

# **Лабораторная работа № 4**

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

Абу Сувейлим Мухаммед Мунифович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
<b>5</b>	<b>Выводы</b>	<b>12</b>
	<b>Список литературы</b>	<b>13</b>

## Список иллюстраций

4.1	Команда lsattr . . . . .	8
4.2	Команда chmod . . . . .	8
4.3	Команда chattr +a . . . . .	9
4.4	Команда chattr +a через root . . . . .	9
4.5	Команда lsattr f1 на guest . . . . .	9
4.6	Команда echo > f1 на guest . . . . .	9
4.7	Команда cat f1 на guest . . . . .	9
4.8	Команда mv f1 f11 . . . . .	10
4.9	Команда chattr -a . . . . .	10
4.10	Команда echo . . . . .	10
4.11	Команда mv . . . . .	10
4.12	Команда chattr +i . . . . .	10
4.13	Команды echo и mv . . . . .	11

## **Список таблиц**

# 1 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

## 2 Задание

Использовать интерфейс командой строки (CLI) при выполнении лабораторной работы

### 3 Теоретическое введение

В метаданных каждого объекта (в inode файла/директории) содержится список разрешений на доступ к нему для разных категорий субъектов [1].

Атрибуты Minimal ACL поддерживают три базовых класса субъектов доступа к файлу (класс All объединяет все три класса):

User access (u) – доступ для владельца файла; Group access (g) – доступ для группы, владеющей файлом; Other access (o) – доступ для остальных пользователей (кроме пользователя root). All access (a) – доступ для всех субъектов доступа (u, g, o). Для каждого из этих классов определены три типа разрешений:

На чтение содержимого файла (read) – символ «r». На запись внутри файла или изменения его содержимого (write) – символ «w». На исполнение файла (если это бинарный исполняемый файл или файл сценария интерпретатора (execute)) – символ «x» [2].

## 4 Выполнение лабораторной работы

От имени пользователя guest хотели определить расширенные атрибуты файла /home/guest/dir1/f1 командой (рис. 4.1):

```
[guest@smabu ~]$ lsattr /home/guest/dir1/f1
lsattr: Отказано в доступе while trying to stat /home/guest/dir1/f1
```

Рис. 4.1: Команда lsattr

но получили отказ.

Установили командой chmod 600 f1 на файл f1 права, разрешающие чтение и запись для владельца файла (рис. 4.2):

```
[guest@smabu ~]$ chmod 600 /home/guest/dir1/f1
chmod: невозможно получить доступ к '/home/guest/dir1/f1': Отказано в доступе
[guest@smabu ~]$ chmod 777 dir1
[guest@smabu ~]$ ls -l
итого 0
drwxrwxrwx. 2 guest guest 16 сен 21 15:54 dir1
drwxr-xr-x. 2 guest guest  6 сен 13 23:22 Видео
drwxr-xr-x. 2 guest guest  6 сен 13 23:22 Документы
drwxr-xr-x. 2 guest guest  6 сен 13 23:22 Загрузки
drwxr-xr-x. 2 guest guest  6 сен 13 23:22 Изображения
drwxr-xr-x. 2 guest guest  6 сен 13 23:22 Музыка
drwxr-xr-x. 2 guest guest  6 сен 13 23:22 Общедоступные
drwxr-xr-x. 2 guest guest  6 сен 13 23:22 'Рабочий стол'
drwxr-xr-x. 2 guest guest  6 сен 13 23:22 Шаблоны
[guest@smabu ~]$ ls -l dir1
итого 4
----rwx---. 1 guest guest 7 сен 21 15:53 f1
[guest@smabu ~]$ chmod 600 /home/guest/dir1/f1
[guest@smabu ~]$ ls -l dir1
итого 4
-rw-----. 1 guest guest 7 сен 21 15:53 f1
[guest@smabu ~]$
```

Рис. 4.2: Команда chmod

Попробавли установить на файл /home/guest/dir1/f1 расширенный атрибут a от имени пользователя guest (рис. 4.3):

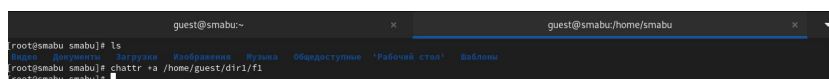


```
[guest@smabu ~]$ chmod +a /home/guest/dir1/f1
chmod: Операция не разрешена while setting flags on /home/guest/dir1/f1
[guest@smabu ~]$
```

Рис. 4.3: Команда `chmod +a`

В ответ мы получили отказ от выполнения операции.

Повысили свои права с помощью команды `su`. Попробовали установить расширенный атрибут `a` на файл `/home/guest/dir1/f1` от имени суперпользователя (рис. 4.4):



```
guest@smabu:~$ su
root@smabu:~# ls
root@smabu:~# chmod +a /home/guest/dir1/f1
root@smabu:~#
```

Рис. 4.4: Команда `chmod +a` через `root`

От пользователя `guest` проверим правильность установления атрибута (рис. 4.5):

```
[guest@smabu ~]$ lsattr /home/guest/dir1/f1
-----a----- /home/guest/dir1/f1
[guest@smabu ~]$
```

Рис. 4.5: Команда `lsattr f1` на `guest`

Выполним запись в файл `f1` слова «test» командой (рис. 4.6):

```
[guest@smabu ~]$ echo "test" > /home/guest/dir1/f1
bash: /home/guest/dir1/f1: Операция не разрешена
```

Рис. 4.6: Команда `echo > f1` на `guest`

После этого выполним чтение файла `file1` командой (рис. 4.7):

```
[guest@smabu ~]$ cat /home/guest/dir1/f1
test65
```

Рис. 4.7: Команда `cat f1` на `guest`

Переименовать файл `f1` невозможно (рис. 4.8):

```
[guest@smabu ~]$ mv /home/guest/dir1/f1 /home/guest/dir1/f11
mv: невозможно переместить '/home/guest/dir1/f1' в '/home/guest/dir1/f11': Операция не позволена
[guest@smabu ~]$
```

Рис. 4.8: Команда mv f1 f11

После снятия расширенный атрибут a с файла /home/guest/dir1/f1 от имени суппользователя командой (рис. 4.9):

```
[root@smabu smabu]# chatter -a /home/guest/dir1/f1
```

Рис. 4.9: Команда chatter -a

Все команды, которые мы не смогли выполнить выполнялись (рис. 4.10, 4.11):

```
[guest@smabu ~]$ echo "test" > /home/guest/dir1/f1
[guest@smabu ~]$ cat /home/guest/dir1/f1
test
[guest@smabu ~]$
```

Рис. 4.10: Команда echo

```
[guest@smabu ~]$ mv /home/guest/dir1/f1 /home/guest/dir1/f11
[guest@smabu ~]$ ls -l dir1
итого 4
-rw-----. 1 guest guest 5 сен 28 13:33 f11
[guest@smabu ~]$
```

Рис. 4.11: Команда mv

Повторим наши действия по шагам, заменив атрибут «a» атрибутом «i» (рис. 4.12):

```
[root@smabu smabu]# chatter +i /home/guest/dir1/f1
[root@smabu smabu]#
```

Рис. 4.12: Команда chatter +i

Получили отказ (рис. 4.13):

```
[guest@smabu ~]$ lsattr /home/guest/dir1/fl
-----i----- /home/guest/dir1/fl
[guest@smabu ~]$ echo "test2" > /home/guest/dir1/fl
bash: /home/guest/dir1/fl: Операция не позволена
[guest@smabu ~]$ cat /home/guest/dir1/fl
test
[guest@smabu ~]$ mv /home/guest/dir1/fl1 /home/guest/dir1/fl
mv: не удалось выполнить stat для '/home/guest/dir1/fl1': Нет такого файла или каталога
[guest@smabu ~]$ mv /home/guest/dir1/fl /home/guest/dir1/fl1
mv: невозможно переместить '/home/guest/dir1/fl' в '/home/guest/dir1/fl1': Операция не позволена
[guest@smabu ~]$
```

Рис. 4.13: Команды echo и mv

## 5 Выводы

В результате выполнения работы мы повысили свои навыки использования интерфейса командой строки(CLI), познакомились на примерах с тем, как используются основные и расширенные атрибуты при разграничении доступа. Имели возможность связать теорию дискреционного разделения доступа (дискреционная политика безопасности) с её реализацией на практике в ОС Linux. Составили наглядные таблицы, поясняющие какие операции возможны при тех или иных установленных правах. Опробовали действие на практике расширенных атрибутов «а» и «і».

## Список литературы

1. // skillbox.ru.
2. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.