

# **Отчет по лабораторной работе №3**

**Основы информационной безопасности**

Малюга Валерия Васильевна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>9</b>
4.1	Заполнение таблицы 3.1 . . . . .	13
4.2	Заполнение таблицы 3.2 . . . . .	19
<b>5</b>	<b>Выводы</b>	<b>20</b>
<b>6</b>	<b>Список литературы. Библиография</b>	<b>21</b>

## Список иллюстраций

4.1	Создание пользователя . . . . .	9
4.2	Добавление пользователя в группу . . . . .	9
4.3	Вход в терминал от имени другого пользователя . . . . .	10
4.4	Текущая директория для guest . . . . .	10
4.5	Текущая директория для guest2 . . . . .	10
4.6	Информация о пользователе guest2 . . . . .	11
4.7	Информация о пользователе guest . . . . .	11
4.8	Содержимое файла etc/group . . . . .	12
4.9	Регистрация пользователя в группе . . . . .	12
4.10	Изменение прав директории . . . . .	12
4.11	Изменение прав директории . . . . .	13
4.12	Пример заполнения таблицы 3.1 . . . . .	13

## Список таблиц

# 1 Цель работы

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

## 2 Задание

1. Создание пользователя `guest2`, добавление его в группу пользователей `guest`
2. Заполнение таблицы 3.1
3. Заполнение таблицы 3.2 на основе таблицы 3.1.

### 3 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]

**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]

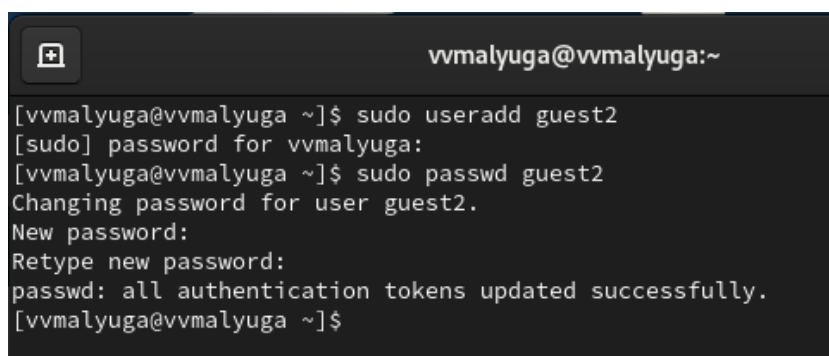
- daemon - от имени этой группы и пользователя daemon запускаются сервисы, которым необходима возможность записи файлов на диск.
- sys - группа открывает доступ к исходникам ядра и файлам - include сохраненным в системе
- sync - позволяет выполнять команду /bin/sync
- games - разрешает играм записывать 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/vcsa` 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 `root` 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

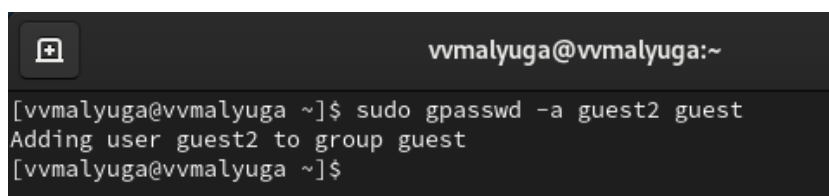
1. Пользователь guest был создан в лабораторной работе №2, поэтому в этой лабораторной работе его не создаем заново
2. Пароль для пользователя guest тоже был задан в лабораторной работе №2.
3. С правами администратора создаю пользователя guest с помощью команды `useradd`, далее с помощью команды `passwd` задаю пароль пользователю (рис. 1).

A terminal window with a dark background. The title bar shows a window icon and the text 'vvmalyuga@vvmalyuga:~'. The terminal content shows a user running 'sudo useradd guest2', followed by a password prompt for 'vvmalyuga:'. Then, the user runs 'sudo passwd guest2', which prompts for a new password and its retype, followed by the message 'passwd: all authentication tokens updated successfully.' and the prompt returns to the user.

```
vvmalyuga@vvmalyuga:~  
[vvmalyuga@vvmalyuga ~]$ sudo useradd guest2  
[sudo] password for vvmalyuga:  
[vvmalyuga@vvmalyuga ~]$ sudo passwd guest2  
Changing password for user guest2.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[vvmalyuga@vvmalyuga ~]$
```

Рис. 4.1: Создание пользователя

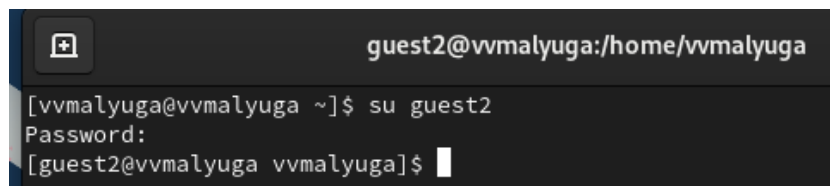
4. Добавляю пользователя guest2 в группу guest (рис. 2).

A terminal window with a dark background. The title bar shows a window icon and the text 'vvmalyuga@vvmalyuga:~'. The terminal content shows a user running 'sudo gpasswd -a guest2 guest', which results in the message 'Adding user guest2 to group guest' and the prompt returns to the user.

```
vvmalyuga@vvmalyuga:~  
[vvmalyuga@vvmalyuga ~]$ sudo gpasswd -a guest2 guest  
Adding user guest2 to group guest  
[vvmalyuga@vvmalyuga ~]$
```

Рис. 4.2: Добавление пользователя в группу

5. Зашла на двух разных консолях от имени двух разных пользователей с помощью команды `su <имя пользователя>` (рис. 3).

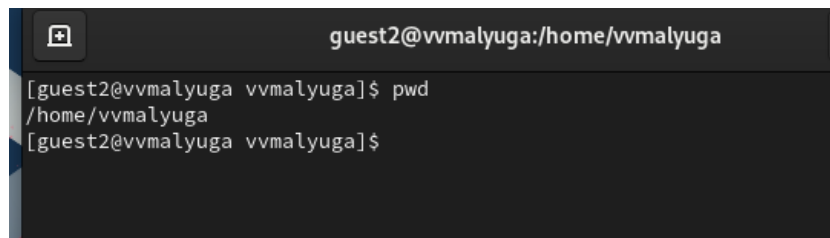


```
guest2@vvmalyuga:/home/vvmalyuga
[vvmalyuga@vvmalyuga ~]$ su guest2
Password:
[guest2@vvmalyuga vvmalyuga]$
```

Рис. 4.3: Вход в терминал от имени другого пользователя

6. Проверяю путь директории, в которой я нахожусь с помощью `pwd`.

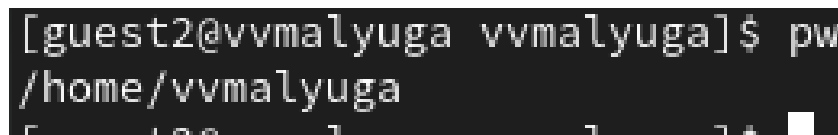
Проверка для пользователя `guest` (рис. 4).



```
guest2@vvmalyuga:/home/vvmalyuga
[guest2@vvmalyuga vvmalyuga]$ pwd
/home/vvmalyuga
[guest2@vvmalyuga vvmalyuga]$
```

Рис. 4.4: Текущая директория для `guest`

Проверка для пользователя `guest2` (рис. 5).



```
[guest2@vvmalyuga vvmalyuga]$ pwd
/home/vvmalyuga
[guest2@vvmalyuga vvmalyuga]$
```

Рис. 4.5: Текущая директория для `guest2`

Стоит отметить, что вход в терминал от имени пользователей был выполнен в домашней директории пользователя `evdvorkina`, которую команда `pwd` вывела. Домашней директорией пользователей она не является. Текущая директория с приглашением командной строки совпадает.

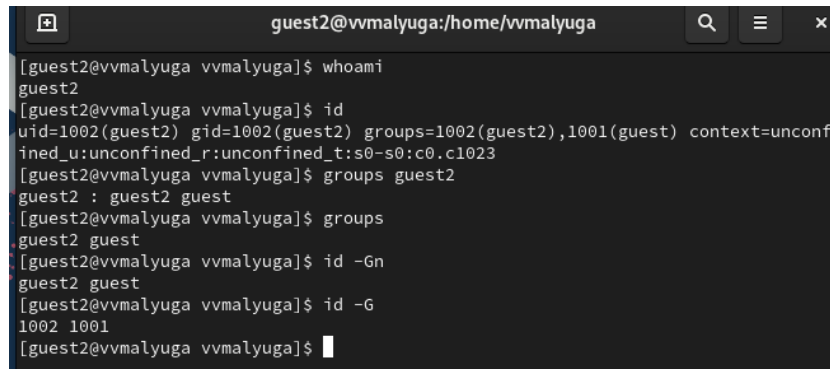
7. Проверяю имя пользователей с помощью команды `whoami`, с помощью команды `id` могу увидеть группы, к которым принадлежит пользователь

и коды этих групп (gid), команда `groups` просто выведет список групп, в которые входит пользователь.

`id -Gn` - выведет названия групп, которым принадлежит пользователь

`id -G` - выведет только код групп, которым принадлежит пользователь.

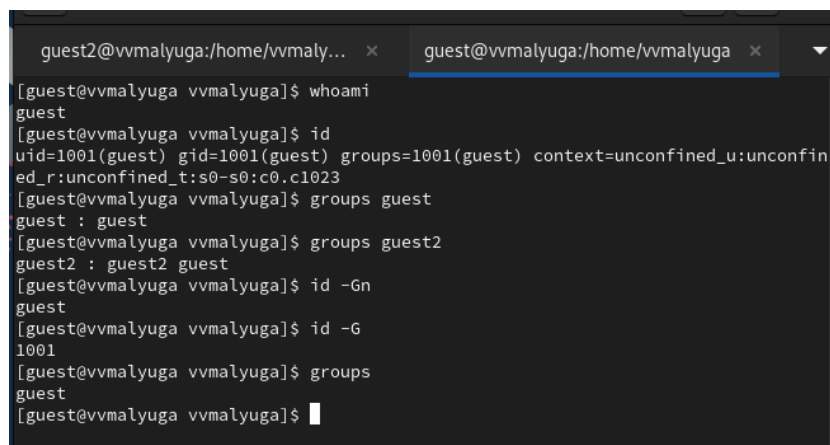
Проверка для пользователя `guest2` (рис. 6).



```
guest2@vmmalyuga:/home/vmmalyuga
[guest2@vmmalyuga vmmalyuga]$ whoami
guest2
[guest2@vmmalyuga vmmalyuga]$ id
uid=1002(guest2) gid=1002(guest2) groups=1002(guest2),1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@vmmalyuga vmmalyuga]$ groups guest2
guest2 : guest2 guest
[guest2@vmmalyuga vmmalyuga]$ groups
guest2 guest
[guest2@vmmalyuga vmmalyuga]$ id -Gn
guest2 guest
[guest2@vmmalyuga vmmalyuga]$ id -G
1002 1001
[guest2@vmmalyuga vmmalyuga]$
```

Рис. 4.6: Информация о пользователе `guest2`

Проверка для пользователя `guest` (рис. 7).

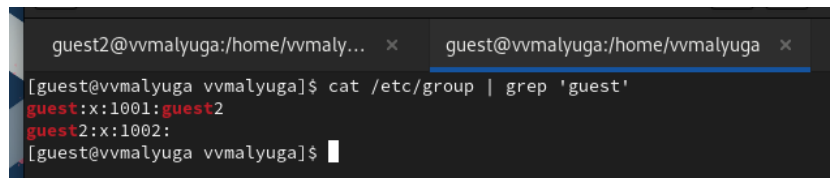


```
guest2@vmmalyuga:/home/vmmalyuga x guest@vmmalyuga:/home/vmmalyuga x
[guest@vmmalyuga vmmalyuga]$ whoami
guest
[guest@vmmalyuga vmmalyuga]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@vmmalyuga vmmalyuga]$ groups guest
guest : guest
[guest@vmmalyuga vmmalyuga]$ groups guest2
guest2 : guest2 guest
[guest@vmmalyuga vmmalyuga]$ id -Gn
guest
[guest@vmmalyuga vmmalyuga]$ id -G
1001
[guest@vmmalyuga vmmalyuga]$ groups
guest
[guest@vmmalyuga vmmalyuga]$
```

Рис. 4.7: Информация о пользователе `guest`

Пользователь `guest2` входит в две группы пользователей: в группу `guest`, потому что я сама его туда добавила, и в группу `guest2`, которая создавалась автоматически при создании пользователя.

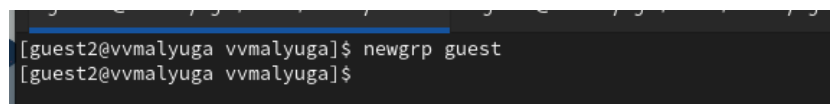
8. Вывела интересующее меня содержимое файла `etc/group`, видно, что в группе `guest` два пользователя, а в группе `guest2` один (рис. 8).



```
guest2@vmmalyuga:/home/vmmalyuga$ cat /etc/group | grep 'guest'
guest:x:1001:guest
guest2:x:1002:
[guest@vmmalyuga vmmalyuga]$
```

Рис. 4.8: Содержимое файла `etc/group`

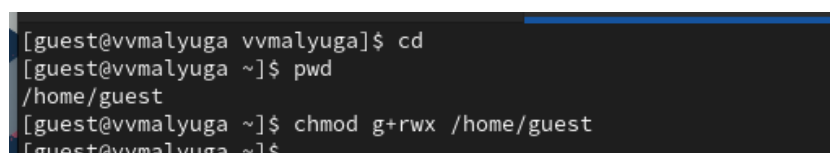
9. От имени пользователя `guest2` регистрирую его в группе `guest` с помощью команды `newgrp` (рис. 9).



```
[guest2@vmmalyuga vmmalyuga]$ newgrp guest
[guest@vmmalyuga vmmalyuga]$
```

Рис. 4.9: Регистрация пользователя в группе

10. Добавляю права на чтение, запись и исполнение группе пользователей `guest` (`guest`, `guest2`) на директорию `home/guest` в которой находятся все файлы для последующей работы (рис. 10).



```
[guest@vmmalyuga vmmalyuga]$ cd
[guest@vmmalyuga ~]$ pwd
/home/guest
[guest@vmmalyuga ~]$ chmod g+rw /home/guest
[guest@vmmalyuga ~]$
```

Рис. 4.10: Изменение прав директории

11. От имени пользователя `guest` снимаю все атрибуты с директории `dir1`, созданной в предыдущей лабораторной работе. Проверяю, что права действительно сняты (рис. 11).

```
[guest@vvmalyuga ~]$ chmod g+rwX /home/guest
[guest@vvmalyuga ~]$ ls
Desktop Documents Music Public testdir
dir1 Downloads Pictures Templates Videos
[guest@vvmalyuga ~]$ chmod 000 dir1
[guest@vvmalyuga ~]$ ls
Desktop Documents Music Public testdir
dir1 Downloads Pictures Templates Videos
[guest@vvmalyuga ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Mar 8 18:38 Desktop
d----- . 2 guest guest 6 Mar 8 18:48 dir1
drwxr-xr-x. 2 guest guest 6 Mar 8 18:38 Documents
drwxr-xr-x. 2 guest guest 6 Mar 8 18:38 Downloads
drwxr-xr-x. 2 guest guest 6 Mar 8 18:38 Music
drwxr-xr-x. 2 guest guest 6 Mar 8 18:38 Pictures
drwxr-xr-x. 2 guest guest 6 Mar 8 18:38 Public
drwxr-xr-x. 2 guest guest 6 Mar 8 18:38 Templates
drw--x--x. 2 guest guest 22 Mar 8 19:04 testdir
drwxr-xr-x. 2 guest guest 6 Mar 8 18:38 Videos
[guest@vvmalyuga ~]$
```

Рис. 4.11: Изменение прав директории

4.1 Заполнение таблицы 3.1

Далее проверяю как пользователь guest2 будет взаимодействовать с файлами в этой директории (рис. 12).

Пример заполнения таблицы 3.1

Рис. 4.12: Пример заполнения таблицы 3.1

Права директории	Права файла	Просмотр							
		Запись				файлов		Смена	
		Создание файла	Изменение файла	Чтение файла	Смена файла	Просмотр директории	Переименование файла	Смена атрибута файла	
d-----	-----	-	-	-	-	-	-	-	-
(000)	(000)								
d-----x--	-----	-	-	-	-	-	-	-	+
(010)	(000)								
d----w---	-----	-	-	-	-	-	-	-	-
(020)	(000)								

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

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

Права директории	Права файла	Просмотр							
		Запись		Просмотр		Смена		Смена	
		Создание файла	Изменение файла	Чтение файла	Смена директории	Просмотр файла	Смена файла	Просмотр файла	Смена файла
d---wx--	-----wx--	+	+	+	-	+	-	+	+
(030)	(030)								
d---r----	-----wx--	-	-	-	-	-	+	-	-
(040)	(030)								
d---r-x--	-----wx--	-	-	+	-	+	+	-	+
(050)	(030)								
d---rw---	-----wx--	-	-	-	-	-	+	-	-
(060)	(030)								
d---rwx--	-----wx--	+	+	+	-	+	+	+	+
(070)	(030)								
d-----	----r----	-	-	-	-	-	-	-	-
(000)	(040)								
d-----x--	----r----	-	-	-	+	+	-	-	+
(010)	(040)								
d---w---	----r----	-	-	-	-	-	-	-	-
(020)	(040)								
d---wx--	----r----	+	+	-	+	+	-	+	+
(030)	(040)								
d---r----	----r----	-	-	-	-	-	+	-	-
(040)	(040)								
d---r-x--	----r----	-	-	-	+	+	+	-	+
(050)	(040)								
d---rw---	----r----	-	-	-	-	-	+	-	-
(060)	(040)								



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

Права директории	Права файла	Права							
		Создание файла	Удаление файла	Запись файл	Чтение файла	Смена директи	Просмотр файлов	Переименование файла	Смена атрибутов файла
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)	-	-	-	-	-	+	-	-

		Права							
Права директории	Права файла	Создание		Удаление		Чтение		Запись	Просмотр
		файла	файла	файл	файл	файла	файла	файлов	Смена
		файла	файла	файл	файл	дирек	три	файл	файла
d---rwx-- (070)	----rwx-- (070)	+	+	+	+	+	+	+	+

Таблица 3.1 «Установленные права и разрешённые действия для групп»

## 4.2 Заполнение таблицы 3.2

На основе таблицы 3.1 заполняю таблицу 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»

## 5 Выводы

Были получены практические навыки работы в консоли с атрибутами файлов для групп пользователей

## 6 Список литературы. Библиография

[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#Что\\_такое\\_группы](https://losst.pro/gruppy-polzovatelej-linux#Что_такое_группы)