

Отчёт о лабораторной работе

Лабораторная работа 3

Баранов Никита Дмитриевич

Содержание

1. Цель работы

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

2. Задание

Выполнить задания, прописанные в файле.

3. Выполнение лабораторной работы

Откройте терминал с учётной записью root. В корневом каталоге создайте каталоги /data/main и /data/third. Посмотрите, кто является владельцем этих каталогов. Прежде чем устанавливать разрешения, измените владельцев этих каталогов с root на main и third соответственно. Посмотрите, кто теперь является владельцем этих каталогов. 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. [fig:001?]).

```
Activities Terminal Sep 5 17:56 en
root@ndbaranov:~
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# mkdir -p /data/main
[root@ndbaranov ~]# ls
anaconda-ks.cfg
[root@ndbaranov ~]# mkdir -p /data/main /data/third
[root@ndbaranov ~]# ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 Sep  5 17:53 main
drwxr-xr-x. 2 root root 6 Sep  5 17:54 third
[root@ndbaranov ~]# chgrp main /data/main
[root@ndbaranov ~]# chgrp third /data/third
[root@ndbaranov ~]# ls -Al /data
total 0
drwxr-xr-x. 2 root main  6 Sep  5 17:53 main
drwxr-xr-x. 2 root third 6 Sep  5 17:54 third
[root@ndbaranov ~]# chmod 770 /data/main
[root@ndbaranov ~]# chmod 770 /data/third
[root@ndbaranov ~]# ls -Al /data
total 0
drwxrwx---. 2 root main  6 Sep  5 17:53 main
drwxrwx---. 2 root third 6 Sep  5 17:54 third
[root@ndbaranov ~]#
```

Выполняем все перечисленные действия

В другом терминале перейдите под учётную запись пользователя bob. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге. Под пользователем bob попробуйте перейти в каталог /data/third и создать файл emptyfile в этом каталоге(рис. [fig:002?]).

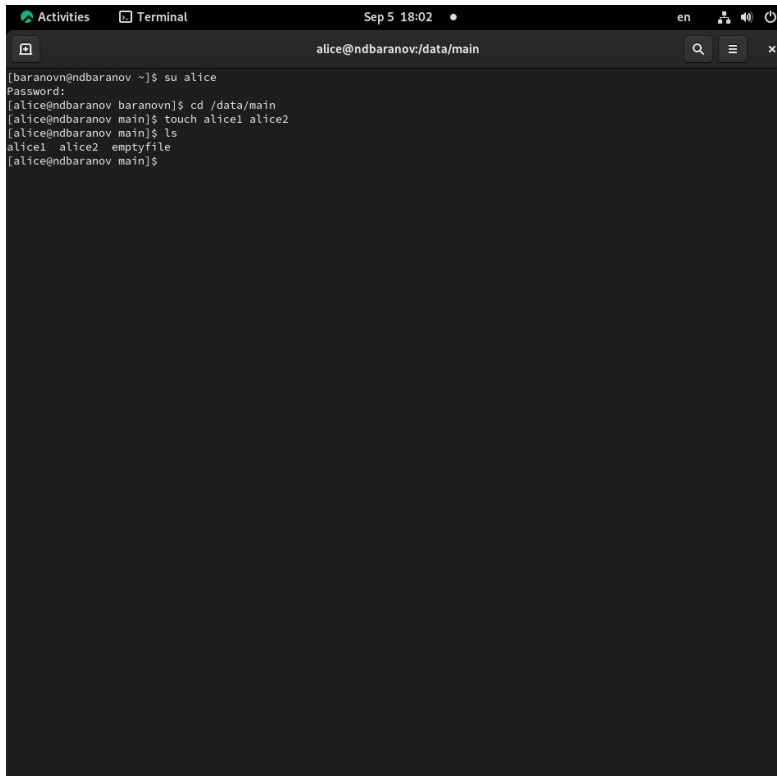
```
Activities Terminal Sep 5 18:00 en
bob@ndbaranov:~
[baranov@ndbaranov ~]$ su - bob
Password:
su: Authentication failure
[baranov@ndbaranov ~]$ su - bob
Password:
su: Authentication failure
[baranov@ndbaranov ~]$ sudo useradd bob
[sudo] password for baranov:
useradd: user 'bob' already exists
[baranov@ndbaranov ~]$ su - bob
Password:
su: Authentication failure
[baranov@ndbaranov ~]$ su - bob
Password:
su: Authentication failure
[baranov@ndbaranov ~]$ id bob
uid=1003(bob) gid=1003(bob) groups=1003(bob),1004(main)
[baranov@ndbaranov ~]$ sudo passwd bob
Changing password for user bob.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[baranov@ndbaranov ~]$ su - bob
Password:
[bob@ndbaranov ~]$ cd /data/main
[bob@ndbaranov main]$ touch emptyfile
[bob@ndbaranov main]$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Sep  5 17:59 emptyfile
[bob@ndbaranov main]$ cd /data/third
-bash: cd: /data/third: Permission denied
[bob@ndbaranov main]$ ls
emptyfile
[bob@ndbaranov main]$ cd
[bob@ndbaranov ~]$ cd /data/third
-bash: cd: /data/third: Permission denied
[bob@ndbaranov ~]$
```

Выполняем все перечисленные действия

Пользователь bob успешно перешёл в каталог /data/main и создал там файл emptyfile, так как он является членом группы main (которая указана в выводе команды id bob: groups=1003(bob),1004(main)). Каталог /data/main имеет права доступа 770 для владельца (root) и группы main, что позволяет участникам группы main читать, писать и исполнять каталог. Поэтому bob, как член группы main, имеет полные права на запись в этот каталог.

Пользователь bob не смог перейти в каталог /data/third или создать в нём файл, так как он не является членом группы third. Каталог /data/third имеет права доступа 770, что разрешает доступ только владельцу (root) и группе third. Bob не входит в группу third (его группы: bob и main), поэтому ему запрещён любой доступ к каталогу, что приводит к ошибке “Permission denied” при попытке выполнения команд cd или touch.

Откройте новый терминал под пользователем alice. Перейдите в каталог /data/main. Создайте два файла, владельцем которых является alice(рис. [fig:003?]).



```
[baranov@ndbaranov ~]$ su alice
Password:
[alice@ndbaranov baranov]$ cd /data/main
[alice@ndbaranov main]$ touch alice1 alice2
[alice@ndbaranov main]$ ls
alice1 alice2 emptyfile
[alice@ndbaranov main]$
```

Создаем файлы `alice1,2`

. В другом терминале перейдите под учётную запись пользователя bob. Перейдите в каталог `/data/main`. И в этом каталоге введите `ls -l`. Попробуйте удалить файлы, принадлежащие пользователю alice. Создайте два файла, которые принадлежат пользователю bob (рис. [fig:004?]).

```
Activities Terminal Sep 5 18:05 en
bob@ndbaranov:/data/main

[baranov@ndbaranov ~]$ su bob
Password:
[bob@ndbaranov baranov]$ exit
exit
[baranov@ndbaranov ~]$ su - bob
Password:
[bob@ndbaranov ~]$ ls
[bob@ndbaranov ~]$ cd /data/main
[bob@ndbaranov main]$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Sep  5 18:01 alice1
-rw-r--r--. 1 alice alice 0 Sep  5 18:01 alice2
-rw-r--r--. 1 bob  bob  0 Sep  5 17:59 emptyfile
[bob@ndbaranov main]$ rm -f alice*
[bob@ndbaranov main]$ ls
emptyfile
[bob@ndbaranov main]$ ls -l
total 0
-rw-r--r--. 1 bob bob 0 Sep  5 17:59 emptyfile
[bob@ndbaranov main]$ touch bob1 bob2
[bob@ndbaranov main]$ ls
bob1 bob2 emptyfile
[bob@ndbaranov main]$
```

Выполняем все перечисленные действия

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

```
root@ndbaranov:~

[baranov@ndbaranov ~]$ su
Password:
su: Authentication failure
[baranov@ndbaranov ~]$
[baranov@ndbaranov ~]$
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# chmod g+s,o+t /data/main
[root@ndbaranov ~]#
```

Устанавливаем бит идентификатора группы

В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4. В терминале под пользователем alice попробуйте удалить файлы, принадлежащие пользователю bob (рис. [fig:005?]).

```
Activities Terminal Sep 5 18:07 en
alice@ndbaranov:/data/main
[baranov@ndbaranov ~]$ su alice
Password:
[alice@ndbaranov baranov]$ cd /data/main
[alice@ndbaranov main]$ touch alice1 alice2
[alice@ndbaranov main]$ ls
alice1 alice2 emptyfile
[alice@ndbaranov main]$ touch alice3 alice4
[alice@ndbaranov main]$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Sep  5 18:06 alice3
-rw-r--r--. 1 alice main 0 Sep  5 18:06 alice4
-rw-r--r--. 1 bob  bob  0 Sep  5 18:05 bob1
-rw-r--r--. 1 bob  bob  0 Sep  5 18:05 bob2
-rw-r--r--. 1 bob  bob  0 Sep  5 17:59 emptyfile
[alice@ndbaranov main]$ rm -rf bob*
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
[alice@ndbaranov main]$
```

Создаем файлы и пытаемся удалить файлы боба

Откройте терминал с учётной записью root. 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. Используйте команду `getfacl`, чтобы убедиться в правильности установки разрешений. Создайте новый файл с именем `newfile1` в каталоге /data/main. Используйте `getfacl` для проверки текущих назначений полномочий. Выполните аналогичные действия для каталога /data/third. Установите ACL по умолчанию для каталога /data/main. Добавьте ACL по умолчанию для каталога /data/third. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main. Используйте `getfacl` для проверки текущих назначений полномочий. Выполните аналогичные действия для каталога /data/third (рис. [fig:006?])(рис. [fig:007?]).

```
Activities Terminal Sep 5 18:17 en
root@ndbaranov:~

[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# setfacl -m g:third:rx /data/main
[root@ndbaranov ~]# setfacl -m g:main:rx /data/third
[root@ndbaranov ~]# 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@ndbaranov ~]# 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@ndbaranov ~]# touch /data/main/newfile1
[root@ndbaranov ~]# 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@ndbaranov ~]# touch /data/third/newfile1
[root@ndbaranov ~]# 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@ndbaranov ~]# getfacl /data/third/newfile1
getfacl: Removing leading '/' from absolute path names
```

Выполняем все действия

```
Activities Terminal Sep 5 18:17 en
root@ndbaranov:~

other::r--

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

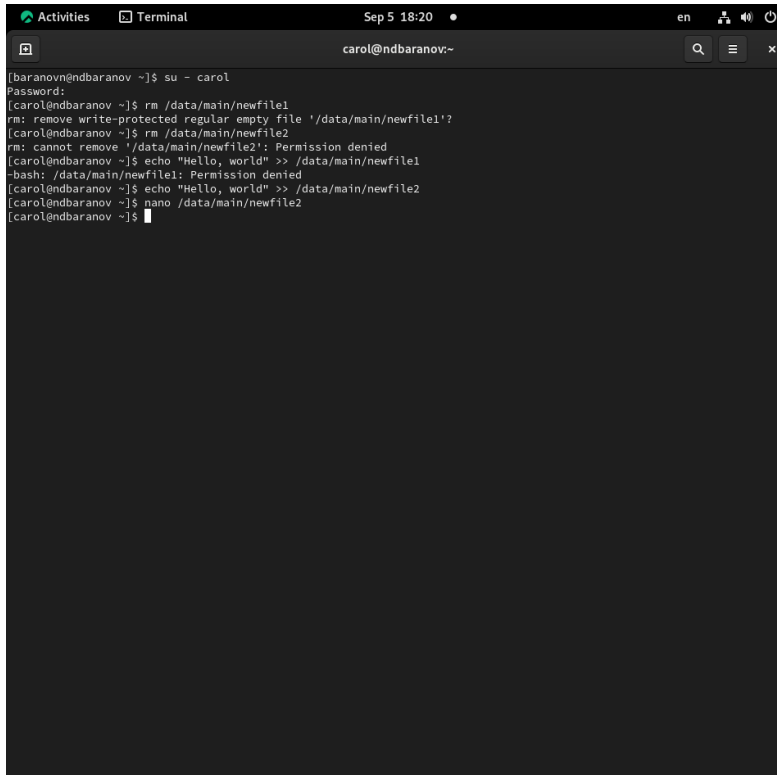
[root@ndbaranov ~]# setfacl -m d:g:third:rwx /data/main
[root@ndbaranov ~]# setfacl -m d:g:main:rwx /data/third
[root@ndbaranov ~]# touch /data/main/newfile2
[root@ndbaranov ~]# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root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

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

[root@ndbaranov ~]#
```

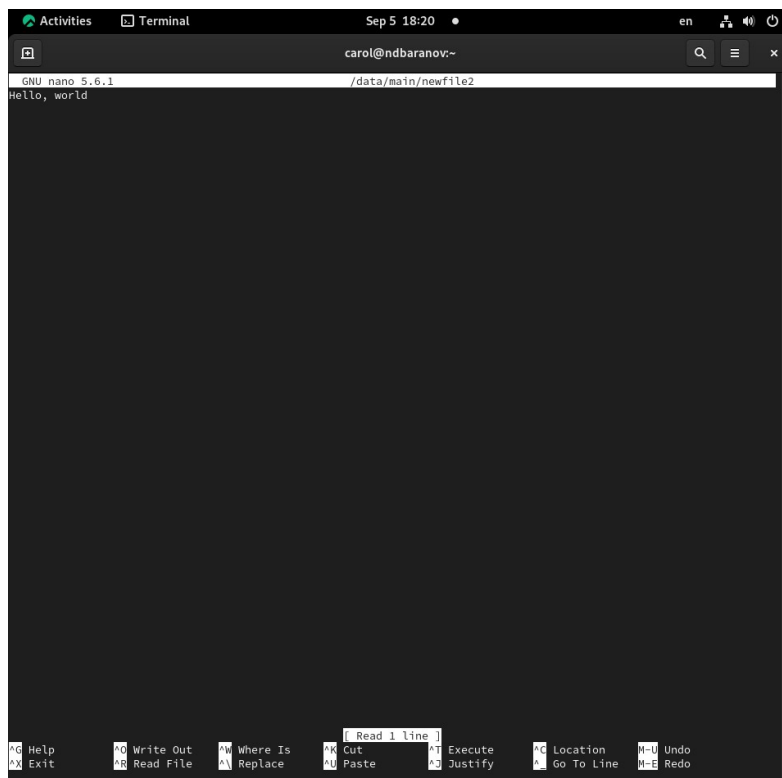
Выполняем все действия

Для проверки полномочий группы third в каталоге /data/third войдите в другом терминале под учётной записью члена группы third. Проверьте операции с файлами. Проверьте, возможно ли осуществить запись в файл (рис. [fig:008?]) (рис. [fig:009?]).



```
Activities Terminal Sep 5 18:20 en
carol@ndbaranov:~
[baranov@ndbaranov ~]$ su - carol
Password:
[carol@ndbaranov ~]$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1'?
[carol@ndbaranov ~]$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
[carol@ndbaranov ~]$ echo "Hello, world" >> /data/main/newfile1
-bash: /data/main/newfile1: Permission denied
[carol@ndbaranov ~]$ echo "Hello, world" >> /data/main/newfile2
[carol@ndbaranov ~]$ nano /data/main/newfile2
[carol@ndbaranov ~]$
```

Заходим под carol и проверяем операции с файлами



```
Activities Terminal Sep 5 18:20 en
carol@ndbaranov:~
GNU nano 5.6.1 /data/main/newfile2
Hello, world

Ctrl+G Help      Ctrl+O Write Out  Ctrl+W Where Is   Ctrl+K Cut        Ctrl+T Execute    Ctrl+Q Location   Ctrl+U Undo
Ctrl+X Exit      Ctrl+R Read File  Ctrl+A Replace    Ctrl+J Paste      Ctrl+_ Justify    Ctrl+G Go To Line Ctrl+B Redo
```

Мы смогли записать изменения в файл

4. Выводы

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