



## РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук  
Кафедра прикладной информатики и теории вероятностей

### ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

Настройка прав доступа в операционной системе Linux

Студент: Эйвази Мани

Группа: НПИбд-03-24

Студенческий билет №: 1032245107

### **Цель работы**

Целью данной лабораторной работы является получение практических навыков настройки базовых, специальных и расширенных прав доступа в операционной системе Linux, а также изучение механизмов разграничения доступа для различных групп пользователей.

**Первый шаг:** В начале работы был выполнен вход в систему под учетной записью суперпользователя root. В корневом каталоге были созданы директории /data/main и /data/third.

```
root@localhost:/# whoami
root
root@localhost:/# mkdir -p /data/main /data/third
root@localhost:/# ls -Al /data
ls: cannot access '-': No such file or directory
ls: cannot access 'Al': No such file or directory
/data:
main  third
root@localhost:/# ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 Dec 16 04:54 main
drwxr-xr-x. 2 root root 6 Dec 16 04:54 third
```

**Второй шаг:** для созданных директорий была изменена группа-владелец с root на соответствующие группы main и third. После этого были установлены базовые права доступа, разрешающие чтение, запись и выполнение для владельца и группы, а также запрещающие доступ для остальных пользователей.

```
root@localhost:/# chgrp main /data/main
root@localhost:/# chgrp third /data/third
root@localhost:/# ls -Al data
total 0
drwxr-xr-x. 2 root main 6 Dec 16 04:54 main
drwxr-xr-x. 2 root third 6 Dec 16 04:54 third
root@localhost:/# chmod 770 /data/main
root@localhost:/# chmod 770 /data/third
```

**Третий шаг:** под учетной записью пользователя bob были выполнены попытки доступа к каталогам. Было подтверждено, что пользователь может работать с каталогом своей группы и не имеет доступа к каталогу другой группы.

```
root@localhost:/# su bob
bob@localhost:/$ cd /data/main
bob@localhost:/data/main$ touch emptyfile
bob@localhost:/data/main$ ls -Al
total 0
-rw-r--r--. 1 bob users 0 Dec 16 04:57 emptyfile
bob@localhost:/data/main$ ls -a
. .. emptyfile
bob@localhost:/data/main$ cd /data/third
bash: cd: /data/third: Permission denied
```

**Четвертый шаг:** для организации безопасной совместной работы в каталоге /data/main были настроены специальные права доступа. Был установлен бит идентификатора группы (SetGID), обеспечивающий наследование группы каталога для новых файлов. также был установлен sticky-bit, который предотвращает удаление файлов пользователями, не являющимися владельцами этих файлов, даже если они имеют доступ к каталогу.

```
root@localhost:/data/main# chmod g+s,o+t /data/main
alice@localhost:/data/main$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Dec 16 05:03 alice3
-rw-r--r--. 1 alice main 0 Dec 16 05:03 alice4
-rw-r--r--. 1 bob users 0 Dec 16 05:01 bob1
-rw-r--r--. 1 bob users 0 Dec 16 05:01 bob2
-rw-r--r--. 1 bob users 0 Dec 16 04:57 emptyfile
```

**Пятый шаг:** далее были использованы списки контроля доступа (ACL) для расширения стандартных прав. Группе `third` были предоставлены права чтения и выполнения в каталоге `/data/main`, а группе `main` — аналогичные права в каталоге `/data/third`.

**Шестой шаг:** с помощью команды `getfacl` была выполнена проверка корректности установленных ACL. Было подтверждено, что дополнительные разрешения применены без изменения базовых прав.

[illegible]

**Седьмой шаг:** для обеспечения наследования расширенных прав доступа были настроены ACL по умолчанию. После этого новые файлы, создаваемые в каталогах, автоматически получали соответствующие права.

```
manieyvazi@localhost:~$ su
Password:
root@localhost:/home/manieyvazi# setfacl -m g:third:rx /data/main
root@localhost:/home/manieyvazi# setfacl -m g:main:rx /data/third
root@localhost:/home/manieyvazi# detfacl /data/main
bash: detfacl: command not found...
root@localhost:/home/manieyvazi# 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:---
```

**Восьмой шаг:** в заключение работа прав доступа была проверена под учетной записью пользователя carol. Результаты показали, что пользователи могут выполнять только разрешенные действия, что подтверждает корректность настройки прав доступа

```
alice@localhost:/data/main$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Dec 16 05:03 alice3
-rw-r--r--. 1 alice main 0 Dec 16 05:03 alice4
-rw-r--r--. 1 bob users 0 Dec 16 05:01 bob1
-rw-r--r--. 1 bob users 0 Dec 16 05:01 bob2
-rw-r--r--. 1 bob users 0 Dec 16 04:57 emptyfile
```

## **заключение**

В этой лабораторной работы были изучены механизмы управления правами доступа в Linux, включая базовые разрешения, специальные атрибуты и расширенные списки контроля доступа (ACL). Полученные навыки позволяют гибко и безопасно настраивать доступ пользователей и групп к ресурсам операционной системы.

1. Как следует использовать команду `chown`, чтобы установить владельца группы для файла? Приведите пример.

```
chown user: group file.txt  
chown bob:developers script.sh
```

2. С помощью какой команды можно найти все файлы, принадлежащие конкретному пользователю? Приведите пример.

```
find / -user bob 2>/dev/null
```

3. Как применить разрешения на чтение, запись и выполнение для всех файлов в каталоге `/data` для пользователей и владельцев групп, не устанавливая никаких прав для других? Приведите пример.

```
chmod -R ug+rw, o-rwx /data
```

4. Какая команда позволяет добавить разрешение на выполнение для файла, который необходимо сделать исполняемым?

```
chmod +x file.sh
```

5. Какая команда позволяет убедиться, что групповые разрешения для всех новых файлов, создаваемых в каталоге, будут присвоены владельцу группы этого каталога? Приведите пример.

```
chmod g+s /data/shared  
ls -ld /data/shared
```

6. Необходимо, чтобы пользователи могли удалять только те файлы, владельцами которых они являются, или которые находятся в каталоге, владельцами которого они являются. С помощью какой команды можно это сделать? Приведите пример.

```
chmod +t /data/shared
```

7. Какая команда добавляет ACL, который предоставляет членам группы права доступа на чтение для всех существующих файлов в текущем каталоге?

```
setfacl-m g:team:r *
```

8. Что нужно сделать для гарантии того, 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? Приведите пример.

```
setfacl-R-m g:team:r /path/to/dir
```

```
setfacl-R-d-m g:team:r /path/to/dir
```

9. Какое значение umask нужно установить, чтобы «другие» пользователи не получали какие-либо разрешения на новые файлы? Приведите пример. Кулябов Д. С., Королькова А. В. Основы администрирования операционных систем 31

```
umask 007
```

10. Какая команда гарантирует, что никто не сможет удалить файл myfile случайно? При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1—5].

```
chattr +i myfile
```

```
# Удалить атрибут:
```

```
chattr-i myfile
```