

# Лабораторная работа №3

## Настройка прав доступа

Чекмарев Александр Дмитриевич | Группа НПИбд-03-24

Российский университет дружбы народов, Москва, Россия

20 сентября 2025

## Section 1

# Информация

# Докладчик

- Чекмарев Александр Дмитриевич
- Группа НПИбд-03-24
- Российский университет дружбы народов
- <https://github.com/nenokixd?tab=repositories>

## Section 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.

## Section 3

### Ход лабораторной работы

# Создание и просмотр файлов

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

```
adchekmarev@adchekmarev:~$ su -
```

Пароль:

Последний вход в систему: Сб сен 13 15:53:30 MSK 2025 на pts/0

```
root@adchekmarev:~# mkdir -p /data/main /data/third
```

```
root@adchekmarev:~# ls -Al /data
```

итого 0

```
drwxr-xr-x. 2 root root 6 сен 19 22:20 main
```

```
drwxr-xr-x. 2 root root 6 сен 19 22:20 third
```



## Изменение владельцев каталогов

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

```
root@adchekmarev:~# chgrp main /data/main
root@adchekmarev:~# chgrp third /data/third

root@adchekmarev:~# ls -Al /data
итого 0
drwxr-xr-x. 2 root main  6 сен 19 22:20 main
drwxr-xr-x. 2 root third 6 сен 19 22:20 third
```

## Изменение прав доступа к файлам

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

```
root@adchekmarev:~# chmod 770 /data/main
root@adchekmarev:~# chmod 770 /data/third
root@adchekmarev:~# ls -Al /data
итого 0
drwxrwx---. 2 root main  6 сен 19 22:20 main
drwxrwx---. 2 root third 6 сен 19 22:20 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@adchekmarev:~$ cd /data/main
bob@adchekmarev:/data/main$ touch emptyfile
bob@adchekmarev:/data/main$ ls -Al
итого 0
-rw-r--r--. 1 bob bob 0 сен 19 22:23 emptyfile
```

## Попытка изменений в другом каталоге под учетной записью bob

- Под пользователем bob попробуем перейти в каталог /data/third и создать файл emptyfile в этом каталоге

```
bob@adchekmarev:/data/main$ cd /data/third  
-bash: cd: /data/third: Отказано в доступе
```

- Мы не можем перейти в данный каталог и создать файл, так как у bob'а нет прав к каталогу third.

## Создание каталогов и файлов под учетной записью alice

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

```
adchekmarev@adchekmarev:~$ su - alice
```

Пароль:

Последний вход в систему: Сб сен 13 15:47:56 MSK 2025 на pts/0

```
alice@adchekmarev:~$ cd /data/main
```

```
alice@adchekmarev:/data/main$ touch alice1
```

```
alice@adchekmarev:/data/main$ touch alice2
```

## Просмотр каталога и удаление файлов под учётную запись bob

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

```
bob@adchekmarev:/data/main$ ls -l
итого 0
-rw-r--r--. 1 alice alice 0 сен 19 22:27 alice1
-rw-r--r--. 1 alice alice 0 сен 19 22:27 alice2
-rw-r--r--. 1 bob   bob   0 сен 19 22:23 emptyfile
```

```
bob@adchekmarev:/data/main$ rm -f alice*
bob@adchekmarev:/data/main$ ls -l
итого 0
-rw-r--r--. 1 bob bob 0 сен 19 22:23 emptyfile
```

# Создание файлов под учётной записью bob

- Создадим два файла

```
bob@adchekmarev:/data/main$ touch bob1
```

```
bob@adchekmarev:/data/main$ touch bob2
```

## Изменение параметров

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

```
root@adchekmarev:~# chmod g+s,o+t /data/main
```



# 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

```
alice@adchekmarev:/data/main$ touch alice3
alice@adchekmarev:/data/main$ touch alice4
alice@adchekmarev:/data/main$ ls -l
итого 0
-rw-r--r--. 1 alice main 0 сен 19 22:28 alice3
-rw-r--r--. 1 alice main 0 сен 19 22:28 alice4
-rw-r--r--. 1 bob   bob   0 сен 19 22:28 bob1
-rw-r--r--. 1 bob   bob   0 сен 19 22:28 bob2
-rw-r--r--. 1 bob   bob   0 сен 19 22:23 emptyfile
```

## Попытка удаление файлов bob'a

- Под пользователем alice попробуем удалить файлы, принадлежащие пользователю bob

```
alice@adchekmarev:/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@adchekmarev:~# setfacl -m g:third:rx /data/main
```

```
root@adchekmarev:~# setfacl -m g:main:rx /data/third
```

# Просмотр информации о разрешениях для каталогов

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

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

## Создание файла и просмотр информации в каталоге third

- Создадим новый файл с именем newfile1 в каталоге /data/third и посмотрим информацию

```
root@adchekmarev:~# touch /data/third/newfile1
root@adchekmarev:~# 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--
```

## Установка ACL по умолчанию

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

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



## Проверка ACL в main

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

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

## Проверка ACL в third

- Создадим новый файл newfile2 в каталог /data/third и проверим текущие назначения полномочий

```
root@adchekmarev:~# touch /data/third/newfile2
root@adchekmarev:~# 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::---
```

## 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@adchekmarev:~$ rm /data/main/newfile1
rm: удалить защищённый от записи пустой обычный файл '/data/main/newfile1'? yes
rm: невозможно удалить '/data/main/newfile1': Отказано в доступе
carol@adchekmarev:~$ 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@adchekmarev:~$ echo "Hello, world" >> /data/main/newfile1
-bash: /data/main/newfile1: Отказано в доступе
carol@adchekmarev:~$ echo "Hello, world" >> /data/main/newfile2
```

- 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.