Отчёт по лабораторной работе №4. Дискреционное разграничение прав в Linux. Расширенные атрибуты.

Предмет: информационная безопасность

Александр Сергеевич Баклашов

Содержание

[1 Цель работы 1](#_Toc115012122)

[2 Теоретическое введение 1](#_Toc115012123)

[3 Выполнение лабораторной работы 1](#_Toc115012124)

[4 Вывод 4](#_Toc115012125)

[5 Библиография 4](#_Toc115012126)

# 1 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов. [1]

# 2 Теоретическое введение

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

chmod (от англ. change mode) — команда для изменения прав доступа к файлам и каталогам, используемая в Unix-подобных операционных системах. Входит в стандарт POSIX, в Coreutils. [3]

# 3 Выполнение лабораторной работы

1. От имени пользователя guest определим расширенные атрибуты файла /home/guest/dir1/file1 командой. Установим командой chmod 600 file1 на файл file1 права, разрешающие чтение и запись для владельца файла. (рис. [1](#fig:001))

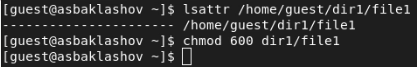


Figure 1: Атрибуты и права

1. Попробуем установить на файл /home/guest/dir1/file1 расширенный атрибут a от имени пользователя guest: chattr +a /home/guest/dir1/file1 (рис. [2](#fig:002))

Figure 2: Расш. атр.

Figure 2: Расш. атр.

В ответ получили отказ от выполнения операции.

1. Зайдём на третью консоль с правами администратора либо повысим свои права с помощью команды su. Попробуем установить расширенный атрибут a на файл /home/guest/dir1/file1 от имени суперпользователя: chattr +a /home/guest/dir1/file1 (рис. [3](#fig:003))

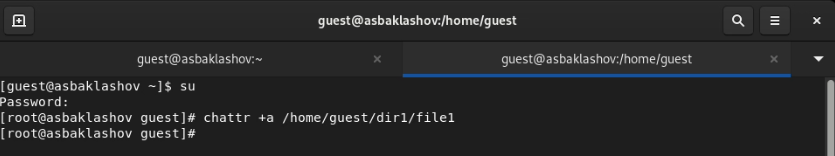


Figure 3: su +a

1. От пользователя guest проверим правильность установления атрибута: lsattr /home/guest/dir1/file1.

Выполним дозапись в файл file1 слова «test» командой echo “test” >> /home/guest/dir1/file1

После этого выполним чтение файла file1 командой cat /home/guest/dir1/file1

Убедимся, что слово test было успешно записано в file1.

Попробуем удалить файл file1 либо стереть имеющуюся в нём информацию командой echo “abcd” > /home/guest/dirl/file1

Попробуем переименовать файл.

Попробуем с помощью команды chmod 000 file1 установить на файл file1 права, например, запрещающие чтение и запись для владельца файла. (рис. [4](#fig:004))

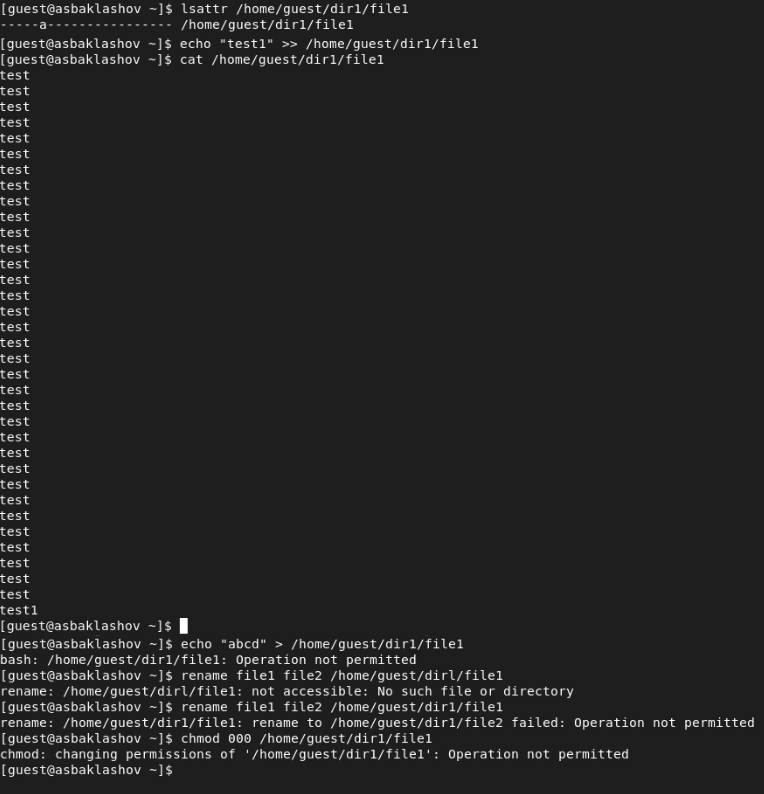


Figure 4: Выполнение команд с +a

1. Снимем расширенный атрибут a с файла /home/guest/dirl/file1 от имени суперпользователя командой chattr -a /home/guest/dir1/file1 Повторим операции, которые ранее не удавалось выполнить. Наблюдения занесём в отчёт. (рис. [5](#fig:005), рис. [6](#fig:006))

Figure 5: Снятем атрибута a

Figure 5: Снятем атрибута a

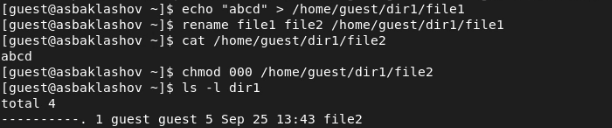


Figure 6: Команды без атр. a

1. Повторим действия по шагам, заменив атрибут «a» атрибутом «i». Удалось ли дозаписать информацию в файл? Наблюдения занесём в отчёт. (рис. [7](#fig:007), рис. [8](#fig:008))

Figure 7: +i

Figure 7: +i

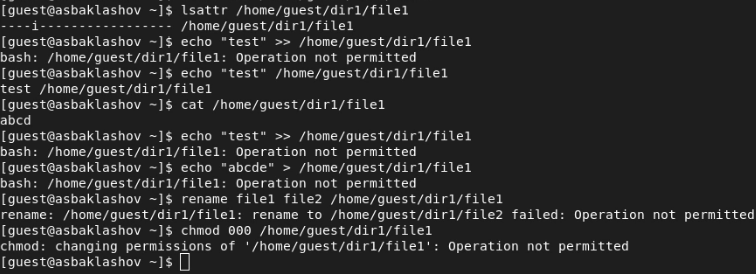


Figure 8: Выполнение команд с +i

При применении расширенного атрибута “i” ни одного из действий, представленных в лабораторной работе, совершить не удалось.

# 4 Вывод

В результате выполнения работы я повысил свои навыки использования интерфейса командой строки (CLI), познакомился на примерах с тем, как используются основные и расширенные атрибуты при разграничении доступа. Имел возможность связать теорию дискреционного разделения доступа (дискреционная политика безопасности) с её реализацией на практике в ОС Linux. Опробовал действие на практике расширенных атрибутов «а» и «i».

# 5 Библиография

1. Лабораторная работа №4. Дискреционное разграничение прав в Linux. Расширенные атрибуты. - 4 с. [Электронный ресурс]. М. URL: [Лабораторная работа №4](https://esystem.rudn.ru/pluginfile.php/1651887/mod_resource/content/3/004-lab_discret_extattr.pdf) (Дата обращения: 25.09.2022).
2. Rocky Linux Documentation. [Электронный ресурс]. М. URL: [Rocky Linux Documentation](https://docs.rockylinux.org) (Дата обращения: 25.09.2022).
3. Chmod. [Электронный ресурс]. М. URL: [Chmod](https://ru.wikipedia.org/wiki/Chmod) (Дата обращения: 25.09.2022).