

# **Лабораторная работа № 3**

**Настройка прав доступа**

Жукова София Викторовна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>16</b>

# Список иллюстраций

2.1	Роль супер-пользователя . . . . .	6
2.2	каталоги /data/main и /data/third . . . . .	6
2.3	Изменим владельцев каталогов . . . . .	7
2.4	Права доступа . . . . .	7
2.5	Учётная запись пользователя bob . . . . .	7
2.6	emptyfile . . . . .	8
2.7	Нам отказано в доступе, нет нужных прав . . . . .	8
2.8	alice . . . . .	8
2.9	Создадим два файла . . . . .	8
2.10	Мы видим два файла, созданные пользователем alice . . . . .	9
2.11	Файлы удалены . . . . .	9
2.12	Два файла, которые принадлежат пользователю bob . . . . .	9
2.13	установим идентификатор группы, а также sticky-бит для разделяе- мого каталога группы . . . . .	9
2.14	Файлы alice3 и alice4 . . . . .	10
2.15	Операция недоступна . . . . .	10
2.16	права на чтение и выполнение . . . . .	10
2.17	Правильность установки разрешений . . . . .	11
2.18	Правильность установки разрешени . . . . .	11
2.19	Установим и проверим . . . . .	11
2.20	Добавим . . . . .	12
2.21	Добавим новый файл в каталог . . . . .	12
2.22	Проверим . . . . .	12
2.23	Выполним . . . . .	12
2.24	Нельзя . . . . .	13
2.25	Можно только во втором случае . . . . .	13

## **Список таблиц**

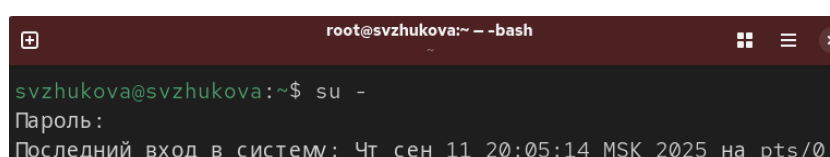
# 1 Цель работы

Целью данной работы является получение навыков настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.

## 2 Выполнение лабораторной работы

### Управление базовыми разрешениями

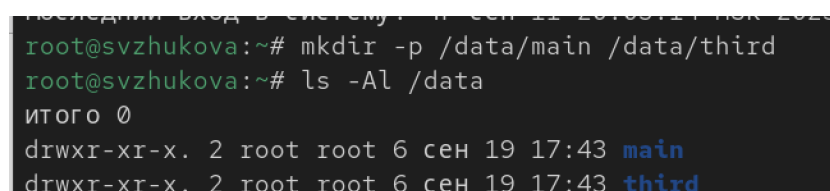
Откроем терминал с учётной записью root (рис. 2.1).



```
root@svzhukova:~ -- -bash
svzhukova@svzhukova:~$ su -
Пароль:
Последний вход в систему: Чт сен 11 20:05:14 MSK 2025 на pts/0
```

Рис. 2.1: Роль супер-пользователя

В корневом каталоге создадим каталоги /data/main и /data/third. Посмотрим, кто является владельцем этих каталогов. (рис. 2.2).



```
Последний вход в систему: Чт сен 11 20:05:14 MSK 2025 на pts/0
root@svzhukova:~# mkdir -p /data/main /data/third
root@svzhukova:~# ls -Al /data
итого 0
drwxr-xr-x. 2 root root 6 сен 19 17:43 main
drwxr-xr-x. 2 root root 6 сен 19 17:43 third
```

Рис. 2.2: каталоги /data/main и /data/third

Прежде чем устанавливать разрешения, изменим владельцев этих каталогов с root на main и third соответственно. Посмотрим, кто теперь является владельцем этих каталогов (рис. 2.3).

```

root@svzhukova:~# chgrp main /data/main
root@svzhukova:~# chgrp third /data/third
root@svzhukova:~# ls -Al /data
итого 0
drwxr-xr-x. 2 root main  6 сен 19 17:43 main
drwxr-xr-x. 2 root third 6 сен 19 17:43 third

```

Рис. 2.3: Изменим владельцев каталогов

Установим разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам. Проверим установленные права доступа (рис. 2.4).

```

root@svzhukova:~# chmod 770 /data/main
root@svzhukova:~# chmod 770 /data/third
root@svzhukova:~# ls -Al /data
итого 0
drwxrwx---. 2 root main  6 сен 19 17:43 main
drwxrwx---. 2 root third 6 сен 19 17:43 third
root@svzhukova:~#

```

Рис. 2.4: Права доступа

В другом терминале перейдем под учётную запись пользователя bob (рис. 2.5).

```

svzhukova@svzhukova:~$ su - bob
Пароль:
Последняя неудачная попытка входа в систему: Пт сен 19 17:47:22
MSK 2025 на pts/1
Со времени последнего входа была 1 неудачная попытка.

```

Рис. 2.5: Учётная запись пользователя bob

Под пользователем bob попробуем перейти в каталог /data/main и создать файл emptyfile в этом каталоге (рис. 2.6).

```

bob@svzhukova:~$ cd /data/main
bob@svzhukova:/data/main$ ^C
bob@svzhukova:/data/main$ touch emptyfile
bob@svzhukova:/data/main$ ls -Al
итого 0
-rw-r--r--. 1 bob bob 0 сен 19 17:48 emptyfile

```

Рис. 2.6: emptyfile

Под пользователем bob попробуем перейти в каталог /data/third и создать файл emptyfile в этом каталоге (рис. 2.7).

```

bob@svzhukova:/data/main$ cd /data/third
-bash: cd: /data/third: Отказано в доступе
bob@svzhukova:/data/main$ P

```

Рис. 2.7: Нам отказано в доступе, нет нужных прав

### Управление специальными разрешениями

Откроем новый терминал под пользователем alice (рис. 2.8).

```

svzhukova@svzhukova:~$ su - alice
Пароль:
Последний вход в систему: Чт сен 11 20:08:51 MSK 2025 на pts/0
alice@svzhukova:~$ cd /data/main

```

Рис. 2.8: alice

Перейдите в каталог /data/main и создадим два файла, владельцем которых является alice (рис. 2.9).

```

alice@svzhukova:/data/main$ touch alice1
alice@svzhukova:/data/main$ touch alice2

```

Рис. 2.9: Создадим два файла

В другом терминале перейдем под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice) Перейдем в каталог /data/main и в этом каталоге введем (рис. 2.10).



```
svzhukova@svzhukova:~$ su - bob
Пароль:
Последний вход в систему: Пт сен 19 17:47:29 MSK 2025 на pts/1
bob@svzhukova:~$ cd /data/main
bob@svzhukova:/data/main$ ls -l
итого 0
-rw-r--r--. 1 alice alice 0 сен 19 17:51 alice1
-rw-r--r--. 1 alice alice 0 сен 19 17:51 alice2
-rw-r--r--. 1 bob bob 0 сен 19 17:48 emptyfile
```

Рис. 2.10: Мы видим два файла, созданные пользователем alice

Попробуем удалить файлы, принадлежащие пользователю alice (рис. 2.11).

```
bob@svzhukova:/data/main$ rm -f alice*
bob@svzhukova:/data/main$ ls -l
итого 0
-rw-r--r--. 1 bob bob 0 сен 19 17:48 emptyfile
```

Рис. 2.11: Файлы удалены

Создадим два файла, которые принадлежат пользователю bob (рис. 2.12).

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

Рис. 2.12: Два файла, которые принадлежат пользователю bob

В терминале под пользователем root установим для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы (рис. 2.13).

```
root@svzhukova:~# chmod g+s,o+t /data/main
root@svzhukova:~#
```

Рис. 2.13: установим идентификатор группы, а также sticky-бит для разделяемого каталога группы

В терминале под пользователем alice создадим в каталоге /data/main файлы alice3 и alice4(рис. 2.14).

```

alice@svzhukova:/data/main$ touch alice3
alice@svzhukova:/data/main$ touch alice4
alice@svzhukova:/data/main$ ls -l
итого 0
-rw-r--r--. 1 alice main 0 сен 19 17:56 alice3
-rw-r--r--. 1 alice main 0 сен 19 17:56 alice4
-rw-r--r--. 1 bob   bob   0 сен 19 17:54 bob1
-rw-r--r--. 1 bob   bob   0 сен 19 17:54 bob2
-rw-r--r--. 1 bob   bob   0 сен 19 17:48 emptyfile

```

Рис. 2.14: Файлы alice3 и alice4

Теперь мы видим, что два созданных нами файла принадлежат группе main, которая является группой-владельцем каталога /data/main

В терминале под пользователем alice попробуем удалить файлы, принадлежащие пользователю bob(рис. 2.15).

```

alice@svzhukova:/data/main$ rm -rf bob*
rm: невозможно удалить 'bob1': Операция не позволена
rm: невозможно удалить 'bob2': Операция не позволена

```

Рис. 2.15: Операция недоступна

### Управление расширенными разрешениями с использованием списков ACL

Откроем терминал с учётной записью root 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. 2.16).

```

root@svzhukova:~# setfacl -m g:third:rx /data/main
root@svzhukova:~# setfacl -m g:main:rx /data/third

```

Рис. 2.16: права на чтение и выполнение

Используем команду getfacl, чтобы убедиться в правильности установки разрешений(рис. 2.17). (рис. 2.18).

```

root@svzhukova:~# 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::---

```

Рис. 2.17: Правильность установки разрешений

```

root@svzhukova:~# 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@svzhukova:~# P

```

Рис. 2.18: Правильность установки разрешени

Создадим новый файл с именем newfile1 в каталоге /data/main: Проверим текущие назначения полномочий. (рис. 2.19).

```

root@svzhukova:~# touch /data/third/newfile1
root@svzhukova:~# 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@svzhukova:~#

```

Рис. 2.19: Установим и проверим

Установим ACL по умолчанию для каталога /data/main:

Добавим ACL по умолчанию для каталога /data/third(рис. 2.20).

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

Рис. 2.20: Добавим

Убедимся, что настройки ACL работают, добавив новый файл в каталог /data/main:(рис. 2.21).

```
root@svzhukova:~# touch /data/main/newfile2
```

Рис. 2.21: Добавим новый файл в каталог

Проверим текущие назначения полномочий.(рис. 2.22).

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

Рис. 2.22: Проверим

Выполним аналогичные действия для каталога /data/third. (рис. 2.23).

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

Рис. 2.23: Выполним

Для проверки полномочий группы third в каталоге /data/third войдем в другом терминале под учётной записью члена группы third Проверим операции с файлами(рис. 2.24).

```
svzhukova@svzhukova:~$ su - carol
Пароль:
Последний вход в систему: Чт сен 11 20:07:07 MSK 2025 на pts/0
carol@svzhukova:~$ rm /data/main/newfile1
rm: удалить защищённый от записи пустой объёмный файл '/data/main/newfile1'? y
rm: невозможно удалить '/data/main/newfile1': Отказано в доступе
carol@svzhukova:~$
```

Рис. 2.24: Нельзя

Проверим, возможно ли осуществить запись в файл(рис. 2.25).

```
carol@svzhukova:~$ rm /data/main/newfile2
rm: невозможно удалить '/data/main/newfile2': Отказано в доступе
carol@svzhukova:~$ echo "Hello, world" >> /data/main/newfile1
-bash: /data/main/newfile1: Отказано в доступе
carol@svzhukova:~$ echo "Hello, world" >> /data/main/newfile2
carol@svzhukova:~$
```

Рис. 2.25: Можно только во втором случае

## Контрольные вопросы

1. Использование команды `chown` Чтобы установить владельца и группу для файла, используется команда `chown`. Пример:

```
chown user:group filename.txt
```

Чтобы сменить владельца файла `filename.txt` на `user` и группу на `group`.

2. Поиск файлов, принадлежащих конкретному пользователю Для этого можно использовать команду `find`. Пример:

```
find /path/to/search -user username
```

Это найдет все файлы в указанном пути, принадлежащие пользователю `username`.

3. Применение разрешений для всех файлов в `/data` Чтобы установить разрешения на чтение, запись и выполнение для всех владельцев и группы, но не для других, используйте команду `chmod`:

```
chmod 770 /data/★
```

Здесь 7 дает полные права для владельца и группы, а 0 — никаких прав для других.

4. Добавление разрешения на выполнение для файла Используйте команду `chmod`, чтобы сделать файл исполняемым. Пример:

```
chmod +x filename.sh
```

Это добавит разрешение на выполнение для файла `filename.sh`.

5. Установка групповых разрешений для новых файлов Чтобы все новые файлы, создаваемые в каталоге, наследовали группу этого каталога, используйте `chmod` с настройкой битов SGID. Пример:

```
chmod g+s /path/to/directory
```

6. Удаление файлов только владельцами Для ограничения прав удаления можно использовать `chmod`, чтобы убрать права на удаление для группы и других. Пример:

```
chmod o-w /path/to/directory
```

Эта команда убирает права записи для других пользователей, предотвращая их возможность удаления файлов.

7. Добавление ACL для группы С помощью `setfacl` можно добавить права доступа для группы. Пример:

```
setfacl -m g:groupname:r /path/to/directory/★
```

Это добавит права на чтение для группы `groupname` для всех существующих файлов в каталоге.

8. Гарантия прав чтения для всех файлов Для того чтобы члены группы получили права чтения на все файлы и подкаталоги, используйте:

```
setfacl -R -m g:groupname:rX /path/to/directory
```

Это даст права чтения и выполнения для всех файлов и каталогов.

9. Установка `umask` для ограничения прав Для того чтобы «другие» пользователи не получали разрешения на новые файлы, установите `umask` на `007`.  
Пример:

```
umask 007
```

Это гарантирует, что файлы создаются с правами `664` и каталоги с правами `775`.

10. Защита файла от удаления Чтобы гарантировать, что файл `myfile` не может быть удален случайно, можно установить только права на чтение и запись для владельца. Пример:

```
chmod 444 myfile
```

Это уберет все права на запись, что предотвратит случайное удаление файла.

## **3 Выводы**

Мы получили навыки настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.