Отчёт по лабораторной работе 4

Дискреционное разграничение прав в Linux. Расширенные атрибуты

Гебриал Ибрам Есам Зекри НПИ-01-18

Содержание

# Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

# Теоретические сведения

В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов.

Один из подходов к разграничению доступа — так называемый дискреционный (от англ, discretion — чье-либо усмотрение) — предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют.

Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ в (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей. [1]

Предположим вы хотите защитить некоторые важные файлы в Linux. При чем они должны быть защищены не только от перезаписи но и от случайного или преднамеренного удаления и перемещения. Предотвратить перезапись или изменение битов доступа к файлов можно с помощью стандартных утилит chmod и chown, но это не идеальное решение, так как у суперпользователя по прежнему остается полный доступ. Но есть еще одно решение. Это команда chattr.

Утилиты chattr и lsattr входят в пакет e2fsprogs и предустановлены во всех современных дистрибутивах. Базовый синтаксис chattr выглядит следующим образом:

chattr опции [оператор][атрибуты] файлы

Вот основные опции утилиты, которые вы можете использовать:

-R - рекурсивная обработка каталога;

-V - максимально подробный вывод;

-f - игнорировать сообщения об ошибках;

-v - вывести версию.

Оператор может принимать значения:

* + включить выбранные атрибуты;
  + отключить выбранные атрибуты;

= - оставить значение атрибута таким, каким оно было у файла.

Вот некоторые доступные атрибуты:

a - файл может быть открыт только в режиме добавления;

A - не обновлять время перезаписи;

c - автоматически сжимать при записи на диск;

C - отключить копирование при записи;

D - работает только для папки, когда установлен, все изменения синхронно записываются на диск сразу же;

e - использовать extent’ы блоков для хранения файла;

i - сделать неизменяемым;

j - все данные перед записью в файл будут записаны в журнал;

s - безопасное удаление с последующей перезаписью нулями;

S - синхронное обновление, изменения файлов с этим атрибутом будут сразу же записаны на диск;

t - файлы с этим атрибутом не будут хранится в отдельных блоках;

u - содержимое файлов с этим атрибутом не будет удалено при удалении самого файла и потом может быть восстановлено. [2]

# Выполнение лабораторной работы

1. От имени пользователя guest определил расширенные атрибуты файла /home/guest/dir1/file1 (рис. 1)

С помощью команды:

lsattr /home/guest/dir1/file1

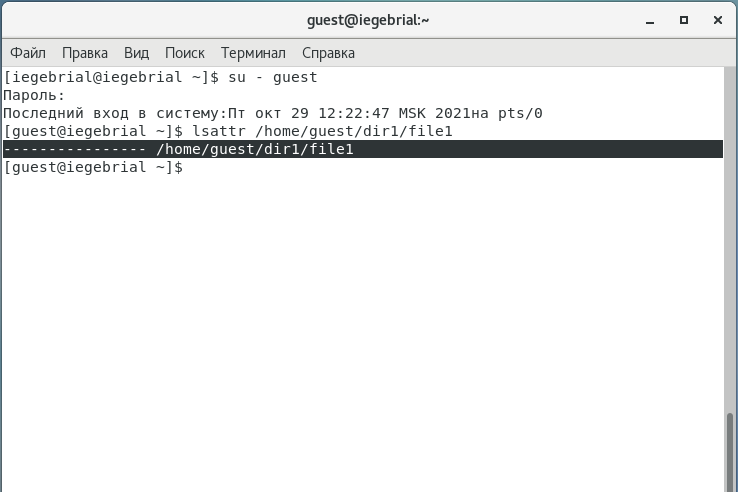


Figure 1: Определение расширенных атрибутов файла /home/guest/dir1/file1

1. Установил командой chmod на файл file1 права, разрешающие чтение и запись для владельца фай- ла. (рис. 2)

С помощью команды:

chmod 600 file1

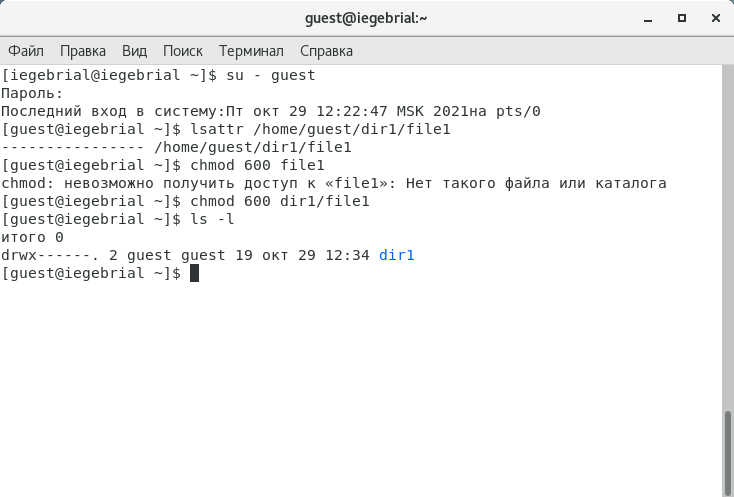


Figure 2: Установление командой chmod

1. Попробовал установить на файл /home/guest/dir1/file1 расширенный атрибут a от имени пользователя guest (рис. 3):

С помощью команды:

chattr +a /home/guest/dir1/file1

В ответ получил отказ от выполнения операции.



Figure 3: Попытка установления расширенный атрибут a

1. Повысил свои права с помощью команды su. установил расширенный атрибут a на файл /home/guest/dir1/file1 от имени суперпользователя:(рис. 4)

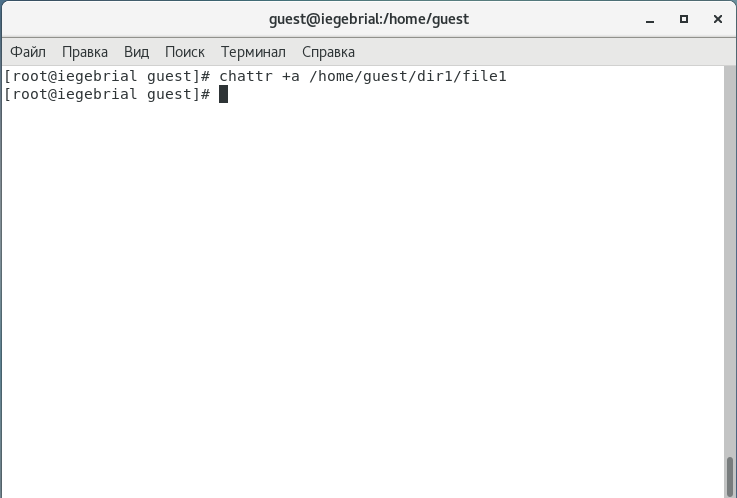


Figure 4: Установление расширенного атрибута a

5.От пользователя guest проверил правильность установления атрибута: (рис. 5)



Figure 5: Проверка правительности установления атрибута

1. Выполнил дозапись в файл file1 слова «test» командой echo “test” /home/guest/dir1/file1 После этого выполнил чтение файла file1 командой cat /home/guest/dir1/file1 (рис. 6)



Figure 6: Дозапись в файл file1 слова «test»

1. Попробовал удалить файл file1 либо стереть имеющуюся в нём информацию командой echo “abcd” > /home/guest/dirl/file1 Попробовал переименовать файл. (рис. 7)

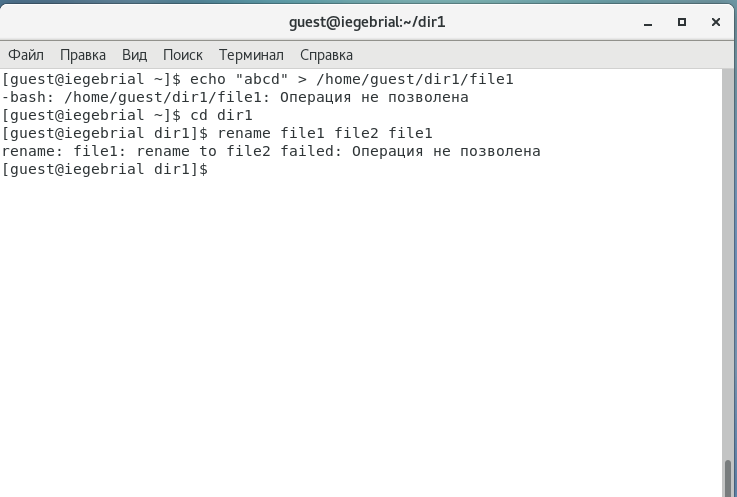


Figure 7: Проверка стерения имеющуюся в file1 и переменования файла

1. Попробовал с помощью команды chmod 000 file1 установить на файл file1 права, например, запрещающие чтение и запись для владельца файла. (рис. 8)

Не удалось установить.

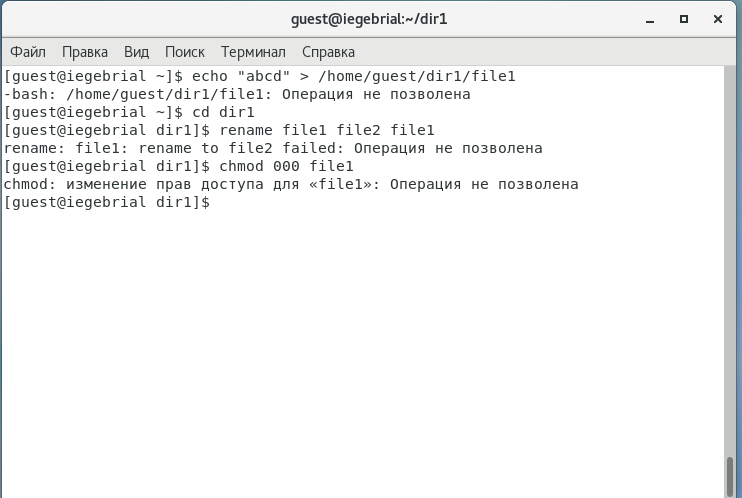


Figure 8: Установление прав 000 на file1

1. Снимил расширенный атрибут a с файла /home/guest/dirl/file1 от имени суперпользователя командой chattr -a /home/guest/dir1/file1: (рис. 9)

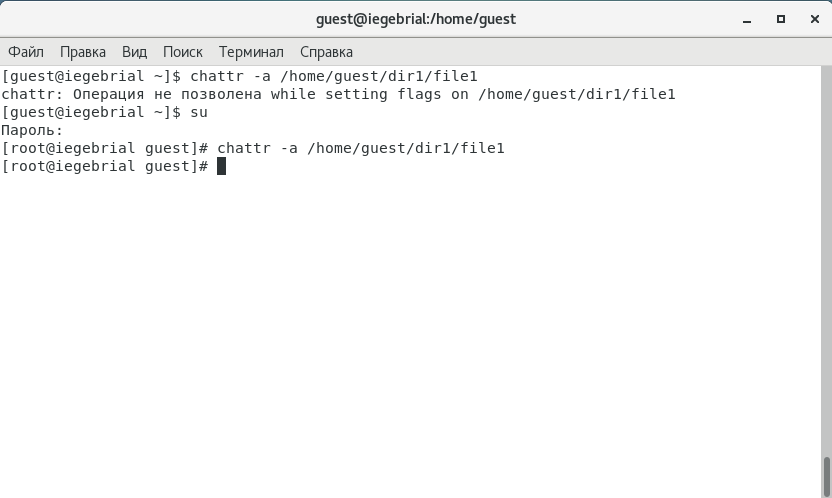


Figure 9: Изменение прав /home/guest/dirl/file1

1. Повторил операции, которые мнеранее не удавалось выполнить. (рис. 10)

Получилось у нас произвести все изменение.



Figure 10: Проверка установленных прав

1. Повторил все действия по шагам, заменив атрибут «a» атрибутом «i». (рис. 11)

ни одного действие не получилось делать.

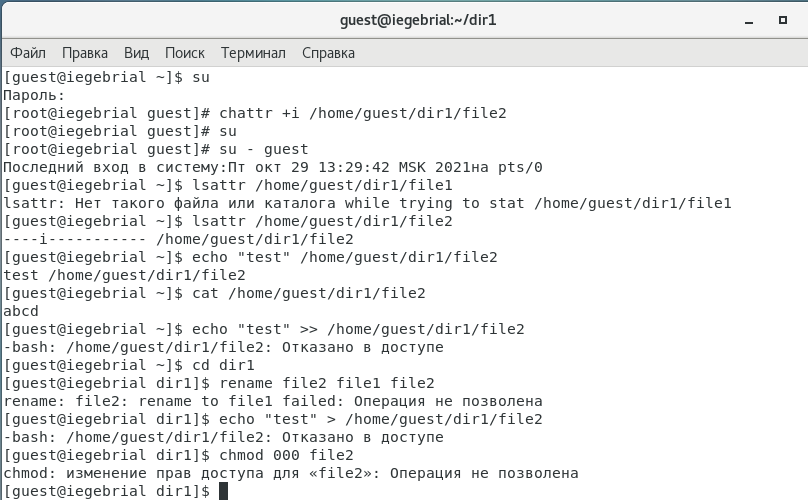


Figure 11: Установление атрибута i

1. Снимал атрибут «i» и повторил действии. (рис. 12)

Получилось делать все действии.

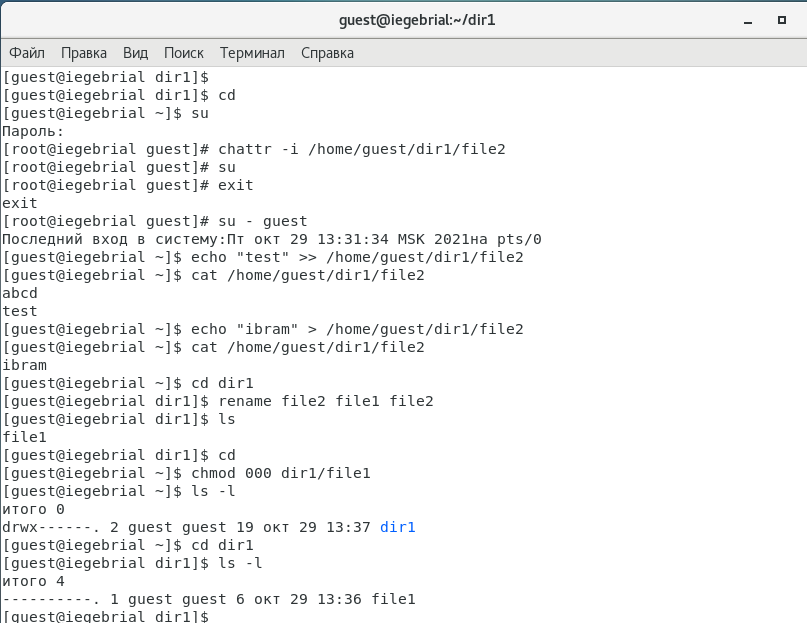


Figure 12: Снимание атрибута i и тестирование

# Выводы

Получил практические навыки работы в консоли с расширенными атрибутами файлов.

# Список литературы

1. Дискреционное разграничение доступа Linux. // Алексеев.Д. URL:https://debianinstall.ru

/diskretsionnoe-razgranichenie-dostupa-linux/ (дата обращения 27.11.2018).

1. Команда CHATTR в LINUX. //Losst.2020. URL:https://losst.ru/neizmenyaemye-fajly-v-linux (дата обращения 4.05.2020).