

# **Основы информационной безопасности**

**Лабораторная работа № 4. Дискреционное разграничение прав в Linux.  
Расширенные атрибуты**

Сунгурова Мариян

# Содержание

|   |                                |   |
|---|--------------------------------|---|
| 1 | Цель работы                    | 4 |
| 2 | Теоретические сведения         | 5 |
| 3 | Выполнение лабораторной работы | 6 |
| 4 | Выводы                         | 8 |
|   | Список литературы              | 9 |

## Список иллюстраций

|     |   |   |
|-----|---|---|
| 3.1 | Просмотр и попытка изменения расширенных атрибутов файла от имени guest . . . . . | 6 |
| 3.2 | Изменение расширенных атрибутов файла от имени суперпользователя . . . . .        | 6 |
| 3.3 | Проверка прав с расширенным атрибутом i . . . . .                                 | 7 |
| 3.4 | Проверка прав с расширенным атрибутом i . . . . .                                 | 7 |

# 1 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

## 2 Теоретические сведения

При работе с командой `chmod` важно понимать основные права доступа, которые назначают файлам или каталогам. В Linux используется три основных типа прав доступа[1]:

- Чтение (Read) — обозначается буквой «r». Предоставляет возможность просматривать содержимое файла или каталога.
- Запись (Write) — обозначается буквой «w». Позволяет создавать, изменять и удалять файлы внутри каталога, а также изменять содержимое файла.
- Выполнение (Execute) — обозначается буквой «x». Дает разрешение на выполнение файла или на вход в каталог.

Каждый из указанных выше типов прав доступа может быть назначен трем группам пользователей:

- Владелец (Owner) — пользователь, который является владельцем файла или каталога.
- Группа (Group) — группа пользователей, к которой принадлежит файл или каталог.
- Остальные пользователи (Others) — все остальные пользователи системы.

Комбинация этих базовых прав доступа для каждой из групп пользователей определяет полный набор прав доступа для файла или каталога.

### 3 Выполнение лабораторной работы

От имени пользователя `guest` определим расширенные атрибуты файла `/home/guest/dir1/file1`, в данный момент их нет. 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`. В отчет получим отказ(рис. fig. 3.1)

```
[guest@mmsungurova ~]$ lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[guest@mmsungurova ~]$ chmod 600 file1
chmod: невозможно получить доступ к 'file1': Нет такого файла или каталога
[guest@mmsungurova ~]$ cd /home/guest/dir1/file1
bash: cd: /home/guest/dir1/file1: Это не каталог
[guest@mmsungurova ~]$ cd /home/guest/dir1
[guest@mmsungurova dir1]$ chmod 600 file1
[guest@mmsungurova dir1]$ chatter +a /home/guest/dir1/file1
chattr: Операция не позволена while setting flags on /home/guest/dir1/file1
```

Рис. 3.1: Просмотр и попытка изменения расширенных атрибутов файла от имени `guest`

Зайдем на третью консоль с правами администратора и попробуем установить расширенный атрибут `a` на файл `/home/guest/dir1/file1` от имени суперпользователя(рис. fig. 3.2)

```
[root@mmsungurova dir1]# chatter +a /home/guest/dir1/file1
[root@mmsungurova dir1]# su guest
[guest@mmsungurova dir1]$ lsattr /home/guest/dir1/file1
-----a----- /home/guest/dir1/file1
```

Рис. 3.2: Изменение расширенных атрибутов файла от имени суперпользователя

От пользователя `guest` проверим правильность установления атрибута. Затем выполним дозапись в файл `file1` слова «test» командой, после этого выполним чтение файла `file1` командой и убедимся, что слово `test` было успешно записано

в file1. Попробуем удалить файл file1, стереть имеющуюся в нём информацию командой, переименовать файл и изменить его атрибуты – ничего из этого сделать

```
[guest@mmsungurova dir1]$ echo "abcd" > file1
bash: file1: Операция не позволена
[guest@mmsungurova dir1]$ echo "abcd" > file1
```

не удастся(рис. fig. ??)

```
[guest@mmsungurova dir1]$ echo "test" >> file1
[guest@mmsungurova dir1]$ cat file1
TEST
test
[guest@mmsungurova dir1]$
```

Уберем из суперпользователя атрибут a и повторим все действия, которые ранее не удалось совершить(рис. fig. ??).

Проверка прав без расширенных атрибутов

Теперь мы имеем права на все эти действия

```
[guest@mmsungurova dir1]$ chmod 000 file1
chmod: изменение прав доступа для 'file1': Операция не позволена
[guest@mmsungurova dir1]$
```

Рис. 3.3: Проверка прав с расширенным атрибутом i

Попробуем повторить всё ещё раз, установив атрибут i(рис. fig. 3.4).

```
[guest@mmsungurova dir1]$ su
Пароль:
[root@mmsungurova dir1]# chattr -a /home/guest/dir1/file1
[root@mmsungurova dir1]# su guest
[guest@mmsungurova dir1]$ lsattr file1
----- file1
[guest@mmsungurova dir1]$
```

Рис. 3.4: Проверка прав с расширенным атрибутом i

Теперь над недоступна в том числе и дозапись в файл, то есть запрещены любые действия с этим файлом.

## 4 Выводы

В результате выполнения работы были приобретены практические навыки работы в консоли с расширенными атрибутами файлов.



# Список литературы

1. Граннеман С. Скотт Граннеман: Linux. Карманный справочник. 2-е изд. Вильямс, 2019. 464 с.