

# **Шаблон отчёта по лабораторной работе**

**Простейший вариант**

Дмитрий Сергеевич Кулябов

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Задание</b>	<b>6</b>
<b>3 Теоретическое введение</b>	<b>7</b>
<b>4 Выполнение лабораторной работы</b>	<b>8</b>
<b>5 Выводы</b>	<b>27</b>
<b>Список литературы</b>	<b>28</b>

# Список иллюстраций

4.1 подключение к учётной записи root . . . . .	8
4.2 создание каталогов main и third . . . . .	9
4.3 проверка каталогов . . . . .	9
4.4 изменение владельцев . . . . .	10
4.5 проверка владельцев . . . . .	10
4.6 установление разрешений . . . . .	11
4.7 проверка разрешений . . . . .	11
4.8 подключение к учётной записи пользователя bob . . . . .	12
4.9 создание каталогов в каталоге main . . . . .	12
4.10 новый терминал . . . . .	13
4.11 перемещение в каталог cd /data/main . . . . .	14
4.12 создание файлов . . . . .	14
4.13 новый терминал с пользователем bob . . . . .	15
4.14 перемещение в каталог data/main . . . . .	15
4.15 просмотр файлов в каталоге /data/main . . . . .	16
4.16 удаление файлов . . . . .	16
4.17 создание файлов bob1 и bob2 . . . . .	17
4.18 установление каталогов . . . . .	17
4.19 создание файлов alice3 и alice4 . . . . .	18
4.20 удаление файлов . . . . .	19
4.21 установление прав . . . . .	19
4.22 создание файла newfile1 . . . . .	20
4.23 проверка текущих назначений полномочий . . . . .	20
4.24 Повторение предыдущих шагов . . . . .	21
4.25 установление ACL . . . . .	21
4.26 установление ACL . . . . .	22
4.27 создание файла newfile2 . . . . .	22
4.28 проверка файла newfile2 . . . . .	23
4.29 создание файла newfile3 . . . . .	23
4.30 проверка файла newfile3 . . . . .	24
4.31 подключение к учётной записи пользователя carol . . . . .	24
4.32 удаление файлов . . . . .	25
4.33 echo . . . . .	25

# **Список таблиц**

# **1 Цель работы**

Здесь приводится формулировка цели лабораторной работы. Формулировки цели для каждой лабораторной работы приведены в методических указаниях.

Цель данного шаблона – максимально упростить подготовку отчётов по лабораторным работам. Модифицируя данный шаблон, студенты смогут без труда подготовить отчёт по лабораторным работам, а также познакомиться с основными возможностями разметки Markdown.

## **2 Задание**

Здесь приводится описание задания в соответствии с рекомендациями методического пособия и выданным вариантом.

## **3 Теоретическое введение**

Более подробно про Unix см. в [1–4].

# 4 Выполнение лабораторной работы

я начал эту лабораторную работу открывая терминал и подключаясь к учётной записи root (рис. 4.1).

```
su -
```

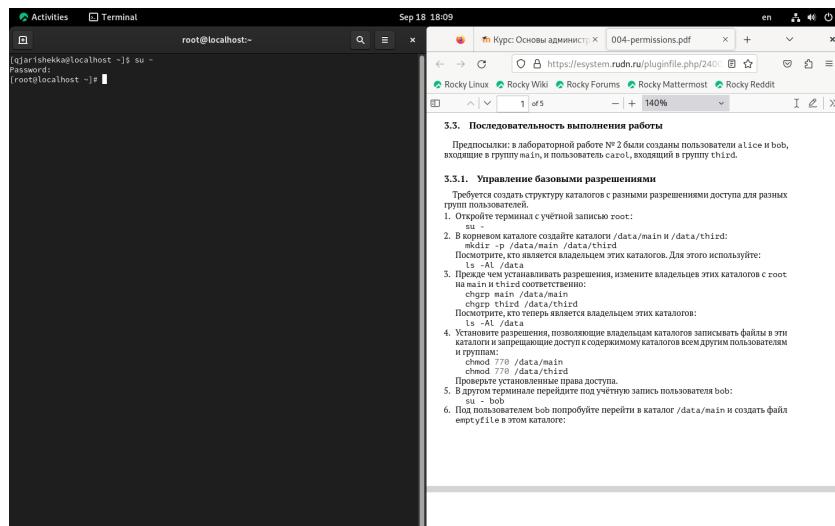


Рис. 4.1: подключение к учётной записи root

Потом я создал каталог main и third в каталоге data (рис. 4.2).

```
mkdir -p /data/main /data/third
```

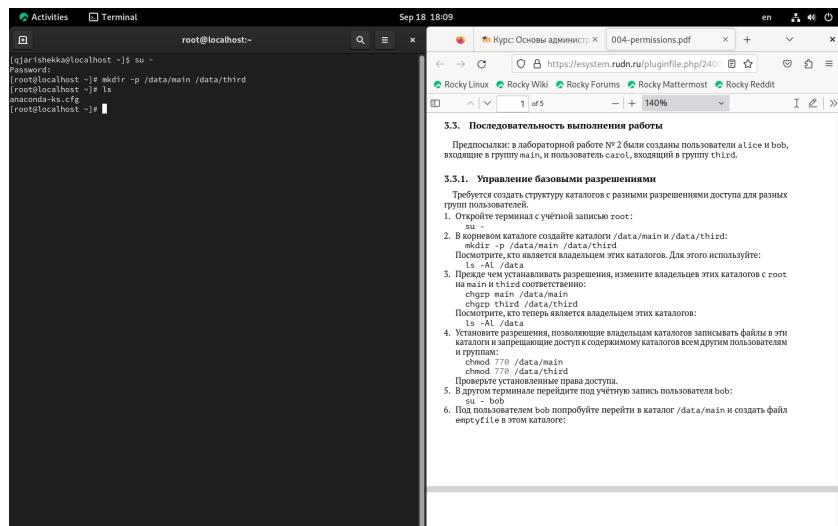


Рис. 4.2: создание каталогов main и third

и затем я убедился что каталоги создались правильно и кто является владельцем (рис. 4.3).

```
ls -l /data
```

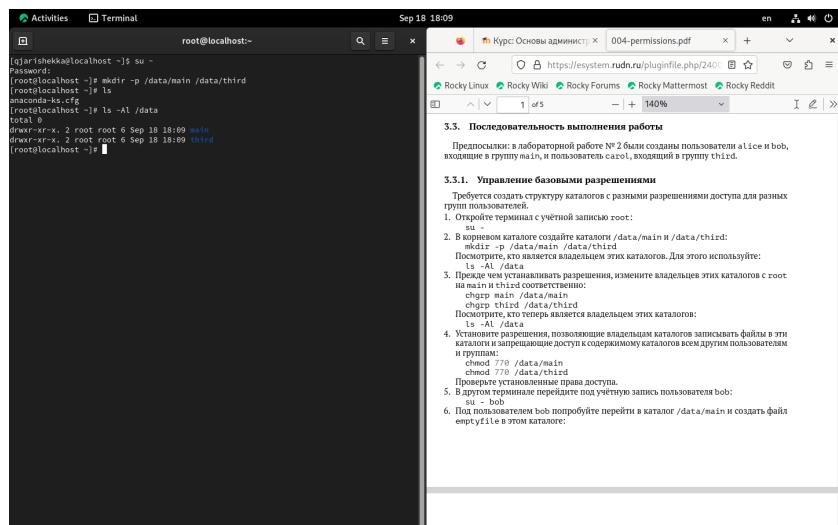


Рис. 4.3: проверка каталогов

Потом я изменил владельцев этих каталогов с root на main и third (рис. 4.4).

```
chgrp main /data/main
chgrp third /data/third
```

```

root@localhost ~]# su -
[password]
[root@localhost ~]# mkdir -p /data/main /data/third
[root@localhost ~]# ls
mainconda-ks.cfg
[root@localhost ~]# chgrp main /data/main
[root@localhost ~]# chgrp third /data/third
[root@localhost ~]#

```

3.3. Последовательность выполнения работы

Предположим, в лабораторной работе № 2 были созданы пользователи alice и bob, входящие в группу bob, и пользователь casper, входящий в группу third.

3.3.1. Управление базовыми разрешениями

Требуется создать структуру каталогов с различными разрешениями доступа для разных групп пользователей.

1. Откройте терминал с учётной записью root:
2. В корневом каталоге создайте каталоги /data/main и /data/third. Помогите, кто является владельцем этих каталогов. Для этого используйте:

```
ls -Al /data
```

3. Прежде чем устанавливать разрешения, измените владельцев этих каталогов с root на alice и third соответственно:

```
chgrp main /data/main
chgrp third /data/third
```

Помогите, кто теперь является владельцем этих каталогов:

4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:

```
chmod 770 /data/main
chmod 770 /data/third
```

Проверьте установленные права доступа.

5. В другом терминале перейдите под учётную запись пользователя bob:

```
su - bob
```

6. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге:

Рис. 4.4: изменение владельцев каталогов

Дальше я еще раз посмотрел кто теперь является владельцем каталогов (рис. 4.5).

`ls -Al /data`

```

root@localhost ~]# su -
[password]
[root@localhost ~]# mkdir -p /data/main /data/third
[root@localhost ~]# ls
mainconda-ks.cfg
[root@localhost ~]# chgrp main /data/main
[root@localhost ~]# chgrp third /data/third
[root@localhost ~]# ls -Al /data
total 0
drwxr-xr-x 2 root root 6 Sep 18 18:09 main
drwxr-xr-x 2 root root 6 Sep 18 18:09 third
[root@localhost ~]#

```

3.3. Последовательность выполнения работы

Предположим, в лабораторной работе № 2 были созданы пользователи alice и bob, входящие в группу bob, и пользователь casper, входящий в группу third.

3.3.1. Управление базовыми разрешениями

Требуется создать структуру каталогов с различными разрешениями доступа для разных групп пользователей.

1. Откройте терминал с учётной записью root:
2. В корневом каталоге создайте каталоги /data/main и /data/third. Помогите, кто является владельцем этих каталогов. Для этого используйте:

```
ls -Al /data
```

3. Прежде чем устанавливать разрешения, измените владельцев этих каталогов с root на main и third соответственно:

```
chgrp main /data/main
chgrp third /data/third
```

Помогите, кто теперь является владельцем этих каталогов:

4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:

```
chmod 770 /data/main
chmod 770 /data/third
```

Проверьте установленные права доступа.

5. В другом терминале перейдите под учётную запись пользователя bob:

```
su - bob
```

6. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге:

Рис. 4.5: проверка владельцев

Потом я установил разрешения этих каталогов (рис. 4.6).

`chmod 770 /data/main`

`chmod 770 /data/third`

```

root@localhost ~$ su -
Password:
[root@localhost ~]# mkdir -p /data/main /data/third
[root@localhost ~]# ls
main.conf k3.cfg
[root@localhost ~]# ls -Al /data
total 0
drwxr-xr-x 2 root root 6 Sep 18 18:09 main
drwxr-xr-x 2 root root 6 Sep 18 18:09 third
[root@localhost ~]# chgrp main /data/main
[root@localhost ~]# chmod 777 /data/main
[root@localhost ~]# ls -Al /data
total 0
drwxr-xr-x 2 root main 6 Sep 18 18:09 main
drwxr-xr-x 2 root third 6 Sep 18 18:09 third
[root@localhost ~]# chmod 777 /data/third
[root@localhost ~]#

```

Лабораторная работа №3. Настройка прав доступа

- Посмотрите, кто является владельцем этих каталогов. Для этого используйте: `ls -A /data`
- Прежде чем устанавливать разрешения, измените владельцев этих каталогов с `root` на `main` и `third` следующим образом:

  - `chgrp main /data/main`
  - `chmod 777 /data/main`

- Посмотрите, кто теперь является владельцем этих каталогов:

  - `ls -A /data`

- Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:

  - `chown 777 /data/main`
  - `chmod 777 /data/third`

- Проверьте установленные права доступа.
- В другом терминале перейдите под учётную запись пользователя `bob`:

  - `su - bob`

- Под пользователем `bob` попробуйте перейти в каталог `/data/main` и создать файл `emptyfile` в этом каталоге.
- Опишите и покажите результат этого действия.

3.3.2. Управление специальными разрешениями

Требуется, используя специальные разрешения для групп пользователей, обеспечить

Рис. 4.6: установление разрешений

Дальше я проверял еще раз разрешения (рис. 4.7).

`ls -l /data`

```

root@localhost ~# ls -Al /data
total 0
drwxr-xr-x 2 root main 6 Sep 18 18:09 main
drwxr-xr-x 2 root third 6 Sep 18 18:09 third
[root@localhost ~]#

```

Лабораторная работа №3. Настройка прав доступа

- Посмотрите, кто является владельцем этих каталогов. Для этого используйте: `ls -A /data`
- Прежде чем устанавливать разрешения, измените владельцев этих каталогов с `root` на `main` и `third` следующим образом:

  - `chgrp main /data/main`
  - `chgrp third /data/third`

- Посмотрите, кто теперь является владельцем этих каталогов:

  - `ls -A /data`

- Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:

  - `chmod 777 /data/main`
  - `chmod 777 /data/third`

- Проверьте установленные права доступа.
- В другом терминале перейдите под учётную запись пользователя `bob`:

  - `su - bob`

- Под пользователем `bob` попробуйте перейти в каталог `/data/third` и создать файл `emptyfile` в этом каталоге.
- Опишите и покажите результат этого действия.

3.3.2. Управление специальными разрешениями

Требуется, используя специальные разрешения для групп пользователей, обеспечить

Рис. 4.7: проверка разрешений

Потом я открыл другой терминал и подключился к учётной записи пользователя `bob` который я создал на прошлую лабораторную работу, его пароль - `beta1234` (рис. 4.8).

```
su - bob
```

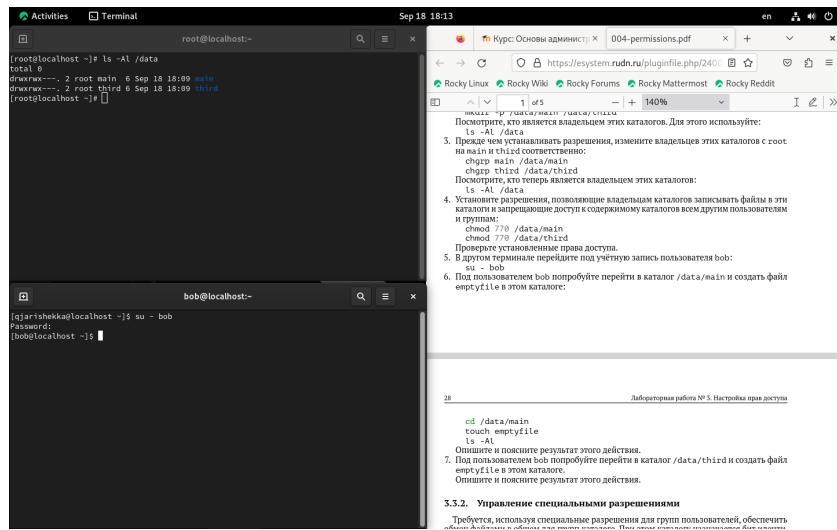


Рис. 4.8: подключение к учётной записи пользователя bob

Дальше я попробовал перейти в каталог `/data/main` и создать файл `emptyfile` (рис. 4.9).

```
cd /data/main  
touch emptyfile  
ls -Al
```

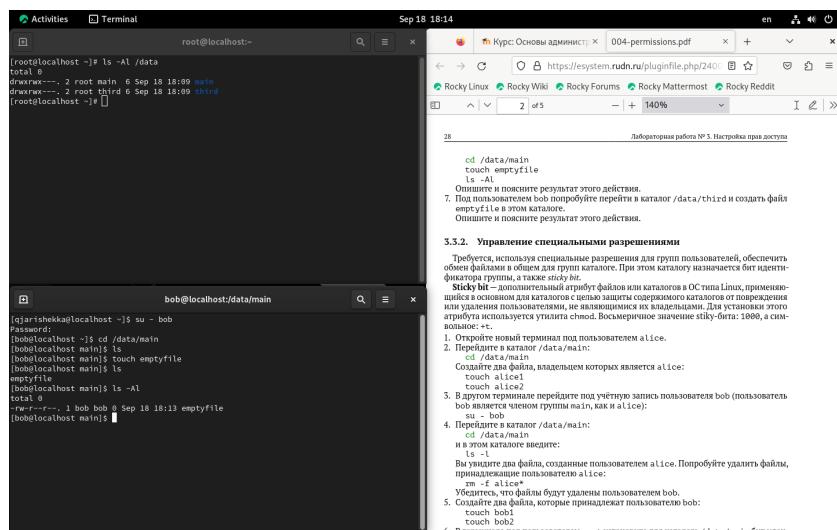


Рис. 4.9: создание каталогов в каталоге main

я смог создать этот файл потому что все в группе main являются владельцами каталога main

Потом я еще раз открыл новый терминал и подключился к учетной записи alice, её пароль - alfa1234 (рис. 4.10).

```
su - alice
```

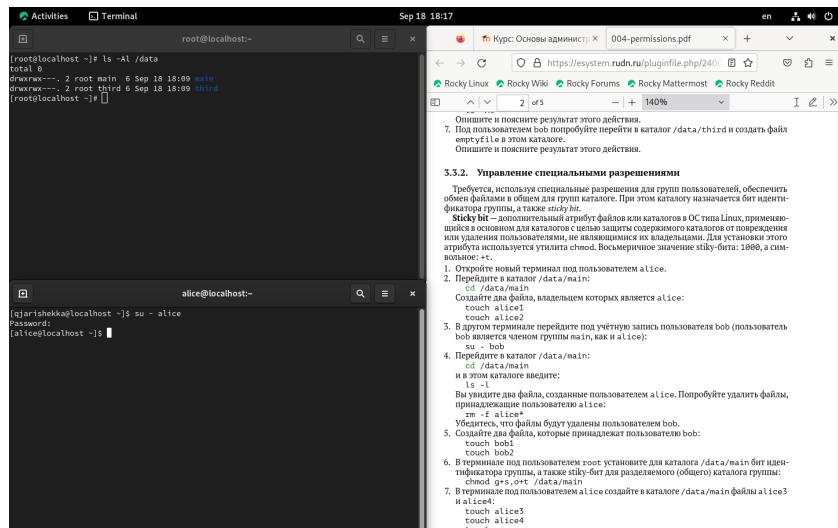


Рис. 4.10: новый терминал

Потом я перешел в каталог /data/main (рис. 4.11).

```
cd /data/main
```

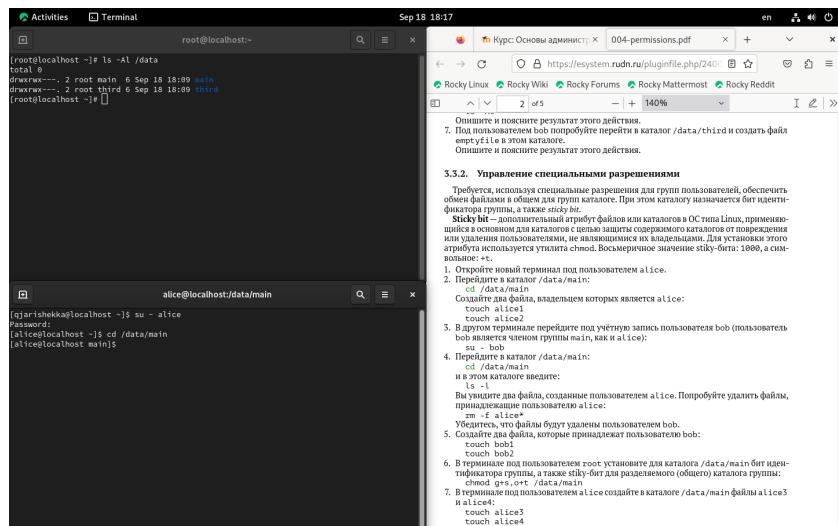


Рис. 4.11: перемещение в каталог cd /data/main

Дальше я создал файлы alice1 и alice2 (рис. 4.12).

```
touch alice1
touch alice2
ls -Al /data/main
```

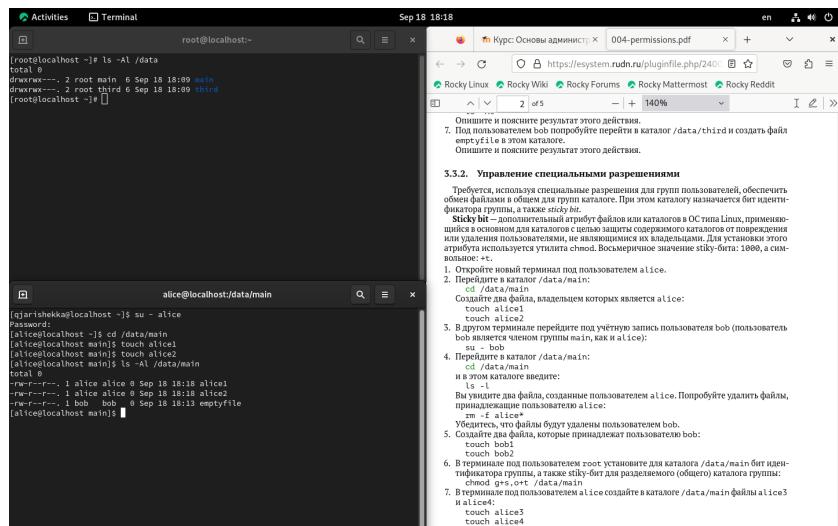


Рис. 4.12: создание файлов

Потом я открыл новый терминал и подключился к учётной записи пользователя bob (рис. 4.13).

```
su - bob
```

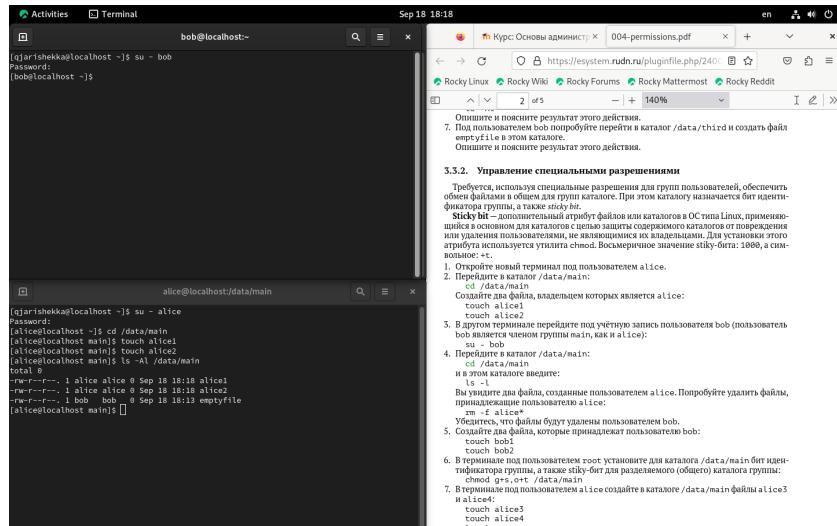


Рис. 4.13: новый терминал с пользователем bob

Дальше я перешел в каталог /data/main (рис. 4.14).

```
cd /data/main
```

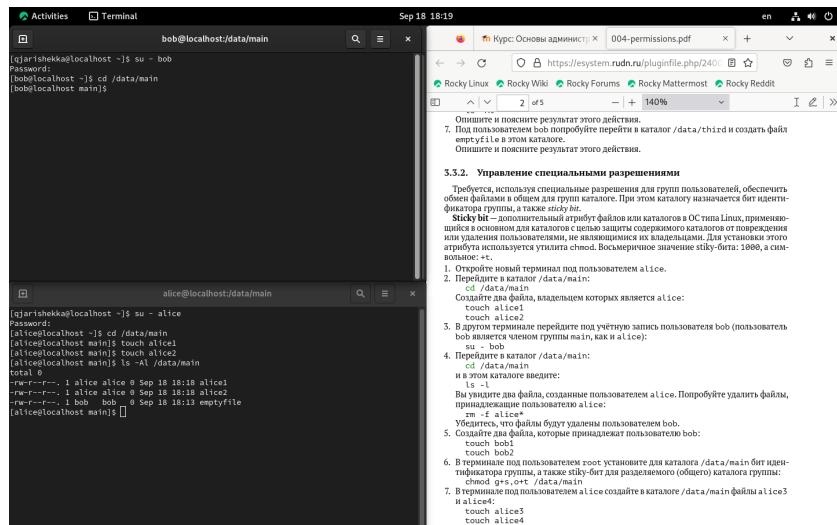


Рис. 4.14: перемещение в каталог data/main

Потом я смотрел какие файлы там находятся (рис. 4.15).

```
ls -l
```

```
bob@localhost:/data/main
[qarishkekka@localhost ~]$ su - bob
Password:
[bob@localhost ~]$ cd /data/main
[bob@localhost main]$ ls -l
total 0
-rw-r--r--, 1 alice alice 0 Sep 18 18:18 alice1
-rw-r--r--, 1 alice alice 0 Sep 18 18:18 alice2
-rw-r--r--, 1 bob bob 0 Sep 18 18:13 emptyfile
[bob@localhost main]$ ls -A /data/main
total 6
-rw-r--r--, 1 alice alice 0 Sep 18 18:18 alice1
-rw-r--r--, 1 alice alice 0 Sep 18 18:18 alice2
-rw-r--r--, 1 bob bob 0 Sep 18 18:13 emptyfile
[alice@localhost main]$ [REDACTED]
```

alice@localhost:/data/main

```
[qarishkekka@localhost ~]$ su - alice
Password:
[alice@localhost ~]$ cd /data/main
[alice@localhost main]$ touch alice1
[alice@localhost main]$ touch alice2
[alice@localhost main]$ ls -A /data/main
total 6
-rw-r--r--, 1 alice alice 0 Sep 18 18:18 alice1
-rw-r--r--, 1 alice alice 0 Sep 18 18:18 alice2
-rw-r--r--, 1 bob bob 0 Sep 18 18:13 emptyfile
[alice@localhost main]$ [REDACTED]
```

Курс: Основы администрирования Rocky Linux | 004-permissions.pdf

3.2. Управление специальными разрешениями

Требуется, используя специальные разрешения для групп пользователей, обеспечить обмен файлами в общем для групп каталоге. При этом каталогу назначается бит индикатора группы, а также sticky-bit.

**sticky-bit** – дополнительный бит доступа к файлам или каталогам в OS типа Linux, применявшийся в основном для каталогов с целью защиты содержимого каталогов от переноса или удаления пользователями, не являющимися их владельцами. Для установки этого битового используется утилита chmod. Восьмёрочное значение sticky-биты: 1000, а символическое: +t.

- Откройте новый терминал под пользователем alice.
- Перейдите в каталог /data/main:  
cd /data/main  
Создайте два файла, владельцем которых является alice:  
touch alice1  
touch alice2
- В другом терминале перейдите под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice):  
su - bob
- Перейдите в каталог /data/main:  
cd /data/main  
и в это каталоге введите:  
ls -l.  
Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие группе, а также sticky-bit для разделенного (общего) каталога группы:
- Убедитесь, что файлы будут удалены пользователем bob:  
rm -f alice1  
touch bob1
- В терминале под пользователем bob установите для каталога /data/main бит индикатора группы, а также sticky-bit для разделенного (общего) каталога группы:  
chmod g+s,ott /data/main
- В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4:  
touch alice3  
touch alice4

Рис. 4.15: просмотр файлов в каталоге /data/main

потом я удалил все файлы пользователя alice (рис. 4.16).

```
rm -f alice*
```

```
bob@localhost:/data/main
[qarishkekka@localhost ~]$ su - bob
Password:
[bob@localhost ~]$ cd /data/main
[bob@localhost main]$ ls -l
total 0
-rw-r--r--, 1 Alice alice 0 Sep 18 18:18 alice1
-rw-r--r--, 1 Alice alice 0 Sep 18 18:18 alice2
-rw-r--r--, 1 bob bob 0 Sep 18 18:13 emptyfile
[bob@localhost main]$ rm -f alice*
[bob@localhost main]$ ls -A /data/main
total 0
-rw-r--r--, 1 bob bob 0 Sep 18 18:13 emptyfile
[bob@localhost main]$ [REDACTED]
```

alice@localhost:/data/main

```
[qarishkekka@localhost ~]$ su - alice
Password:
[alice@localhost ~]$ cd /data/main
[alice@localhost main]$ touch alice1
[alice@localhost main]$ touch alice2
[alice@localhost main]$ ls -A /data/main
total 6
-rw-r--r--, 1 alice alice 0 Sep 18 18:18 alice1
-rw-r--r--, 1 alice alice 0 Sep 18 18:18 alice2
-rw-r--r--, 1 bob bob 0 Sep 18 18:13 emptyfile
[alice@localhost main]$ [REDACTED]
```

Курс: Основы администрирования Rocky Linux | 004-permissions.pdf

3.2. Управление специальными разрешениями

Требуется, используя специальные разрешения для групп пользователей, обеспечить обмен файлами в общем для групп каталоге. При этом каталогу назначается бит индикатора группы, а также sticky-bit.

**sticky-bit** – дополнительный бит доступа к файлам или каталогам в OS типа Linux, применявшийся в основном для каталогов с целью защиты содержимого каталогов от переноса или удаления пользователями, не являющимися их владельцами. Для установки этого битового используется утилита chmod. Восьмёрочное значение sticky-биты: 1000, а символическое: +t.

- Откройте новый терминал под пользователем alice.
- Перейдите в каталог /data/main:  
cd /data/main  
Создайте два файла, владельцем которых является alice:  
touch alice1  
touch alice2
- В другом терминале перейдите под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice):  
su - bob
- Перейдите в каталог /data/main:  
cd /data/main  
и в этом каталоге введите:  
ls.  
Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие группе:
- Убедитесь, что файлы будут удалены пользователем bob:  
rm -f alice1  
touch bob1
- В терминале под пользователем bob установите для каталога /data/main бит индикатора группы, а также sticky-bit для разделенного (общего) каталога группы:  
chmod g+s,ott /data/main
- В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4:  
touch alice3  
touch alice4

Рис. 4.16: удаление файлов

Потом я создал два файла с пользователем bob (bob1 и bob2) (рис. 4.17).

```
touch bob1
```

```
touch bob2
```

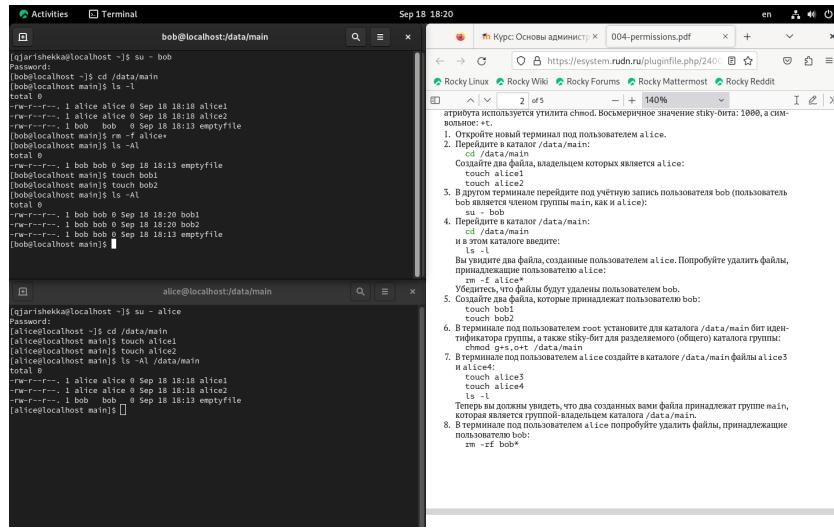


Рис. 4.17: создание файлов bob1 и bob2

ПОТОМ В ТЕРМИНАЛЕ ПОД ПОЛЬЗОВАТЕЛЕМ root я установил бит идентификатора группы для каталога /data/main, а также sticky-bit для разделяемого каталога группы (рис. 4.17).

```
chmod g+s,o+t /data/main
```

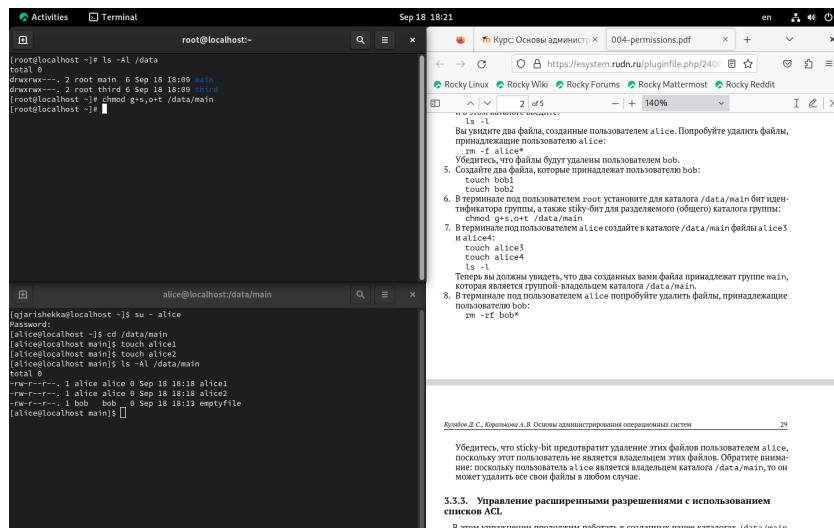


Рис. 4.18: установление каталогов

Потом в терминале под пользователем alice я создал в каталоге /data/main файлы alice3 и alice4 (рис. 4.19).

```
touch alice3
```

```
touch alice4
```

```
ls -l
```

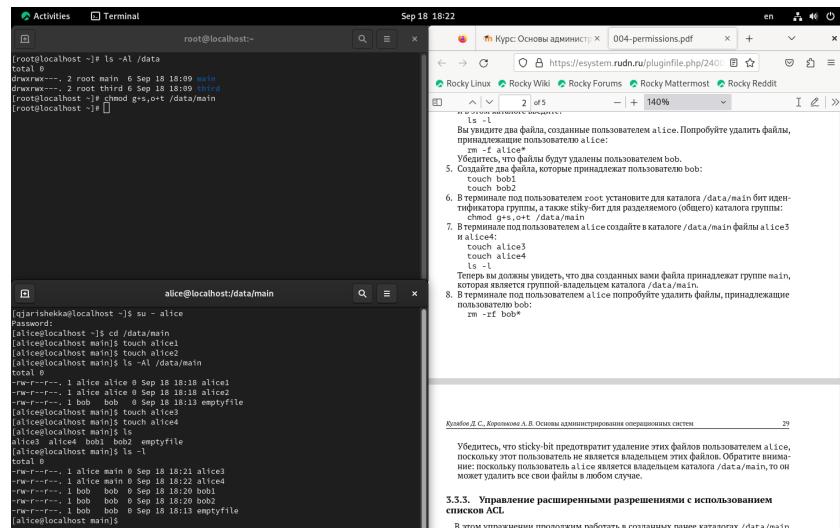


Рис. 4.19: создание файлов alice3 и alice4

Дальше в терминале под пользователем alice я попробовал удалить файлы bob1 и bob2 (рис. 4.20).

```
rm -rf bob*
```

```

[alice@localhost main]$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Sep 18 18:22 alicex3
-rw-r--r--. 1 alice main 0 Sep 18 18:22 alicex4
-rw-r--r--. 1 bob  bob  0 Sep 18 18:20 bob1
-rw-r--r--. 1 bob  bob  0 Sep 18 18:20 bob2
-rw-r--r--. 1 bob  bob  0 Sep 18 18:19 emptyfile
[alice@localhost main]$ rm -f bob1
rm: cannot remove 'bob1': Operation not permitted
[alice@localhost main]$ rm -f bob2
rm: cannot remove 'bob2': Operation not permitted
[alice@localhost main]$

```

Лабораторная работа №3. Настройка прав доступа

Рис. 4.20: удаление файлов

конечно это действие запрещено потому что у alica нет доступа на эти файлы

Потом еще раз в терминале под пользователем root я установил 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 (рис. 4.21).

```

setfacl -m g:third:rx /data/main
setfacl -m g:main:rx /data/third

```

```

[alice@localhost main]$ setfacl -m g:third:rx /data/main
[alice@localhost main]$ setfacl -m g:main:rx /data/third
[alice@localhost main]$

[alice@localhost main]$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Sep 18 18:22 alicex3
-rw-r--r--. 1 alice main 0 Sep 18 18:22 alicex4
-rw-r--r--. 1 bob  bob  0 Sep 18 18:20 bob1
-rw-r--r--. 1 bob  bob  0 Sep 18 18:20 bob2
-rw-r--r--. 1 bob  bob  0 Sep 18 18:19 emptyfile
[alice@localhost main]$ rm -f bob1
rm: cannot remove 'bob1': Operation not permitted
[alice@localhost main]$ rm -f bob2
rm: cannot remove 'bob2': Operation not permitted
[alice@localhost main]$

```

Лабораторная работа №3. Настройка прав доступа

Рис. 4.21: установление прав

Потом я создал файл newfile1 в каталоге /data/main (рис. 4.22).

```
touch /data/main/newfile1
```

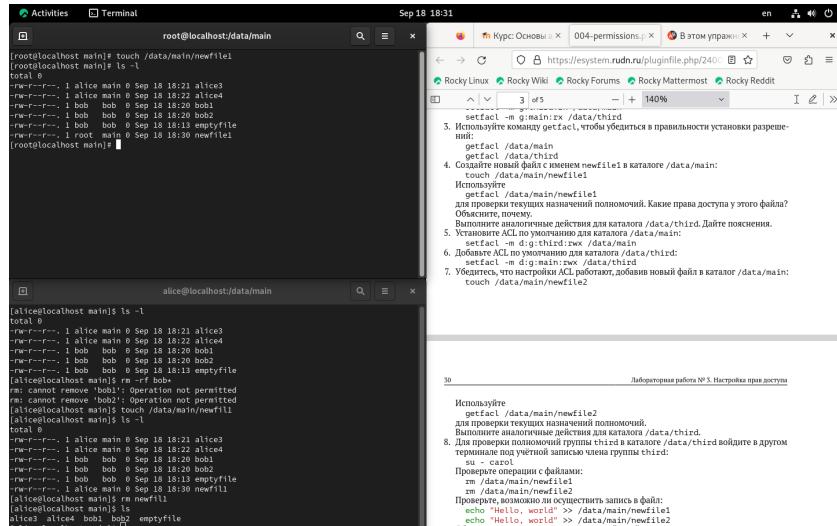


Рис. 4.22: создание файла newfile1

Потом я проверял текущие назначения полномочий (рис. 4.23).

```
getfacl /data/main/newfile1
```

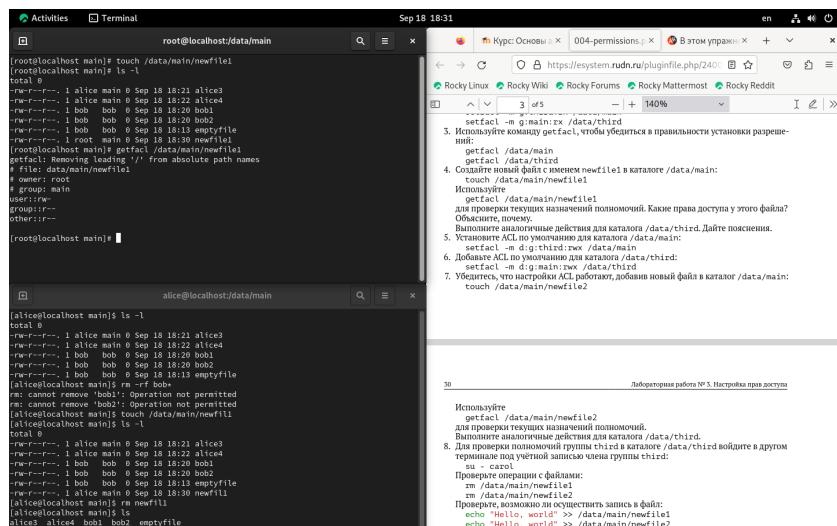


Рис. 4.23: проверка текущих назначений полномочий

Потом я повторил действие в каталоге third (рис. 4.24).

```
touch /data/main/newfile1
getfacl /data/main/newfile1
```

The terminal window shows the following session:

```
[root@localhost main]# touch /data/main/newfile1
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile1
# owner: root
# group: main
user::rwx
group::r--
other::r--
[root@localhost main]# cd /data/third
[root@localhost third]# touch /data/third/newfile2
touch: cannot touch '/data/third/newfile2': No such file or directory
[root@localhost third]# getfacl /data/third/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile2
# owner: root
# group: root
user::rwx
group::r--
other::r--
[root@localhost third]# [alice@localhost main]$ ls -l
total 8
-rw-r--r--, 1 alice main 0 Sep 18 18:22 alice3
-rw-r--r--, 1 alice main 0 Sep 18 18:22 alice4
-rw-r--r--, 1 bob  bob 0 Sep 18 18:20 bob1
-rw-r--r--, 1 bob  bob 0 Sep 18 18:20 bob2
-rw-r--r--, 1 bob  bob 0 Sep 18 18:13 emptyfile
[alice@localhost main]$ rm -rf bob*
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
[alice@localhost main]$ touch /data/main/newfile1
[alice@localhost main]$ ls -l
total 8
-rw-r--r--, 1 alice main 0 Sep 18 18:22 alice3
-rw-r--r--, 1 alice main 0 Sep 18 18:22 alice4
-rw-r--r--, 1 bob  bob 0 Sep 18 18:20 bob1
-rw-r--r--, 1 bob  bob 0 Sep 18 18:20 bob2
-rw-r--r--, 1 bob  bob 0 Sep 18 18:13 emptyfile
-rw-r--r--, 1 bob  bob 0 Sep 18 18:30 newfile1
[alice@localhost main]$ ls
alice3 alice4 bob1 bob2 emptyfile
```

The help window contains the following text:

Лабораторная работа №3. Настройка прав доступа

Используйте  
getfacl /data/main/newfile1  
для проверки текущих назначенных полномочий.

Выполните аналогичные действия для каталога /data/third.

3. Используйте команду getfacl, чтобы убедиться в правильности установки разрешений.

4. Создайте новый файл с именем newfile1 в каталоге /data/main:  
touch /data/main/newfile1

Используйте  
getfacl /data/main/newfile1  
для проверки текущих назначенных полномочий. Какие права доступа у этого файла? Объясните, почему.

Выполните аналогичные действия для каталога /data/third. Дайте пояснения.

5. Установите ACL по умолчанию для каталога /data/main:  
setfacl -m d:g:third:rwx /data/main

6. Добавьте ACL по умолчанию для каталога /data/third:  
setfacl -m d:g:main:rwx /data/third

7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main:  
touch /data/main/newfile2

Рис. 4.24: Повторение предыдущих шагов

Потом я установил ACL по умолчанию для каталога /data/main (рис. 4.25).

```
setfacl -m d:g:third:rwx /data/main
```

The terminal window shows the following session:

```
[root@localhost main]# setfacl -m d:g:third:rwx /data/main
[root@localhost main]# [alice@localhost main]$ ls -l
total 8
-rw-r--r--, 1 alice main 0 Sep 18 18:22 alice3
-rw-r--r--, 1 alice main 0 Sep 18 18:22 alice4
-rw-r--r--, 1 bob  bob 0 Sep 18 18:20 bob1
-rw-r--r--, 1 bob  bob 0 Sep 18 18:20 bob2
-rw-r--r--, 1 bob  bob 0 Sep 18 18:13 emptyfile
[alice@localhost main]$ rm -rf bob*
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
[alice@localhost main]$ touch /data/main/newfile1
[alice@localhost main]$ ls -l
total 8
-rw-r--r--, 1 alice main 0 Sep 18 18:22 alice3
-rw-r--r--, 1 alice main 0 Sep 18 18:22 alice4
-rw-r--r--, 1 bob  bob 0 Sep 18 18:20 bob1
-rw-r--r--, 1 bob  bob 0 Sep 18 18:20 bob2
-rw-r--r--, 1 bob  bob 0 Sep 18 18:13 emptyfile
-rw-r--r--, 1 bob  bob 0 Sep 18 18:30 newfile1
[alice@localhost main]$ ls
alice3 alice4 bob1 bob2 emptyfile
```

The help window contains the following text:

Лабораторная работа №3. Настройка прав доступа

Используйте  
getfacl /data/main/newfile2  
для проверки текущих назначенных полномочий.

Выполните аналогичные действия для каталога /data/third.

3. Используйте команду getfacl, чтобы убедиться в правильности установки разрешений.

4. Создайте новый файл с именем newfile1 в каталоге /data/main:  
touch /data/main/newfile1

Используйте  
getfacl /data/main/newfile1  
для проверки текущих назначенных полномочий. Какие права доступа у этого файла? Объясните, почему.

Выполните аналогичные действия для каталога /data/third. Дайте пояснения.

5. Установите ACL по умолчанию для каталога /data/main:  
setfacl -m d:g:third:rwx /data/main

6. Добавьте ACL по умолчанию для каталога /data/third:  
setfacl -m d:g:main:rwx /data/third

7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main:  
touch /data/main/newfile2

Прикрепите файлы:  
rm /data/main/newfile1  
rm /data/main/newfile2

Проверьте, возможно ли осуществить запись в файл:  
echo "Hello, world" >> /data/main/newfile1  
echo "Hello, world" >> /data/main/newfile2

Рис. 4.25: установление ACL

Дальше установил ACL для каталога /data/third (рис. 4.26).

```
setfacl -m d:g:main:rwx /data/third
```

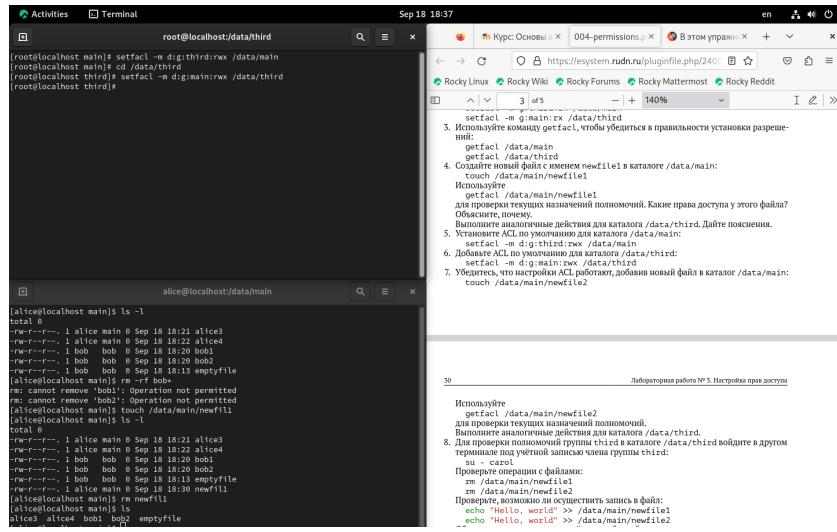


Рис. 4.26: установление ACL

Потом я создал файл newfile2 в каталоге /data/main

```
touch /data/main/newfile2
```

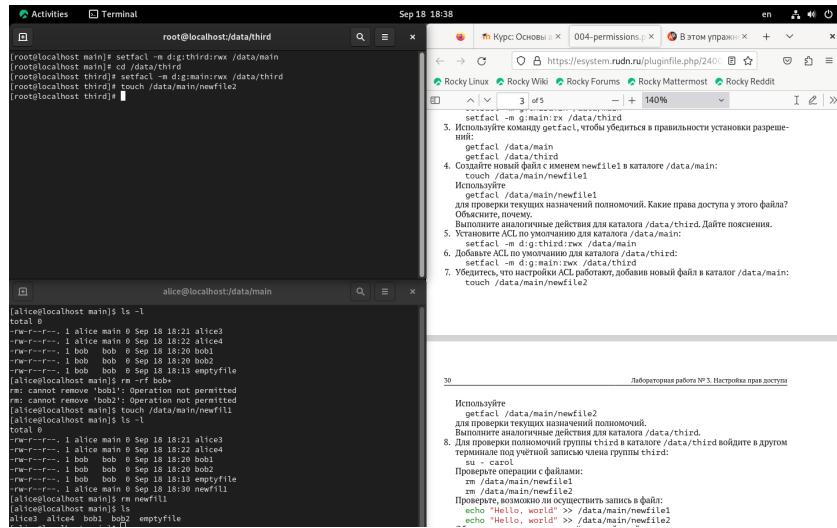
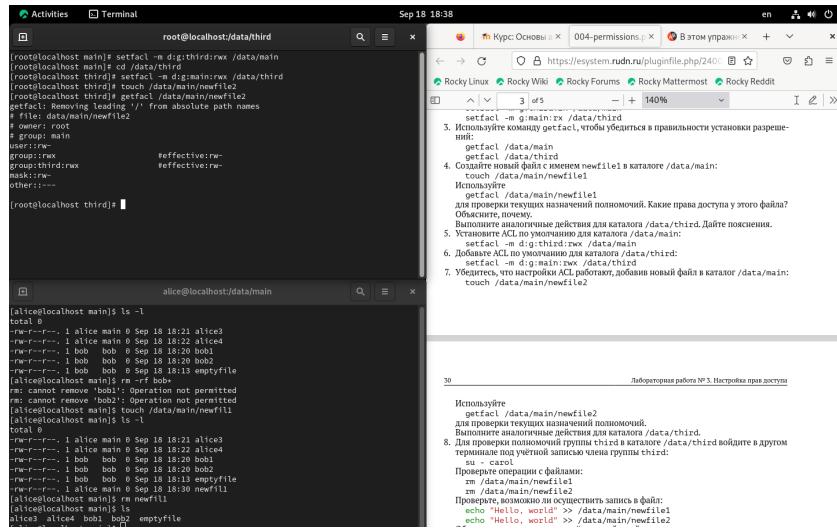


Рис. 4.27: создание файла newfile2

И использовал getfacl для проверки (рис. 4.28).

```
getfacl /data/main/newfile2
```



```
root@localhost main# getfacl -m dig:third:rwx /data/main
[root@localhost main]# cd /data/third
[root@localhost third]# setfacl -m dig:main:rwx /data/third
[root@localhost third]# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root
# group: main
user::rwx
group::rwx
mask::rwx
other::---
[root@localhost third]# 

[alice@localhost main]$ ls -l
total 0
-rw-r--r-- 1 alice main 0 Sep 18 18:22 alice3
-rw-r--r-- 1 bob bob 0 Sep 18 18:22 bob1
-rw-r--r-- 1 bob bob 0 Sep 18 18:20 bob2
-rw-r--r-- 1 bob bob 0 Sep 18 18:18 bob3
-rw-r--r-- 1 bob bob 0 Sep 18 18:13 emptyfile
[root@localhost main]$ rm newfile1
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
rm: cannot remove 'bob3': Operation not permitted
[alice@localhost main]$ touch /data/main/newfile1
[alice@localhost main]$ ls
alice3 bob1 bob2 emptyfile
[alice@localhost main]$ ls -l
total 0
-rw-r--r-- 1 alice main 0 Sep 18 18:22 alice3
-rw-r--r-- 1 alice main 0 Sep 18 18:22 alice4
-rw-r--r-- 1 bob bob 0 Sep 18 18:20 bob1
-rw-r--r-- 1 bob bob 0 Sep 18 18:20 bob2
-rw-r--r-- 1 bob bob 0 Sep 18 18:13 emptyfile
[root@localhost main]$ rm newfile1
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
[alice@localhost main]$ touch /data/main/newfile1
[alice@localhost main]$ ls
alice3 bob1 bob2 emptyfile
```

Курс: Основы | 004-permissions.php | В этом упражнении | + | - | 140% | | |

3. Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:

```
getfacl /data/main
# file: data/main
# owner: root
# group: main
group::rwx
#effective:rwx
mask::rwx
other::---
```

4. Создайте новый файл с именем newfile1 в каталоге /data/main:

```
touch /data/main/newfile1
Используйте команду getfacl для проверки текущих назначений разрешений. Какие права доступа у этого файла?
```

Обратите внимание на то, что права доступа к файлу newfile1 были изменены.

5. Установите ACL по умолчанию для каталога /data/main:

```
setfacl -m d:g:third:rwx /data/main
```

6. Добавьте новый файл newfile2 в каталог /data/main:

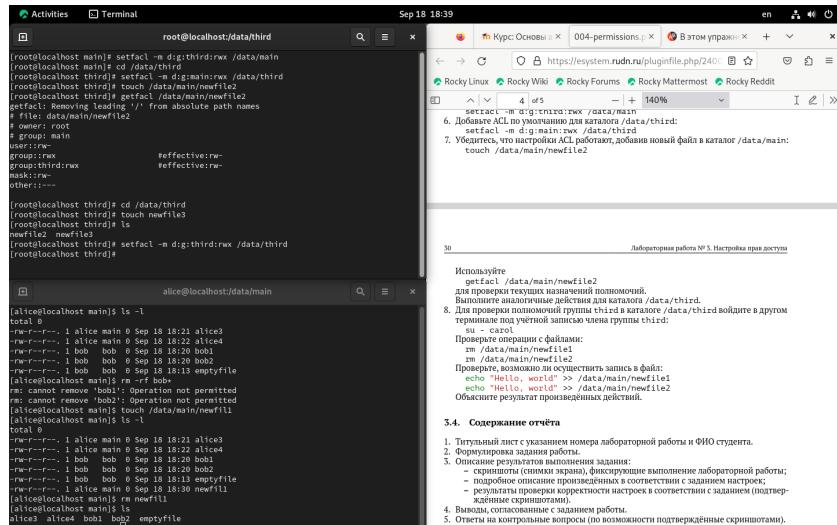
```
touch /data/main/newfile2
```

7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main:

```
touch /data/main/newfile2
```

Рис. 4.28: проверка файла newfile2

Потом я сделал еще раз те действия для каталога data/third (рис. 4.29) (рис. 4.30).



```
root@localhost main# setfacl -m dig:third:rwx /data/main
[root@localhost main]# cd /data/third
[root@localhost third]# setfacl -m dig:main:rwx /data/third
[root@localhost third]# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root
# group: main
user::rwx
group::rwx
mask::rwx
other::---
[root@localhost third]# cd /data/third
[root@localhost third]# touch newfile3
[root@localhost third]# ls
newfile2 newfile3
[root@localhost third]# setfacl -m d:g:third:rwx /data/third
[root@localhost third]# 

[alice@localhost main]$ ls -l
total 0
-rw-r--r-- 1 alice main 0 Sep 18 18:22 alice3
-rw-r--r-- 1 alice main 0 Sep 18 18:22 alice4
-rw-r--r-- 1 bob bob 0 Sep 18 18:20 bob1
-rw-r--r-- 1 bob bob 0 Sep 18 18:20 bob2
-rw-r--r-- 1 bob bob 0 Sep 18 18:13 emptyfile
[root@localhost main]$ rm newfile1
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
rm: cannot remove 'bob3': Operation not permitted
[alice@localhost main]$ touch /data/main/newfile1
[alice@localhost main]$ ls
alice3 bob1 bob2 emptyfile
[alice@localhost main]$ ls -l
total 0
-rw-r--r-- 1 alice main 0 Sep 18 18:22 alice3
-rw-r--r-- 1 alice main 0 Sep 18 18:22 alice4
-rw-r--r-- 1 bob bob 0 Sep 18 18:20 bob1
-rw-r--r-- 1 bob bob 0 Sep 18 18:20 bob2
-rw-r--r-- 1 bob bob 0 Sep 18 18:13 emptyfile
[root@localhost main]$ rm newfile1
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
[alice@localhost main]$ touch /data/main/newfile1
[alice@localhost main]$ ls
alice3 bob1 bob2 emptyfile
```

Курс: Основы | 004-permissions.php | В этом упражнении | + | - | 140% | | |

3. Используйте команду getfacl /data/main/newfile2 для проверки текущих назначений разрешений. Выполните аналогичные действия для каталога /data/third.

8. Для проверки полномочий группы third в каталоге /data/third войдите в другой терминал под учётной записью члена группы third:

```
su - caro
```

Проверьте операции с файлами:

```
rm /data/main/newfile1
rm /data/main/newfile2
```

Проверьте, возможно ли осуществлять запись в файл:

```
echo "Hello, world" >> /data/main/newfile1
echo "Hello, world" >> /data/main/newfile2
```

Обратите внимание на то, что права доступа к файлам изменились.

3.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результата выполнения задания:
  - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
  - описание полученных результатов в соответствии с заданным инструкцией;
  - результаты проверки корректности настроек в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласование с заданием работы.
5. Ответы на контрольные вопросы (по возможности подтверждённые скриншотами).

Рис. 4.29: создание файла newfile3

The terminal window shows the following command history:

```

root@localhost third# cd /data/third
[root@localhost third]# touch newfile3
[root@localhost third]# ls
newfile2 newfile3
[root@localhost third]# getfacl -m g::>rwX /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile3
# owner: root
# group: root
user::rwx
group::rwx      #effective:rwx
group:main:rwx  #effective:rwx
mask::rwx
other::rwx
[root@localhost third]#
[root@localhost main]$ ls -l
total 0
-rw-r--r-- 1 Alice main 0 Sep 18 18:22 alice3
-rw-r--r-- 1 Alice main 0 Sep 18 18:22 bob1
-rw-r--r-- 1 Bob  bob 0 Sep 18 18:20 bob2
-rw-r--r-- 1 Bob  bob 0 Sep 18 18:20 bob3
-rw-r--r-- 1 Bob  bob 0 Sep 18 18:19 emptyfile
[root@localhost main]$ rm bob1
rm: cannot remove 'bob1': Operation not permitted
[root@localhost main]$ rm bob2
rm: cannot remove 'bob2': Operation not permitted
[root@localhost main]$ touch /data/main/newfile1
[root@localhost main]$ ls
alice3 alice bob1 emptyfile

```

The browser window displays the following lab instructions:

- Используйте `getfacl -m g::>rwX /data/main/newfile2` для проверки текущих назначений полномочий.
- Выполните аналогичные действия для каталога `/data/third`.
- Добавьте ACL по умолчанию для каталога `/data/main`:

```

setfacl -m g::main:rwx /data/main

```

Рис. 4.30: проверка файла newfile3

Потом я подключился к учётной записи пользователя carol (пароль - gama1234) (рис. 4.31).

`su - carol`

The terminal window shows the following command history:

```

root@localhost third# setfacl -m g::main:rwx /data/third
[root@localhost third]# getfacl -m g::>rwX /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile3
# owner: root
# group: root
user::rwx
group::rwx      #effective:rwx
group:main:rwx  #effective:rwx
mask::rwx
other::rwx
[root@localhost third]#
[root@localhost main]$ su - bob
Password:
[bob@localhost ~]$ cd /data/main
[bob@localhost main]$ ls -l
total 0
-rw-r--r-- 1 Alice alice 0 Sep 18 18:18 alice1
-rw-r--r-- 1 Alice alice 0 Sep 18 18:18 alice2
-rw-r--r-- 1 Bob  bob 0 Sep 18 18:13 emptyfile
[bob@localhost main]$ rm -f alice1
[bob@localhost main]$ ls -l
total 0
-rw-r--r-- 1 Bob  bob 0 Sep 18 18:13 emptyfile
[bob@localhost main]$ touch bob1
[bob@localhost main]$ ls -l
total 0
-rw-r--r-- 1 Bob  bob 0 Sep 18 18:20 bob1
-rw-r--r-- 1 Bob  bob 0 Sep 18 18:20 bob2
-rw-r--r-- 1 Bob  bob 0 Sep 18 18:13 emptyfile
[bob@localhost main]$ su - carol
Password:
[carol@localhost ~]$

```

The browser window displays the following lab instructions:

- Титульный лист с указанием номера лабораторной работы и ФИО студента.
- Формализация задания работы.
- Описание результатов выполнения задания:
  - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
  - подтверждение правильности настроек в соответствии с заданием (подтверждённые скриншотами);
- Выходы, согласованные с заданием работы.
- Ответы на контрольные вопросы (по возможности подтверждённые скриншотами).

Рис. 4.31: поключение к учётной записи пользователя carol

Потом я попробовал удалить файлы newfile 1 и newfile2 (рис. 4.32).

```

rm /data/main/newfile1
rm /data/main/newfile2

```

```

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

```

Лабораторная работа №3. Настройка прав доступа

Используйте:

```

getfacl /data/main/newfile2

```

для проверки текущих назначений полномочий.

Выполните аналогичные действия для каталога /data/third.

8. Для проверки полномочий группы third в каталоге /data/third войдите в другой терминал под учётной записью члена группы third:

- su - carol
- Проделайте операции с файлами:

```

rm /data/main/newfile1
rm /data/main/newfile2

```

- Проверьте, возможно ли осуществить запись в файл:

```

echo "Hello, world" >> /data/main/newfile1
echo "Hello, world" >> /data/main/newfile2

```

- Объясните результат произведённых действий.

3.4. Содержание отчёта

- Титульный лист с указанием номера лабораторной работы и ФИО студента.
- Формулировка задания работы.
- Описание результатов выполнения задания:
  - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
  - подробное описание произведённых действий в соответствии с заданием настройки;
  - результаты проверки корректности настроек в соответствии с заданием (подтверждённые скриншотами).
- Выходы, согласованные с заданием работы.
- Ответы на контрольные вопросы (по возможности подтверждённые скриншотами).

Рис. 4.32: удаление файлов

Потом я попробовал другую команду в терминале (рис. 4.33).

```

[carol@localhost ~]$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1'? y
rm: cannot remove '/data/main/newfile1': Permission denied
[carol@localhost ~]$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
[carol@localhost ~]$ echo "Hello, world" >> /data/main/newfile1
-bash: /data/main/newfile1: Permission denied
[carol@localhost ~]$ echo "Hello, world" >> /data/main/newfile2
[carol@localhost ~]$

```

Лабораторная работа №3. Настройка прав доступа

Используйте:

```

getfacl /data/main/newfile2

```

для проверки текущих назначений полномочий.

Выполните аналогичные действия для каталога /data/third.

8. Для проверки полномочий группы third в каталоге /data/third войдите в другой терминал под учётной записью члена группы third:

- su - carol
- Проделайте операции с файлами:

```

rm /data/main/newfile1
rm /data/main/newfile2

```

- Проверьте, возможно ли осуществить запись в файл:

```

echo "Hello, world" >> /data/main/newfile1
echo "Hello, world" >> /data/main/newfile2

```

- Объясните результат произведённых действий.

3.4. Содержание отчёта

- Титульный лист с указанием номера лабораторной работы и ФИО студента.
- Формулировка задания работы.
- Описание результатов выполнения задания:
  - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
  - подробное описание произведённых действий в соответствии с заданием настройки;
  - результаты проверки корректности настроек в соответствии с заданием (подтверждённые скриншотами).
- Выходы, согласованные с заданием работы.
- Ответы на контрольные вопросы (по возможности подтверждённые скриншотами).

Рис. 4.33: echo

пользователь carol не может изменять ничего в каталогах потому что у неё нет доступа

Контрольные вопросы 1. Как следует использовать команду chown, чтобы установить владельца группы для файла? Приведите пример.

- С помощью какой команды можно найти все файлы, принадлежащие конкретному пользователю? Приведите пример.

3. Как применить разрешения на чтение, запись и выполнение для всех файлов в каталоге /data для пользователей и владельцев групп, не устанавливая никаких прав для других? Приведите пример.
4. Какая команда позволяет добавить разрешение на выполнение для файла, который необходимо сделать исполняемым?
5. Какая команда позволяет убедиться, что групповые разрешения для всех новых файлов, создаваемых в каталоге, будут присвоены владельцу группы этого каталога? Приведите пример.
6. Необходимо, чтобы пользователи могли удалять только те файлы, владельцами которых они являются, или которые находятся в каталоге, владельцами которого они являются. С помощью какой команды можно это сделать? Приведите пример.
7. Какая команда добавляет ACL, который предоставляет членам группы права доступа на чтение для всех существующих файлов в текущем каталоге?
8. Что нужно сделать для гарантии того, что члены группы получат разрешения на чтение для всех файлов в текущем каталоге и во всех его подкаталогах, а также для всех файлов, которые будут созданы в этом каталоге в будущем? Приведите пример.
9. Какое значение umask нужно установить, чтобы «другие» пользователи не получали какие-либо разрешения на новые файлы? Приведите пример

## **5 Выводы**

В этой лабораторной работе мы смотрели как работать с другими пользователями, как давать им права доступа используя их группы. также мы смотрели как использовать другие команды как setfacl, getfacl

## **Список литературы**

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.
2. Robbins A. Bash Pocket Reference. O'Reilly Media, 2016. 156 с.
3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.
4. Newham C. Learning the bash Shell: Unix Shell Programming. O'Reilly Media, 2005. 354 с.