Лабораторная работа №4

Дискреционное разграничение прав в Linux. Расширенные атрибуты

Щербак Маргарита Романовна, НПИбд-02-21

2024

Содержание

# Цель работы

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

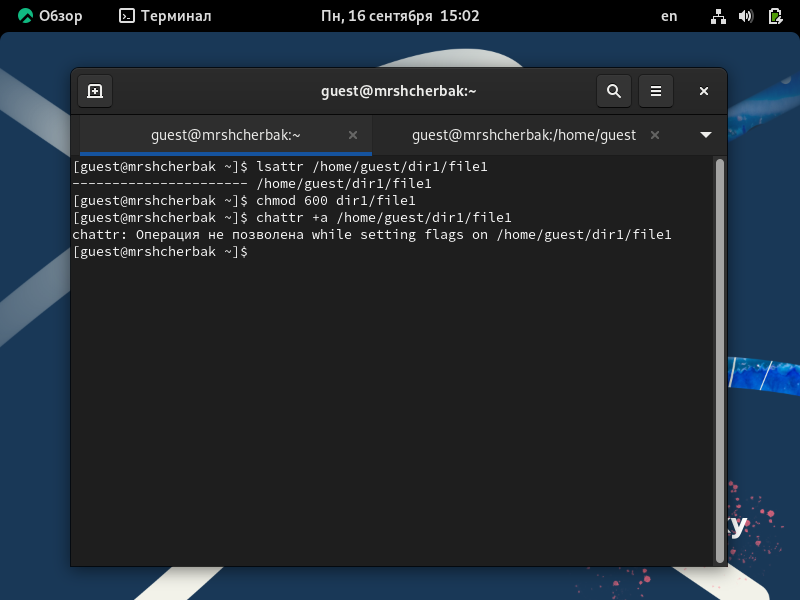
# Теоретическое введение

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.

Права доступа в системах управляют тем, какие операции может выполнять пользователь с определенными файлами и папками. Правильная настройка прав доступа помогает создать безопасную среду, где никто не сможет изменять ваши данные или нарушать работу важных системных файлов. Помимо групп root и users, в системе существует множество других, которые созданы для управления доступом программ к общим ресурсам. Участники каждой группы получают права на чтение или изменение конкретных файлов и каталогов, что регулирует их доступ и действия. Эти же права передаются процессам, которые запускает пользователь [2].

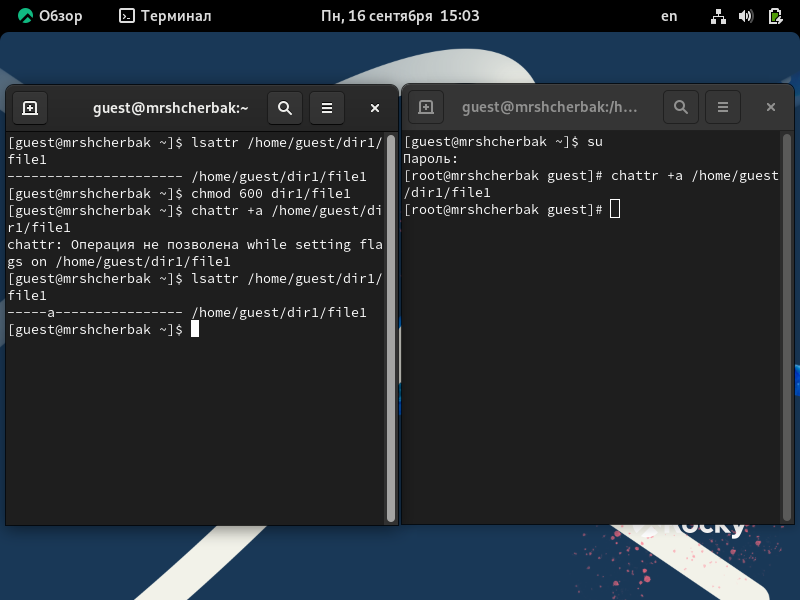
# Выполнение лабораторной работы

1. От имени пользователя guest определим расширенные атрибуты файла /home/guest/dir1/file1 командой lsattr /home/guest/dir1/file1.Установим командой chmod 600 file1 на файл file1 права, разрешающие чтение и запись для владельца файла. Попробуем установить на файл /home/guest/dir1/file1 расширенный атрибут a от имени пользователя guest: chattr +a /home/guest/dir1/file1 (рис.1). В ответ получили отказ.



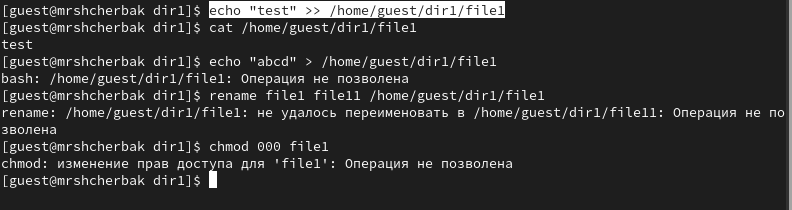
Выполнение команд

1. Зайдём на консоль с правами администратора. Попробуем установить расширенный атрибут a на файл /home/guest/dir1/file1 от имени суперпользователя: chattr +a /home/guest/dir1/file1. От пользователя guest проверим правильность установления атрибута: lsattr /home/guest/dir1/file1 (рис.2).



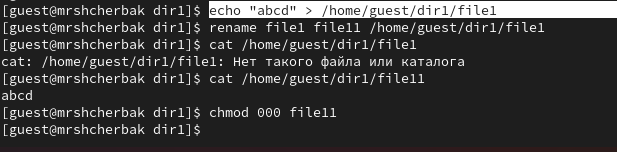
Выполнение команд

1. 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.3).



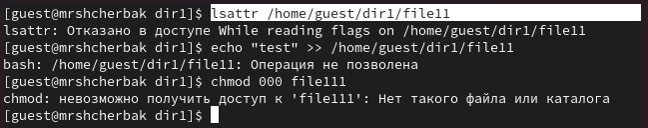
Выполнение команд с +a

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 (рис.4).



Выполнение команд с -a

1. Повторим действия по шагам, заменив атрибут «a» атрибутом «i» (рис.5).



Выполнение команд с +i

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

# Вывод

Таким образом, в ходе ЛР№4 я получила практические навыки работы в консоли с расширенными атрибутами файлов.

# Библиография

1. Методические материалы курса.
2. Chmod. [Электронный ресурс]. М. URL: [Файловая система](https://ru.wikipedia.org/wiki/Chmod) (Дата обращения: 16.09.2024).