

# **Отчёт по лабораторной работе №3**

## **Информационная безопасность**

**Дискреционное разграничение прав в Linux. Два пользователя**

Выполнил: Махорин Иван Сергеевич,  
НПИБд-02-21, 1032211221

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Теоретическое введение</b>	<b>5</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>7</b>
3.1	Атрибуты файлов . . . . .	7
3.2	Заполнение таблицы 3.1 . . . . .	11
3.3	Заполнение таблицы 3.2 . . . . .	18
<b>4</b>	<b>Вывод</b>	<b>20</b>
<b>5</b>	<b>Список литературы. Библиография</b>	<b>21</b>

## Список иллюстраций

3.1	useradd guest . . . . .	7
3.2	passwd guest2 . . . . .	8
3.3	gpasswd -a guest2 guest . . . . .	8
3.4	Открытие двух пользователей на двух консолях . . . . .	8
3.5	pwd . . . . .	9
3.6	id -Gn; id -G; id; groups guest/guest2 . . . . .	9
3.7	cat /etc/group . . . . .	10
3.8	newgrp guest . . . . .	10
3.9	chmod g+rx /home/guest . . . . .	11
3.10	chmod 000 dir1 . . . . .	11
3.11	ls -l . . . . .	11

# 1 Цель работы

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

## 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].

**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].

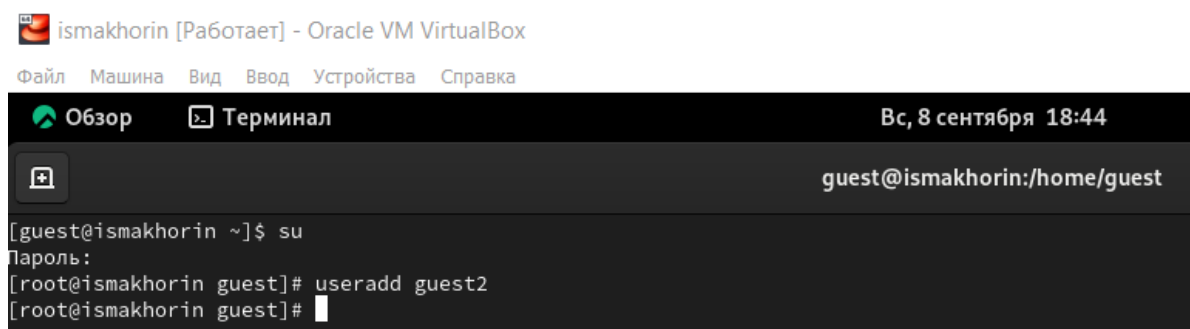
- daemon - от имени этой группы и пользователя daemon запускаются сервисы, которым необходима возможность записи файлов на диск.
- sys - группа открывает доступ к исходникам ядра и файлам - include сохраненным в системе
- sync - позволяет выполнять команду /bin/sync
- games - разрешает играм записывать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

## 3 Выполнение лабораторной работы

### 3.1 Атрибуты файлов

1. В установленной операционной системе создадим учётную запись пользователя guest2 (используя учётную запись администратора). guest1 был создан в предыдущей лабораторной работе.



```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Вс, 8 сентября 18:44
guest@ismakhorin:/home/guest
[guest@ismakhorin ~]$ su
Пароль:
[root@ismakhorin guest]# useradd guest2
[root@ismakhorin guest]#
```

Рис. 3.1: useradd guest

2. Далее зададим пароль для пользователя guest2:

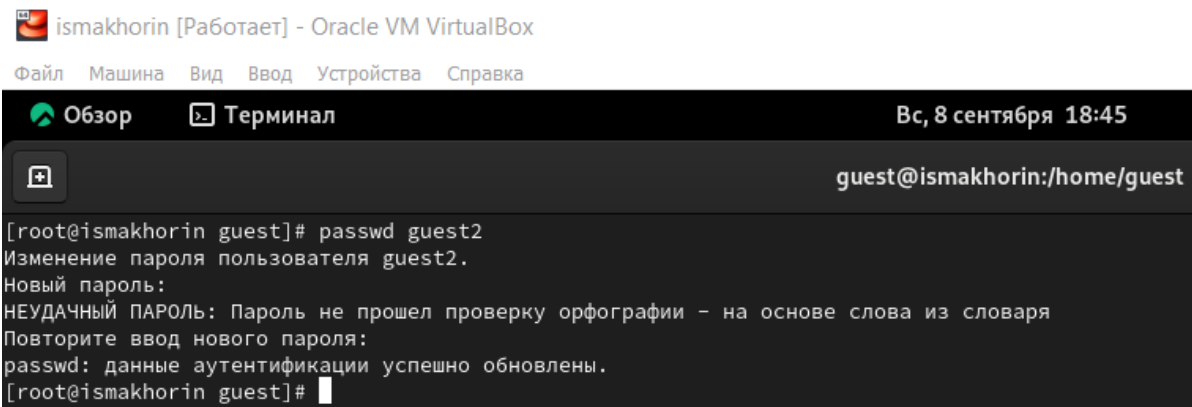


Рис. 3.2: passwd guest2

3. Добавим пользователя guest2 в группу guest:

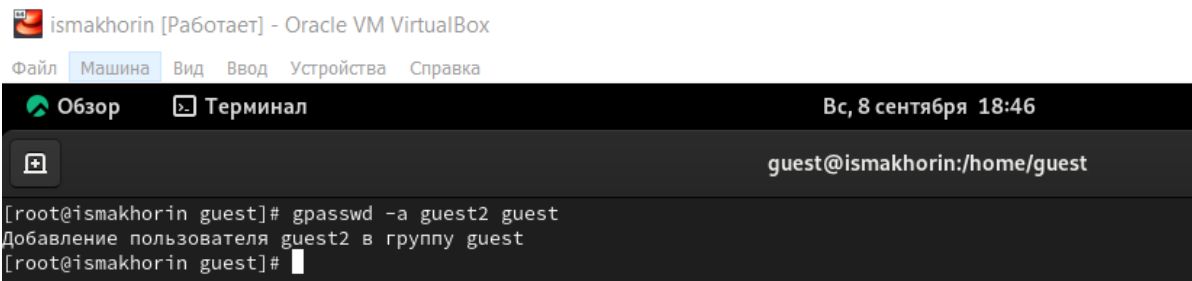


Рис. 3.3: gpasswd -a guest2 guest

4. Следующим шагом осуществим вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли:

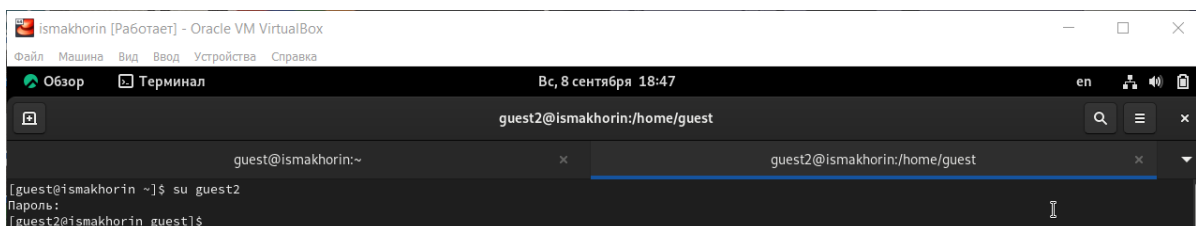


Рис. 3.4: Открытие двух пользователей на двух консолях

5. Для обоих пользователей командой `pwd` определим директорию, в которой мы находимся и сравним её с приглашениями командной строки:



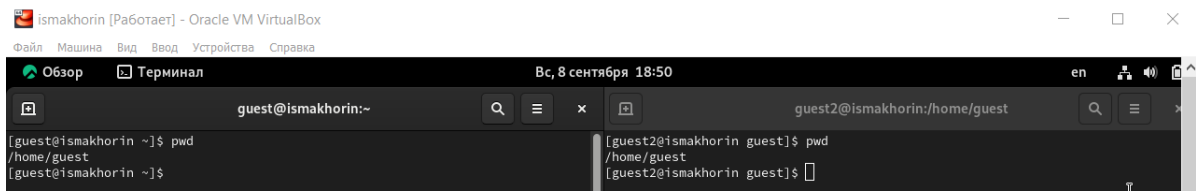


Рис. 3.5: pwd

- Уточним имя нашего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определим командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`. Затем сравним вывод команды `groups` с выводом команд `id -Gn` и `id -G`:

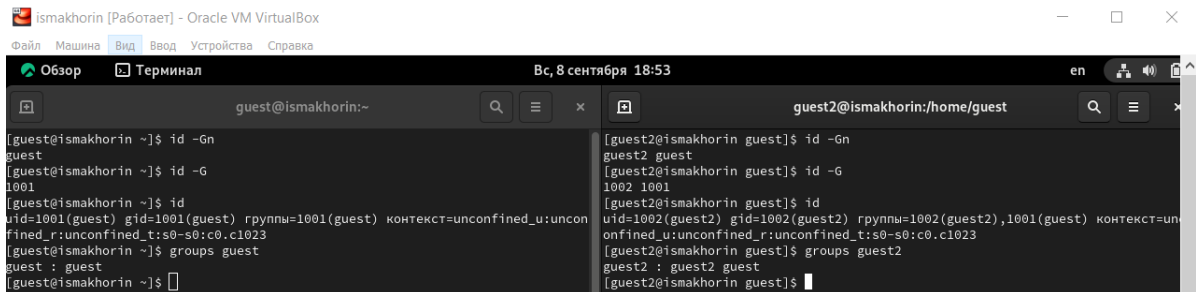


Рис. 3.6: id -Gn; id -G; id; groups guest/guest2

- Сравним полученную информацию с содержимым файла `/etc/group`:

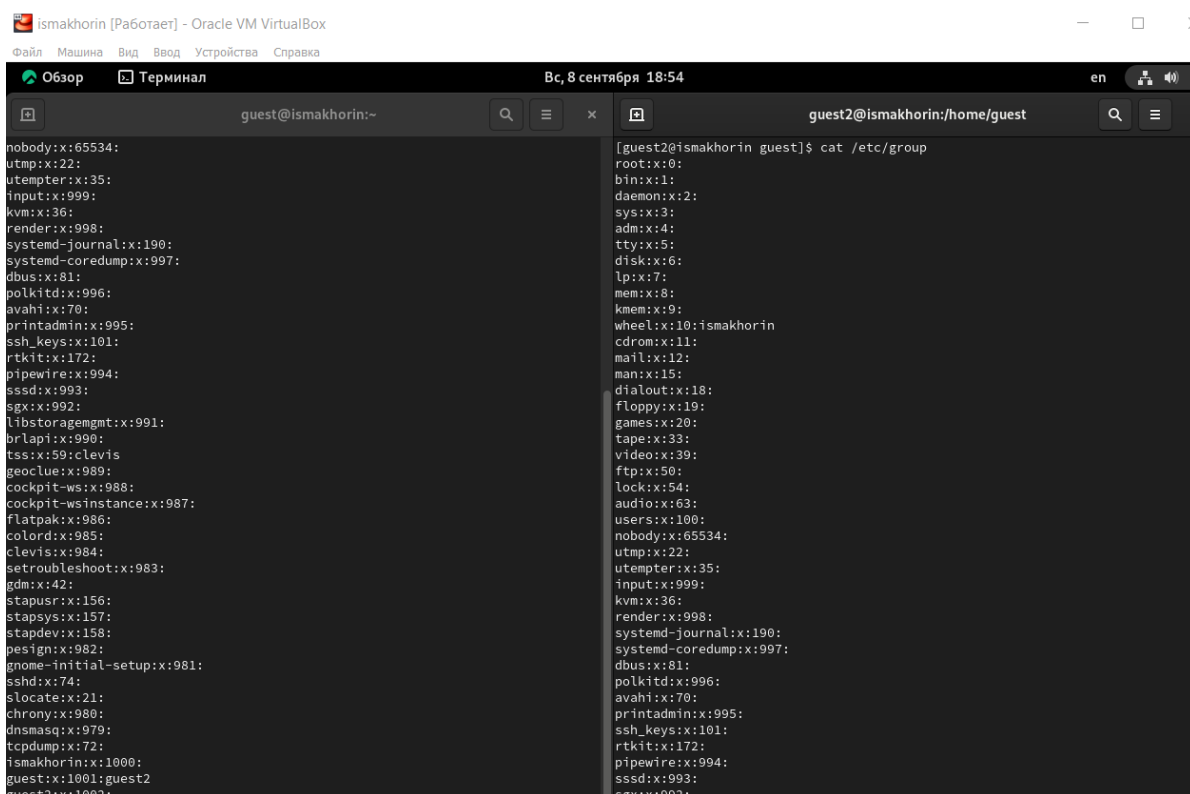


Рис. 3.7: cat /etc/group

8. От имени пользователя guest2 выполним регистрацию пользователя guest2 в группе guest командой newgrp guest:

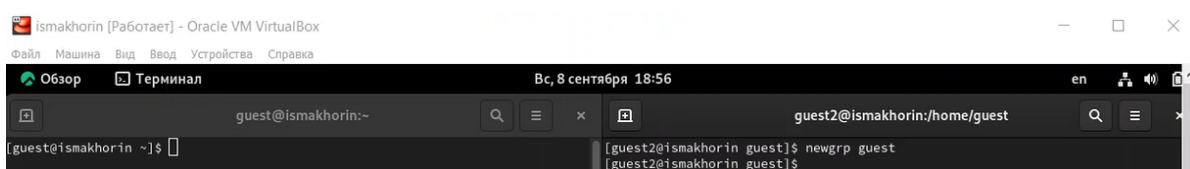


Рис. 3.8: newgrp guest

9. От имени пользователя guest изменим права директории /home/guest, разрешив все действия для пользователей группы: chmod g+rwX /home/guest

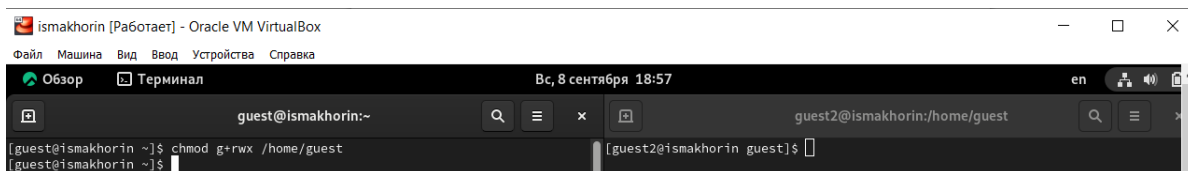


Рис. 3.9: chmod g+rwx /home/guest

10. От имени пользователя guest снимем с директории /home/guest/dir1 все атрибуты командой chmod 000 dir1:

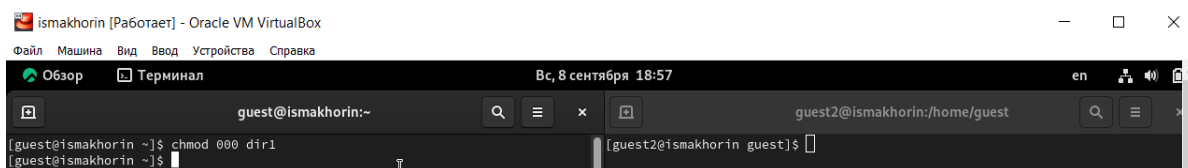


Рис. 3.10: chmod 000 dir1

11. В конце проверим правильность снятия атрибутов:

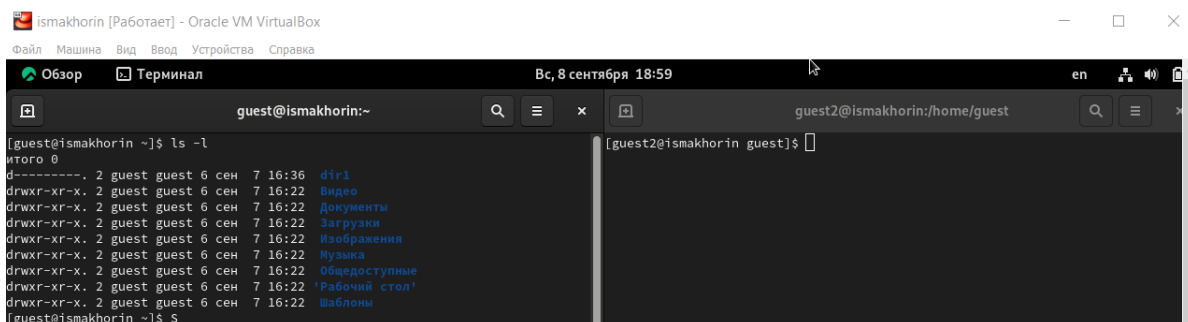


Рис. 3.11: ls -l

## 3.2 Заполнение таблицы 3.1

11. Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполним табл. 3.1, определив опытным путём, какие операции разрешены, а какие нет. После чего сравним табл. 2.1 (из лабораторной работы №2) и табл. 3.1.

Права директории	Права файла	<div> <div> <div>Про-</div> <div>смотр</div> <div>фай-</div> <div>Сме-</div> <div>лов</div> <div>ре-</div> <div>ат-</div> </div> <div> <div>Сме-</div> <div>на</div> <div>в</div> <div>име-</div> <div>ри-</div> <div>бу-</div> <div>тов</div> </div> <div> <div>Со-</div> <div>Уда-</div> <div>За-</div> <div>Чте-</div> <div>ди-</div> <div>рек-</div> <div>то-</div> </div> <div> <div>зда-</div> <div>ле-</div> <div>пись</div> <div>ние</div> <div>фай-</div> <div>фай-</div> <div>в</div> <div>фай-</div> <div>то-</div> <div>ри</div> <div>ри</div> <div>файл</div> <div>ла</div> </div> </div>							
		ла	ла	файл	ла	рии	рии	файл	ла
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-----x---	-----x---	-	-	-	-	-	-	-	-
(000)	(010)								
d-----x---	-----x---	-	-	-	-	+	-	-	+
(010)	(010)								

Права директории	Права файла	<div> <div>Про- смотр фай-</div> <div>Сме- на ре- ат-</div> <div>Сме- лов ре- ва-</div> <div>на в име-</div> <div>на ди- рек-</div> <div>ди- рек-</div> <div>но- бу-</div> <div>ри- бу-</div> <div>ри- тов</div> <div>фай-</div> </div>							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ре- к- то- рии	ре- к- то- рии	фай- ла	фай- ла
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)								
d---rwx---	-----x---	+	+	-	-	+	+	+	+
(070)	(010)								
d-----	-----w----	-	-	-	-	-	-	-	-
(000)	(020)								
d-----x---	-----w----	-	-	+	-	+	-	-	+
(010)	(020)								
d----w----	-----w----	-	-	-	-	-	-	-	-
(020)	(020)								
d----wx---	-----w----	+	+	+	-	+	-	+	+
(030)	(020)								

Права директории	Права файла	<div> <div>Про-</div> <div>смотр</div> <div>Сме-</div> <div>фай-</div> <div>Пе-</div> <div>на</div> <div>Сме-</div> <div>лов</div> <div>ре-</div> <div>ат-</div> <div>на</div> <div>в</div> <div>име-</div> <div>ри-</div> <div>бу-</div> <div>тов</div> <div>фай-</div> <div>ла</div> </div>							
		Со-	Уда-	За-	Чте-	ди-	ди-	но-	ри-
		зда-	ле-	пись	ние	рек-	рек-	ва-	бу-
		ние	ние	в	фай-	то-	то-	ние	тов
		фай-	фай-	файл	фай-	то-	то-	файл	фай-
		ла	ла	файл	ла	рии	рии	файл	ла
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)								
d----wx---	-----wx---	+	+	+	-	+	-	+	+
(030)	(030)								
d---r-----	-----wx---	-	-	-	-	-	+	-	-
(040)	(030)								
d---r-x---	-----wx---	-	-	+	-	+	+	-	+
(050)	(030)								

		Права							
		Создание файла	Удаление файла	Запись в файл	Чтение файла	Сме- на ди- рек- то- рии	Про- смотр фай- лов в ди- рек- то- рии	Пе- ре- име- но- вание файл	Сме- на ат- ри- бу- тов фай-
Права директории	Права файла	ла	ла	файл	ла	рии	рии	файл	ла
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)								
d---rwx---	----r-----	+	+	-	+	+	+	+	+
(070)	(040)								

		Права							
		См				Сме-			
		на				ат-			
		ри-				ри-			
		бу-				бу-			
		тов				тов			
		фай-				фай-			
Права	Права файла	ла	ла	файл	ла	рии	рии	файл	ла
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)								



		Права							
		Права директории				Права файла			
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- ди- рек- то- рии	Про- смотр фай- лов в ди- рек- то- рии	Пе- ре- име- но- вание файл	Сме- на ат- ри- бу- тов фай- ла
d----	w----	-	-	-	-	-	-	-	-
(020)	(060)								
d----	wx---	+	+	+	+	+	-	+	+
(030)	(060)								
d---r-----	-----rw----	-	-	-	-	-	+	-	-
(040)	(060)								
d---r-x---	-----rw----	-	-	+	+	+	+	-	+
(050)	(060)								
d---rw----	-----rw----	-	-	-	-	-	+	-	-
(060)	(060)								
d---rwx---	-----rw----	+	+	+	+	+	+	+	+
(070)	(060)								
d-----	-----rwx---	-	-	-	-	-	-	-	-
(000)	(070)								
d-----x---	-----rwx---	-	-	+	+	+	-	-	+
(010)	(070)								
d-----w----	-----rwx---	-	-	-	-	-	-	-	-
(020)	(070)								
d-----wx---	-----rwx---	+	+	+	+	+	-	+	+
(030)	(070)								

Права директории	Права файла	<div> <div>Про- смотр фай-</div> <div>Сме- на ре- ат-</div> <div>Сме- лов ре- ва-</div> <div>на в име- но-</div> <div>ри- бу- тов фай-</div> </div>							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	ди- рек- то- рии	фай- ла	фай- ла
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»

### 3.3 Заполнение таблицы 3.2

12. На основании заполненной таблицы определим те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполним табл. 3.2.

Операция	Права на директорию	Права на файл
Создание файла	d----wx--- (030)	----- (000)

Операция	Права на директорию	Права на файл
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.

## 4 Вывод

В ходе выполнения лабораторной работы были получены практические навыки работы в консоли с атрибутами файлов для групп пользователей.

## 5 Список литературы. Библиография

[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%B>