

Лабораторная работа 3

Дискреционное разграничение прав в Linux. Два пользователя

Бешкуров Михаил Борисович

Содержание

1	Цель работы	3
2	Задание	4
3	Выполнение лабораторной работы	5
4	Выводы	17
5	Список литературы	18

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 guest`

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

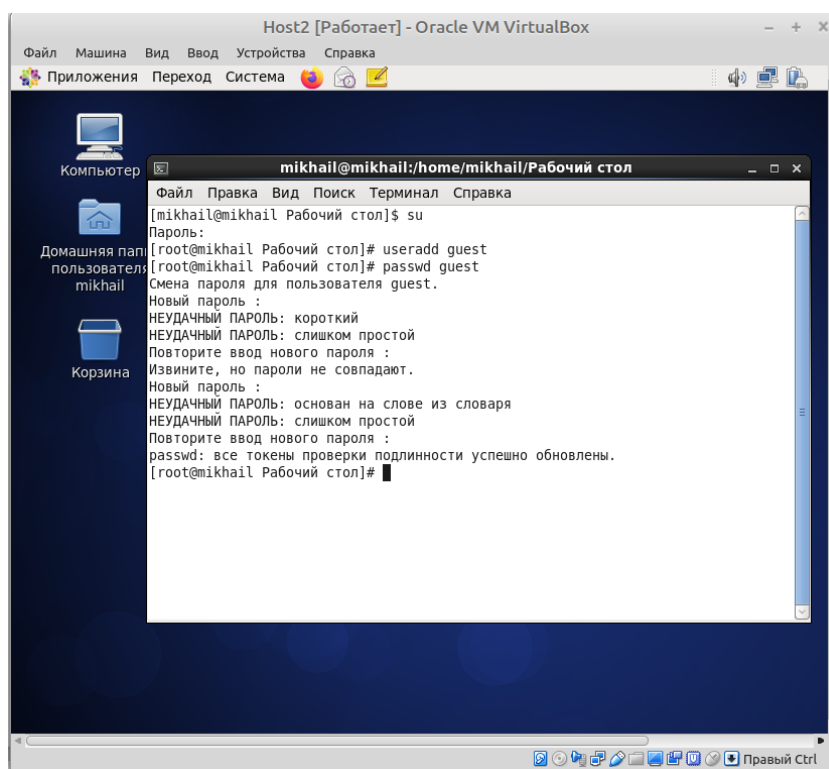


Рис. 3.1: Создание учетной записи guest

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

```
[mikhail@mikhail home]$ su
Пароль:
[root@mikhail home]# useradd guest2
[root@mikhail home]# passwd guest2
Смена пароля для пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: основан на слове из словаря
НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой
Повторите ввод нового пароля :
passwd: все токены проверки подлинности успешно обновлены.
```

Рис. 3.2: Создание учетной записи guest2

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

```
[root@mikhail ~]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[root@mikhail ~]# █
```

Рис. 3.3: Добавление пользователя guest2 в группу guest

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

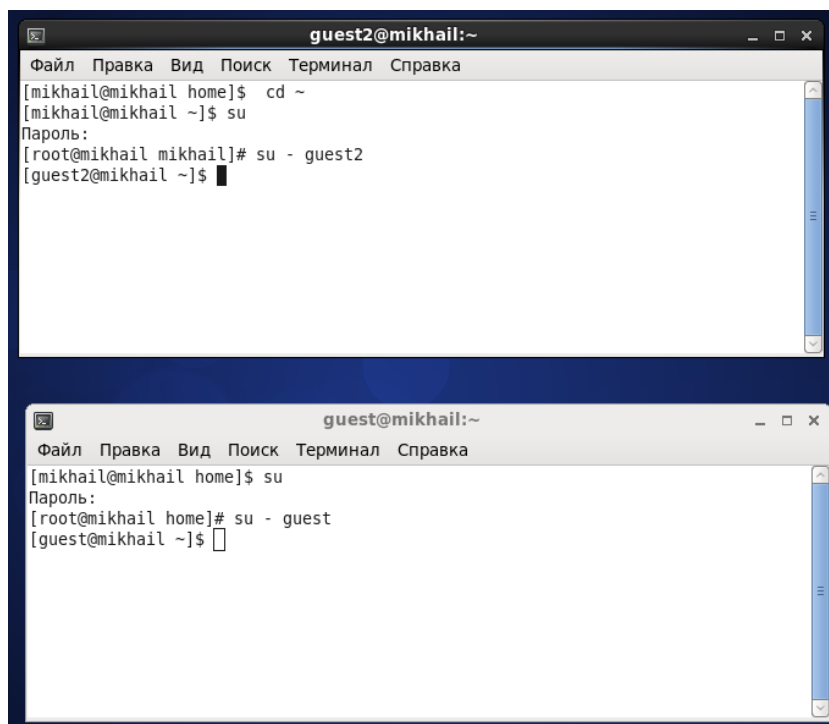


Рис. 3.4: Вход в систему для двух пользователей

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

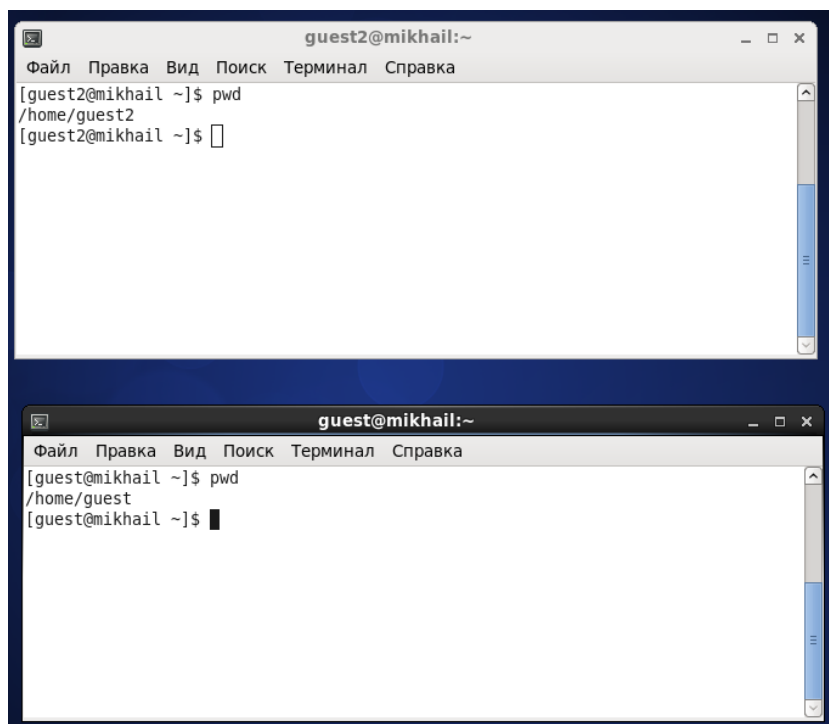


Рис. 3.5: Определение текущей директории

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).

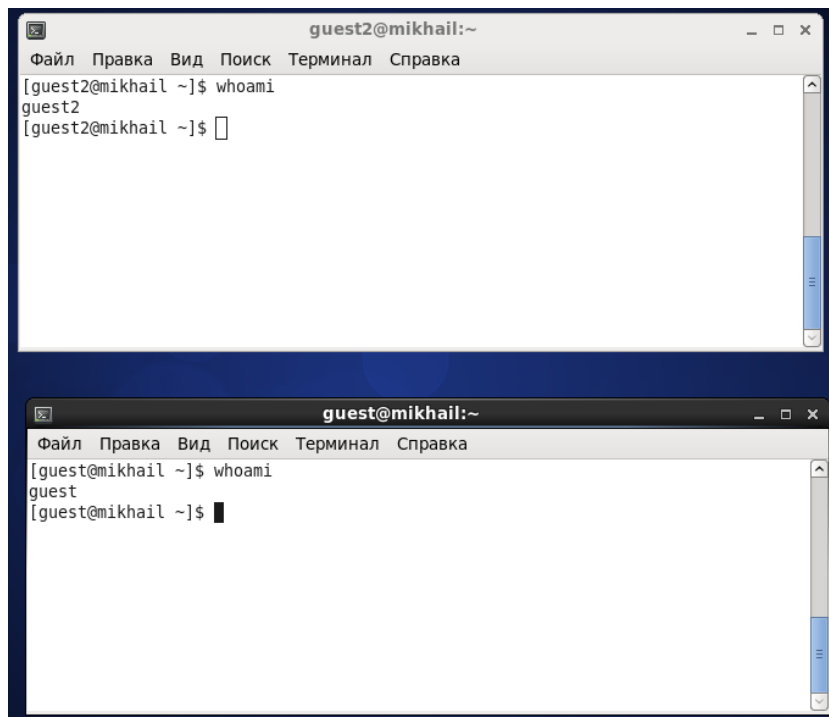
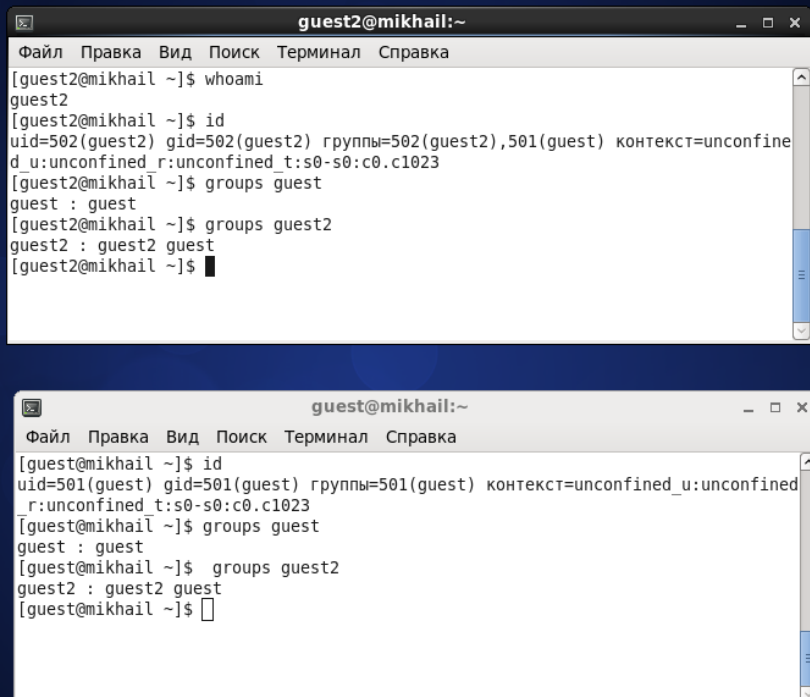


Рис. 3.6: Уточнение имени пользователей



The image shows two terminal windows from the Mikhael Linux distribution. The top window is titled 'guest2@mikhail:~' and shows the execution of 'whoami' (returns 'guest2'), 'id' (returns 'uid=502(guest2) gid=502(guest2) группы=502(guest2),501(guest) контекст=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023'), and 'groups guest' (returns 'guest : guest'). The bottom window is titled 'guest@mikhail:~' and shows the execution of 'id' (returns 'uid=501(guest) gid=501(guest) группы=501(guest) контекст=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023'), 'groups guest' (returns 'guest : guest'), and 'groups guest2' (returns 'guest2 : guest2 guest').

```
guest2@mikhail:~  
Файл Правка Вид Поиск Терминал Справка  
[guest2@mikhail ~]$ whoami  
guest2  
[guest2@mikhail ~]$ id  
uid=502(guest2) gid=502(guest2) группы=502(guest2),501(guest) контекст=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023  
[guest2@mikhail ~]$ groups guest  
guest : guest  
[guest2@mikhail ~]$ groups guest2  
guest2 : guest2 guest  
[guest2@mikhail ~]$  
  
guest@mikhail:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@mikhail ~]$ id  
uid=501(guest) gid=501(guest) группы=501(guest) контекст=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023  
[guest@mikhail ~]$ groups guest  
guest : guest  
[guest@mikhail ~]$ groups guest2  
guest2 : guest2 guest  
[guest@mikhail ~]$
```

Рис. 3.7: 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.

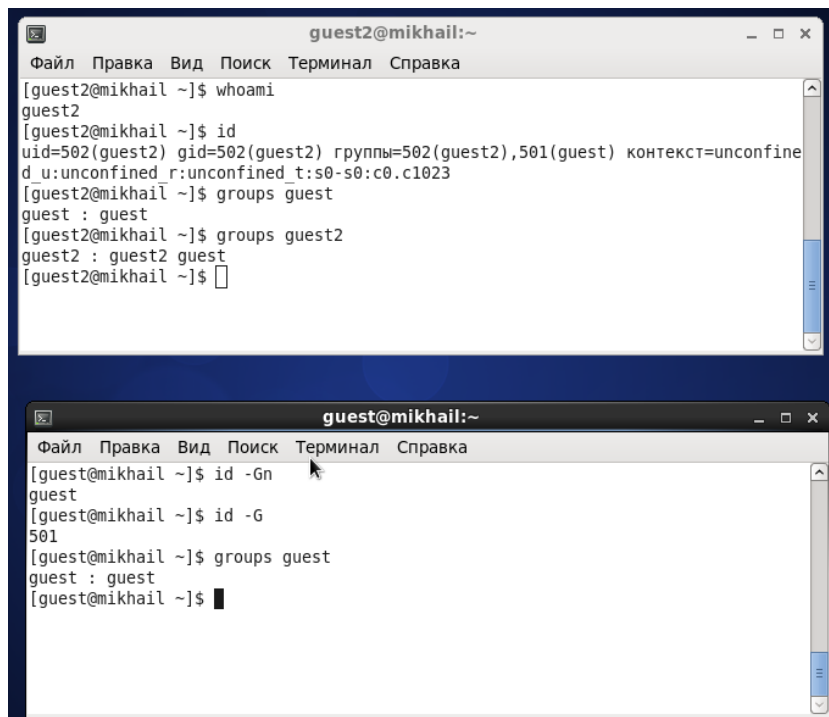


Рис. 3.8: Уточнение имени пользователей

Сравнил полученную информацию с содержимым файла /etc/group. Просмотрел файл командой `cat /etc/group` (рис @fig:010, рис @fig:011)

```
[guest2@mikhail ~]$ 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:
```

Рис. 3.9: Сравнение полученной информации (часть 1)

```

apache:x:48:
saslauth: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:
mikhail:x:500:
guest:x:501:guest2
guest2:x:502:

```

Рис. 3.10: 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)

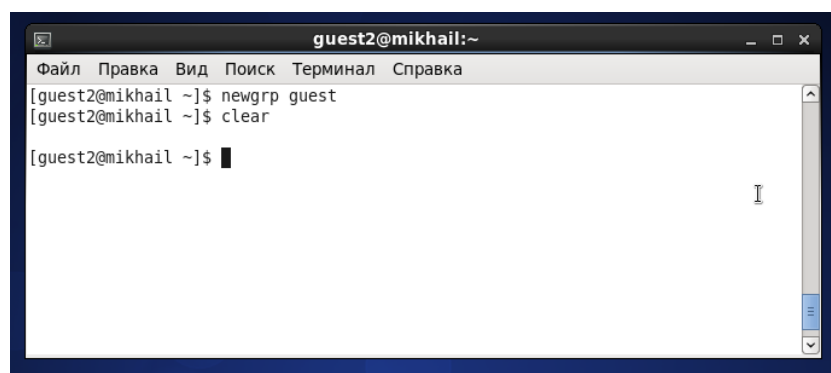


Рис. 3.11: Регистрация пользователя guest2 в группе guest

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

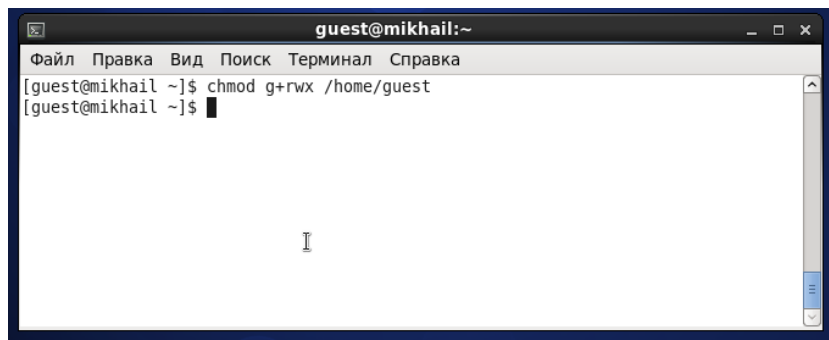


Рис. 3.12: Изменение прав директории

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)

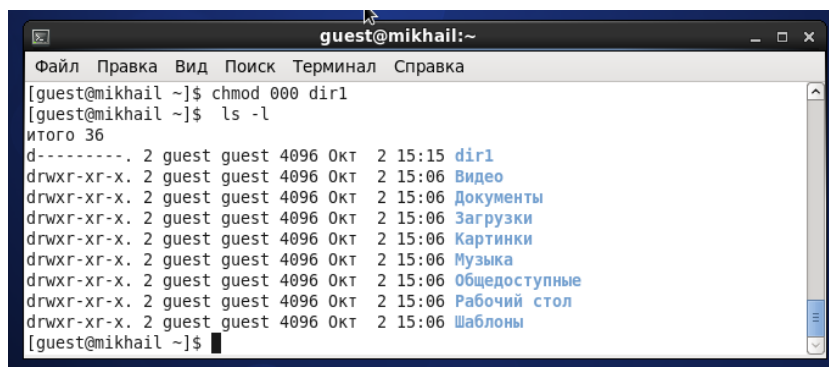


Рис. 3.13: Снятие всех атрибутов с директории

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

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

Пра- ва	Со- зда- ние	Уда- 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(020)	(050)	-	-	-	-	-	-	-
d(020)	(060)	-	-	-	-	-	-	-
d(020)	(070)	-	-	-	-	-	-	-
d(030)	(000)	+	+	-	-	+	-	+
d(030)	(010)	+	+	-	-	+	-	+
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)	-	-	+	-	-	+	-

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