

# Лабораторная работа №3

Дискреционное разграничение прав в Linux. Два пользователя

Ли Тимофей Александрович

# Содержание

Цель работы	5
Выполнение лабораторной работы	6
Выводы	13

## Список таблиц

0.1	Установленные права и разрешённые действия для групп . . . . .	9
0.2	Минимальные права для совершения операций от имени пользователей, входящих в группу . . . . .	12

## Список иллюстраций

0.1	создание и добавление в группу . . . . .	6
0.2	pwd для обоих . . . . .	6
0.3	whoami, groups, id . . . . .	7
0.4	etc/groups . . . . .	7
0.5	регистрация и доступ . . . . .	8
0.6	фрагмент проверки разрешений . . . . .	8
0.7	проверка создания поддиректории . . . . .	12

## Цель работы

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

# Выполнение лабораторной работы

Пользователь `guest1` у меня уже был с прошлой лабораторной работы, поэтому, используя `root`, создал пользователя `guest2`, установил для него пароль и добавил его в группу к пользователю `guest1`: (рис. @fig:001):

```
[guest1@localhost ~]$ su root
Пароль:
[root@localhost guest1]# useradd guest2
[root@localhost guest1]# passwd guest2
Изменение пароля пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@localhost guest1]# su guest1
[guest1@localhost ~]$ gpasswd -a guest2 guest1
gpasswd: доступ запрещён.
[guest1@localhost ~]$ su root
Пароль:
[root@localhost guest1]# gpasswd -a guest2 guest1
Добавление пользователя guest2 в группу guest1
```

Рис. 0.1: создание и добавление в группу

Затем, в другом окне терминала зашел в пользователя `guest2` и в обоих окнах посмотрел папку, в которой нахожусь: (рис. @fig:002)

```
[guest1@localhost ~]$ pwd
/home/guest1
[guest1@localhost ~]$ su guest2
Пароль:
[guest2@localhost guest1]$ pwd
/home/guest1
```

Рис. 0.2: pwd для обоих

Для первого пользователя местонахождение совпадает с приглашением командной строки, а для второго нет, поскольку вход в терминал был осуществлен через первого пользователя.

В обоих окнах уточнил имя пользователя командой `whoami`, вывел, в какие группы входят пользователи: (рис. @fig:003)

```
[guest1@localhost ~]$ whoami
guest1
[guest1@localhost ~]$ groups guest1
guest1 : guest1
[guest1@localhost ~]$ id -Gn
guest1
[guest1@localhost ~]$ id -G
1002

[guest2@localhost guest1]$ whoami
guest2
[guest2@localhost guest1]$ groups guest2
guest2 : guest2 guest1
[guest2@localhost guest1]$ id -Gn
guest2 guest1
[guest2@localhost guest1]$ id -G
1003 1002
[guest2@localhost guest1]$ id
uid=1003(guest2) gid=1003(guest2) группы=1003(guest2),1002(guest1) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 0.3: `whoami`, `groups`, `id`

Посмотрел файл `etc/group`: (рис. @fig:004)

```
[guest2@localhost guest1]$ cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
...
tim:x:1000:
guest:x:1001:
guest1:x:1002:guest2
guest2:x:1003:
```

Рис. 0.4: `etc/groups`

Как видно, действительно в группу `guest1` входят оба пользователя, а в `guest2` только `guest2`.

Далее, зарегистрировался от второго пользователя в группе первого и от имени первого разрешил членам группы все действия (рис. @fig:005)

```
[guest2@localhost guest1]$ newgrp guest1
```

```
[guest1@localhost ~]$ chmod g+rxw /home/guest1
```

Рис. 0.5: регистрация и доступ

Затем, с помощью уже существующих папки `dir1` и файла `test` я от имени `guest1` начал менять права доступа, а от имени `guest2` начал проверять, какие операции разрешены, а какие нет. Для этого использовал команды `cd` (смена директории), `touch` (создание файла), `rm` (удаление файла), `echo` (запись в файл), `cat` (чтение файла), `ls` (просмотр содержимого), `mv` (переименование файла), `chmod` (смена атрибутов): (рис. @fig:006)

```
guest1@localhost:~
[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 070 dir1/test
[guest1@localhost ~]$ chmod 010 dir1
[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 000 dir1/test
[guest1@localhost ~]$ chmod 020 dir1
[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 030 dir1
[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 010 dir1/test
[guest1@localhost ~]$ chmod 030 dir1
[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 020 dir1/test
[guest1@localhost ~]$ chmod 030 dir1
[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 030 dir1/test
[guest1@localhost ~]$ chmod 030 dir1
[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 040 dir1/test
[guest1@localhost ~]$ chmod 030 dir1
[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 050 dir1/test
[guest1@localhost ~]$ chmod 030 dir1
[guest1@localhost ~]$ chmod 060 dir1/test
[guest1@localhost ~]$ chmod 030 dir1
[guest1@localhost ~]$ chmod 070 dir1/test
[guest1@localhost ~]$ chmod 030 dir1
[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 000 dir1/test
[guest1@localhost ~]$ chmod 040 dir1
[guest1@localhost ~]$ chmod 050 dir1
[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 010 dir1/test
[guest1@localhost ~]$ chmod 050 dir1
[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 020 dir1/test
[guest1@localhost ~]$ chmod 050 dir1
[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 030 dir1/test
[guest1@localhost ~]$ chmod 050 dir1
[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 040 dir1/test
[guest1@localhost ~]$ chmod 050 dir1

guest2@localhost:/home/guest1
ls: невозможно открыть каталог '.': Отказано в доступе
[guest2@localhost dir1]$ mv test k
mv: невозможно переместить 'test' в 'k': Отказано в доступе
[guest2@localhost dir1]$ chmod 010 test
chmod: изменение прав доступа для 'test': Операция не позволена
[guest2@localhost dir1]$ cd ..
[guest2@localhost guest1]$ cd dir1
[guest2@localhost dir1]$ touch l
touch: невозможно выполнить touch для 'l': Отказано в доступе
[guest2@localhost dir1]$ rm test
rm: удалить защищенный от записи обычный файл 'test'? y
rm: невозможно удалить 'test': Отказано в доступе
[guest2@localhost dir1]$ echo "dfghj" > test
bash: test: Отказано в доступе
[guest2@localhost dir1]$ cat test
cat: test: Отказано в доступе
[guest2@localhost dir1]$ ls
ls: невозможно открыть каталог '.': Отказано в доступе
[guest2@localhost dir1]$ mv test h
mv: невозможно переместить 'test' в 'h': Отказано в доступе
[guest2@localhost dir1]$ chmod 020 test
chmod: изменение прав доступа для 'test': Операция не позволена
[guest2@localhost dir1]$ cd ..
[guest2@localhost guest1]$ cd dir1
[guest2@localhost dir1]$ touch r
touch: невозможно выполнить touch для 'r': Отказано в доступе
[guest2@localhost dir1]$ rm test
rm: невозможно удалить 'test': Отказано в доступе
[guest2@localhost dir1]$ echo "poiuy" > test
[guest2@localhost dir1]$ cat test
cat: test: Отказано в доступе
[guest2@localhost dir1]$ ls
ls: невозможно открыть каталог '.': Отказано в доступе
[guest2@localhost dir1]$ mv test r
mv: невозможно переместить 'test' в 'r': Отказано в доступе
[guest2@localhost dir1]$ chmod 030 test
chmod: изменение прав доступа для 'test': Операция не позволена
[guest2@localhost dir1]$ cd ..
[guest2@localhost guest1]$ cd dir1
[guest2@localhost dir1]$ touch r
touch: невозможно выполнить touch для 'r': Отказано в доступе
[guest2@localhost dir1]$ rm test
rm: невозможно удалить 'test': Отказано в доступе
[guest2@localhost dir1]$ echo "cvb" > test
[guest2@localhost dir1]$ cat test
```

Рис. 0.6: фрагмент проверки разрешений

На основе полученных ответов заполнил таблицу (таб. 3.1)



Таблица 0.1: Установленные права и разрешённые действия для групп

Права дирек- тории	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	Смена дирек- тории	Просмотр файлов в директо- рии	Переимено- 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(010)	(070)	-	-	+	+	+	-	-	-
d(020)	(000)	-	-	-	-	-	-	-	-
d(020)	(010)	-	-	-	-	-	-	-	-
d(020)	(020)	-	-	-	-	-	-	-	-
d(020)	(030)	-	-	-	-	-	-	-	-
d(020)	(040)	-	-	-	-	-	-	-	-
d(020)	(050)	-	-	-	-	-	-	-	-
d(020)	(060)	-	-	-	-	-	-	-	-

Права дирек- тории	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	Смена дирек- тории	Просмотр файлов в директо- рии	Переимено- вание файла	Смена атрибу- тов файла
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)	-	-	+	-	+	+	-	-
d(050)	(040)	-	-	-	+	+	+	-	-
d(050)	(050)	-	-	-	+	+	+	-	-
d(050)	(060)	-	-	+	+	+	+	-	-
d(050)	(070)	-	-	+	+	+	+	-	-

Права дирек- тории	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	Смена дирек- тории	Просмотр файлов в директо- рии	Переимено- вание файла	Смена атрибу- тов файла
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)	+	+	+	+	+	+	+	-

У полученной таблицы лишь одно отличие от таблицы 2.1 - сменить атрибуты файла на этот раз не получилось нигде.

Затем, на основе полученных ответов заполнил таблицу 3.2. Также для заполнения этой таблицы проверил минимальные разрешения для создания/удаления поддиректории: (рис. @fig:007):

```

[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 060 dir1/test
[guest1@localhost ~]$ chmod 070 dir1
[guest1@localhost ~]$ chmod 700 dir1
[guest1@localhost ~]$ chmod 070 dir1/test
[guest1@localhost ~]$ chmod 070 dir1
[guest1@localhost ~]$ chmod 000 dir1
[guest1@localhost ~]$ chmod 010 dir1
[guest1@localhost ~]$ chmod 020 dir1
[guest1@localhost ~]$ chmod 030 dir1
[guest1@localhost ~]$ chmod 020 dir1
[guest1@localhost ~]$ █

[guest2@localhost guest1]$ mkdir dir1/dir3
mkdir: невозможно создать каталог «dir1/dir3»: Отказано в доступе
[guest2@localhost guest1]$ mkdir dir1/dir3
mkdir: невозможно создать каталог «dir1/dir3»: Отказано в доступе
[guest2@localhost guest1]$ mkdir dir1/dir3
mkdir: невозможно создать каталог «dir1/dir3»: Отказано в доступе
[guest2@localhost guest1]$ mkdir dir1/dir3
[guest2@localhost guest1]$ rmdir dir1/dir3
[guest2@localhost guest1]$ mkdir dir1/dir3
[guest2@localhost guest1]$ rmdir dir1/dir3
rmdir: не удалось удалить 'dir1/dir3': Отказано в доступе
[guest2@localhost guest1]$ █

```

Рис. 0.7: проверка создания поддиректории

В итоге получил следующую таблицу: (таб. 2.2)

Таблица 0.2: Минимальные права для совершения операций от имени пользователей, входящих в группу

Операция	min права на директорию	min права на файл
Создание файла	d(030)	(000)
Удаление файла	d(030)	(000)
Чтение файла	d(010)	(040)
Запись в файл	d(010)	(020)
Переименование файла	d(030)	(000)
Создание поддиректории	d(030)	(000)
Удаление поддиректории	d(030)	(000)

## Выводы

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