Отчет по лаборатной работе №4

по предмету Информационная безопасность

Алхимова Дарья Сергеевна

Содержание

[Цель работы 1](#__RefHeading___Toc510_3449507279)

[Задание 1](#__RefHeading___Toc512_3449507279)

[Теоретическое введение 2](#__RefHeading___Toc514_3449507279)

[Выполнение лабораторной работы 3](#__RefHeading___Toc516_3449507279)

[Выводы 8](#__RefHeading___Toc518_3449507279)

[Список литературы 8](#__RefHeading___Toc520_3449507279)

# Цель работы

Целью данной работы является получение практических навыков работы в консоли с расширенными атрибутами файлов.

# Задание

1. От имени пользователя guest определите расширенные атрибуты файла /home/guest/dir1/file1 командой lsattr /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.
5. От пользователя guest проверьте правильность установления атрибута: lsattr /home/guest/dir1/file1.
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.
7. Попробуйте удалить файл file1 либо стереть имеющуюся в нём информацию командой echo "abcd" > /home/guest/dirl/file1.  
   Попробуйте переименовать файл.
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? Снимите расширенный атрибутa с файла /home/guest/dirl/file1 от имени суперпользователя командой chattr -a /home/guest/dir1/file1. Повторите операции, которые вам ранее не удавалось выполнить. Ваши наблюдения занесите в отчёт. Повторите ваши действия по шагам, заменив атрибут «a» атрибутом «i». Удалось ли вам дозаписать информацию в файл? Ваши наблюдения занесите в отчёт.

# Теоретическое введение

Утилита chattr позволяет устанавливать и отключать атрибуты файлов, на уровне файловой системы не зависимо от стандартных (чтение, запись, выполнение). Для просмотра текущих аттрибутов можно использовать lsattr. Изначально атрибуты управляемые chattr и lsattr поддерживались только файловыми системами семейства ext (ext2,ext3,ext4), но теперь эта возможность доступна и в других популярных файловых системах таких как XFS, Btrfs, ReiserFS, и т д.

Утилиты chattr и lsattr входят в пакет e2fsprogs и предустановлены во всех современных дистрибутивах. Базовый синтаксис chattr выглядит следующим образом:

$ chattr опции [оператор][атрибуты] файлы

Вот основные опции утилиты, которые вы можете использовать:

* R - рекурсивная обработка каталога;
* V - максимально подробный вывод;
* f - игнорировать сообщения об ошибках;
* v - вывести версию.

Оператор может принимать значения:

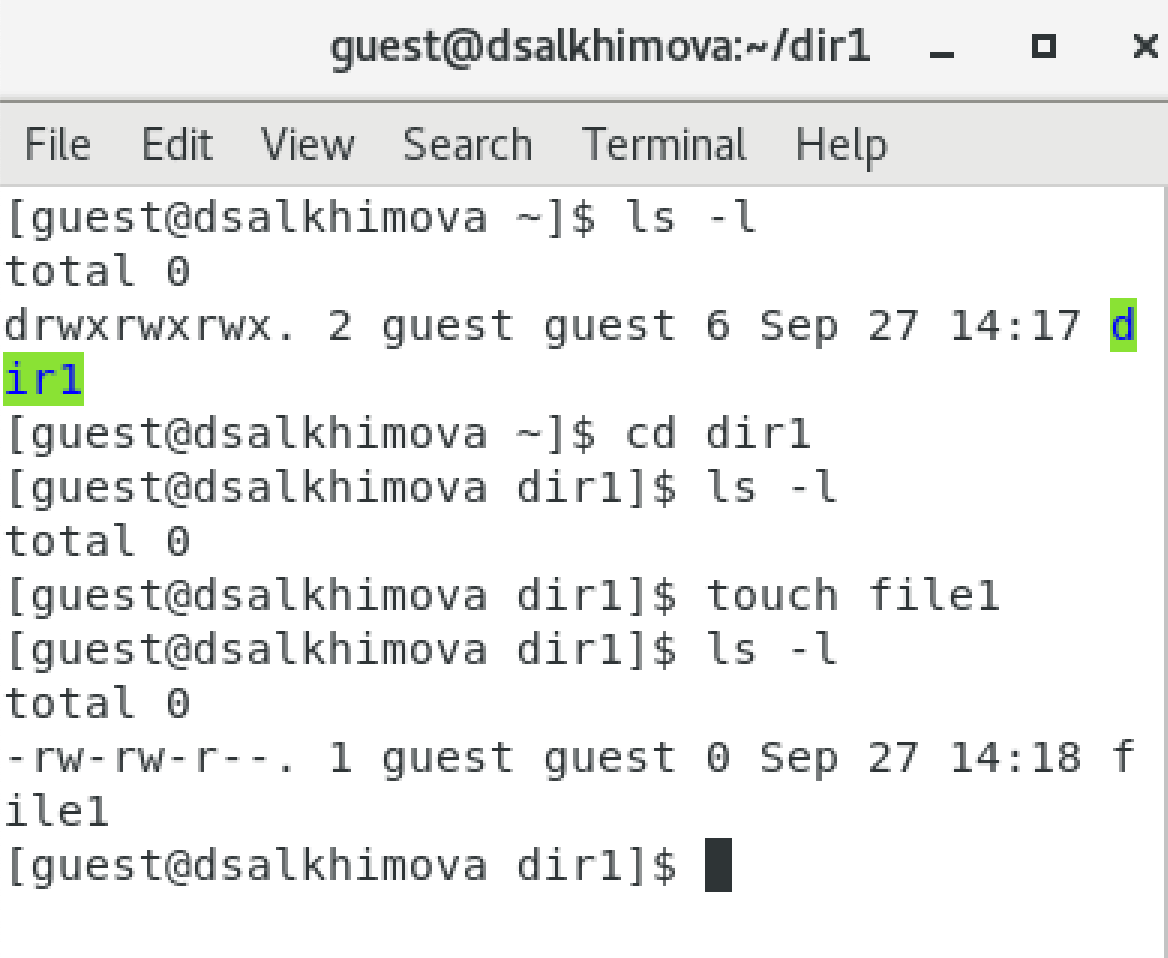
* + - включить выбранные атрибуты;
* - - отключить выбранные атрибуты;
* = - оставить значение атрибута таким, каким оно было у файла.

Доступные атрибуты:

* 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 хранится в отдельных блоках;
* u - содержимое файлов с этим атрибутом не будет удалено при удалении самого файла и потом может быть восстановлено.

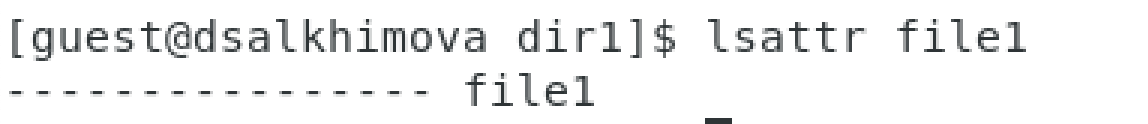
# Выполнение лабораторной работы

1. Проверила наличие файла file в директории dir1. Создала file1 в директории dir1 ([рис. 1](images4/1.png)).



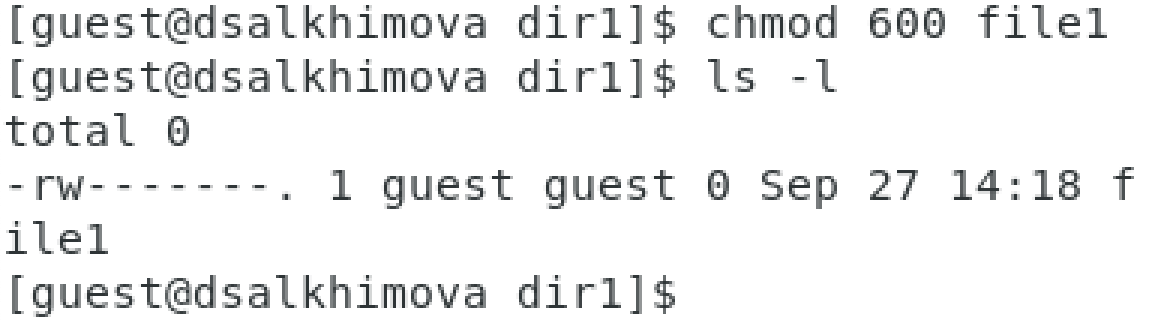
Создание файла

1. От имени пользователя guest определила расширенные атрибуты файла с помощью команды lsattr file1. Расширенных атрибутов не установлено ([рис. 2](images4/2.png)).



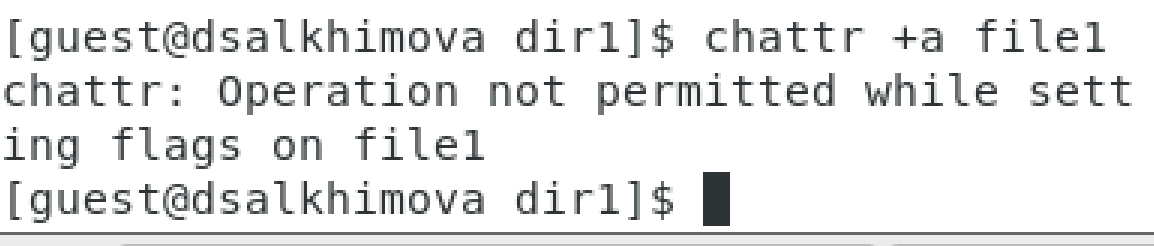
Проверка расширенных атрибутов файла

1. Установила командой chmod 600 file1 на файл file1 права, разрешающие чтение и запись для владельца файла ([рис. 3](images4/3.png)).



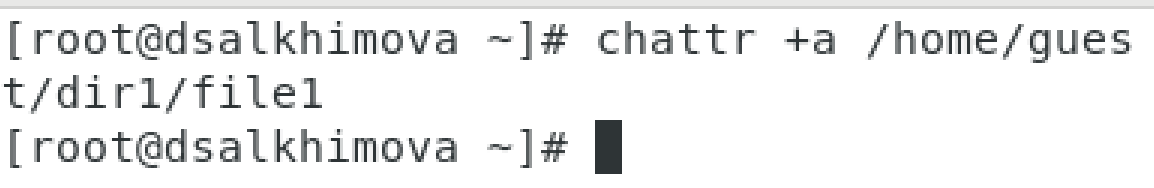
Установка прав для владельца файла

1. Попробовала установить на file1 расширенный атрибут a от имени пользователя guest командой chattr +a /home/guest/dir1/file1. В ответ получила отказ на выполнение операции ([рис. 4](images4/4.png)).



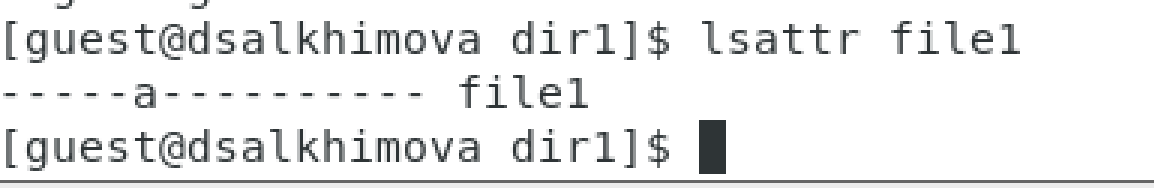
Установка расширенных прав от имени guest

1. Зашла в консоль от имени суперпользователя и попробовала установить расширенный атрибут a на файл командой chattr +a /home/guest/dir1/file1 ([рис. 5](images4/5.png)).



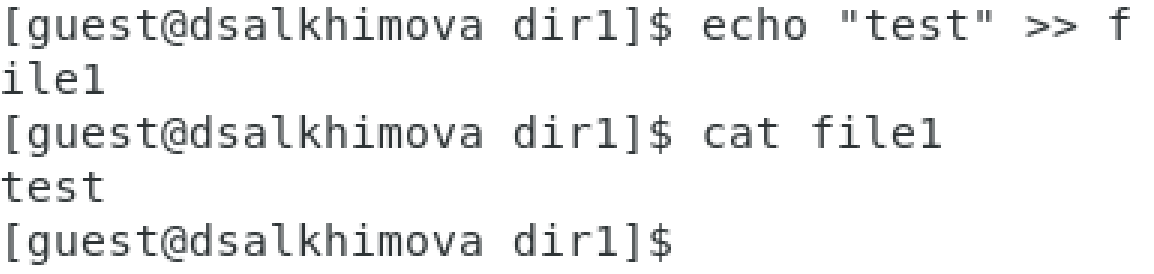
Установка расширенных прав от имени суперпользователя

1. От пользователя guest проверила правильность установления атрибута с помощью команды lsattr /home/guest/dir1/file1. Атрибут a установился ([рис. 6](images4/6.png)).



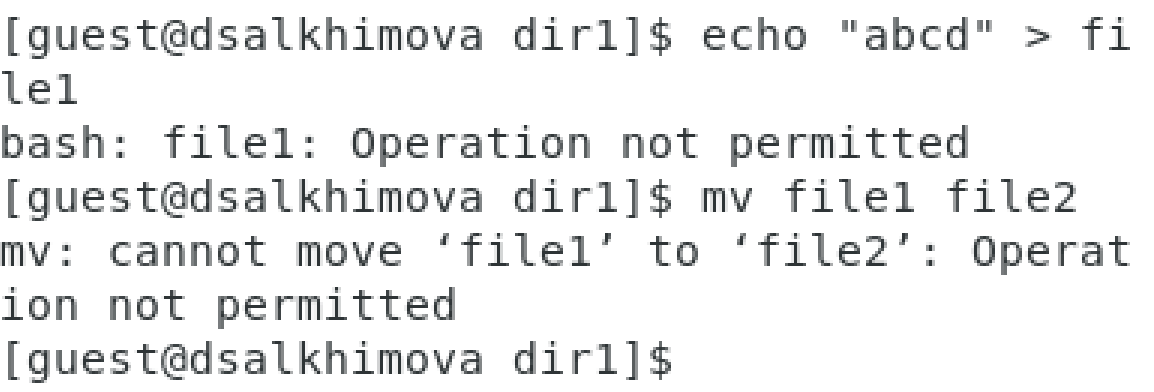
Проверка установки расширенного атрибута

1. Выполнила дозапись в файл file1 слова «test» командой echo "test" /home/guest/dir1/file1. После этого выполнила чтение файла file1 командой cat /home/guest/dir1/file1. Убедилась, что слово test было успешно записано в file1 ([рис. 7](images4/7.png)).



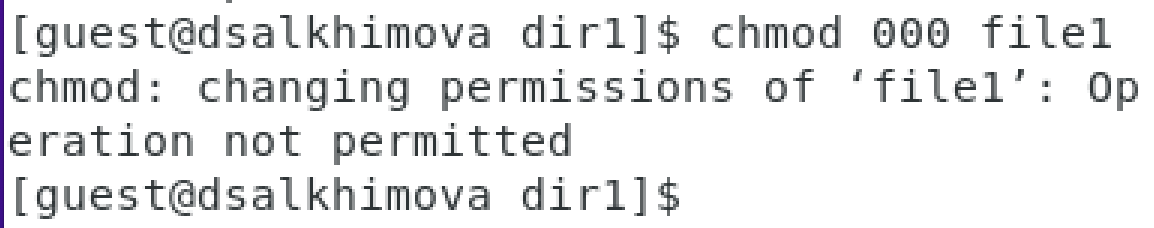
Дозапись в файл

1. Попробовала стереть имеющуюся в file1 информацию командой echo "abcd" > /home/guest/dirl/file1, переименовать файл командой mv - доступ запрещен. ([рис. 8](images4/8.png))



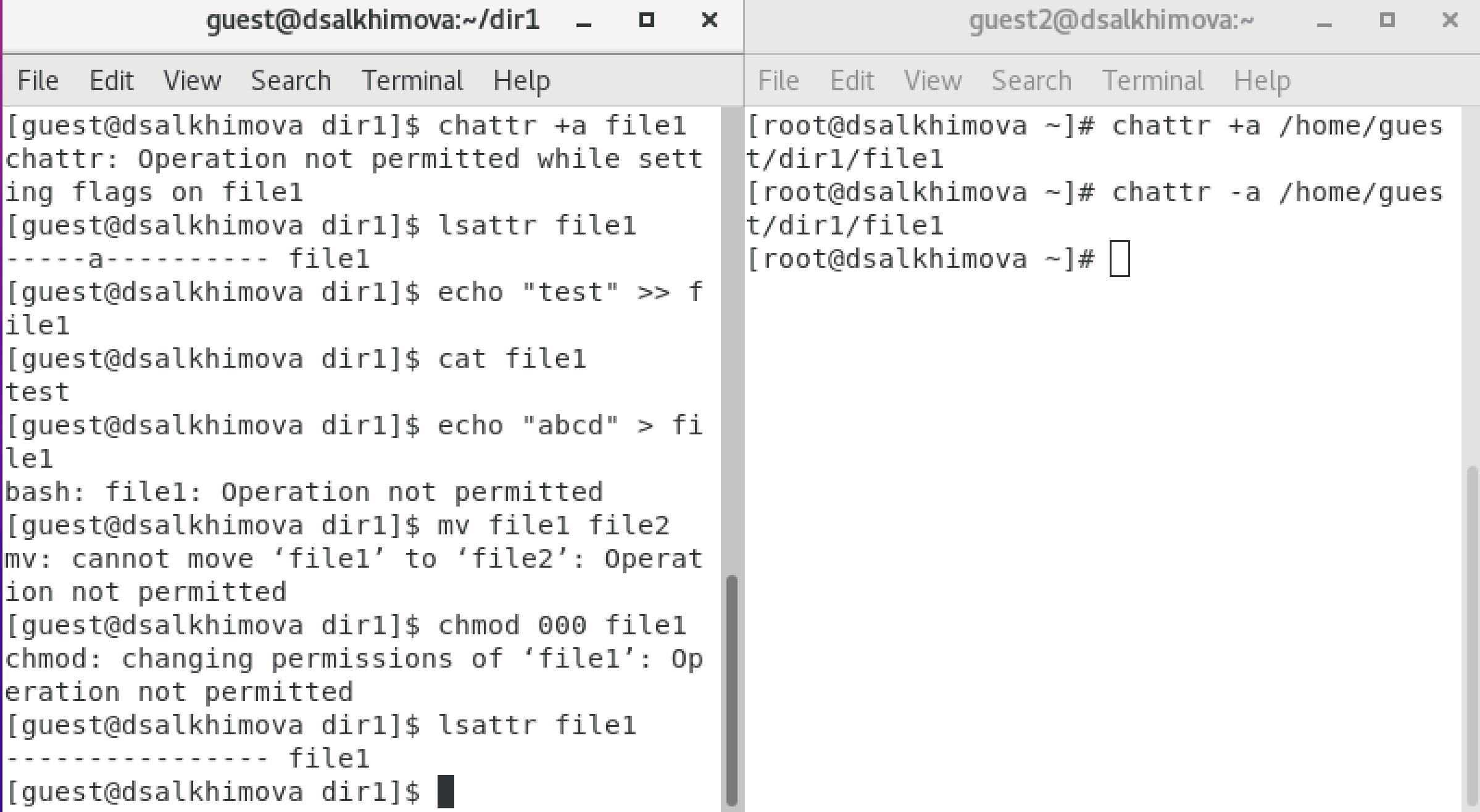
Изменение файла

1. От имени пользователя guest попробовала снять с файла file1 все атрибуты командой chmod 000 file1 - доступ запрещен ([рис. 9](images4/9.png)).



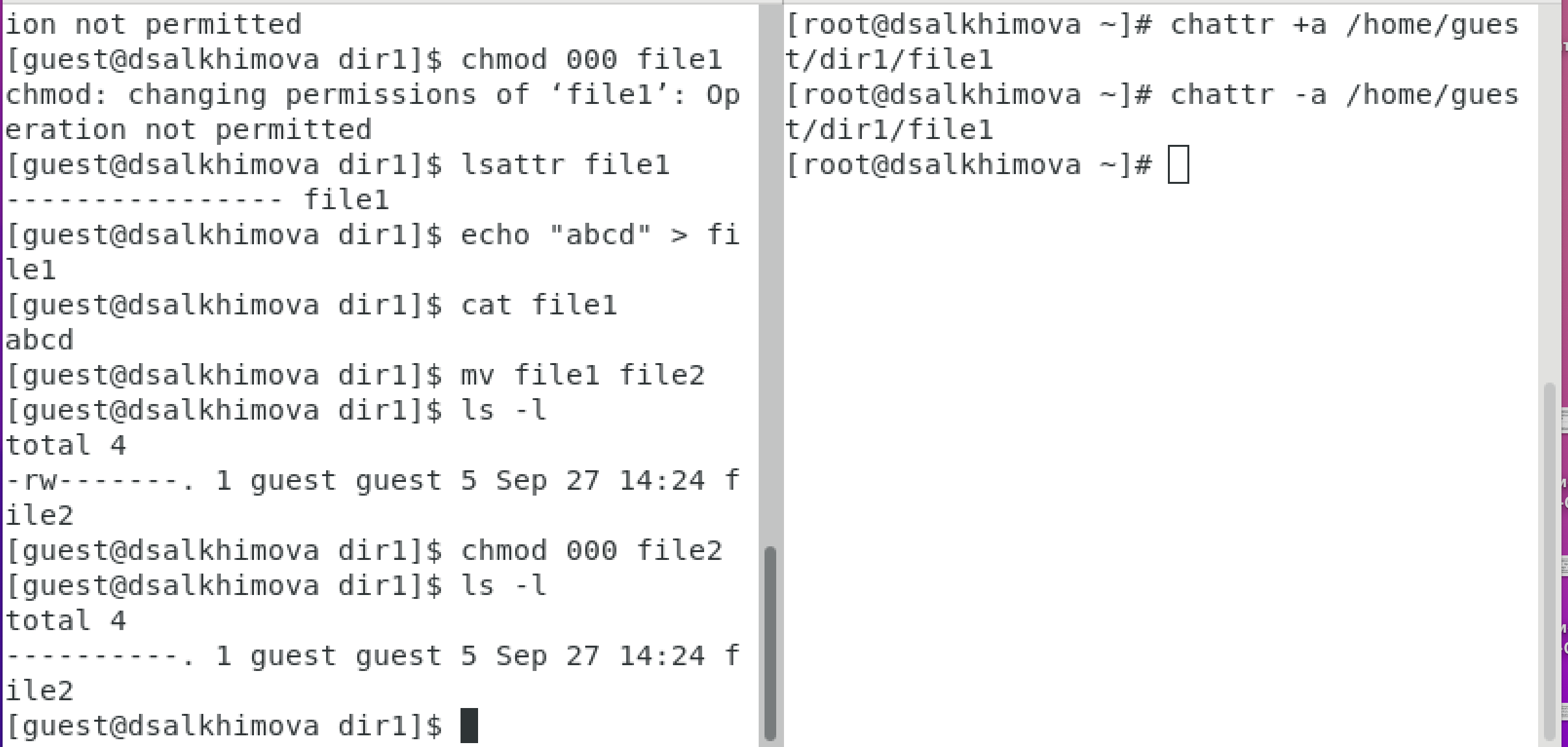
Редактрирование прав файла от имени guest

1. Сняла расширенный атрибут a с файла file1 от имени суперпользователя командой chattr -a /home/guest/dir1/file1 ([рис. 10](images4/10.png)).



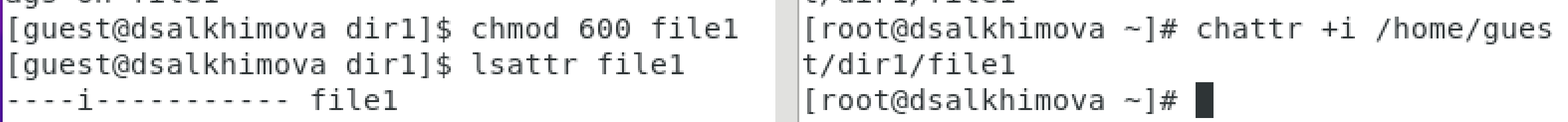
Снятие атрибута а

Повторила операции, которые ранее не удавалось выполнить. Операции выполнены успешно ([рис. 11](images4/11.png)).



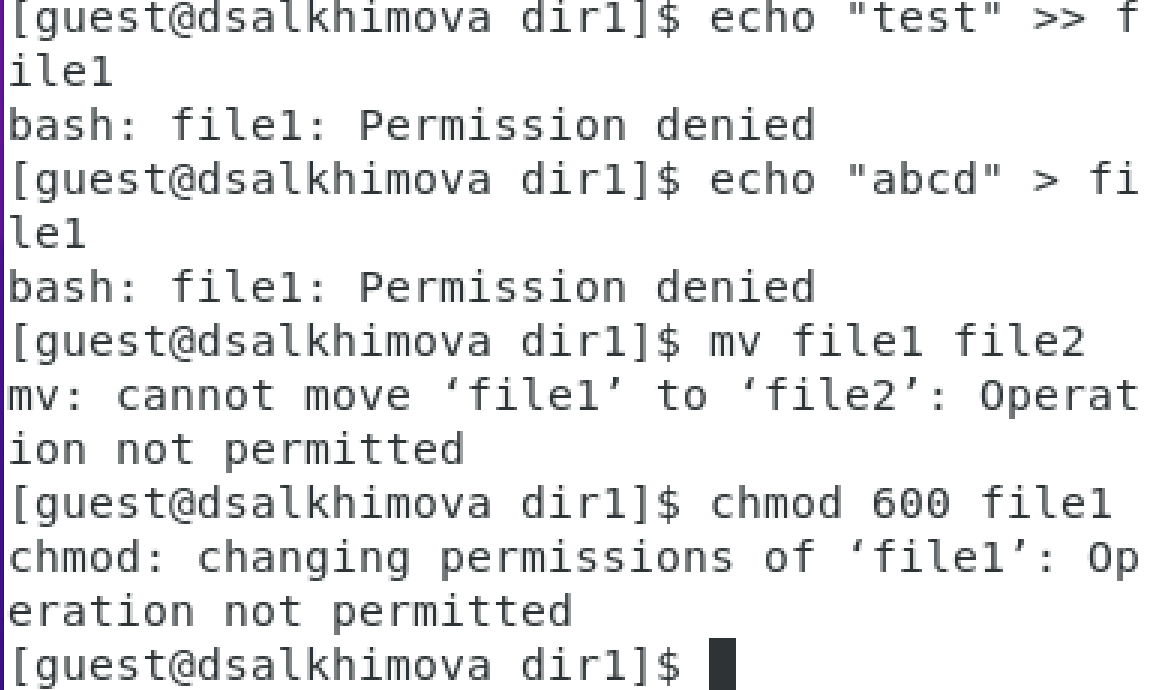
Повтор операций без атрибута а

1. Вернула владельцу права на чтение и запись для файла file1. Заменила атрибут «a» атрибутом «i» ([рис. 12](images4/12.png)).



Смена атрибута а на i

Повторила предыдущие действия с файлом. Операции выполнить не удалось, так как доступ запрещен - атрибут i делает файл неизменяемым ([рис. 13](images4/13.png)).



Действия с файлом при наличии атрибута i

# Выводы

В процессе выполнения данной лабораторной работы я повысила навыки использования интерфейса командой строки (CLI), познакомилась на примерах с тем, как используются основные и расширенные атрибуты при разграничении доступа. Связала теорию дискреционного разделения доступа (дискреционная политика безопасности) с её реализацией на практике в ОС Linux, а также опробовала действие на практике расширенных атрибутов «a» и «i».

# Список литературы

1. Команда CHATTR в LINUX — URL: <https://losst.ru/neizmenyaemye-fajly-v-linux?ysclid=l8k3gdovtw184374249>
2. File attribute. — URL: <https://en.wikipedia.org/wiki/File_attribute>