Лабораторная работа №3

Настройка прав доступа

Колонтырский Илья Русланович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

2.1 Управление базовыми разрешениями

Создим структуру каталогов с разными разрешениями доступа для разных групп пользователей.

Откроем терминал с учётной записью root, создадим каталоги и посмотрим, кто является их владельцем (рис. 2.1).

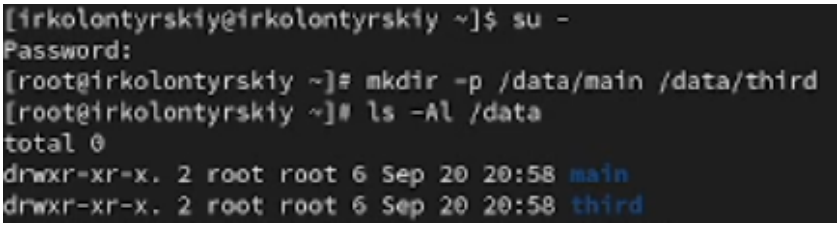

Рис. 2.1: владелец каталогов

Изменим владельцев этих каталогов с **root** на **main** и **third**(рис. 2.2).

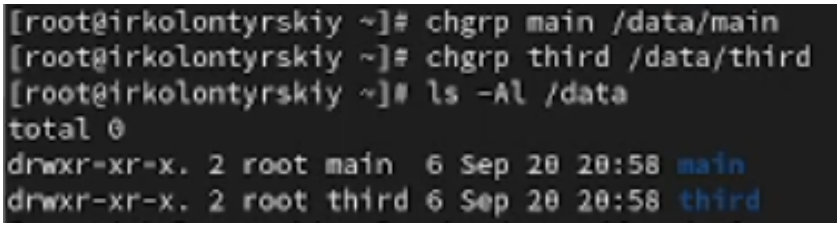

Рис. 2.2: изменение владельцев

Установим разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам (рис. 2.3).

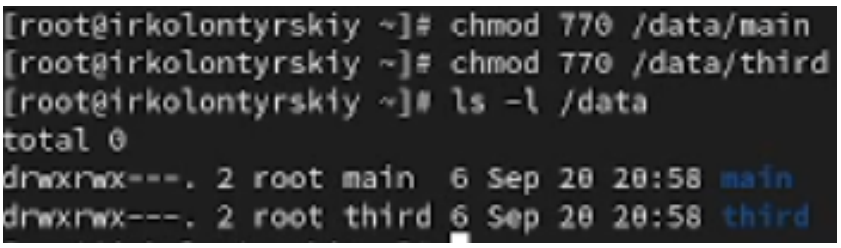

Рис. 2.3: установка разрешений

В другом терминале перейдём под учётную запись пользователя bob и попробуем перейти в каталог **/data/main** и создать файл **emptyfile**. У нас получится это сделать, так как боб состоит в группе main, а права доступа == 770 (рис. 2.4).

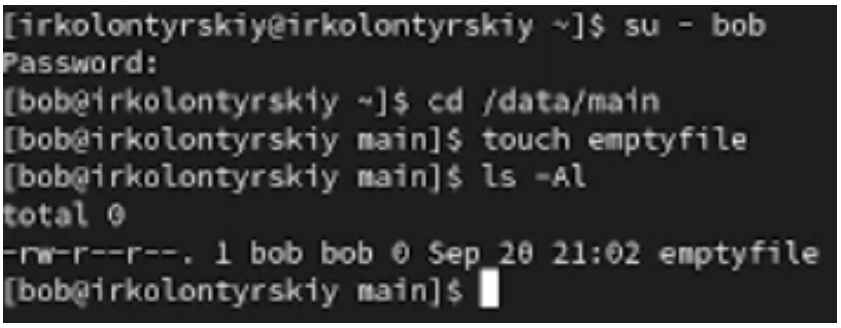

Рис. 2.4: попытка редактирования main бобом

Под пользователем bob попробуем перейти в каталог **/data/third** и создать файл **emptyfile** в этом каталоге. У нас не получится даже перейти в каталог, так как боб не состоит в группе **third**

Создадим пользователя bob и посмотрим, в каких группах он состоит(рис. 2.5).

Рис. 2.5: попытка редактирования third бобом

2.2 Управление специальными разрешениями

Разберем работу со **sticky bit**

Откроем терминал под пользователем alice и создадим в каталоге **/data/main** два файла(рис. 2.6)

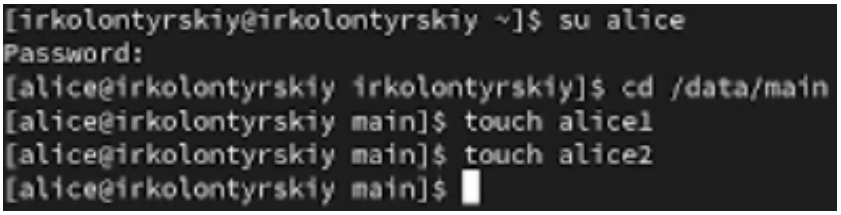

Рис. 2.6: Создание файлов элис

Перейдём под учётную запись пользователя bob и попытаемся удалить файлы пользователя alice. Убедимся, что они удалены (рис. 2.7)

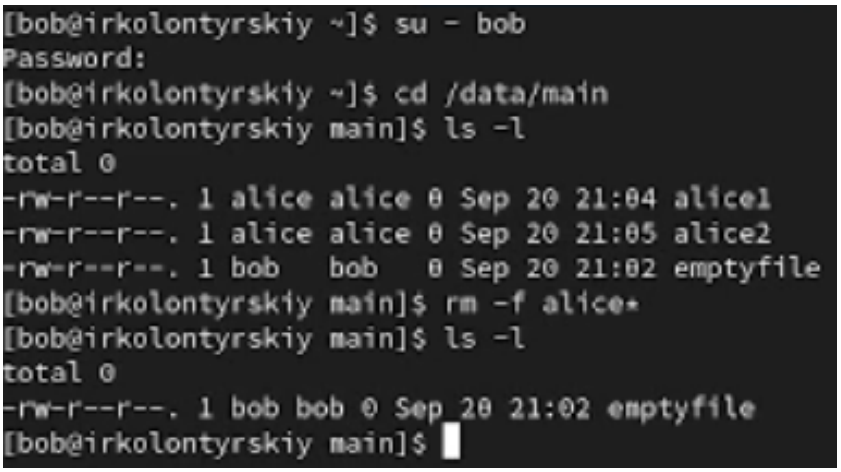

Рис. 2.7: удаление файлов элис с учетки боба

Создадим два файла с учетной записи пользователя **bob** (рис. 2.8).

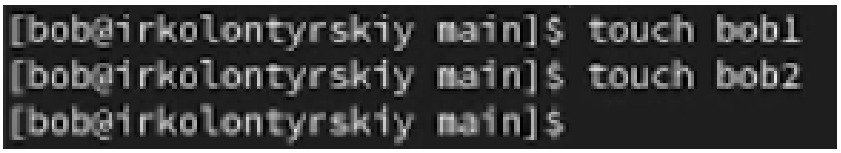

Рис. 2.8: создание файлов боба

В терминале под пользователем root установим для каталога /data/main бит идентификатора группы, а также stiky-бит для разделяемого (общего) каталога группы (рис. 2.9)

Рис. 2.9: установка бит для каталога

Переключимся на учётную запись пользователя alice, создадим два файла. Видим, что они принадлежат группе main. Также попробуем удалить файлы, принадлежащие бобу. У нас это не выйдет, так как sticky-bit предотвратит удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов (рис. 2.10)

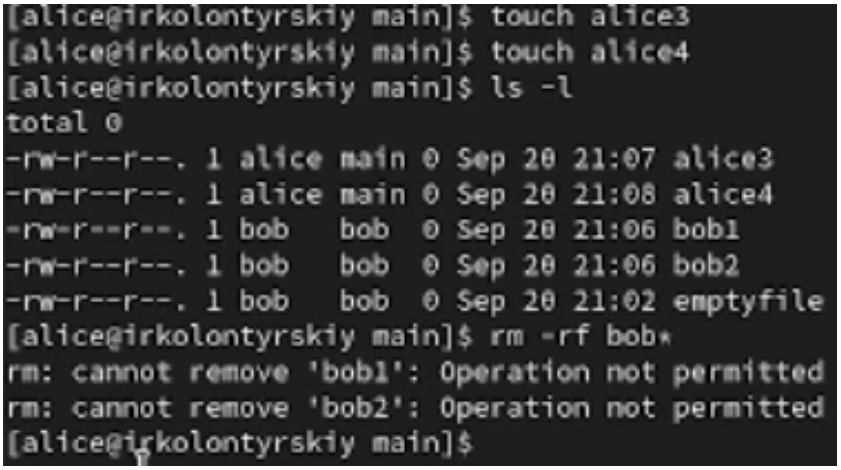

Рис. 2.10: работа с файлами и доступом

2.3 Управление расширенными разрешениями с использованием списков ACL

Откроем терминал с учётной записью **root**, установим права на чтение и выполнение в каталогах и используем команду **getfacl**, чтобы убедиться в правильности установки разрешений (рис. 2.11)

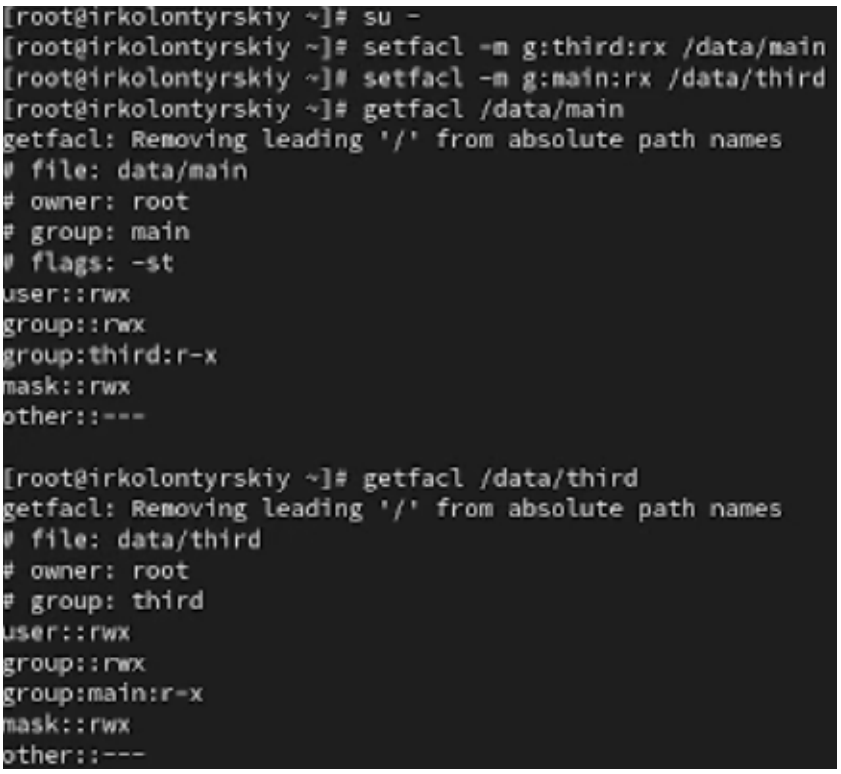

Рис. 2.11: работа с разрешениями

Создадим новый файл с именем **newfile1** в каталоге **/data/main**, проверим текущие назначенные ему полномочия. Люди из группы и остальные имеют только право на чтение (мы это назначили) (файл неисполняем) (рис. 2.12)

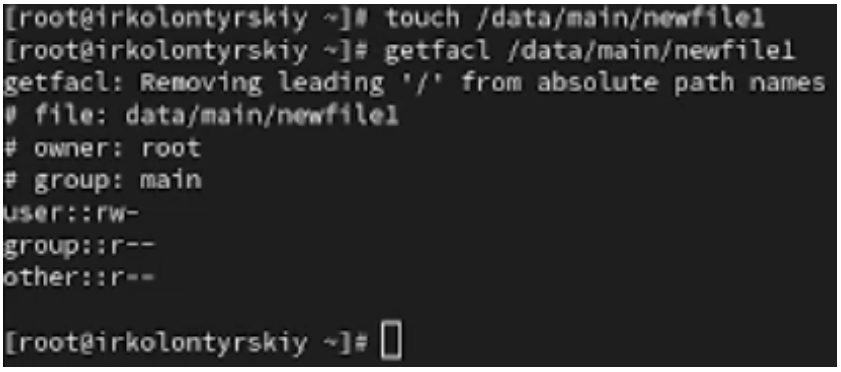

Рис. 2.12: проверка полномочий

Выполним аналогичные действия для каталога **/data/third**. Полномочия такие же, отличается только группа. (рис. 2.13)

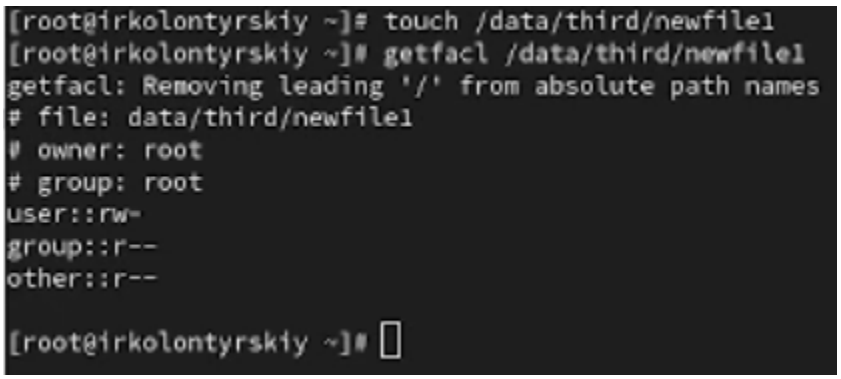

Рис. 2.13: аналогичные действия

Установим ACL по умолчанию для каталогов и убедимся, что настройки работают, добавив новый файл в каталог. (рис. 2.14)

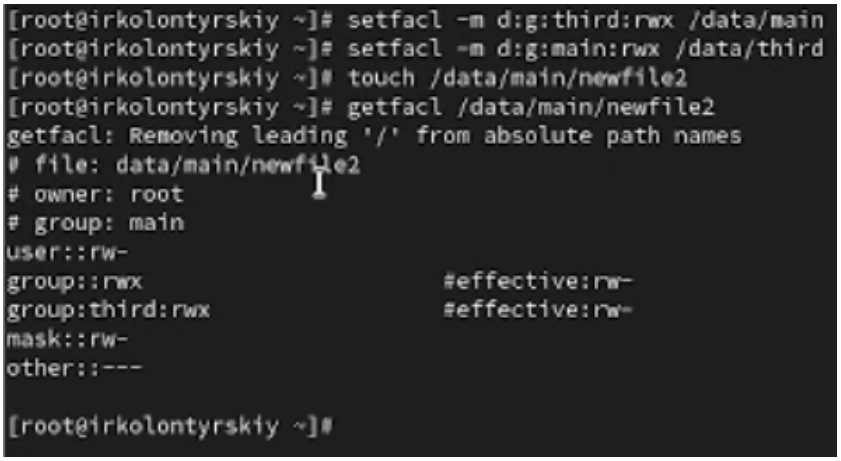

Рис. 2.14: проверка настроек ACL

Проведем аналогичные действия для каталога /data/third (рис. 2.15).

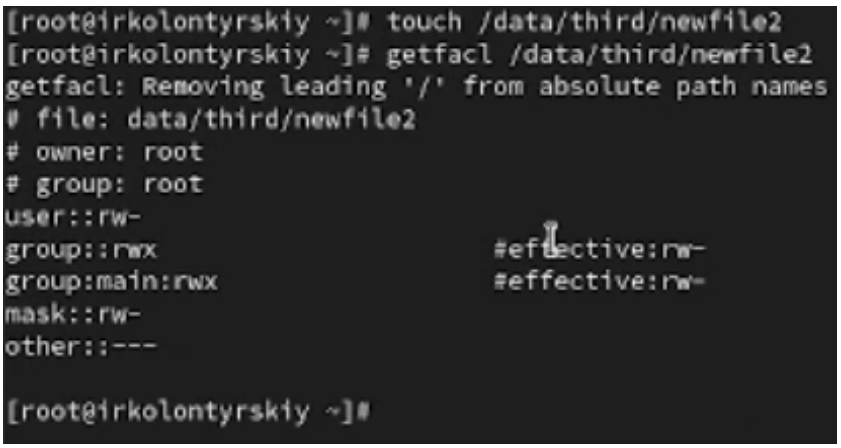

Рис. 2.15: настройки ACL

Для проверки полномочий группы **third** в каталоге **/data/third** войдём в другом терминале под учётной записью члена группы **third** и проверим операции с файлами

Удалить файлы не получится, так как он не является владельцем, однако сможет внести изменения во второй файл, потому что мы создали его после изменения настроек полномочий(рис. 2.16)

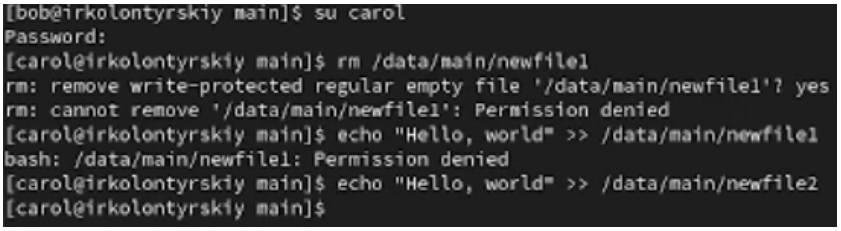

Рис. 2.16: проверка полномочий пользователя группы third

3 Контрольные вопросы

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

Чтобы установить владельца и группу для файла, нужно использовать команду chown следующим образом:

chown :groupname filename

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

Для этого можно использовать команду find:

find /path/to/search -user username

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?**

Используем команду chmod:

chmod 770 /data/*

4. **Какая команда позволяет добавить разрешение на выполнение для файла, который необходимо сделать исполняемым?**

chmod +x filename

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

chmod g+s /path/to/directory

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?**

chmod g+s,o+t /путь

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

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

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?**

Использовать команду setfacl с флагом -R (рекурсивно)
setfacl -R -m g:groupname:rX /path/to/directory

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

umask 007

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

chattr +i myfile

4 Вывод

В ходе выполнения лабораторной работы я получил навыки настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.

Список литературы

Туис, курс Администрирование операционных систем