

Отчёт по лабораторной работе

Лабораторная работа № 4

Живцова Анна

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	8
4	Выводы	10
	Список литературы	11

Список иллюстраций

3.1	Попытки выполнить операции с файлом с установленным атрибутом -а и без него	8
3.2	Попытки выполнить операции с файлом с установленным атрибутом -і и без него	9

Список таблиц

1 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

2 Теоретическое введение

Каждый файл или каталог имеет права доступа, обозначаемые комбинацией букв латинского (обозначает разрешение) алфавита и знаков – (обозначает отсутствие разрешения). Для файла: r — разрешено чтение, w — разрешена запись, x — разрешено выполнение, для каталога: r — разрешён просмотр списка входящих файлов, w — разрешены создание и удаление файлов, x — разрешён доступ в каталог и есть возможность сделать его текущим, - — право доступа отсутствует. В сведениях о файле или каталоге указываются: – тип файла (символ (-) обозначает файл, а символ (d) — каталог);

- права для владельца файла;
- права для членов группы;
- права для всех остальных [1].

Каждый файл имеет возможность задания ряда атрибутов:

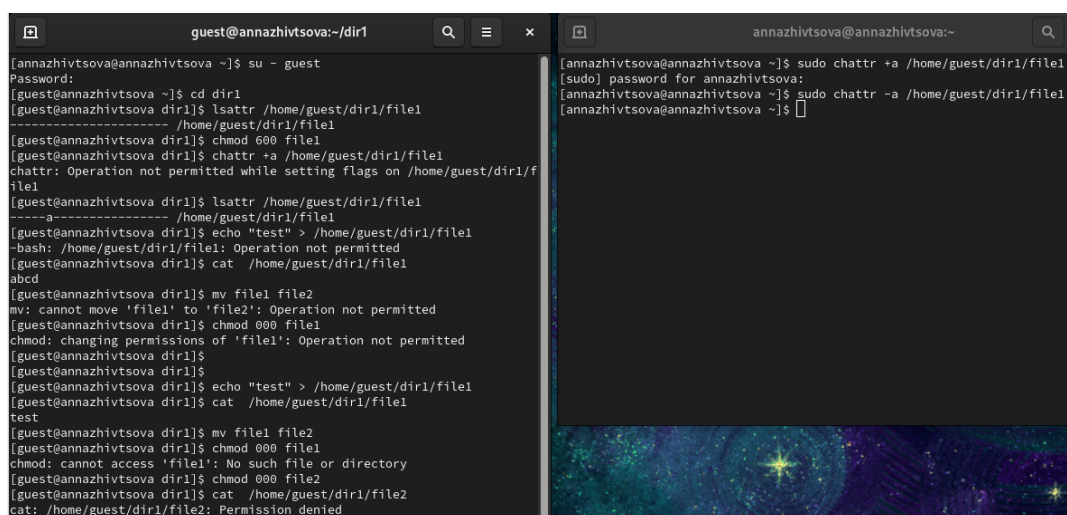
- a - файл может быть открыт только в режиме добавления;
- A - не обновлять время перезаписи;
- c - автоматически сжимать при записи на диск;
- C - отключить копирование при записи;
- D - работает только для папки, когда установлен, все изменения синхронно записываются на диск сразу же;
- e - использовать extent'ы блоков для хранения файла;
- i - сделать неизменяемым;
- j - все данные перед записью в файл будут записаны в журнал;
- s - безопасное удаление с последующей перезаписью нулями;

- S - синхронное обновление, изменения файлов с этим атрибутом будут сразу же записаны на диск;
- t - файлы с этим атрибутом не будут храниться в отдельных блоках;
- u - содержимое файлов с этим атрибутом не будет удалено при удалении самого файла и потом может быть восстановлено [2] .

3 Выполнение лабораторной работы

Создали файл с правами доступа 600 и, изменяя атрибуты через суперпользователя, протестировали возможность записи, открытия, переименования и установления прав доступа 000.

С установленными атрибутами `a` и `i` не удалось записать данные в файл, переименовать файл или назначить право доступа 000. Без атрибутов операции выполнить удалось (см. рис. 3.1 3.2).

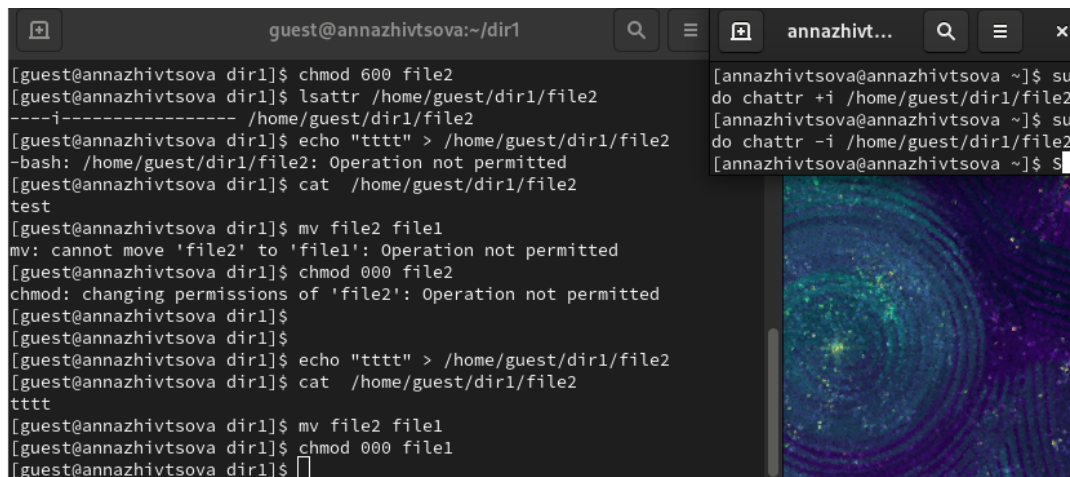


The image shows two terminal windows side-by-side. The left window is titled 'guest@annazhivtsova:~/dir1' and shows a series of commands and their outputs. The right window is titled 'annazhivtsova@annazhivtsova:~' and shows commands executed with 'sudo'.

```
guest@annazhivtsova:~/dir1
[annazhivtsova@annazhivtsova ~]$ su - guest
Password:
[guest@annazhivtsova ~]$ cd dir1
[guest@annazhivtsova dir1]$ lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[guest@annazhivtsova dir1]$ chmod 600 file1
[guest@annazhivtsova dir1]$ chattr +a /home/guest/dir1/file1
chattr: Operation not permitted while setting flags on /home/guest/dir1/f
ile1
[guest@annazhivtsova dir1]$ lsattr /home/guest/dir1/file1
-----a----- /home/guest/dir1/file1
[guest@annazhivtsova dir1]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Operation not permitted
[guest@annazhivtsova dir1]$ cat /home/guest/dir1/file1
abcd
[guest@annazhivtsova dir1]$ mv file1 file2
mv: cannot move 'file1' to 'file2': Operation not permitted
[guest@annazhivtsova dir1]$ chmod 000 file1
chmod: changing permissions of 'file1': Operation not permitted
[guest@annazhivtsova dir1]$
[guest@annazhivtsova dir1]$ echo "test" > /home/guest/dir1/file1
[guest@annazhivtsova dir1]$ cat /home/guest/dir1/file1
test
[guest@annazhivtsova dir1]$ mv file1 file2
[guest@annazhivtsova dir1]$ chmod 000 file1
chmod: cannot access 'file1': No such file or directory
[guest@annazhivtsova dir1]$ chmod 000 file2
[guest@annazhivtsova dir1]$ cat /home/guest/dir1/file2
cat: /home/guest/dir1/file2: Permission denied
```

```
annazhivtsova@annazhivtsova:~
[annazhivtsova@annazhivtsova ~]$ sudo chattr +a /home/guest/dir1/file1
[sudo] password for annazhivtsova:
[annazhivtsova@annazhivtsova ~]$ sudo chattr -a /home/guest/dir1/file1
[annazhivtsova@annazhivtsova ~]$
```

Рис. 3.1: Попытки выполнить операции с файлом с установленным атрибутом `-a` и без него



The screenshot shows a terminal window with two panes. The left pane shows a series of commands and their outputs from a user named 'guest' in a directory named 'dir1'. The commands include setting permissions to 600, checking attributes, creating a file with 'echo', attempting to move it to 'file1' (which fails), attempting to change permissions to 000 (which fails), and finally moving it to 'file1' after setting permissions to 000. The right pane shows a user named 'annazhivtsova' using 'su' to become root, then using 'chattr +i' to set the immutable attribute on '/home/guest/dir1/file2', and finally using 'chattr -i' to remove it. The terminal has a dark background with a colorful, abstract pattern on the right side.

```
[guest@annazhivtsova dir1]$ chmod 600 file2
[guest@annazhivtsova dir1]$ lsattr /home/guest/dir1/file2
----i----- /home/guest/dir1/file2
[guest@annazhivtsova dir1]$ echo "tttt" > /home/guest/dir1/file2
-bash: /home/guest/dir1/file2: Operation not permitted
[guest@annazhivtsova dir1]$ cat /home/guest/dir1/file2
test
[guest@annazhivtsova dir1]$ mv file2 file1
mv: cannot move 'file2' to 'file1': Operation not permitted
[guest@annazhivtsova dir1]$ chmod 000 file2
chmod: changing permissions of 'file2': Operation not permitted
[guest@annazhivtsova dir1]$
[guest@annazhivtsova dir1]$
[guest@annazhivtsova dir1]$ echo "tttt" > /home/guest/dir1/file2
[guest@annazhivtsova dir1]$ cat /home/guest/dir1/file2
tttt
[guest@annazhivtsova dir1]$ mv file2 file1
[guest@annazhivtsova dir1]$ chmod 000 file1
[guest@annazhivtsova dir1]$
```

```
[annazhivtsova@annazhivtsova ~]$ su
do chattr +i /home/guest/dir1/file2
[annazhivtsova@annazhivtsova ~]$ su
do chattr -i /home/guest/dir1/file2
[annazhivtsova@annazhivtsova ~]$
```

Рис. 3.2: Попытки выполнить операции с файлом с установленным атрибутом -i и без него

4 Выводы

Повысили свои навыки использования интерфейса командой строки, 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.

Список литературы

1. Робачевский А., Немнюгин С., Стесик О. Операционная система UNIX. 2-е изд. БХВ-Петербург, 2010. 656 с.
2. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.