Лабораторная работа №3

Настройка прав доступа

Перфилов Александр Константинович | группа НПИбд 03-24

Содержание

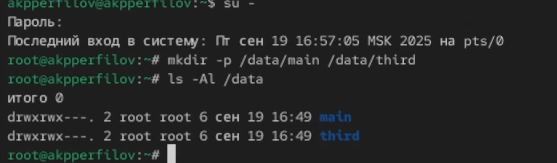
# 1. Цель работы

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

# 2. Выполнение лабораторной работы

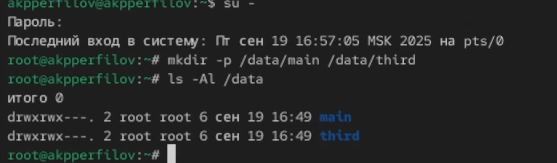
## 2.1 Управление базовыми разрешениями

Откроем терминал с учётной записью root В корневом каталоге создадим каталоги /data/main и /data/third: mkdir -p /data/main /data/third



Создание каталогов с root

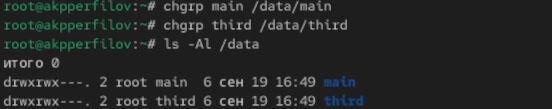
Посмотрим, кто является владельцем этих каталогов. Для этого используем: ls -Al /data



Просмотр информации о каталогах

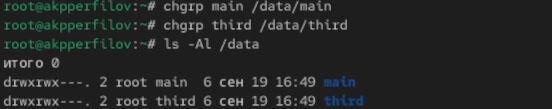
Прежде чем устанавливать разрешения, изменим владельцев этих каталогов с root на main и third соответственно:

chgrp main /data/main chgrp third /data/third



Изменение владельцев каталогов

Посмотрим, кто теперь является владельцем этих каталогов: ls -Al /data

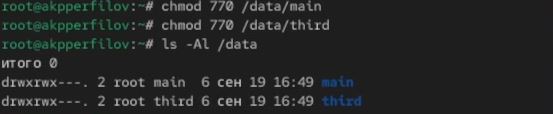


Просмотр информации о каталогах

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

chmod 770 /data/main chmod 770 /data/third

Проверим установленные права доступа

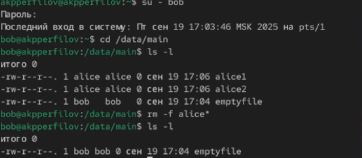


Изменение разрешений и просмотр прав доступа

В другом терминале перейдем под учётную запись пользователя bob Попробуем перейти в каталог /data/main и создать файл emptyfile в этом каталоге:

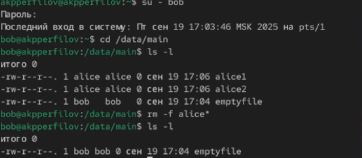
cd /data/main touch emptyfile ls -Al

Создался файл с правами под учетную запись пользователя bob



Создание файла под учётной записью bob

Под пользователем bob попробуем перейти в каталог /data/third и создать файл emptyfile в этом каталоге

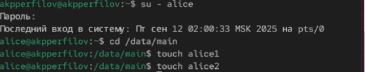


Попытка перейти в каталог

## 2.2 Управление специальными разрешениями

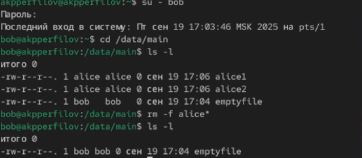
Откроем новый терминал под пользователем alice. Перейдем в каталог /data/main: cd /data/main Создадим два файла, владельцем которых является alice:

touch alice1 touch alice2



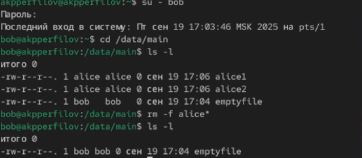
Создание файлов под учётной записью alice в каталоге /data/main

В другом терминале перейдем под учётную запись пользователя bob Перейдем в каталог /data/main и введем: ls -l



Просмотр информации о каталоге

Мы увидим два файла, созданные пользователем alice. Попробуем удалить файлы, принадлежащие пользователю alice: rm -f alice\* Убедимся, что файлы будут удалены пользователем bob.



Удаление файлов alice и просмотр информации каталога

Создадим два файла, которые принадлежат пользователю bob:

touch bob1 touch bob2

Создание файлов под учётной записью bob

Создание файлов под учётной записью bob

В терминале под пользователем root установим для каталога /data/main бит идентификатора группы, а также stiky-бит для разделяемого (общего) каталога группы: chmod g+s,o+t /data/main

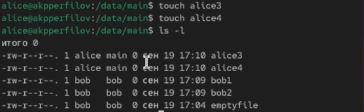
Изменение бит индентификатора группы и sticky-бит для общего каталога группы

Изменение бит индентификатора группы и sticky-бит для общего каталога группы

В терминале под пользователем alice создадим в каталоге /data/main файлы alice3 и alice4:

touch alice3 touch alice4 ls -l

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



Создание файлов и просмотр информации о них

В терминале под пользователем alice попробуем удалить файлы, принадлежащие пользователю bob: rm -rf bob\*

Попытка удаление файлов

Попытка удаление файлов

Как мы видим sticky-bit предотвратил удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов. Обратим внимание: поскольку пользователь alice является владельцем каталога /data/main, то он может удалить все свои файлы в любом случае.

## 2.3 Управление расширенными разрешениями с использованием списков ACL

Применим команды setfacl и getfacl для выполнения поставленной задачи. 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:

setfacl -m g:third:rx /data/main setfacl -m g:main:rx /data/third

Изменение прав каталогов для групп

Изменение прав каталогов для групп

Используем команду getfacl, чтобы убедиться в правильности установки разрешений:

getfacl /data/main getfacl /data/third

(image/5363977445180569467.jpg)

Создадим новый файл с именем newfile1 в каталоге /data/main: touch /data/main/newfile1 Используем getfacl /data/main/newfile1 для проверки текущих назначений полномочий.

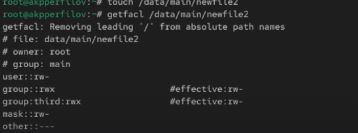


Создание файла и просмотр информации о нём

Установим ACL по умолчанию для каталога /data/main: setfacl -m d:g:third:rwx /data/main

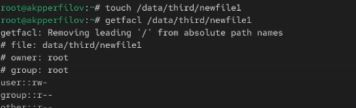
Убедимся, что настройки ACL работают, добавив новый файл в каталог /data/main: touch /data/main/newfile2

Используем getfacl /data/main/newfile2 для проверки текущих назначений полномочий



Создание файла и просмотр информации

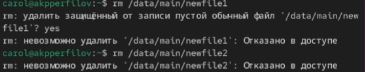
Выполним аналогичные действия для каталога /data/third. Создадим новый файл newfile2 в каталог /data/third и проверим текущие назначения полномочий



Создание файла и просмотр информации

Для проверки полномочий группы third в каталоге /data/third войдем в другом терминале под учётной записью члена группы third: su - carol Проверим операции с файлами:

rm /data/main/newfile1 rm /data/main/newfile2



Попытка удаление файлов под учётной записью carol

Удалить файлы мы не смогли, так как newfile1 принадлежит пользователю root и группе main, newfile2 также принадлежит root, main и third, хоть и carol находится в последней группе, у группы недостаточно прав.

Проверим, возможно ли осуществить запись в файл:

echo “Hello, world” >> /data/main/newfile1 echo “Hello, world” >> /data/main/newfile2

Попытка осуществить запись в файлы под учётной записью carol

Попытка осуществить запись в файлы под учётной записью carol

Мы не смогли осуществить запись в newfile1, так как прав у группы third на нее нет. А вот уже в newfile2 все получилось, так как права на изменение файла у данной группы есть.

# 3. Выводы

Приобретены умения по управлению базовыми и специальными правами доступа для групп пользователей в ОС Linux.

# Список литературы