

Лабораторная работа №3

Настройка прав доступа

Жибицкая Е.Д.

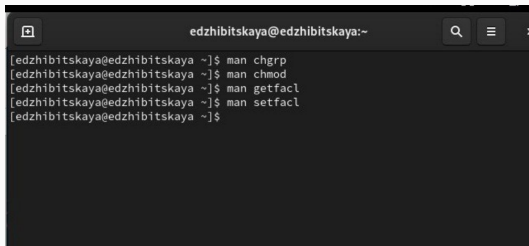
Российский университет дружбы народов, Москва, Россия

Цель работы

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

Выполнение работы

Изучение команд с помощью man



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

Рис. 1: Знакомство с командами

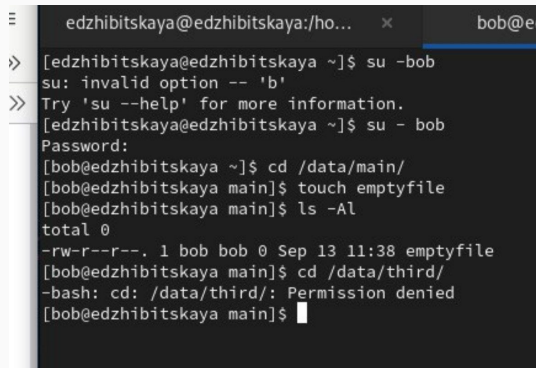
3.3.1. Управление базовыми разрешениями

```
[edzhbitskaya@edzhbitskaya ~]$ su
Password:
[root@edzhbitskaya edzhbitskaya]# mkdir -p /data/main /data/third
[root@edzhbitskaya edzhbitskaya]# 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@edzhbitskaya edzhbitskaya]# chgrp main /d
data/ dev/
[root@edzhbitskaya edzhbitskaya]# chgrp main /data/main/
[root@edzhbitskaya edzhbitskaya]# chgrp third /data/third
[root@edzhbitskaya edzhbitskaya]# 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@edzhbitskaya edzhbitskaya]# chmod 770 /data/main
[root@edzhbitskaya edzhbitskaya]# chmod 770 /data/third
[root@edzhbitskaya edzhbitskaya]# 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@edzhbitskaya edzhbitskaya]#
```

Рис. 2: Установка прав доступа

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.

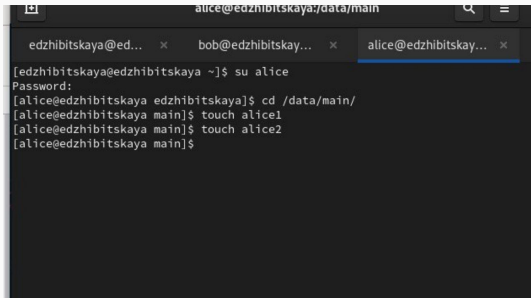
3.3.1



```
edzhibitskaya@edzhibitskaya:/ho... x bob@edzhibitskaya
>> [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. 3: Права доступа для Bob

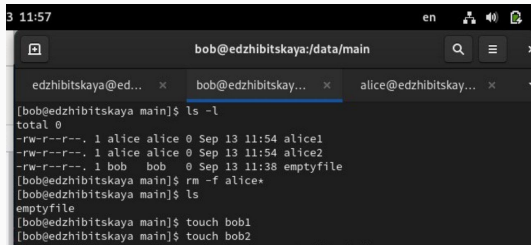
3.3.2. Управление специальными разрешениями



A terminal window titled 'alice@edzhbitskaya:/data/main'. It shows the process of switching to the 'alice' user and creating two files, 'alice1' and 'alice2', in the current directory. The window has three tabs: 'edzhbitskaya@ed...', 'bob@edzhbitskay...', and 'alice@edzhbitskay...'. The 'alice@edzhbitskay...' tab is selected.

```
alice@edzhbitskaya:/data/main
[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. 4: Создание файлов



A terminal window titled 'bob@edzhbitskaya:/data/main'. It shows the process of listing files, deleting 'alice1' and 'alice2', and creating 'bob1' and 'bob2'. The window has three tabs: 'edzhbitskaya@ed...', 'bob@edzhbitskay...', and 'alice@edzhbitskay...'. The 'bob@edzhbitskay...' tab is selected.

```
3 11:57 en
[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. 5: Работа с файлами

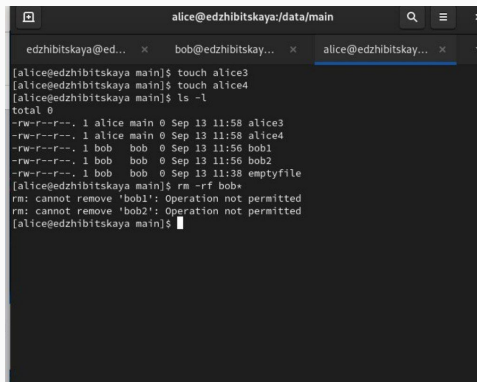

```
[bob@edzhbitskaya main]$ su
Password:
[root@edzhbitskaya main]# chmod g+s,o+t /data/main
[root@edzhbitskaya main]#
```

Рис. 6: Идентификатор и sticky-бит

Установим для каталога `/data/main` бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы.

3.3.2

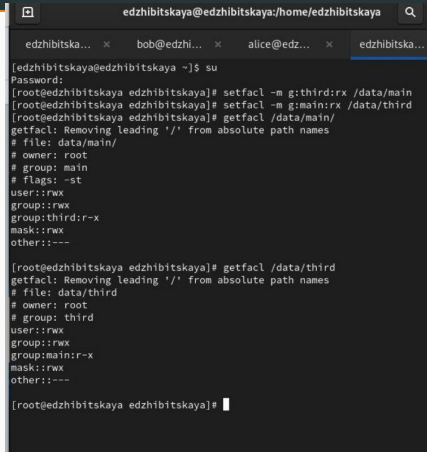
Вернемся к Alice. Создадим еще 2 файла, посмотрим на их владельца(alice main). Попробуем удалить файлы, принадлежащие Бобу. Это невозможно из-за подключенного sticky-бита.



```
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. 7: Работа с файлами и sticky-битом

3.3.2



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

[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:---

[root@edzhibitskaya edzhibitskaya]#
```

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:

Рис. 8: Права на чтение и запись

3.3.2

```
[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--

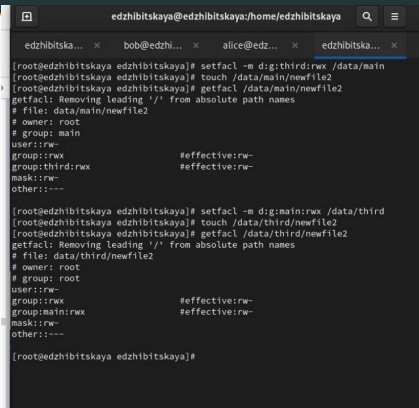
[root@edzhbitskaya edzhbitskaya]# touch /data/main/newfile2
[root@edzhbitskaya edzhbitskaya]# rm /data/main/newfile2
rm: remove regular empty file '/data/main/newfile2'? y
[root@edzhbitskaya edzhbitskaya]# touch /data/third/newfile1
[root@edzhbitskaya edzhbitskaya]# getfacl data/third/newfile1
getfacl: 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]#
```

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. 9: Разрешения newfile1

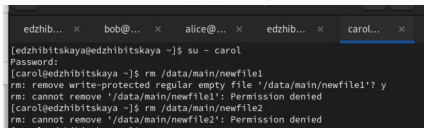
3.3.3. Управление расширенными разрешениями с использованием списков ACL

A terminal window with a dark background and light text. The window title is 'edzhibitskaya@edzhibitskaya:/home/edzhibitskaya'. There are four tabs at the top: 'edzhibitska...', 'bob@edzhi...', 'alice@edz...', and 'edzhibitska...'. The terminal shows a series of commands and their outputs. The first command is 'setfacl -m d:g:third:rw /data/main', followed by 'touch /data/main/newfile2'. Then 'getfacl /data/main/newfile2' is run, showing the ACL for the file. The second command is 'setfacl -m d:g:main:rw /data/third', followed by 'touch /data/third/newfile2'. Then 'getfacl /data/third/newfile2' is run, showing the ACL for the file. The terminal output for the first set of commands is: [root@edzhibitskaya edzhibitskaya]# setfacl -m d:g:third:rw /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:rw /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::---

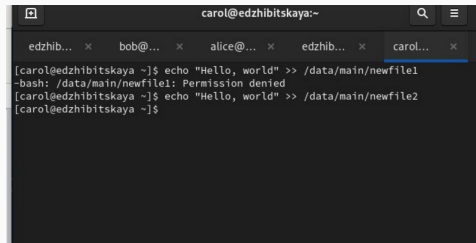
[root@edzhibitskaya edzhibitskaya]#

Рис. 10: ACL



```
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. 11: Удаление файлов Carol



```
carol@edzhibitskaya:~
edzhib... x bob@... x alice@... x edzhib... x carol... x
[carol@edzhibitskaya ~]$ echo "Hello, world" >> /data/main/newfile1
-bash: /data/main/newfile1: Permission denied
[carol@edzhibitskaya ~]$ echo "Hello, world" >> /data/main/newfile2
[carol@edzhibitskaya ~]$
```

Рис. 12: Запись в файлы

Вывод

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