# Постановка задачи

Получение навыков настройки базовых и специальных прав доступа для групп

пользователей в операционной системе типа Linux.

# Выполнение работы

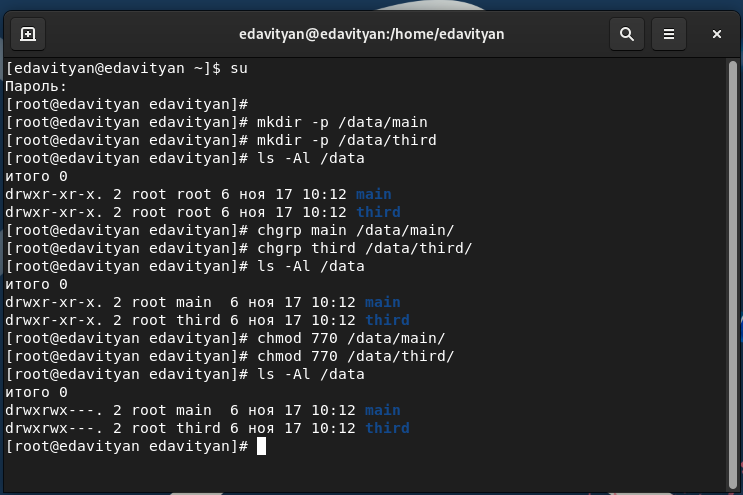
**3.3.1. Управление базовыми разрешениями Требуется создать структуру каталогов с разными разрешениями доступа для разных групп пользователей.**

1. Откройте терминал с учётной записью root: su –

2. В корневом каталоге создайте каталоги /data/main и /data/third: mkdir -p /data/main /data/third Посмотрите, кто является владельцем этих каталогов. Для этого используйте: ls - Al /data

3. Прежде чем устанавливать разрешения, измените владельцев этих каталогов с root на main и third соответственно: chgrp main /data/main chgrp third /data/third Посмотрите, кто теперь является владельцем этих каталогов.

4. Установите 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 Проверьте установленные права доступа.

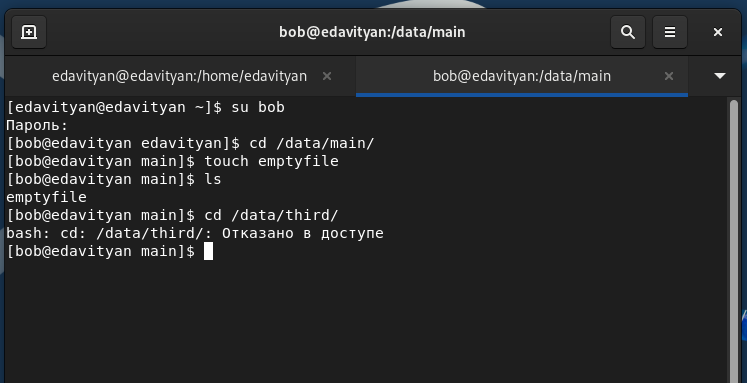


5. В другом терминале перейдите под учётную запись пользователя bob: su - bob

6. Под пользователем bob перейдите в каталог /data/main: cd /data/main Попробуйте создать файл emptyfile в этом каталоге: touch emptyfile Опишите и поясните результат этого действия.

7. Под пользователем bob перейдите в каталог /data/third: cd /data/third Попробуйте создать файл emptyfile в этом каталоге: touch emptyfile Опишите и поясните результат этого действия.

Bob смог создать файл только в каталоге /data/main, в каталог /data/third он даже не смог перейти. Этот каталог принадлежит группе, в которую Bob не входит



**3.3.2. Управление специальными разрешениями**

Требуется, используя специальные разрешения для групп пользователей, обеспечить обмен файлами в общем для групп каталоге. При этом каталогу назначается бит идентификатора группы, а также sticky bit. Sticky bit — дополнительный атрибут файлов или каталогов в ОС типа Linux, применяющийся в основном для каталогов с целью защиты содержимого каталогов от повреждения или удаления пользователями, не являющимися их владельцами. Для установки этого атрибута используется утилита chmod. Восьмеричное значение stiky-бита: 1000, а символьное: +t.

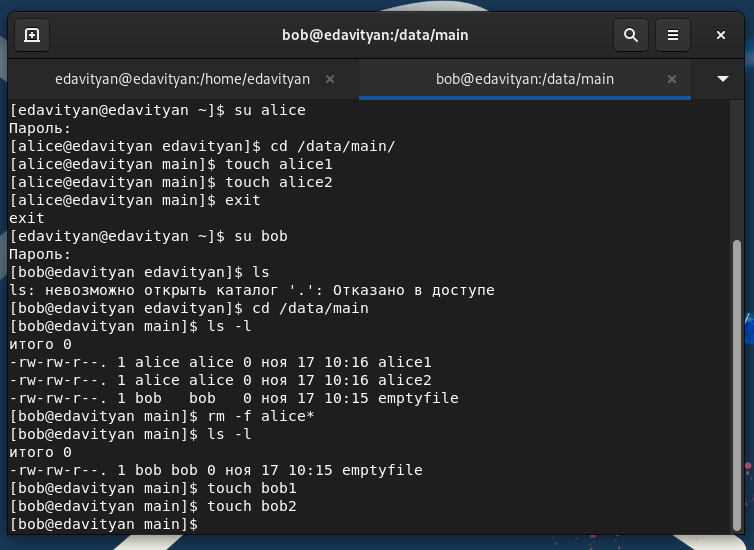
1. Откройте новый терминал под пользователем alice.

2. Перейдите в каталог /data/main: cd /data/main Создайте два файла, владельцем которых является alice: touch alice1 touch alice2

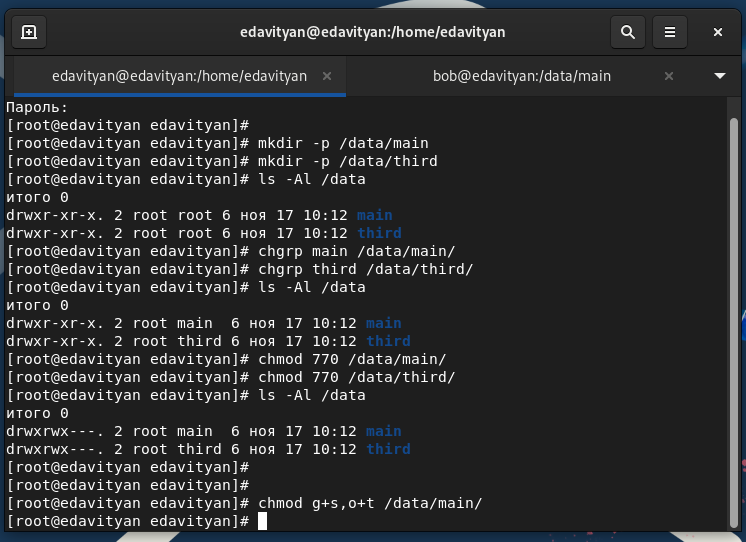
3. В другом терминале перейдите под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice): su - bob

4. Перейдите в каталог /data/main: cd /data/main и в этом каталоге введите: ls -l Вы увидите два файла, созданные пользователем alice. Попробуйте удалить фалы, принадлежащие пользователю alice: rm -f alice\* Убедитесь, что файлы будут удалены пользователем bob.

5. Создайте два файла, которые принадлежат пользователю bob: touch bob1 touch bob2

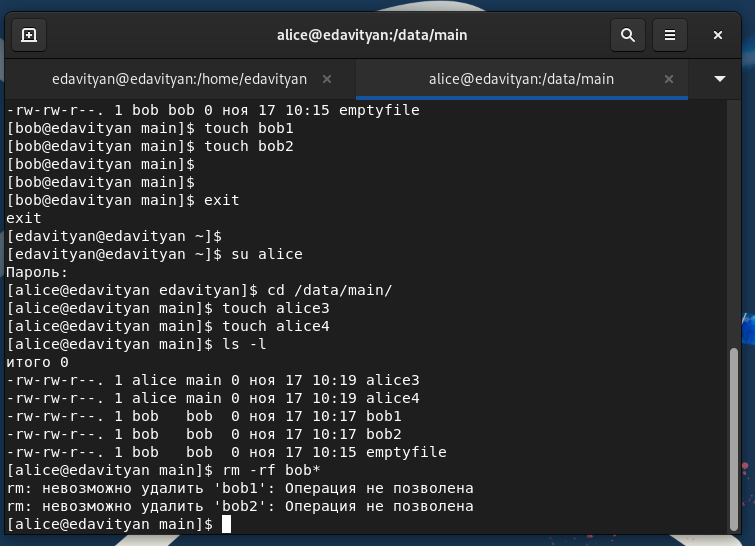


6. В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также stiky-бит для разделяемого (общего) каталога группы: chmod g+s,o+t /data/main



7. В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4: touch alice3 touch alice4 Теперь вы должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main.

8. В терминале под пользователем alice попробуйте удалить файлы, принадлежащие пользователю bob: rm -rf bob\* Убедитесь, что sticky-bit предотвратит удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов. Обратите внимание: поскольку пользователь alice является владельцем каталога /data/main, то он может удалить все свои файлы в любом случае.



**3.3.3. Управление расширенными разрешениями с использованием списков ACL**

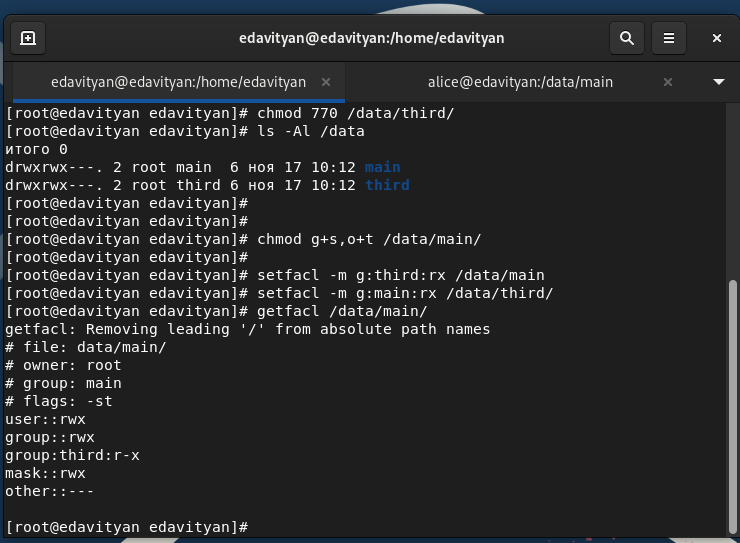
В этом упражнении продолжим работать в созданных ранее каталогах /data/main и /data/third. В предыдущих упражнениях для группы main были установлены разрешения на каталог /data/main, а у группы third —- на каталог /data/third. Требуется установить для группы third разрешения на чтение в каталоге /data/main, а для группы main — разрешения на чтение в каталоге /data/third. Затем требуется установить права доступа по умолчанию, чтобы убедиться в правильности установки разрешений для новых элементов этих каталогов. Для этого будет использоваться пакет acl и команды setfacl (для установки прав) и getfacl (для просмотра установленных прав). Кратко опишем синтаксис команды setfacl. Установить разрешения для пользователя: setfacl -m "u:user:permissions" Установить разрешения для группы: setfacl -m "g:group:permissions" Наследование записи ACL родительского каталога: setfacl -dm "entry"

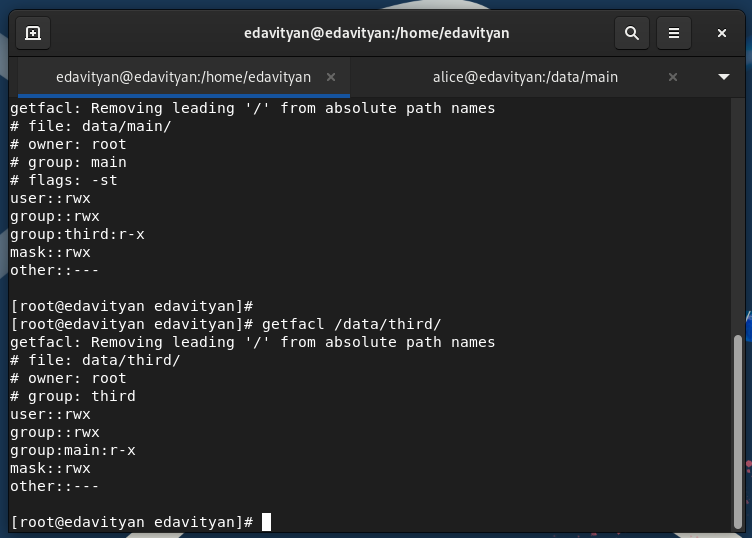
Удаление записи ACL: setfacl -x "entry" Синтаксис команды getfacl: getfacl Применим команды setfacl и getfacl для выполнения поставленной задачи.

1. Откройте терминал с учётной записью root su –

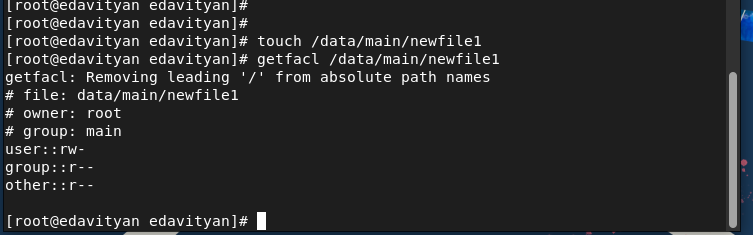
2. Установите права на чтение и выполнение в каталоге /data/main для группы third и права на чтение и выполнение для группы main в каталоге /data/third: setfacl -m g:third:rx /data/main setfacl -m g:main:rx /data/third

3. Используйте команду getfacl, чтобы убедиться в правильности установки разрешений: getfacl /data/main getfacl /data/third





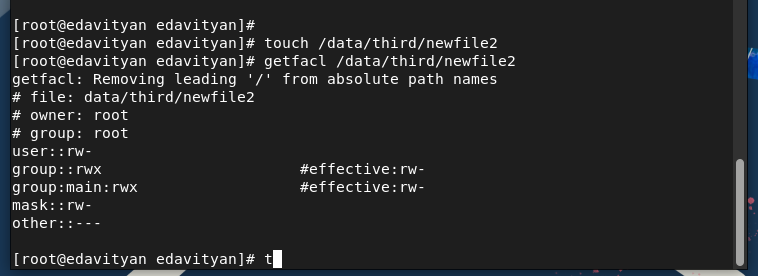
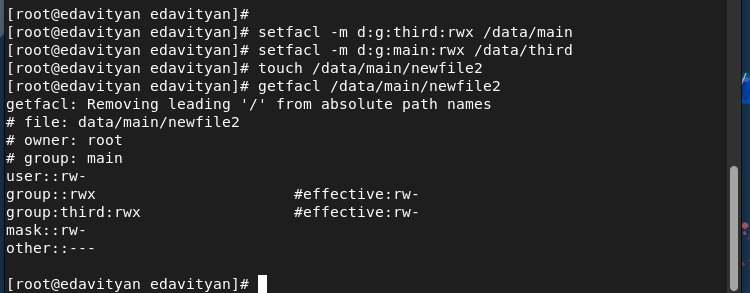
4. Создайте новый файл с именем newfile1 в каталоге /data/main: touch /data/main/newfile1 Используйте getfacl /data/main/newfile1 для проверки текущих назначений полномочий. Какие права доступа у этого файла? Объясните, почему? Выполните аналогичные действия для каталога /data/third. Дайте пояснения.



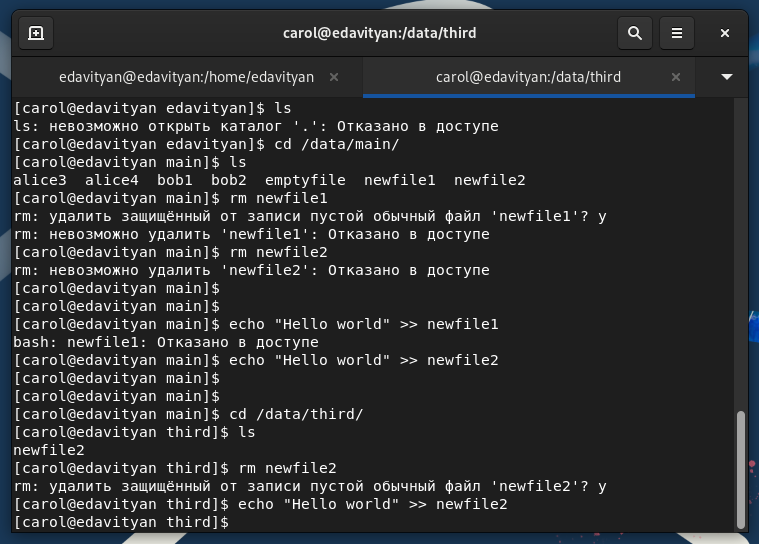
5. Установите ACL по умолчанию для каталога /data/main: setfacl -m d:g:third:rwx /data/main

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

7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main: touch /data/main/newfile2 Используйте getfacl /data/main/newfile2 для проверки текущих назначений полномочий. Выполните аналогичные действия для каталога /data/third.



8. Для проверки полномочий группы third в каталоге /data/third войдите в другом терминале под учётной записью члена группы third: su - carol Проверьте операции с файлами: rm /data/main/newfile1 rm /data/main/newfile1 Проверьте, возможно ли осуществить запись в файл: echo "Hello, world" >> /data/main/newfile1 echo "Hello, world" >> /data/main/newfile2 Объясните результат произведённых действий.



# Контрольные вопросы

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

сhown "новый владелец" "имя файла"

если же вы хотите поменять не только владелец, но и группу, то

chown "новый владелец":"новая группа" "имя файла"

Кстати, никто не мешает указать в команде "старого" владельца, тогда изменится только группа.

Ну и, конечно, если вы хотите заменить владельца (группу) сразу на нескольких файлах, вместо имени файла можно указать подходящий "шаблон", например "\*" (выполнить операцию для всех файлов в текущей директории).

Если же вы хотите, чтобы аналогичная операция была проделана не только в текущей директории, но и во всех "нижележащих" поддиректориях, вам поможет ключ -R (recursively).

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

Find “папка” –user “имя пользователя”

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? Приведите пример.

Chmod –R u=rwx g=rwx /data

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

Chmod +x file

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

Команда getfacl

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? Приведите пример.

Нужно отобрать права на запись для всех кроме владельца

Chmog u+w g-w o-w file

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

Setfacl

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? Приведите пример.

Установить на каталог права через setfacl g:groupname:r

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

Значение 0277 – режим только чтение

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

Установка sticky-бита

# Заключение

Получены навыки настройки групп пользователей