

Лабораторная работа №3. Настройка прав доступа

Дисциплина: Основы администрирования операционных систем

Жукова Арина Александровна

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
3.1	Управление базовыми разрешениями	7
3.2	Управление специальными разрешениями	9
3.3	Управление расширенными разрешениями с использованием спис- ков ACL	12
4	Ответы на контрольные вопросы	17
5	Выводы	20
	Список литературы	21

Список иллюстраций

3.1	Создание каталогов	7
3.2	Работа команды ls -Al	7
3.3	Изменение владельцев каталогов	8
3.4	Установка разрешений	8
3.5	Создание файла	8
3.6	Права доступа	9
3.7	Переход в папку third	9
3.8	Создание файлов	10
3.9	Переход в каталог main	10
3.10	Удаление файлов	10
3.11	Создание двух файлов	11
3.12	Устанавливаем бит индентификатора и sticky-бит	11
3.13	Создание файлов alice3/4	11
3.14	Удаление файлов пользователя bob	12
3.15	Установка прав, проверка установки разрешений	13
3.16	Установка прав, проверка установки разрешений	14
3.17	Установка ACL для каталога main	15
3.18	Установка ACL для каталога third	15
3.19	Проверка полномочий группы third	16

Список таблиц

1 Цель работы

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

2 Задание

1. Прочитайте справочное описание `man` по командам `chgrp`, `chmod`, `getfacl`, `setfacl`.
2. Выполните действия по управлению базовыми разрешениями для групп пользователей (раздел 3.3.1).
3. Выполните действия по управлению специальными разрешениями для групп пользователей (раздел 3.3.2).
4. Выполните действия по управлению расширенными разрешениями с использованием списков ACL для групп пользователей (раздел 3.3.3).

3 Выполнение лабораторной работы

3.1 Управление базовыми разрешениями

1. Открываем терминал с учётной записью root. В корневом каталоге создаём каталоги /data/main и /data/third при помощи команд `mkdir -p /data/main /data/third` (рис. 3.1).

```
[aazhukoval@aazhukoval ~]$ su -  
Пароль:  
[root@aazhukoval ~]# mkdir -p /data/main /data/third
```

Рис. 3.1: Создание каталогов

2. Просматриваем, кто является владельцем созданных каталогов, используем команду `ls -Al /data` (рис. 3.2).

```
[root@aazhukoval data]# ls -Al /data  
итого 0  
drwxr-xr-x. 2 root root 6 сен 21 12:34 main  
drwxr-xr-x. 2 root root 6 сен 21 12:34 third  
[root@aazhukoval data]#
```

Рис. 3.2: Работа команды `ls -Al`

3. Изменяем владельцев этих каталогов с root на main и third, проверяем, кто теперь является владельцем этих каталогов (рис. 3.3).

```
[root@aazhukoval data]# chgrp main /data/main
[root@aazhukoval data]# chgrp third /data/third
[root@aazhukoval data]# ls -Al /data
итого 0
drwxr-xr-x. 2 root main  6 сен 21 12:34 main
drwxr-xr-x. 2 root third 6 сен 21 12:34 third
[root@aazhukoval data]#
```

Рис. 3.3: Изменение владельцев каталогов

4. Устанавливаем разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам. Проверяем установленные права доступа (рис. 3.4).

```
[root@aazhukoval data]# chmod 770 /data/main
[root@aazhukoval data]# chmod 770 /data/third
[root@aazhukoval data]# ls -Al /data
итого 0
drwxrwx---. 2 root main  6 сен 21 12:34 main
drwxrwx---. 2 root third 6 сен 21 12:34 third
[root@aazhukoval data]#
```

Рис. 3.4: Установка разрешений

5. Переходим под учётную запись пользователя bob, переходим в каталог main, создаём файл emptyfile (рис. 3.5).

```
[aazhukoval@aazhukoval ~]$ su - bob
Пароль:
[bob@aazhukoval ~]$ cd /data/main
[bob@aazhukoval main]$ touch emptyfile
[bob@aazhukoval main]$ ls
emptyfile
```

Рис. 3.5: Создание файла

Проверяем созданный файл (рис. 3.6).

```
[bob@aazhukoval main]$ ls -Al
итого 0
-rw-r--r--. 1 bob bob 0 сен 21 12:39 emptyfile
[bob@aazhukoval main]$
```

Рис. 3.6: Права доступа

Так как пользователь bob является владельцем каталога main, нам удалось перейти в этот каталог и создать в нём новый файл.

6. Под пользователем bob пробуем перейти в каталог /data/third и создать файл emptyfile в этом каталоге (рис. 3.7).

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

Рис. 3.7: Переход в папку third

Так как пользователь bob не является владельцем каталога third, нам не удалось перейти в этот каталог и создать в нём новый файл.

3.2 Управление специальными разрешениями

1. Открываем новый терминал под пользователем alice, переходим в каталог main. Создаём два файла, владельцем которых является alice, проверяем создание файлов (рис. 3.8).

```
[aazhukoval@aazhukoval ~]$ su - alice
Пароль:
[alice@aazhukoval ~]$ cd /data/main
[alice@aazhukoval main]$ touch alice1
[alice@aazhukoval main]$ touch alice2
[alice@aazhukoval main]$ ls
alice1  alice2  emptyfile
```

Рис. 3.8: Создание файлов

2. В другом терминале переходим под учётную запись пользователя bob, перейдите в каталог /data/main, в этом каталоге вводим `ls -l` (рис. 3.9).

```
[bob@aazhukoval ~]$ cd /data/main
[bob@aazhukoval main]$ ls -l
итого 0
-rw-r--r--. 1 alice alice 0 сен 21 12:43 alice1
-rw-r--r--. 1 alice alice 0 сен 21 12:43 alice2
-rw-r--r--. 1 bob  bob  0 сен 21 12:39 emptyfile
[bob@aazhukoval main]$
```

Рис. 3.9: Переход в каталог main

Удаляем файлы, принадлежащие пользователю alice, при помощи команды `rm -f alice*`, проверяем, что файлы удалены (рис. 3.10).

```
[bob@aazhukoval main]$ ls -l
итого 0
-rw-r--r--. 1 alice alice 0 сен 21 12:43 alice1
-rw-r--r--. 1 alice alice 0 сен 21 12:43 alice2
-rw-r--r--. 1 bob  bob  0 сен 21 12:39 emptyfile
[bob@aazhukoval main]$ rm -f alice*
[bob@aazhukoval main]$ ls -l
итого 0
-rw-r--r--. 1 bob bob 0 сен 21 12:39 emptyfile
[bob@aazhukoval main]$
```

Рис. 3.10: Удаление файлов

3. Создание двух файлов, которые принадлежат пользователю bob (рис. 3.11).

```
[bob@aazhukoval main]$ touch bob1
[bob@aazhukoval main]$ touch bob2
[bob@aazhukoval main]$ ls -l
итого 0
-rw-r--r--. 1 bob bob 0 сен 21 12:45 bob1
-rw-r--r--. 1 bob bob 0 сен 21 12:45 bob2
-rw-r--r--. 1 bob bob 0 сен 21 12:39 emptyfile
[bob@aazhukoval main]$
```

Рис. 3.11: Создание двух файлов

4. В терминале под пользователем root устанавливаем для каталога main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы, при помощи команды `chmod g+s,o+t /data/main` (рис. 3.12).

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

Рис. 3.12: Устанавливаем бит идентификатора и sticky-бит

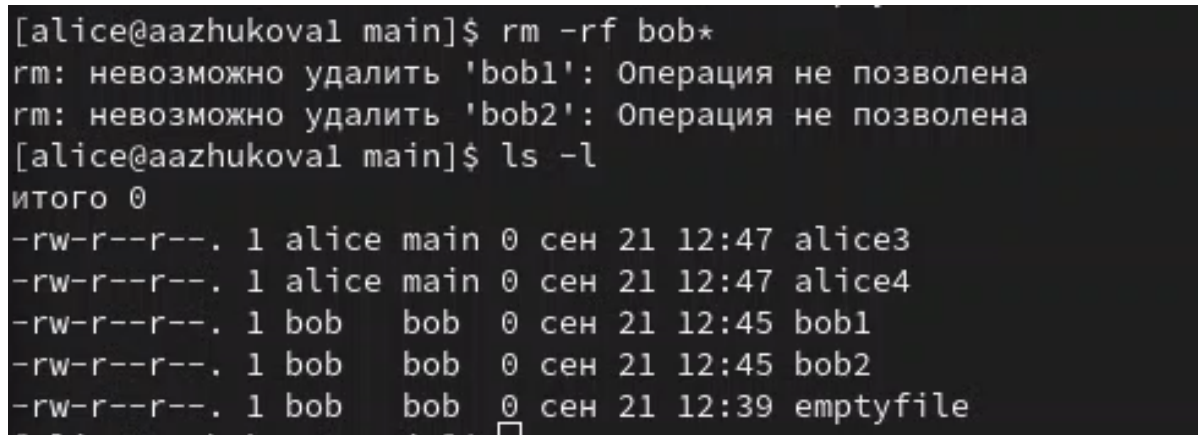
5. В терминале под пользователем alice создаём в каталоге main файлы alice3 и alice4, проверяем права доступа и владельцев файлов (рис. 3.13).

```
alice3 alice4 emptyfile
[alice@aazhukoval main]$ touch alice3
[alice@aazhukoval main]$ touch alice4
[alice@aazhukoval main]$ ls -l
итого 0
-rw-r--r--. 1 alice main 0 сен 21 12:47 alice3
-rw-r--r--. 1 alice main 0 сен 21 12:47 alice4
-rw-r--r--. 1 bob bob 0 сен 21 12:45 bob1
-rw-r--r--. 1 bob bob 0 сен 21 12:45 bob2
-rw-r--r--. 1 bob bob 0 сен 21 12:39 emptyfile
[alice@aazhukoval main]$
```

Рис. 3.13: Создание файлов alice3/4

Два созданных файла принадлежат группе main, которая является группой-владельцем каталога /data/main.

6. В терминале под пользователем alice удаляем файлы, принадлежащие пользователю bob командой `rm -rf bob*` (рис. 3.14).



```
[alice@aazhukoval main]$ rm -rf bob*
rm: невозможно удалить 'bob1': Операция не позволена
rm: невозможно удалить 'bob2': Операция не позволена
[alice@aazhukoval main]$ ls -l
итого 0
-rw-r--r--. 1 alice main 0 сен 21 12:47 alice3
-rw-r--r--. 1 alice main 0 сен 21 12:47 alice4
-rw-r--r--. 1 bob bob 0 сен 21 12:45 bob1
-rw-r--r--. 1 bob bob 0 сен 21 12:45 bob2
-rw-r--r--. 1 bob bob 0 сен 21 12:39 emptyfile
```

Рис. 3.14: Удаление файлов пользователя bob

sticky-bit предотвратил удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов.

3.3 Управление расширенными разрешениями с использованием списков ACL

1. Открываем терминал с учётной записью root. Устанавливаем права на чтение и выполнение в каталоге main для группы third и права на чтение и выполнение для группы main в каталоге third. Используем команду `getfacl`, чтобы убедиться в правильности установки разрешений (рис. 3.15).

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

Рис. 3.15: Установка прав, проверка установки разрешений

2. Создаём новый файл с именем newfile1 в каталоге main, используем getfacl /data/main/newfile1 для проверки текущих назначений полномочий, а также выполняем аналогичные действия для каталога /data/third (рис. 3.16).

```

[root@aazhukoval ~]# touch /data/main/newfile1
[root@aazhukoval ~]# 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@aazhukoval ~]# touch /data/third/newfile1
[root@aazhukoval ~]# 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--

```

Рис. 3.16: Установка прав, проверка установки разрешений

Каталог main: у пользователя есть права только на чтение и запись, у группы и других только чтение. Каталог third: у пользователя есть права только на чтение и запись, у группы и других только чтение.

3. Устанавливаем ACL по умолчанию для каталога main командой `setfacl -m d:g:third:rwX /data/main` и для каталога third `setfacl -m d:g:main:rwX /data/third`. Проверяем работу настроек, создав новый файл и используя команду `getfacl /data/main/newfile2` для проверки текущих назначений полномочий (рис. 3.17).

```

[root@aazhukoval ~]# setfacl -m d:g:third:rw- /data/main
[root@aazhukoval ~]# setfacl -m d:g:main:rw- /data/third
[root@aazhukoval ~]# touch /data/main/newfile2
[root@aazhukoval ~]# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root
# group: main
user::rw-
group::rw-                #effective:rw-
group:third:rw-           #effective:rw-
mask::rw-
other::---

```

Рис. 3.17: Установка ACL для каталога main

Выполняем аналогичные действия для каталога third (рис. 3.18).

```

getfacl /data/main/newfile2: getfacl: Permission denied
[root@aazhukoval ~]# touch /data/third/newfile2
[root@aazhukoval ~]# getfacl /data/third/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile2
# owner: root
# group: root
user::rw-
group::rw-                #effective:rw-
group:main:rw-            #effective:rw-
mask::rw-
other::---

```

Рис. 3.18: Установка ACL для каталога third

4. Для проверки полномочий группы third в каталоге third войдём в другом терминале под учётной записью пользователю carol. Проверяем операции с файлами, пробуя удалить файлы newfile1, newfile2 и проверяем, возможно ли осуществить запись в файл echo "Hello, world" >> /data/main/newfile1 и echo "Hello, world" >> /data/main/newfile2 (рис. 3.19).

```
getfacl /data/third/newfile2: getfacl: cannot open file: /data/third/newfile2: No such file or directory
[root@aazhukoval ~]# touch /data/third/newfile2
[root@aazhukoval ~]# 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::---
```

Рис. 3.19: Проверка полномочий группы third

Система не даёт удалить оба файлы, также мы проверили возможность осуществления записи в файл: в newfile1 записать не получилось, а вот в newfile2 всё получилось.

4 Ответы на контрольные вопросы

1. Чтобы установить владельца группы для файла: `chown :[group_name] [file_name]` Пример: `chown :developers report.txt`
2. Чтобы найти все файлы, принадлежащие конкретному пользователю: `find / -user [user_name]` пример: `find / -user carol`
3. Чтобы применить разрешения на чтение, запись и выполнение для всех файлов в каталоге `/data` для пользователей и владельцев групп, не устанавливая никаких прав для других: `chmod g+rw,u+rx /data/*` Эта команда устанавливает разрешения `rx` (чтение, запись, выполнение) для владельца и `rw` (чтение, запись) для группы для всех файлов в каталоге `/data`.
4. Чтобы добавить разрешение на выполнение для файла, который необходимо сделать исполняемым: `chmod +x [file_name]` Пример: `chmod +x script.sh`
5. Чтобы убедиться, что групповые разрешения для всех новых файлов, создаваемых в каталоге, будут присвоены владельцу группы этого каталога: `umask 002`. Эта команда устанавливает значение `umask` равным `002`, что означает, что групповые разрешения на запись будут отключены для всех новых файлов, создаваемых в каталоге.
6. Чтобы пользователи могли удалять только те файлы, владельцами которых они являются, или которые находятся в каталоге, владельцами которого они

являются: `setfacl -m u::rwx,d::rwx [file_name]` Эта команда устанавливает ACL для файла, предоставляя пользователю права на чтение, запись и выполнение для файла, если он является владельцем, или если он является владельцем каталога, в котором находится файл.

7. Чтобы добавить ACL, который предоставляет членам группы права доступа на чтение для всех существующих файлов в текущем каталоге: `setfacl -m g:[group_name]:r *` Эта команда устанавливает ACL для всех файлов в текущем каталоге, предоставляя членам группы `[group_name]` права на чтение.
8. Чтобы гарантировать, 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: `setfacl -m -d g:[group_name]:r *` Эта команда устанавливает ACL для всех файлов в текущем каталоге и во всех его подкаталогах, предоставляя членам группы `[group_name]` права на чтение. Параметр `-d` устанавливает ACL по умолчанию для всех файлов, созданных в этом каталоге в будущем.
9. Чтобы «другие» пользователи не получали никаких разрешений на новые файлы, установите значение `umask` равным `077`: `umask 077` Эта команда устанавливает значение `umask` равным `077`, что означает, что все разрешения для «других» пользователей будут отключены для всех новых файлов, создаваемых в каталоге.
10. Чтобы гарантировать, что никто не сможет удалить файл `myfile` случайно, нужно установить атрибут «только для чтения» (`read-only`) для этого файла:
`chmod -w myfile`
 - `chmod` — команда для изменения разрешений файлов.
 - `-w` — опция, удаляющая разрешение на запись для файла.

- myfile — имя файла, для которого нужно установить атрибут “только для чтения”.

5 Выводы

В ходе выполнения лабораторной работы были получены навыки настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.

Список литературы

1. Робачевский А., Немнюгин С., Стесик О. Операционная система UNIX. — 2-е изд. — БХВ-Петербург, 2010.
2. Колисниченко Д. Н. Самоучитель системного администратора Linux. — СПб. : БХВПетербург, 2011. — (Системный администратор).
3. Таненбаум Э., Бос Х. Современные операционные системы. — 4-е изд. — СПб. : Питер,
4. — (Классика Computer Science).
5. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016.
6. Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т. Хейн, Б. Уэйли, Д. Макни. — 5-е изд. — СПб. : ООО «Диалектика», 2020