

# **Основы информационной безопасности**

**Лабораторная работа № 3. Дискреционное разграничение прав в Linux.  
Два пользователя**

Подлесный Иван Сергеевич

# Содержание

|   |                                |   |
|---|--------------------------------|---|
| 1 | Цель работы                    | 4 |
| 2 | Выполнение лабораторной работы | 5 |
| 3 | Выводы                         | 9 |

## Список иллюстраций

|     |  |   |
|-----|--|---|
| 2.1 | первый пункт был выполнен еще в Лабораторной Работе №2 . . .                     | 5 |
| 2.2 | Создание нового пользователя guest2 и добавление его в группу<br>guest . . . . . | 6 |
| 2.3 | Просмотр информации о группах пользователей . . . . .                            | 6 |
| 2.4 | Просмотр информации о группах пользователей в файле /etc/group                   | 7 |
| 2.5 | Изменение прав доступа . . . . .   | 7 |

# 1 Цель работы

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

## 2 Выполнение лабораторной работы

В установленной операционной системе создайте учётную запись пользователя guest(рис. fig. 2.1)

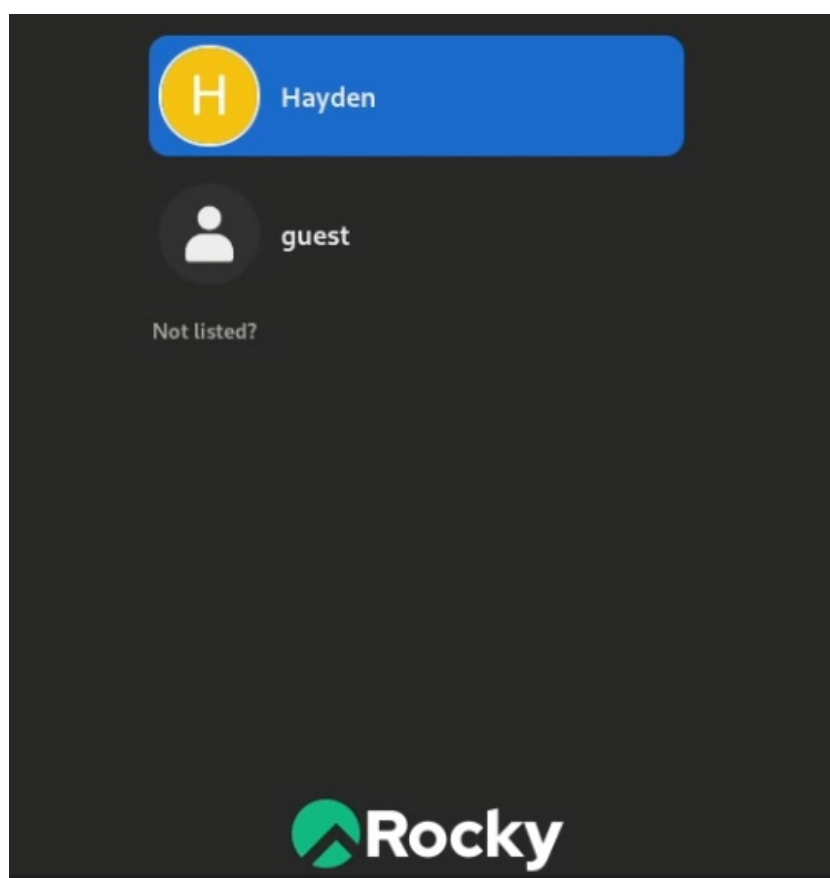


Рис. 2.1: первый пункт был выполнен еще в Лабораторной Работе №2

В установленной при выполнении предыдущей лабораторной работы ОС создадим учетную запись пользователя guest2 и добавляем его в группу guest(рис. fig. 2.2)

```
hayden@localhost:~$ sudo useradd guest2
[sudo] password for hayden:
useradd: warning: the home directory /home/guest2 already exists.
useradd: Not copying any file from skel directory into it.
Creating mailbox file: File exists
[hayden@localhost ~]$ sudo passwd guest2
Changing password for user guest2.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[hayden@localhost ~]$ gpasswd -a guest2 guest
gpasswd: Permission denied.
[hayden@localhost ~]$ sudo gpasswd -a guest2 guest
Adding user guest2 to group guest
[hayden@localhost ~]$
```

Рис. 2.2: Создание нового пользователя guest2 и добавление его в группу guest

Осуществим вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли. Для обоих пользователей командой `pwd` определим директорию, в которой находимся, увидим, что она совпадает с приглашениями командной строки. Уточните имя нашего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определим командами `groups guest` и `groups guest2`, в какие группы входят пользователи guest и guest2. Увидим, что guest принадлежит одной группе guet с id 2001, а двум группам guest и guest2 с id 1001 и 1002. С помощью команд `id -Gn` и `id -G` можно увидеть только id существующих групп и название соответственно(рис. fig. 2.3)

```
guest@localhost:~$ pwd
/home/guest
guest@localhost:~$ groups guest
guest : guest2 guest
guest@localhost:~$ id -G
1002 1001
guest2@localhost:~$
```

```
guest2@localhost:~$ pwd
/home/guest2
guest2@localhost:~$ groups guest2
guest2 : guest2 guest
guest2@localhost:~$ id -G
1002 1001
guest2@localhost:~$
```

Рис. 2.3: Просмотр информации о группах пользователей

Посмотрев информацию о группах этих пользователей в файле `/etc/group` получим аналогичную информацию(рис. fig. 2.4)

От имени пользователя guest2 выполните регистрацию пользователя guest2 в группе guest командой `newgrp guest`.

```
guest@localhost:~$ cat /etc/group | grep "guest"
guest:x:1001:guest2
guest2:x:1002:

guest@localhost:~$ chmod g+rxw /home/guest
guest@localhost:~$ chmod 000 dir1
ls: cannot open directory 'dir1': Permission denied
guest@localhost:~$ ls -l
total 0
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 desktop
d-----r-x. 2 guest guest 0 Sep 14 00:27 dir1
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 documents
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 downloads
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 music
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 pictures
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 public
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 templates
-rw-r--r--. 1 guest guest 0 Sep 14 00:20 text.txt
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 videos
guest@localhost:~$ chmod g+rxw /home/guest2

guest2@localhost:~$ pwd
/home/guest2
guest2:~$ groups guest2
guest2:~$ id -G
1002 1001
guest2@localhost:~$ newgrp guest
guest2@localhost:~$ ls -l dir1
ls: cannot access 'dir1': No such file or directory
guest2@localhost:~$ ls -l
total 0
guest2@localhost:~$
```

Рис. 2.4: Просмотр информации о группах пользователей в файле /etc/group

От имени пользователя guest изменим права директории /home/guest, разрешив все действия для пользователей группы и снимем с директории /home/guest/dir1 все атрибуты, затем проверим правильность атрибутов(рис. fig. 2.5).

```
guest@localhost:~$ ls -l
total 0
drwxr-xr-x. 2 guest guest 0 Sep 14 00:27 dir1
d-----r-x. 2 guest guest 0 Sep 14 00:27 dir1
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 documents
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 downloads
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 music
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 pictures
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 public
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 templates
-rw-r--r--. 1 guest guest 0 Sep 14 00:20 text.txt
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 videos
guest@localhost:~$ chmod g+rxw /home/guest
guest@localhost:~$ ls -l
total 0
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 desktop
d-----r-x. 2 guest guest 0 Sep 14 00:27 dir1
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 documents
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 downloads
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 music
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 pictures
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 public
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 templates
-rw-r--r--. 1 guest guest 0 Sep 14 00:20 text.txt
drwxr-xr-x. 2 guest guest 0 Sep 13 23:46 videos
guest@localhost:~$ chmod g+rxw /home/guest2
guest@localhost:~$
```

Рис. 2.5: Изменение прав доступа

В таблице приведены данные о том, какие операции разрешены, а какие нет для владельца данных.

Минимальные права для совершения операций

| Операция       | Минимальные         |                           |
|----------------|---------------------|---------------------------|
|                | права на директорию | Минимальные права на файл |
| Создание файла | d(030)              | (000)                     |
| Удаление файла | d(030)              | (000)                     |
| Чтение файла   | d(010)              | (040)                     |
| Запись в файл  | d(010)              | (020)                     |

| Операция               | Минимальные            |                              |
|------------------------|------------------------|------------------------------|
|                        | права на<br>директорию | Минимальные<br>права на файл |
| Переименование файла   | d(030)                 | (000)                        |
| Создание поддиректории | d(030)                 | (000)                        |
| Удаление поддиректории | d(030)                 | (000)                        |

При сравнении с таблицей в лабораторной работе №2 можно увидеть, что отличие состоит только в том, что не владелец файла никогда не имеет прав на изменение его атрибутов. Менять права доступа (записывать в inode) может владелец файла или администратор. Члены группы файла никаких особых прав на inode не имеют. Пользователь может отобрать у себя собственные права на чтение и запись в файл, но право на запись в inode (в т.ч. право на смену прав) сохраняется у владельца файла при любых обстоятельствах. Пользователь не может передать право собственности на файл другому пользователю и не может забрать право собственности на файл у другого пользователя.



## **3 Выводы**

В результате выполнения работы были приобретены практические навыки работы в консоли с атрибутами файлов для групп пользователей.