

# **Отчёта по лабораторной работе № 4**

**Информационная безопасность**

Адебайо Ридвануллахи Айофе

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Теорическое введение</b>	<b>6</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
<b>4</b>	<b>Выводы</b>	<b>11</b>
<b>5</b>	<b>Список литературы</b>	<b>12</b>

## Список иллюстраций

3.1	Определение атрибутов . . . . .	8
3.2	Расширенные атрибуты . . . . .	8
3.3	Установка расширенного атрибута от имени суперпользователя .	9
3.4	Чтение . . . . .	9
3.5	Переименование . . . . .	9
3.6	Удаление . . . . .	10
3.7	Удаление . . . . .	10
3.8	Запись . . . . .	10

## **Список таблиц**

# 1 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

## 2 Теорическое введение

В операционной системе Linux есть много отличных функций безопасности, но одна из самых важных - это система прав доступа к файлам. Изначально каждый файл имел три параметра доступа. Вот они:

- Чтение - разрешает получать содержимое файла, но на запись нет. Для каталога позволяет получить список файлов и каталогов, расположенных в нем
- Запись - разрешает записывать новые данные в файл или изменять существующие, а также позволяет создавать и изменять файлы и каталоги
- Выполнение - невозможно выполнить программу, если у нее нет флага выполнения. Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система может понять, что этот файл нужно запускать как программу

Команды, которые могут понадобиться при работе с правами доступа:

- “ls -l” - для просмотра прав доступа к файлам и каталогам
- “chmod категория действие флаг файл или каталог” - для изменения прав доступа к файлам и каталогам (категорию действие и флаг можно заменить на набор из трех цифр от 0 до 7)

Значения флагов прав:

- -- нет никаких прав

- -x - разрешено только выполнение файла, как программы, но не изменение и не чтение
- -w- - разрешена только запись и изменение файла
- -wx - разрешено изменение и выполнение, но в случае с каталогом, невозможно посмотреть его содержимое
- r- - права только на чтение
- r-x - только чтение и выполнение, без права на запись
- rw- - права на чтение и запись, но без выполнения
- rwx - все права

### 3 Выполнение лабораторной работы

1. От имени пользователя guest определите расширенные атрибуты файла /home/guest/dir1/file1 командой `lsattr /home/guest/dir1/file1`

```
[guest@raadebayjo ~]$ lsattr /home/guest/dir1/file1
lsattr: No such file or directory while trying to stat /home/guest/dir1/file1
[guest@raadebayjo ~]$ touch /home/guest/dir1/file1
[guest@raadebayjo ~]$ lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[guest@raadebayjo ~]$
[guest@raadebayjo ~]$
```

Рис. 3.1: Определение атрибутов

2. Установите командой `chmod 600 file1` на файл `file1` права, разрешающие чтение и запись для владельца файла.
3. Попробуйте установить на файл /home/guest/dir1/file1 расширенный атрибут `a` от имени пользователя `guest`: `chattr +a /home/guest/dir1/file1`

```
[guest@raadebayjo ~]$ chmod 600 /home/guest/dir1/file1
[guest@raadebayjo ~]$ chattr +a /home/guest/dir1/file1
chattr: Operation not permitted while setting flags on /home/guest/dir1/file1
[guest@raadebayjo ~]$
```

Рис. 3.2: Расширенные атрибуты

4. Зайдите на третью консоль с правами администратора либо повысьте свои права с помощью команды `su`. Попробуйте установить расширенный атрибут `a` на файл /home/guest/dir1/file1 от имени суперпользователя: `chattr +a /home/guest/dir1/file1`



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

Рис. 3.3: Установка расширенного атрибута от имени суперпользователя

5. От пользователя guest проверьте правильность установления атрибута:  
lsattr /home/guest/dir1/file1 (см. 3.4)
6. Выполните дозапись в файл file1 слова «test» командой echo "test" /home/guest/dir1/file1 После этого выполните чтение файла file1 командой cat /home/guest/dir1/file1 Убедитесь, что слово test было успешно записано в file1.

```
[guest@raadebayjo ~]$ lsattr /home/guest/dir1/file1
-----a----- /home/guest/dir1/file1
[guest@raadebayjo ~]$ echo "test" /home/guest/dir1/file1
test /home/guest/dir1/file1
[guest@raadebayjo ~]$ cat /home/guest/dir1/file1
[guest@raadebayjo ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Operation not permitted
[guest@raadebayjo ~]$ echo "test" >/home/guest/dir1/file1
bash: /home/guest/dir1/file1: Operation not permitted
[guest@raadebayjo ~]$ echo "test" >> /home/guest/dir1/file1
[guest@raadebayjo ~]$ cat /home/guest/dir1/file1
test
[guest@raadebayjo ~]$
```

Рис. 3.4: Чтение

7. Попробуйте удалить файл file1 либо стереть имеющуюся в нём информацию командой echo "abcd" > /home/guest/dir1/file1 Попробуйте переименовать файл.

```
[guest@raadebayjo ~]$ echo "abcd" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Operation not permitted
[guest@raadebayjo ~]$ mv /home/guest/dir1/file1 file2
mv: cannot move '/home/guest/dir1/file1' to 'file2': Operation not permitted
[guest@raadebayjo ~]$
```

Рис. 3.5: Переименование

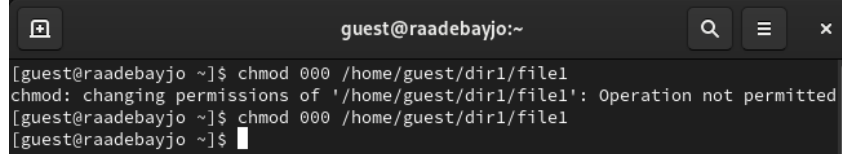
8. Попробуйте с помощью команды `chmod 000 file1` установить на файл `file1` права, например, запрещающие чтение и запись для владельца файла. Удалось ли вам успешно выполнить указанные команды?

```
[guest@raadebayjo ~]$ chmod 000 /home/guest/dir1/file1
chmod: changing permissions of '/home/guest/dir1/file1': Operation not permitted
[guest@raadebayjo ~]$
```

Рис. 3.6: Удаление

9. Снимите расширенный атрибут `a` с файла `/home/guest/dir1/file1` от имени суперпользователя командой `chattr -a /home/guest/dir1/file1`. Повторите операции, которые вам ранее не удавалось выполнить.

```
[root@raadebayjo guest]# chattr -a /home/guest/dir1/file1
[root@raadebayjo guest]#
```



```
[guest@raadebayjo ~]$ chmod 000 /home/guest/dir1/file1
chmod: changing permissions of '/home/guest/dir1/file1': Operation not permitted
[guest@raadebayjo ~]$ chmod 000 /home/guest/dir1/file1
[guest@raadebayjo ~]$
```

Рис. 3.7: Удаление

10. Повторите ваши действия по шагам, заменив атрибут «`a`» атрибутом «`i`». Удалось ли вам дозаписать информацию в файл? - Нет, не удалось

```
[guest@raadebayjo ~]$ chattr +I /home/guest/dir1/file1
Usage: chattr [-pRVf] [--aAcCdDeijPsStTuFh] [-v version] files...
[guest@raadebayjo ~]$ chattr +i /home/guest/dir1/file1
chattr: Permission denied while reading flags on /home/guest/dir1/file1
[guest@raadebayjo ~]$ lsattr /home/guest/dir1/file1
lsattr: Permission denied while reading flags on /home/guest/dir1/file1
[guest@raadebayjo ~]$ echo "test" >> /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Operation not permitted
[guest@raadebayjo ~]$ cat /home/guest/dir1/file1
cat: /home/guest/dir1/file1: Permission denied
[guest@raadebayjo ~]$
[guest@raadebayjo ~]$
[guest@raadebayjo ~]$
```

Рис. 3.8: Запись

## 4 Выводы

В результате выполнения работы вы 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».

## 5 Список литературы

1. Кулябов Д. С. \*Лабораторная работа №4\*\*: 004-lab\_discret\_extattr.pdf\*
2. Изменение атрибутов файлов в Linux [Электронный ресурс]. 2023.URL: <https://linux-notes.org/izmenenie-atributov-flagov-na-fajlah-v-unix-linux/> (дата обращения: 23.09.2023)