Лабораторная работа № 3

Настройка прав доступа

Жукова София Викторовна

Содержание

# 1 Цель работы

Целью данной работы является получение навыков настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.

# 2 Выполнение лабораторной работы

**Управление базовыми разрешениями**

Откройем терминал с учётной записью root (рис. 1).

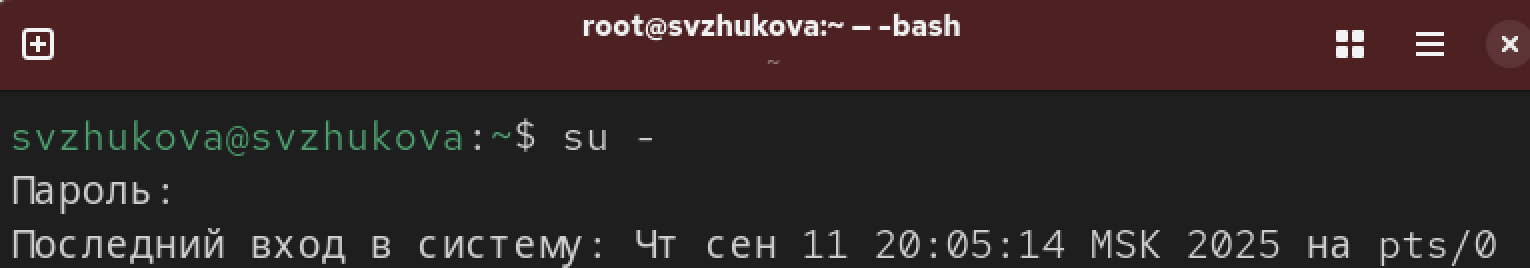


Рис. 1: Pоль супер-пользователя

В корневом каталоге создадим каталоги /data/main и /data/third Посмотрим, кто является владельцем этих каталогов. (рис. 2).

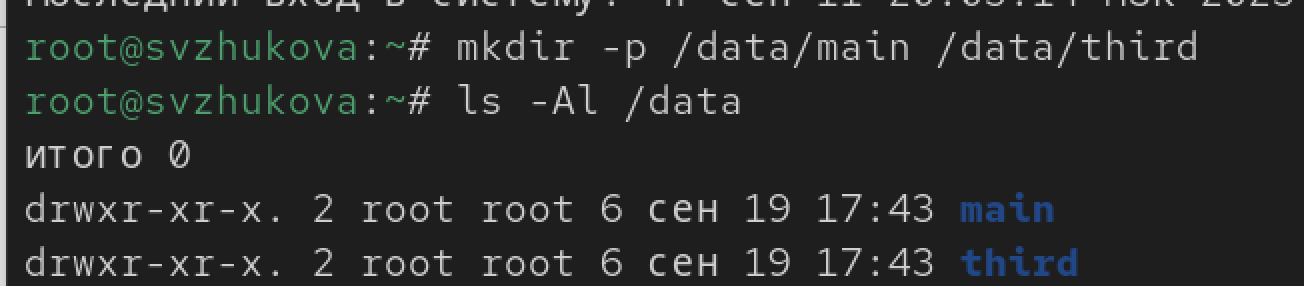


Рис. 2: каталоги /data/main и /data/third

Прежде чем устанавливать разрешения, изменим владельцев этих каталогов с root на main и third соответственно Посмотрим, кто теперь является владельцем этих каталогов (рис. 3).

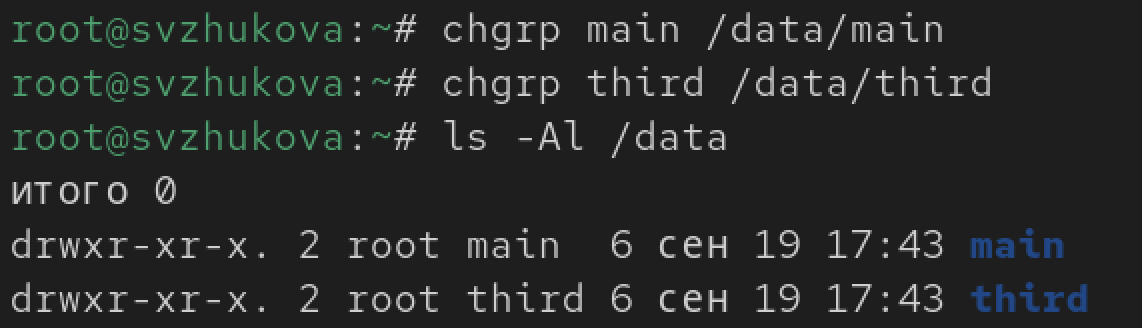


Рис. 3: Изменим владельцев каталогов

Установим разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам Проверим установленные права доступа (рис. 4).

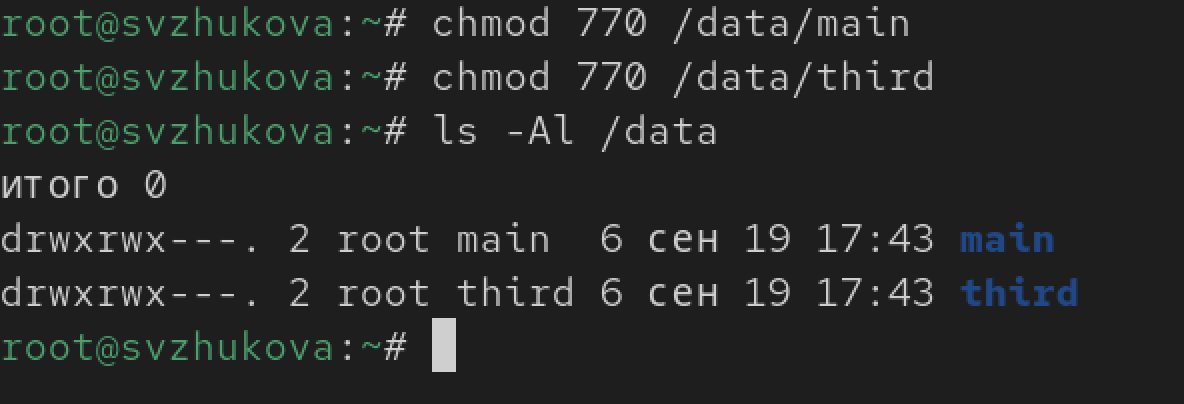


Рис. 4: Права доступа

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

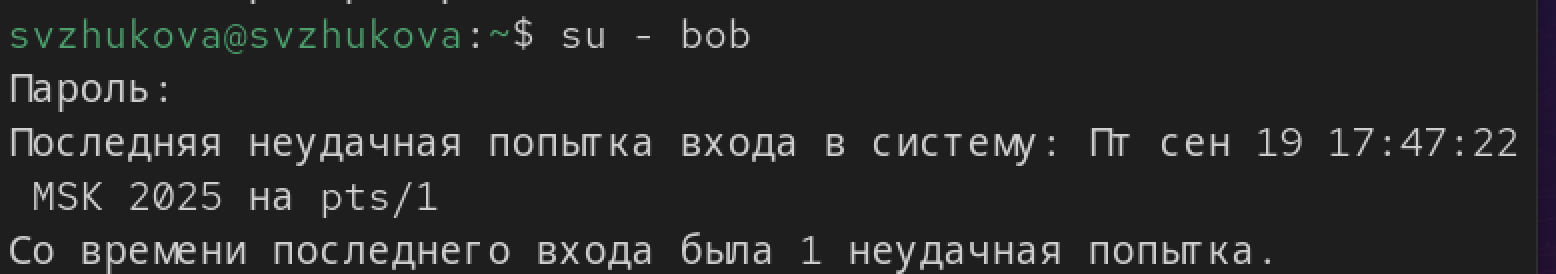


Рис. 5: Учётная запись пользователя bob

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

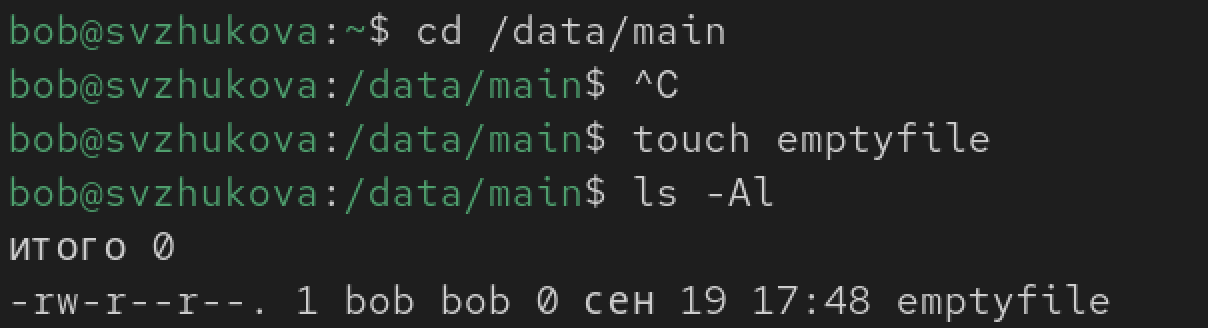


Рис. 6: emptyfile

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

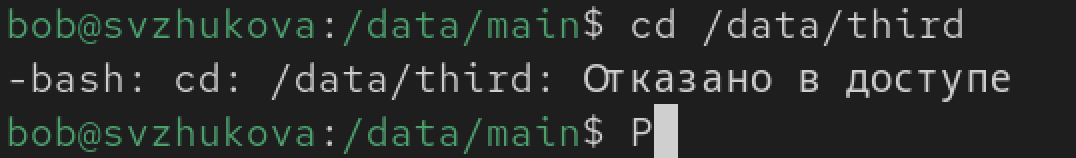


Рис. 7: Нам отказано в доступе, нет нужных прав

**Управление специальными разрешениями**

Откроем новый терминал под пользователем alice (рис. 8).

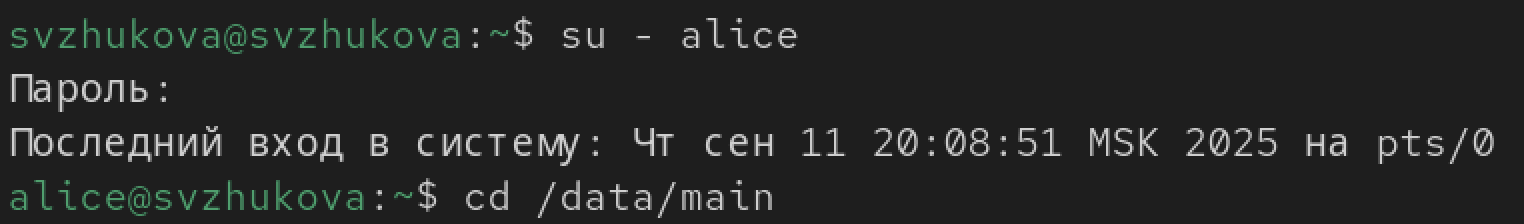


Рис. 8: alice

Перейдите в каталог /data/main и создадим два файла, владельцем которых является alice (рис. 9).

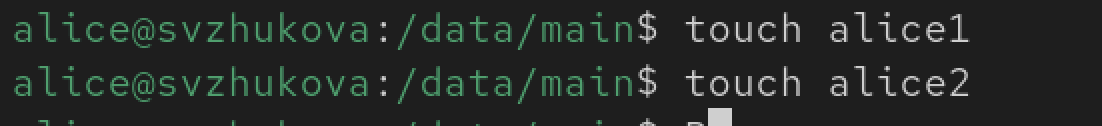


Рис. 9: Создадим два файла

В другом терминале перейдем под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice) Перейдем в каталог /data/main и в этом каталоге введем (рис. 10).

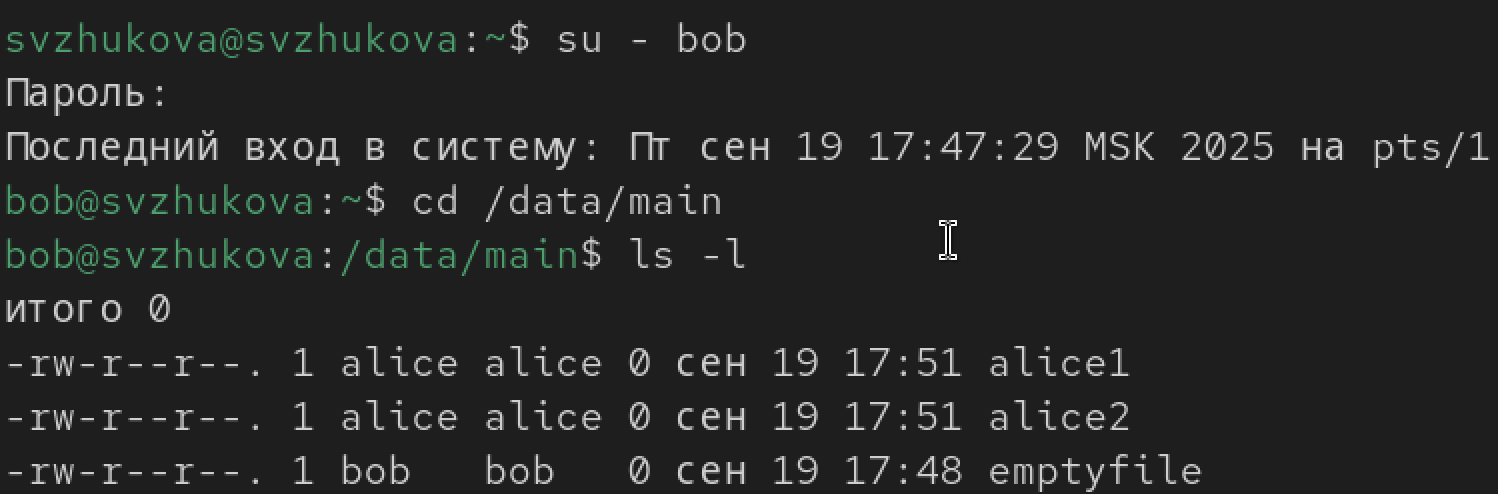


Рис. 10: Мы видим два файла, созданные пользователем alice

Попробуем удалить файлы, принадлежащие пользователю alice (рис. 11).

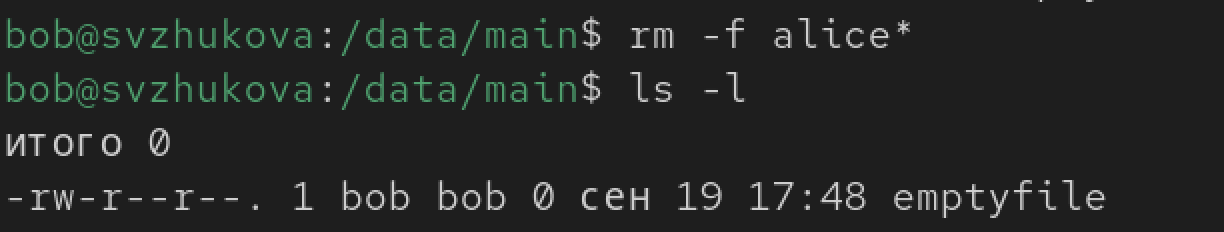


Рис. 11: Файлы удалены

Создадим два файла, которые принадлежат пользователю bob (рис. 12).

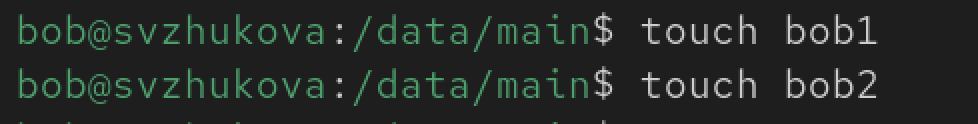


Рис. 12: Два файла, которые принадлежат пользователю bob

В терминале под пользователем root установим для каталога /data/main бит идентификатора группы, а также stiky-бит для разделяемого (общего) каталога группы (рис. 13).

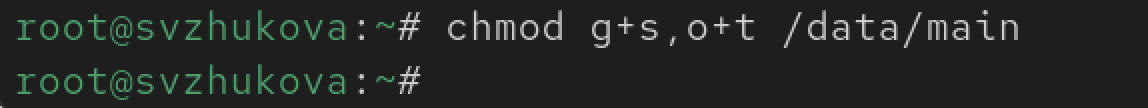


Рис. 13: установим идентификатор группы, а также stiky-бит для разделяемого каталога группы

В терминале под пользователем alice создадим в каталоге /data/main файлы alice3 и alice4(рис. 14).

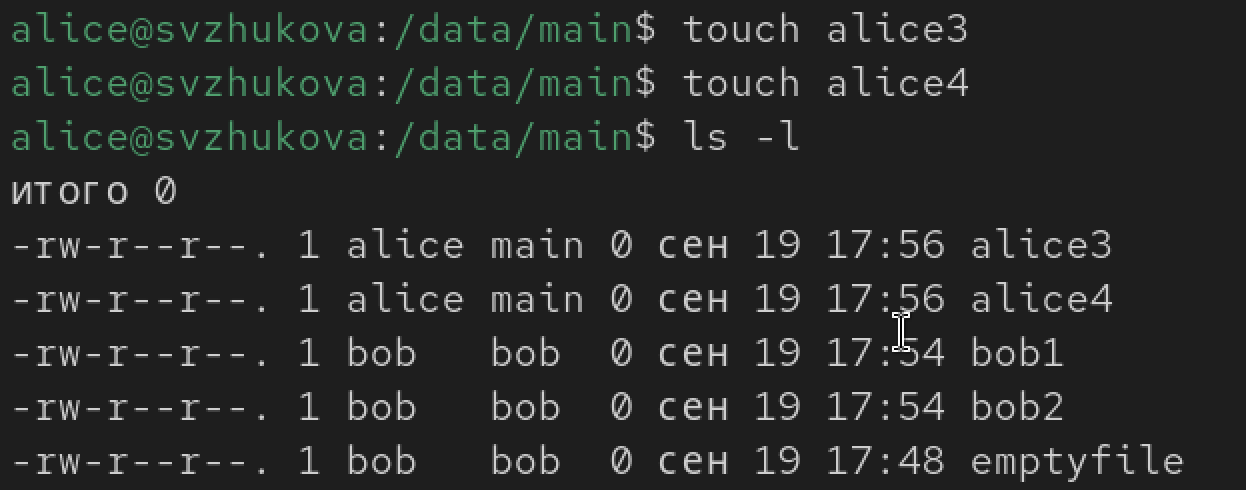


Рис. 14: Файлы alice3 и alice4

Теперь мы видим, что два созданных нами файла принадлежат группе main, которая является группой-владельцем каталога /data/main

В терминале под пользователем alice попробуем удалить файлы, принадлежащие пользователю bob(рис. 15).

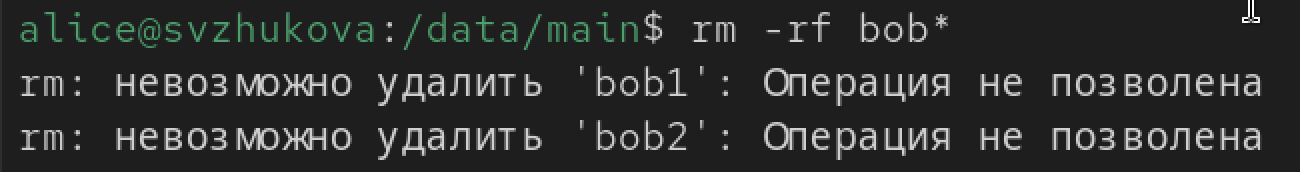


Рис. 15: Операция недоступна

**Управление расширенными разрешениями с использованием списков ACL**

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:(рис. 16).

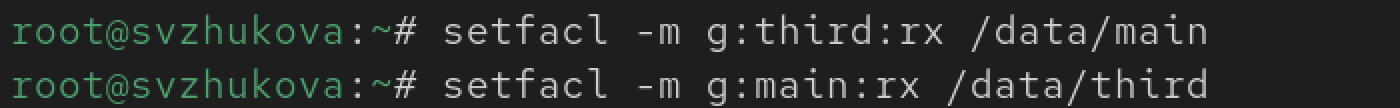


Рис. 16: права на чтение и выполнение

Используем команду getfacl, чтобы убедиться в правильности установки разреше- ний(рис. 17). (рис. 18).

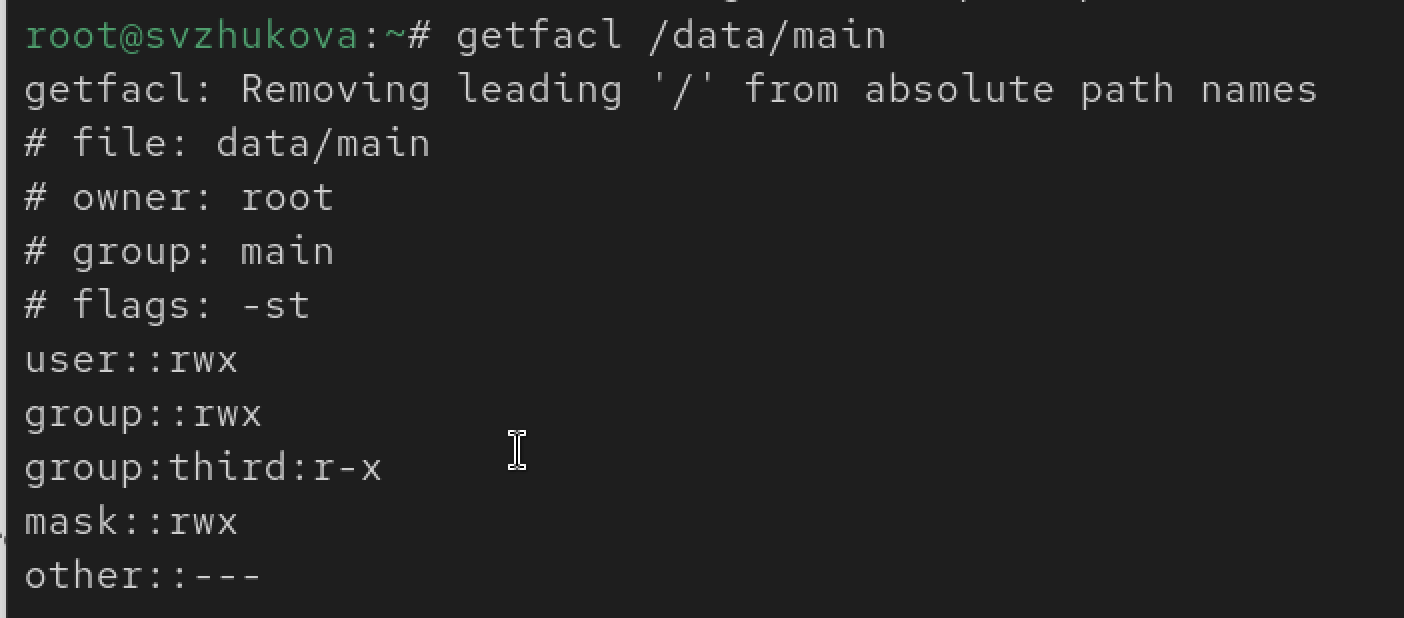


Рис. 17: Правильность установки разрешений

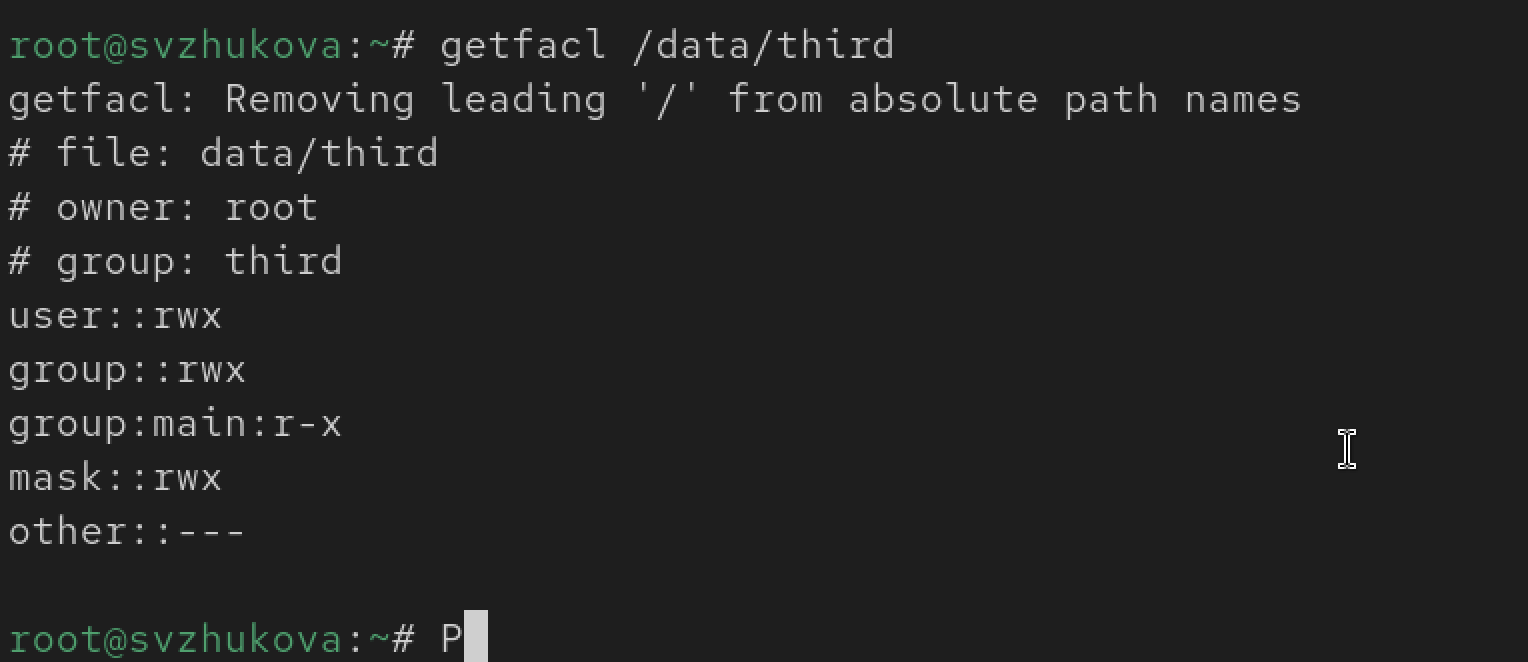


Рис. 18: Правильность установки разрешени

Создадим новый файл с именем newfile1 в каталоге /data/main: Проверим текущие назначения полномочий. (рис. 19).

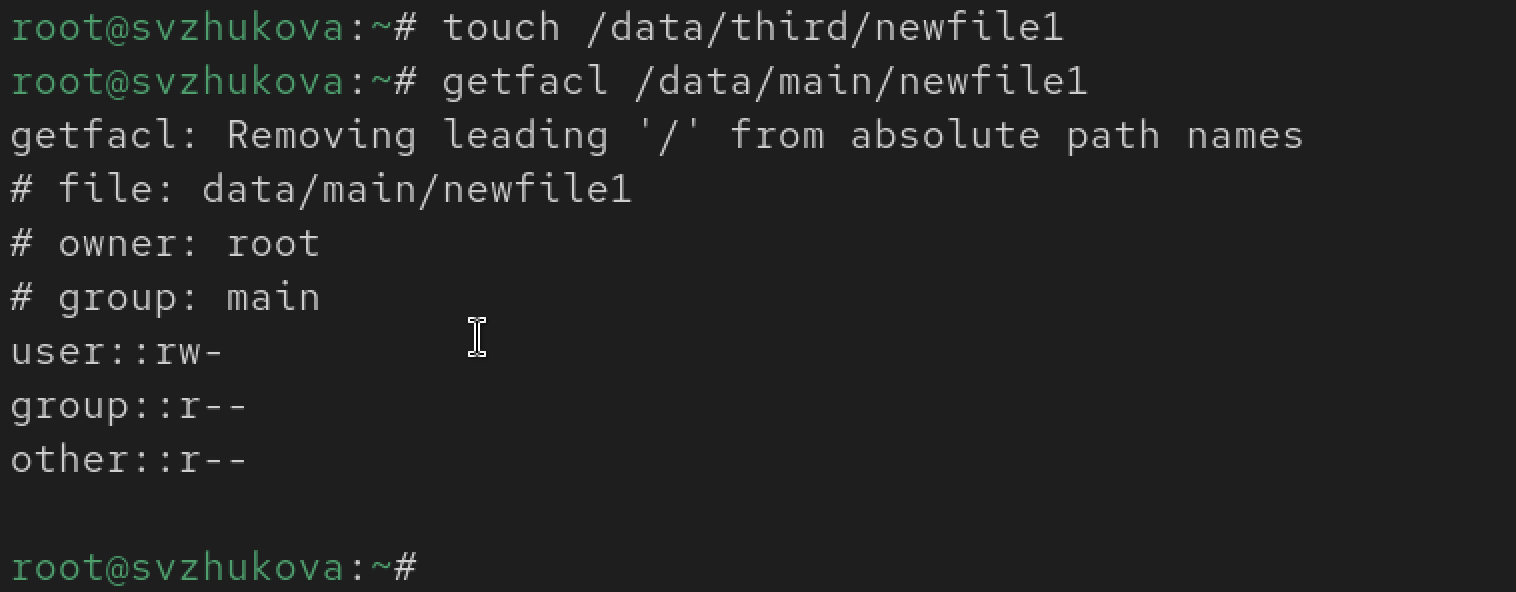


Рис. 19: Установим и проверим

Установим ACL по умолчанию для каталога /data/main:

Добавим ACL по умолчанию для каталога /data/third(рис. 20).

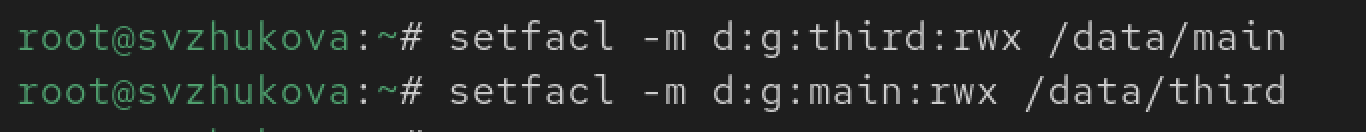


Рис. 20: Добавим

Убедимся, что настройки ACL работают, добавив новый файл в каталог /data/main:(рис. 21).

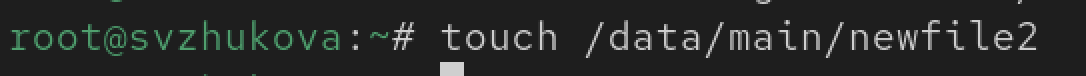


Рис. 21: Добавим новый файл в каталог

Проверим текущие назначения полномочий.(рис. 22).



Рис. 22: Проверим

Выполним аналогичные действия для каталога /data/third. (рис. 23).

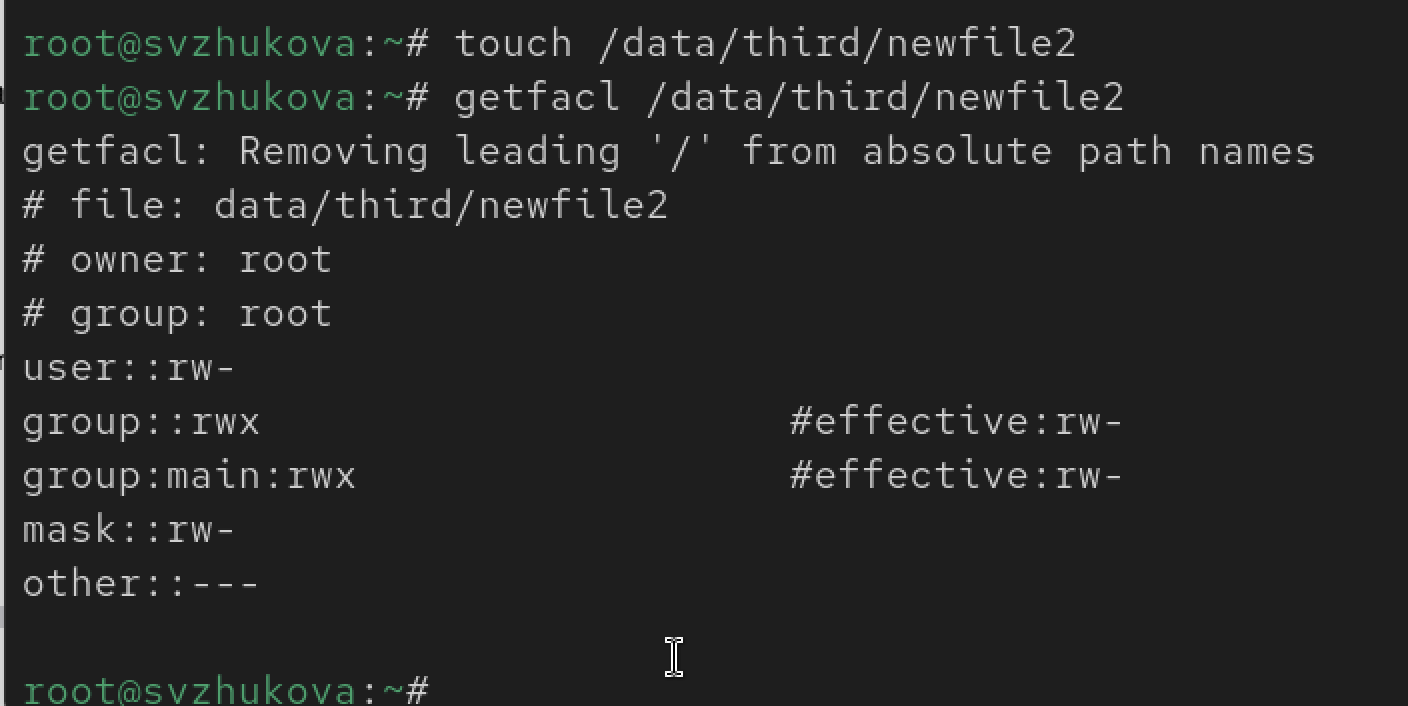


Рис. 23: Выполним

Для проверки полномочий группы third в каталоге /data/third войдем в другом терминале под учётной записью члена группы third Проверим операции с файлами(рис. 24).

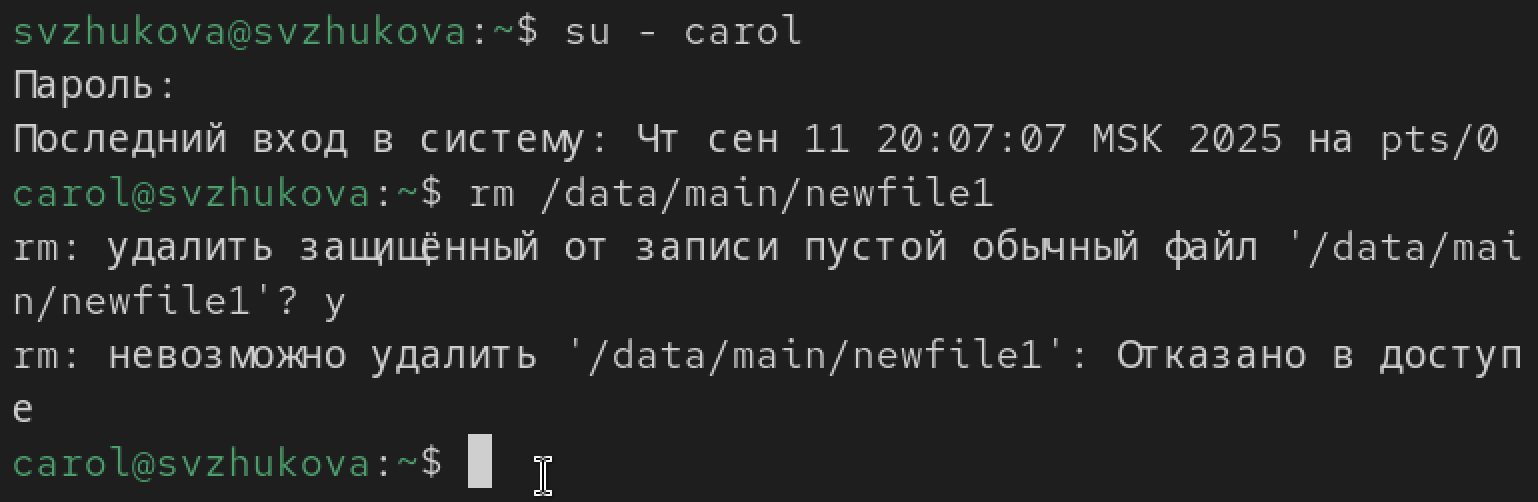


Рис. 24: Нельзя

Проверим, возможно ли осуществить запись в файл(рис. 25).

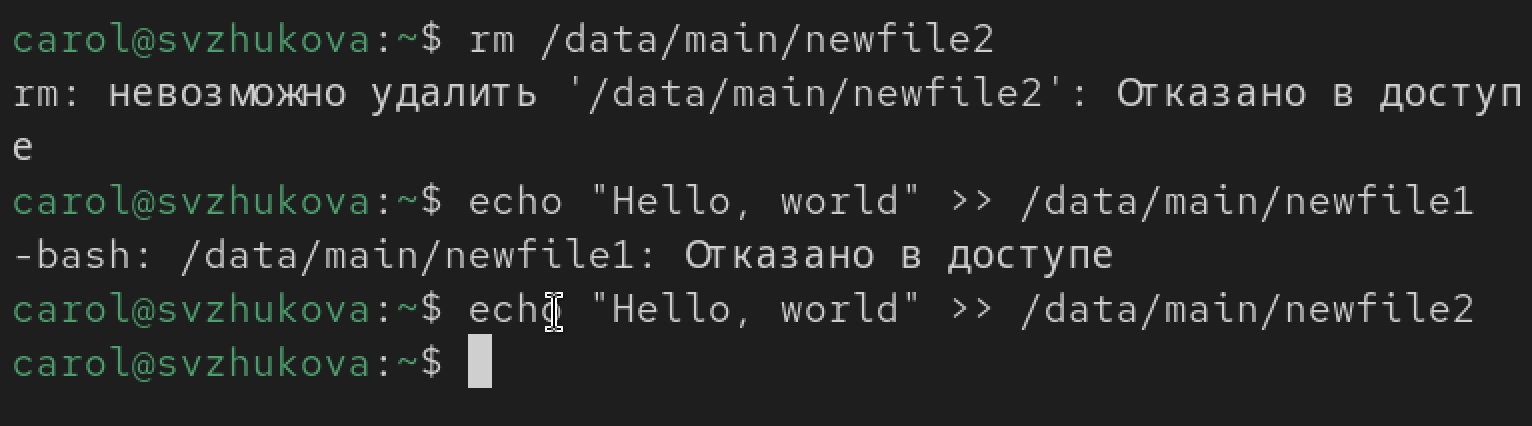


Рис. 25: Можно только во втором случае

**Контрольные вопросы**

1. Использование команды chown Чтобы установить владельца и группу для файла, используется команда chown. Пример:

chown user:group filename.txt

Чтобы сменить владельца файла filename.txt на user и группу на group.

1. Поиск файлов, принадлежащих конкретному пользователю Для этого можно использовать команду find. Пример:

find /path/to/search -user username

Это найдет все файлы в указанном пути, принадлежащие пользователю username.

1. Применение разрешений для всех файлов в /data Чтобы установить разрешения на чтение, запись и выполнение для всех владельцев и группы, но не для других, используйте команду chmod:

chmod 770 /data/\*

Здесь 7 дает полные права для владельца и группы, а 0 — никаких прав для других.

1. Добавление разрешения на выполнение для файла Используйте команду chmod, чтобы сделать файл исполняемым. Пример:

chmod +x filename.sh

Это добавит разрешение на выполнение для файла filename.sh.

1. Установка групповых разрешений для новых файлов Чтобы все новые файлы, создаваемые в каталоге, наследовали группу этого каталога, используйте chmod с настройкой битов SGID. Пример:

chmod g+s /path/to/directory

1. Удаление файлов только владельцами Для ограничения прав удаления можно использовать chmod, чтобы убрать права на удаление для группы и других. Пример:

chmod o-w /path/to/directory

Эта команда убирает права записи для других пользователей, предотвращая их возможность удаления файлов.

1. Добавление ACL для группы С помощью setfacl можно добавить права доступа для группы. Пример:

setfacl -m g:groupname:r /path/to/directory/\*

Это добавит права на чтение для группы groupname для всех существующих файлов в каталоге.

1. Гарантия прав чтения для всех файлов Для того чтобы члены группы получили права чтения на все файлы и подкаталоги, используйте:

setfacl -R -m g:groupname:rX /path/to/directory

Это даст права чтения и выполнения для всех файлов и каталогов.

1. Установка umask для ограничения прав Для того чтобы «другие» пользователи не получали разрешения на новые файлы, установите umask на 007. Пример:

umask 007

Это гарантирует, что файлы создаются с правами 664 и каталоги с правами 775.

1. Защита файла от удаления Чтобы гарантировать, что файл myfile не может быть удален случайно, можно установить только права на чтение и запись для владельца. Пример:

chmod 444 myfile

Это уберет все права на запись, что предотвратит случайное удаление файла.

# 3 Выводы

Мы получили навыки настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.