

# Отчёт по лабораторной работе №4

## Информационная безопасность

### Дискреционное разграничение прав в Linux. Расширенные атрибуты

Выполнил: Тараканов Борис Александрович,  
НПИбд-02-21, 1032212284

#### Содержание

1	Цель работы .....	1
2	Теоретическое введение.....	1
3	Выполнение лабораторной работы.....	2
4	Вывод .....	6
5	Список литературы. Библиография.....	6

## 1 Цель работы

Получить практические навыки работы в консоли с расширенными атрибутами файлов.

## 2 Теоретическое введение

**Права доступа** определяют, какие действия конкретный пользователь может или не может совершать с определенными файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы [1].

**Расширенные атрибуты файлов Linux** представляют собой пары имя: значение, которые постоянно связаны с файлами и каталогами, подобно тому как строки окружения связаны с процессом. Атрибут может быть определён или не определён. Если он определён, то его значение может быть или пустым, или не пустым [2].

Расширенные атрибуты дополняют обычные атрибуты, которые связаны со всеми inode в файловой системе (т. е., данные stat(2)). Часто они используются для предоставления дополнительных возможностей файловой системы, например, дополнительные возможности безопасности, такие как списки контроля доступа (ACL), могут быть реализованы через расширенные атрибуты [3].

*Установить атрибуты:*

- `chattr filename`

*Значения:*

- `chattr +a #` только добавление. Удаление и переименование запрещено;
- `chattr +A #` не фиксировать данные об обращении к файлу
- `chattr +c #` сжатый файл
- `chattr +d #` неархивируемый файл
- `chattr +i #` неизменяемый файл
- `chattr +S #` синхронное обновление
- `chattr +s #` безопасное удаление, (после удаления место на диске переписывается нулями)
- `chattr +u #` неудаляемый файл
- `chattr -R #` рекурсия

*Просмотреть атрибуты:*

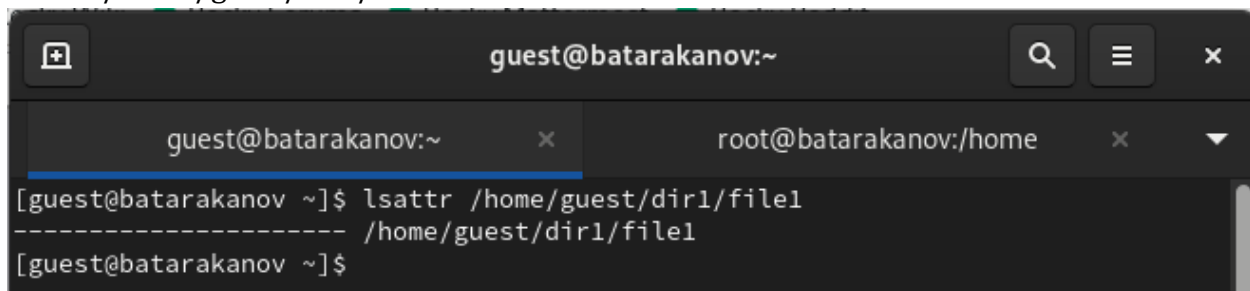
- `lsattr filename`

*Опции:*

- `lsattr -R #` рекурсия
- `lsattr -a #` вывести все файлы (включая скрытые)
- `lsattr -d #` не выводить содержимое директории

### 3 Выполнение лабораторной работы

1. От имени пользователя `guest` определим расширенные атрибуты файла `/home/guest/dir1/file1`



The screenshot shows a terminal window with two tabs. The active tab is titled `guest@batarakanov:~`. The command `lsattr /home/guest/dir1/file1` has been executed, and the output is `----- /home/guest/dir1/file1`. The prompt `[guest@batarakanov ~]$` is visible at the bottom.

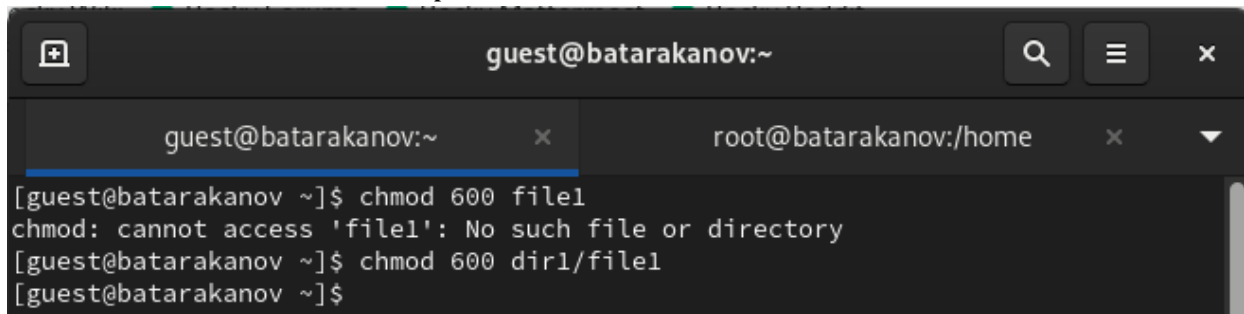
```

[guest@batarakanov ~]$ lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[guest@batarakanov ~]$

```

*Рис. 1: `lsattr /home/guest/dir1/file1`*

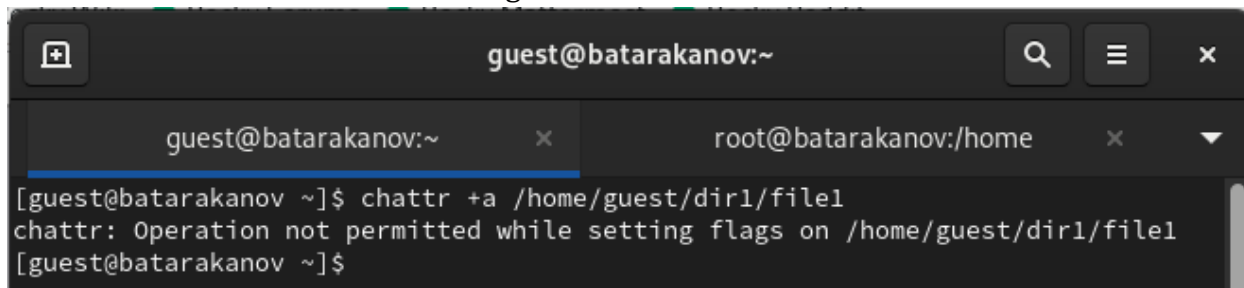
- Следующим шагом установим на файл file1 права, разрешающие чтение и запись для владельца файла



```
guest@batarakanov:~  
[guest@batarakanov ~]$ chmod 600 file1  
chmod: cannot access 'file1': No such file or directory  
[guest@batarakanov ~]$ chmod 600 dir1/file1  
[guest@batarakanov ~]$
```

Рис. 2: `chmod 600 /home/guest/dir1/file1`

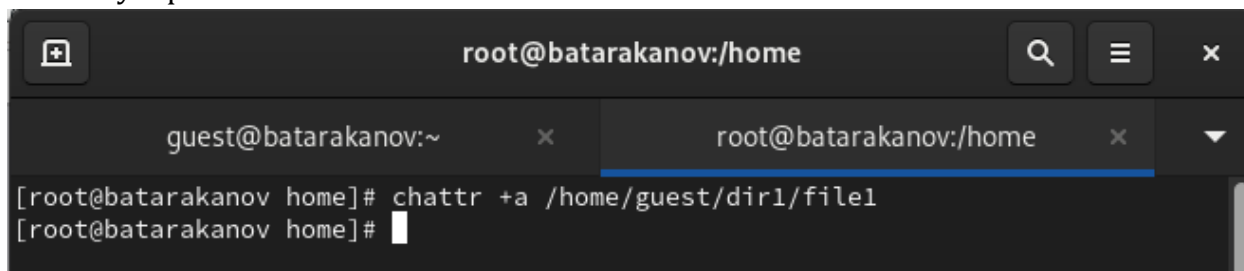
- Попробуем установить на файл /home/guest/dir1/file1 расширенный атрибут «a» от имени пользователя guest



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

Рис. 3: `chattr +a /home/guest/dir1/file1`

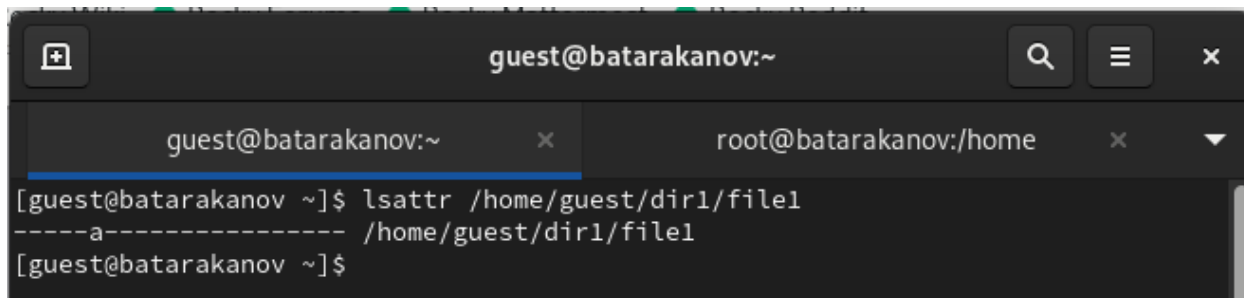
- Повысим свои права с помощью команды su и попробуем установить расширенный атрибут «a» на файл /home/guest/dir1/file1 от имени суперпользователя



```
root@batarakanov:/home  
[root@batarakanov home]# chattr +a /home/guest/dir1/file1  
[root@batarakanov home]#
```

Рис. 4: `chattr +a /home/guest/dir1/file1`

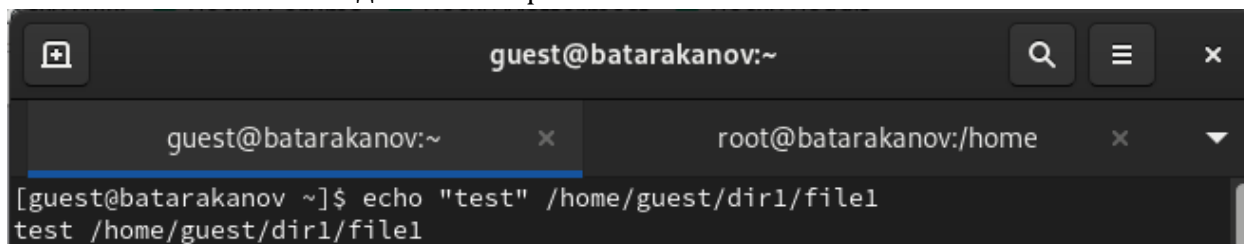
- От пользователя guest проверим правильность установления атрибута



```
guest@batarakanov:~  
[guest@batarakanov ~]$ lsattr /home/guest/dir1/file1  
-----a----- /home/guest/dir1/file1  
[guest@batarakanov ~]$
```

Рис. 5: `lsattr /home/guest/dir1/file1`

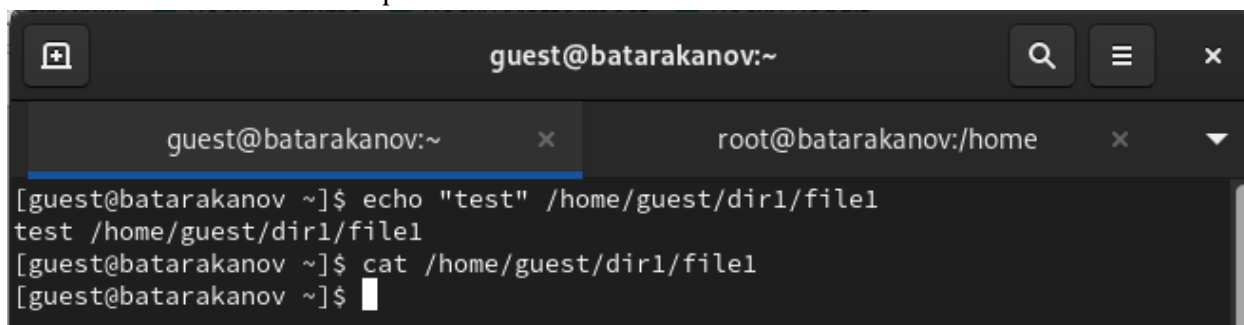
6. Затем выполним дозапись в файл `file1` слова «test»



```
guest@batarakanov:~  
[guest@batarakanov ~]$ echo "test" /home/guest/dir1/file1  
test /home/guest/dir1/file1
```

Рис. 6: `echo "test" /home/guest/dir1/file1`

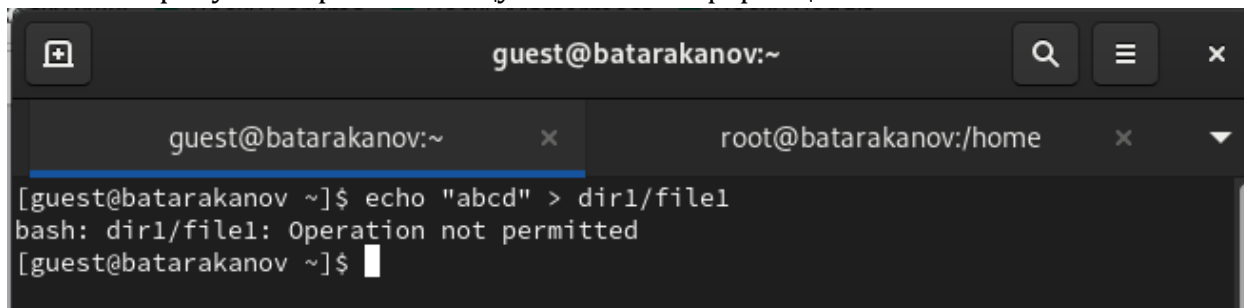
7. Выполним чтение файла `file1`



```
guest@batarakanov:~  
[guest@batarakanov ~]$ echo "test" /home/guest/dir1/file1  
test /home/guest/dir1/file1  
[guest@batarakanov ~]$ cat /home/guest/dir1/file1  
[guest@batarakanov ~]$
```

Рис. 7: `cat /home/guest/dir1/file1`

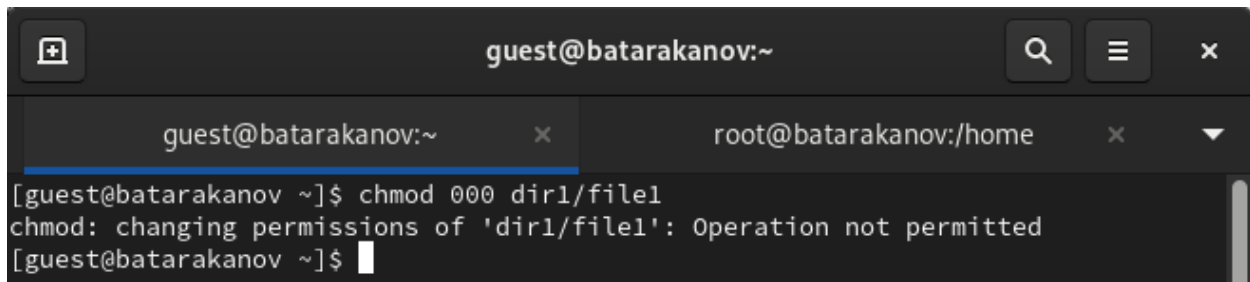
8. Попробуем стереть имеющуюся в нём информацию



```
guest@batarakanov:~  
[guest@batarakanov ~]$ echo "abcd" > dir1/file1  
bash: dir1/file1: Operation not permitted  
[guest@batarakanov ~]$
```

Рис. 8: `echo "abcd" > /home/guest/dir1/file1`

9. Далее попробуем установить на файл `file1` права запрещающие чтение и запись для владельца файла

A terminal window with a dark background. The title bar shows 'guest@batarakanov:~'. There are two tabs: 'guest@batarakanov:~' (active) and 'root@batarakanov:/home'. The terminal content shows a command prompt '[guest@batarakanov ~]\$' followed by 'chmod 000 dir1/file1'. The next line shows the error message 'chmod: changing permissions of 'dir1/file1': Operation not permitted'. The prompt returns to '[guest@batarakanov ~]\$' with a cursor.

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

*Рис. 9: chmod 000 file1*

10. Снимем расширенный атрибут «a» с файла /home/guest/dir1/file1 от имени суперпользователя и повторим операции, которые нам ранее не удавалось выполнить

*Рис. 10: chattr -a /home/guest/dir1/file1*

11. В конце повторим наши действия по шагам, заменив атрибут «a» атрибутом «i»

*Рис. 11: Повторение действий по шагам с атрибутом «i»*

## 4 Вывод

В ходе выполнения лабораторной работы были получены практические навыки работы в консоли с расширенными атрибутами файлов.

## 5 Список литературы. Библиография

[1] Права доступа: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>

[2] Расширенные атрибуты: <https://ru.manpages.org/xattr/7>

[3] Операции с расширенными атрибутами: <https://p-n-z-8-8.livejournal.com/64493.html>