

Отчеты по лабораторной работе №4

Основы информационной безопасности

Беспутий Глеб Антонович, НКАбд01-23

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	8
4	Выводы	22
5	Список литературы. Библиография	23

Список иллюстраций

3.1	Определение атрибутов	8
3.2	Изменение прав доступа	9
3.3	Попытка установки расширенных атрибутов	10
3.4	Установка расширенных атрибутов	11
3.5	Проверка атрибутов	12
3.6	Дозапись в файл	13
3.7	Попытка удалить файл	14
3.8	Попытка переименовать файл	15
3.9	Попытка изменить права доступа	16
3.10	Снятие расширенных атрибутов	17
3.11	Проверка выполнения действий	18
3.12	Попытка добавить расширенный атрибут	19
3.13	Добавление расширенного атрибута	20
3.14	Проверка выполнения действий	21

Список таблиц

1 Цель работы

Получение практических навыков 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, созданного в прошлых лабораторных работах, определяю расширенные атрибуты файла /home/guest/dir1/file1 (рис. 1).

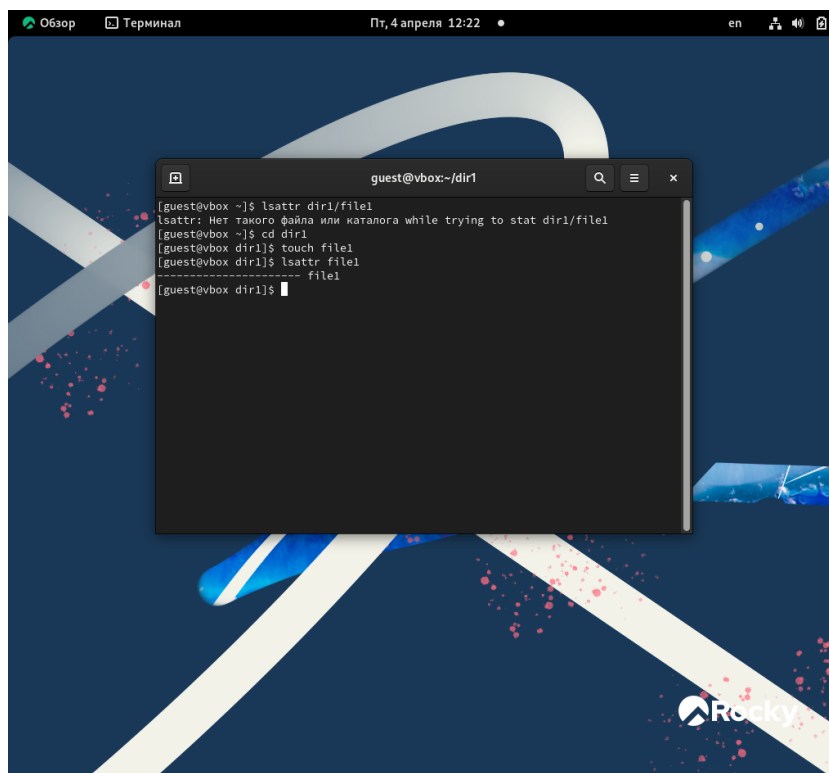


Рис. 3.1: Определение атрибутов

2. Изменяю права доступа для файла home/guest/dir1/file1 с помощью chmod 600 (рис. 2).

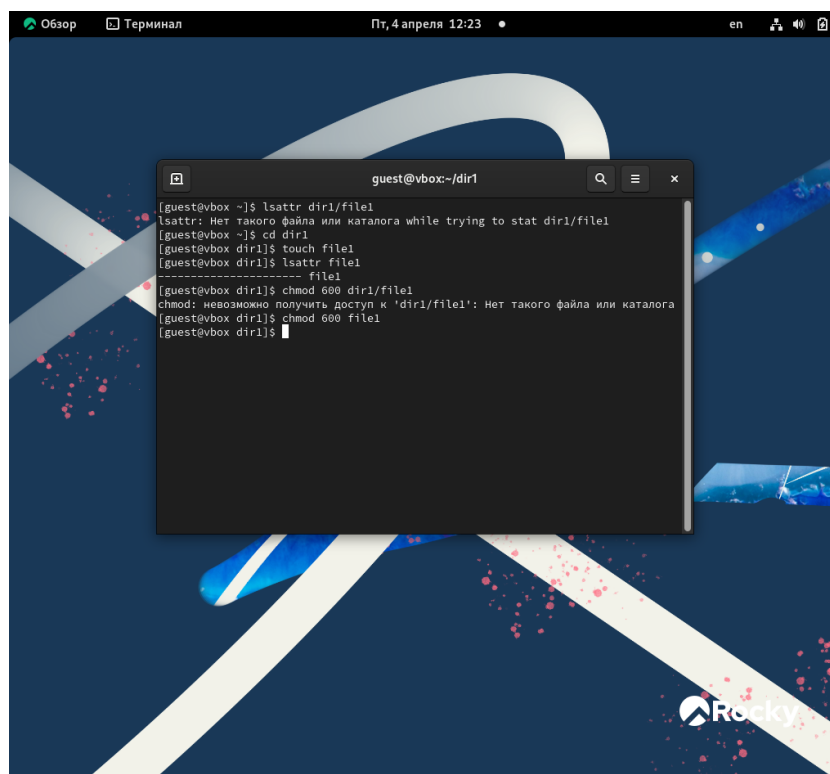


Рис. 3.2: Изменение прав доступа

3. Пробую установить на файл `/home/guest/dir1/file1` расширенный атрибут `a` от имени пользователя `guest`, в ответ получаю отказ от выполнения операции (рис. 3).

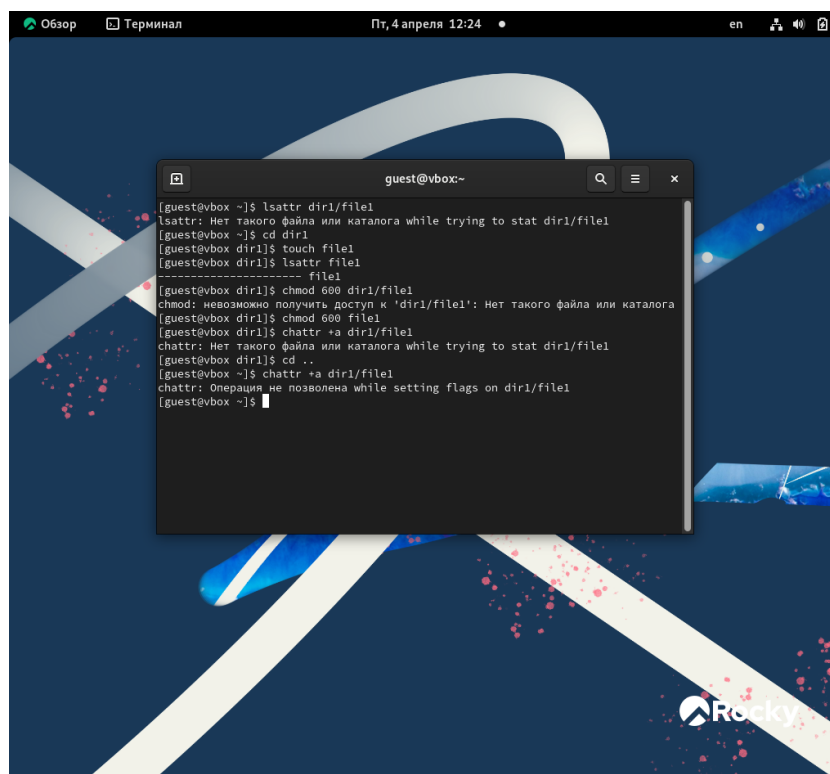


Рис. 3.3: Попытка установки расширенных атрибутов

4. Устанавливаю расширенные права уже от имени суперпользователя, теперь нет отказа от выполнения операции (рис. 4).

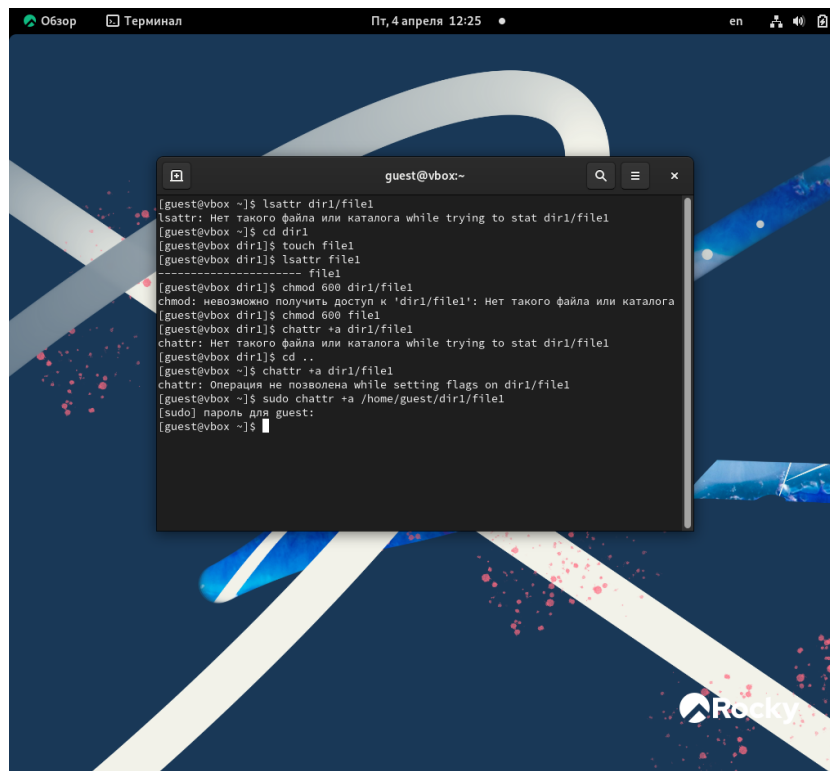


Рис. 3.4: Установка расширенных атрибутов

5. От пользователя guest проверяю правильность установки атрибута (рис. 5).

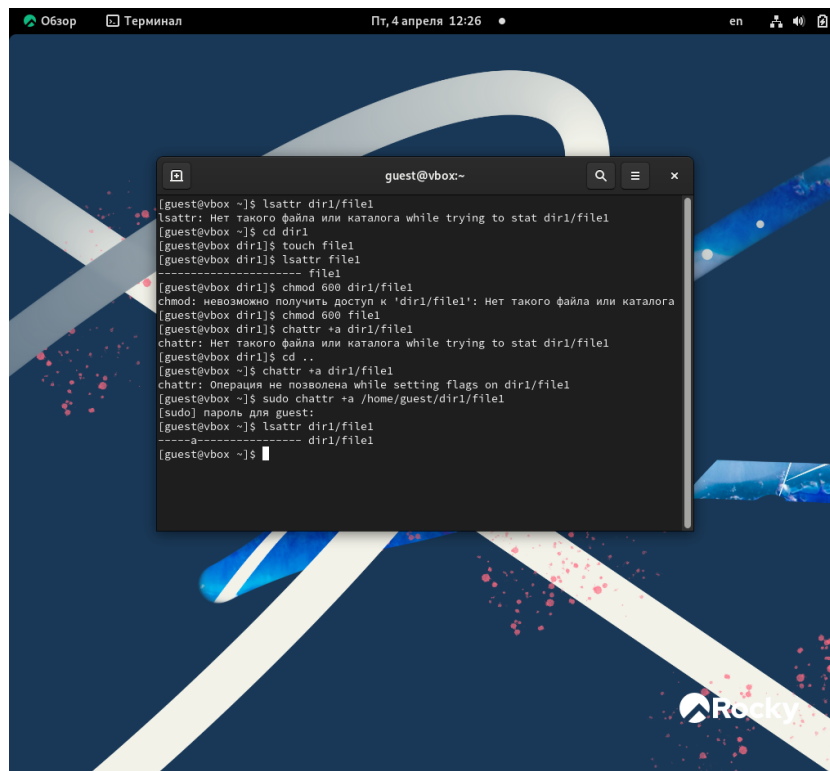
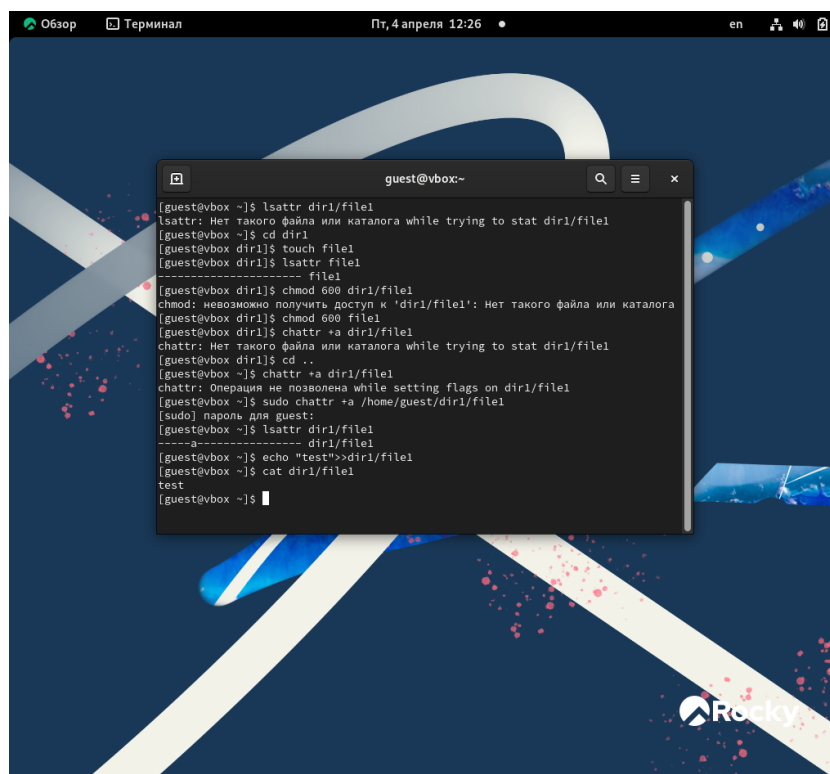


Рис. 3.5: Проверка атрибутов

6. Выполняю **дозапись** в файл с помощью `echo 'test' >> dir1/file1`, далее выполняю чтение файла, убеждаюсь, что дозапись была выполнена (рис. 6).



```
guest@vbox:~  
[guest@vbox ~]$ lsattr dir1/file1  
lsattr: Нет такого файла или каталога while trying to stat dir1/file1  
[guest@vbox ~]$ cd dir1  
[guest@vbox dir1]$ touch file1  
[guest@vbox dir1]$ lsattr file1  
-----  
file1  
[guest@vbox dir1]$ chmod 600 dir1/file1  
[guest@vbox dir1]$ lsattr file1  
lsattr: невозможно получить доступ к 'dir1/file1': Нет такого файла или каталога  
[guest@vbox dir1]$ chmod 600 file1  
[guest@vbox dir1]$ chattr +a dir1/file1  
chattr: Нет такого файла или каталога while trying to stat dir1/file1  
[guest@vbox dir1]$ cd ..  
[guest@vbox ~]$ chattr +a dir1/file1  
chattr: Операция не позволена while setting flags on dir1/file1  
[guest@vbox ~]$ sudo chattr +a /home/guest/dir1/file1  
[sudo] пароль для guest:  
[guest@vbox ~]$ lsattr dir1/file1  
-----a----- dir1/file1  
[guest@vbox ~]$ echo "test">>dir1/file1  
[guest@vbox ~]$ cat dir1/file1  
test  
[guest@vbox ~]$
```

Рис. 3.6: Дозапись в файл

7. Пробую удалить файл, получаю отказ от выполнения действия. (рис. 7).

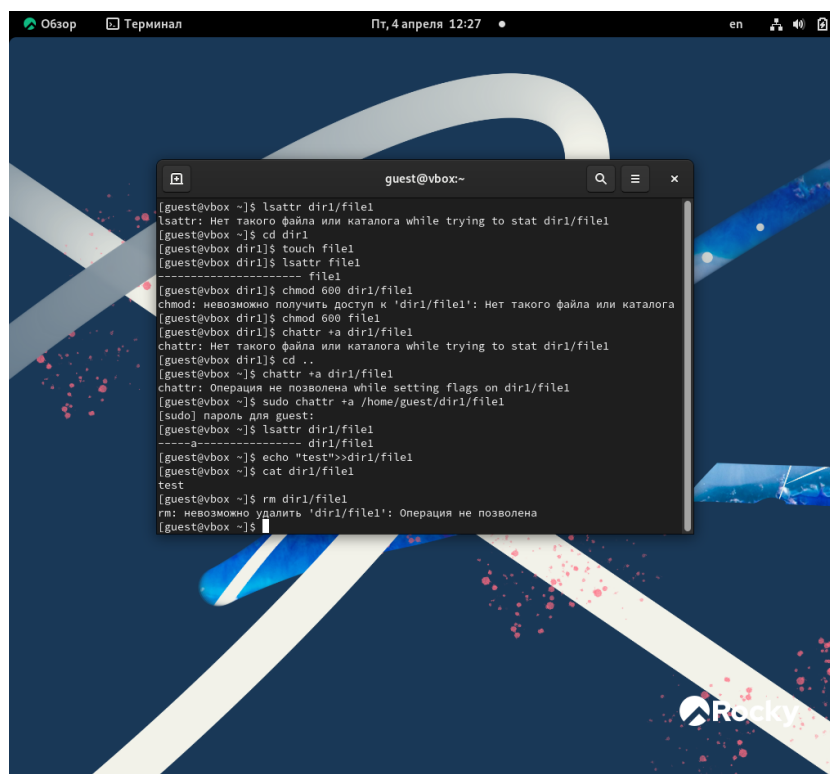


Рис. 3.7: Попытка удалить файл

То же самое получаю при попытке переименовать файл(рис. 8).

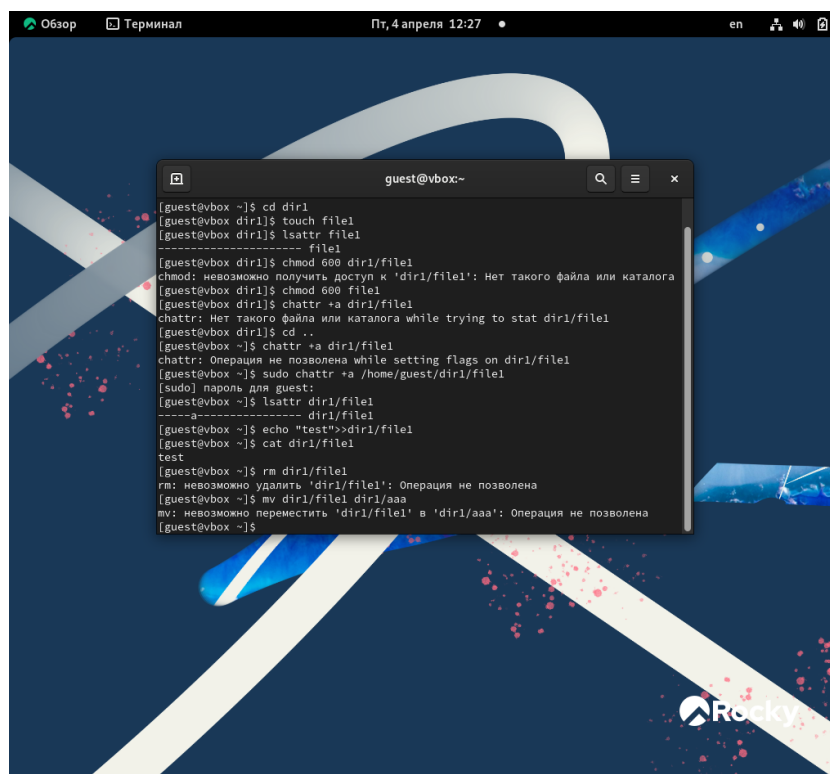


Рис. 3.8: Попытка переименовать файл

8. Получаю отказ от выполнения при попытке установить другие права доступа (рис. 9).

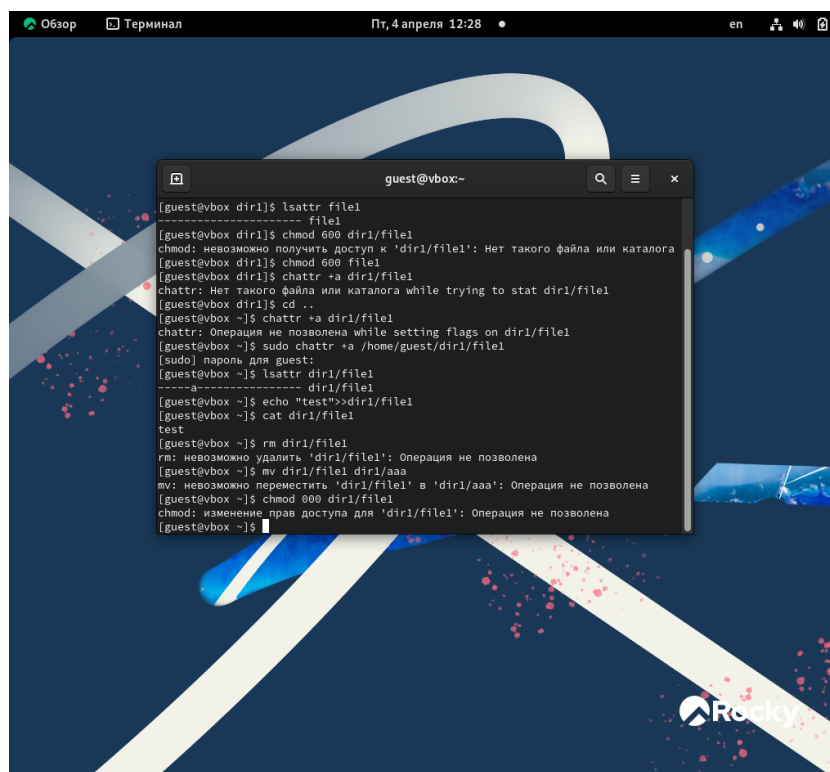


Рис. 3.9: Попытка изменить права доступа

9. Снимаю расширенные атрибуты с файла (рис. 10).

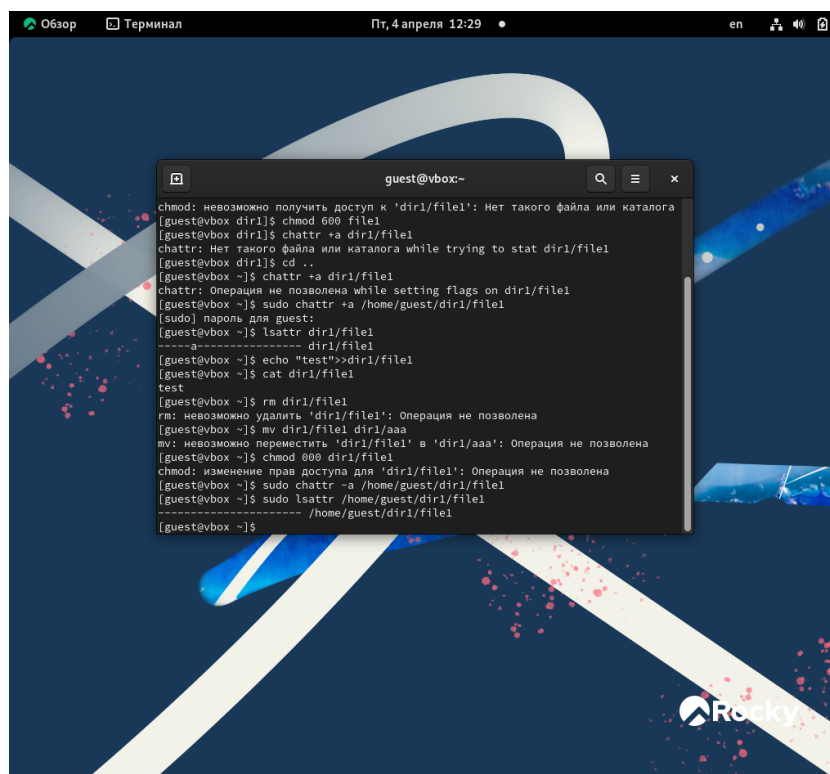


Рис. 3.10: Снятие расширенных атрибутов

Проверяю ранее не удавшиеся действия: чтение, переименование, изменение прав доступа. Теперь все из этого выполняется (рис. 11).

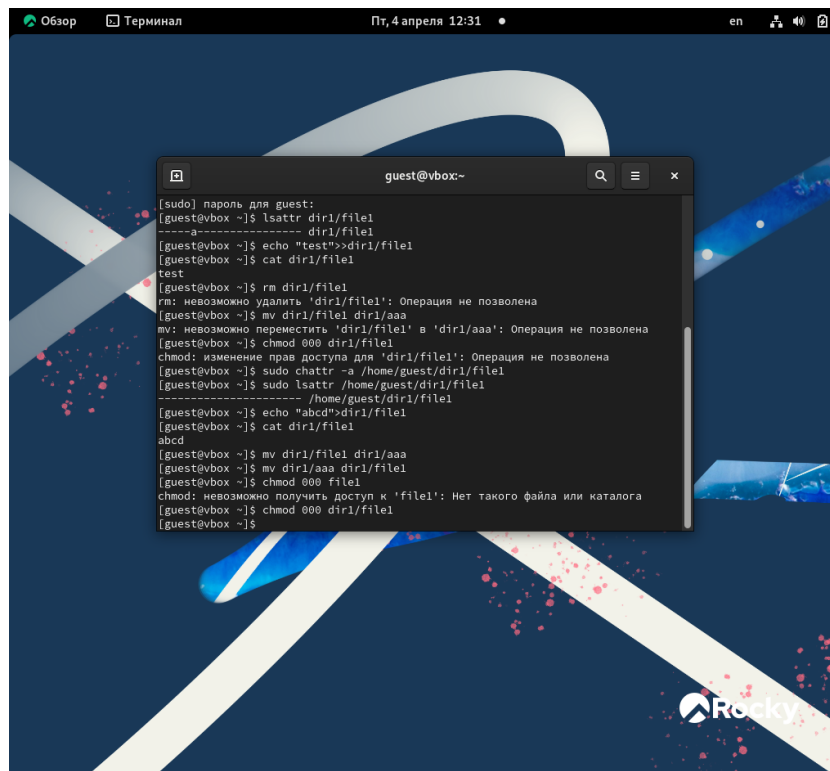


Рис. 3.11: Проверка выполнения действий

10. Пытаюсь добавить расширенный атрибут `i` от имени пользователя `guest`, как и раньше, получаю отказ (рис. 12).

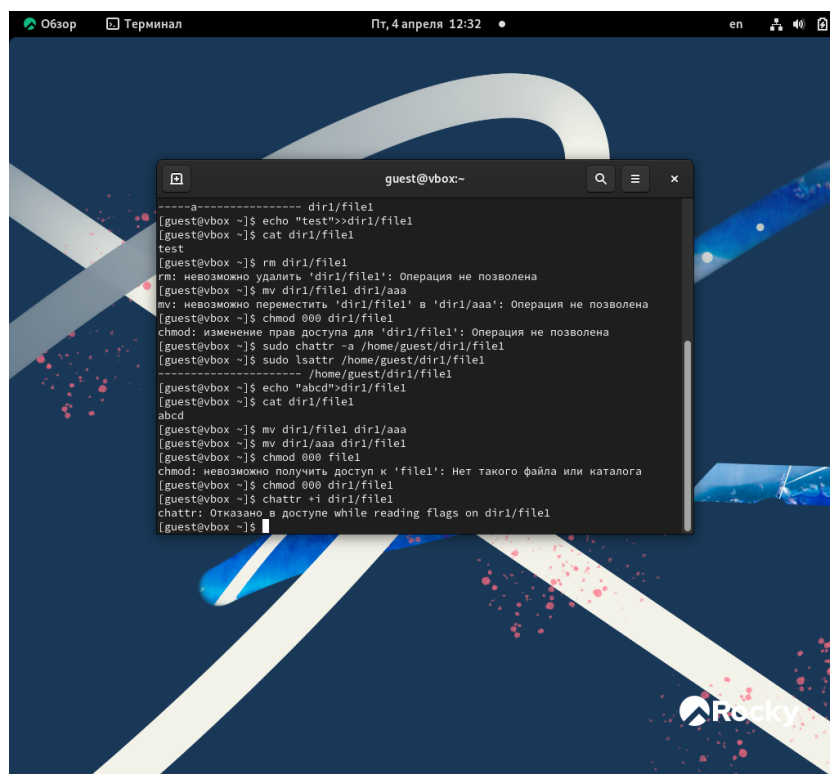


Рис. 3.12: Попытка добавить расширенный атрибут

Добавляю расширенный атрибут `i` от имени суперпользователя, теперь все выполнено верно (рис. 13).

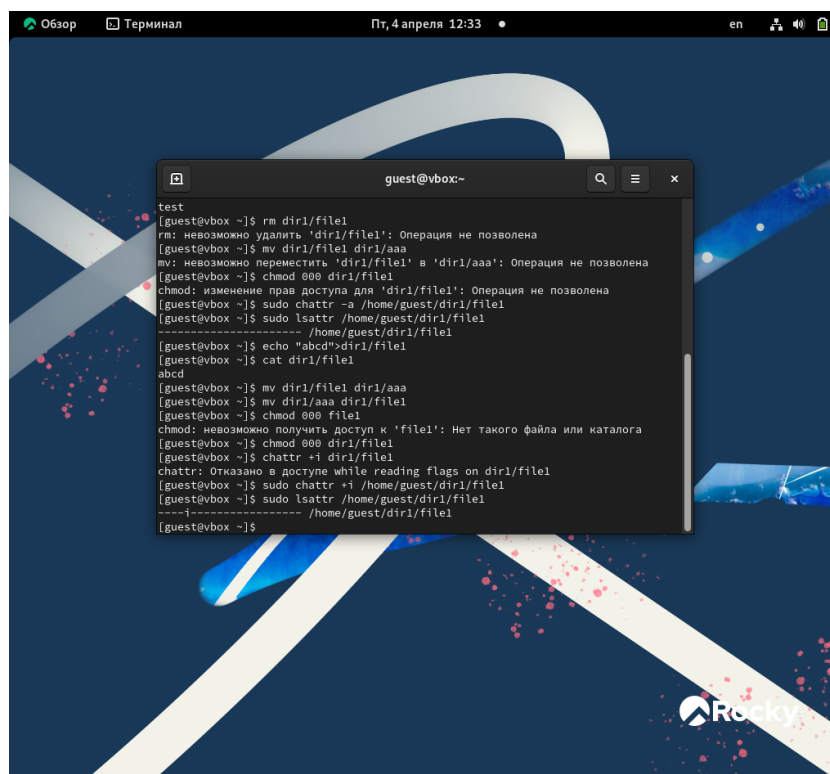


Рис. 3.13: Добавление расширенного атрибута

Пытаюсь записать в файл, дозаписать, переименовать или удалить, ничего из этого сделать нельзя (рис. 14).

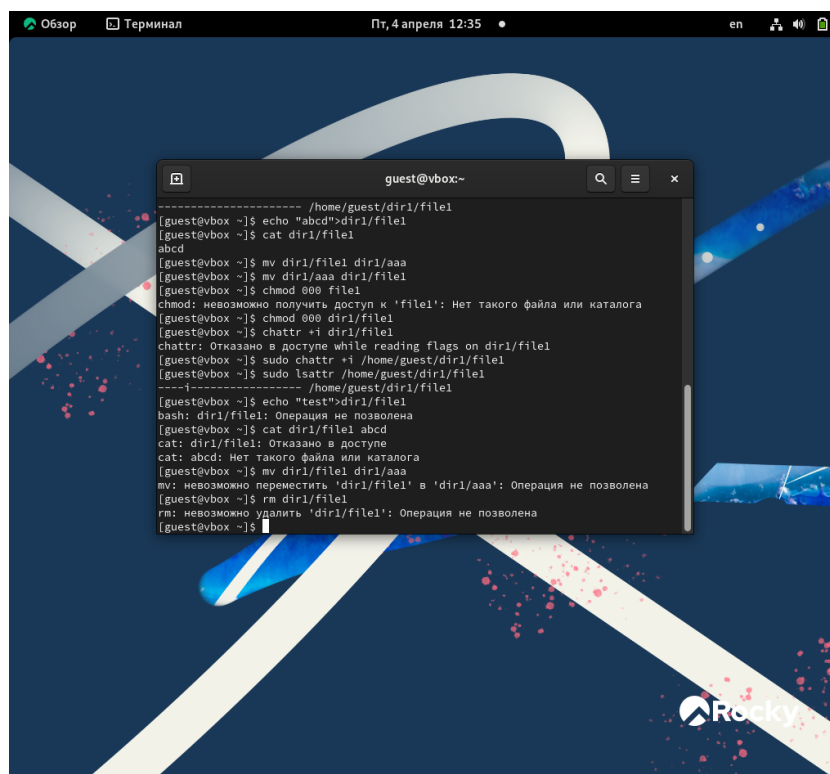


Рис. 3.14: Проверка выполнения действий

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. Опробовали действие на практике расширенных атрибутов «а» и «і»

5 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>