Отчет по лабораторной работе №3

Основы информационной безопасности

Ганина Таисия Сергеевна, НКАбд-01-22

Содержание

# 1 Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

# 2 Задание

1. Создать еще одного пользователя.
2. Провести работу с группами пользователей.

# 3 Теоретическое введение

**Права доступа** определяют, какие действия конкретный пользователь может или не может совершать с определенным 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]

**Группы пользователей Linux** кроме стандартных root и users, здесь есть еще пару десятков групп. Это группы, созданные программами, для управления доступом этих программ к общим ресурсам. Каждая группа разрешает чтение или запись определенного файла или каталога системы, тем самым регулируя полномочия пользователя, а следовательно, и процесса, запущенного от этого пользователя. Здесь можно считать, что пользователь - это одно и то же что процесс, потому что у процесса все полномочия пользователя, от которого он запущен. [2]

* daemon - от имени этой группы и пользователя daemon запускаютcя сервисы, которым необходима возможность записи файлов на диск.
* sys - группа открывает доступ к исходникам ядра и файлам - include сохраненным в системе
* sync - позволяет выполнять команду /bin/sync
* games - разрешает играм записывать свои файлы настроек и историю в определенную папку
* man - позволяет добавлять страницы в директорию /var/cache/man
* lp - позволяет использовать устройства параллельных портов
* mail - позволяет записывать данные в почтовые ящики /var/mail/
* proxy - используется прокси серверами, нет доступа записи файлов на диск
* www-data - с этой группой запускается веб-сервер, она дает доступ на запись /var/www, где находятся файлы веб-документов
* list - позволяет просматривать сообщения в /var/mail
* nogroup - используется для процессов, которые не могут создавать файлов на жестком диске, а только читать, обычно применяется вместе с пользователем nobody.
* adm - позволяет читать логи из директории /var/log
* tty - все устройства /dev/vca разрешают доступ на чтение и запись пользователям из этой группы
* disk - открывает доступ к жестким дискам /dev/sd\* /dev/hd\*, можно сказать, что это аналог рут доступа.
* dialout - полный доступ к серийному порту
* cdrom - доступ к CD-ROM
* wheel - позволяет запускать утилиту sudo для повышения привилегий
* audio - управление аудиодрайвером
* src - полный доступ к исходникам в каталоге /usr/src/
* shadow - разрешает чтение файла /etc/shadow
* utmp - разрешает запись в файлы /var/log/utmp /var/log/wtmp
* video - позволяет работать с видеодрайвером
* plugdev - позволяет монтировать внешние устройства USB, CD и т д
* staff - разрешает запись в папку /usr/local

# 4 Выполнение лабораторной работы

1. Создаю еще одного пользователя. Первый пользователь “guest” был создан в прошлой работе, создаю “guest2”, устанавливаю пароль, добавляю его в группу “guest” (рис. [1](#fig:001)).

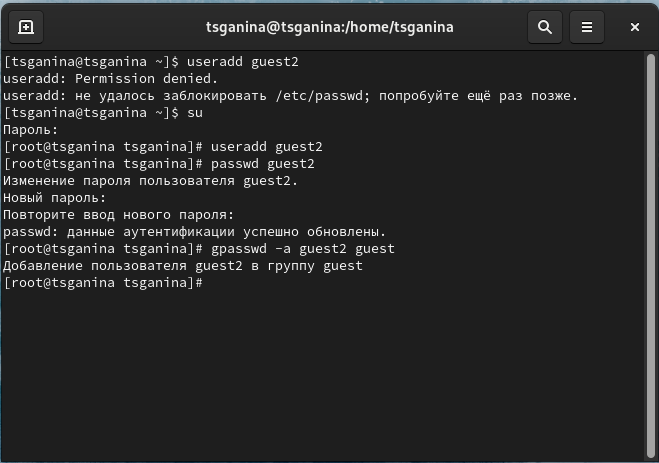


Figure 1: Еще один пользователь

1. Вхожу в систему от двух пользователей на двух разных консолях. Уточнаяю имя пользователя, его группу (рис. [2](#fig:002), [3](#fig:003), [4](#fig:004)).

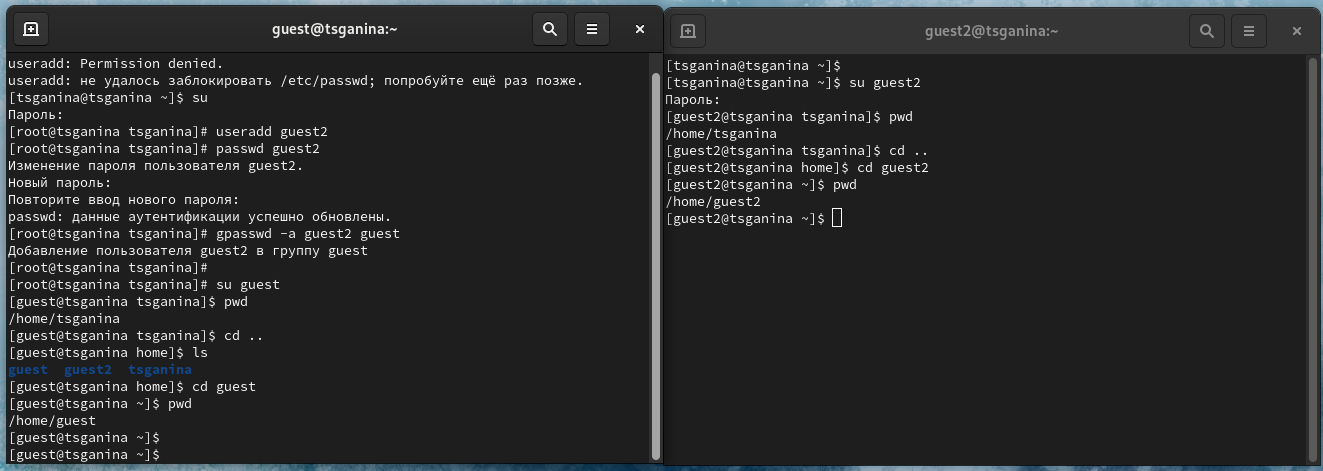


Figure 2: Работа с двумя пользователями

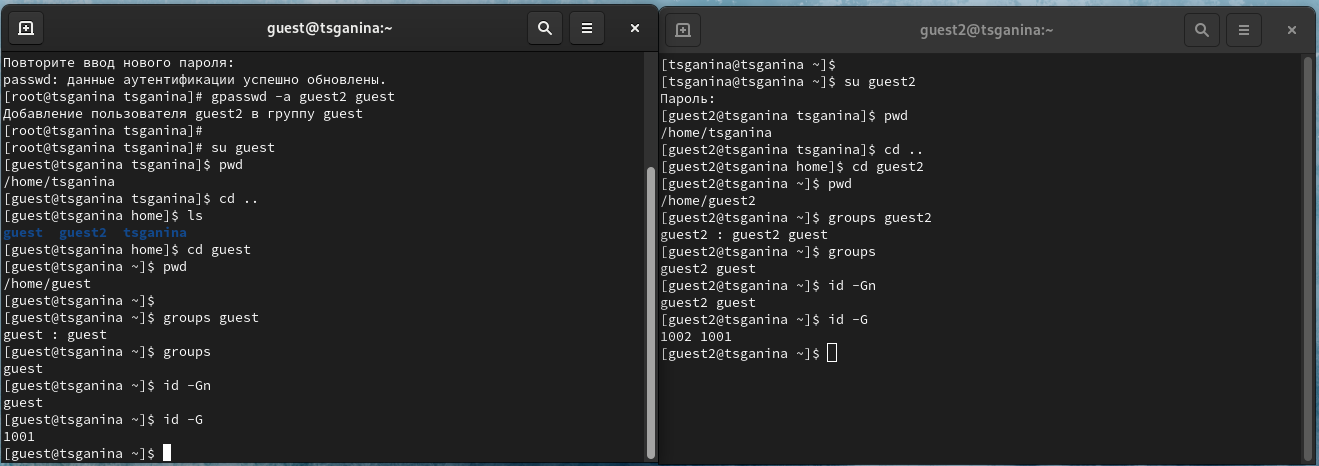


Figure 3: Работа с двумя пользователями

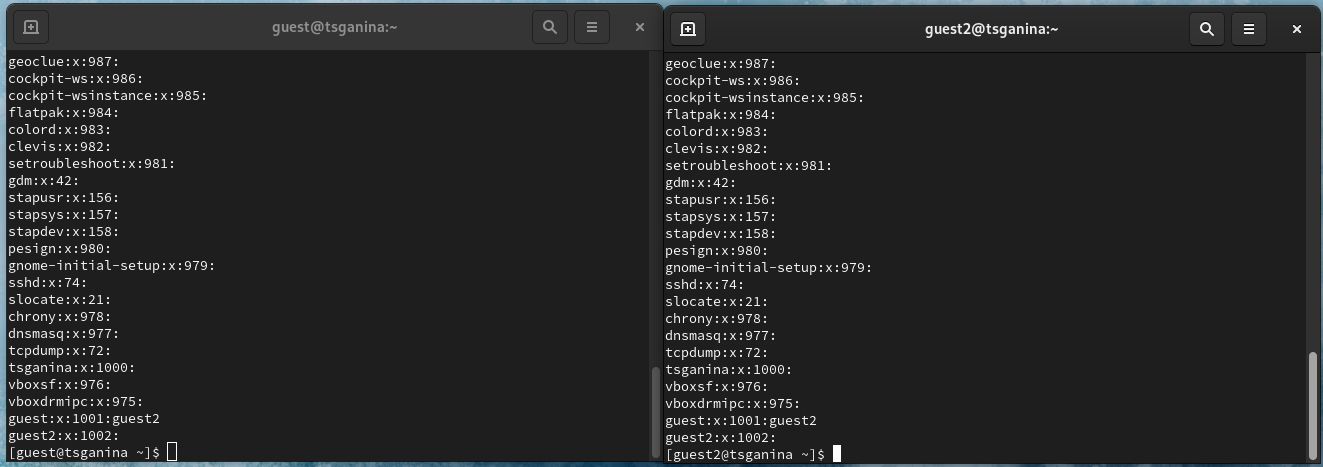


Figure 4: Работа с двумя пользователями

1. От имени пользователя guest2 выполняю регистрацию пользователя guest2 в группе guest. От имени пользователя guest меняю права директории, разрешая все действия для пользователей группы. От имени пользователя guest снимаю с директории dir1 все атрибуты (рис. [5](#fig:005), [6](#fig:006), [7](#fig:007)).

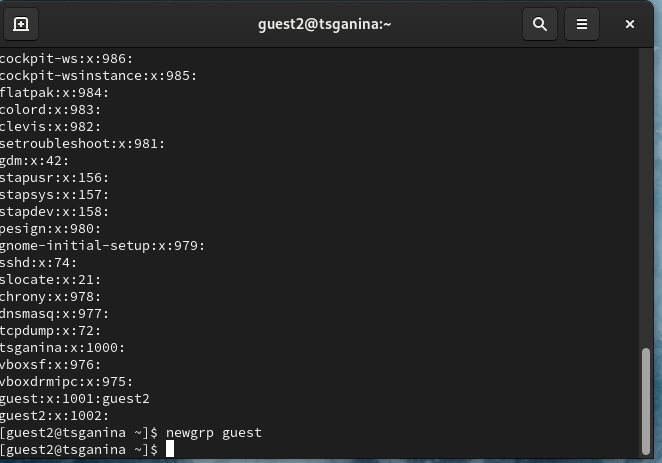


Figure 5: Регистрация в группе

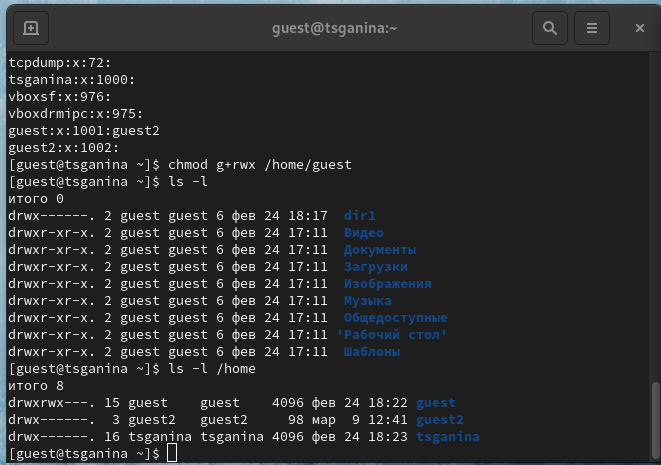


Figure 6: Меняю права директории

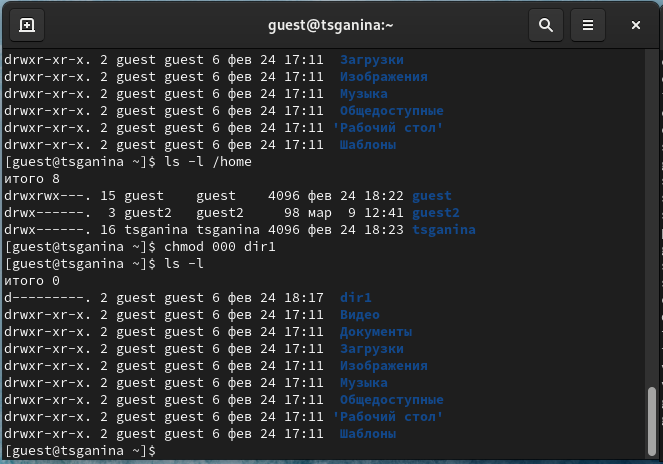


Figure 7: Снимаю атрибуты

1. Опытным путем определяю, какие операции разрешены, а какие нет (рис. [8](#fig:008), [9](#fig:009)).

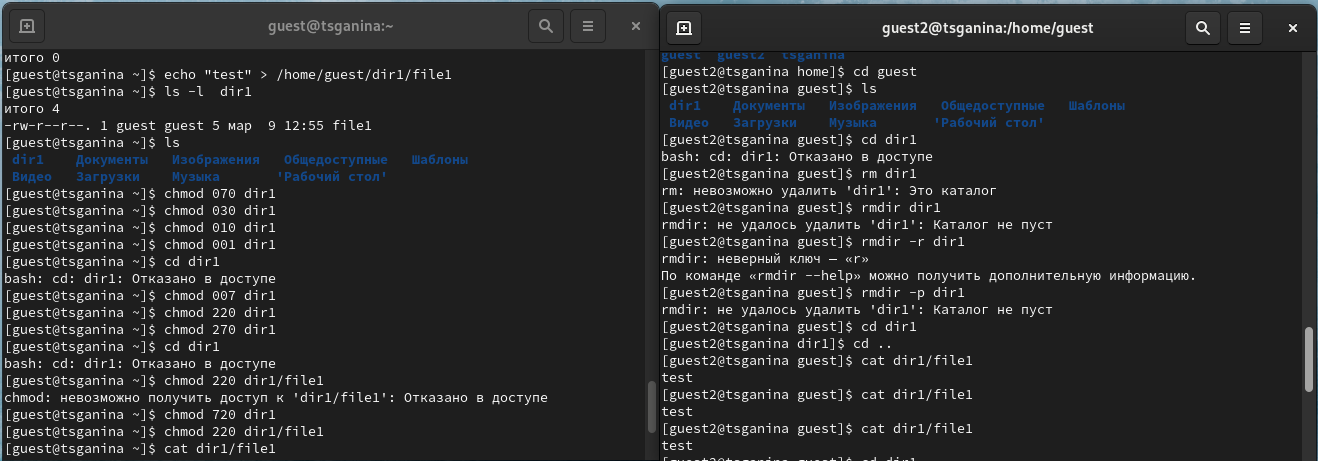


Figure 8: Опыты 1

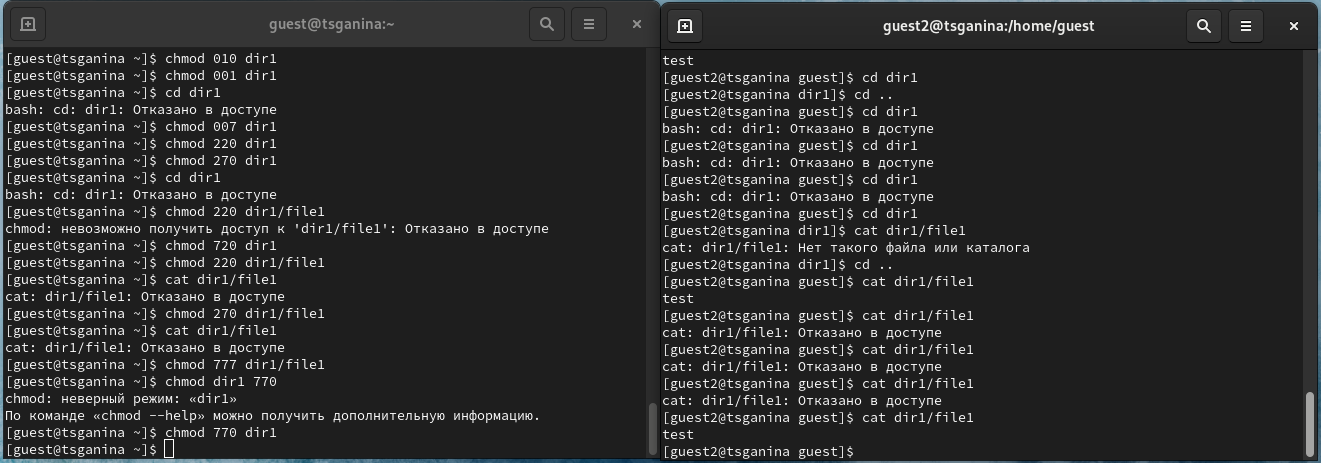


Figure 9: Опыты 2

## 4.1 Заполнение таблицы 3.1

1. Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполните табл. 3.1, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-». Сравните табл. 2.1 (из лабораторной работы № 2) и табл. 3.1.

| Права директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение файла | Смена директории | Просмотр файлов в директории | Переименование файл | Смена атрибутов файла |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| d--------- (000) | ---------- (000) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ---------- (000) | - | - | - | - | + | - | - | + |
| d----w---- (020) | ---------- (000) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ---------- (000) | + | + | - | - | + | - | + | + |
| d---r----- (040) | ---------- (000) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ---------- (000) | - | - | - | - | + | + | - | + |
| d---rw---- (060) | ---------- (000) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ---------- (000) | + | + | - | - | + | + | + | + |
| d--------- (000) | ------x--- (010) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ------x--- (010) | - | - | - | - | + | - | - | + |
| d----w---- (020) | ------x--- (010) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ------x--- (010) | + | + | - | - | + | - | + | + |
| d---r----- (040) | ------x--- (010) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ------x--- (010) | - | - | - | - | + | + | - | + |
| d---rw---- (060) | ------x--- (010) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ------x--- (010) | + | + | - | - | + | + | + | + |
| d--------- (000) | -----w---- (020) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | -----w---- (020) | - | - | + | - | + | - | - | + |
| d----w---- (020) | -----w---- (020) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | -----w---- (020) | + | + | + | - | + | - | + | + |
| d---r----- (040) | -----w---- (020) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | -----w---- (020) | - | - | + | - | + | + | - | + |
| d---rw---- (060) | -----w---- (020) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | -----w---- (020) | + | + | + | - | + | + | + | + |
| d--------- (000) | -----wx--- (030) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | -----wx--- (030) | - | - | + | - | + | - | - | + |
| d----w---- (020) | -----wx--- (030) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | -----wx--- (030) | + | + | + | - | + | - | + | + |
| d---r----- (040) | -----wx--- (030) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | -----wx--- (030) | - | - | + | - | + | + | - | + |
| d---rw---- (060) | -----wx--- (030) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | -----wx--- (030) | + | + | + | - | + | + | + | + |
| d--------- (000) | ----r----- (040) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ----r----- (040) | - | - | - | + | + | - | - | + |
| d----w---- (020) | ----r----- (040) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ----r----- (040) | + | + | - | + | + | - | + | + |
| d---r----- (040) | ----r----- (040) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ----r----- (040) | - | - | - | + | + | + | - | + |
| d---rw---- (060) | ----r----- (040) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ----r----- (040) | + | + | - | + | + | + | + | + |
| d--------- (000) | ----r-x--- (050) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ----r-x--- (050) | - | - | - | + | + | - | - | + |
| d----w---- (020) | ----r-x--- (050) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ----r-x--- (050) | + | + | - | + | + | - | + | + |
| d---r----- (040) | ----r-x--- (050) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ----r-x--- (050) | - | - | - | + | + | + | - | + |
| d---rw---- (060) | ----r-x--- (050) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ----r-x--- (050) | + | + | - | + | + | + | + | + |
| d--------- (000) | ----rw---- (060) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ----rw---- (060) | - | - | + | + | + | - | - | + |
| d----w---- (020) | ----rw---- (060) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ----rw---- (060) | + | + | + | + | + | - | + | + |
| d---r----- (040) | ----rw---- (060) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ----rw---- (060) | - | - | + | + | + | + | - | + |
| d---rw---- (060) | ----rw---- (060) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ----rw---- (060) | + | + | + | + | + | + | + | + |
| d--------- (000) | ----rwx--- (070) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ----rwx--- (070) | - | - | + | + | + | - | - | + |
| d----w---- (020) | ----rwx--- (070) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ----rwx--- (070) | + | + | + | + | + | - | + | + |
| d---r----- (040) | ----rwx--- (070) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ----rwx--- (070) | - | - | + | + | + | + | - | + |
| d---rw---- (060) | ----rwx--- (070) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ----rwx--- (070) | + | + | + | + | + | + | + | + |

Таблица 3.1 «Установленные права и разрешённые действия для групп»

## 4.2 Заполнение таблицы 3.2

1. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполните табл. 3.2

| Операция | Права на директорию | 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) |

Таблица 3.2 «Минимальные права для совершения операций от имени пользователей входящих в группу»

Сравнивая таблицу 3.1. с таблицей 2.1, можно сказать, что они одинаковы. Единственное различие в том, что в предыдущий раз мы присваивали права владельцу, а в этот раз группе.

# 5 Выводы

Я получила практические навыки работы в консоли с атрибутами файлов для групп пользователей.

# Список литературы

[0] Методические материалы курса

[1] Права доступа: https://codechick.io/tutorials/unix-linux/unix-linux-permissions

[2] Группы пользователей: https://losst.pro/gruppy-polzovatelej-linux#%D0%A7%D1%82%D0%BE\_%D1%82%D0%B0%D0%BA%D0%BE%D0%B5\_%D0%B3%D1%80%D1%83%D0%BF%D0%BF%D1%8B