

# Дискреционное разграничение прав в Linux. Расширенные атрибуты

## Содержание

|                                       |   |
|---------------------------------------|---|
| Цель работы .....                     | 1 |
| Теоретическое введение .....          | 1 |
| Выполнение лабораторной работы .....  | 2 |
| Вывод .....                           | 4 |
| Список литературы. Библиография ..... | 4 |

## Цель работы

Получить практические навыки работы в консоли с расширенными атрибутами файлов

## 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 определен или не определен. Если он определен, 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:*

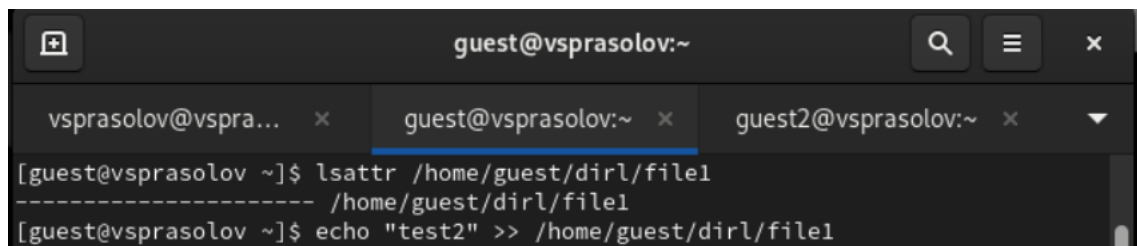
- `lsattr filename`

*Опции:*

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

## Выполнение лабораторной работы

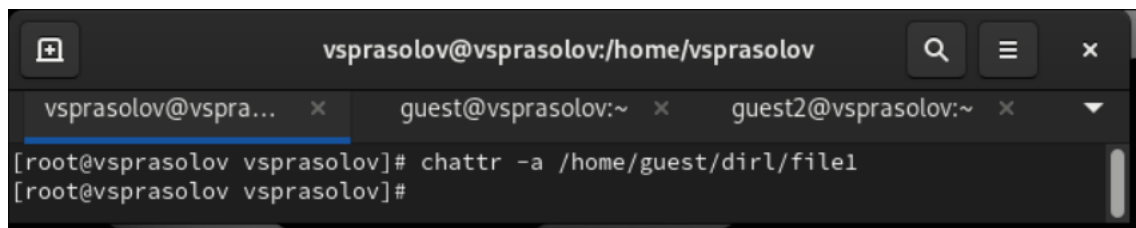
1. От имени пользователя `guest` определите расширенные атрибуты файла `/home/guest/dir1/file1` командой `lsattr /home/guest/dir1/file1`



The screenshot shows a terminal window with the title `guest@vsprasolov:~`. The terminal has three tabs: `vsprasolov@vspra...`, `guest@vsprasolov:~` (which is active), and `guest2@vsprasolov:~`. The active tab shows the following commands and output:

```
[guest@vsprasolov ~]$ lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[guest@vsprasolov ~]$ echo "test2" >> /home/guest/dir1/file1
```

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`. В ответ вы должны получить отказ от выполнения операции.
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`

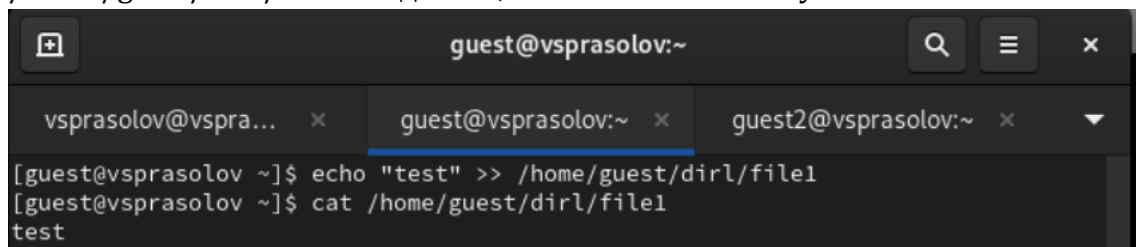


```
vsprsolov@vsprsolov:/home/vsprsolov
vsprsolov@vspra... x guest@vsprsolov:~ x guest2@vsprsolov:~ x
[root@vsprsolov vsprsolov]# chattr -a /home/guest/dirl/file1
[root@vsprsolov vsprsolov]#
```

5. От пользователя guest проверьте правильность установления атрибута: lsattr /home/guest/dir1/file1

(рис. 1. 1-5 пункты задания лабораторной)

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.



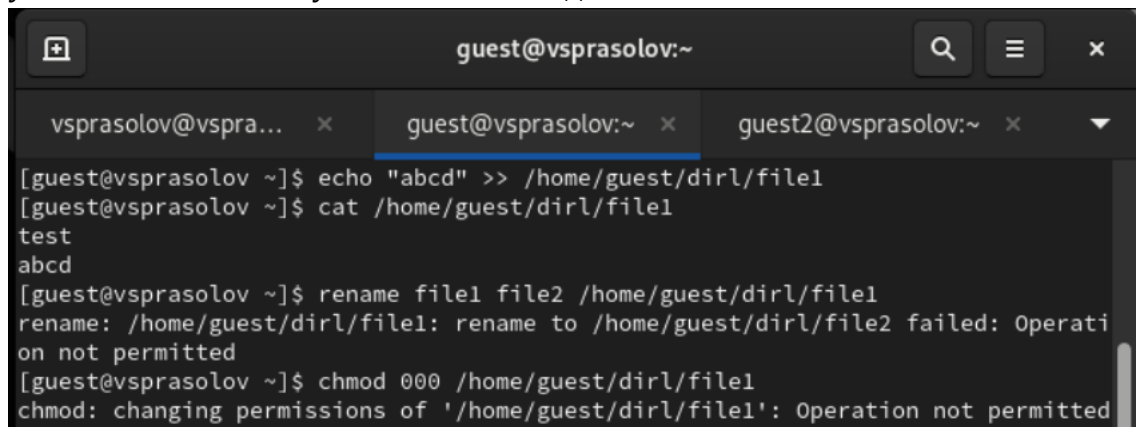
```
guest@vsprsolov:~
vsprsolov@vspra... x guest@vsprsolov:~ x guest2@vsprsolov:~ x
[guest@vsprsolov ~]$ echo "test" >> /home/guest/dirl/file1
[guest@vsprsolov ~]$ cat /home/guest/dirl/file1
test
```

(рис. 2. 6 пункт задания лабораторной)

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

(рис. 3. 7 пункт задания лабораторной)

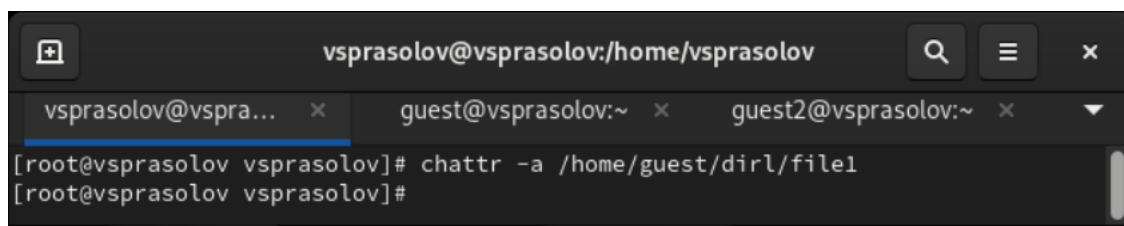
8. Попробуйте с помощью команды chmod 000 file1 установить на файл file1 права, например, запрещающие чтение и запись для владельца файла. Удалось ли вам успешно выполнить указанные команды?



```
guest@vsprsolov:~
vsprsolov@vspra... x guest@vsprsolov:~ x guest2@vsprsolov:~ x
[guest@vsprsolov ~]$ echo "abcd" >> /home/guest/dirl/file1
[guest@vsprsolov ~]$ cat /home/guest/dirl/file1
test
abcd
[guest@vsprsolov ~]$ rename file1 file2 /home/guest/dirl/file1
rename: /home/guest/dirl/file1: rename to /home/guest/dirl/file2 failed: Operation not permitted
[guest@vsprsolov ~]$ chmod 000 /home/guest/dirl/file1
chmod: changing permissions of '/home/guest/dirl/file1': Operation not permitted
```

Этого сделать не удалось.

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

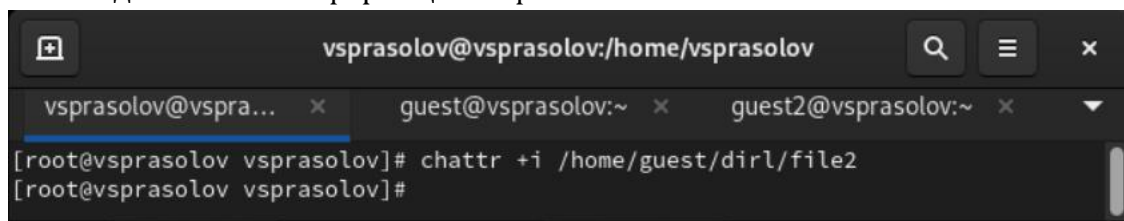


```
vsprasolov@vsprasolov:/home/vsprasolov
vsprasolov@vspra... x guest@vsprasolov:~ x guest2@vsprasolov:~ x
[root@vsprasolov vsprasolov]# chattr -a /home/guest/dirl/file1
[root@vsprasolov vsprasolov]#
```

Теперь все операции выполняются.

(рис. 4. 9 пункт задания лабораторной)

10. Повторите ваши действия по шагам, заменив атрибут «а» атрибутом «і». Удалось ли вам дозаписать информацию в файл?



```
vsprasolov@vsprasolov:/home/vsprasolov
vsprasolov@vspra... x guest@vsprasolov:~ x guest2@vsprasolov:~ x
[root@vsprasolov vsprasolov]# chattr +i /home/guest/dirl/file2
[root@vsprasolov vsprasolov]#
```

Дозаписать информацию в файл не удалось.

(рис. 5. 10 пункт задания лабораторной)

## Вывод

Были получены практические навыки работы в консоли с расширенными атрибутами файлов

## Список литературы. Библиография

- [0] Методические материалы курса
- [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>