

## Лабораторная работа №3

Настройка прав доступа в Linux

---

Щемелев Илья Владимирович

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

## Формулировка цели

---

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

## Ход выполнения работы

---

## Проверка доступа пользователя bob

```
ivschemelev@ivschemelev:~$ su
Password:
root@ivschemelev:/home/ivschemelev# mkdir -p /data/main /data/third
root@ivschemelev:/home/ivschemelev# ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 Jan 15 12:23 main
drwxr-xr-x. 2 root root 6 Jan 15 12:23 third
root@ivschemelev:/home/ivschemelev# chgrp main /data/main/
root@ivschemelev:/home/ivschemelev# chgrp third /data/third/
root@ivschemelev:/home/ivschemelev# ls -Al /data
total 0
drwxr-xr-x. 2 root main 6 Jan 15 12:23 main
drwxr-xr-x. 2 root third 6 Jan 15 12:23 third
root@ivschemelev:/home/ivschemelev# chmod 770 /data/main
root@ivschemelev:/home/ivschemelev# chmod 770 /data/third/
root@ivschemelev:/home/ivschemelev# ls -Al /data
total 0
drwxrwx---. 2 root main 6 Jan 15 12:23 main
drwxrwx---. 2 root third 6 Jan 15 12:23 third
root@ivschemelev:/home/ivschemelev# su bob
bob@ivschemelev:/home/ivschemelev$ cd /data/main/
bob@ivschemelev:/data/main$ touch emptyfile
bob@ivschemelev:/data/main$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Jan 15 12:25 emptyfile
bob@ivschemelev:/data/main$ cd /data/third/
bash: cd: /data/third/: Permission denied
bob@ivschemelev:/data/main$ █
```

## Установка setgid и sticky bit

```
alice@ivschemelev:/data/main$ cd /data/main
alice@ivschemelev:/data/main$ touch alice1
alice@ivschemelev:/data/main$ touch alice2
alice@ivschemelev:/data/main$ 
exit
bob@ivschemelev:/data/main$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Jan 15 12:28 alice1
-rw-r--r--. 1 alice alice 0 Jan 15 12:28 alice2
-rw-r--r--. 1 bob   bob   0 Jan 15 12:25 emptyfile
bob@ivschemelev:/data/main$ rm -f alice*
bob@ivschemelev:/data/main$ ls -l
total 0
-rw-r--r--. 1 bob   bob   0 Jan 15 12:25 emptyfile
bob@ivschemelev:/data/main$ touch bob1
bob@ivschemelev:/data/main$ touch bob2
bob@ivschemelev:/data/main$ 
exit
root@ivschemelev:/home/ivschemelev# chmod g+s,o+t /data/main/
root@ivschemelev:/home/ivschemelev# su alice
alice@ivschemelev:/home/ivschemelev$ cd /data/main/
alice@ivschemelev:/data/main$ touch alice3
alice@ivschemelev:/data/main$ touch alice4
alice@ivschemelev:/data/main$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Jan 15 12:29 alice3
-rw-r--r--. 1 alice main 0 Jan 15 12:29 alice4
-rw-r--r--. 1 bob   bob   0 Jan 15 12:28 bob1
-rw-r--r--. 1 bob   bob   0 Jan 15 12:28 bob2
-rw-r--r--. 1 bob   bob   0 Jan 15 12:25 emptyfile
alice@ivschemelev:/data/main$ rm -rf bob*
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
alice@ivschemelev:/data/main$
```

## Настройка ACL для каталогов

```
root@ivschemelev:/home/ivschemelev# 
root@ivschemelev:/home/ivschemelev# setfacl -m g:third:rx /data/main
root@ivschemelev:/home/ivschemelev# setfacl -m g:main:rx /data/third
root@ivschemelev:/home/ivschemelev# 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@ivschemelev:/home/ivschemelev# 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@ivschemelev:/home/ivschemelev#
```

## Проверка прав нового файла

```
root@ivschemelev:/home/ivschemelev# touch /data/main/newfile1
root@ivschemelev:/home/ivschemelev# 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@ivschemelev:/home/ivschemelev# touch /data/third/newfile1
root@ivschemelev:/home/ivschemelev# 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@ivschemelev:/home/ivschemelev#
```

## Наследование ACL новыми файлами

```
root@ivschemelev:/home/ivschemelev# 
root@ivschemelev:/home/ivschemelev# setfacl -m d:g:third:rwx /data/main/
root@ivschemelev:/home/ivschemelev# setfacl -m d:g:main:rwx /data/third/
root@ivschemelev:/home/ivschemelev# touch /data/main/newfile2
root@ivschemelev:/home/ivschemelev# 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@ivschemelev:/home/ivschemelev# touch /data/third/newfile2
root@ivschemelev:/home/ivschemelev# 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@ivschemelev:/home/ivschemelev# 
root@ivschemelev:/home/ivschemelev# 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@ivschemelev:/home/ivschemelev# 
```

## Проверка доступа пользователем carol

```
root@ivschemelev:/home/ivschemelev#
root@ivschemelev:/home/ivschemelev# su carol
carol@ivschemelev:/home/ivschemelev$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1'? y
rm: cannot remove '/data/main/newfile1': Permission denied
carol@ivschemelev:/home/ivschemelev$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
carol@ivschemelev:/home/ivschemelev$ echo "Hello world" >> /data/main/newfile1
bash: /data/main/newfile1: Permission denied
carol@ivschemelev:/home/ivschemelev$ echo "Hello world" >> /data/main/newfile2
carol@ivschemelev:/home/ivschemelev$
```

Рис. 6: Проверка прав доступа пользователем carol

## Итоги работы

---

В ходе лабораторной работы были последовательно изучены механизмы управления доступом в Linux:

базовые права доступа, специальные атрибуты setgid и sticky bit, а также расширенные списки контроля доступа ACL.

Практические эксперименты подтвердили эффективность данных механизмов для безопасной организации совместного доступа пользователей к файловым ресурсам.