

# **Лабораторная работа №4**

**Дискреционное разграничение прав в Linux. Расширенные атрибуты**

Щербак Маргарита Романовна, НПИБд-02-21

2024

# Содержание

<b>Цель работы</b>	<b>4</b>
<b>Теоретическое введение</b>	<b>5</b>
<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>Вывод</b>	<b>9</b>
<b>Библиография</b>	<b>10</b>

## Список иллюстраций

1	Выполнение команд . . . . .	6
2	Выполнение команд . . . . .	7
3	Выполнение команд с +a . . . . .	8
4	Выполнение команд с -a . . . . .	8
5	Выполнение команд с +i . . . . .	8

## **Цель работы**

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

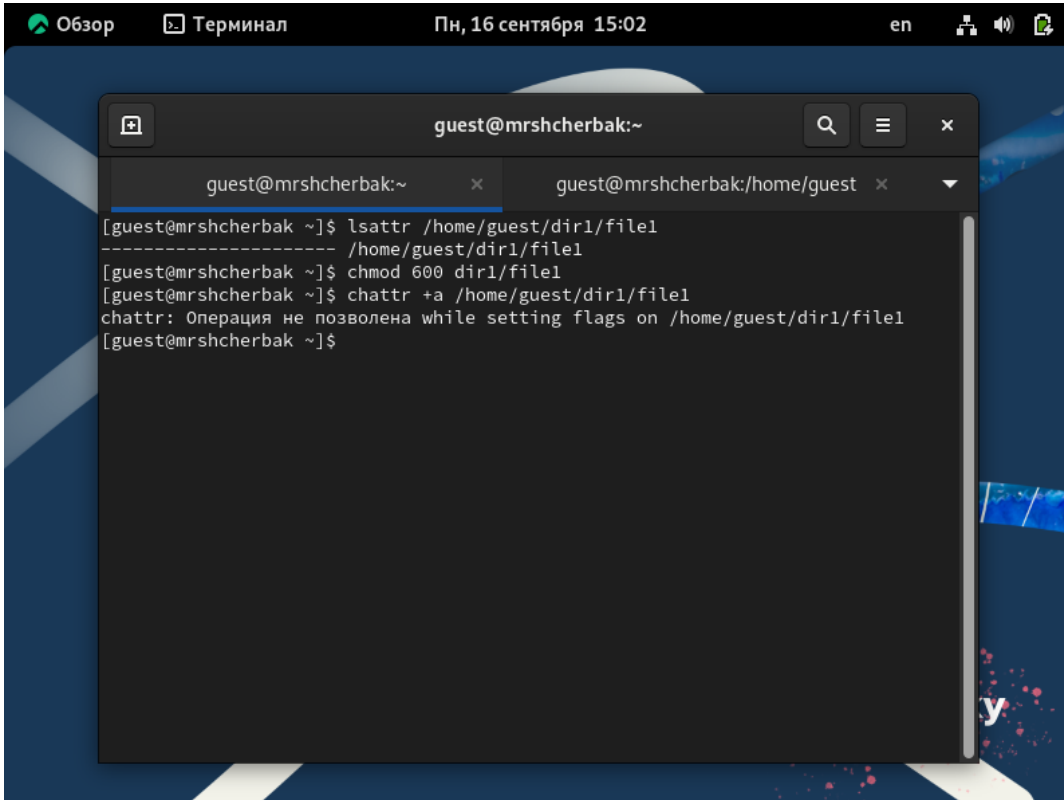
# Теоретическое введение

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.

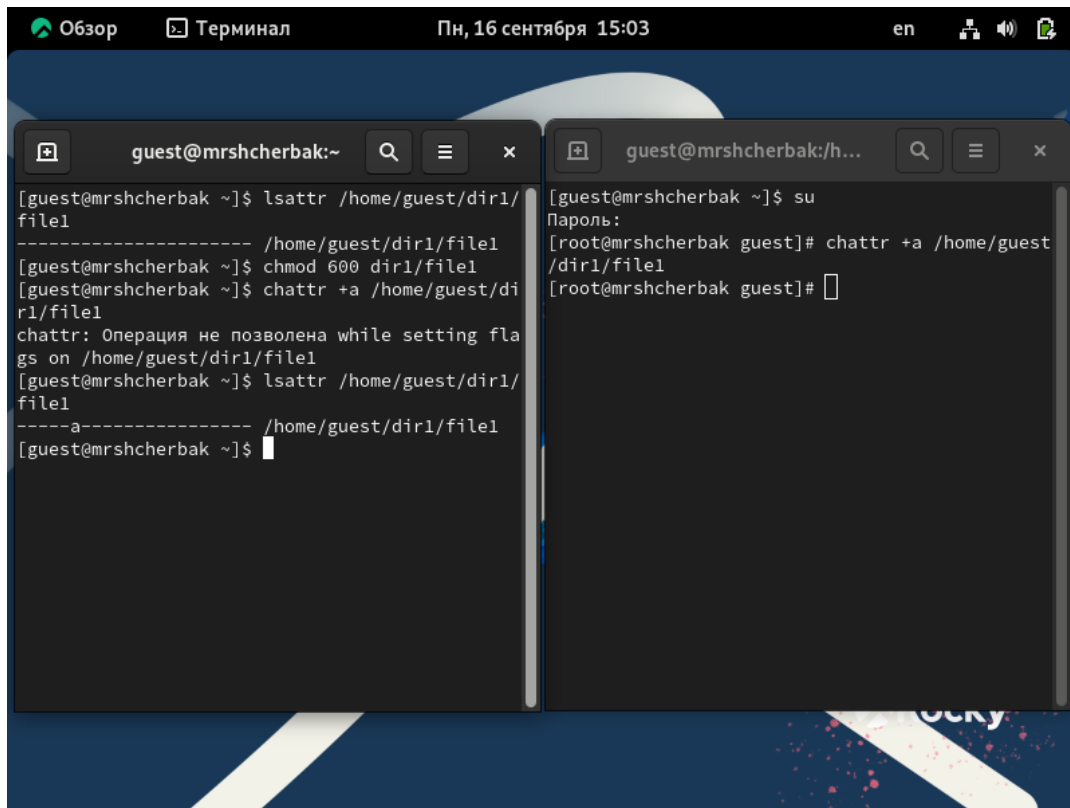


The screenshot shows a terminal window titled "guest@mrshcherbak:~". The terminal has two tabs: "guest@mrshcherbak:~" and "guest@mrshcherbak:/home/guest". The commands and their outputs are as follows:

```
[guest@mrshcherbak ~]$ lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[guest@mrshcherbak ~]$ chmod 600 dir1/file1
[guest@mrshcherbak ~]$ chattr +a /home/guest/dir1/file1
chattr: Операция не позволена while setting flags on /home/guest/dir1/file1
[guest@mrshcherbak ~]$
```

Рис. 1: Выполнение команд

2. 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).



```
guest@mrshcherbak:~$ lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[guest@mrshcherbak ~]$ chmod 600 dir1/file1
[guest@mrshcherbak ~]$ chattr +a /home/guest/dir1/file1
chattr: Операция не позволена while setting flags on /home/guest/dir1/file1
[guest@mrshcherbak ~]$ lsattr /home/guest/dir1/file1
-----a----- /home/guest/dir1/file1
[guest@mrshcherbak ~]$

[guest@mrshcherbak ~]$ su
Пароль:
[root@mrshcherbak guest]# chattr +a /home/guest/dir1/file1
[root@mrshcherbak guest]#
```

Рис. 2: Выполнение команд

3. 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/dir1/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).

```
[guest@mrshcherbak dir1]$ echo "test" >> /home/guest/dir1/file1
[guest@mrshcherbak dir1]$ cat /home/guest/dir1/file1
test
[guest@mrshcherbak dir1]$ echo "abcd" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Операция не позволена
[guest@mrshcherbak dir1]$ rename file1 file11 /home/guest/dir1/file1
rename: /home/guest/dir1/file1: не удалось переименовать в /home/guest/dir1/file11: Операция не по
зволена
[guest@mrshcherbak dir1]$ chmod 000 file1
chmod: изменение прав доступа для 'file1': Операция не позволена
[guest@mrshcherbak dir1]$
```

Рис. 3: Выполнение команд с +a

4. Снимем расширенный атрибут a с файла /home/guest/dir1/file1 от имени суперпользователя командой `chattr -a /home/guest/dir1/file1` Повторим операции, которые ранее не удавалось выполнить (рис.4).

```
[guest@mrshcherbak dir1]$ echo "abcd" > /home/guest/dir1/file1
[guest@mrshcherbak dir1]$ rename file1 file11 /home/guest/dir1/file1
[guest@mrshcherbak dir1]$ cat /home/guest/dir1/file1
cat: /home/guest/dir1/file1: Нет такого файла или каталога
[guest@mrshcherbak dir1]$ cat /home/guest/dir1/file11
abcd
[guest@mrshcherbak dir1]$ chmod 000 file11
[guest@mrshcherbak dir1]$
```

Рис. 4: Выполнение команд с -a

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

```
[guest@mrshcherbak dir1]$ lsattr /home/guest/dir1/file11
lsattr: Отказано в доступе While reading flags on /home/guest/dir1/file11
[guest@mrshcherbak dir1]$ echo "test" >> /home/guest/dir1/file11
bash: /home/guest/dir1/file11: Операция не позволена
[guest@mrshcherbak dir1]$ chmod 000 file111
chmod: невозможно получить доступ к 'file111': Нет такого файла или каталога
[guest@mrshcherbak dir1]$
```

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 (Дата обращения: 16.09.2024).