Лабораторная работа №3

Настройка прав доступа

Перфилов Александр Константинович | Группа НПИбд-03-24

Российский университет дружбы народов, Москва, Россия

20 сентября 2025

Раздел 1

Информация

Докладчик

- Перфилов Александр Константинович
- Группа НПИбд-03-24
- Российский университет дружбы народов
- https://github.com/AlexanderPErfilovKonstantinivich?tab=repositories

Раздел 2

Вводная часть

Объект и предмет исследования

- Настройка прав доступа для групп пользователей в Linux

Цель работы

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

Раздел 3

Ход лабораторной работы

Создание и просмотр файлов

- Создадим каталоги /data/main и /data/third под учетной записью root. Просмотрим информацию о владельце

```
akpperfilov@akpperfilov:~$ su -
Пароль:
Последний вход в систему: Пт сен 19 16:57:05 MSK 2025 на pts/0
root@akpperfilov:~# mkdir -p /data/main /data/third
root@akpperfilov:~# ls -Al /data
итого 0
drwxrwx---. 2 root root 6 сен 19 16:49 main
drwxrwx---. 2 root root 6 сен 19 16:49 third
root@akpperfilov:~#
```

```
root@akpperfilov:~# chgrp main /data/main
root@akpperfilov:~# chgrp third /data/third
root@akpperfilov:~# ls -Al /data
итого 0
drwxrwx---. 2 root main  6 сен 19 16:49 main
drwxrwx---. 2 root third 6 сен 19 16:49 third
```

Измнение владельцев каталогов

- Изменим владельцев этих каталогов с root на main и third. Просмотрим информацию о владельце

```
root@akpperfilov:~# chgrp main /data/main
root@akpperfilov:~# chgrp third /data/third
root@akpperfilov:~# ls -Al /data
итого 0
drwxrwx---. 2 root main  6 сен 19 16:49 main
drwxrwx---. 2 root third 6 сен 19 16:49 third
```

Измнение прав доступа к файлам

- Установим права на запись для владельцев каталогов, запретив доступ остальным. Проверим установленные права доступа

```
root@akpperfilov:~# chmod 770 /data/main
root@akpperfilov:~# chmod 770 /data/third
root@akpperfilov:~# ls -Al /data
итого 0
drwxrwx---. 2 root main  6 сен 19 16:49 main
drwxrwx---. 2 root third 6 сен 19 16:49 third
```

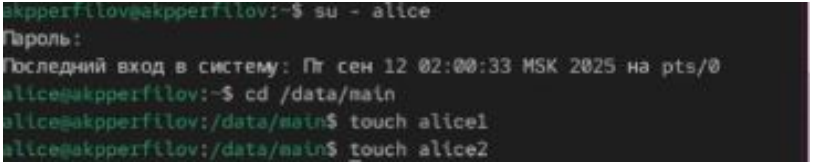
Создание файла под другой учетной записью для проверки изменений

- Перейдем под учётную запись пользователя bob
- Попробуем перейти в каталог /data/main и создать файл emptyfile в этом каталоге

```
bob@akpperfilov:~$ cd /data/main
bob@akpperfilov:/data/main$ touch emptyfile
bob@akpperfilov:/data/main$ ls - Al
```

Создание каталогов и файлов под учетной записью alice

- Откроем новый терминал под пользователем alice. Перейдем в каталог /data/main и создадим два файла



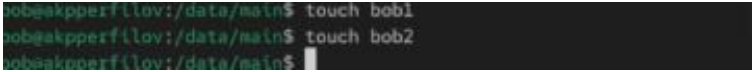
Просмотр каталога и удаление файлов под учётную запись bob

- В другом терминале перейдем под учётную запись bob. Просмотрим инфомарцию о каталоге /data/main
- Попробуем удалить файлы, принадлежащие пользователю alice

```
akpperfilov@akpperfilov:~$ su - bob
Пароль:
Последний вход в систему: Пт сен 19 17:03:46 MSK 2025 на pts/1
bob@akpperfilov:~$ cd /data/main
bob@akpperfilov:/data/main$ ls -l
итого 0
-rw-r--r--. 1 alice alice 0 сен 19 17:06 alice1
-rw-r--r--. 1 alice alice 0 сен 19 17:06 alice2
-rw-r--r--. 1 bob   bob   0 сен 19 17:04 emptyfile
bob@akpperfilov:/data/main$ rm -f alice*
bob@akpperfilov:/data/main$ ls -l
итого 0
-rw-r--r--. 1 bob bob 0 сен 19 17:04 emptyfile
```

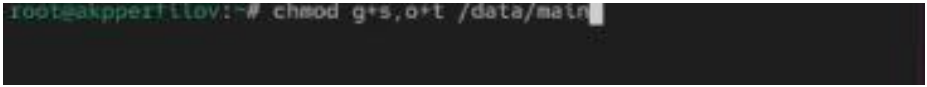
Создание файлов под учётной записью bob

- Создадим два файла



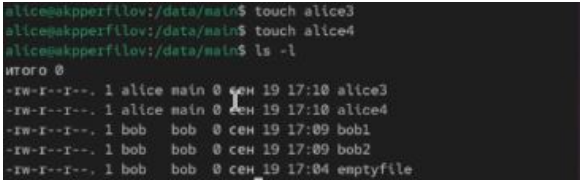
Измение параметров

- В терминале под пользователем root установим для каталога /data/main бит идентификатора группы, а также stiky-бит для общего каталога группы



Создание файлов под учетной записью alice и просмотр информации всех файлов

- Под пользователем alice создадим в каталоге /data/main файлы
- Теперь мы должны увидеть, что два созданных нами файла принадлежат группе main, которая является группой-владельцем каталога /data/main



Попытка удаление файлов bob’a

- Под пользователем alice попробуем удалить файлы, принадлежащие пользователю bob

```
alice@akpperftlov:/data/main$ rm -rf bob*
rm: невозможно удалить 'bob1': Операция не позволена
rm: невозможно удалить 'bob2': Операция не позволена
```

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

Управление расширенными разрешениями с использованием списков ACL

- Для изменений прав доступа группам и пользователям нужно будет использовать 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” <file/dir>**
- Установить разрешения для группы: **setfacl -m “g:group:permissions” <file/dir>**
- Наследование записи ACL родительского каталога: **setfacl -dm “entry” <dir>**
- Удаление записи ACL: **setfacl -x “entry” <file/dir>**
- Синтаксис команды getfacl: **getfacl <file/dir>**

Изменение прав для каталогов

- Откроем терминал с учётной записью root
- 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: ‘

```
root@akpperfilov:~# setfacl -m d:g:third:rwx /data/main
root@akpperfilov:~# setfacl -m d:g:main:rwx /data/third
root@akpperfilov:~# touch /data/main/newfile2
```

Просмотр информации о разрешений для каталогов

- Используем команду getfacl, чтобы убедиться в правильности установки разрешений:

```
root@AKpperfilov:~# 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@AKpperfilov:~# 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::---
```

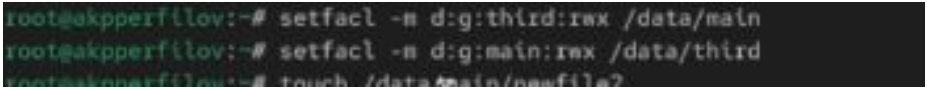
Создание файла и просмотр информации в каталоге main

- Создадим новый файл с именем newfile1 в каталоге /data/main
- Проверим текущие назначения полномочий

```
root@akpperfilov:~# touch /data/main/newfile1
root@akpperfilov:~# 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--
```

Установка ACL по умолчанию

- Установим ACL по умолчанию для каталога /data/main
- Добавим ACL по умолчанию для каталога /data/third



Проверка ACL в main

- Убедимся, что настройки ACL работают, создадим новый файл в каталог /data/main
- Проверим текущие назначения полномочий

```
root@akpperfilov:~# touch /data/main/newfile2
root@akpperfilov:~# 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::---
```

Проверка полномочий группы third, удаление файлов

- Для проверки полномочий группы third в каталоге /data/third войдем в другом терминале под учётной записью члена группы third
- Проверим операции с файлами

```
carol@akpperfilov:~$ rm /data/main/newfile1
rm: удалить защищённый от записи пустой обычный файл '/data/main/new
file1'? yes
rm: невозможно удалить '/data/main/newfile1': Отказано в доступе
carol@akpperfilov:~$ rm /data/main/newfile2
rm: невозможно удалить '/data/main/newfile2': Отказано в доступе
```

- Удалить файлы мы не смогли, так как newfile1 принадлежит пользователю root и группе main, newfile2 также принадлежит root, main и third, хоть и carol находится в последней группе, у группы недостаточно прав.

Проверка полномочий группы third, запись файлов

- Проверим, возможно ли осуществить запись в файл

```
carol@akpperfilov:~$ rm /data/main/newfile1
rm: удалить защищённый от записи пустой обычный файл '/data/main/new
file1'? yes
rm: невозможно удалить '/data/main/newfile1': Отказано в доступе
carol@akpperfilov:~$ rm /data/main/newfile2
rm: невозможно удалить '/data/main/newfile2': Отказано в доступе
```

- Мы не смогли осуществить запись в newfile1, так как прав у группы third на нее нет. А вот уже в newfile2 все получилось, так как права на изменение файла у данной группы есть.

Вывод:

В ходе работы приобретены умения по управлению базовыми и специальными правами доступа для групп пользователей в ОС Linux.