

# **Лабораторная работа №3**

**Дисциплина: Основы администрирования операционных систем**

Жибицкая Евгения Дмитриевна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Ответы на контрольные вопросы</b>	<b>14</b>
<b>4</b>	<b>Выводы</b>	<b>17</b>

# Список иллюстраций

2.1	Знакомство с командами . . . . .	6
2.2	Права доступа и разрешения . . . . .	7
2.3	Права доступа для Bob . . . . .	7
2.4	Создание файлов . . . . .	8
2.5	Работа с файлами . . . . .	8
2.6	Идентификатор и sticky-бит . . . . .	8
2.7	Работа с файлами и sticky-битом . . . . .	9
2.8	Права на чтение и выполнение . . . . .	10
2.9	Разрешения newfile1 . . . . .	11
2.10	ACL . . . . .	12
2.11	Удаление файлов Carol . . . . .	12
2.12	Запись в файлы . . . . .	13
3.1	Пример . . . . .	14
3.2	Пример . . . . .	15

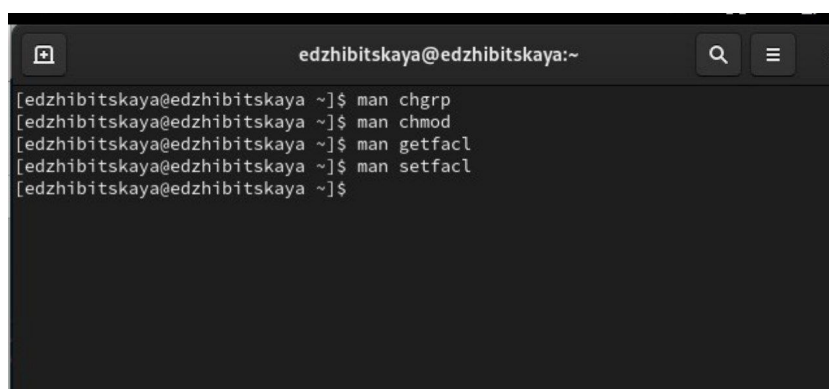
## **Список таблиц**

# 1 Цель работы

Продолжение изучения Linux. Получение навыков настройки базовых и специальных прав доступа для групп пользователей в ОС.

## 2 Выполнение лабораторной работы

В качестве подготовки к работе и выполнения задания 1 изучим принцип работы следующих команд: `chgrp`, `chmod`, `getfacl`, `setfacl` (рис. 2.1).



```
edzhibitskaya@edzhibitskaya:~  
[edzhibitskaya@edzhibitskaya ~]$ man chgrp  
[edzhibitskaya@edzhibitskaya ~]$ man chmod  
[edzhibitskaya@edzhibitskaya ~]$ man getfacl  
[edzhibitskaya@edzhibitskaya ~]$ man setfacl  
[edzhibitskaya@edzhibitskaya ~]$
```

Рис. 2.1: Знакомство с командами

Далее перейдем к управлению базовыми разрешениями. Открываем терминал с `root` и создаем каталоги `/data/main` и `/data/third`. Также смотрим кто является владельцем и меняем их на `main` и `third`. установим разрешения на запись для владельцев и запрет на доступ остальным(рис. 2.2).

```

[edzhibitskaya@edzhibitskaya ~]$ su
Password:
[root@edzhibitskaya edzhibitskaya]# mkdir -p /data/main /data/third
[root@edzhibitskaya edzhibitskaya]# ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 Sep 13 11:35 main
drwxr-xr-x. 2 root root 6 Sep 13 11:35 third
[root@edzhibitskaya edzhibitskaya]# chgrp main /d
data/ dev/
[root@edzhibitskaya edzhibitskaya]# chgrp main /data/main/
[root@edzhibitskaya edzhibitskaya]# chgrp third /data/third
[root@edzhibitskaya edzhibitskaya]# ls -Al /data
total 0
drwxr-xr-x. 2 root main 6 Sep 13 11:35 main
drwxr-xr-x. 2 root third 6 Sep 13 11:35 third
[root@edzhibitskaya edzhibitskaya]# chmod 770 /data/main
[root@edzhibitskaya edzhibitskaya]# chmod 770 /data/third
[root@edzhibitskaya edzhibitskaya]# ls -Al /data
total 0
drwxrwx---. 2 root main 6 Sep 13 11:35 main
drwxrwx---. 2 root third 6 Sep 13 11:35 third
[root@edzhibitskaya edzhibitskaya]#

```

Рис. 2.2: Права доступа и разрешения

Откроем еще один терминал и войдем в учетную запись Bob. Перейдем в нужный каталог и попытаемся создать файл. При попытке посмотреть содержимое каталога main с новым файлом проблем не возникает, а при тех же действиях в каталоге third, пишут, что доступ запрещен, так как до этого мы сами установили такие права доступа (Bob принадлежит к группе main) (рис. 2.3).

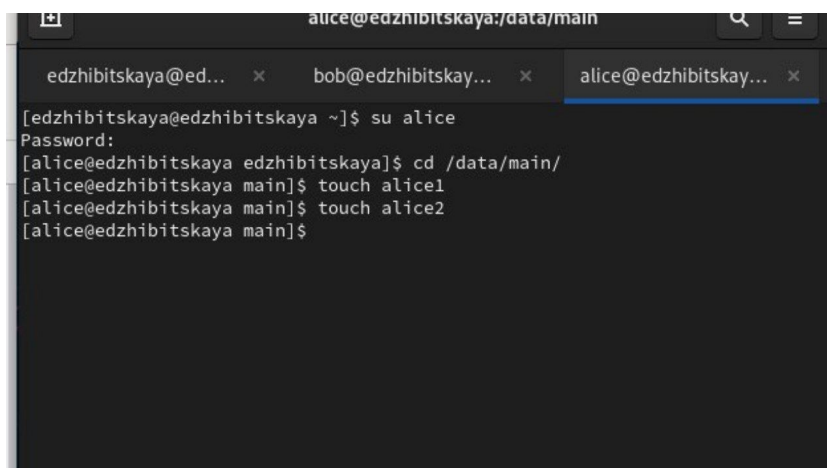
```

edzhibitskaya@edzhibitskaya:/ho... x bob@ed
>> [edzhibitskaya@edzhibitskaya ~]$ su -bob
su: invalid option -- 'b'
>> Try 'su --help' for more information.
[edzhibitskaya@edzhibitskaya ~]$ su - bob
Password:
[bob@edzhibitskaya ~]$ cd /data/main/
[bob@edzhibitskaya main]$ touch emptyfile
[bob@edzhibitskaya main]$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Sep 13 11:38 emptyfile
[bob@edzhibitskaya main]$ cd /data/third/
-bash: cd: /data/third/: Permission denied
[bob@edzhibitskaya main]$

```

Рис. 2.3: Права доступа для Bob

Откроем еще терминал под учетной записью Alice. Создадим 2 файла (рис. 2.4).

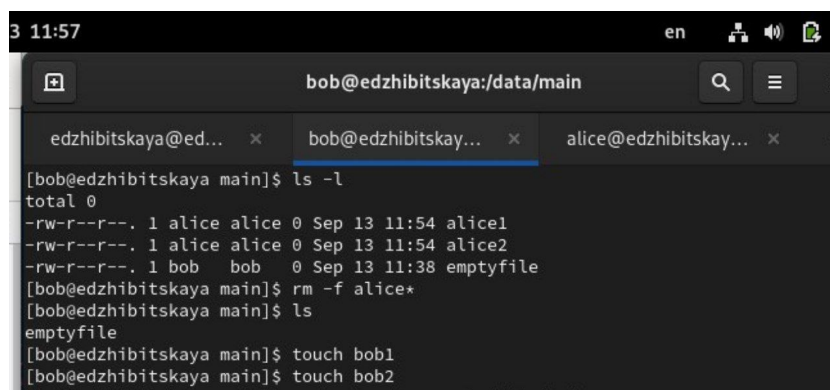
A terminal window titled 'alice@edzhbitskaya:/data/main'. It shows a sequence of commands: 'su alice' (switching to Alice), 'cd /data/main/' (changing to the main directory), 'touch alice1' (creating file alice1), and 'touch alice2' (creating file alice2). The prompt returns to '[alice@edzhbitskaya main]\$' after each command.

```
alice@edzhbitskaya:/data/main
edzhbitskaya@ed... x bob@edzhbitskay... x alice@edzhbitskay... x
[edzhbitskaya@edzhbitskaya ~]$ su alice
Password:
[alice@edzhbitskaya edzhbitskaya]$ cd /data/main/
[alice@edzhbitskaya main]$ touch alice1
[alice@edzhbitskaya main]$ touch alice2
[alice@edzhbitskaya main]$
```

Рис. 2.4: Создание файлов

Вернемся к Bob. Командой `ls -l` посмотрим содержимое и удалим все файлы принадлежащие Alice.

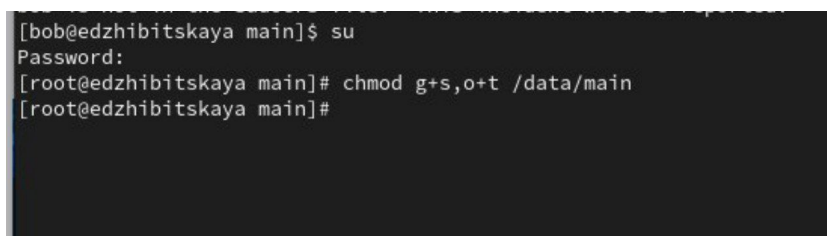
Убедимся, что они удалены и создадим еще два файла Bob1, Bob2 (рис. 2.5).

A terminal window titled 'bob@edzhbitskaya:/data/main'. It shows the command 'ls -l' which lists three files: 'alice1', 'alice2', and 'emptyfile', all owned by 'alice'. Then, the command 'rm -f alice\*' is executed to delete the files owned by Alice. Finally, 'touch bob1' and 'touch bob2' are executed to create new files owned by Bob. The prompt returns to '[bob@edzhbitskaya main]\$' after each command.

```
3 11:57 en
bob@edzhbitskaya:/data/main
edzhbitskaya@ed... x bob@edzhbitskay... x alice@edzhbitskay... x
[bob@edzhbitskaya main]$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Sep 13 11:54 alice1
-rw-r--r--. 1 alice alice 0 Sep 13 11:54 alice2
-rw-r--r--. 1 bob bob 0 Sep 13 11:38 emptyfile
[bob@edzhbitskaya main]$ rm -f alice*
[bob@edzhbitskaya main]$ ls
emptyfile
[bob@edzhbitskaya main]$ touch bob1
[bob@edzhbitskaya main]$ touch bob2
```

Рис. 2.5: Работа с файлами

В терминале с root установим для каталога `/data/main` бит идентификатора группы, а также `sticky`-бит для разделяемого (общего) каталога группы(рис. 2.6).

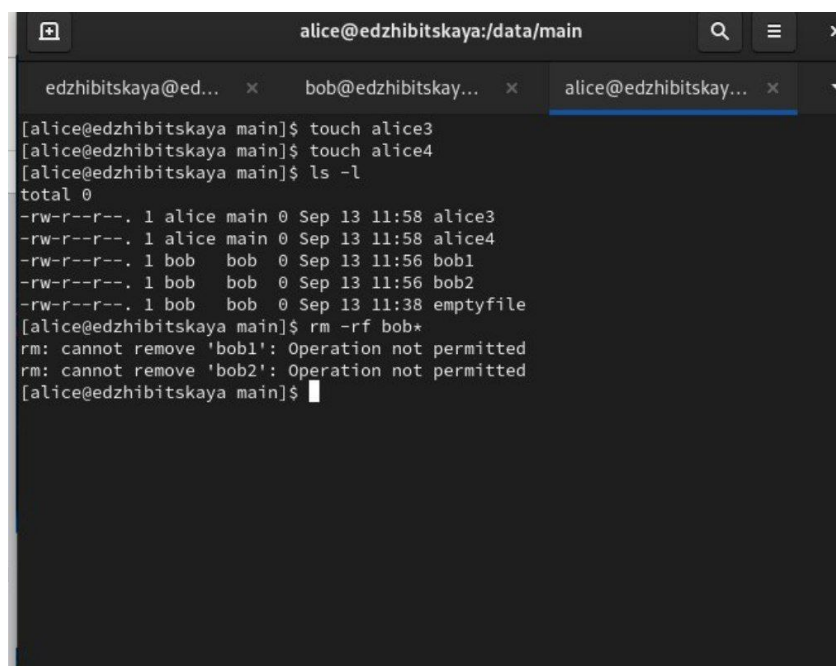
A terminal window showing a switch to root ('su') and then the command 'chmod g+s,o+t /data/main'. The prompt returns to '[root@edzhbitskaya main]#'.

```
[bob@edzhbitskaya main]$ su
Password:
[root@edzhbitskaya main]# chmod g+s,o+t /data/main
[root@edzhbitskaya main]#
```

Рис. 2.6: Идентификатор и sticky-бит



Затем вернемся к Alice. Создадим еще 2 файла, посмотрим на их владельца(alice main). Попробуем удалить файлы, принадлежащие Бобу. Это невозможно из-за подключенного sticky-бита(рис. 2.7).

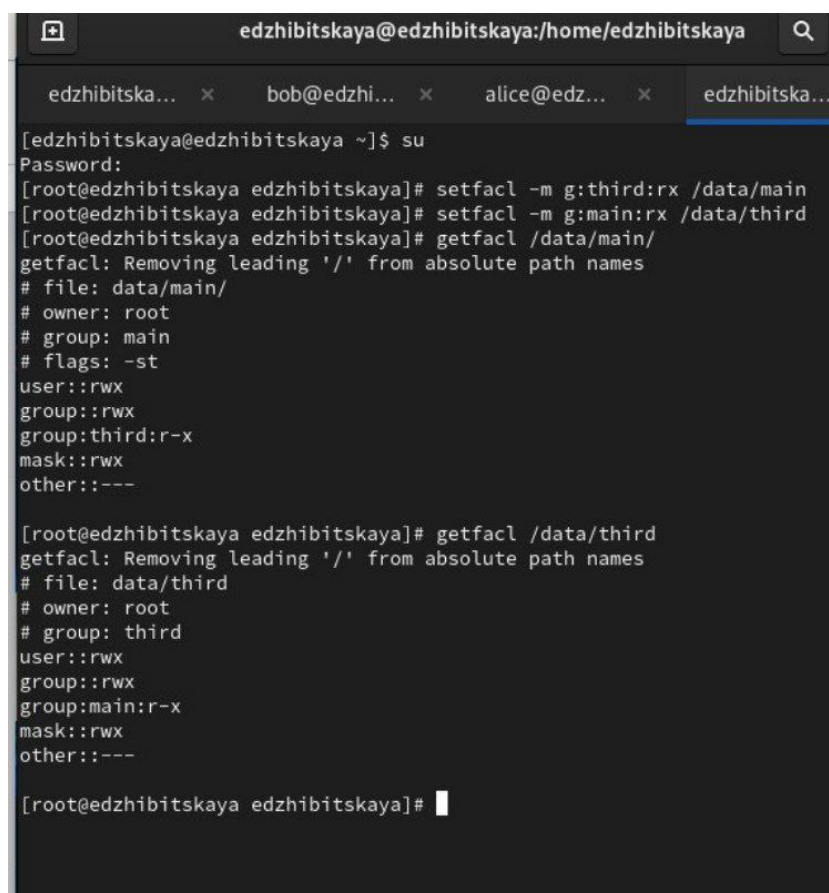


```
alice@edzhibitskaya:/data/main
edzhibitskaya@ed... x bob@edzhibitskay... x alice@edzhibitskay... x
[alice@edzhibitskaya main]$ touch alice3
[alice@edzhibitskaya main]$ touch alice4
[alice@edzhibitskaya main]$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Sep 13 11:58 alice3
-rw-r--r--. 1 alice main 0 Sep 13 11:58 alice4
-rw-r--r--. 1 bob bob 0 Sep 13 11:56 bob1
-rw-r--r--. 1 bob bob 0 Sep 13 11:56 bob2
-rw-r--r--. 1 bob bob 0 Sep 13 11:38 emptyfile
[alice@edzhibitskaya main]$ rm -rf bob*
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
[alice@edzhibitskaya main]$
```

Рис. 2.7: Работа с файлами и sticky-битом

Перейдем в root. Установим права на чтение и выполнение в каталоге /data/main для группы third и права на чтение и выполнение для группы main в каталоге /data/third:

Используем команду `getfacl`, чтобы убедиться в правильности установки разрешений(рис. 2.8).

A terminal window titled 'edzhbitskaya@edzhbitskaya:/home/edzhbitskaya' with several tabs. The active tab shows a shell session where the user 'edzhbitskaya' switches to 'root' using 'su'. Then, 'root' sets permissions for '/data/main' with 'setfacl -m g:third:rx /data/main' and for '/data/third' with 'setfacl -m g:main:rx /data/third'. Finally, 'root' uses 'getfacl' to display the permissions for both files. The output for '/data/main/' shows owner 'root', group 'main', and permissions 'rwx' for user, group, and third. The output for '/data/third' shows owner 'root', group 'third', and permissions 'rwx' for user, group, and main.

```
[edzhbitskaya@edzhbitskaya ~]$ su
Password:
[root@edzhbitskaya edzhbitskaya]# setfacl -m g:third:rx /data/main
[root@edzhbitskaya edzhbitskaya]# setfacl -m g:main:rx /data/third
[root@edzhbitskaya edzhbitskaya]# getfacl /data/main/
getfacl: Removing leading '/' from absolute path names
# file: data/main/
# owner: root
# group: main
# flags: -st
user::rwx
group::rwx
group:third:r-x
mask::rwx
other::---

[root@edzhbitskaya edzhbitskaya]# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: third
user::rwx
group::rwx
group:main:r-x
mask::rwx
other::---
```

Рис. 2.8: Права на чтение и выполнение

Создадим новый файл newfile1 и проверим его полномочия(каталог main). Запись означает, что только владелец(root) имеет право на запись и чтение, у остальных только чтение. Прделаем аналогичные действия для third. Там все то же самое, только группа уже root, а не main(рис. 2.9).

```

[root@edzhbitskaya edzhbitskaya]# touch /data/main/newfile1
[root@edzhbitskaya edzhbitskaya]#
[root@edzhbitskaya edzhbitskaya]# getfacl /data/main/newfile1
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile1
# owner: root
# group: main
user::rw-
group::r--
other::r--

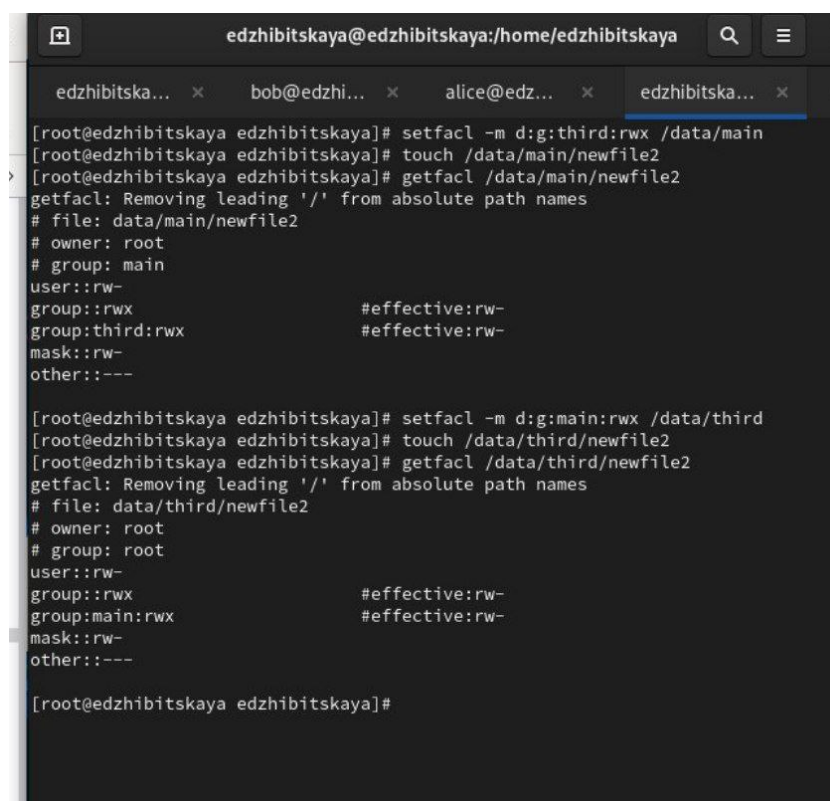
[root@edzhbitskaya edzhbitskaya]# touch /data/main/newfile2
[root@edzhbitskaya edzhbitskaya]# rm /data/main/newfile2
rm: remove regular empty file '/data/main/newfile2'? y
[root@edzhbitskaya edzhbitskaya]# touch /data/third/newfile1
[root@edzhbitskaya edzhbitskaya]# getfacl data/third/newfile1
getfacl: data/third/newfile1: No such file or directory
[root@edzhbitskaya edzhbitskaya]# getfacl /data/third/newfile1
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile1
# owner: root
# group: root
user::rw-
group::r--
other::r--

[root@edzhbitskaya edzhbitskaya]#

```

Рис. 2.9: Разрешения newfile1

Установим права на чтение и выполнение в каталоге /data/main для группы third и права на чтение и выполнение для группы main в каталоге /data/third. Командой getfacl, убедимся в правильности установки разрешений: (рис. 2.10).



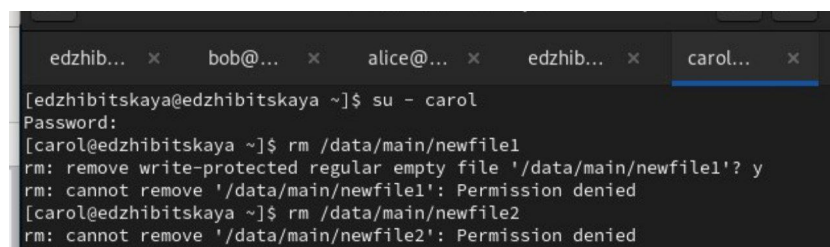
```
edzhibitskaya@edzhibitskaya:/home/edzhibitskaya
edzhibitska... x bob@edzhi... x alice@edz... x edzhibitska... x

[root@edzhibitskaya edzhibitskaya]# setfacl -m d:g:third:rwx /data/main
[root@edzhibitskaya edzhibitskaya]# touch /data/main/newfile2
[root@edzhibitskaya edzhibitskaya]# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root
# group: main
user::rw-
group::rwx                #effective:rw-
group:third:rwx           #effective:rw-
mask::rw-
other::---

[root@edzhibitskaya edzhibitskaya]# setfacl -m d:g:main:rwx /data/third
[root@edzhibitskaya edzhibitskaya]# touch /data/third/newfile2
[root@edzhibitskaya edzhibitskaya]# getfacl /data/third/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile2
# owner: root
# group: root
user::rw-
group::rwx                #effective:rw-
group:main:rwx            #effective:rw-
mask::rw-
other::---
```

Рис. 2.10: ACL

Войдем в учетную запись Carol и попробуем удалить файлы - запрет(так как нет прав администратора)(рис. 2.11).

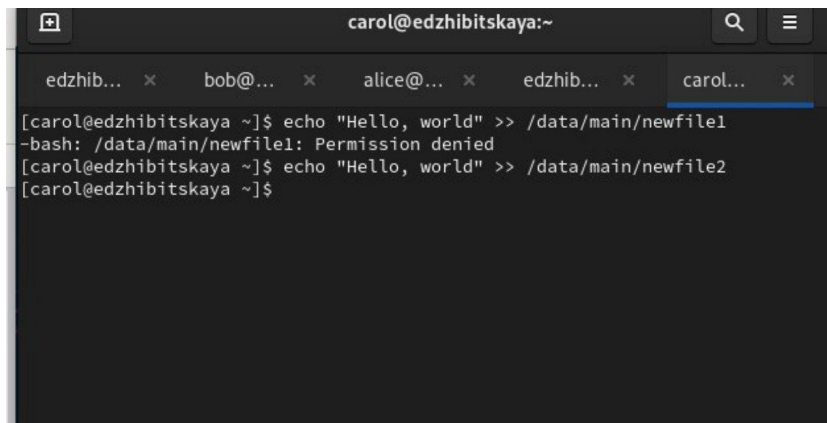


```
edzhib... x bob@... x alice@... x edzhib... x carol... x

[edzhibitskaya@edzhibitskaya ~]$ su - carol
Password:
[carol@edzhibitskaya ~]$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1'? y
rm: cannot remove '/data/main/newfile1': Permission denied
[carol@edzhibitskaya ~]$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
```

Рис. 2.11: Удаление файлов Carol

Наконец попробуем записать что-то в файлы. В 1 файл ничего записать не удастся(нет права на исполнение у группы third), а во второй, благодаря ACL, это возможно(рис. 2.12).



A terminal window titled 'carol@edzhbitskaya:~' with a search icon and a menu icon in the top right. The window has five tabs: 'edzhib...', 'bob@...', 'alice@...', 'edzhib...', and 'carol...'. The 'carol...' tab is selected. The terminal shows the following commands and output:

```
[carol@edzhbitskaya ~]$ echo "Hello, world" >> /data/main/newfile1
-bash: /data/main/newfile1: Permission denied
[carol@edzhbitskaya ~]$ echo "Hello, world" >> /data/main/newfile2
[carol@edzhbitskaya ~]$
```

Рис. 2.12: Запись в файлы

### 3 Ответы на контрольные вопросы

1. Для установки владельца группы для файла с помощью команды `chown` нужно использовать:

`chown :группа файл`

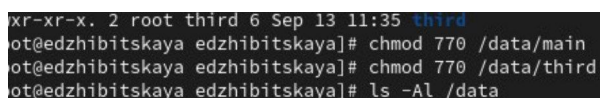
Пример: `chown bob:main /data/third/newfile1`

2. Для поиска всех файлов, принадлежащих конкретному пользователю, можно использовать команду `find`. Пример:

`find /путь/к/каталогу -user имя_пользователя`

Пример: `find /home -user bob`

3. Чтобы применить разрешения на чтение, запись и выполнение для всех файлов в каталоге `/data` для пользователей и владельцев групп, не устанавливая никаких прав для других, можно использовать команду `chmod` следующим образом(рис. 3.1).



```

-r-xr-xr-x. 2 root third 6 Sep 13 11:35 third
ot@edzhibitskaya edzhibitskaya]# chmod 770 /data/main
ot@edzhibitskaya edzhibitskaya]# chmod 770 /data/third
ot@edzhibitskaya edzhibitskaya]# ls -Al /data
```

Рис. 3.1: Пример

`chmod 770 /data/*`

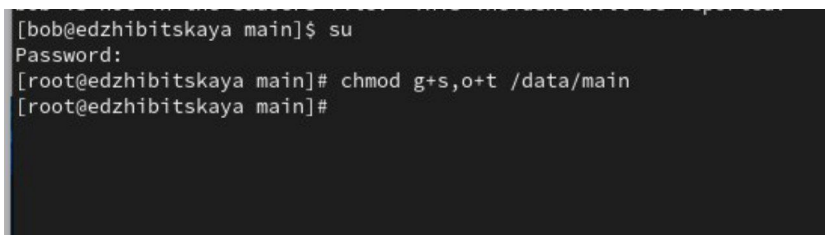
4. Чтобы добавить разрешение на выполнение для файла, необходимо использовать команду `chmod`. Пример:

`chmod +x файл`

Пример: `chmod +x script.sh`

5. Команда, которая позволяет убедиться, что групповые разрешения для всех новых файлов, создаваемых в каталоге, будут присвоены владельцу группы этого каталога, называется `chmod` с установленным битом SGID. Пример(рис. 3.2).

`chmod g+s /путь/к/каталогу`



```
[bob@edzhibitskaya main]$ su
Password:
[root@edzhibitskaya main]# chmod g+s,o+t /data/main
[root@edzhibitskaya main]#
```

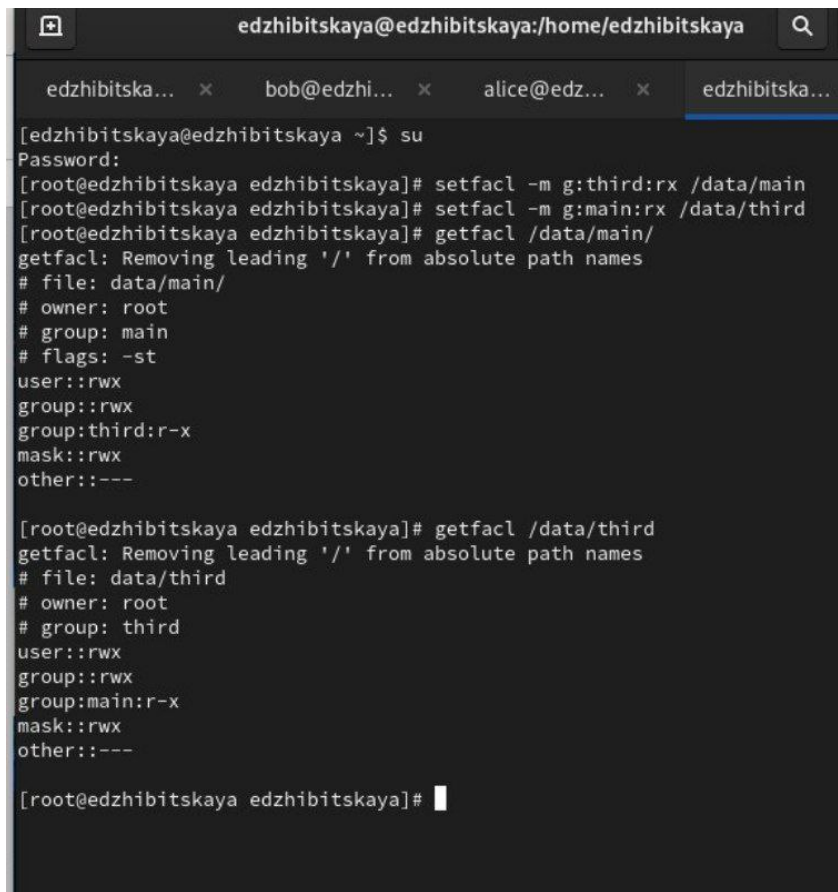
Рис. 3.2: Пример

6. Можно использовать команду `chmod`. Например, установить права доступа к каталогу, где находятся файлы, таким образом, чтобы только владелец мог удалять файлы. Это может выглядеть так:

`chmod 700 /path/to/directory`

7. Для добавления ACL, который предоставляет членам группы права доступа на чтение для всех существующих файлов в текущем каталоге, можно использовать команду `setfacl`. Например, чтобы предоставить группе “mygroup” права на чтение, используйте следующую команду(рис. ??).

`setfacl -m g:mygroup:r /path/to/directory/*`

A terminal window titled 'edzhibitskaya@edzhibitskaya:/home/edzhibitskaya' with a search icon in the top right. It has four tabs: 'edzhibitska...', 'bob@edzhi...', 'alice@edz...', and 'edzhibitska...'. The terminal shows a user switching to root with 'su', then setting ACLs for '/data/main' and '/data/third'. It then displays the ACLs for both directories. The ACL for '/data/main/' shows permissions for root, main group, and third group. The ACL for '/data/third' shows permissions for root, third group, and main group.

```
[edzhibitskaya@edzhibitskaya ~]$ su
Password:
[root@edzhibitskaya edzhibitskaya]# setfacl -m g:third:rx /data/main
[root@edzhibitskaya edzhibitskaya]# setfacl -m g:main:rx /data/third
[root@edzhibitskaya edzhibitskaya]# getfacl /data/main/
getfacl: Removing leading '/' from absolute path names
# file: data/main/
# owner: root
# group: main
# flags: -st
user::rwx
group::rwx
group:third:r-x
mask::rwx
other::---

[root@edzhibitskaya edzhibitskaya]# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: third
user::rwx
group::rwx
group:main:r-x
mask::rwx
other::---
```

8. Чтобы гарантировать, что члены группы получают разрешения на чтение для всех файлов в текущем каталоге и во всех его подкаталогах, а также для всех файлов, которые будут созданы в этом каталоге в будущем, можно использовать следующие команды:

```
setfacl -R -m g:mygroup:rX /path/to/directory setfacl -R -d -m g:mygroup:rX /path/to/directory
```

9. Нужно установить umask на 007. `umask 007`
10. Защита файла от случайного удаления

```
chattr +i myfile
```

После этого файл не сможет быть удалён или изменён ни одним пользователем, пока атрибут не будет снят с помощью `chattr -i myfile`.



## 4 Выводы

В ходе работы было произведено знакомство с правами доступа и разрешениями для групп пользователей в ОС Linux, реализовано наделение ими.