

Настройка прав доступа

Майоров Дмитрий Андреевич

Содержание i

1. Цель работы

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

2. Выполнение лабораторной работы

Открываем терминал с учетной записью root. Создаем каталоги /data/main и /data/third. Смотрим кто является владельцем этих каталогов.

```
mayorovda@mayorovda:~$ su -
Password:
Last login: Fri Jan 30 15:14:44 MSK 2026 on pts/0
root@mayorovda:~# mkdir -p /data/main /data/third
root@mayorovda:~# ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 Feb  1 15:02 main
drwxr-xr-x. 2 root root 6 Feb  1 15:02 third
root@mayorovda:~# █
```

Рисунок 1

3. Выполнение лабораторной работы

Изменяем владельцев этих каталогов с root на main и third соответственно.

```
root@mayorovda:~# chgrp main /data/main
root@mayorovda:~# chgrp third /data/third
root@mayorovda:~# ls -Al /data
total 0
drwxr-xr-x. 2 root main 6 Feb 1 15:02 main
drwxr-xr-x. 2 root third 6 Feb 1 15:02 third
```

Рисунок 2

4. Выполнение лабораторной работы

Устанавливаем разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам

```
root@mayorovda:~# chmod 770 /data/main
root@mayorovda:~# chmod 770 /data/third
root@mayorovda:~# ls -Al /data
total 0
drwxrwx---. 2 root main 6 Feb 1 15:02 main
drwxrwx---. 2 root third 6 Feb 1 15:02 third
```

Рисунок 3

5. Выполнение лабораторной работы

В другом терминале под пользователем bob переходим в каталог /data/main и создаем файл

```
mayorovda@mayorovda:~$ su - bob
Password:
bob@mayorovda:~$ cd /data/main
bob@mayorovda:/data/main$ touch emptyfile
bob@mayorovda:/data/main$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Feb 1 15:04 emptyfile
```

Рисунок 4

6. Выполнение лабораторной работы

Пробуем перейти в каталог /data/third. В разрешении отказано, так как bob не является владельцем каталога

```
bob@mayotovda:/data/main$ cd  
bob@mayotovda:~$ cd /data/third  
-bash: cd: /data/_third: Permission denied
```

Рисунок 5

7. Выполнение лабораторной работы

В другом терминале под пользователем alice переходим в каталог /data/main и создаем файлы alice1 и alice2

```
mayorovda@mayorovda:~$ su - alice
Password:
Last login: Fri Jan 30 15:23:14 MSK 2026 on pts/0
alice@mayorovda:~$ cd /data/main
alice@mayorovda:/data/main$ touch alice1
alice@mayorovda:/data/main$ touch alice2
alice@mayorovda:/data/main$ █
```

Рисунок 6

8. Выполнение лабораторной работы

Под пользователем bob переходим в каталог /data/main, просматриваем все файлы каталога. Удаляем файлы, созданные alice

```
bob@mayorovda:~$ cd /data/main
bob@mayorovda:/data/main$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Feb 1 15:07 alicel
-rw-r--r--. 1 alice alice 0 Feb 1 15:07 alice2
-rw-r--r--. 1 bob    bob    0 Feb 1 15:05 emptyfile
bob@mayorovda:/data/main$ rm -f alice*
bob@mayorovda:/data/main$ ls -l
total 0
-rw-r--r--. 1 bob    bob    0 Feb 1 15:05 emptyfile
```

Рисунок 7

9. Выполнение лабораторной работы

Создаем два файла, которые принадлежат пользователю bob

```
bob@mayorovda:/data/main$ touch bob1  
bob@mayorovda:/data/main$ touch bob2
```

Рисунок 8

10. Выполнение лабораторной работы

В терминале под пользователем root устанавливаем для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы

```
job@mayorovda:/data/main$ su -
'password:
.last login: Sun Feb  1 15:02:17 MSK 2026 on pts/0
root@mayorovda:~# chmod g+s,o+t /data/main
```

Рисунок 9

11. Выполнение лабораторной работы

В терминале под пользователем alice создаем в каталоге /data/main файлы alice3 и alice4. Теперь видим, что два созданных файла принадлежат группе main, которая является группой-владельцем каталога /data/main

```
alice@mayorovda:/data/main$ touch alice3
alice@mayorovda:/data/main$ touch alice4
alice@mayorovda:/data/main$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Feb  1 15:08 alice3
-rw-r--r--. 1 alice main 0 Feb  1 15:08 alice4
-rw-r--r--. 1 bob    bob   0 Feb  1 15:08 bob1
-rw-r--r--. 1 bob    bob   0 Feb  1 15:08 bob2
-rw-r--r--. 1 bob    bob   0 Feb  1 15:05 emptyfile
```

Рисунок 10

12. Выполнение лабораторной работы

Пробуем удалить файлы пользователя bob. Sticky-bit предотвратил удаление этих файлов

```
alice@mayorovda:/data/main$ rm -rf bob*
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
...
```

Рисунок 11

13. Выполнение лабораторной работы

Устанавливаем 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

```
mayorovda@mayorovda:~$ su -
Password:
Last login: Sun Feb  1 15:08:27 MSK 2026 on pts/1
root@mayorovda:~# setfacl -m g:third:rx /data/main
root@mayorovda:~# setfacl -m g:main:rx /data/third
```

Рисунок 12

14. Выполнение лабораторной работы

Убеждаемся в правильности установки разрешений

```
root@mayorovda:~# 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@mayorovda:~# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
```

Рисунок 13

15. Выполнение лабораторной работы

Создаем файл newfile1 в каталоге /data/main. Проверяем текущие назначения полномочий. Права доступа: Владелец(root) может читать и писать(rw-). Группа(main) может только читать(r-). Остальные могут только читать(r-)

```
root@mayorovda:~# touch /data/main/newfile1
root@mayorovda:~# 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--
```

Рисунок 14

16. Выполнение лабораторной работы

Выполняем такие же действия для каталога third. Права доступа такие же как и у /data/main.

```
root@mayorovda:~# touch /data/third/newfile1
root@mayorovda:~# 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--
```

Рисунок 15

17. Выполнение лабораторной работы

Устанавливаем ACL по умолчанию для каталога /data/main и /data/third

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

Рисунок 16

18. Выполнение лабораторной работы

Убеждаемся, что настройки ACL работают, добавив новый файл в каталог /data/main и проверяя текущие назначения полномочий. Выполняем такие же действия для каталога third

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

Рисунок 17

19. Выполнение лабораторной работы

Проверяем операции с файлами под пользователем carol. Пользователю отказано в разрешении ко всем файлам, кроме записи в newfile2

```
mayorovda@mayorovda:~$ su - carol
Password:
Last login: Fri Jan 30 15:22:43 MSK 2026 on pts/0
carol@mayorovda:~$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1'? y
rm: cannot remove '/data/main/newfile1': Permission denied
carol@mayorovda:~$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
carol@mayorovda:~$ echo "Hello, world" >> /data/main/newfile1
-bash: /data/main/newfile1: Permission denied
carol@mayorovda:~$ echo "Hello, world" >> /data/main/newfile2
```

Рисунок 18

20. Выводы

Получены навыки настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux