

Лабораторная работа 3

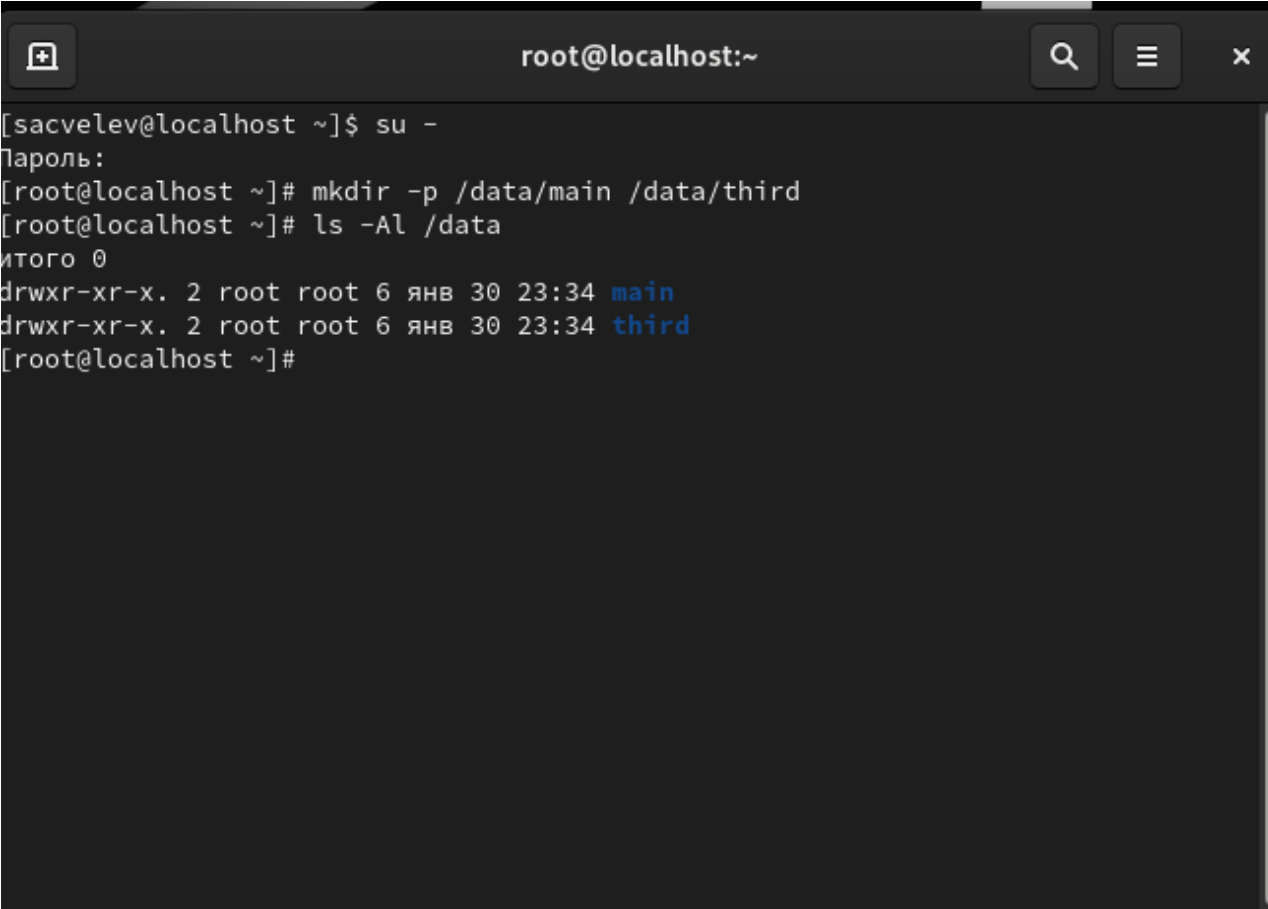
Настройка прав доступа

Цвелев С.А. НПИбд-02-22

Цель работы

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

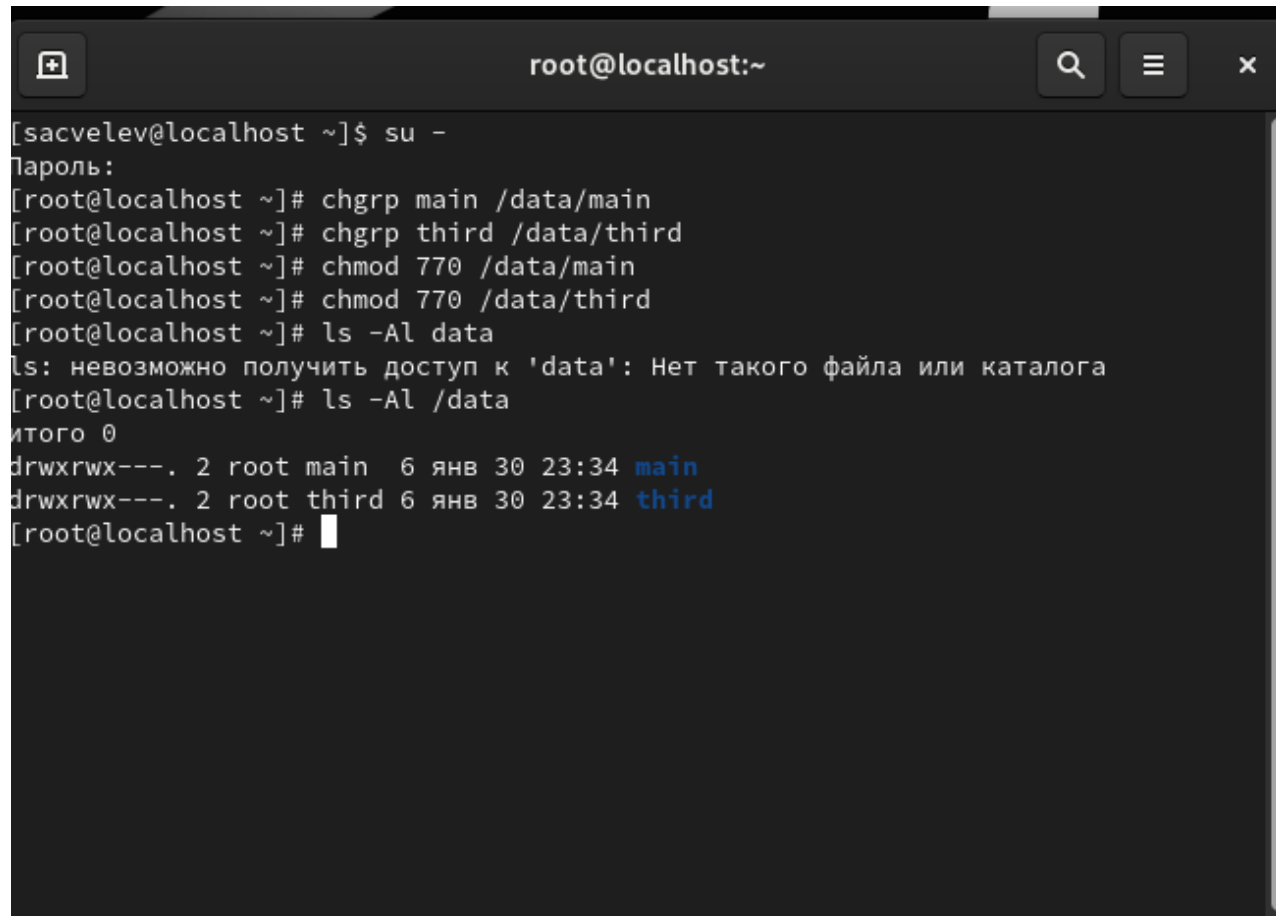
Создание новых каталогов

A terminal window titled 'root@localhost:~' with search, menu, and close icons in the title bar. The terminal shows a user switching to root and creating two directories. The output of the 'ls' command is displayed in a table format.

```
root@localhost:~  
[sacvelev@localhost ~]$ su -  
Пароль:  
[root@localhost ~]# mkdir -p /data/main /data/third  
[root@localhost ~]# ls -Al /data  
итого 0  
drwxr-xr-x. 2 root root 6 янв 30 23:34 main  
drwxr-xr-x. 2 root root 6 янв 30 23:34 third  
[root@localhost ~]#
```

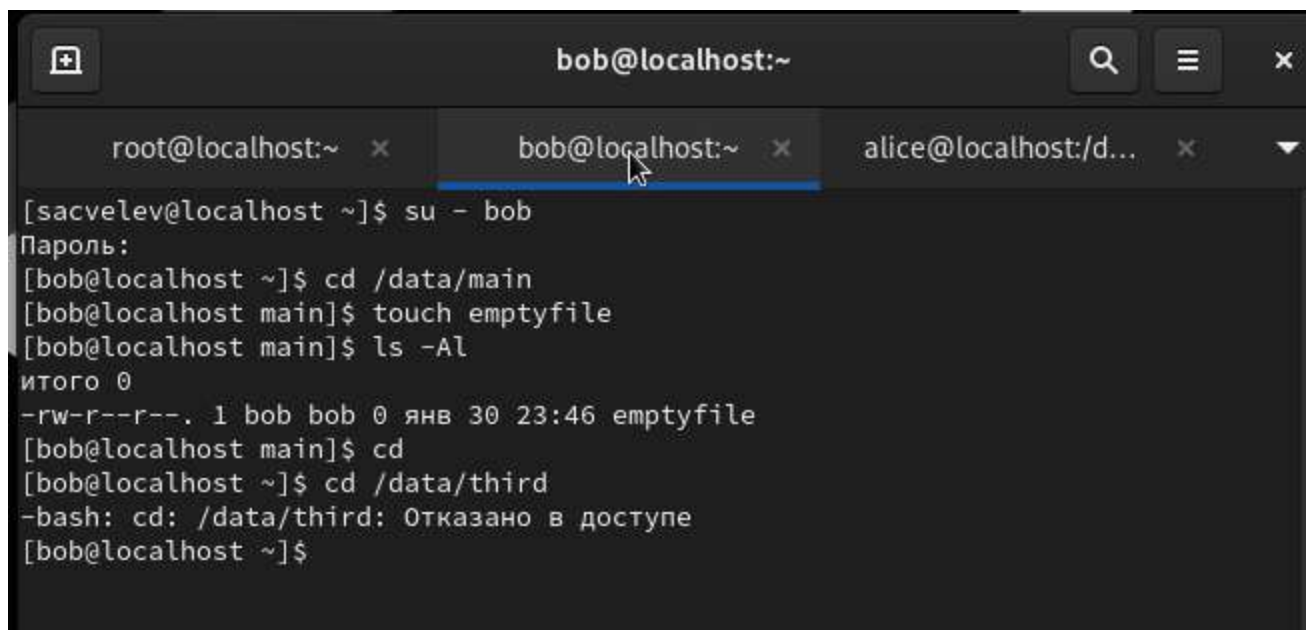
Permissions	Links	User	Group	Size	Month	Day	Time	Directory
drwxr-xr-x	2	root	root	6	янв	30	23:34	main
drwxr-xr-x	2	root	root	6	янв	30	23:34	third

Установка владельца и разрешений на каталоги



```
root@localhost:~  
[sacvelev@localhost ~]$ su -  
Пароль:  
[root@localhost ~]# chgrp main /data/main  
[root@localhost ~]# chgrp third /data/third  
[root@localhost ~]# chmod 770 /data/main  
[root@localhost ~]# chmod 770 /data/third  
[root@localhost ~]# ls -Al data  
ls: невозможно получить доступ к 'data': Нет такого файла или каталога  
[root@localhost ~]# ls -Al /data  
итого 0  
drwxrwx---. 2 root main  6 янв 30 23:34 main  
drwxrwx---. 2 root third 6 янв 30 23:34 third  
[root@localhost ~]#
```

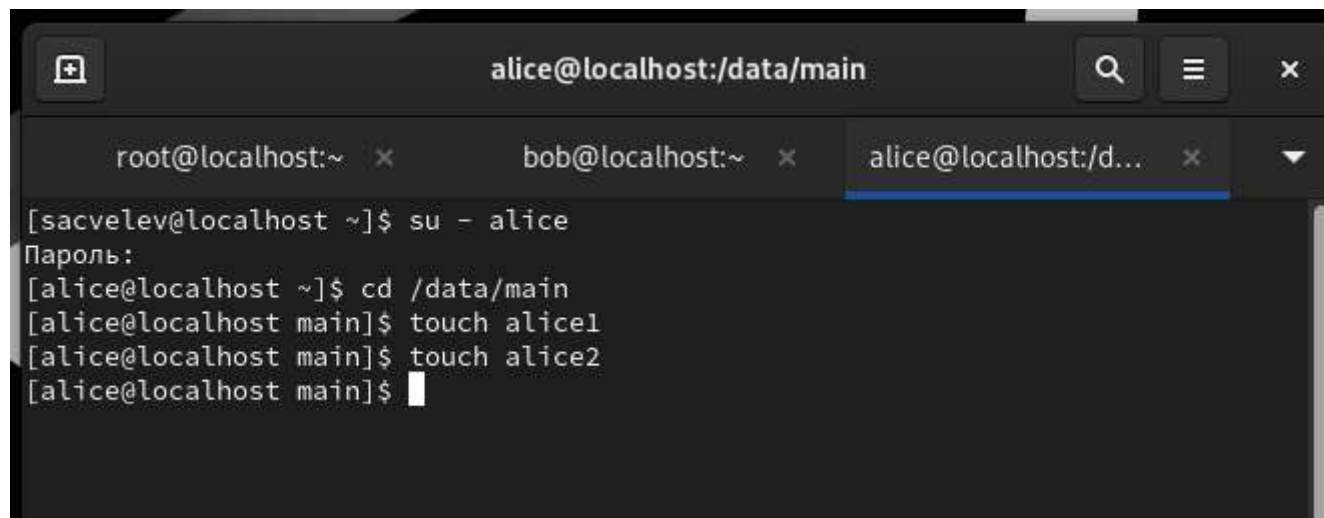
Проверка доступа пользователем bob



A terminal window with a dark background and light text. The title bar shows 'bob@localhost:~'. The terminal content shows a sequence of commands and their outputs. The user switches from root to bob, creates a file, and then attempts to change to a directory where access is denied.

```
root@localhost:~ x bob@localhost:~ x alice@localhost:/d... x
[sacvelev@localhost ~]$ su - bob
Пароль:
[bob@localhost ~]$ cd /data/main
[bob@localhost main]$ touch emptyfile
[bob@localhost main]$ ls -Al
итого 0
-rw-r--r--. 1 bob bob 0 янв 30 23:46 emptyfile
[bob@localhost main]$ cd
[bob@localhost ~]$ cd /data/third
-bash: cd: /data/third: Отказано в доступе
[bob@localhost ~]$
```

Создание файлов alice1 и alice2

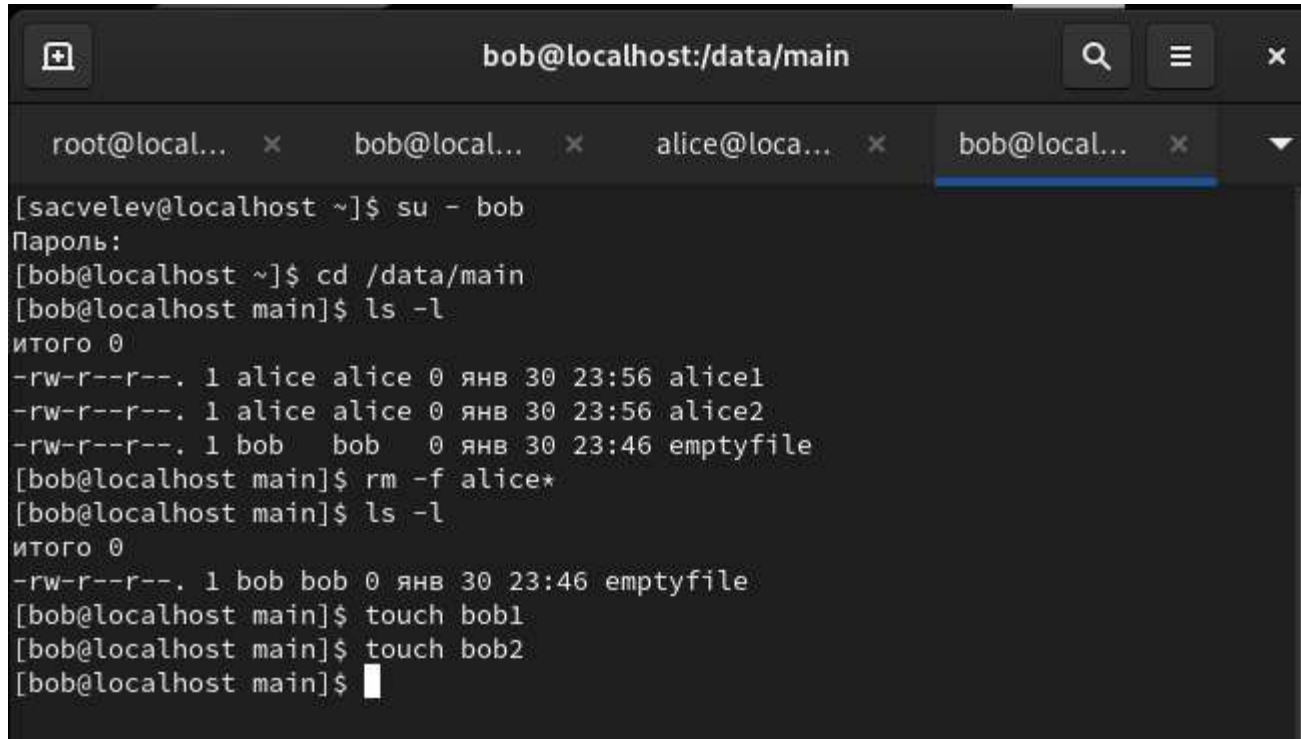


```
alice@localhost:/data/main

root@localhost:~ x bob@localhost:~ x alice@localhost:/d... x

[sacvelev@localhost ~]$ su - alice
Пароль:
[alice@localhost ~]$ cd /data/main
[alice@localhost main]$ touch alice1
[alice@localhost main]$ touch alice2
[alice@localhost main]$
```

Пользователь bob удаляет файлы пользователя alice и создаёт свои файлы



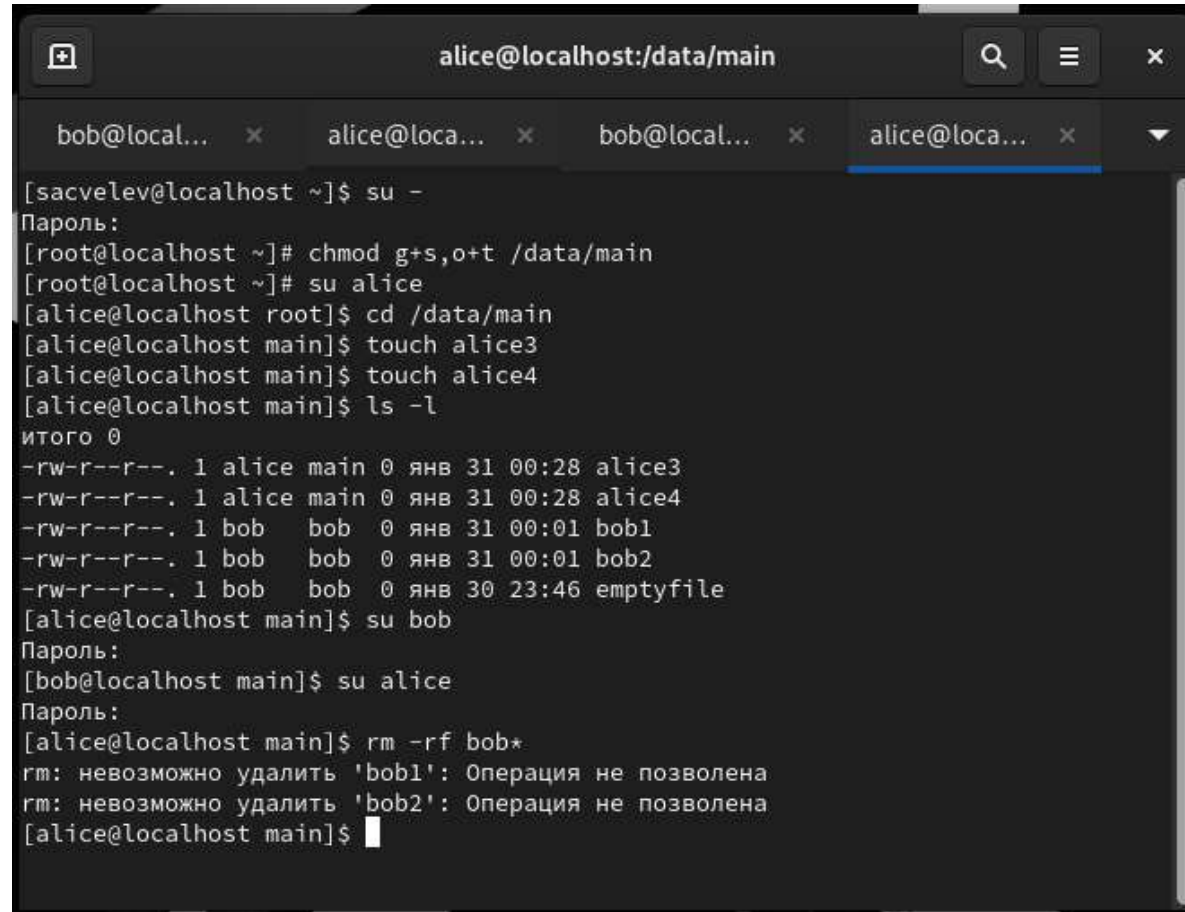
The image shows a terminal window with a dark background. At the top, the title bar reads 'bob@localhost:/data/main'. Below the title bar, there are four tabs: 'root@local...', 'bob@local...', 'alice@loca...', and 'bob@local...'. The 'bob@local...' tab is selected and highlighted with a blue underline. The terminal content shows a sequence of commands and their outputs:

```
[sacvelev@localhost ~]$ su - bob
Пароль:
[bob@localhost ~]$ cd /data/main
[bob@localhost main]$ ls -l
итого 0
-rw-r--r--. 1 alice alice 0 янв 30 23:56 alice1
-rw-r--r--. 1 alice alice 0 янв 30 23:56 alice2
-rw-r--r--. 1 bob  bob  0 янв 30 23:46 emptyfile
[bob@localhost main]$ rm -f alice*
[bob@localhost main]$ ls -l
итого 0
-rw-r--r--. 1 bob bob 0 янв 30 23:46 emptyfile
[bob@localhost main]$ touch bob1
[bob@localhost main]$ touch bob2
[bob@localhost main]$
```

Создание пользователя carol

```
carol@localhost:~  
Пароль:  
[alice@localhost sacvelev]$ sudo -i useradd carol  
[sudo] пароль для alice:  
[alice@localhost sacvelev]$ sudo passwd carol  
Изменение пароля пользователя carol.  
Новый пароль:  
Повторите ввод нового пароля:  
passwd: данные аутентификации успешно обновлены.  
[alice@localhost sacvelev]$ su carol  
Пароль:  
[carol@localhost sacvelev]$ id  
uid=1003(carol) gid=1003(carol) группы=1003(carol) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[carol@localhost sacvelev]$ cd  
[carol@localhost ~]$ ls -Al  
итого 16  
-rw-r--r--. 1 carol carol 18 янв 24 2023 .bash_logout  
-rw-r--r--. 1 carol carol 141 янв 24 2023 .bash_profile  
-rw-r--r--. 1 carol carol 492 янв 24 2023 .bashrc  
drwxr-xr-x. 2 carol carol 6 янв 28 00:23 Documents  
drwxr-xr-x. 4 carol carol 39 янв 24 00:52 .mozilla  
drwxr-xr-x. 2 carol carol 6 янв 28 00:23 Pictures  
-rw-----. 1 carol carol 130 янв 28 00:55 .xauthPNsD6C  
[carol@localhost ~]$
```

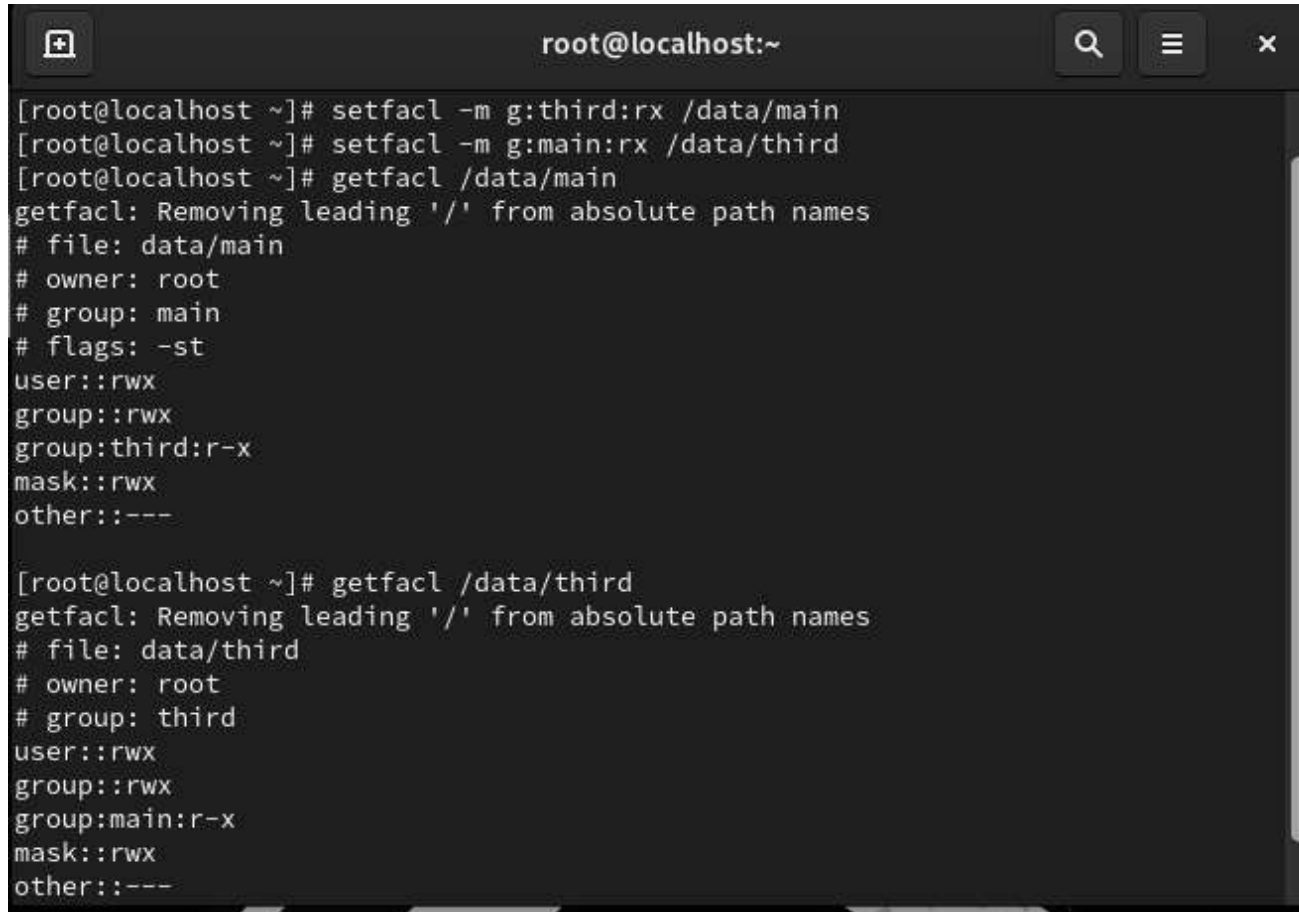

Установка бита идентификатора и sticky-бита для общего каталога группы



```
alice@localhost:/data/main

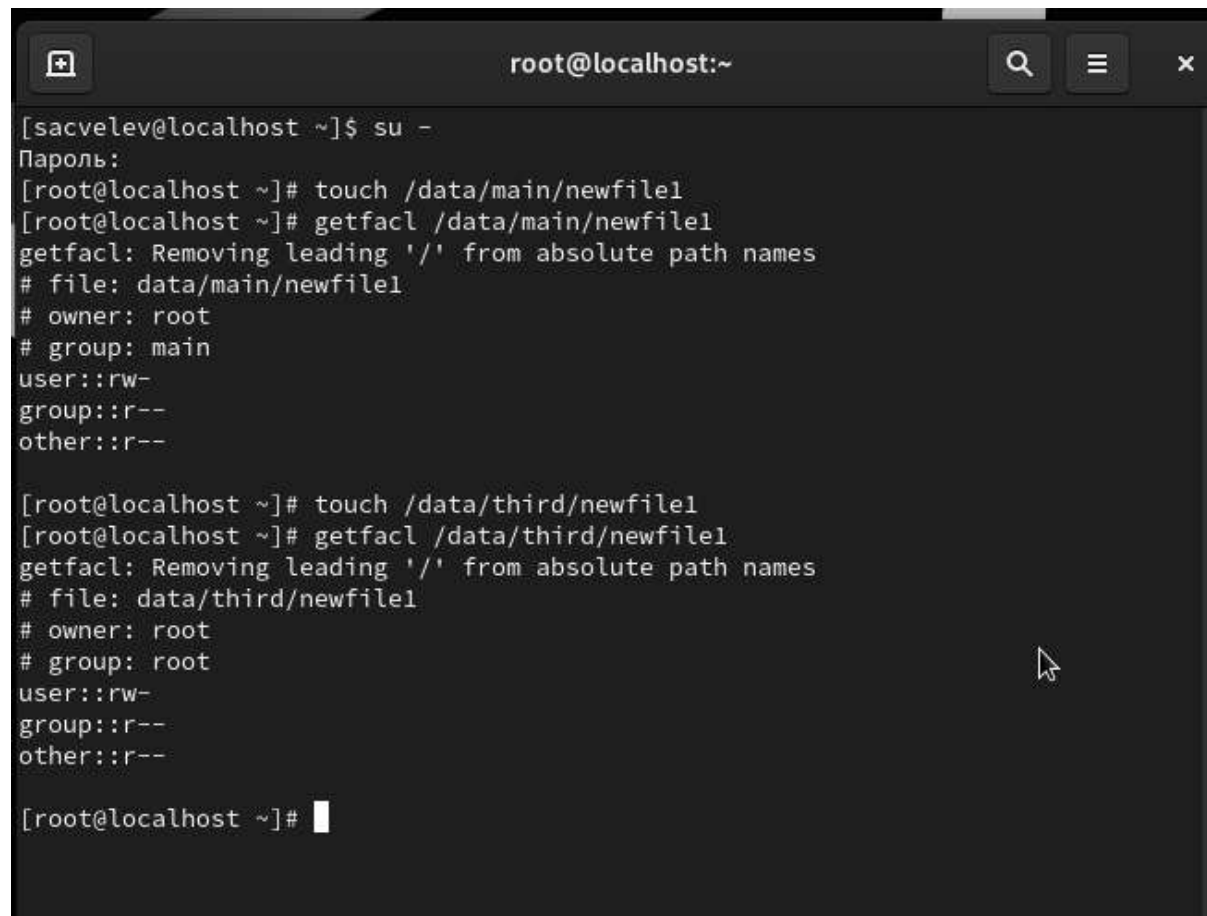
[sacvelev@localhost ~]$ su -
Пароль:
[root@localhost ~]# chmod g+s,o+t /data/main
[root@localhost ~]# su alice
[alice@localhost root]$ cd /data/main
[alice@localhost main]$ touch alice3
[alice@localhost main]$ touch alice4
[alice@localhost main]$ ls -l
итого 0
-rw-r--r--. 1 alice main 0 янв 31 00:28 alice3
-rw-r--r--. 1 alice main 0 янв 31 00:28 alice4
-rw-r--r--. 1 bob   bob   0 янв 31 00:01 bob1
-rw-r--r--. 1 bob   bob   0 янв 31 00:01 bob2
-rw-r--r--. 1 bob   bob   0 янв 30 23:46 emptyfile
[alice@localhost main]$ su bob
Пароль:
[bob@localhost main]$ su alice
Пароль:
[alice@localhost main]$ rm -rf bob*
rm: невозможно удалить 'bob1': Операция не позволена
rm: невозможно удалить 'bob2': Операция не позволена
[alice@localhost main]$
```

Установка прав на чтение и выполнение в каталогах



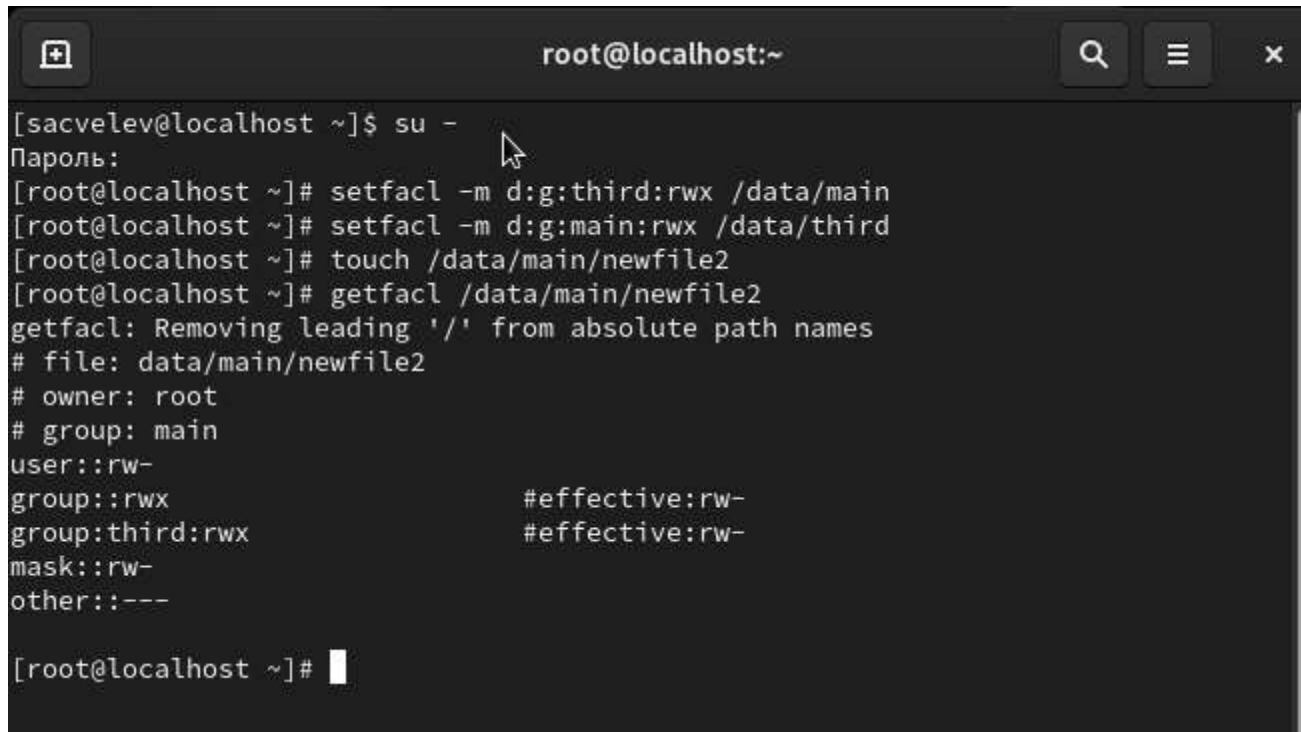
```
root@localhost:~  
[root@localhost ~]# setfacl -m g:third:rx /data/main  
[root@localhost ~]# setfacl -m g:main:rx /data/third  
[root@localhost ~]# getfacl /data/main  
getfacl: Removing leading '/' from absolute path names  
# file: data/main  
# owner: root  
# group: main  
# flags: -st  
user::rwx  
group::rwx  
group:third:r-x  
mask::rwx  
other::---  
  
[root@localhost ~]# 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::---
```

Проверка полномочий



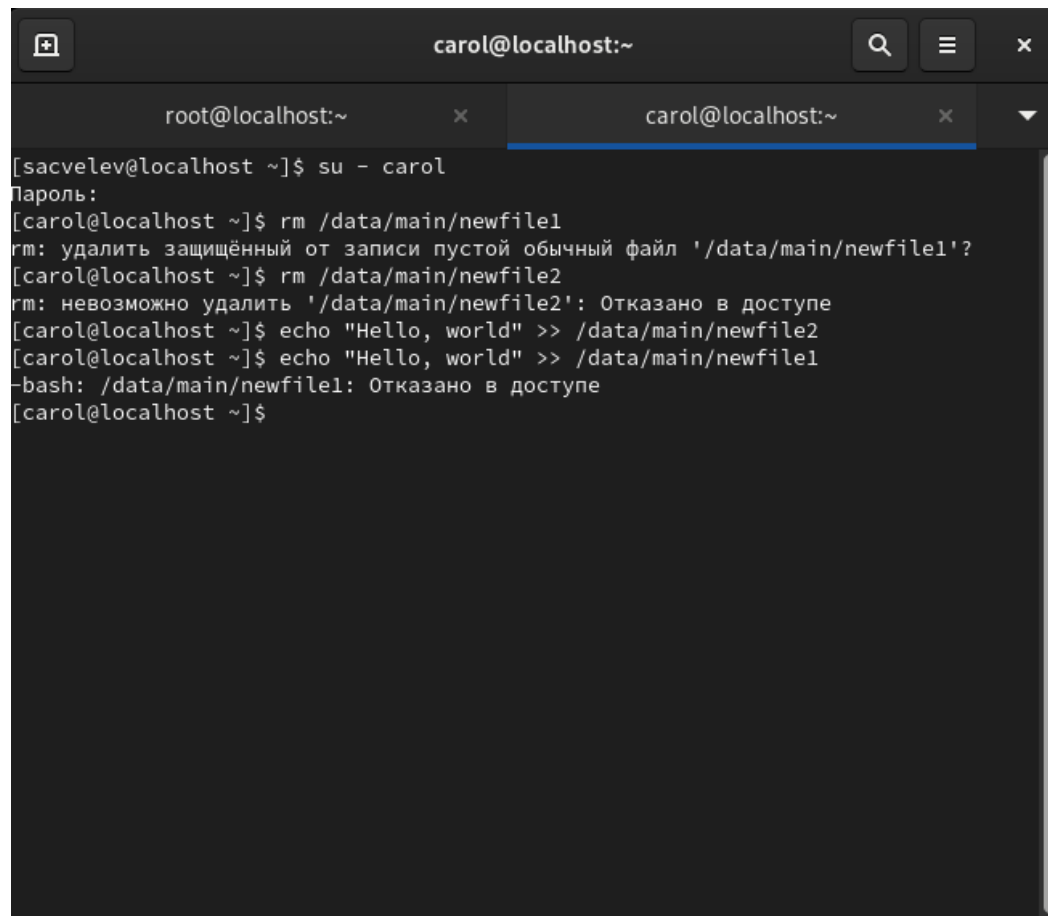
```
root@localhost:~  
[sacvelev@localhost ~]$ su -  
Пароль:  
[root@localhost ~]# touch /data/main/newfile1  
[root@localhost ~]# getfacl /data/main/newfile1  
getfacl: Removing leading '/' from absolute path names  
# file: data/main/newfile1  
# owner: root  
# group: main  
user::rw-  
group::r--  
other::r--  
  
[root@localhost ~]# touch /data/third/newfile1  
[root@localhost ~]# 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@localhost ~]#
```

Установка ACL по умолчанию

A terminal window titled 'root@localhost:~' with search, menu, and close icons in the title bar. The terminal shows a user switching to root via 'su -', then using 'setfacl' to set permissions on '/data/main' and '/data/third', creating a file, and finally using 'getfacl' to display the resulting ACL settings.

```
root@localhost:~  
[sacvelev@localhost ~]$ su -  
Пароль:  
[root@localhost ~]# setfacl -m d:g:third:rw- /data/main  
[root@localhost ~]# setfacl -m d:g:main:rw- /data/third  
[root@localhost ~]# touch /data/main/newfile2  
[root@localhost ~]# getfacl /data/main/newfile2  
getfacl: Removing leading '/' from absolute path names  
# file: data/main/newfile2  
# owner: root  
# group: main  
user::rw-  
group::rw- #effective:rw-  
group:third:rw- #effective:rw-  
mask::rw-  
other::---  
[root@localhost ~]#
```

Проверка операций с файлами



```
carol@localhost:~  
root@localhost:~ x carol@localhost:~ x  
[sacvelev@localhost ~]$ su - carol  
Пароль:  
[carol@localhost ~]$ rm /data/main/newfile1  
rm: удалить защищённый от записи пустой обычный файл '/data/main/newfile1'?  
[carol@localhost ~]$ rm /data/main/newfile2  
rm: невозможно удалить '/data/main/newfile2': Отказано в доступе  
[carol@localhost ~]$ echo "Hello, world" >> /data/main/newfile2  
[carol@localhost ~]$ echo "Hello, world" >> /data/main/newfile1  
-bash: /data/main/newfile1: Отказано в доступе  
[carol@localhost ~]$
```