

# **Лабораторная работа № 3.**

**Настройка прав доступа**

Диана Алексеевна Садова

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Последовательность выполнения работы</b>	<b>6</b>
2.1	Управление базовыми разрешениями . . . . .	6
2.2	Управление специальными разрешениями . . . . .	9
2.3	Управление расширенными разрешениями с использованием списков ACL . . . . .	13
<b>3</b>	<b>Выводы</b>	<b>19</b>

## Список иллюстраций

2.1	Переходим в учётную запись root . . . . .	6
2.2	Создаем каталоги /data/main и /data/third в корневом каталоге . .	6
2.3	Просматриваем кто является владельцем каталогов . . . . .	7
2.4	Изменяем владельцев каталогов main и third . . . . .	7
2.5	Просматриваем кто является владельцем каталогов . . . . .	7
2.6	Устанавливаем и проверяем разрешение . . . . .	8
2.7	Переходим к учётной записи пользователя bob . . . . .	8
2.8	Переходим в каталог и создаем файл . . . . .	8
2.9	Переходим в каталог и создаем файл . . . . .	9
2.10	Переходим к учётной записи пользователя alice . . . . .	10
2.11	Переходим в каталог . . . . .	10
2.12	Создаем два файла . . . . .	10
2.13	Переходим к учётной записи пользователя bob . . . . .	10
2.14	Переходим в каталог . . . . .	11
2.15	Просматриваем всю информацию о файлах . . . . .	11
2.16	Пытаемся удалить файл . . . . .	11
2.17	Убедимся в том что файлы удалены . . . . .	11
2.18	Создаем файлы . . . . .	12
2.19	Устанавливаем бит идентификатора группы, а так же sticky-бит . .	12
2.20	Создаем файлы и проверяем их группы . . . . .	13
2.21	Пытаемся удалить файлы . . . . .	13
2.22	Переходим в учётную запись root . . . . .	14
2.23	Устанавливаем права чтения . . . . .	15
2.24	Используем команду getfacl для main . . . . .	15
2.25	Используем команду getfacl для third . . . . .	15
2.26	Создаем файл newfile1 . . . . .	16
2.27	Создаем файл newfile2 . . . . .	16
2.28	Установили ACL для /data/main . . . . .	16
2.29	Установили ACL для /data/third . . . . .	16
2.30	Добавляем новый файл в main . . . . .	17
2.31	Добавляем новый файл в third . . . . .	17
2.32	Переходим к учётной записи пользователя carol . . . . .	18
2.33	Пытаемся удалить файлы из каталогов . . . . .	18
2.34	Пытаемся записать "Hello, world" в файл . . . . .	18
2.35	Пытаемся записать "Hello, world" в файл . . . . .	18

## **Список таблиц**

# 1 Цель работы

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

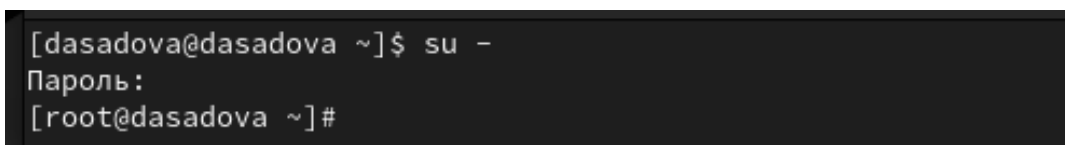
## 2 Последовательность выполнения работы

Предпосылки: в лабораторной работе № 2 были созданы пользователи alice и bob, входящие в группу main, и пользователь carol, входящий в группу third.

### 2.1 Управление базовыми разрешениями

Требуется создать структуру каталогов с разными разрешениями доступа для разных групп пользователей.

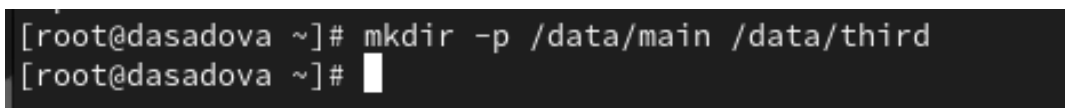
1. Откройте терминал с учётной записью root:(рис. 2.1).



```
[dasadova@dasadova ~]$ su -  
Пароль:  
[root@dasadova ~]#
```

Рис. 2.1: Переходим в учётную запись root

2. В корневом каталоге создайте каталоги /data/main и /data/third:(рис. 2.2).



```
[root@dasadova ~]# mkdir -p /data/main /data/third  
[root@dasadova ~]#
```

Рис. 2.2: Создаем каталоги /data/main и /data/third в корневом каталоге

Посмотрите, кто является владельцем этих каталогов. Для этого используйте:(рис. 2.3).

```
[root@dasadova ~]# ls -Al /data
итого 0
drwxr-xr-x. 2 root root 6 сен 16 18:10 main
drwxr-xr-x. 2 root root 6 сен 16 18:10 third
[root@dasadova ~]#
```

Рис. 2.3: Просматриваем кто является владельцем каталогов

3. Прежде чем устанавливать разрешения, измените владельцев этих каталогов с root на main и third соответственно:(рис. 2.4).

```
[root@dasadova ~]# chgrp main /data/main
[root@dasadova ~]# chgrp third /data/third
[root@dasadova ~]#
```

Рис. 2.4: Изменяем владельцев каталогов main и third

Посмотрите, кто теперь является владельцем этих каталогов:(рис. 2.5).

```
[root@dasadova ~]# ls -Al /data
итого 0
drwxr-xr-x. 2 root main 6 сен 16 18:10 main
drwxr-xr-x. 2 root third 6 сен 16 18:10 third
[root@dasadova ~]#
```

Рис. 2.5: Просматриваем кто является владельцем каталогов

4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам. Проверьте установленные права доступа(рис. 2.6).

```
[root@dasadova ~]# chmod 770 /data/main
[root@dasadova ~]# chmod 770 /data/third
[root@dasadova ~]# ls -Al /data
итого 0
drwxrwx---. 2 root main  6 сен 16 18:10 main
drwxrwx---. 2 root third 6 сен 16 18:10 third
[root@dasadova ~]#
```

Рис. 2.6: Устанавливаем и проверяем разрешение

5. В другом терминале перейдите под учётную запись пользователя bob:(рис. 2.7).

```
[root@dasadova ~]# su - bob
[bob@dasadova ~]$
```

Рис. 2.7: Переходим к учётной записи пользователя bob

6. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге:(рис. 2.8).

```
[bob@dasadova ~]$ cd /data/main
[bob@dasadova main]$ touch emptyfile
[bob@dasadova main]$ ls -Al
итого 0
-rw-r--r--. 1 bob bob 0 сен 16 18:14 emptyfile
[bob@dasadova main]$
```

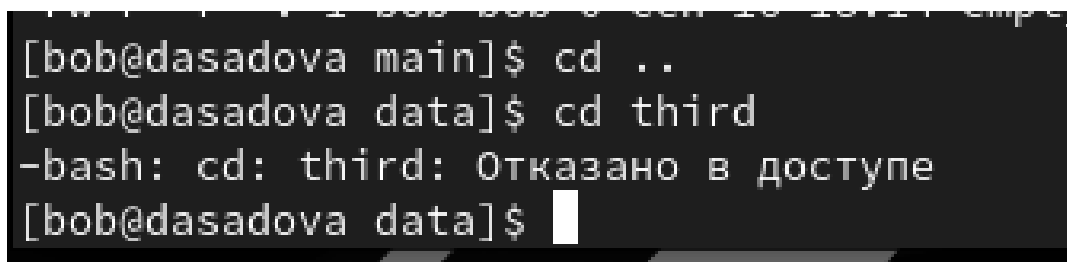
Рис. 2.8: Переходим в каталог и создаем файл

Опишите и поясните результат этого действия.

Пользователь bob может создать файл в каталоге main, так как имеет права доступа в каталоге



7. Под пользователем bob попробуйте перейти в каталог /data/third и создать файл emptyfile в этом каталоге.(рис. 2.9).



```
[bob@dasadova main]$ cd ..  
[bob@dasadova data]$ cd third  
-bash: cd: third: Отказано в доступе  
[bob@dasadova data]$
```

Рис. 2.9: Переходим в каталог и создаем файл

Опишите и поясните результат этого действия.

Пользователь bob не может создать файл в каталоге third, так как сам не принадлежит к этому каталогу и не имеет прав доступа

## 2.2 Управление специальными разрешениями

Требуется, используя специальные разрешения для групп пользователей, обеспечить обмен файлами в общем для групп каталоге. При этом каталогу назначается бит идентификатора группы, а также sticky bit.

Sticky bit — дополнительный атрибут файлов или каталогов в ОС типа Linux, применяющийся в основном для каталогов с целью защиты содержимого каталогов от повреждения или удаления пользователями, не являющимися их владельцами. Для установки этого атрибута используется утилита chmod. Восьмеричное значение stiky-бита: 1000, а символьное: +t.

1. Откройте новый терминал под пользователем alice.(рис. 2.10).

```
[bob@dasadova data]$ su - alice
Пароль:
[alice@dasadova ~]$
```

Рис. 2.10: Переходим к учётной записи пользователя alice

2. Перейдите в каталог /data/main:(рис. 2.11).

```
[alice@dasadova ~]$ cd /data/main
[alice@dasadova main]$
```

Рис. 2.11: Переходим в каталог

- Создайте два файла, владельцем которых является alice:(рис. 2.12).

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

Рис. 2.12: Создаем два файла

3. В другом терминале перейдите под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice):(рис. 2.13).

```
[alice@dasadova main]$ su - bob
Пароль:
[bob@dasadova ~]$
```

Рис. 2.13: Переходим к учётной записи пользователя bob

4. Перейдите в каталог /data/main:(рис. 2.14).

```
[bob@dasadova ~]$ cd /data/main  
[bob@dasadova main]$
```

Рис. 2.14: Переходим в каталог

и в этом каталоге введите:(рис. 2.15).

```
[bob@dasadova main]$ ls -l  
итого 0  
-rw-r--r--. 1 alice alice 0 сен 16 18:18 alice1  
-rw-r--r--. 1 alice alice 0 сен 16 18:18 alice2  
-rw-r--r--. 1 bob bob 0 сен 16 18:14 emptyfile  
[bob@dasadova main]$
```

Рис. 2.15: Просматриваем всю информацию о файлах

Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:(рис. 2.16).

```
[alice@dasadova ~]$ rm -f alice*  
[alice@dasadova ~]$
```

Рис. 2.16: Пробуем удалить файл

Убедитесь, что файлы будут удалены пользователем bob.(рис. 2.17).

```
[bob@dasadova main]$ ls -l  
итого 0  
-rw-r--r--. 1 bob bob 0 сен 16 18:14 emptyfile  
[bob@dasadova main]$
```

Рис. 2.17: Убедимся в том что файлы удалены

5. Создайте два файла, которые принадлежат пользователю bob:(рис. 2.18).

```
[bob@dasadova main]$ touch bob1
[bob@dasadova main]$ touch bob2
[bob@dasadova main]$ ls -l
итого 0
-rw-r--r--. 1 bob bob 0 сен 16 18:21 bob1
-rw-r--r--. 1 bob bob 0 сен 16 18:21 bob2
-rw-r--r--. 1 bob bob 0 сен 16 18:14 emptyfile
[bob@dasadova main]$
```

Рис. 2.18: Создаем файлы

6. В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы:(рис. 2.19).

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

Рис. 2.19: Устанавливаем бит идентификатора группы, а так же sticky-бит

7. В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4:(рис. 2.20).

Теперь вы должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main.(рис. 2.20).

```

[alice@dasadova ~]$ cd /data/main
[alice@dasadova main]$ touch alice3
[alice@dasadova main]$ touch alice4
[alice@dasadova main]$ ls -l
итого 0
-rw-r--r--. 1 alice main 0 сен 16 18:26 alice3
-rw-r--r--. 1 alice main 0 сен 16 18:26 alice4
-rw-r--r--. 1 bob   bob   0 сен 16 18:21 bob1
-rw-r--r--. 1 bob   bob   0 сен 16 18:21 bob2
-rw-r--r--. 1 bob   bob   0 сен 16 18:14 emptyfile
[alice@dasadova main]$

```

Рис. 2.20: Создаем файлы и проверяем их группы

8. В терминале под пользователем alice попробуйте удалить файлы, принадлежащие пользователю bob:(рис. 2.21).

```

[alice@dasadova main]$ rm -rf bob*
rm: невозможно удалить 'bob1': Операция не позволена
rm: невозможно удалить 'bob2': Операция не позволена
[alice@dasadova main]$

```

Рис. 2.21: Пробуем удалить файлы

Убедитесь, что sticky-bit предотвратит удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов. Обратите внимание: поскольку пользователь alice является владельцем каталога /data/main, то он может удалить все свои файлы в любом случае.

## 2.3 Управление расширенными разрешениями с использованием списков ACL

В этом упражнении продолжим работать в созданных ранее каталогах /data/main и /data/third. В предыдущих упражнениях для группы main были

установлены разрешения на каталог /data/main, а у группы third — на каталог /data/third.

Требуется установить для группы third разрешения на чтение в каталоге /data/main, а для группы main — разрешения на чтение в каталоге /data/third. Затем требуется установить права доступа по умолчанию, чтобы убедиться в правильности установки разрешений для новых элементов этих каталогов. Для этого будет использоваться пакет acl и команды setfacl (для установки прав) и getfacl (для просмотра установленных прав).

Кратко опишем синтаксис команды setfacl.

Установить разрешения для пользователя:

```
setfacl -m "u:user:permissions"
```

Установить разрешения для группы:

```
setfacl -m "g:group:permissions"
```

Наследование записи ACL родительского каталога:

```
setfacl -dm "entry"
```

Удаление записи ACL:

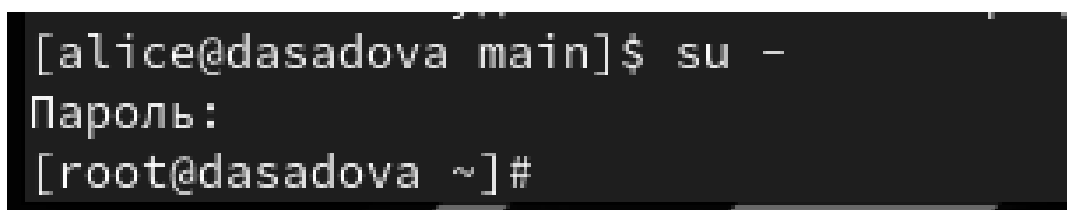
```
setfacl -x "entry"
```

Синтаксис команды getfacl:

```
getfacl
```

Применим команды setfacl и getfacl для выполнения поставленной задачи.

1. Откройте терминал с учётной записью root(рис. 2.22).



```
[alice@dasadova main]$ su -  
Пароль:  
[root@dasadova ~]#
```

Рис. 2.22: Переходим в учётную запись 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:(рис. 2.23).

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

Рис. 2.23: Устанавливаем права чтения

3. Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:(рис. 2.24),(рис. 2.25).

```
[root@dasadova ~]# 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@dasadova ~]#
```

Рис. 2.24: Используем команду getfacl для main

```
[root@dasadova ~]# 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@dasadova ~]#
```

Рис. 2.25: Используем команду getfacl для third

4. Создайте новый файл с именем newfile1 в каталоге /data/main:(рис. 2.26).

```
[root@dasadova ~]# ls -l /data/main/newfile1
-rw-r--r--. 1 root main 0 сен 16 18:32 /data/main/newfile1
[root@dasadova ~]#
```

Рис. 2.26: Создаем файл newfile1

Используйте `getfacl /data/main/newfile1` для проверки текущих назначений полномочий. Какие права доступа у этого файла?

Объясните, почему.

Права доступа у файла “-rw-r--r--” - это значит что владелец файла имеет права только на чтение и запись (rw), а группа и остальные пользователи — только на чтение (r)

Выполните аналогичные действия для каталога /data/third. Дайте пояснения.(рис. 2.27).

```
[root@dasadova ~]# ls -l /data/third/newfile2
-rw-r--r--. 1 root root 0 сен 16 18:33 /data/third/newfile2
[root@dasadova ~]#
```

Рис. 2.27: Создаем файл newfile2

5. Установите ACL по умолчанию для каталога /data/main:(рис. 2.28).

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

Рис. 2.28: Установили ACL для /data/main

6. Добавьте ACL по умолчанию для каталога /data/third:(рис. 2.29).

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

Рис. 2.29: Установили ACL для /data/third



7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main. Используйте `getfacl /data/main/newfile2` для проверки текущих назначений полномочий.(рис. 2.30).

```
[root@dasadova ~]# getfacl /data/main/newfile3
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile3
# owner: root
# group: main
user::rw-
group::rwx                #effective:rw-
group:main:rwx            #effective:rw-
group:third:rwx           #effective:rw-
mask::rw-
other::---
```

Рис. 2.30: Добавляем новый файл в main

Выполните аналогичные действия для каталога /data/third.(рис. 2.31).

```
[root@dasadova ~]# touch /data/third/newfile4
[root@dasadova ~]# getfacl /data/third/newfile4
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile4
# owner: root
# group: root
user::rw-
group::rwx                #effective:rw-
group:main:rwx            #effective:rw-
mask::rw-
other::---
```

Рис. 2.31: Добавляем новый файл в third

8. Для проверки полномочий группы third в каталоге /data/third войдите в другом терминале под учётной записью члена группы third:(рис. 2.32).

```
[root@dasadova ~]# su - carol
[carol@dasadova ~]$
```

Рис. 2.32: Переходим к учётной записи пользователя carol

Проверьте операции с файлами:(рис. 2.33).

```
[carol@dasadova ~]$ rm /data/main/newfile1
rm: удалить защищённый от записи пустой обычный файл '/data/main/newfile1'?
[carol@dasadova ~]$ rm /data/main/newfile3
rm: невозможно удалить '/data/main/newfile3': Отказано в доступе
[carol@dasadova ~]$
```

Рис. 2.33: Пытаемся удалить файлы из каталогов

Проверьте, возможно ли осуществить запись в файл:(рис. 2.34),(рис. 2.35).

```
[carol@dasadova ~]$ echo "Hello, world" >> /data/main/newfile1
-bash: /data/main/newfile1: Отказано в доступе
[carol@dasadova ~]$
```

Рис. 2.34: Пытаемся записать “Hello, world” в файл

```
[carol@dasadova ~]$ echo "Hello, world" >> /data/main/newfile3
[carol@dasadova ~]$ cat /data/main/newfile3
Hello, world
[carol@dasadova ~]$
```

Рис. 2.35: Пытаемся записать “Hello, world” в файл

Объясните результат произведённых действий.

В первом случае у нас отказ в доступе - это связано с правами доступа файла newfile1. Пользователь carol, который записан в каталоге third не имеет прав доступа редактировать файла newfile1 не своего каталога (каталога main).

Во втором случае получилось записать в файл newfile3, так как его прова доступа разрешают редактировать его другим пользователям (остальные пользователи)

## 3 Выводы

Получили навыки настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux. Больше узнали о правах доступа пользователей # Список литературы{.unnumbered}