

Отчёт по лабораторной работе №3

Дисциплина: Основы администрирования операционных систем

Верниковская Екатерина Андреевна

Содержание

1	Цель работы	6
2	Задание	7
3	Выполнение лабораторной работы	8
3.1	Справочное описание команд	8
3.2	Управление базовыми разрешениями	9
3.3	Управление специальными разрешениями	12
3.4	Управление расширенными разрешениями с использованием списков ACL	15
4	Контрольные вопросы + ответы	20
5	Выводы	22
6	Список литературы	23

Список иллюстраций

3.1	Команда <code>map</code>	8
3.2	Справка по команде <code>chgrp</code>	8
3.3	Справка по команде <code>chmod</code>	9
3.4	Справка по команде <code>getfacl</code>	9
3.5	Справка по команде <code>setfacl</code>	9
3.6	Учётная запись <code>root</code>	10
3.7	Создание каталогов <code>/data/main</code> и <code>/data/third</code>	10
3.8	Информация о каталогах <code>/data/main</code> и <code>/data/third</code> (1)	10
3.9	Изменение владельцев каталогов <code>/data/main</code> и <code>/data/third</code>	10
3.10	Информация о каталогах <code>/data/main</code> и <code>/data/third</code> (2)	10
3.11	Установление разрешений	11
3.12	Установленные права доступа	11
3.13	Учётная запись <code>bob</code>	11
3.14	Каталог <code>/data/main</code> в учётной записи <code>bob</code> и создание файла	11
3.15	Каталог <code>/data/third</code> в учётной записи <code>bob</code> и создание файла	12
3.16	Учётная запись <code>alice</code>	12
3.17	Переход в каталог <code>/data/main</code> под <code>alice</code>	12
3.18	Создание файлов <code>alice1</code> и <code>alice2</code>	12
3.19	Файлы, которые видит <code>bob</code>	13
3.20	Удаление файлов (1)	13
3.21	Создание файлов <code>bob1</code> и <code>bob2</code>	13
3.22	Установка бит идентификатора группы и <code>sticky</code> -бит для разделяе- мого (общего) каталога группы	14
3.23	Информация о файлах <code>alice3</code> и <code>alice4</code>	14
3.24	Удаление файлов (2)	14
3.25	Установка прав на чтение и выполнение в каталогах для групп	15
3.26	Проверка правильности установки разрешений в каталоге <code>main</code>	15
3.27	Проверка правильности установки разрешений в каталоге <code>third</code>	16
3.28	Создание <code>newfile1</code> в каталоге <code>/data/main</code>	16
3.29	Информация о файле <code>newfile1</code> в каталоге <code>/data/main</code>	16
3.30	Информация о файле <code>newfile1</code> в каталоге <code>/data/third</code>	17
3.31	Утановка ACL по умолчанию для каталога <code>/data/main</code>	17
3.32	Утановка ACL по умолчанию для каталога <code>/data/third</code>	17
3.33	Создание <code>newfile2</code> в каталоге <code>/data/main</code>	17
3.34	Информация о файле <code>newfile2</code> в каталоге <code>/data/main</code>	18
3.35	Создание <code>newfile2</code> в каталоге <code>/data/third</code>	18
3.36	Информация о файле <code>newfile2</code> в каталоге <code>/data/third</code>	18

3.37 Учётная запись carol	19
3.38 Проверка операции удаления	19
3.39 Проверка операции записи в файл	19

Список таблиц

1 Цель работы

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

2 Задание

1. Прочитать справочное описание man по нескольким командам.
2. Выполнить действия по управлению базовыми разрешениями для групп пользователей.
3. Выполнить действия по управлению специальными разрешениями для групп пользователей.
4. Выполнить действия по управлению расширенными разрешениями с использованием списков ACL для групп пользователей.

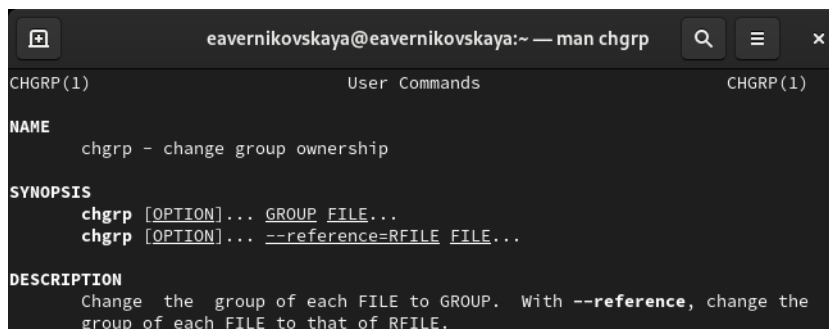
3 Выполнение лабораторной работы

3.1 Справочное описание команд

Открываем терминал и читаем справочное описание man по командам ls, whoami, id, groups, su, sudo, passwd, vi, visudo, useradd, usermod, userdel, groupadd, groupdel (рис. 3.1), (рис. 3.2), (рис. 3.3), (рис. 3.4), (рис. 3.5)

```
[eavernikovskaya@eavernikovskaya ~]$ man chgrp
[eavernikovskaya@eavernikovskaya ~]$ man chmod
[eavernikovskaya@eavernikovskaya ~]$ man getfacl
[eavernikovskaya@eavernikovskaya ~]$ man setfacl
[eavernikovskaya@eavernikovskaya ~]$
```

Рис. 3.1: Команда man



```
CHGRP(1) User Commands CHGRP(1)

NAME
  chgrp - change group ownership

SYNOPSIS
  chgrp [OPTION]... GROUP FILE...
  chgrp [OPTION]... --reference=RFILE FILE...

DESCRIPTION
  Change the group of each FILE to GROUP. With --reference, change the
  group of each FILE to that of RFILE.
```

Рис. 3.2: Справка по команде chgrp


```
eavernikovskaya@eavernikovskaya:~ — man chmod
CHMOD(1) User Commands CHMOD(1)

NAME
  chmod - change file mode bits

SYNOPSIS
  chmod [OPTION]... MODE[,MODE]... FILE...
  chmod [OPTION]... OCTAL-MODE FILE...
  chmod [OPTION]... --reference=RFILE FILE...

DESCRIPTION
  This manual page documents the GNU version of chmod. chmod changes the
```

Рис. 3.3: Справка по команде chmod

```
eavernikovskaya@eavernikovskaya:~ — man getfacl
GETFACL(1) Access Control Lists GETFACL(1)

NAME
  getfacl - get file access control lists

SYNOPSIS
  getfacl [-aceEsRLPtpndvh] file ...

  getfacl [-aceEsRLPtpndvh] -

DESCRIPTION
  For each file, getfacl displays the file name, owner, the group, and
```

Рис. 3.4: Справка по команде getfacl

```
eavernikovskaya@eavernikovskaya:~ — man setfacl
SETFACL(1) Access Control Lists SETFACL(1)

NAME
  setfacl - set file access control lists

SYNOPSIS
  setfacl [-bkndRLPvh] [{-m|-x} acl_spec] [{-M|-X} acl_file] file ...

  setfacl --restore=file

DESCRIPTION
  This utility sets Access Control Lists (ACLs) of files and directories.
```

Рис. 3.5: Справка по команде setfacl

3.2 Управление базовыми разрешениями

Открываем терминал с учётной записью root: *su* - (рис. 3.6)

```
[eavernikovskaya@eavernikovskaya ~]$ su -  
Password:  
[root@eavernikovskaya ~]#
```

Рис. 3.6: Учётная запись root

В корневом каталоге создаём каталоги /data/main и /data/third (рис. 3.7)

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

Рис. 3.7: Создание каталогов /data/main и /data/third

Смотрим, кто является владельцем этих каталогов. Владелец каталогов является суперпользователь root (рис. 3.8)

```
[root@eavernikovskaya ~]# ls -Al /data/  
total 0  
drwxr-xr-x. 2 root root 6 Sep 15 21:32 main  
drwxr-xr-x. 2 root root 6 Sep 15 21:32 third  
[root@eavernikovskaya ~]#
```

Рис. 3.8: Информация о каталогах /data/main и /data/third (1)

Далее меняем владельцев этих каталогов с root на main и third соответственно, с помощью команды *chgrp* (рис. 3.9)

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

Рис. 3.9: Изменение владельцев каталогов /data/main и /data/third

Проверяем, кто теперь является владельцем этих каталогов. (рис. 3.10)

```
[root@eavernikovskaya ~]# ls -Al /data/  
total 0  
drwxr-xr-x. 2 root main 6 Sep 15 21:32 main  
drwxr-xr-x. 2 root third 6 Sep 15 21:32 third  
[root@eavernikovskaya ~]#
```

Рис. 3.10: Информация о каталогах /data/main и /data/third (2)

Устанавливаем разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам (рис. 3.11)

```
[root@eavernikovskaya ~]# chmod 770 /data/main/  
[root@eavernikovskaya ~]# chmod 770 /data/third/  
[root@eavernikovskaya ~]#
```

Рис. 3.11: Установление разрешений

Далее проверяем установленные права доступа (рис. 3.12)

```
[root@eavernikovskaya ~]# ls -Al /data/  
total 0  
drwxrwx---. 2 root main  6 Sep 15 21:32 main  
drwxrwx---. 2 root third 6 Sep 15 21:32 third  
[root@eavernikovskaya ~]#
```

Рис. 3.12: Установленные права доступа

В другом терминале переходим под учётную запись пользователя bob: `su - bob` (рис. 3.13)

```
[eavernikovskaya@eavernikovskaya ~]$ su - bob  
Password:  
[bob@eavernikovskaya ~]$
```

Рис. 3.13: Учётная запись bob

Под пользователем bob пробуем перейти в каталог `/data/main` и создать файл `emptyfile` в этом каталоге. Так как пользователь bob является владельцем каталога main, нам удалось перейти в этот каталог и создать в нём новый файл (рис. 3.14)

```
[bob@eavernikovskaya ~]$ cd /data/main/  
[bob@eavernikovskaya main]$ touch emptyfile  
[bob@eavernikovskaya main]$ ls -Al  
total 0  
-rw-r--r--. 1 bob bob 0 Sep 15 21:41 emptyfile  
[bob@eavernikovskaya main]$
```

Рис. 3.14: Каталог `/data/main` в учётной записи bob и создание файла

Под пользователем bob пробуем перейти в каталог /data/third и создать файл emptyfile в этом каталоге. Так как пользователь bob не является владельцем каталога third, нам не удалось перейти в этот каталог и создать в нём новый файл (рис. 3.15)

```
[bob@eavernikovskaya main]$ cd /data/third/  
-bash: cd: /data/third/: Permission denied  
[bob@eavernikovskaya main]$
```

Рис. 3.15: Каталог /data/third в учётной записи bob и создание файла

3.3 Управление специальными разрешениями

Открываем новый терминал под пользователем alice (рис. 3.16)

```
[eavernikovskaya@eavernikovskaya ~]$ su - alice  
Password:  
[alice@eavernikovskaya ~]$
```

Рис. 3.16: Учётная запись alice

Переходим в каталог /data/main и создаём два файла, владельцем которых является alice (рис. 3.17), (рис. 3.18)

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

Рис. 3.17: Переход в каталог /data/main под alice

```
[alice@eavernikovskaya main]$ touch alice1  
[alice@eavernikovskaya main]$ touch alice2  
[alice@eavernikovskaya main]$
```

Рис. 3.18: Создание файлов alice1 и alice2

В другом терминале переходим под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice). Далее переходим в каталог /data/main и видим там два файла, созданные пользователем alice (рис. 3.19)

```
[bob@eavernikovskaya main]$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Sep 15 21:44 alice1
-rw-r--r--. 1 alice alice 0 Sep 15 21:44 alice2
-rw-r--r--. 1 bob  bob  0 Sep 15 21:41 emptyfile
[bob@eavernikovskaya main]$
```

Рис. 3.19: Файлы, которые видит bob

Попробуем удалить файлы, принадлежащие пользователю alice. Файлы успешно удалены (рис. 3.20)

```
[bob@eavernikovskaya main]$ rm -f alice*
[bob@eavernikovskaya main]$ ls
emptyfile
[bob@eavernikovskaya main]$
```

Рис. 3.20: Удаление файлов (1)

Создаём два файла, которые принадлежат пользователю bob (рис. 3.21)

```
[bob@eavernikovskaya main]$ touch bob1
[bob@eavernikovskaya main]$ touch bob2
[bob@eavernikovskaya main]$ ls -l
total 0
-rw-r--r--. 1 bob bob 0 Sep 15 21:47 bob1
-rw-r--r--. 1 bob bob 0 Sep 15 21:47 bob2
-rw-r--r--. 1 bob bob 0 Sep 15 21:41 emptyfile
[bob@eavernikovskaya main]$
```

Рис. 3.21: Создание файлов bob1 и bob2

В терминале под пользователем root устанавливаем для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы `chmod g+s,o+t /data/main` (рис. 3.22)

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

Рис. 3.22: Установка бит идентификатора группы и sticky-бит для разделяемого (общего) каталога группы

В терминале под пользователем alice создаём в каталоге /data/main файлы alice3 и alice4. Теперь мы видим, что два созданных нами файла принадлежат группе main, которая является группой-владельцем каталога /data/main (рис. 3.23)

```
[alice@eavernikovskaya main]$ touch alice3
[alice@eavernikovskaya main]$ touch alice4
[alice@eavernikovskaya main]$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Sep 15 21:51 alice3
-rw-r--r--. 1 alice main 0 Sep 15 21:51 alice4
-rw-r--r--. 1 bob   bob   0 Sep 15 21:47 bob1
-rw-r--r--. 1 bob   bob   0 Sep 15 21:47 bob2
-rw-r--r--. 1 bob   bob   0 Sep 15 21:41 emptyfile
[alice@eavernikovskaya main]$
```

Рис. 3.23: ИНформация о файлах alice3 и alice4

В терминале под пользователем alice пробуем удалить файлы, принадлежащие пользователю bob. Sticky-bit предотвратит удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов (operation not permitted)(рис. 3.24)

```
[alice@eavernikovskaya main]$ rm -rf bob*
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
[alice@eavernikovskaya main]$
```

Рис. 3.24: Удаление файлов (2)

3.4 Управление расширенными разрешениями с использованием списков ACL

Открываем терминал с учётной записью root и устанавливаем 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, используя *setfacl -m* (рис. 3.25)

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

Рис. 3.25: Установка прав на чтение и выполнение в каталогах для групп

Используем команду *getfacl*, чтобы убедиться в правильности установки разрешений (рис. 3.26), (рис. 3.27)

```
[root@eavernikovskaya ~]# 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. 3.26: Проверка правильности установки разрешений в каталоге main

```
[root@eavernikovskaya ~]# 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@eavernikovskaya ~]#
```

Рис. 3.27: Проверка правильности установки разрешений в каталоге third

Создаём новый файл с именем newfile1 в каталоге /data/main (рис. 3.28)

```
[root@eavernikovskaya ~]# cd /data/main/
[root@eavernikovskaya main]# touch newfile1
[root@eavernikovskaya main]#
```

Рис. 3.28: Создание newfile1 в каталоге /data/main

Используем `getfacl /data/main/newfile1` для проверки текущих назначений полномочий. У пользователя только чтение и запись, у группы и других только чтение. Работать с этим файлом пользователи не могут, потому что мы устанавливали права на чтение и выполнение именно для каталогов, а не для созданных в нём файлов (рис. 3.29)

```
[root@eavernikovskaya ~]# 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--
```

Рис. 3.29: Информация о файле newfile1 в каталоге /data/main

Выполняем аналогичные действия для каталога /data/third. Пояснения те же самые что и к прошлому пункту (рис. 3.30)


```
[root@eavernikovskaya ~]# touch /data/third/newfile1
[root@eavernikovskaya ~]# 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. 3.30: Информация о файле newfile1 в каталоге /data/third

Устанавливаем ACL по умолчанию для каталога /data/main, с помощью *setfacl -m d:g:third:rwX* (рис. 3.31)

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

Рис. 3.31: Установка ACL по умолчанию для каталога /data/main

Устанавливаем ACL по умолчанию для каталога /data/third (рис. 3.32)

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

Рис. 3.32: Установка ACL по умолчанию для каталога /data/third

Добавляем новый файл newfile2 в каталог /data/main и проверяем, что настройки ACL работают (рис. 3.33), (рис. 3.34)

```
[root@eavernikovskaya ~]# touch /data/main/newfile2
[root@eavernikovskaya ~]#
```

Рис. 3.33: Создание newfile2 в каталоге /data/main

```
[root@eavernikovskaya ~]# 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::---
```

Рис. 3.34: Информация о файле newfile2 в каталоге /data/main

Выполняем аналогичные действия для каталога /data/third (рис. 3.35), (рис. 3.36)

```
[root@eavernikovskaya ~]# touch /data/third/newfile2
[root@eavernikovskaya ~]#
```

Рис. 3.35: Создание newfile2 в каталоге /data/third

```
[root@eavernikovskaya ~]# 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. 3.36: Информация о файле newfile2 в каталоге /data/third

Для созданных файлов группы main возможны действия от пользователей группы third и наоборот

Далее заходим в другом терминале под учётной записью члена группы third - это carol (рис. 3.37)

```
[eavernikovskaya@eavernikovskaya ~]$ su - carol
Password:
[carol@eavernikovskaya ~]$
```

Рис. 3.37: Учётная запись carol

Далее проверяем операции с файлами newfile1 и newfile2. Пытаемся их удалить. Система не даёт нам этого сделать, так как удаление файлов это действие с каталогом, а к каталогу main у группы third нет полномочий (рис. 3.38)

```
[carol@eavernikovskaya ~]$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1'? y
rm: cannot remove '/data/main/newfile1': Permission denied
[carol@eavernikovskaya ~]$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
[carol@eavernikovskaya ~]$
```

Рис. 3.38: Проверка операции удаления

Далее пытаемся осуществить запись в файлы. Система не даёт осуществить запись в newfile1, но разрешает сделать это в файле newfile2, так как ранее мы установили определённые разрешения (рис. 3.39)

```
[carol@eavernikovskaya ~]$ echo "Hello< world" >> /data/main/newfile1
-bash: /data/main/newfile1: Permission denied
[carol@eavernikovskaya ~]$ echo "Hello< world" >> /data/main/newfile2
[carol@eavernikovskaya ~]$
```

Рис. 3.39: Проверка операции записи в файл

4 Контрольные вопросы + ответы

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

`chown bob:main /data/third/newfile`

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

`find ~ -user bob -print.`

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 770 /data` (скриншот есть в лабораторной работе).

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

`chmod +x file.`

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

`getfacl "имя каталога"` (скриншот есть в лабораторной работе).

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 g+s,o+t /data/main` (скриншот есть в лабораторной работе).

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

`setfacl -m g:group:r` (скриншот есть в лабораторной работе).

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 -dm g:group:r /dir.`

9. Какое значение `umask` нужно установить, чтобы «другие» пользователи не получали какие-либо разрешения на новые файлы? Приведите пример.

007

10. Какая команда гарантирует, что никто не сможет удалить файл `myfile` случайно?

`sudo chattr +i myfile.`

5 Выводы

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

6 Список литературы

1. Лабораторная работа №3 [Электронный ресурс] URL: <https://esystem.rudn.ru/pluginfile.php/permissions.pdf>