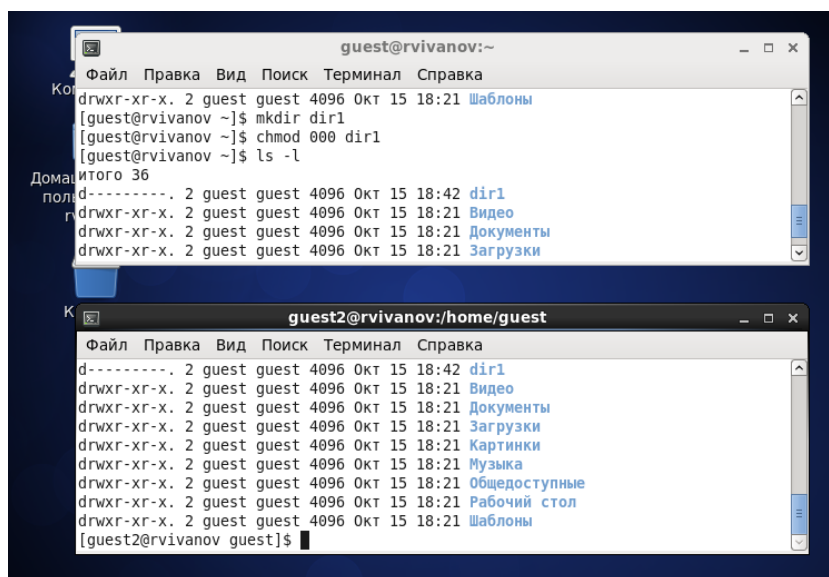


Рис. 3.14: Снятие всех атрибутов с директории

3. Заполнил таблицу “Установленные права и разрешенные действия для групп”, меняя атрибуты у директории `dir1` и файла `file1` от имени пользователя `guest`, делая проверку от пользователя `guest2` и определяя опытным путем, какие операции разрешены, а какие нет. “+” - операция разрешена, “-” - операция не разрешена (таб. 3.1)

Таблица 3.1: Установленные права и разрешенные действия для групп

Права	Сме-								
	Со-	Уда-				на			
ди-рек-то-рии	Права фай-ла	зда-ние фай-ла	ле-ние фай-ла	За-пись в файл	Чте-ние фай-ла	ди-рек-то-рии	Просмотр файлов в директо-рии	Пере-имено-вание файла	Смена атрибу-тов фай-ла
d(000)	(000)	-	-	-	-	-	-	-	-
d(000)	(010)	-	-	-	-	-	-	-	-
d(000)	(020)	-	-	-	-	-	-	-	-

Пра- ва	Со- зда- ние	Уда- ле- ние	За- пись	Чте- ние	Сме- на	Просмотр	Пере- имено- вание	Смена
ди- рек- то- рии	Пра- ва фай- ла	зда- ние фай- ла	ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	файлов в директо- рии	атрибу- тов файла
d(000)	(030)	-	-	-	-	-	-	-
d(000)	(040)	-	-	-	-	-	-	-
d(000)	(050)	-	-	-	-	-	-	-
d(000)	(060)	-	-	-	-	-	-	-
d(000)	(070)	-	-	-	-	-	-	-
d(010)	(000)	-	-	-	-	-	-	-
d(010)	(010)	-	-	-	-	-	-	-
d(010)	(020)	-	-	+	-	-	-	-
d(010)	(030)	-	-	+	-	-	-	-
d(010)	(040)	-	-	-	+	-	-	-
d(010)	(050)	-	-	-	+	-	-	-
d(010)	(060)	-	-	+	+	-	-	-
d(100)	(070)	-	-	+	+	-	-	-
d(020)	(000)	-	-	-	-	-	-	-
d(020)	(010)	-	-	-	-	-	-	-
d(020)	(020)	-	-	-	-	-	-	-
d(020)	(030)	-	-	-	-	-	-	-
d(020)	(040)	-	-	-	-	-	-	-
d(020)	(050)	-	-	-	-	-	-	-
d(020)	(060)	-	-	-	-	-	-	-
d(020)	(070)	-	-	-	-	-	-	-
d(030)	(000)	+	+	-	-	+	-	+
d(030)	(010)	+	+	-	-	+	-	+

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

Пра- ва	Пра-	Со-	Уда-	За-	Чте-	Сме-			
ди-	ва	зда-	ле-	пись	ние	ди-	Просмотр	Пере-	Смена
рек-	фай-	фай-	фай-	в	фай-	рек-	файлов в	имено-	атрибу-
то-	ла	ла	ла	файл	ла	то-	директо-	вание	тов
рии	ла	ла	ла	файл	ла	рии	рии	файла	файла
d(060)	(010)	-	-	-	-	-	+	-	-
d(060)	(020)	-	-	-	-	-	+	-	-
d(060)	(030)	-	-	-	-	-	+	-	-
d(060)	(040)	-	-	-	-	-	+	-	-
d(060)	(050)	-	-	-	-	-	+	-	-
d(060)	(060)	-	-	-	-	-	+	-	-
d(060)	(070)	-	-	-	-	-	+	-	-
d(070)	(000)	+	+	-	-	+	+	+	+
d(070)	(010)	+	+	-	-	+	+	+	+
d(070)	(020)	+	+	-	-	+	+	+	+
d(070)	(030)	+	+	-	-	+	+	+	+
d(070)	(040)	+	+	-	-	+	+	+	+
d(070)	(050)	+	+	-	-	+	+	+	+
d(070)	(060)	+	+	-	-	+	+	+	+
d(070)	(070)	+	+	-	-	+	+	+	+

4. На основании заполненной выше таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории `dir1`, заполняя таблицу “Минимальные права для совершения операций от имени пользователей, входящих в группу” (таб. 3.2).

Таблица 3.2: Минимальные права для совершения операций от имени пользователей, входящих в группу

Операция	min права на директорию	min права на файл
Создание файла	(- w x)	(- - -)
Удаление файла	(- w x)	(- - -)
Чтение файла	(- - x)	(r - -)
Запись в файл	(- - x)	(- w -)
Переименование файла	(- w x)	(- - -)
Создание поддиректории	(- w x)	(- - -)
Удаление поддиректории	(- w x / r-x)	(- - -)

По сравнению с таблицей из предыдущей лабораторной работой, в которой рассматривались права доступа владельца, таблица 3.2 не везде имеет права на запись, чтения и изменение атрибутов файлов. Это объясняется тем, что в данной работе рассматривались права доступа для группы, к которой принадлежат владельцы.

4 Выводы

Получил практические навыки работы в консоли с атрибутами файлов для групп пользователей.

5 Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 3. Дискреционное разграничение прав в Linux. Два пользователя