Лабораторная работа №3

Дисциплина: Оcновы администрирования операционных систем

Жибицкая Евгения Дмитриевна

Содержание

# 1 Цель работы

Продолжение изучения Linux. Получение навыков настройки базовых и специальных прав доступа для групп пользователей в ОС.

# 2 Выполнение лабораторной работы

В качестве подготовки к работе и выполненения задания 1 изучим принцип работы следующих команд: chgrp, chmod, getfacl, setfacl (рис. 1).

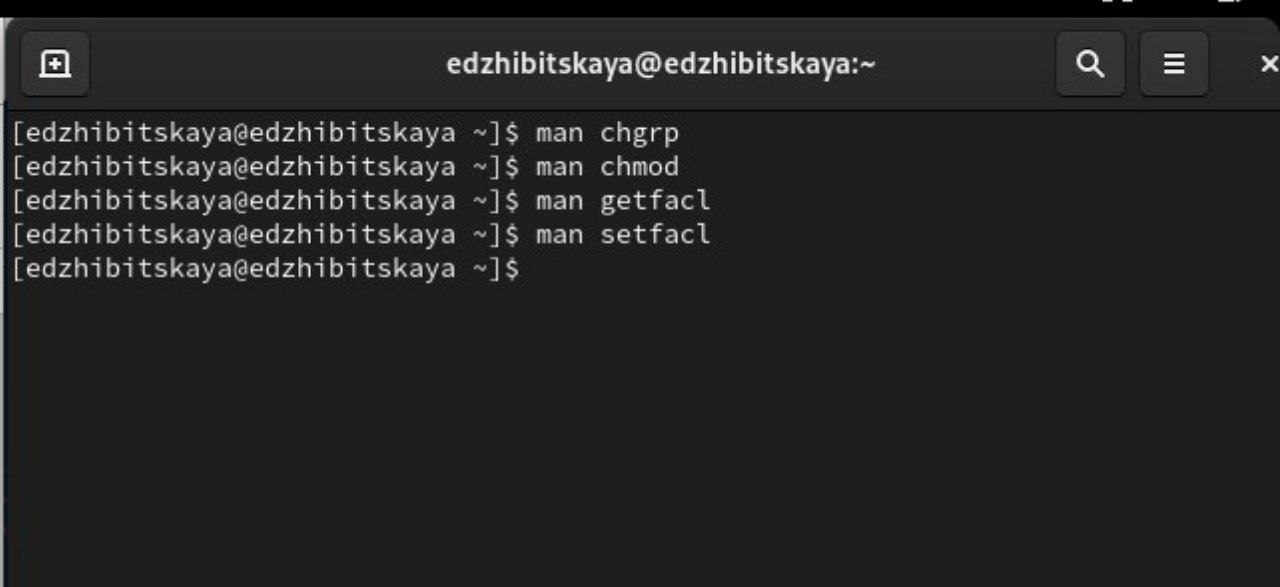


Рис. 1: Знакомство с командами

Далее перейдем к управлению базовыми разрешениями. Открываем терминал с root и создаем каталоги /data/main и /data/third. Также смотрим кто является владельцем и меняем их на main и third. установим разрешения на запись для владельцев и запрет на доступ остальным(рис. 2).

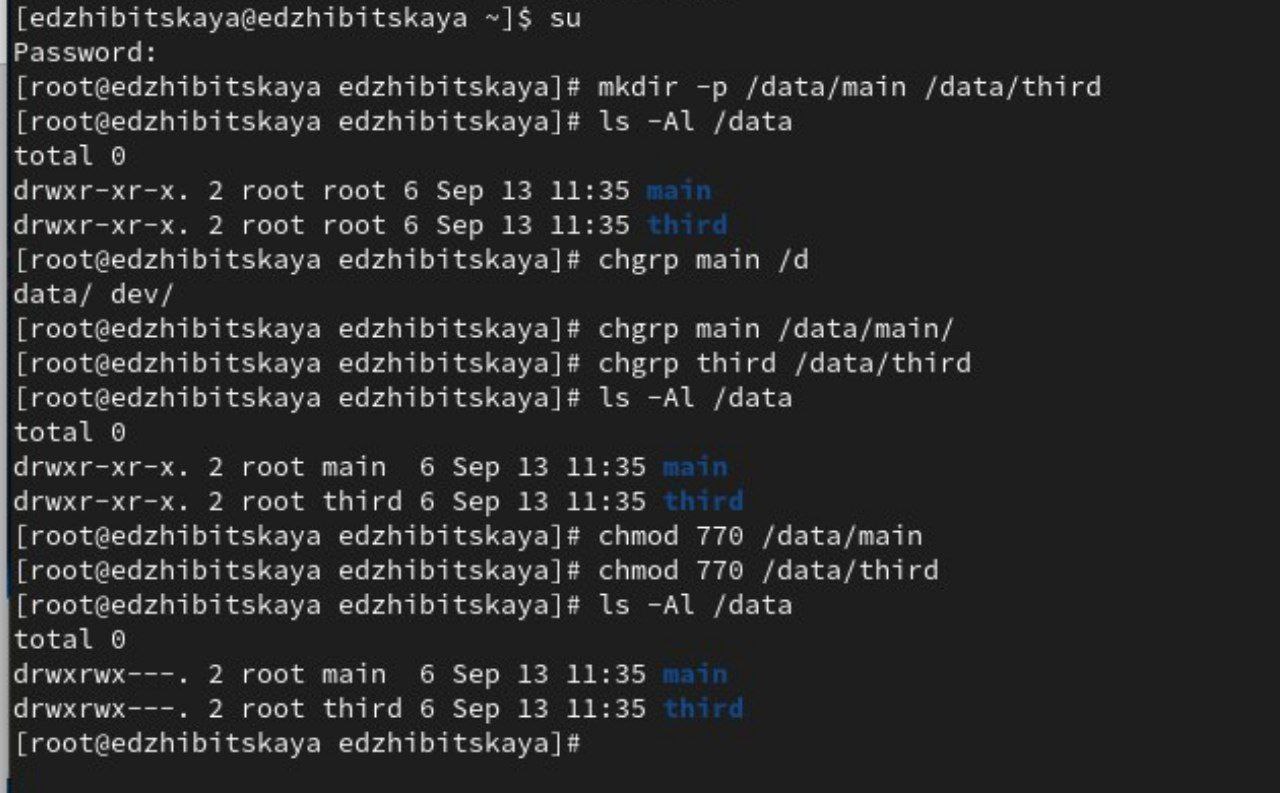


Рис. 2: Права доступа и разрешения

Откроем еще один терминал и войдем в учетную запись Bob. Перейдем в нужный каталог и попытаемся создать файл. При попытке посмотреть содержимое каталога main с новым файлом проблем не возникает, а при тех же действиях в каталоге third, пишут, что доступ запрещен, так как до этого мы сами установили такие права доступа(Bob принадлежит к группе main) (рис. 3).

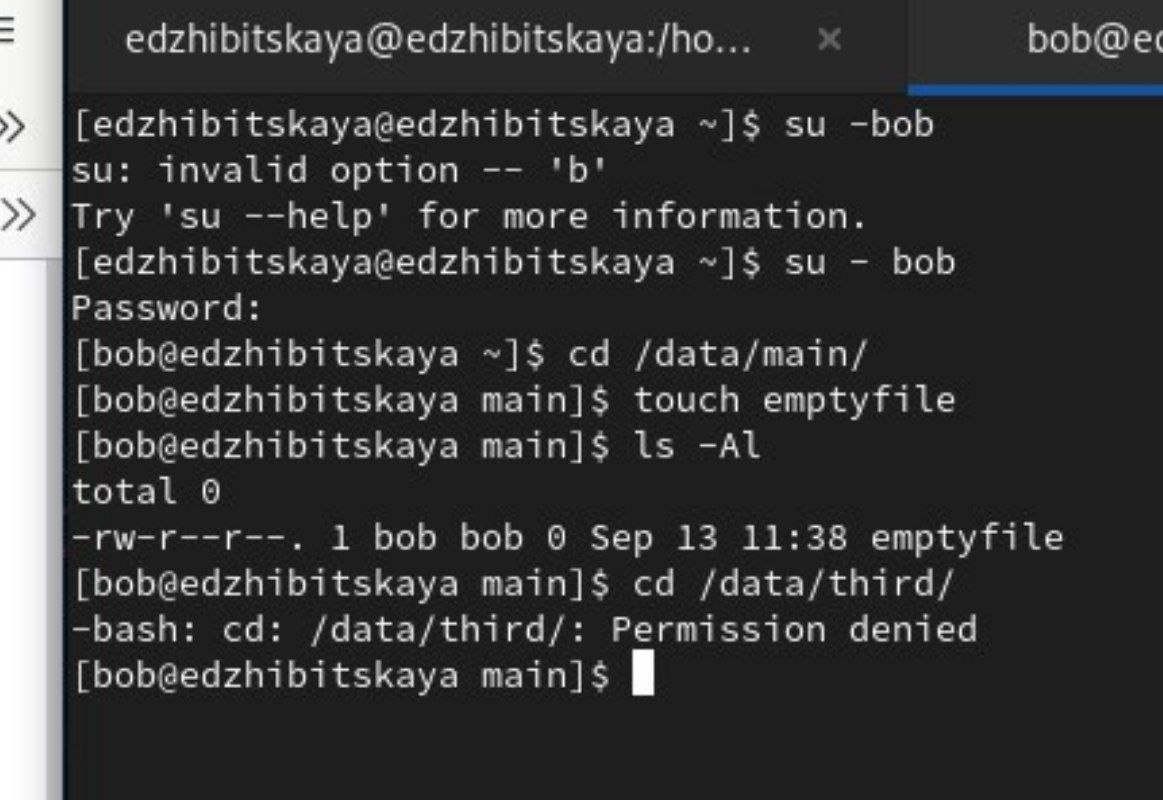


Рис. 3: Права доступа для Bob

Откроем еще терминал под учетной записью Alice. Создадим 2 файла(рис. 4).

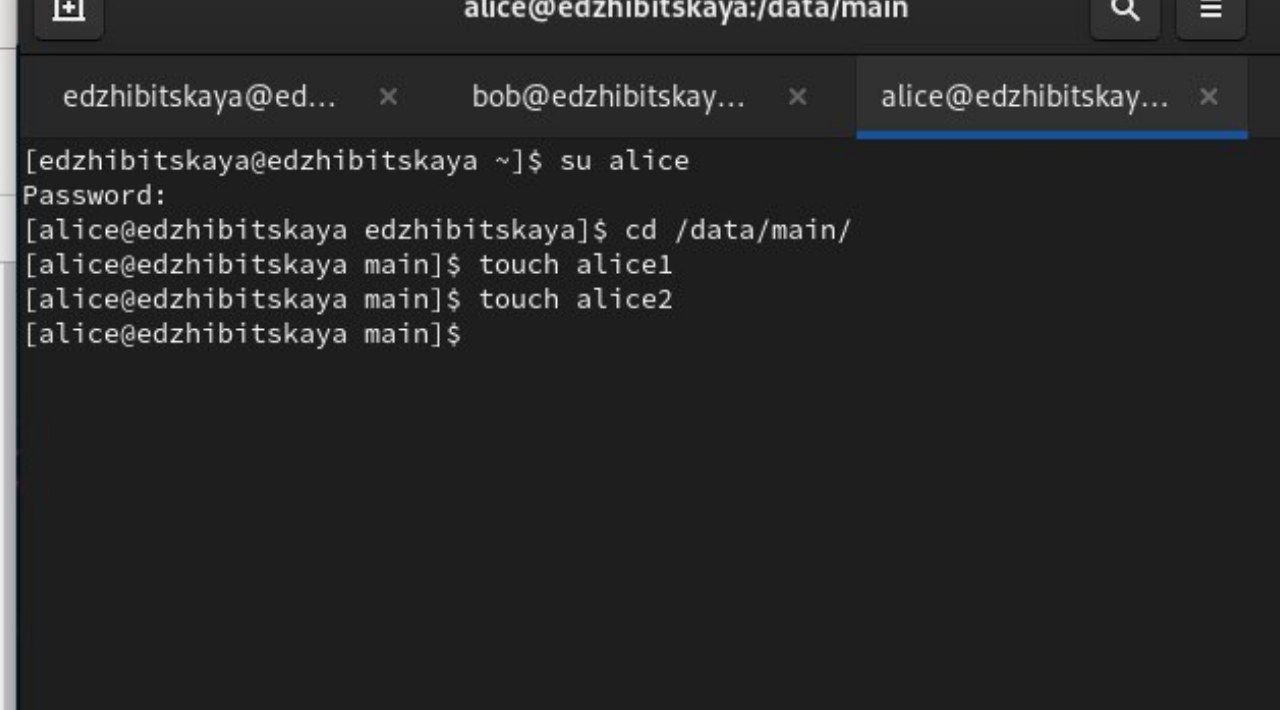


Рис. 4: Создание файлов

Вернемся к Bob. Командой ls -l просмотрим содержимое и удалим все файлы принадлежащие Alice.

Убедимся, что они удалены и создадим еще два файла Bob1, Bob2 (рис. 5).

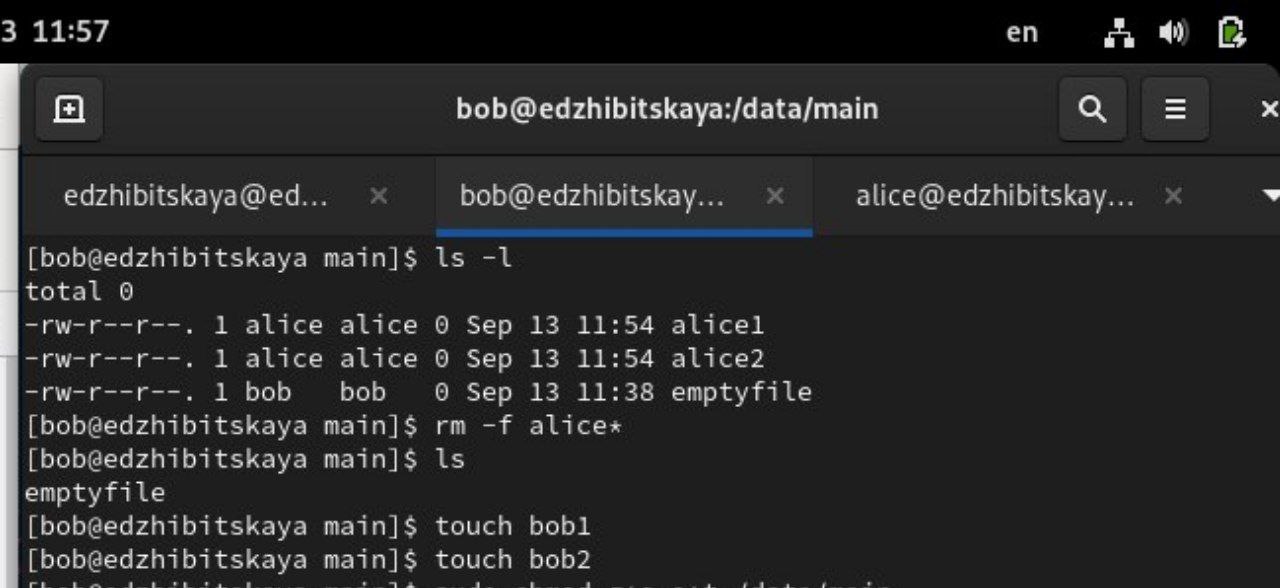


Рис. 5: Работа с файлами

В терминале с root установим для каталога /data/main бит идентификатора группы, а также stiky-бит для разделяемого (общего) каталога группы(рис. 6).

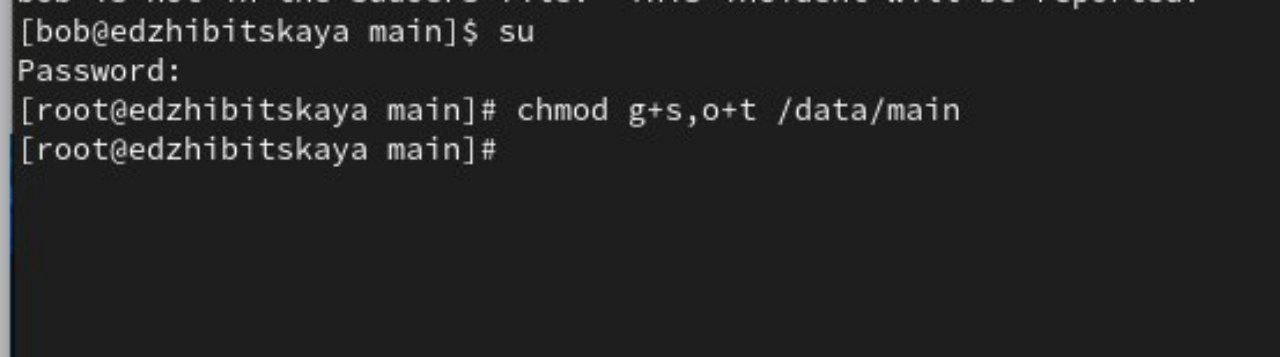


Рис. 6: Идентификатор и sticky-бит

Затем вернемся к Alice. Создадим еще 2 файла, посмотрим на их владельца(alice main). Попробуем удалить файлы, принадлежащие Бобу. Это невозможно из-за подключенного sticky-бита(рис. 7).

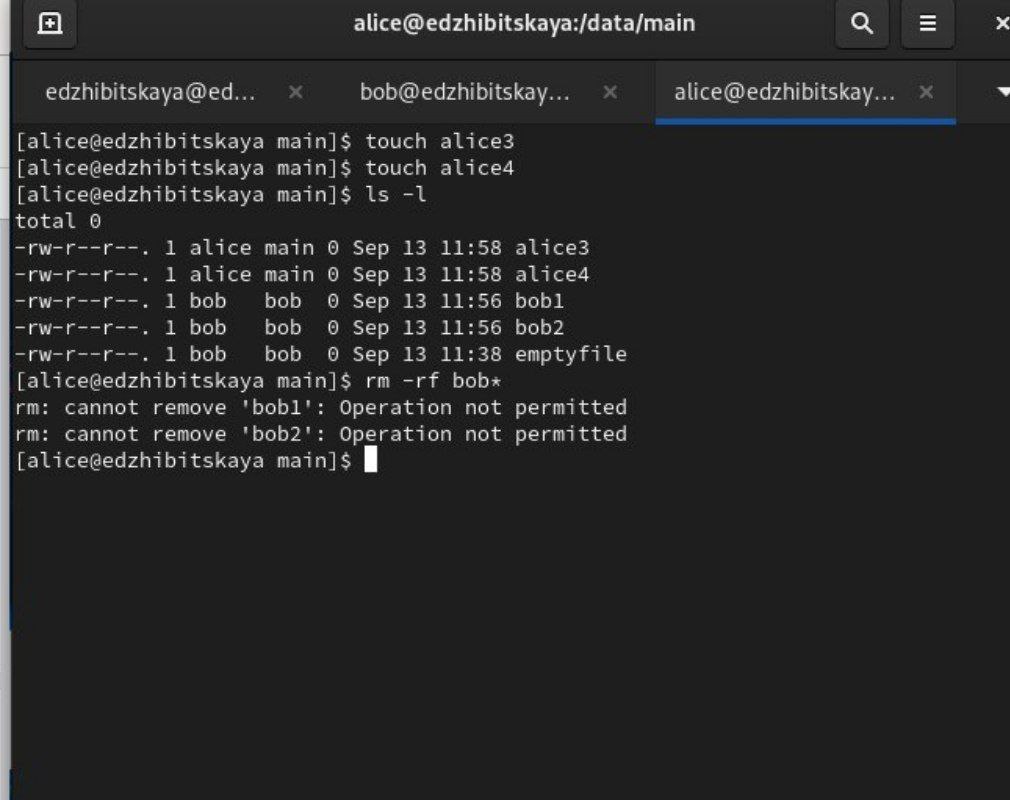


Рис. 7: Работа с файлами и sticky-битом

Перейдем в 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:

Используем команду getfacl, чтобы убедиться в правильности установки разрешений(рис. 8).

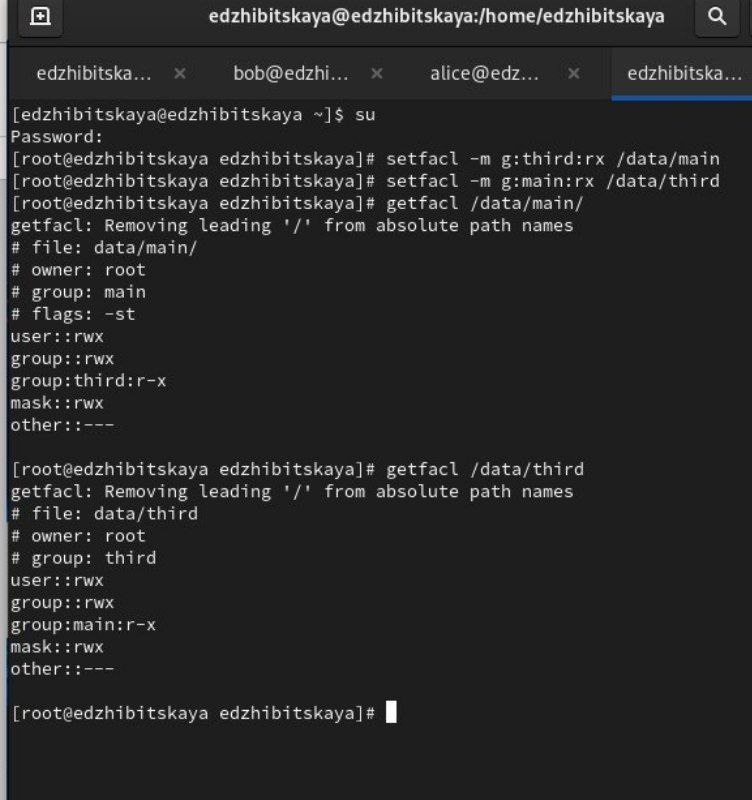


Рис. 8: Права на чтение и выполнение

Создадим новый файл newfile1 и проверим его полномочия(каталог main). Запись означает, что только владелец(root) имеет право на запись и чтение, у остальных только чтение. Проделаем аналогичные действия для third. Там все то же самое, только группа уже root, а не main(рис. 9).

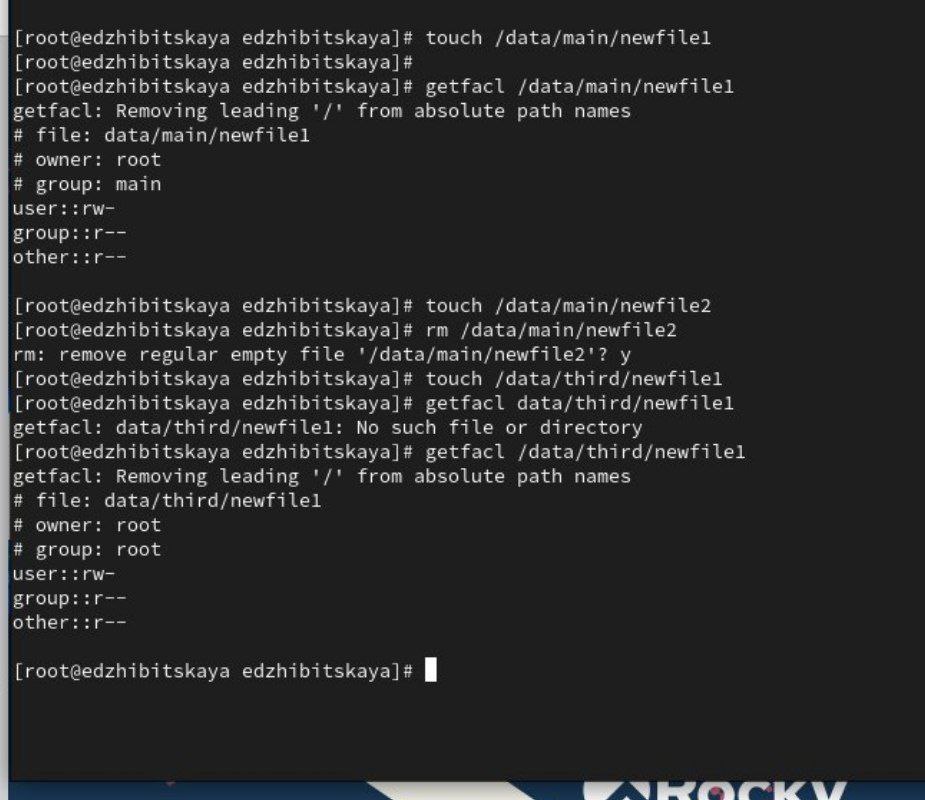


Рис. 9: Разрешения newfile1

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. Командой getfacl, убедимся в правильности установки разрешений: (рис. 10).

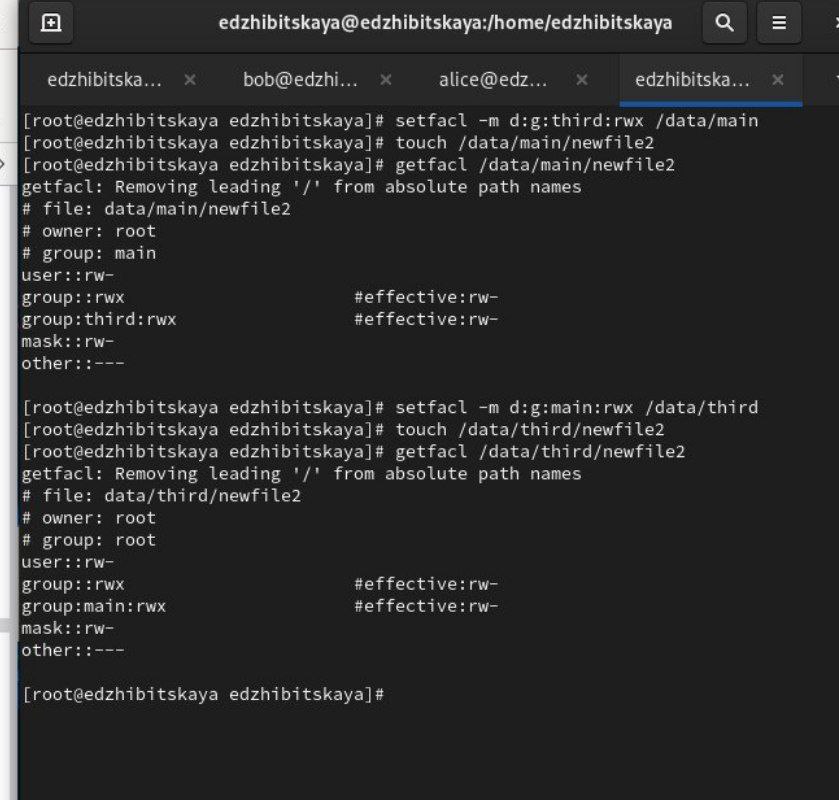


Рис. 10: ACL

Войдем в учетную запись Carol и попробуем удалить файлы - запрет(так как нет прав администратора)(рис. 11).

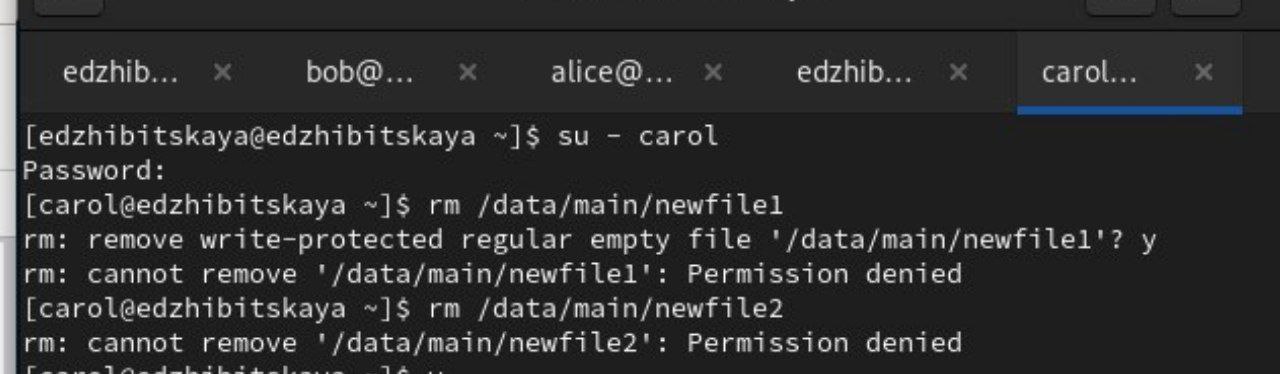


Рис. 11: Удаление файлов Carol

Наконец попробуем записать что-то в файлы. В 1 файл ничего записать не удаестся(нет права на исполнение у группы third), а во второй, благодаря ACL, это возможно(рис. 12).

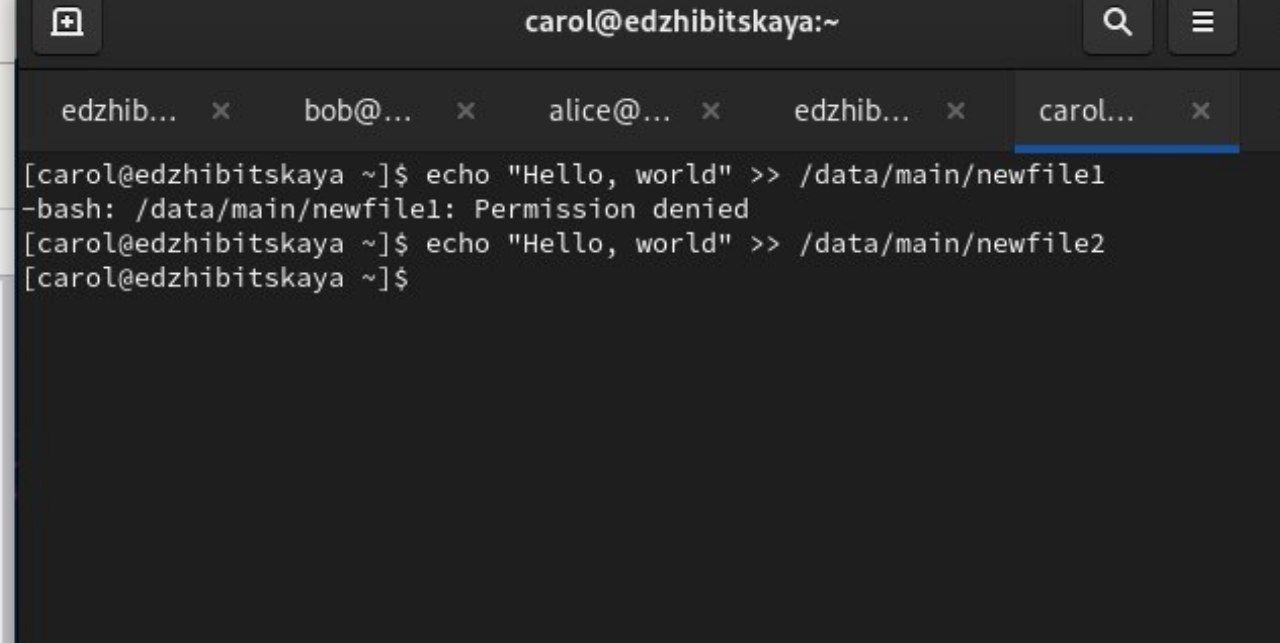


Рис. 12: Запись в файлы

# 3 Ответы на контрольные вопросы

1. Для установки владельца группы для файла с помощью команды chown нужно использовать:

* chown :группа файл

Пример: chown bob:main /data/third/newfile1

1. Для поиска всех файлов, принадлежащих конкретному пользователю, можно использовать команду find. Пример:

* find /путь/к/каталогу -user имя\_пользователя

Пример: find /home -user bob

1. Чтобы применить разрешения на чтение, запись и выполнение для всех файлов в каталоге /data для пользователей и владельцев групп, не устанавливая никаких прав для других, можно использовать команду chmod следующим образом(рис. 13).

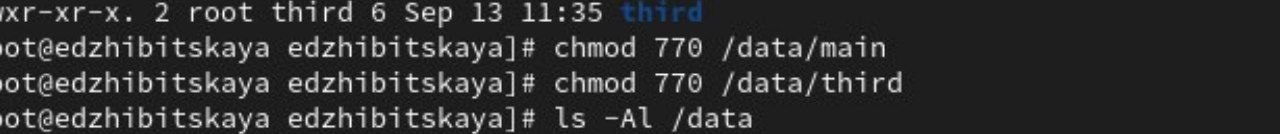


Рис. 13: Пример

chmod 770 /data/\*

1. Чтобы добавить разрешение на выполнение для файла, необходимо использовать команду chmod. Пример:

* chmod +x файл

Пример: chmod +x script.sh

1. Команда, которая позволяет убедиться, что групповые разрешения для всех новых файлов, создаваемых в каталоге, будут присвоены владельцу группы этого каталога, называется chmod с установленным битом SGID. Пример(рис. 14).

* chmod g+s /путь/к/каталогу

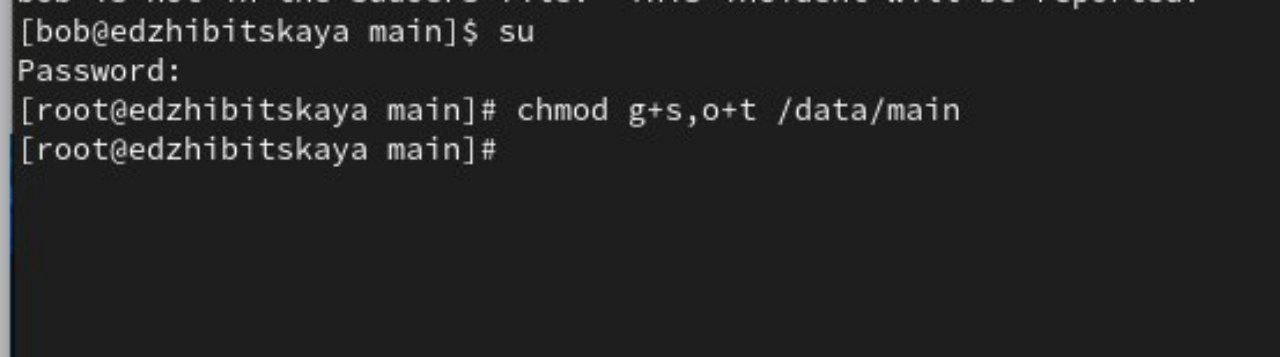


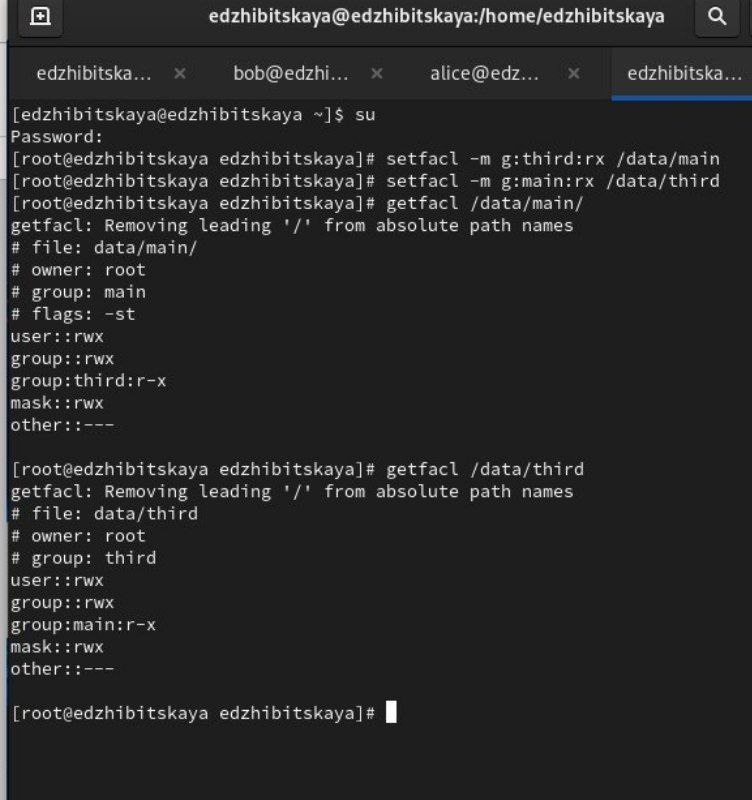
Рис. 14: Пример

1. Можно использовать команду chmod. Например, установить права доступа к каталогу, где находятся файлы, таким образом, чтобы только владелец мог удалять файлы. Это может выглядеть так:

chmod 700 /path/to/directory

1. Для добавления ACL, который предоставляет членам группы права доступа на чтение для всех существующих файлов в текущем каталоге, можно использовать команду setfacl. Например, чтобы предоставить группе “mygroup” права на чтение, используйте следующую команду(рис. **¿fig:015?**).

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

:

1. Чтобы гарантировать, 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, можно использовать следующие команды:

setfacl -R -m g:mygroup:rX /path/to/directory setfacl -R -d -m g:mygroup:rX /path/to/directory

1. Нужно установить umask на 007. umask 007
2. Защита файла от случайного удаления

chattr +i myfile

После этого файл не сможет быть удалён или изменён ни одним пользователем, пока атрибут не будет снят с помощью chattr -i myfile.

# 4 Выводы

В ходе работы было произведено знакомство с правами доступа и разрешениями для групп пользователей в ОС Linux, реализовано наделение ими.