

Настройка прав доступа

Лабораторная работа № 3

Глобин Никита Анатольевич

Содержание

1 Цель работы	5
2 Задание	6
3 Теоретическое введение	7
4 Выполнение лабораторной работы	8
5 Управление базовыми разрешениями	9
6 Управление специальными разрешениями	14
7 Управление расширенными разрешениями с использованием списков ACL	19
8 Контрольные вопросы	24
9 Выводы	26

Список иллюстраций

5.1	1	9
5.2	2	10
5.3	3	10
5.4	4	11
5.5	5	11
5.6	6	12
5.7	7	12
5.8	8	13
5.9	9	13
6.1	10	14
6.2	11	15
6.3	12	15
6.4	13	16
6.5	14	16
6.6	15	17
6.7	16	17
6.8	17	18
6.9	18	18
7.1	19	19
7.2	20	20
7.3	21	20
7.4	22	21
7.5	23	21
7.6	24	22
7.7	25	22
7.8	26	23
7.9	27	23

Список таблиц

1 Цель работы

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

2 Задание

1. Выполните действия по управлению базовыми разрешениями для групп пользователей
2. Выполните действия по управлению специальными разрешениями для групп пользователей
3. Выполните действия по управлению расширенными разрешениями с использованием списков ACL для групп пользователей
4. Контрольные вопросы

3 Теоретическое введение

4 Выполнение лабораторной работы

5 Управление базовыми разрешениями

1. Откроем терминал с учётной записью root (рис. 5.1).

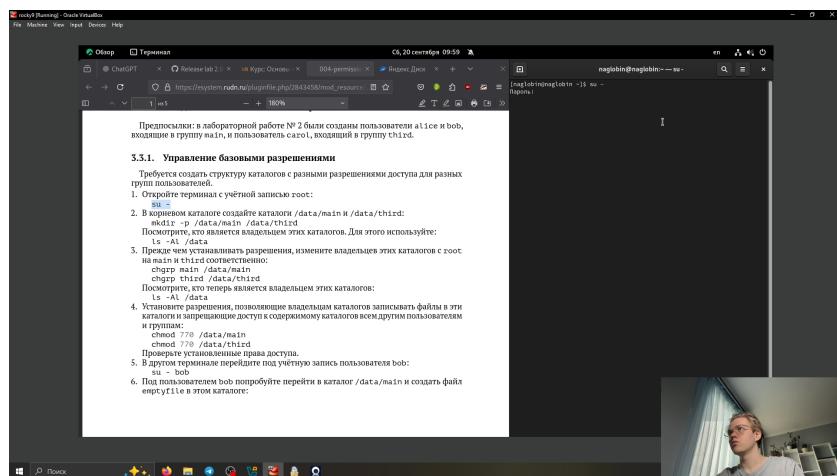


Рис. 5.1: 1

2. В корневом каталоге создаем каталоги /data/main и /data/third (рис. 5.2) (рис. 5.3).

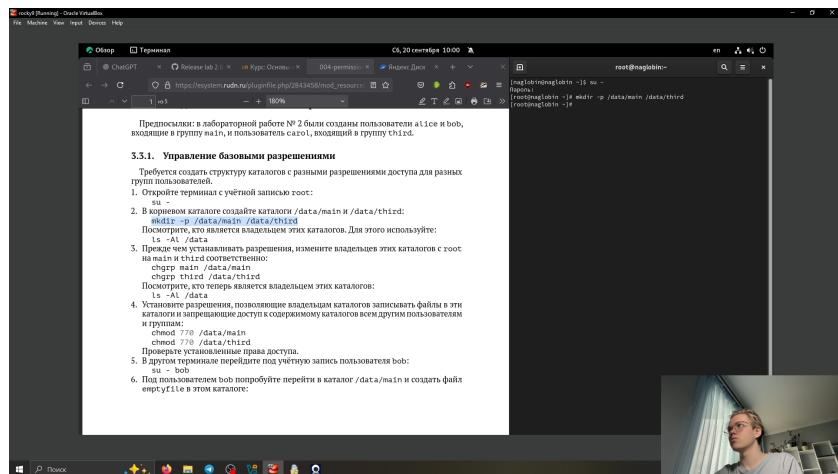


Рис. 5.2: 2

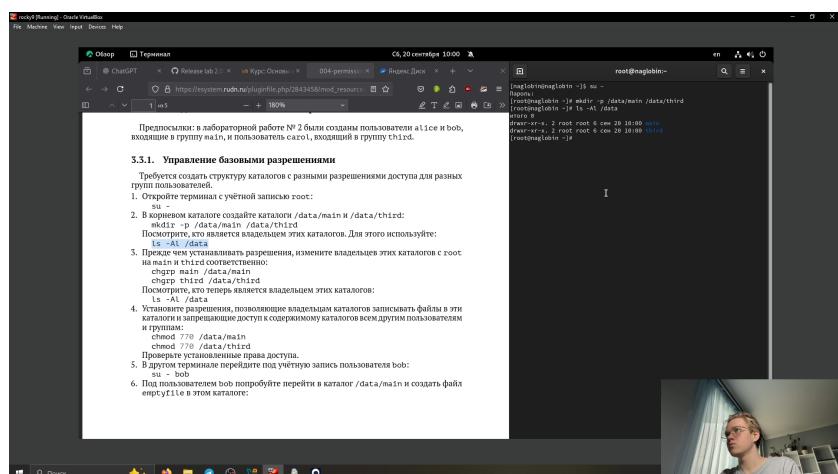


Рис. 5.3: 3

3. Прежде чем устанавливать разрешения, изменим владельцев этих каталогов с root на main и third соответственно (рис. 5.4)

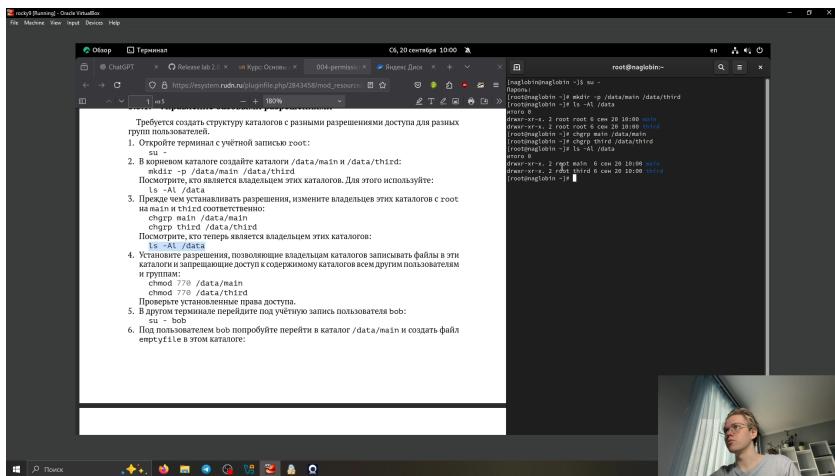


Рис. 5.4: 4

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

1. В корневом каталоге создайте каталоги /data/main и /data/third:
2. В корневом каталоге создайте каталоги /data/main и /data/third:
и создайте файл emptyfile в каталоге /data/main.
- Посмотрите, кто является владельцем этих каталогов. Для этого используйте:
`ls -Al .data`
3. Проверьте, изменяют ли разрешения, измените владельца этих каталогов с root на main и third соответственно:
сдирп main /data/main
сдирп third /data/third
- Посмотрите, кто теперь является владельцем этих каталогов:
`ls -Al .data`
4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:
смод 770 /data/main
смод 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.

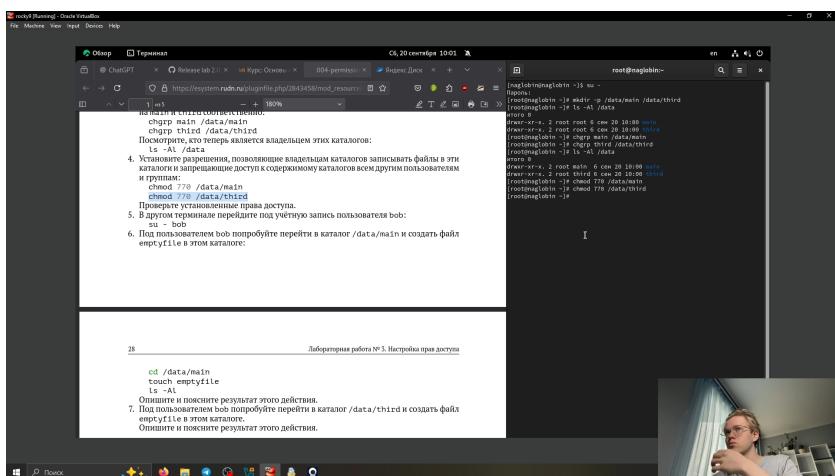


Рис. 5.5: 5

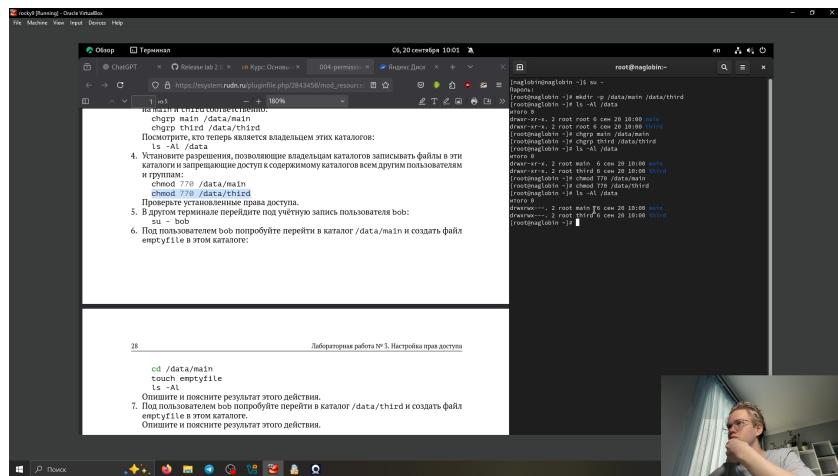


Рис. 5.6: 6

5. В другом терминале перейдем под учётную запись пользователя bob (рис. 5.7)

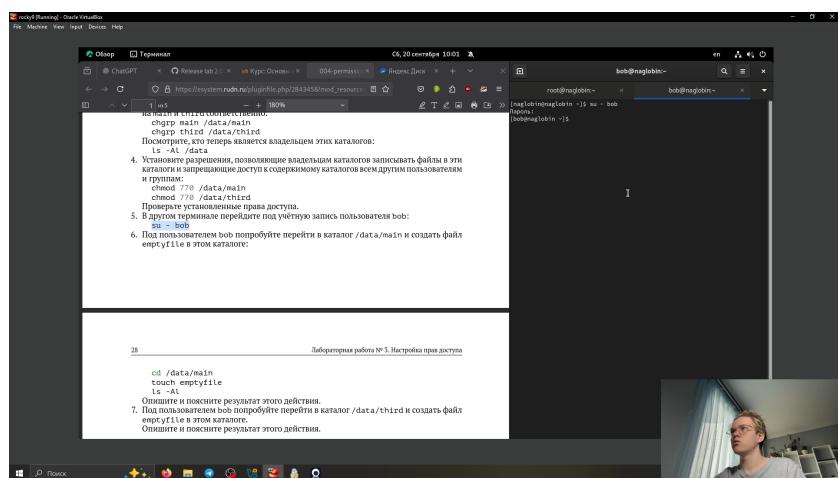


Рис. 5.7: 7

6. Под пользователем bob попробуем перейти в каталог /data/main и создать файл emptyfile в этом каталоге (рис. 5.8)

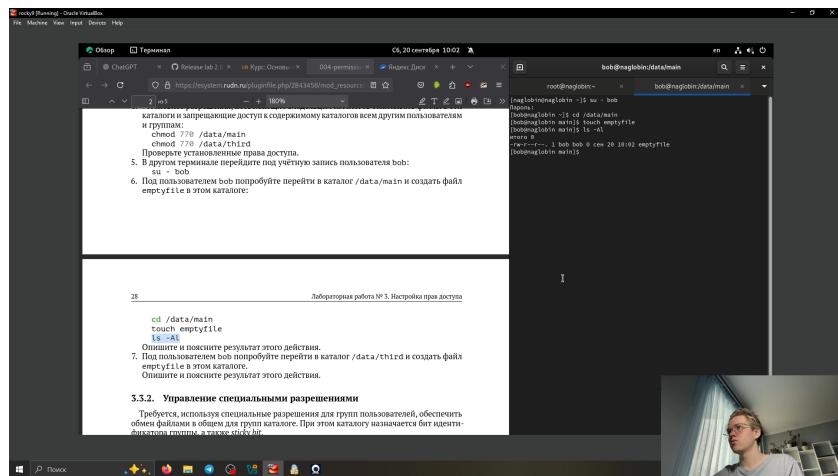


Рис. 5.8: 8

Мы видим время создания файла, автора и группу которые имеют к нему доступ. Так же нам видны права на файл: чтения и письмо.

7. Под пользователем bob попробуем перейти в каталог /data/third и создать файл emptyfile в этом каталоге (рис. 5.9)

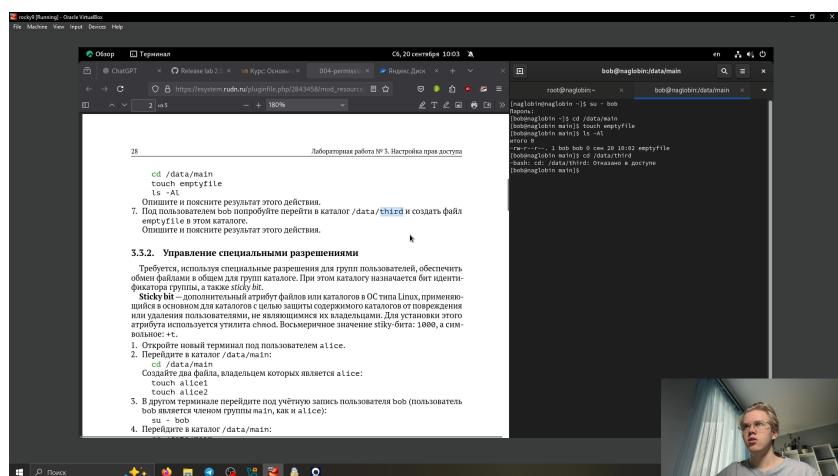


Рис. 5.9: 9

Bob входит в другую группу поэтому у него нет прав на взаимодействие с этим котологом.

6 Управление специальными разрешениями

1. Откроем новый терминал под пользователем alice (рис. 6.1)

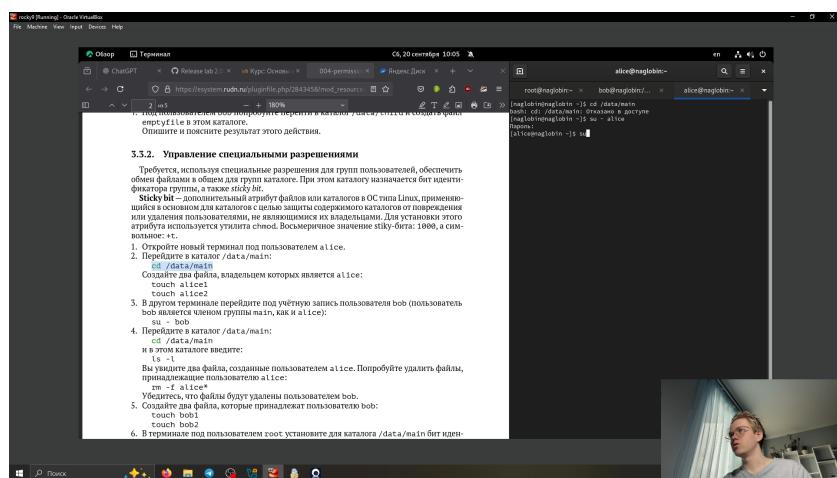


Рис. 6.1: 10

2. Перейдем в каталог /data/main (рис. 6.2)

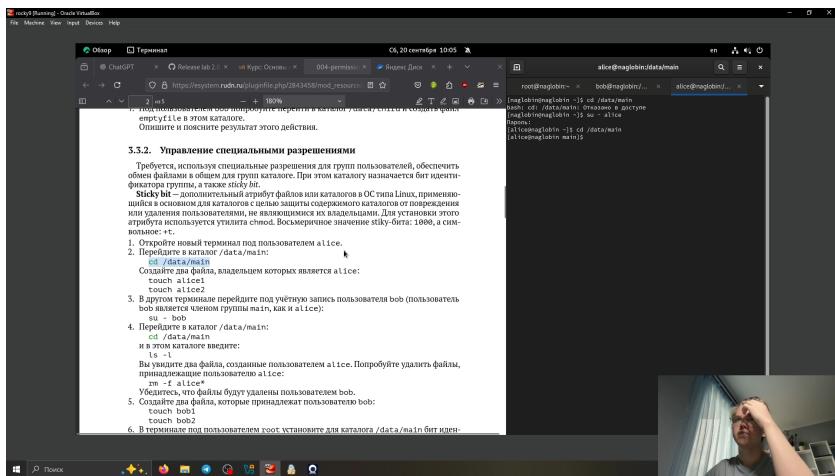


Рис. 6.2: 11

Создем два файла, владельцем которых является alice (рис. 6.3)

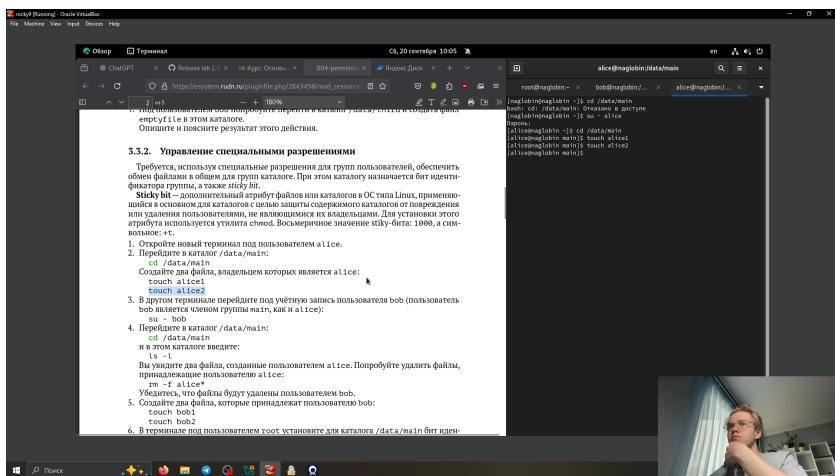


Рис. 6.3: 12

3. В другом терминале перейдем под учётную запись пользователя bob (рис. 6.4)

```

    Требуется использовать специальные разрешения для групп пользователей, обеспечивающие файлами в общем для групп каталоге. При этом каталог называется битом идентификатора группы, а также sticky bit.

    Sticky bit — это бит, который запрещает файлы или каталоги в ОС типа Linux, присоединенные к основному для каталога с целью защиты содержимого каталога от повреждения или удаления пользователями, не являющимися их владельцами. Для установки этого атрибута используется утилита chmod. Восьмизначное значение sticky-биты: 16000, а символическое: +t.

    1. Откройте новый терминал под пользователем alice.
    2. Перейдите в каталог /data/main:
        cd /data/main
        Создайте два файла, владельцем которых является alice:
        touch alice1
        touch alice2
    3. В другом терминале перейдите под учётную запись пользователя bob (пользователь bob имеет членом группы main, как и alice):
        su bob
    4. Перейдите в каталог /data/main:
        cd /data/main
        Из текущего каталога выведите:
        ls -l
        Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:
        rm -f alice*
        Убедитесь, что файлы будут удалены пользователем bob:
        touch bob1
        touch bob2
    5. Создайте два файла, которые принадлежат пользователю bob:
        touch bob1
        touch bob2
    6. В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также sticky-bit для разделенного (общего) каталога группы:
        chmod g+s,o+t /data/main
    7. В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4:
        touch alice3
        touch alice4
        ls -l
        Теперь должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main.
    8. В терминале под пользователем bob попробуйте удалить файлы, принадлежащие пользователю bob:
        rm -f bob1
        rm -f bob2

```

Рис. 6.4: 13

4. Переходим в каталог /data/main (рис. 6.5)

```

    или удаления пользователем, не являющимся их владельцем. Для установки этого атрибута используется утилита chmod. Восьмизначное значение sticky-биты: 16000, а символическое: +t.

    1. Откройте новый терминал под пользователем alice.
    2. Перейдите в каталог /data/main:
        cd /data/main
        Создайте два файла, владельцем которых является alice:
        touch alice1
        touch alice2
    3. В другом терминале перейдите под учётной записью пользователя bob (пользователь bob имеет членом группы main, как и alice):
        su bob
    4. Перейдите в каталог /data/main:
        cd /data/main
        Из текущего каталога выведите:
        ls -l
        Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:
        rm -f alice*
        Убедитесь, что файлы будут удалены пользователем bob:
        touch bob1
        touch bob2
    5. Создайте два файла, которые принадлежат пользователю bob:
        touch bob1
        touch bob2
    6. В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также sticky-bit для разделенного (общего) каталога группы:
        chmod g+s,o+t /data/main
    7. В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4:
        touch alice3
        touch alice4
        ls -l
        Теперь должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main.
    8. В терминале под пользователем bob попробуйте удалить файлы, принадлежащие пользователю bob:
        rm -f bob1
        rm -f bob2

```

Рис. 6.5: 14

5. Создаем два файла, которые принадлежат пользователю bob (рис. 6.6)

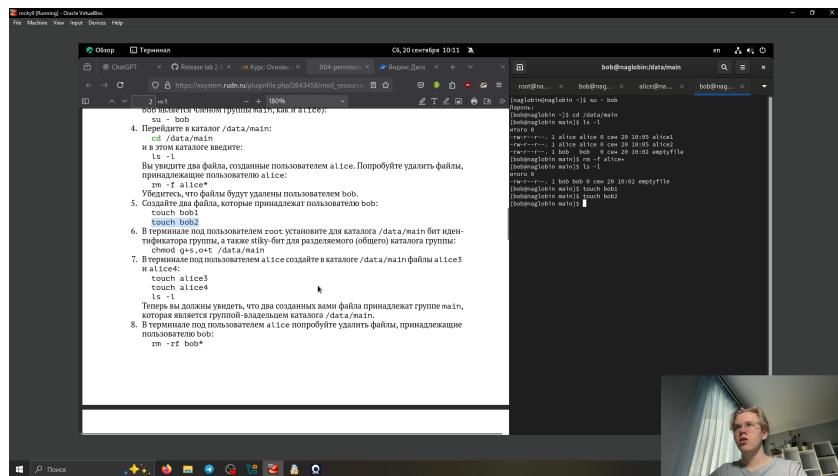


Рис. 6.6: 15

6. В терминале под пользователем root установим для каталога /data/main бит иден-тификатора группы, а также sticky-бит для разделяемого (общего) каталога группы (рис. 6.7)

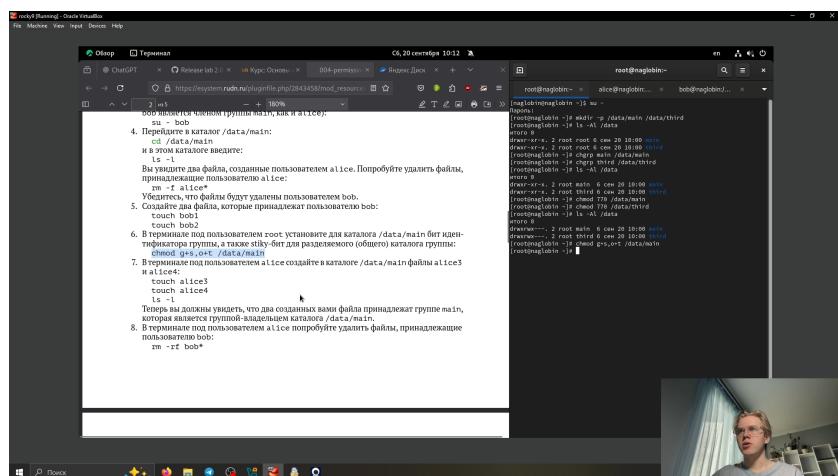


Рис. 6.7: 16

7. В терминале под пользователем alice создаем в каталоге /data/main файлы alice3 и alice4 (рис. 6.8)

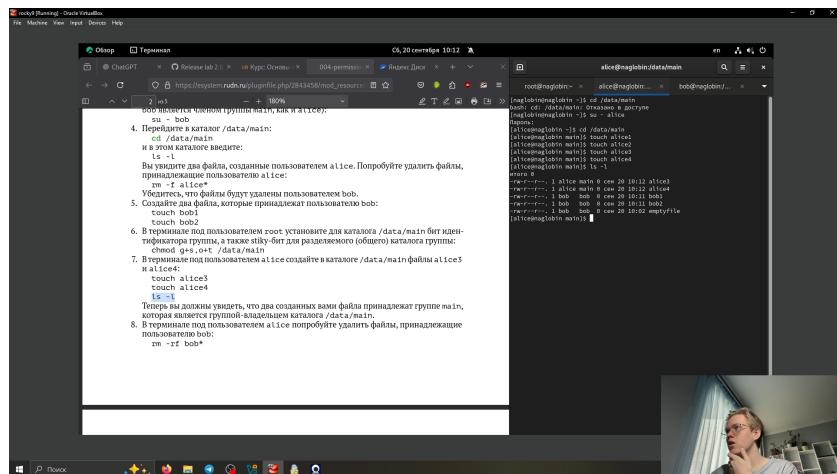


Рис. 6.8: 17

8. В терминале под пользователем alice попробуем удалить файлы, принадлежащие пользователю bob (рис. 6.9)

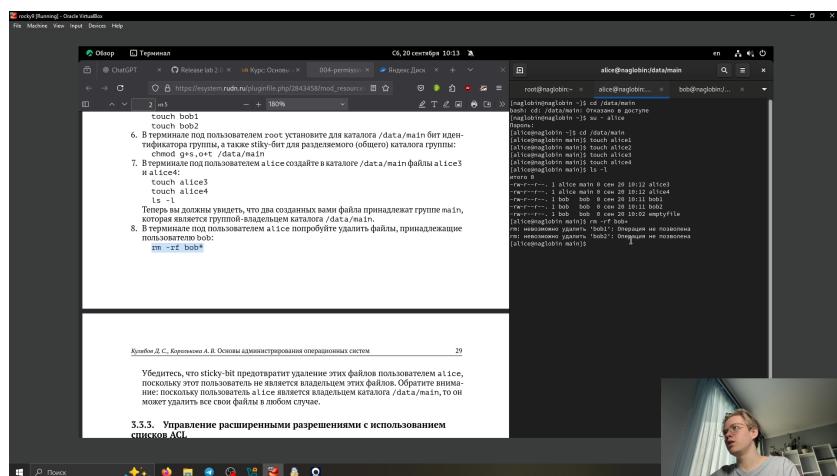


Рис. 6.9: 18

7 Управление расширенными разрешениями с использованием списков ACL

1. Откроем терминал с учётной записью root (рис. 7.1)
2. 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(рис. 7.1)

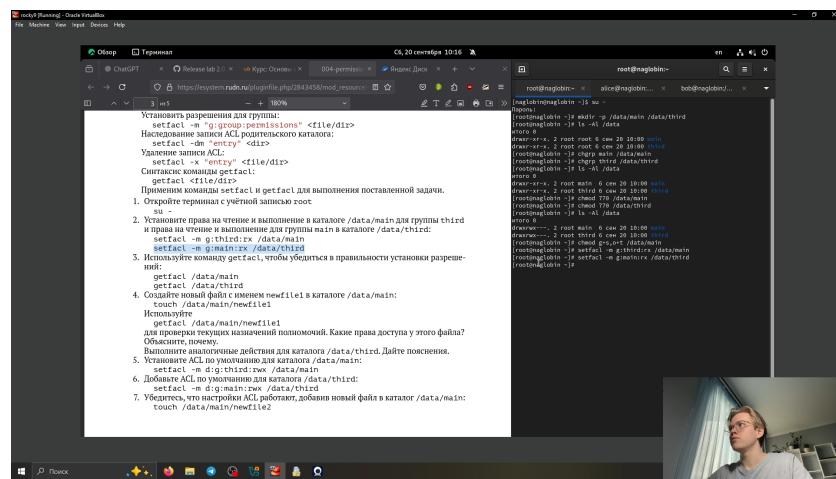


Рис. 7.1: 19

3. Используем команду getfacl, чтобы убедиться в правильности установки разрешений (рис. 7.2)

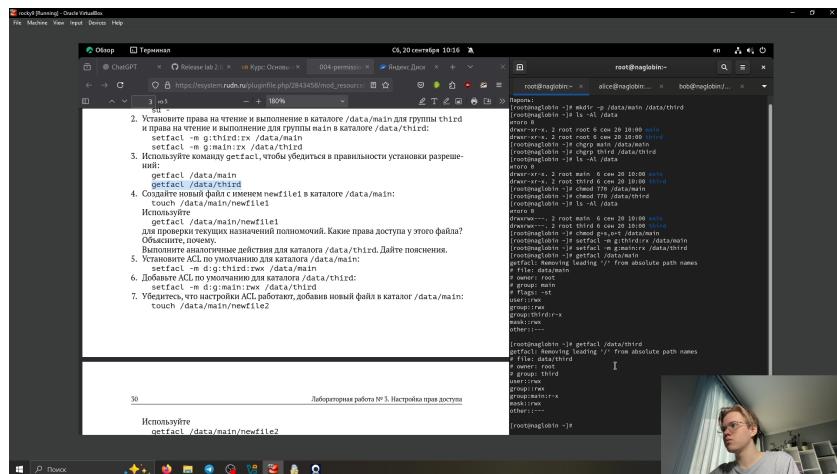


Рис. 7.2: 20

4. Создаем новый файл с именем newfile1 в каталоге /data/main (рис. 7.3)

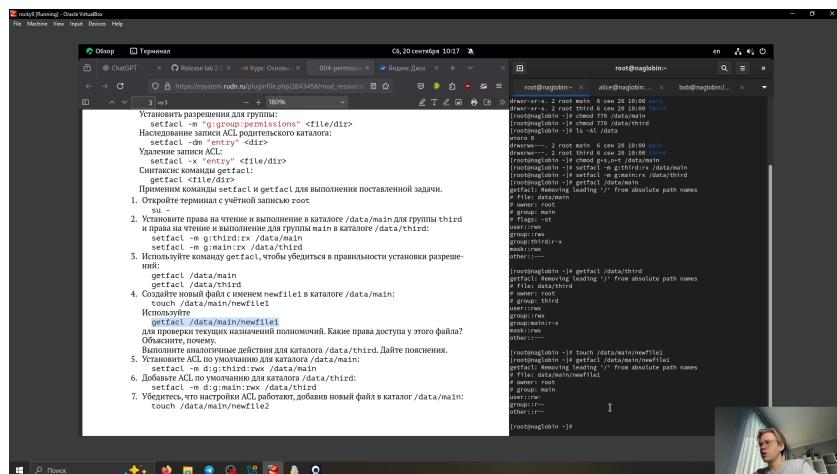


Рис. 7.3: 21

5. Установим ACL по умолчанию для каталога /data/main (рис. 7.4)

```

Установить разрешения для группы:
setfacl -m "g:group:permissions" <file/dir>
Наследование записи ACL родительского каталога:
setfacl -m "entry" <dir>
Удаление записи ACL:
setfacl -m "del" <file/dir>
Синтаксис команды getfacl:
getfacl <file/dir>
Применение команды setfacl и getfacl для выполнения поставленной задачи.
1. Откройте терминал с учётной записью root
su
2. 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:
setfacl -m g:third:rwx /data/main
setfacl -m g:main:rwx /data/third
3. Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:
getfacl /data/main/newfile1
4. Создайте новый файл и назовите его newfile1
touch /data/main/newfile1
Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:
getfacl /data/main/newfile1
для проверки текущих назначений полномочий. Какие права доступа у этого файла?
Объясните почему.
5. Установите ACL по умолчанию для каталога /data/main. Дайте пояснения.
6. Добавьте ACL по умолчанию для каталога /data/third:
setfacl -m d:third:rwx /data/third
7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main:
touch /data/main/newfile2

```

Рис. 7.4: 22

6. Добавем ACL по умолчанию для каталога /data/third (рис. 7.5)

```

Установить разрешения для группы:
setfacl -m "g:group:permissions" <file/dir>
Наследование записи ACL родительского каталога:
setfacl -m "entry" <dir>
Удаление записи ACL:
setfacl -m "del" <file/dir>
Синтаксис команды getfacl:
getfacl <file/dir>
Применение команды setfacl и getfacl для выполнения поставленной задачи.
1. Откройте терминал с учётной записью root
su
2. 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:
setfacl -m g:third:rwx /data/main
setfacl -m g:main:rwx /data/third
3. Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:
getfacl /data/main/newfile1
4. Создайте новый файл и назовите его newfile1
touch /data/main/newfile1
Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:
getfacl /data/main/newfile1
для проверки текущих назначений полномочий. Какие права доступа у этого файла?
Объясните, почему.
5. Установите ACL по умолчанию для каталога /data/main. Дайте пояснения.
6. Добавьте ACL по умолчанию для каталога /data/third:
setfacl -m d:third:rwx /data/third
7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main:
touch /data/main/newfile2

```

Рис. 7.5: 23

7. Убедимся, что настройки ACL работают, добавив новый файл в каталог /data/main (рис. 7.6)

The terminal window shows the following command and its output:

```
root@nagibin:~# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: root
group::rwx
user::rwx
group::rwx
user::rwx
group::rwx
user::rwx
```

The browser window displays the following task:

Лабораторная работа №3. Настройка прав доступа

Используйте
getfacl /data/main/newfile2
для проверки текущих назначенных полномочий.
Выполните аналогичные действия для каталога /data/third.
8. Для проверки полномочий группы third в каталоге /data/third войдите в другом терминале под учётной записью члена группы third:
su - carol
Проверьте создание 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 результаты проведённых действий.

3.4. Содержание отчёта

Рис. 7.6: 24

Выполним аналогичные действия для каталога /data/third (рис. 7.7)

The terminal window shows the following command and its output:

```
root@nagibin:~# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root
# group: root
group::rwx
user::rwx
group::rwx
user::rwx
group::rwx
user::rwx
```

The browser window displays the following task:

Лабораторная работа №3. Настройка прав доступа

Используйте
getfacl /data/main/newfile2
для проверки текущих назначенных полномочий.
Выполните аналогичные действия для каталога /data/third.
8. Для проверки полномочий группы third в каталоге /data/third войдите в другом терминале под учётной записью члена группы third:
su - carol
Проверьте создание 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 результаты проведённых действий.

3.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Фото выполнения работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - подробное описание произведённых в соответствии с заданием настроек;
 - выводы.

Рис. 7.7: 25

8. Для проверки полномочий группы third в каталоге /data/third войдем в другом терминале под учётной записью члена группы third (рис. 7.8)

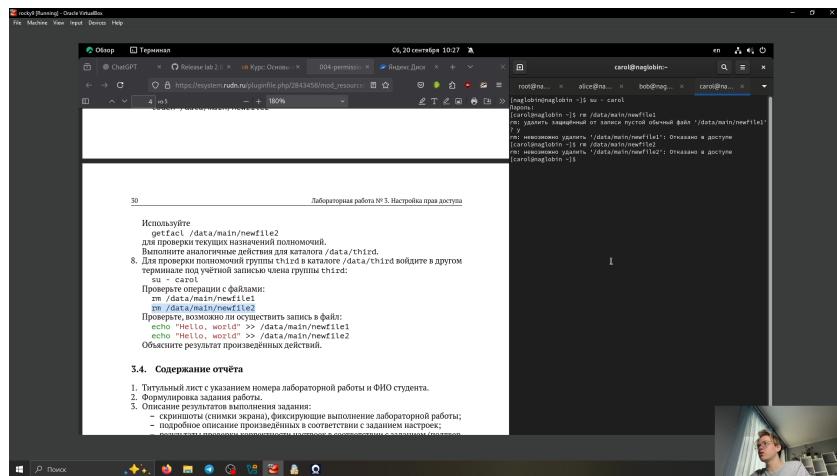


Рис. 7.8: 26

Проверем операции с файлами и возможно ли осуществить запись в файл (рис. 7.9)

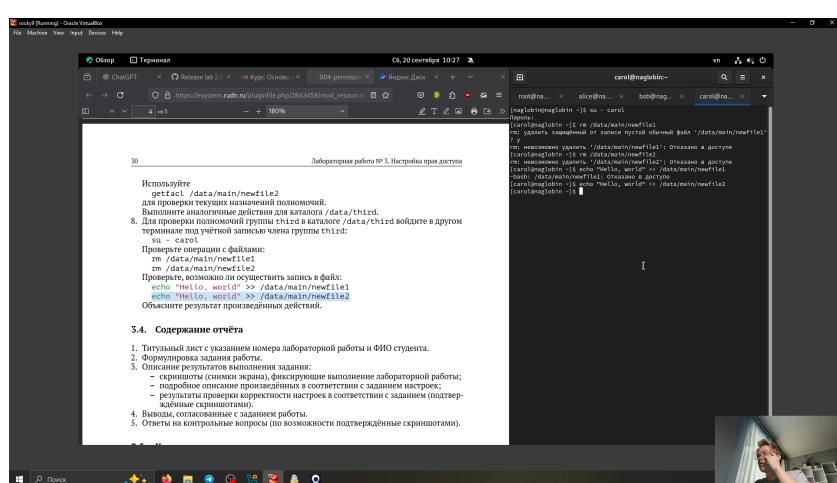


Рис. 7.9: 27

8 Контрольные вопросы

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

Команда chown позволяет изменить владельца и/или группу файла.chown :

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

Команда find позволяет искать файлы по владельцу.find / -user alice

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. chmod -R 770 /data
4. Какая команда позволяет добавить разрешение на выполнение для файла, который необходимо сделать исполняемым?

chmod +x

5. Какая команда позволяет убедиться, что групповые разрешения для всех новых файлов, создаваемых в каталоге, будут присвоены владельцу группы этого каталога? Приведите пример.

Для этого используется бит setgid на каталоге. chmod g+s /data/main

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.

Для этого применяется sticky-bit. После установки sticky-бита только владельцы файлов (или root) смогут их удалять, даже если каталог доступен другим. chmod +t /data/main

7. Какая команда добавляет ACL, который предоставляет членам группы права доступа на чтение для всех существующих файлов в текущем каталоге?

setfacl -m g::r

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.

Нужно использовать ACL по умолчанию (default ACL). setfacl -R -m g:third:r setfacl -d -m g:third:rwx

9. Какое значение umask нужно установить, чтобы «другие» пользователи не получали какие-либо разрешения на новые файлы? Приведите пример.

Значение umask: 007

10. Какая команда гарантирует, что никто не сможет удалить файл myfile случайно?

Самый простой способ – запретить запись в каталог или установить атрибут “immutable”.

9 Выводы

В ходе выполнения лабораторной работы №3 мы научились настраивать базовые, специальные и расширенные права доступа в операционной системе Linux. Были изучены команды chmod, chgrp, chown, getfacl, setfacl, а также их применение на практике.