

Лабораторная работа №3

Основы администрирования операционных систем.

Бызова М.О.

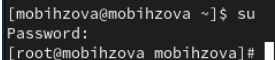
9 сентября 2024

Российский университет дружбы народов, Москва, Россия

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

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).

Открываем терминал с учётной записью root: su - (рис. 1).

A terminal window with a dark background. The prompt is [mobihzova@mobihzova ~]\$ and the command su has been entered. The next line shows Password: followed by a cursor. The final line shows the root prompt [root@mobihzova mobihzova]#.

```
[mobihzova@mobihzova ~]$ su
Password:
[root@mobihzova mobihzova]#
```

Рис. 1: Открытие терминала с учетной записью root

В корневом каталоге создаём каталоги /data/main и /data/third командой: `mkdir -p /data/main /data/third`. (рис. 2).

A terminal window with a dark background. The prompt is [root@mobihzova mobihzova]#. The command mkdir -p /data/main /data/third is entered. The prompt is repeated on the next line, followed by a white cursor block.

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

Рис. 2: Создание каталогов

Посмотрим, кто является владельцем этих каталогов. Для этого используем: `ls -Al /data`. Владелец каталогов является суперпользователь. (рис. 3).

```
[root@mobihzova mobihzova]# ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 Sep  9 14:37 main
drwxr-xr-x. 2 root root 6 Sep  9 14:37 third
[root@mobihzova mobihzova]#
```

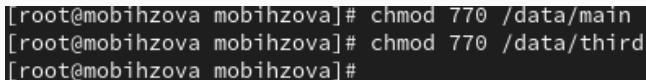
Рис. 3: Просмотр владельца каталогов

Прежде чем устанавливать разрешения, изменим владельцев этих каталогов с root на main и third соответственно: `chgrp main /data/main` и `chgrp third /data/third`. Теперь владельцем этих каталогов является main и third. (рис. 4).

```
[root@mobihzova mobihzova]# chgrp main /data/main
[root@mobihzova mobihzova]# chgrp third /data/third
```

Рис. 4: Изменение владельца каталогов

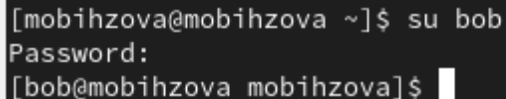
Далее установим разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам: `chmod 770 /data/main` и `chmod 770 /data/third`. После этого проверим права доступа. (рис. 5).

A terminal window with a black background and white text. It shows three lines of commands being executed by the root user on a system named mobihzova. The first two lines are 'chmod 770 /data/main' and 'chmod 770 /data/third', both of which have been executed successfully. The third line is a prompt for a new command.

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

Рис. 5: Установка разрешений

В другом терминале перейдём под учётную запись пользователя bob: `su - bob` (рис. 6).

A terminal window with a dark background and light gray text. The first line shows the prompt [mobihzova@mobihzova ~]\$ followed by the command su bob. The second line shows the prompt Password: followed by a white cursor. The third line shows the prompt [bob@mobihzova mobihzova]\$ followed by a white cursor.

```
[mobihzova@mobihzova ~]$ su bob
Password:
[bob@mobihzova mobihzova]$
```

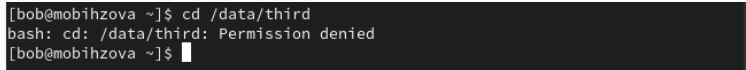
Рис. 6: Смена пользователя

Под пользователем bob попробуем перейти в каталог /data/main и создать файл emptyfile в этом каталоге: cd /data/main и touch emptyfile. Так как пользователь bob является владельцем каталога main, нам удалось перейти в этот каталог и создать в нём новый файл. (рис. 7).

```
[bob@mobihzova main]$ touch emptyfile
[bob@mobihzova main]$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Sep  9 14:40 emptyfile
[bob@mobihzova main]$
```

Рис. 7: Создание файла в каталоге

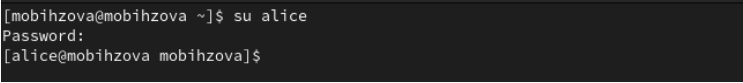
Теперь под пользователем bob попробуем перейти в каталог /data/third и создать файл emptyfile в этом каталоге. Так как пользователь bob не является владельцем каталога third, нам не удалось перейти в этот каталог и создать в нём новый файл (рис. 8).



```
[bob@mobihzova ~]$ cd /data/third
bash: cd: /data/third: Permission denied
[bob@mobihzova ~]$
```

Рис. 8: Создание файла в каталоге

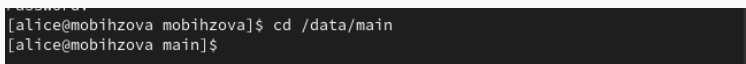
Откроем новый терминал под пользователем alice: `su - alice` (рис. 9).

A terminal window with a dark background. The first line shows the prompt [mobihzova@mobihzova ~]\$ followed by the command su alice. The second line shows the prompt Password: with no visible input. The third line shows the prompt [alice@mobihzova mobihzova]\$ indicating a successful switch to the alice user.

```
[mobihzova@mobihzova ~]$ su alice
Password:
[alice@mobihzova mobihzova]$
```

Рис. 9: Смена пользователя


Перейдём в каталог /data/main: `cd /data/main` (рис. 10).

A terminal window with a dark background. The prompt is [alice@mobihzova mobihzova]\$. The command cd /data/main is entered. The next line shows the prompt has changed to [alice@mobihzova main]\$.

```
[alice@mobihzova mobihzova]$ cd /data/main  
[alice@mobihzova main]$
```

Рис. 10: Переход в каталог


В нём создадим два файла, владельцем которых является alice: touch alice1 и touch alice2 (рис. 11).

A terminal window with a dark background and light-colored text. It shows three lines of text: the first line is the command 'touch alice1', the second line is the command 'touch alice2', and the third line is the prompt '[alice@mobihzova main]\$', which is partially cut off at the bottom.

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

Рис. 11: Создание файлов в каталоге

В другом терминале, под учётной записью пользователя bob (пользователь bob является членом группы main, как и alice) (рис. 12).

A terminal window with a dark background. The first line shows the prompt [mobihzova@mobihzova ~]\$ followed by the command su bob. The second line shows the prompt Password: followed by a single character (likely 'b') and a cursor. The third line shows the prompt [bob@mobihzova mobihzova]\$ followed by a cursor.

```
[mobihzova@mobihzova ~]$ su bob
Password:
[bob@mobihzova mobihzova]$
```

Рис. 12: Смена пользователя

Выполнение лабораторной работы

Перейдём в каталог /data/main: `cd /data/main` (данный каталог уже был открыт в нашем терминале) и в этом каталоге введём: `ls`. Мы увидим два файла, созданные пользователем alice. Теперь попробуем удалить файлы, принадлежащие пользователю alice командой: `rm -f alice*`. Убедимся, что файлы будут удалены пользователем bob (рис. 13).

```
[bob@mobihzova mobihzova]$ cd /data/main
[bob@mobihzova main]$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Sep  9 14:43 alice1
-rw-r--r--. 1 alice alice 0 Sep  9 14:43 alice2
-rw-r--r--. 1 bob  bob  0 Sep  9 14:40 emptyfile
[bob@mobihzova main]$ rm -f alice*
[bob@mobihzova main]$ ls -l
total 0
-rw-r--r--. 1 bob  bob  0 Sep  9 14:40 emptyfile
[bob@mobihzova main]$
```

Рис. 13: Удаление файлов пользователем bob

После проверки командой `ls` создадим два файла, которые принадлежат пользователю `bob`: `touch bob1` и `touch bob2` (рис. 14).

```
[bob@mobihzova main]$ touch bob1  
[bob@mobihzova main]$ touch bob2  
[bob@mobihzova main]$
```

Рис. 14: Создание файлов

В терминале под пользователем root установим для каталога /data/main бит идентификатор группы, а также sticky-бит для разделяемого (общего) каталога группы: `chmod g+s,o+t /data/main` (рис. 15).

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

Рис. 15: Установка бит идентификатора группы, а также sticky-бита для разделяемого (общего) каталога группы

Выполнение лабораторной работы

Переходим в терминал под пользователем alice и создаём в каталоге /data/main файлы alice3 и alice4: touch alice3 и touch alice4. Теперь мы должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main: ls и ls -Al /data (рис. 16).

```
[alice@mobihzova main]$ touch alice3
[alice@mobihzova main]$ touch alice4
[alice@mobihzova main]$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Sep  9 14:47 alice3
-rw-r--r--. 1 alice main 0 Sep  9 14:47 alice4
-rw-r--r--. 1 bob   bob   0 Sep  9 14:45 bob1
-rw-r--r--. 1 bob   bob   0 Sep  9 14:45 bob2
-rw-r--r--. 1 bob   bob   0 Sep  9 14:40 emptyfile
[alice@mobihzova main]$
```

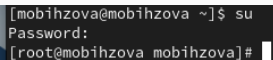
Рис. 16: Создание файлов в каталоге

В этом же терминале попробуем удалить файлы, принадлежащие пользователю bob: `rm -rf bob*`. Убедимся, что sticky-bit предотвратит удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов (Operation not permitted) (рис. 17).

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

Рис. 17: Удаление файлов пользователем alice

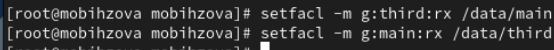
Откроем терминал с учётной записью root (рис. 18).

A terminal window with a dark background. The first line shows the prompt [mobihzova@mobihzova ~]\$ followed by the command su. The second line shows the prompt Password: with no visible input. The third line shows the new prompt [root@mobihzova mobihzova]# with a white cursor block.

```
[mobihzova@mobihzova ~]$ su
Password:
[root@mobihzova mobihzova]#
```

Рис. 18: Смена пользователя

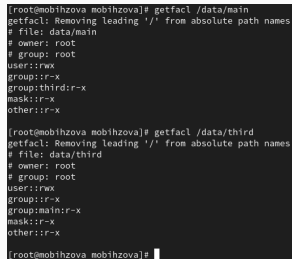
Установим права на чтение и выполнение в каталоге /data/main для группы third и права на чтение и выполнение для группы main в каталоге /data/third: setfacl -m g:third:rx /data/main и setfacl -m g:main:rx /data/third (рис. 19).



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

Рис. 19: Установка прав

Теперь используем команду `getfacl`, чтобы убедиться в правильности установки разрешений: `getfacl /data/main` и `getfacl /data/third` (рис. 20).



```
[root@mobihzova mobihzova]# getfacl /data/main
getfacl: Removing leading '/' from absolute path names
# file: data/main
# owner: root
# group: root
user::rwx
group::r-x
group:third:r-x
mask::r-x
other::r-x

[root@mobihzova mobihzova]# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: root
user::rwx
group::r-x
group:main:r-x
mask::r-x
other::r-x

[root@mobihzova mobihzova]#
```

Рис. 20: Проверка правильности установки разрешений

Выполнение лабораторной работы

Далее создадим новый файл с именем newfile1 в каталоге /data/main: touch /data/main/newfile1. Используем getfacl /data/main/newfile1 для проверки текущих назначений полномочий. У пользователя только чтение и запись, у группы и других только чтение (рис. 21).

```
[root@mobihzova mobihzova]# touch /data/main/newfile1
[root@mobihzova mobihzova]# getfacl /data/main/newfile1
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile1
# owner: root
# group: root
user::rw-
group::r--
other::r--
```

Рис. 21: Создание нового файла и проверка текущих назначенных полномочий

Выполним аналогичные действия для каталога /data/third. Видим, что ситуация аналогичная (рис. 22).

```
[root@mobihzova mobihzova]# touch /data/third/newfile1
[root@mobihzova mobihzova]# 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. 22: Создание нового файла и проверка текущих назначенных полномочий

Установим ACL по умолчанию для каталога /data/main: setfacl -md:g:third:rwx /data/main и для каталога /data/third: setfacl -m d:g:main:rwx /data/third. (рис. 23, рис. 24).

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

Рис. 23: Установка ACL по умолчанию

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

Рис. 24: Установка ACL по умолчанию

Выполнение лабораторной работы

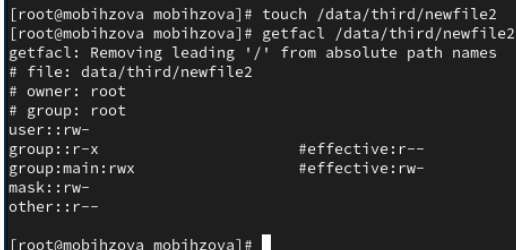
Убедимся, что настройки ACL работают, добавив новый файл в каталог /data/main: touch /data/main/newfile2. Используем getfacl /data/main/newfile2 для проверки текущих назначений полномочий. (рис. 25).

```
[root@mobihzova mobihzova]# touch /data/main/newfile2
[root@mobihzova mobihzova]# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root
# group: root
user::rw-
group::r-x                               #effective:r--
group:third:rw-                          #effective:rw-
mask::rw-
other::r--

[root@mobihzova mobihzova]#
```

Рис. 25: Создание нового файла и проверка текущих назначенных полномочий

Выполним аналогичные действия для каталога /data/third (рис. 26).

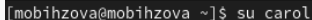
A terminal window with a dark background and light-colored text. The prompt is [root@mobihzova mobihzova]. The first command is touch /data/third/newfile2. The second command is getfacl /data/third/newfile2. The output shows the removal of the leading '/' from the absolute path, followed by file details: file: data/third/newfile2, owner: root, group: root, and permissions: user::rw-, group::r-x, group:main:rw-, mask::rw-, other::r--. There are also #effective:rw- entries for group and mask. The prompt returns to [root@mobihzova mobihzova] with a cursor.

```
[root@mobihzova mobihzova]# touch /data/third/newfile2
[root@mobihzova mobihzova]# getfacl /data/third/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile2
# owner: root
# group: root
user::rw-
group::r-x                               #effective:rw-
group:main:rw-                           #effective:rw-
mask::rw-
other::r--

[root@mobihzova mobihzova]#
```

Рис. 26: Создание нового файла и проверка текущих назначенных полномочий

Для проверки полномочий группы third в каталоге /data/third войдём в другом терминале под учётной записью члена группы third: su – carol (рис. 27).

A terminal window with a dark background. The prompt is [mobihzova@mobihzova ~]\$ and the command being entered is su carol.

```
[mobihzova@mobihzova ~]$ su carol
```

Рис. 27: Смена пользователя

Проверим операции с файлами: `rm /data/main/newfile1` и `rm /data/main/newfile2`. Система не даёт удалить данные файлы (рис. 28).

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

Рис. 28: Удаление файлов пользователем carol

Теперь проверим, возможно ли осуществить запись в файл. В файл newfile1 запись осуществить не получилось, а вот в newfile2 всё выполнилось (рис. 29).

```
[carol@mobihzova mobihzova]$ echo "Hello, world" >> /data/main/newfile1
bash: /data/main/newfile1: Permission denied
[carol@mobihzova mobihzova]$ echo "Hello, world" >> /data/main/newfile2
[carol@mobihzova mobihzova]$ cat /data/main/newfile2
Hello, world
[carol@mobihzova mobihzova]$
```

Рис. 29: Запись в файл пользователем carol

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

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. : БХВ-Петербург, 2011. — (Системный администратор).
3. Таненбаум Э., Бос Х. Современные операционные системы. — 4-е изд. — СПб. : Питер, 2015. — (Классика Computer Science).
4. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016.
5. Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т.Хейн, Б. Уэйли, Д. Макни. — 5-е изд. — СПб. : ООО «Диалектика», 2020.