Отчёт по лабораторной работе 3

Настройка прав доступа

Цвелев С.А. НПИбд-02-22

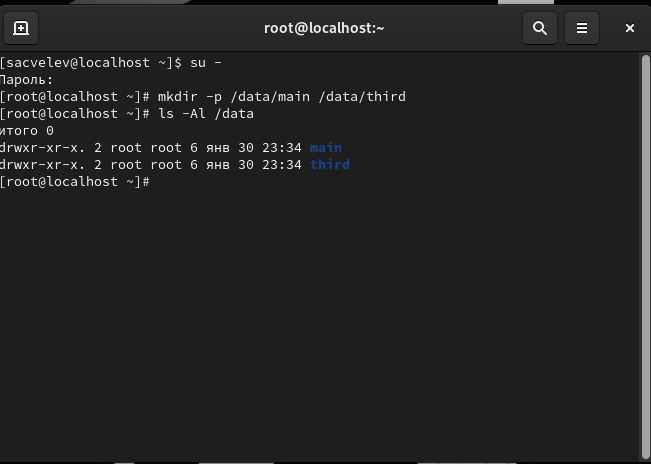
Содержание

# 1 Цель работы

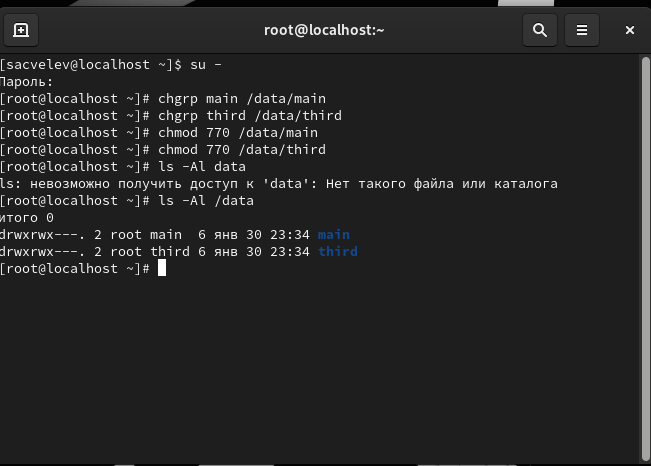
Получение навыков настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.

# 2 Выполнение лабораторной работы

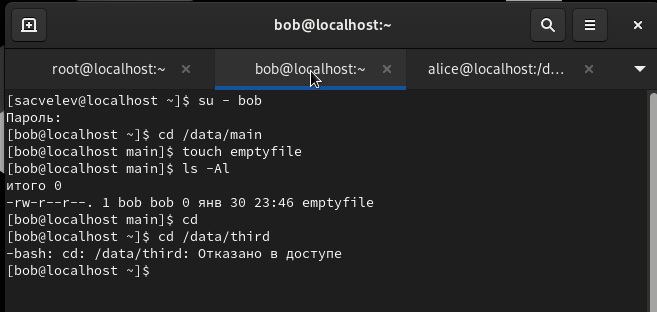
Открываем терминал с учётной записью root, создаём каталоги /data/main и /data/third. Проверяем, кто является их владельцами.



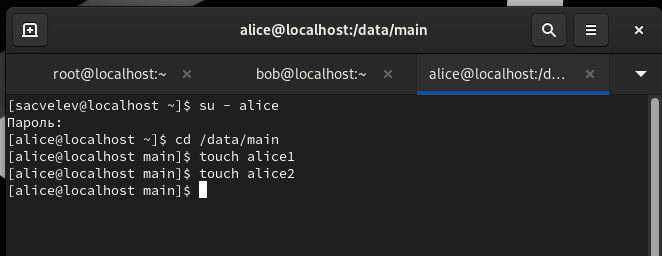
Затем ставим владельцев на main и third, затем устанавливаем им разрешения, позволяющие записывать владельцам файлы в эти каталоги и запрещающие доступ другим пользователям и группам.



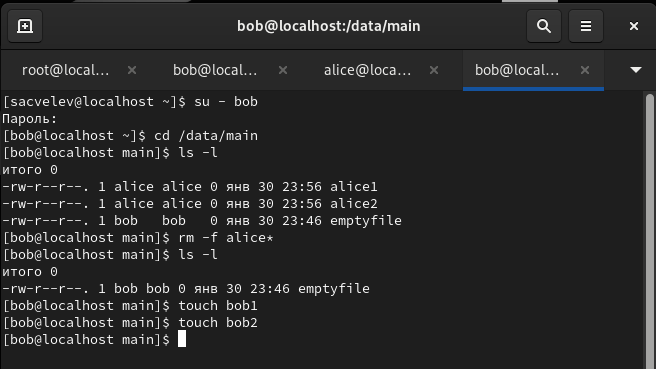
В другом терминале заходим под пользователем bob и, перейдя в каталог /data/main, создаем emptyfile. Получилось. Повторяем то же самое с каталогом /data/third и видим ошибку доступа. Вспоминаем, что в прошлой работе мы назначили bob в группу доступа main, в то время как third находится в отдельной. Вот поэтому и не получилось добавить файл в каталоге third.



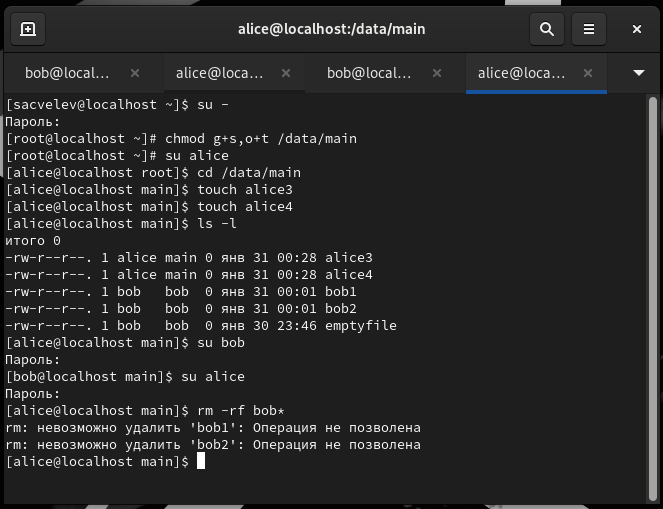
В другом терминале заходим под пользователем alice и создаем в /data/main файлы alice1 и alice2



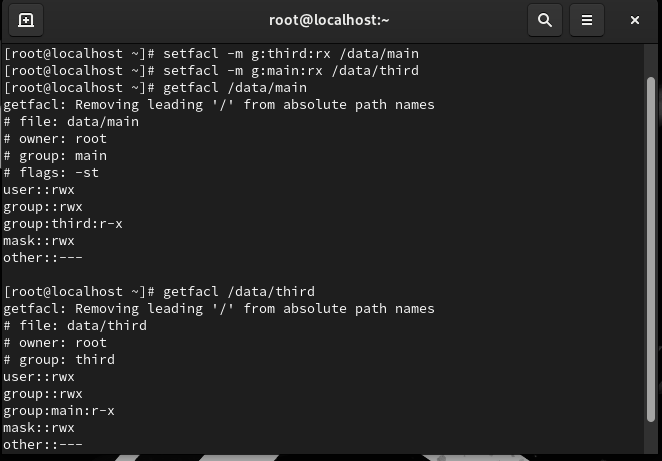
Переходим на пользователя bob и, перейдя в каталог /data/main, удаляем все файлы, принадлежащие пользователю alice (само собой, проверяем). После, создаём файлы bob1 и bob2



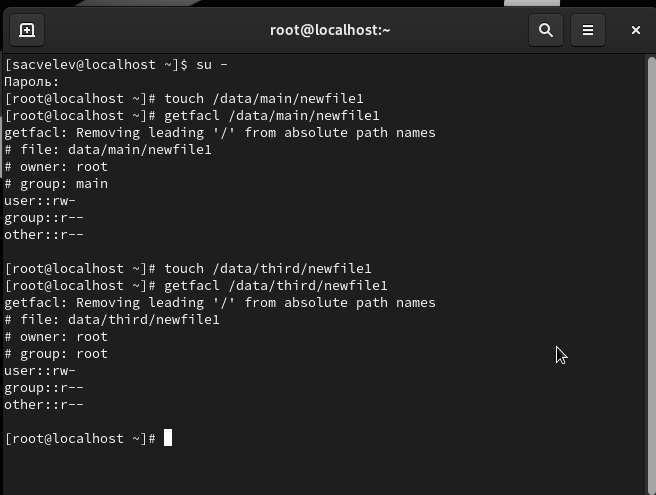
Под пользователем root устанавливаю для /data/main бит идентификатора группы и sticky-бит для общего каталога группы. Теперь, под пользователем alice создаю там файлы alice3 и alice4, что принадлежат группе main. Пробую удалить этим пользователем файлы пользователя bob и убеждаюсь, что это не удаётся.



Устанавливаем права на чтение и выполнение в каталогах /data/main и /data/third для групп third и main. Используем getfacl, чтобы убедиться.



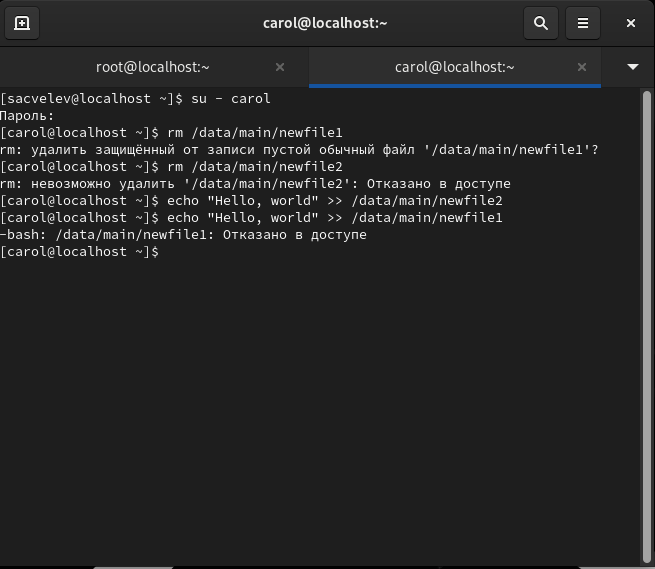
В каталогах /data/main и /data/third создаем файл newfile1. Затем проверяю полномочия с помощью getfacl. Как можно заметить, владельцем /data/third/newfile1 является группа root.



Устанавливаю ACL по умолчанию для каталогов /data/main и /data/third. Убеждаюсь, что настройки работают, добавив в /data/main файл newfile, и проверяю текущие полномочия.



Вхожу под пользователем carol и проверяю операции с файлом. Пытаюсь удалить newfile1 в папке /data/main, а затем newfile2. С newfile1 ничего не получается, ибо он защищён от записи.



# Контрольные вопросы

1. Для установки владельца группы с использованием команды chown нужно указать опцию -R для рекурсивного применения изменений ко всему содержимому каталога. chown bob:main /data/third/newfile
2. Для поиска всех файлов, принадлежащих конкретному пользователю, можно использовать команду find. find ~ -user bob -print
3. Для установки разрешений на чтение, запись и выполнение для всех файлов в каталоге /data для пользователей и владельцев групп используется chmod. Пример: chmod 770 /data
4. Для добавления разрешения на выполнение используйте команду chmod с опцией +x. Пример: chmod +x file
5. Чтобы убедиться, что групповые разрешения для новых файлов сохраняют владельцу группы каталога, используется getfacl. Пример: getfacl “имя каталога”
6. Для ограничения удаления файлов только владельцами используется команда chmod. Пример: chmod g+s,o+t /data/main
7. Для добавления ACL и предоставления членам группы прав на чтение используется setfacl. Пример: setfacl -m g:group:r <file/dir>
8. Чтобы гарантировать разрешения для всех файлов и подкаталогов, используется опция -dm с setfacl. Пример: setfacl -dm g:group:r /dir
9. Чтобы установить umask, чтобы другие пользователи не получали разрешений, используется 007.
10. Для предотвращения случайного удаления файла используется команда chattr с опцией +i. Пример: chattr +i myfile.