Отчёт по лабораторной работе №3 по предмету Информационная безопасность

Дискреционное разграничение прав в Linux. Два пользователя

Саттарова Вита Викторовна

Содержание

[1 Цели и задачи работы 1](#_Toc146403198)

[2 Объект и предмет исследования 2](#_Toc146403199)

[3 Условные обозначения и термины 2](#_Toc146403200)

[4 Задание 2](#_Toc146403201)

[5 Теоретическое введение 3](#_Toc146403202)

[5.1 Основы работы с группами и пользователями в ОС Linux 3](#_Toc146403203)

[5.2 Основы работы с уровнями доступа в ОС Linux 4](#_Toc146403204)

[6 Техническое оснащение и выбранные методы проведения работы 6](#_Toc146403205)

[7 Выполнение лабораторной работы и полученные результаты 7](#_Toc146403206)

[8 Анализ результатов 24](#_Toc146403207)

[9 Заключение и выводы 25](#_Toc146403208)

[10 Список литературы 25](#_Toc146403209)

# 1 Цели и задачи работы

**Цели:**

* Получить практические навыки работы в консоли с атрибутами файлов для групп пользователей.
* Закрепить практические навыки работы в консоли с атрибутами файлов.
* Закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

**Задачи:**

* Создать двух пользователей в одной группе, вспомнить теоретические основы работы с пользователями в Linux.
* Вспомнить теоретические основы атрибутов файлов и директорий в ОС Linux.
* Выполнить все пункты, указанные в методических рекомендациях к лабораторной работе.
* Создать две таблицы: **“Установленные права и разрешённые действия для групп”** и **“Минимальные права для совершения операций от имени пользователей входящих в группу”**.
* Проанализировать, за что отвечают разные атрибуты доступа.
* Написать отчёт с ответами на вопросы, заданные в пунктах для выполнения в методических рекомендациях к лабораторной работе.

# 2 Объект и предмет исследования

**Объект исследования:** разграничение доступа в ОС Linux для групп

**Предмет исследования:** группа пользователей, атрибуты доступа директории, атрибуты доступа файла, минимальные права для совершения операций с файлами и директориями

# 3 Условные обозначения и термины

**Условные обозначения**

* ОС - операционная система

**Термины**

* Дискреционное разграничение доступа
* Права/атрибуты доступа
* Директория

# 4 Задание

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (использую учётную запись администратора): useradd guest.
2. Задайте пароль для пользователя guest (использую учётную запись администратора): passwd guest.
3. Аналогично создайте второго пользователя guest2.
4. Добавьте пользователя guest2 в группу guest: gpasswd -a guest2 guest.
5. Осуществите вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли.
6. Для обоих пользователей командой pwd определите директорию, в которой вы находитесь. Сравните её с приглашениями командной строки.
7. Уточните имя вашего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определите командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2. Сравните вывод команды groups с выводом команд id -Gn и id -G.
8. Сравните полученную информацию с содержимым файла */etc/group*. Просмотрите файл командой cat /etc/group.
9. От имени пользователя guest2 выполните регистрацию пользователя guest2 в группе guest командой newgrp guest.
10. От имени пользователя guest измените права директории */home/guest*, разрешив все действия для пользователей группы: chmod g+rwx /home/guest.
11. От имени пользователя guest снимите с директории */home/guest/dir1* все атрибуты командой chmod 000 dirl и проверьте правильность снятия атрибутов.
12. Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполните табл. **“Установленные права и разрешённые действия для групп”**, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-». Сравните полученную таблицу с таблицей из лабораторной работы № 2.
13. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполните табл. **“Минимальные права для совершения операций от имени пользователей входящих в группу”**.

Более подробно о работе см. в [[1]](bib/cite.bib).

# 5 Теоретическое введение

## 5.1 Основы работы с группами и пользователями в ОС Linux

Добавление пользователя осуществляется при помощи команды useradd. Эта команда создаст в системе нового пользователя. Чтобы изменить настройки создаваемого пользователя, вы можете использовать ключи, например:

-с: Комментарий. В нем вы можете напечатать любой текст.

-d: Название домашнего каталога. По умолчанию название совпадает с именем создаваемого пользователя.

-G: Список вторичных групп в которых будет находится создаваемый пользователь.

Если при создании пользователя не указываются дополнительные ключи, то берутся настройки по умолчанию. Эти настройки вы можете посмотреть выполнив useradd -D. Если вас не устраивают такие настройки, вы можете поменять их выполнив sudo useradd -D -s /bin/bash, где -s это ключ.

Изменение параметров пользователя происходит с помощью утилиты usermod. Изменить пароль пользователю можно при помощи утилиты passwd. У неё также есть ключи, например:

-d: Удалить пароль пользователю. После этого пароль будет пустым, и пользователь сможет входить в систему без предъявления пароля.

-e: Сделать пароль устаревшим. Это заставит пользователя изменить пароль при следующем входе в систему.

-l: Заблокировать учетную запись пользователя.

-u: Разблокировать учетную запись пользователя.

**Получение информации о пользователях**

* w – вывод информации (имя пользователя, рабочий терминал, время входа в систему, информацию о потребленных ресурсах CPU и имя запущенной программы) о всех вошедших в систему пользователях.
* who – вывод информации (имя пользователя, рабочий терминал, время входа в систему) о всех вошедших в систему пользователях.
* who am i или whoami или id – вывод вашего имени пользователя.
* users – вывод имен пользователей, работающих в системе.
* id имя\_пользователя – вывод о идентификаторах пользователя: его uid, имя\_пользователя, gid и имя первичной группы и список групп в которых состоит пользователь
* groups имя\_пользователя – вывод списка групп в которых состоит пользователь.

Программа groupadd создаёт новую группу согласно указанным значениям командной строки и системным значениям по умолчанию. Пример использования: sudo groupadd testgroup.

Изменять параметры пользователей и групп можно не только при помощи специальных утилит, но и вручную. Все настройки хранятся в текстовых файлах. В */etc/group*, как очевидно из названия хранится информация о группах.

Более подробно о работе см. в [[2]](bib/cite.bib).

## 5.2 Основы работы с уровнями доступа в ОС Linux

**Права доступа определяют**, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами.

Есть 3 вида разрешений. Они определяют права пользователя на 3 действия: чтение, запись и выполнение. В Linux эти действия обозначаются вот так:

* r — read (чтение) — право просматривать содержимое файла;
* w — write (запись) — право изменять содержимое файла;
* x — execute (выполнение) — право запускать файл, если это программа или скрипт.

У каждого файла есть 3 группы пользователей, для которых можно устанавливать права доступа.

* owner (владелец) — отдельный человек, который владеет файлом. Обычно это тот, кто создал файл, но владельцем можно сделать и кого-то другого.
* group (группа) — пользователи с общими заданными правами.
* others (другие) — все остальные пользователи, не относящиеся к группе и не являющиеся владельцами.

Чтобы посмотреть права доступа к файлу, нужно вызвать команду ls с опцией -l. Эта опция отвечает за вывода списка в длинном формате.

В выводе первые 10 символов вывода показывают разрешения файла.

* Первый символ определяет тип файла. Если первый символ — прочерк -, то это обычный файл. Если первый символ d, то это каталог.
* Следующие 3 символа показывают разрешения для владельца. Буква означает наличие разрешения, а прочерк - — его отсутствие. В нашем примере у владельца есть все разрешения (чтение, запись и выполнение).
* Следующие 3 символа показывают разрешения для группы. В этом примере у членов группы есть разрешение на чтение, но нет разрешений на запись и выполнение. Обратите внимание, порядок записи разрешений всегда такой: чтение, запись, выполнение.
* Последние 3 символа показывают разрешения для всех остальных пользователей. В этом примере у них есть только разрешение на выполнение.

Для изменения прав доступа к файлу или каталога используется команда chmod (от англ. change mode). Эта команда меняет биты режима файла — если совсем просто, это индикатор разрешений.

Аргументы команды chmod, отвечающие за разрешение, состоят из 3 компонентов:

* Для кого мы меняем разрешение? Обозначается первыми буквами слов: user (пользователь, он же владелец), group (группа), others (другие), all (все).
* Мы предоставляем или отзываем разрешения? Обозначается плюсом +, если предоставляем, минусом -, если отзываем.
* Какое разрешение мы хотим изменить? Чтение (r), запись (w), выполнение (x).

Для разрешений можно установить сокращенные формы записи. С их помощью выдавать разрешения будет быстрее. Сокращения полезны, когда нужно регулярно применять набор разрешений для определенных файлов. Запись сокращений основана на двоичной системе счисления переводимой в восьмеричную. Каждый из параметров r, w, x может как отсутствовать, так и присутствовать, что записывается с помощью 0 или 1. полученный результат переводится в число от 0 до 7 и обозначает права соответствующей группы пользователей, таким образом вместо записи 9 символов r, w, x записываются три цифры от 0 до 7.

Для каталогов можно устанавливать те же права доступа, разница в выводе в наличии или отсутствии на месте первого символа d.

Более подробно о работе см. в [[3]](bib/cite.bib).

# 6 Техническое оснащение и выбранные методы проведения работы

**Техническое оснащение**

* Ноутбук
* CentOS
* Интернет

**Методы проведения работы**

* Изучение методической информации
* Выполнение заданий в соответствии с указаниями
* Анализ результатов
* Обобщение полученных результатов в табличном виде
* Обобщение проведённой деятельности

1. Сравните полученную информацию с содержимым файла */etc/group*. Просмотрите файл командой cat /etc/group.
2. От имени пользователя guest2 выполните регистрацию пользователя guest2 в группе guest командой newgrp guest.
3. От имени пользователя guest измените права директории */home/guest*, разрешив все действия для пользователей группы: chmod g+rwx /home/guest.
4. От имени пользователя guest снимите с директории */home/guest/dir1* все атрибуты командой chmod 000 dirl и проверьте правильность снятия атрибутов.
5. Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполните табл. **“Установленные права и разрешённые действия для групп”**, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-». Сравните полученную таблицу с таблицей из лабораторной работы № 2.
6. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполните табл. **“Минимальные права для совершения операций от имени пользователей входящих в группу”**.

# 7 Выполнение лабораторной работы и полученные результаты

1. Скачала и ознакомилась с методическими указаниями к лабораторной работе (рис. ??).

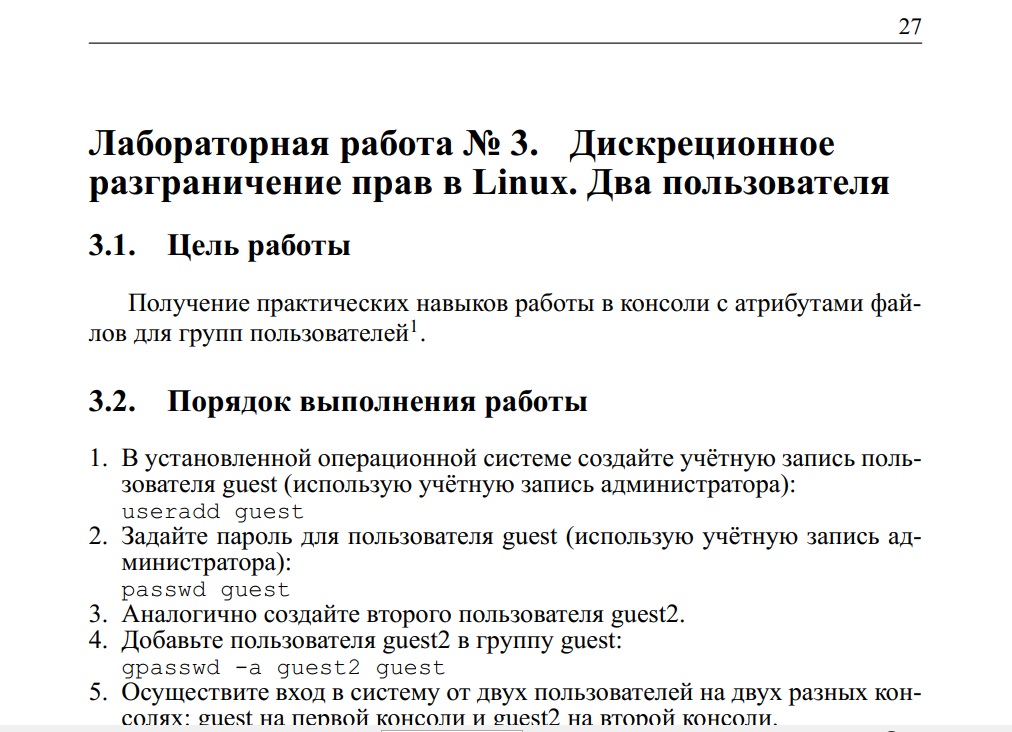


Рис. 1 Лабораторная работа 3

1. Выполнила следующие пункты задания: (рис. ??)

* cоздала второго пользователя guest2 и задала ему пароль.
* добавила пользователя guest2 в группу guest: gpasswd -a guest2 guest.

*Пункты про создание первого пользователя не выполняла, так как они были выполнены в предыдущей работе.*

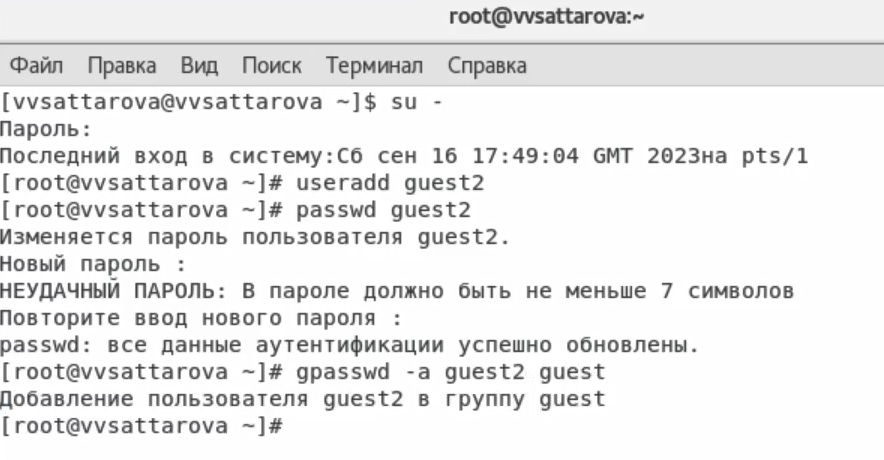


Рис. 2 Создание нового пользователя

1. Выполнила следующие пункты задания: (рис. ??)

* осуществила вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли.
* для обоих пользователей командой pwd определила директорию, в которой нахожусь: */home/vvsattarova*, сравнила её с приглашениями командной строки: они совпадают.
* уточнила имя вашего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам, определила командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2, сравнила вывод команды groups с выводом команд id -Gn и id -G.

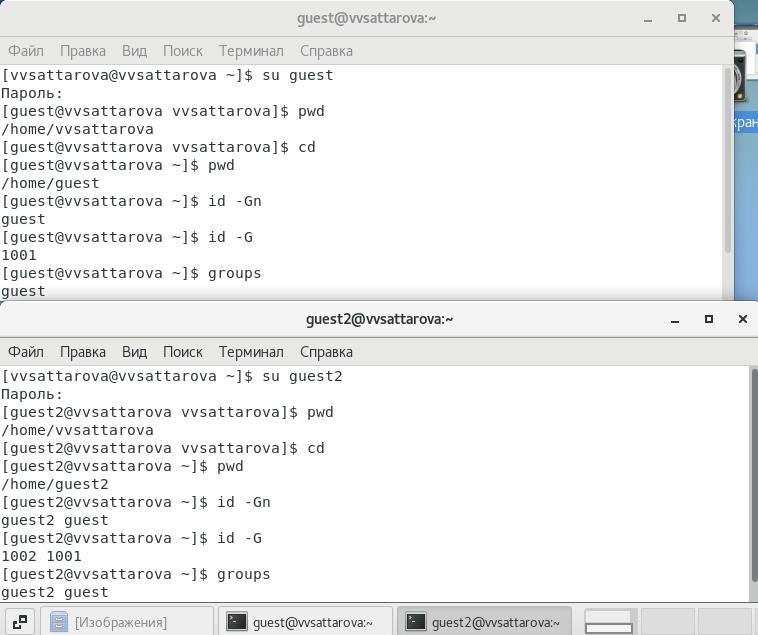


Рис. 3 Определение директории и параметров пользователей

1. Выполнила следующие пункты задания: (рис. ??)

* сравнила полученную информацию с содержимым файла */etc/group*, просмотрев файл командой cat /etc/group.
* от имени пользователя guest2 выполнила регистрацию пользователя guest2 в группе guest командой newgrp guest.

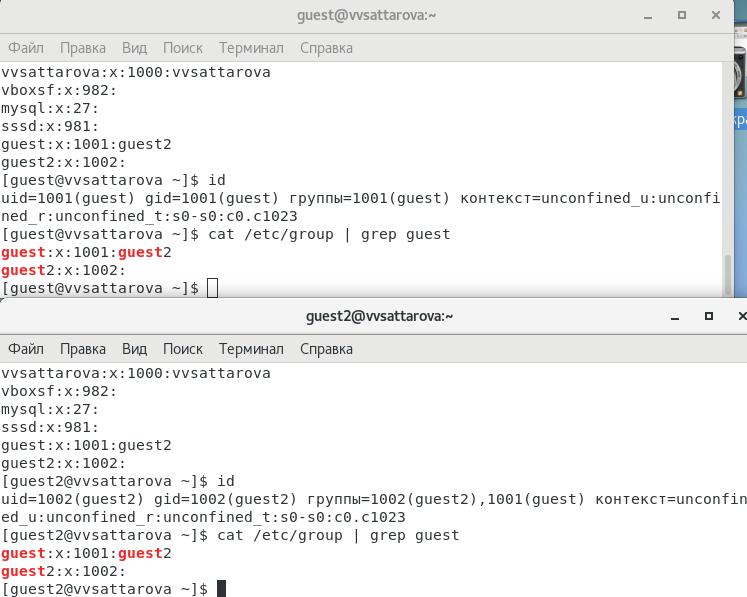


Рис. 4 Пользователь, его группа и регистрация в группе

1. Выполнила следующие пункты задания: (рис. ??)

* от имени пользователя guest изменила права директории */home/guest*, разрешив все действия для пользователей группы: chmod g+rwx /home/guest.

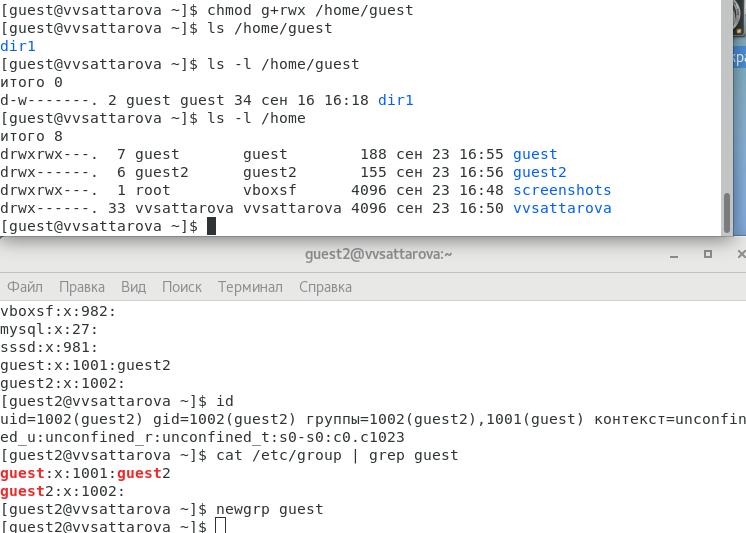


Рис. 5 Изменение прав директории

1. Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполнила табл. **“Установленные права и разрешённые действия для групп”**, определив опытным путём, какие операции разрешены, а какие нет. Сравнила полученную таблицу с таблицей из лабораторной работы № 2: таблицы очень похожи, однако в этой таблице есть дополнительный пункт про просмотр файлов, также важно, что пользователь группы не может менять права доступа к файлу.

(рис. ??) (рис. ??) (рис. ??) (рис. ??) (рис. ??) (рис. ??) (рис. ??) (рис. ??) (рис. ??) (Таблица [1](#tbl:001))

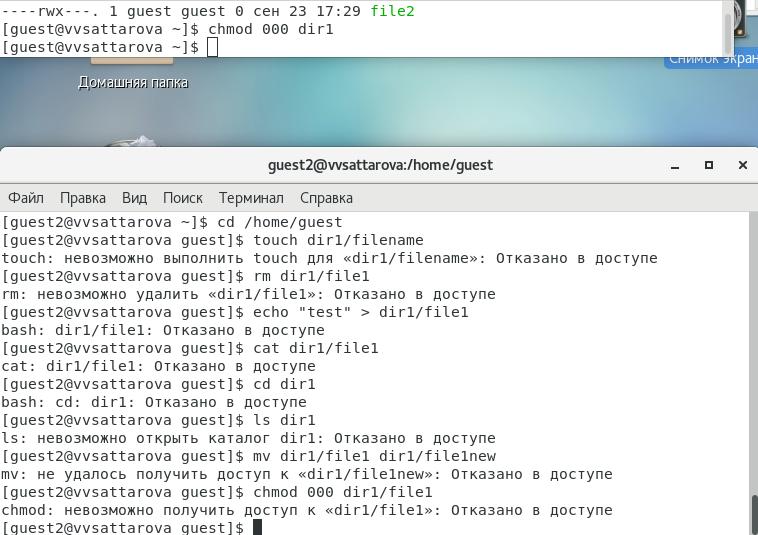


Рис. 7 Возможность выполнения действий для атрибутов 000

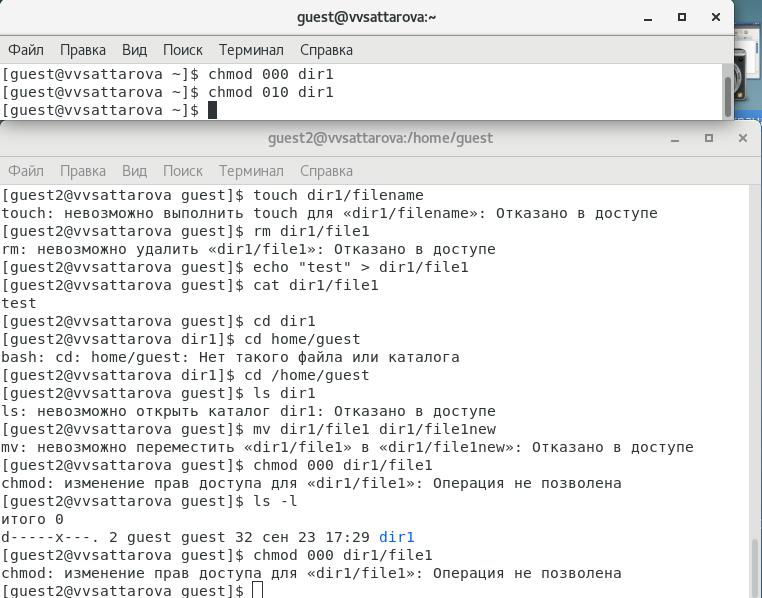


Рис. 8 Возможность выполнения действий для атрибутов 010

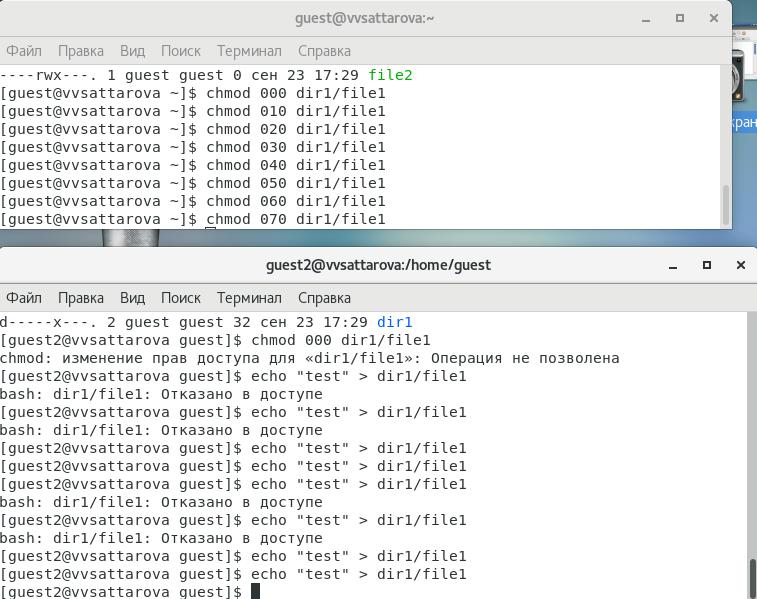


Рис. 9 Чтение текста из файла при различных атрибутах

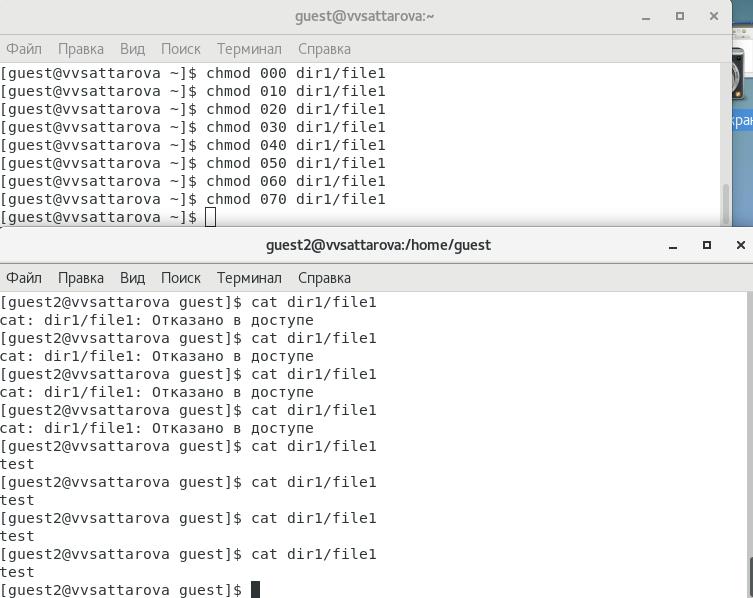


Рис. 10 Запись текста в файл при различных атрибутах

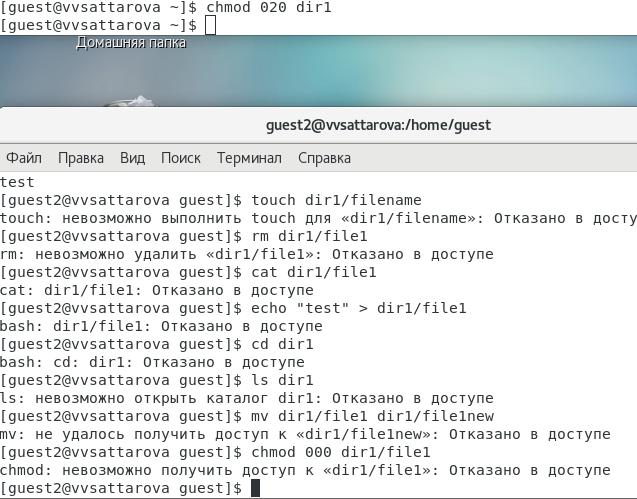


Рис. 11 Возможность выполнения действий для атрибутов 020

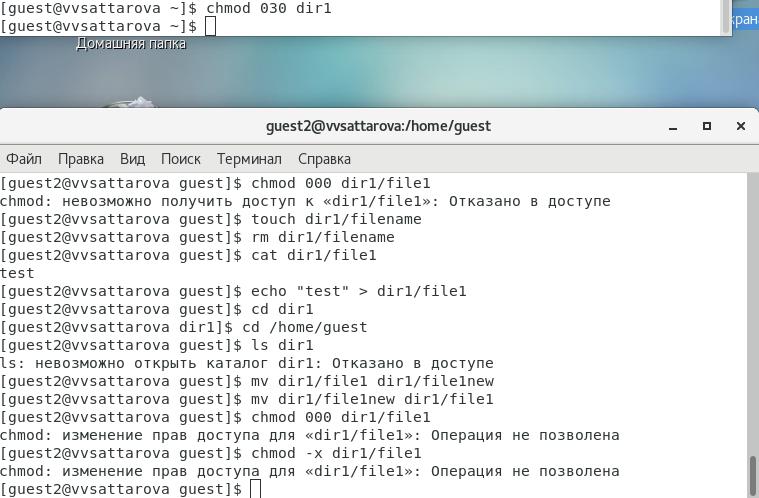


Рис. 12 Возможность выполнения действий для атрибутов 030

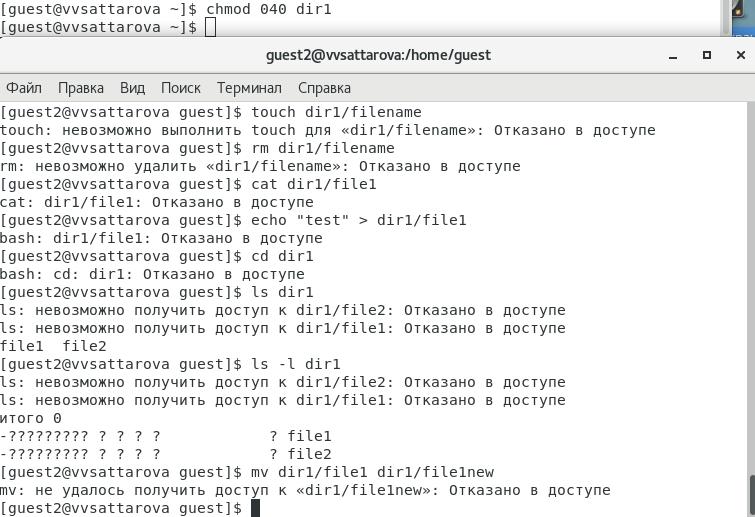


Рис. 13 Возможность выполнения действий для атрибутов 040

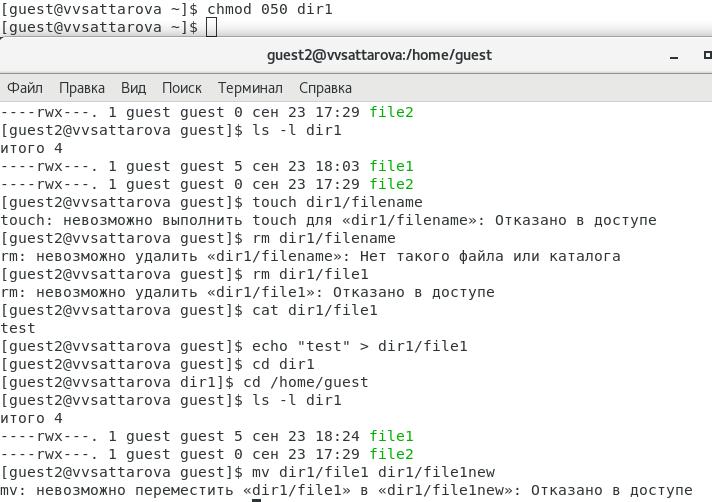


Рис. 14 Возможность выполнения действий для атрибутов 050

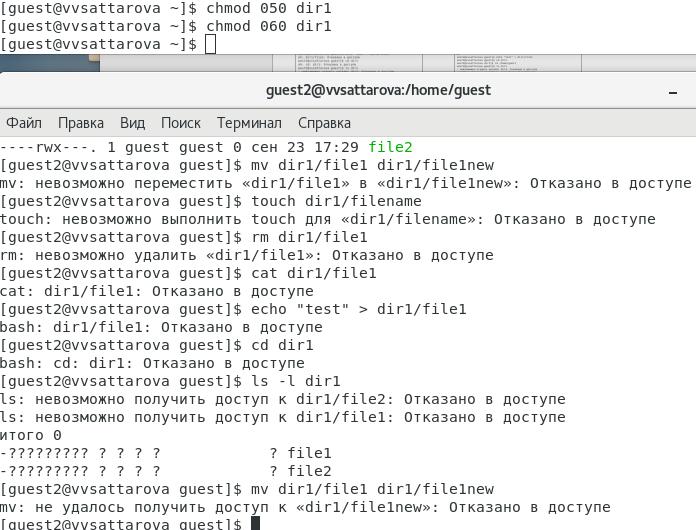


Рис. 15 Возможность выполнения действий для атрибутов 060

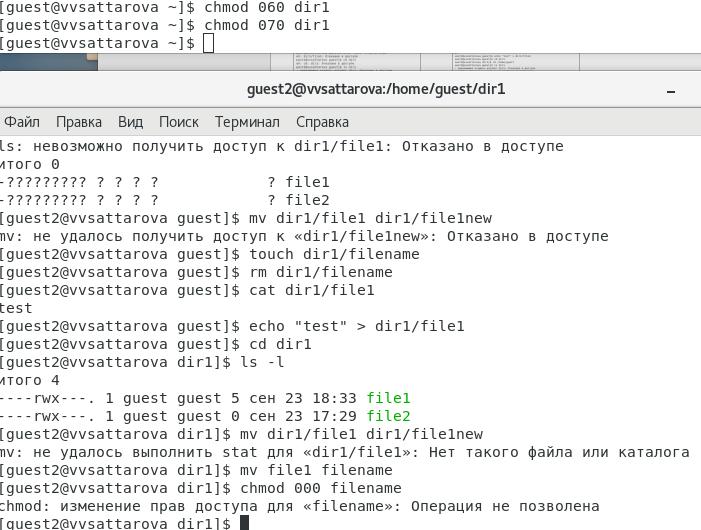


Рис. 16 Возможность выполнения действий для атрибутов 070

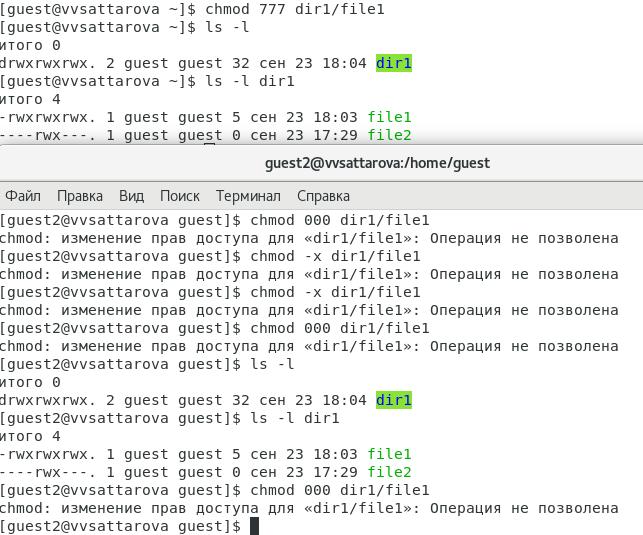


Рис. 17 Невозможность изменения атрибутов файла при любых атрибутах директории

Table 1: Установленные права и разрешённые действия для групп

| Права директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение файла | Смена директории | Просмотр файлов | Переименование файла | Смена атрибутов файла |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| d— (000) | (000) | - | - | - | - | - | - | - | - |
| d— (000) | (010) | - | - | - | - | - | - | - | - |
| d— (000) | (020) | - | - | - | - | - | - | - | - |
| d— (000) | (030) | - | - | - | - | - | - | - | - |
| d— (000) | (040) | - | - | - | - | - | - | - | - |
| d— (000) | (050) | - | - | - | - | - | - | - | - |
| d— (000) | (060) | - | - | - | - | - | - | - | - |
| d— (000) | (070) | - | - | - | - | - | - | - | - |
| d–x (010) | (000) | - | - | - | - | + | - | - | - |
| d–x (010) | (010) | - | - | - | - | + | - | - | - |
| d–x (010) | (020) | - | - | + | - | + | - | - | - |
| d–x (010) | (030) | - | - | + | - | + | - | - | - |
| d–x (010) | (040) | - | - | - | + | + | - | - | - |
| d–x (010) | (050) | - | - | - | + | + | - | - | - |
| d–x (010) | (060) | - | - | + | + | + | - | - | - |
| d–x (010) | (070) | - | - | + | + | + | - | - | - |
| d-w- (020) | (000) | - | - | - | - | - | - | - | - |
| d-w- (020) | (010) | - | - | - | - | - | - | - | - |
| d-w- (020) | (020) | - | - | - | - | - | - | - | - |
| d-w- (020) | (030) | - | - | - | - | - | - | - | - |
| d-w- (020) | (040) | - | - | - | - | - | - | - | - |
| d-w- (020) | (050) | - | - | - | - | - | - | - | - |
| d-w- (020) | (060) | - | - | - | - | - | - | - | - |
| d-w- (020) | (070) | - | - | - | - | - | - | - | - |
| d-wx (030) | (000) | + | + | - | - | + | - | + | - |
| d-wx (030) | (010) | + | + | - | - | + | - | + | - |
| d-wx (030) | (020) | + | + | + | - | + | - | + | - |
| d-wx (030) | (030) | + | + | + | - | + | - | + | - |
| d-wx (030) | (040) | + | + | - | + | + | - | + | - |
| d-wx (030) | (050) | + | + | - | + | + | - | + | - |
| d-wx (030) | (060) | + | + | + | + | + | - | + | - |
| d-wx (030) | (070) | + | + | + | + | + | - | + | - |
| dr– (040) | (000) | - | - | - | - | - | + | - | - |
| dr– (040) | (010) | - | - | - | - | - | + | - | - |
| dr– (040) | (020) | - | - | - | - | - | + | - | - |
| dr– (040) | (030) | - | - | - | - | - | + | - | - |
| dr– (040) | (040) | - | - | - | - | - | + | - | - |
| dr– (040) | (050) | - | - | - | - | - | + | - | - |
| dr– (040) | (060) | - | - | - | - | - | + | - | - |
| dr– (040) | (070) | - | - | - | - | - | + | - | - |
| dr-x (050) | (000) | - | - | - | - | + | + | - | - |
| dr-x (050) | (010) | - | - | - | - | + | + | - | - |
| dr-x (050) | (020) | - | - | + | - | + | + | - | - |
| dr-x (050) | (030) | - | - | + | - | + | + | - | - |
| dr-x (050) | (040) | - | - | - | + | + | + | - | - |
| dr-x (050) | (050) | - | - | - | + | + | + | - | - |
| dr-x (050) | (060) | - | - | + | + | + | + | - | - |
| dr-x (050) | (070) | - | - | + | + | + | + | - | - |
| drw- (060) | (000) | - | - | - | - | - | + | - | - |
| drw- (060) | (010) | - | - | - | - | - | + | - | - |
| drw- (060) | (020) | - | - | - | - | - | + | - | - |
| drw- (060) | (030) | - | - | - | - | - | + | - | - |
| drw- (060) | (040) | - | - | - | - | - | + | - | - |
| drw- (060) | (050) | - | - | - | - | - | + | - | - |
| drw- (060) | (060) | - | - | - | - | - | + | - | - |
| drw- (060) | (070) | - | - | - | - | - | + | - | - |
| drwx (070) | (000) | + | + | - | - | + | + | + | - |
| drwx (070) | (010) | + | + | - | - | + | + | + | - |
| drwx (070) | (020) | + | + | + | - | + | + | + | - |
| drwx (070) | (030) | + | + | + | - | + | + | + | - |
| drwx (070) | (040) | + | + | - | + | + | + | + | - |
| drwx (070) | (050) | + | + | - | + | + | + | + | - |
| drwx (070) | (060) | + | + | + | + | + | + | + | - |
| drwx (070) | (070) | + | + | + | + | + | + | + | - |

1. На основании заполненной таблицы и дополнительных проверок определила те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполнила таблицу **“Минимальные права для совершения операций от имени пользователей входящих в группу”**. (рис. ??) (Таблица [2](#tbl:002))

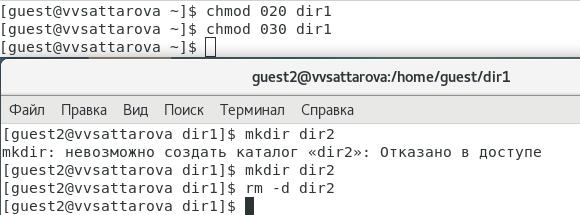


Рис. 18 Исследование возможности создания и удаления поддиректории при различных атрибутах

Table 2: Минимальные права для совершения операций от имени пользователей входящих в группу

| Операция | Минимальные права на директорию | Минимальные права на файл |
| --- | --- | --- |
| Создание файла | d-wx (030) | — (000) |
| Удаление файла | d-wx (030) | — (000) |
| Чтение файла | d–x (010) | r– (040) |
| Запись в файл | d–x (010) | -w- (020) |
| Переименование файла | d-wx (030) | — (000) |
| Создание поддиректории | d-wx (030) | — (000) |
| Удаление поддиректории | d-wx (030) | — (000) |

# 8 Анализ результатов

Полученные таблицы помогают лучше понять, при каких атрибутах какие действия можно выполнять пользователям из одной группы.

# 9 Заключение и выводы

Таким образом, в ходе выполнения лабораторной работы было сделано следующее:

* Созданы два пользователя в одной группе, вспомнены теоретические основы работы с пользователями в Linux.
* Вспомнены теоретические основы атрибутов файлов и директорий в ОС Linux;
* Созданы две таблицы: “Установленные права и разрешённые действия дл групп” и “Минимальные права для совершения операций от имени пользователей входящих в группу”.
* Был проведён анализ, за что отвечают разные атрибуты доступа.
* Написан отчёт с ответами на вопросы, заданные в пунктах для выполнения в методических рекомендациях к лабораторной работе.

# 10 Список литературы

[[1]](bib/cite.bib)

[[2]](bib/cite.bib)

[[3]](bib/cite.bib)

1. Информационная безопасность [Электронный ресурс]. Российский университет дружбы народов, 2023. URL: <https://esystem.rudn.ru/pluginfile.php/2090275/mod_resource/content/4/003-lab_discret_2users.pdf>.

2. Права доступа в Linux [Электронный ресурс]. 2023. URL: <https://help.ubuntu.ru/wiki/пользователи_и_группы>.

3. Права доступа в Linux [Электронный ресурс]. 2023. URL: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>.