

# Отчет по лабораторной работе №3

## Простейший вариант

Лупупа Чилеше

### 1 Цель работы

Получение навыков настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.

### 2 Теоретическое введение

Основные права доступа в Linux в первую очередь определяются разрешениями для файлов и каталогов. Эти разрешения обычно представлены тремя наборами атрибутов `gwx`:

Разрешения пользователя (`u`): применяются к владельцу файла/каталога.

Групповые разрешения (`g`): применяются к членам группы файлов/каталогов.

Другие разрешения (`o`): применить ко всем остальным пользователям.

Каждому набору разрешений можно присвоить одно из трех значений:

Чтение (`r`): позволяет просматривать содержимое файла или просматривать содержимое каталога.

Запись (`w`): позволяет изменять содержимое файла или добавлять/удалять элементы в каталоге.

Выполнить (`x`): позволяет выполнить файл или перейти в каталог.

Эти разрешения объединяются в строку из 9 символов, первый символ которой представляет тип файла (например, `-` для обычного файла, `d` для каталога).

Например, строка разрешения `rw-r--r--` указывает:

Владелец имеет права на чтение/запись

Группа имеет разрешения только на чтение

Другие имеют разрешения только на чтение

### 3 Выполнение лабораторной работы

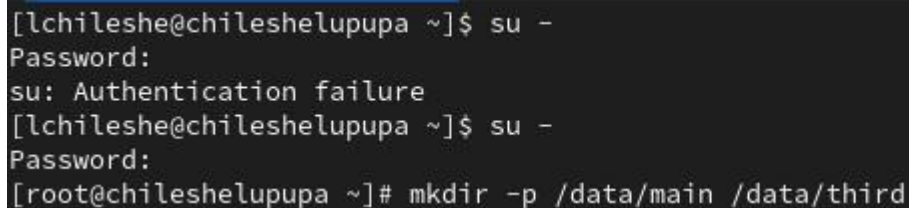
#### Задание

1. Прочитайте справочное описание man по командам chgrp, chmod, getfacl, setfacl.
2. Выполните действия по управлению базовыми разрешениями для групп пользователей (раздел 3.3.1).
3. Выполните действия по управлению специальными разрешениями для групп пользователей (раздел 3.3.2).
4. Выполните действия по управлению расширенными разрешениями с использованием списков ACL для групп пользователей (раздел 3.3.3).

#### Последовательность выполнения работы

1. Откройте терминал с учётной записью root: (fig 1)

su -



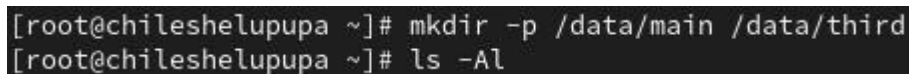
```
[lchileshe@chileshelupupa ~]$ su -  
Password:  
su: Authentication failure  
[lchileshe@chileshelupupa ~]$ su -  
Password:  
[root@chileshelupupa ~]# mkdir -p /data/main /data/third
```

(fig1)

2. В корневом каталоге создайте каталоги /data/main и /data/third (fig 2)

mkdir -p /data/main /data/third

Посмотрите, кто является владельцем этих каталогов. Для этого используйте:  
ls -Al /data



```
[root@chileshelupupa ~]# mkdir -p /data/main /data/third  
[root@chileshelupupa ~]# ls -Al
```

(fig 2)

3. Прежде чем устанавливать разрешения, измените владельцев этих каталогов с root на main и third соответственно: (fig 3)

```
chgrp main /data/main
```

```
chgrp third /data/third
```

Посмотрите, кто теперь является владельцем этих каталогов:

```
ls -Al /data
```

```
[root@chileshelupupa ~]# chgrp main /data/main
[root@chileshelupupa ~]# chgrp third /data/third
[root@chileshelupupa ~]# ls -Al /data
total 0
drwxr-xr-x. 2 root main  6 Sep 21 19:40 main
drwxr-xr-x. 2 root third 6 Sep 21 19:40 third
```

(fig 3)

4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам: (fig 4)

```
chmod 770 /data/main
```

```
chmod 770 /data/third
```

Проверьте установленные права доступа.

```
[root@chileshelupupa ~]# chmod 770 /data/main
[root@chileshelupupa ~]# chmod 770 /data/third
[root@chileshelupupa ~]# ls -Al /data
total 0
drwxrwx---. 2 root main  6 Sep 21 19:40 main
drwxrwx---. 2 root third 6 Sep 21 19:40 third
```

(fig 4)

5. В другом терминале перейдите под учётную запись пользователя bob(fig 5)

```
su - bob
```

```
[root@chileshelupupa ~]# su - bob
[bob@chileshelupupa ~]$ id
uid=1002(bob) gid=1002(bob) groups=1002(bob),1003(main) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

(fig 5)

6. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталог (fig 6)

```
cd /data/main
```

```
touch emptyfile
```

```
ls -Al
```

```
[bob@chileshelupupa ~]$ cd /data/main
[bob@chileshelupupa main]$ touch emptyfile
[bob@chileshelupupa main]$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Sep 21 19:45 emptyfile
```

7. Под пользователем bob попробуйте перейти в каталог /data/third и создать файл emptyfile в этом каталоге. (fig 7)

```
[bob@chileshelupupa main]$ cd /data/third/
-bash: cd: /data/third/: Permission denied
```

(fig 7)

## Управление специальными разрешениями

1. Откройте новый терминал под пользователем alice(fig 8)

```
[lchileshe@chileshelupupa ~]$ su -
Password:
[root@chileshelupupa ~]# su - alice
```

(fig 8)

2. Перейдите в каталог /data/main(fig 9)

```
cd /data/main
```

Создайте два файла, владельцем которых является alice:

```
touch alice1
```

```
touch alice2
```

```
[alice@chileshelupupa ~]$ cd /data/main
[alice@chileshelupupa main]$ touch alice1
[alice@chileshelupupa main]$ touch alice2
```

(fig 9)

3. В другом терминале перейдите под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice):

su - bob

4. Перейдите в каталог /data/main: (fig 10)

cd /data/main

и в этом каталоге введите:

ls -l

```
[bob@chileshepupa main]$ cd /data/main
[bob@chileshepupa main]$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Sep 21 19:48 alice1
-rw-r--r--. 1 alice alice 0 Sep 21 19:48 alice2
-rw-r--r--. 1 bob bob 0 Sep 21 19:45 emptyfile
```

(fig 10)

5. Создайте два файла, которые принадлежат пользователю bob:

touch bob1

touch bob2

6. В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы: (fig 11)

chmod g+s,o+t /data/main

```
[root@chileshepupa ~]# chmod g+s,o+t /data/main
```

(fig 11)

7. В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4: (fig 12)

touch alice3

touch alice4

ls -l

```
[alice@chileshelupupa main]$ touch alice3
[alice@chileshelupupa main]$ touch alice4
[alice@chileshelupupa main]$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Sep 21 19:52 alice3
-rw-r--r--. 1 alice main 0 Sep 21 19:52 alice4
-rw-r--r--. 1 bob   bob   0 Sep 21 19:50 bob1
-rw-r--r--. 1 bob   bob   0 Sep 21 19:51 bob2
-rw-r--r--. 1 bob   bob   0 Sep 21 19:45 emptyfile
```

(fig 12)

## Управление расширенными разрешениями с использованием списков ACL

1. Откройте терминал с учётной записью root
2. Установите 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:

```
setfacl -m g:third:rx /data/main
```

```
setfacl -m g:main:rx /data/third
```

```
[root@chileshelupupa ~]# setfacl -m g:third:rx /data/main/
[root@chileshelupupa ~]# setfacl -m g:main:rx /data/third
```

3. Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:

```
getfacl /data/main
```

```
getfacl /data/third
```

```
[root@chileshelupupa ~]# 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@chileshelupupa ~]# 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:---
```

4. Создайте новый файл с именем newfile1 в каталоге /data/main:

```
touch /data/main/newfile1
```

Используйте

```
getfacl /data/main/newfile1
```

5. Установите ACL по умолчанию для каталога /data/main:

```
setfacl -m d:g:third:rwx /data/main
```

```
[root@chileshelupupa ~]# setfacl -m d:g:third:rwx /data/main
```

6. Добавьте ACL по умолчанию для каталога /data/third:

```
setfacl -m d:g:main:rwx /data/third
```

```
[root@chileshelupupa ~]# setfacl -m d:g:main:rwx /data/third
```

7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main:

```
touch /data/main/newfile2
```

```
[root@chileshepupa ~]# touch /data/main/newfile2
[root@chileshepupa ~]# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root
# group: main
user::rw-
group::rw-                    #effective:rw-
group:third:rw-               #effective:rw-
mask::rw-
other::---
```

8. Для проверки полномочий группы third в каталоге /data/third войдите в другом терминале под учётной записью члена группы third: su - carol Проверьте операции с файлами:

```
rm /data/main/newfile1
```

```
rm /data/main/newfile2
```

Проверьте, возможно ли осуществить запись в файл:

```
echo "Hello, world" >> /data/main/newfile1
```

```
echo "Hello, world" >> /data/main/newfile2
```

```
[lchileshe@chileshepupa ~]$ su - carol
Password:
[carol@chileshepupa ~]$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1'? Y
rm: cannot remove '/data/main/newfile1': Permission denied
[carol@chileshepupa ~]$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
[carol@chileshepupa ~]$ echo "Hello, World" >> /data/main/newfile1
-bash: /data/main/newfile1: Permission denied
[carol@chileshepupa ~]$ echo "Hello, world" >> /data/main/newfile2
[carol@chileshepupa ~]$ less newfile2
newfile2: No such file or directory
[carol@chileshepupa ~]$ less newfile2
newfile2: No such file or directory
[carol@chileshepupa ~]$ cd /data/main/
```

```
Hello, world
newfile2 (END)
```



## 4 Выводы

Я изучил получение функций для установки основных и специальных прав доступа для групп пользователей в таких системах, как Linux.