Отчёт по лабораторной работе №3

Дисциплина: Основы администрирования операционных систем

Верниковская Екатерина Андреевна

Содержание

# 1 Цель работы

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

# 2 Задание

1. Прочитать справочное описание man по нескольким командам.
2. Выполнить действия по управлению базовыми разрешениями для групп пользователей.
3. Выполнить действия по управлению специальными разрешениями для групп пользователей.
4. Выполнить действия по управлению расширенными разрешениями с использованием списков ACL для групп пользователей.

# 3 Выполнение лабораторной работы

## 3.1 Справочное описание команд

Открываем терминал и читаем справочное описание man по командам ls, whoami, id, groups, su, sudo, passwd, vi, visudo, useradd, usermod, userdel, groupadd, groupdel (рис. 1), (рис. 2), (рис. 3), (рис. 4), (рис. 5)

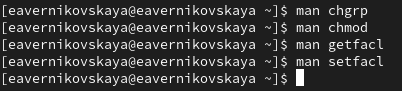


Рис. 1: Команда man

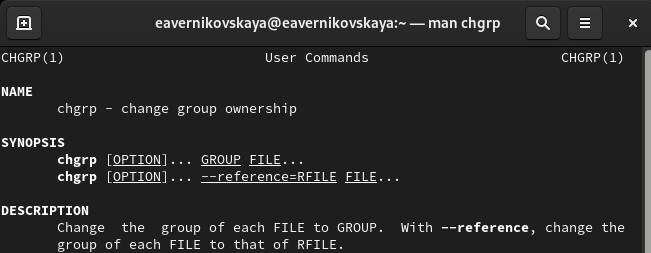


Рис. 2: Справка по команде chgrp

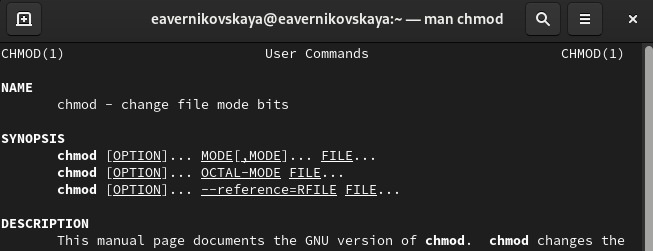


Рис. 3: Справка по команде chmod

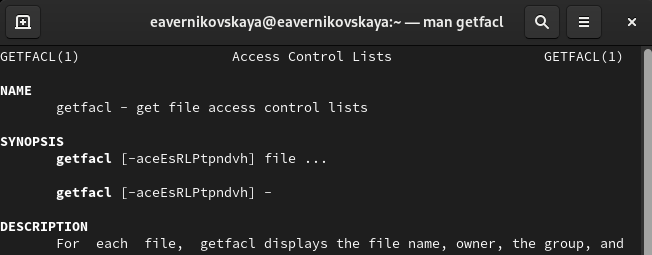


Рис. 4: Справка по команде getfacl

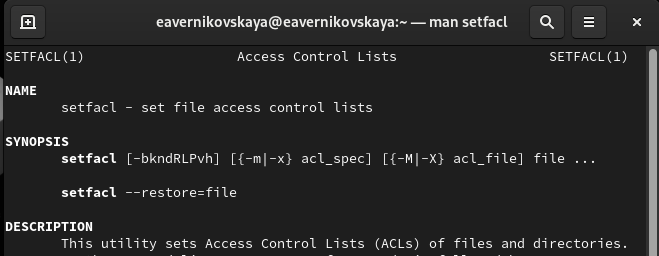


Рис. 5: Справка по команде setfacl

## 3.2 Управление базовыми разрешениями

Открываем терминал с учётной записью root: *su -* (рис. 6)

Учётная запись root

Рис. 6: Учётная запись root

В корневом каталоге создаём каталоги /data/main и /data/third (рис. 7)

Создание каталогов /data/main и /data/third

Рис. 7: Создание каталогов /data/main и /data/third

Смотрим, кто является владельцем этих каталогов. Владельцем каталогов является суперпользователь root (рис. 8)

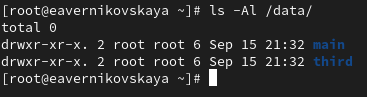


Рис. 8: Информация о каталогах /data/main и /data/third (1)

Далее меняем владельцев этих каталогов с root на main и third соответственно, с помощью команды *chgrp* (рис. 9)

Изменение владельцев каталогов /data/main и /data/third

Рис. 9: Изменение владельцев каталогов /data/main и /data/third

Проверяем, кто теперь является владельцем этих каталогов. (рис. 10)

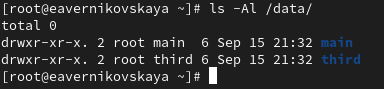


Рис. 10: Информация о каталогах /data/main и /data/third (2)

Установливаем разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам (рис. 11)

Установление разрешений

Рис. 11: Установление разрешений

Далее проверяем установленные права доступа (рис. 12)

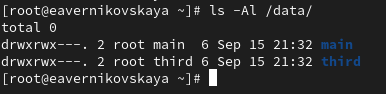


Рис. 12: Установленные права доступа

В другом терминале переходим под учётную запись пользователя bob: *su - bob* (рис. 13)

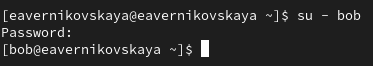


Рис. 13: Учётная запись bob

Под пользователем bob пробуем перейти в каталог /data/main и создать файл emptyfile в этом каталоге. Так как пользователь bob является владельцем каталога main, нам удалось перейти в этот каталог и создать в нём новый файл (рис. 14)

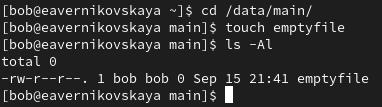


Рис. 14: Каталог /data/main в учётной записи bob и создание файла

Под пользователем bob пробуем перейти в каталог /data/third и создать файл emptyfile в этом каталоге. Так как пользователь bob не является владельцем каталога third, нам не удалось перейти в этот каталог и создать в нём новый файл (рис. 15)

Каталог /data/third в учётной записи bob и создание файла

Рис. 15: Каталог /data/third в учётной записи bob и создание файла

## 3.3 Управление специальными разрешениями

Открываем новый терминал под пользователем alice (рис. 16)

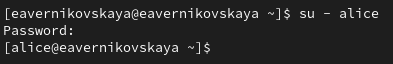


Рис. 16: Учётная запись alice

Переходим в каталог /data/main и создаём два файла, владельцем которых является alice (рис. 17), (рис. 18)

Переход в каталог /data/main под alice

Рис. 17: Переход в каталог /data/main под alice

Создание файлов alice1 и alice2

Рис. 18: Создание файлов alice1 и alice2

В другом терминале переходим под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice). Далее переходим в каталог /data/main и видим там два файла, созданные пользователем alice (рис. 19)

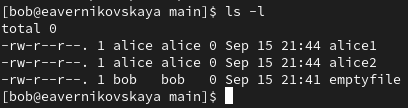


Рис. 19: Файлы, которые видит bob

Попробуем удалить файлы, принадлежащие пользователю alice. Файлы успешно удалены (рис. 20)

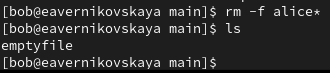


Рис. 20: Удаление файлов (1)

Создаём два файла, которые принадлежат пользователю bob (рис. 21)

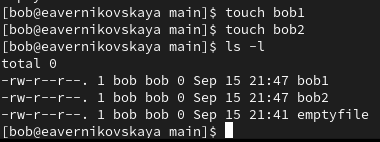


Рис. 21: Создание файлов bob1 и bob2

В терминале под пользователем root устанавливаем для каталога /data/main бит идентификатора группы, а также stiky-бит для разделяемого (общего) каталога группы *chmod g+s,o+t /data/main* (рис. 22)

Установка бит идентификатора группы и stiky-бит для разделяемого (общего) каталога группы

Рис. 22: Установка бит идентификатора группы и stiky-бит для разделяемого (общего) каталога группы

В терминале под пользователем alice создаём в каталоге /data/main файлы alice3 и alice4. Теперь мы видим, что два созданных нами файла принадлежат группе main, которая является группой-владельцем каталога /data/main (рис. 23)

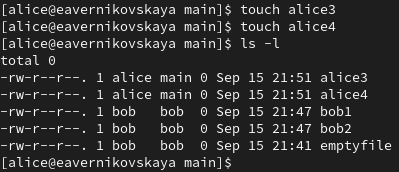


Рис. 23: ИНформация о файлах alice3 и alice4

В терминале под пользователем alice пробуем удалить файлы, принадлежащие пользователю bob. Sticky-bit предотвратит удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов (operation not permitted)(рис. 24)

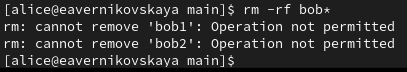


Рис. 24: Удаление файлов (2)

## 3.4 Управление расширенными разрешениями с использованием списков ACL

Открываем терминал с учётной записью root и устанавливаем 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, используя *setfacl -m* (рис. 25)

Установка прав на чтение и выполнение в каталогах для групп

Рис. 25: Установка прав на чтение и выполнение в каталогах для групп

Используем команду *getfacl*, чтобы убедиться в правильности установки разрешений (рис. 26), (рис. 27)

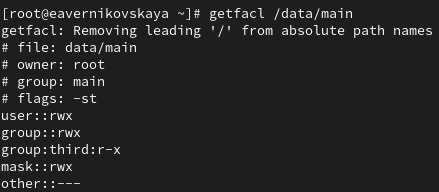


Рис. 26: Проверка правильности установки разрешений в каталоге main

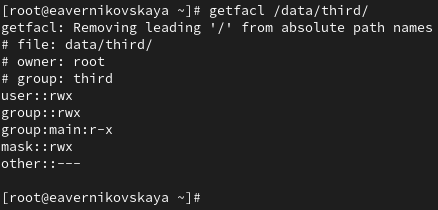


Рис. 27: Проверка правильности установки разрешений в каталоге third

Создаём новый файл с именем newfile1 в каталоге /data/main (рис. 28)

Создание newfile1 в каталоге /data/main

Рис. 28: Создание newfile1 в каталоге /data/main

Используем *getfacl /data/main/newfile1* для проверки текущих назначений полномочий. У пользователя только чтение и запись, у группы и других только чтение. Работать с этим файлом пользователи не могут, потому что мы устанавливали права на чтение и выполнение именно для каталогов, а не для созданных в нём файлов (рис. 29)

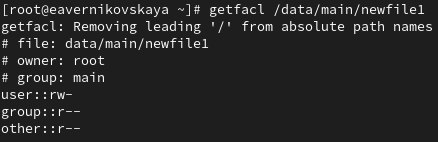


Рис. 29: Информация о файле newfile1 в каталоге /data/main

Выполняем аналогичные дейтвия для каталога /data/third. Пояснения те же самые что и к прошлому пункту (рис. 30)

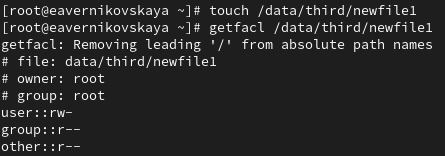


Рис. 30: Информация о файле newfile1 в каталоге /data/third

Устанавливаем ACL по умолчанию для каталога /data/main, с помощью *setfacl -m d:g:third:rwx* (рис. 31)

Утановка ACL по умолчанию для каталога /data/main

Рис. 31: Утановка ACL по умолчанию для каталога /data/main

Устанавливаем ACL по умолчанию для каталога /data/third (рис. 32)

Утановка ACL по умолчанию для каталога /data/third

Рис. 32: Утановка ACL по умолчанию для каталога /data/third

Добавляем новый файл newfile2 в каталог /data/main и проверяем, что настройки ACL работают (рис. 33), (рис. 34)

Создание newfile2 в каталоге /data/main

Рис. 33: Создание newfile2 в каталоге /data/main

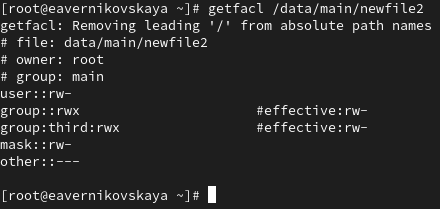


Рис. 34: Информация о файле newfile2 в каталоге /data/main

Выполняем аналогичные действия для каталога /data/third (рис. 35), (рис. 36)

Создание newfile2 в каталоге /data/third

Рис. 35: Создание newfile2 в каталоге /data/third

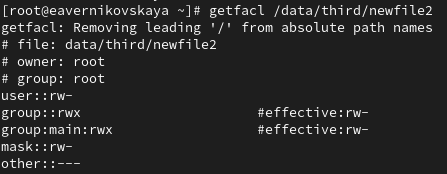


Рис. 36: Информация о файле newfile2 в каталоге /data/third

Для созданных файлов группы main возможны действия от пользователей группы third и наоборот

Далее заходим в другом терминале под учётной записью члена группы third - это carol (рис. 37)

Учётная запись carol

Рис. 37: Учётная запись carol

Далее проверяем операции с файлами newfile1 и newfile2. Пытаемся их удалить. Система не даёт нам этого сделать, так как удаление файлов это действие с каталогом, а к каталогу main у группы third нет полномочий (рис. 38)

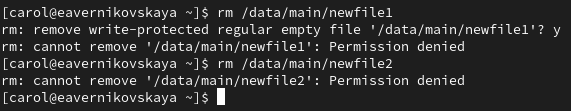


Рис. 38: Проверка операции удаления

Далее пытаемся осуществить запись в файлы. Система не даёт осуществить запись в newfile1, но разрешает сделать это в файле newfile2, так как ранее мы установили определённые разрешения (рис. 39)

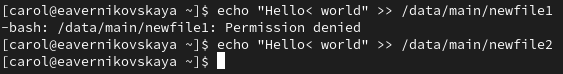


Рис. 39: Проверка операции записи в файл

# 4 Контрольные вопросы + ответы

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

chown bob:main /data/third/newfile

1. С помощью какой команды можно найти все файлы, принадлежащие конкретному пользователю? Приведите пример.

find ~ -user bob -print.

1. 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? Приведите пример.

chmod 770 /data (скриншот есть в лабораторной работе).

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

chmod +x file.

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

getfacl “имя каталога” (скриншот есть в лабораторной работе).

1. 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? Приведите пример.

chmod g+s,o+t /data/main (скриншот есть в лабораторной работе).

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

setfacl -m g:group:r (скриншот есть в лабораторной работе).

1. 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? Приведите пример.

setfacl -dm g:group:r /dir.

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

007

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

sudo chattr +i myfile.

# 5 Выводы

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

# 6 Список литературы

1. Лаборатораня работа №3 [Электронный ресурс] URL: https://esystem.rudn.ru/pluginfile.php/2400684/mod\_resource/content/4/004-permissions.pdf