

Отчет по лабораторной работе №3

Основы информационной безопасности

Бабенко Константин, НКАбд-01-23

Содержание

Цель работы	1
Задание	1
Теоретическое введение	1
Выполнение лабораторной работы	2
Заполнение таблицы 3.1	8
Заполнение таблицы 3.2	17
Выводы	18
Список литературы. Библиография	18

Цель работы

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

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.

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]

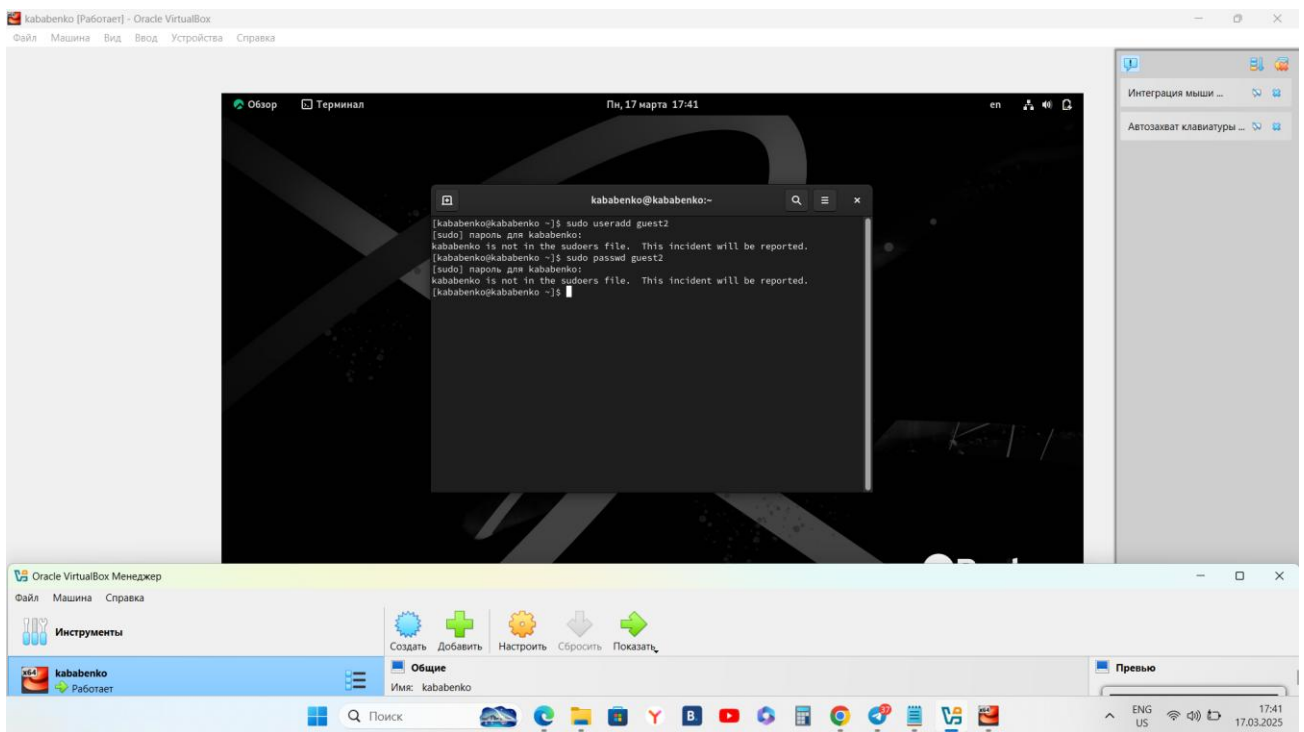
Группы пользователей Linux кроме стандартных `root` и `users`, здесь есть еще пару десятков групп. Это группы, созданные программами, для управления доступом этих программ к общим ресурсам. Каждая группа разрешает чтение или запись определенного файла или каталога системы, тем самым регулируя полномочия 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/
- проху - 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/vsa 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

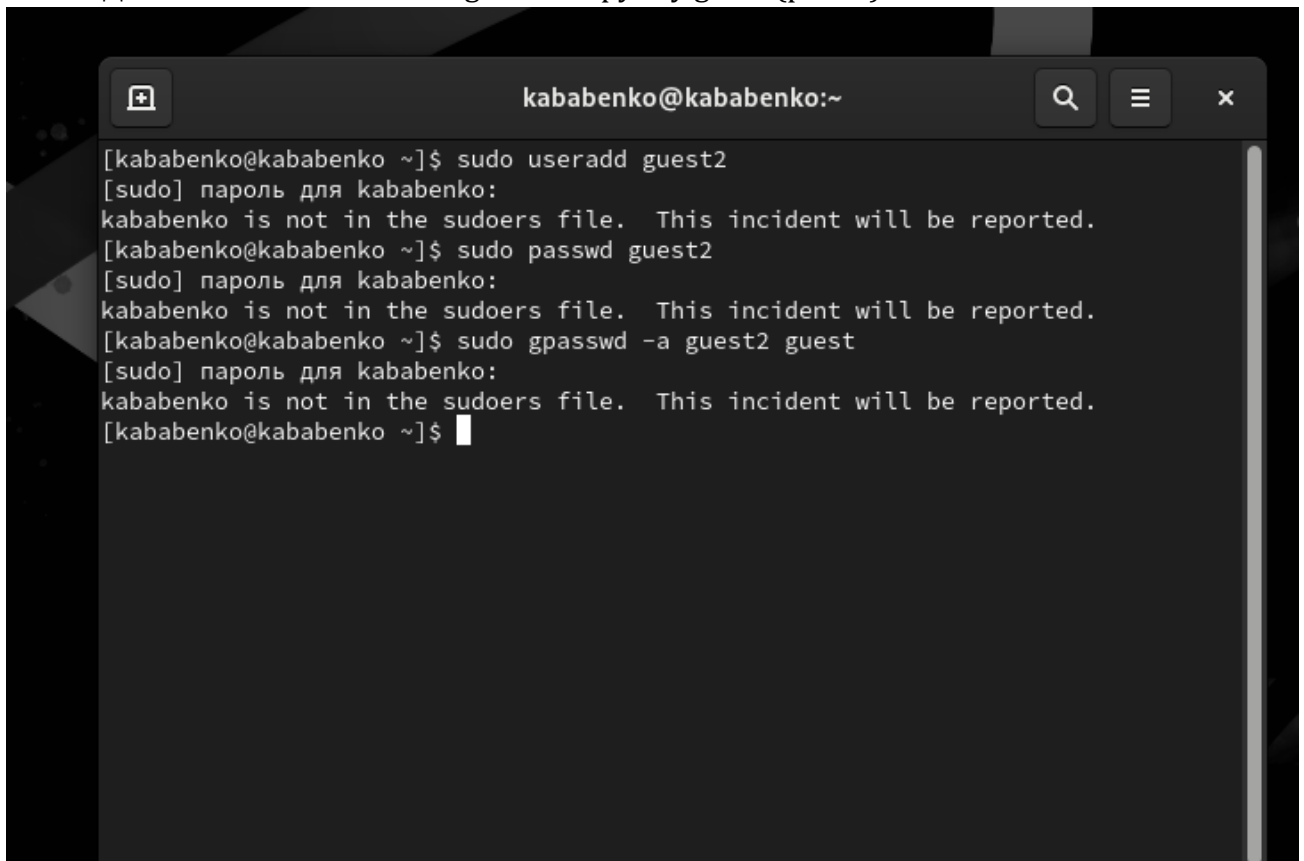
Выполнение лабораторной работы

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).



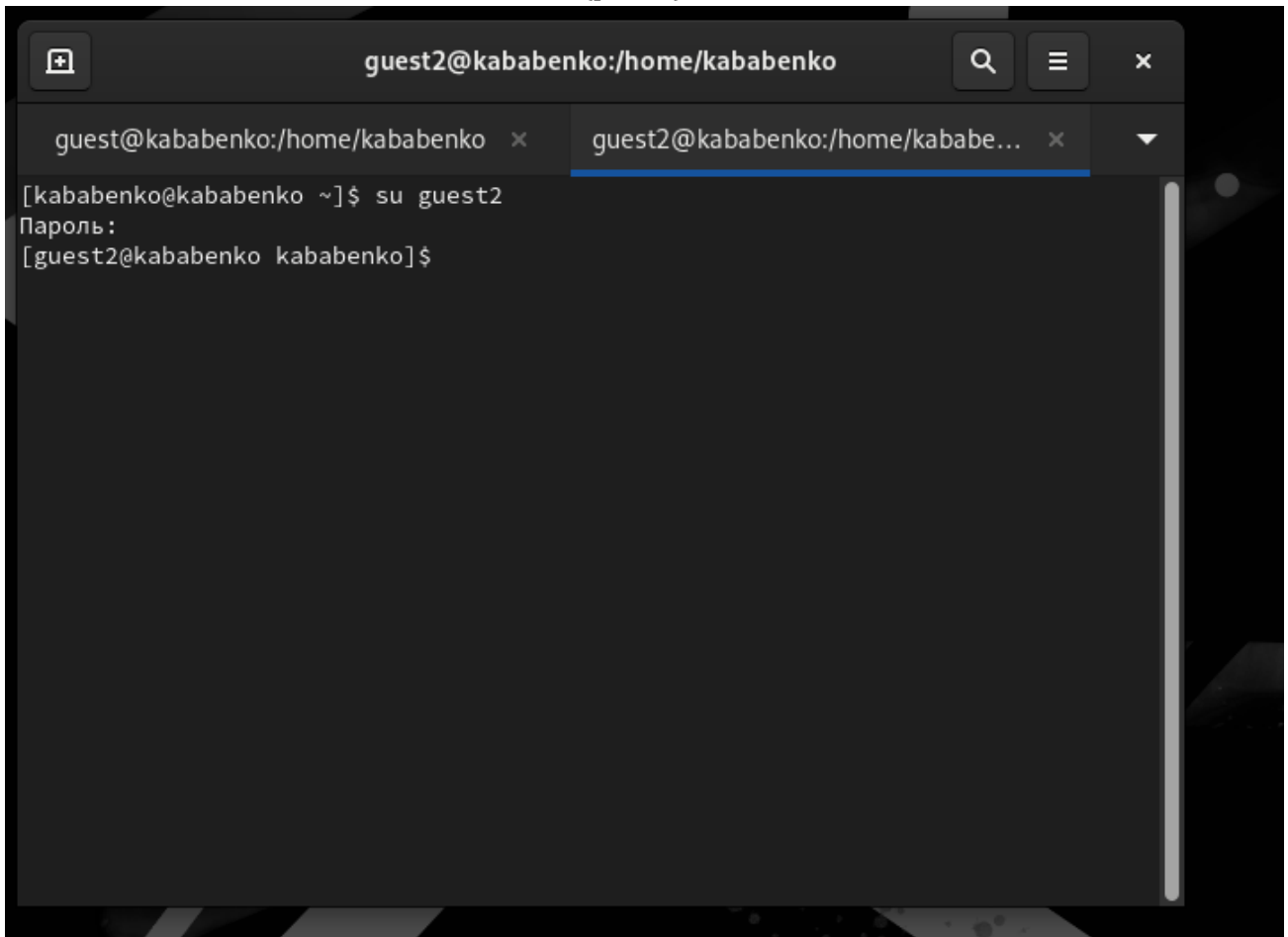
Создание пользователя

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



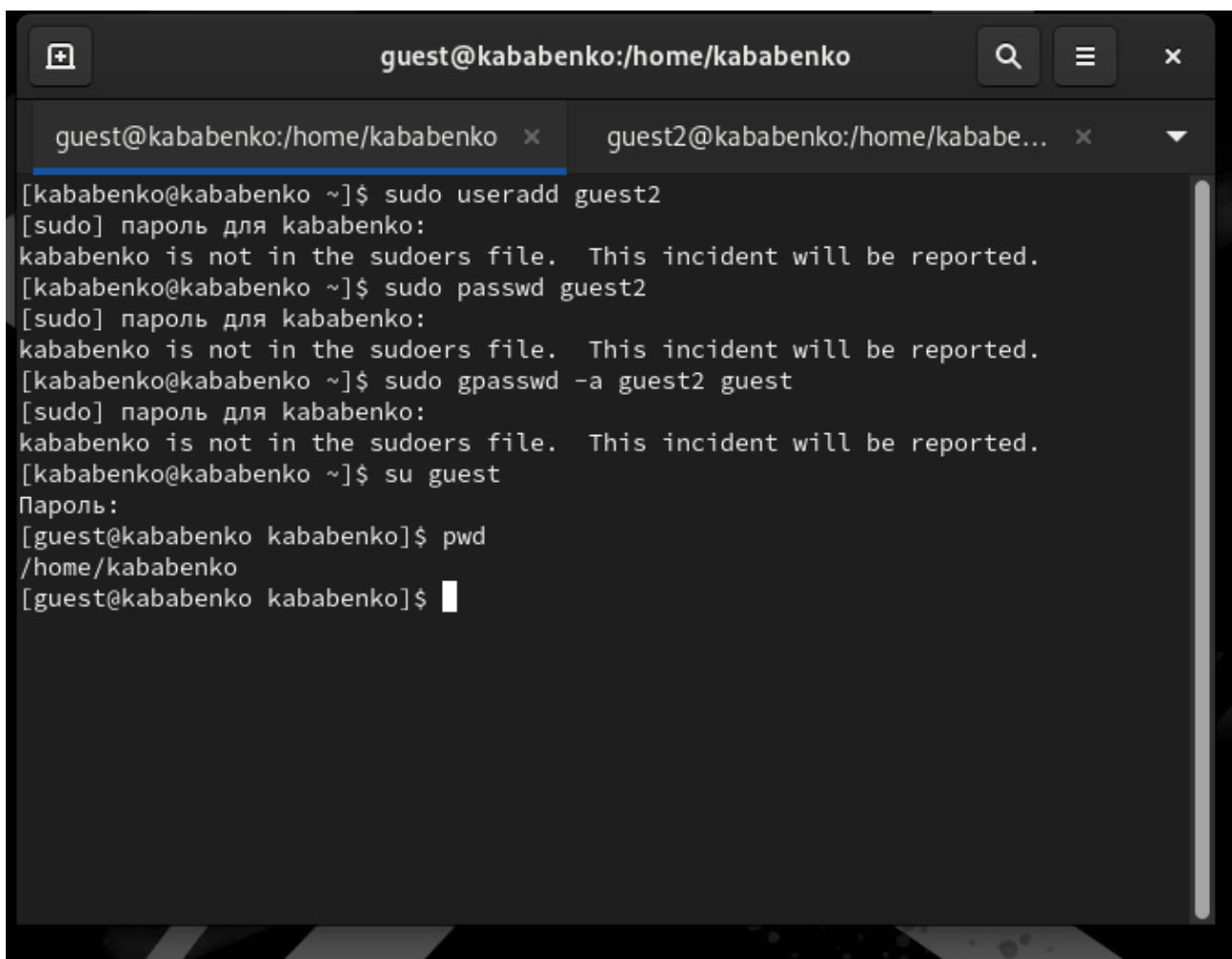
Добавление пользователя в группу

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



Вход в терминал от имени другого пользователя

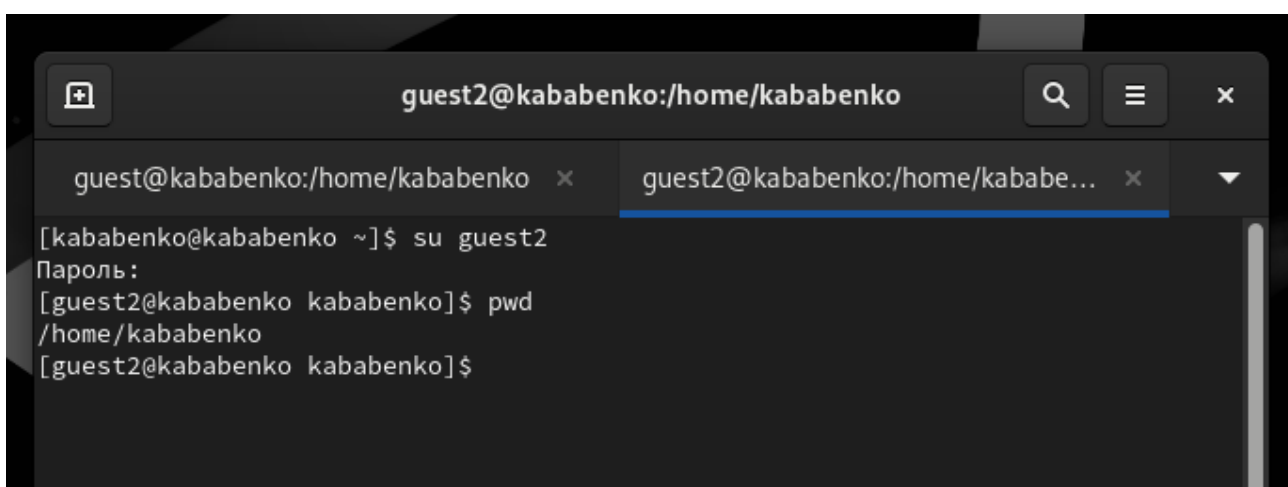
6. Проверяю путь директории, в которой я нахожусь с помощью `pwd`.
Проверка для пользователя `guest` (рис. 4).



```
guest@kababenko:/home/kababenko
[guest@kababenko:/home/kababenko]$ sudo useradd guest2
[sudo] пароль для kababenko:
kababenko is not in the sudoers file. This incident will be reported.
[guest@kababenko:/home/kababenko]$ sudo passwd guest2
[sudo] пароль для kababenko:
kababenko is not in the sudoers file. This incident will be reported.
[guest@kababenko:/home/kababenko]$ sudo gpasswd -a guest2 guest
[sudo] пароль для kababenko:
kababenko is not in the sudoers file. This incident will be reported.
[guest@kababenko:/home/kababenko]$ su guest
Пароль:
[guest@kababenko kababenko]$ pwd
/home/kababenko
[guest@kababenko kababenko]$
```

Текущая директория для guest

Проверка для пользователя guest2 (рис. 5).



```
guest2@kababenko:/home/kababenko
[guest@kababenko:/home/kababenko]$ su guest2
Пароль:
[guest2@kababenko kababenko]$ pwd
/home/kababenko
[guest2@kababenko kababenko]$
```

Текущая директория для guest2

Стоит отметить, что вход в терминал от имени пользователей был выполнен в домашней директории пользователя evdvorkina, которую команда `pwd` вывел.

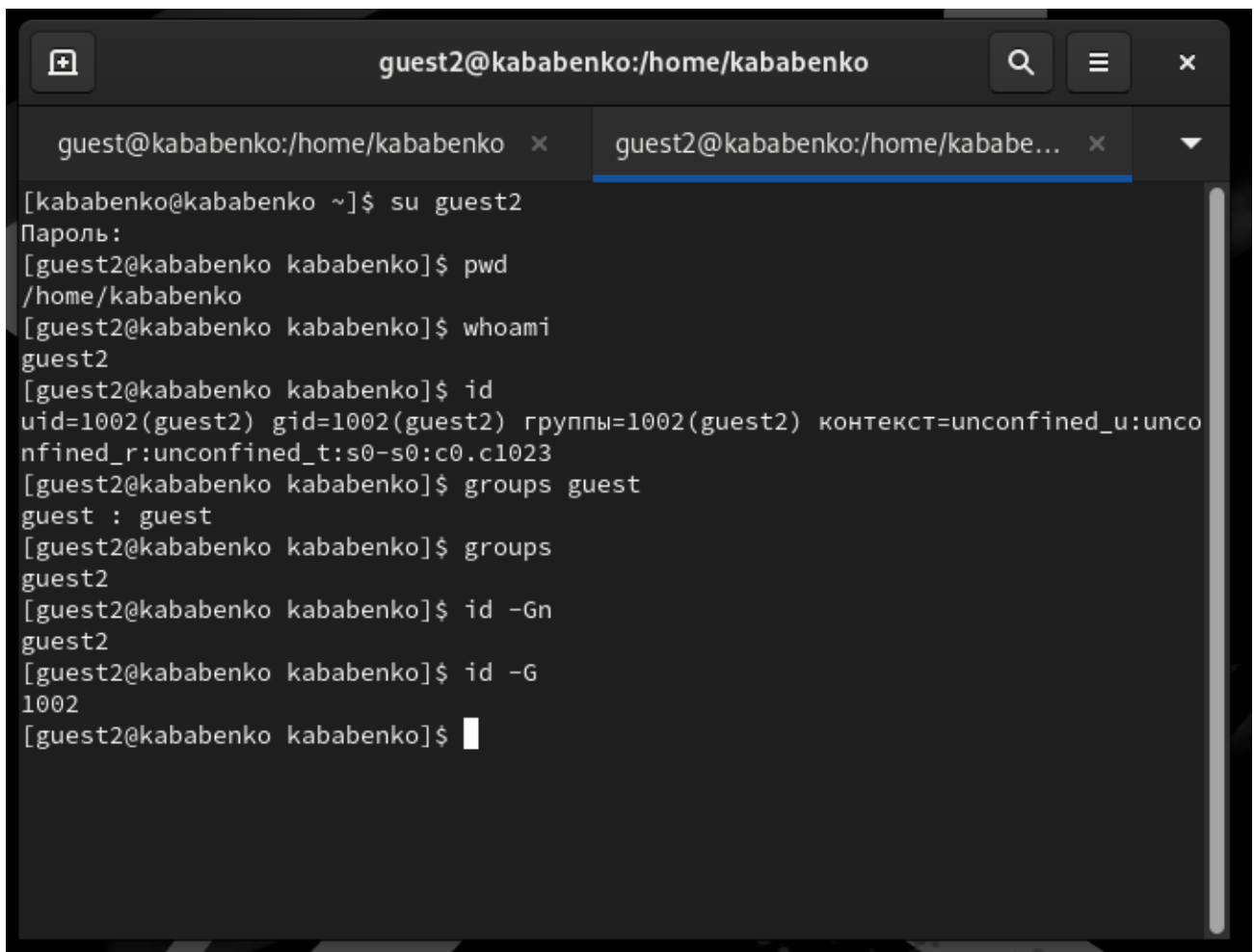
Домашней директорией пользователей она не является. Текущая директория с приглашением командной строки совпадает.

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).

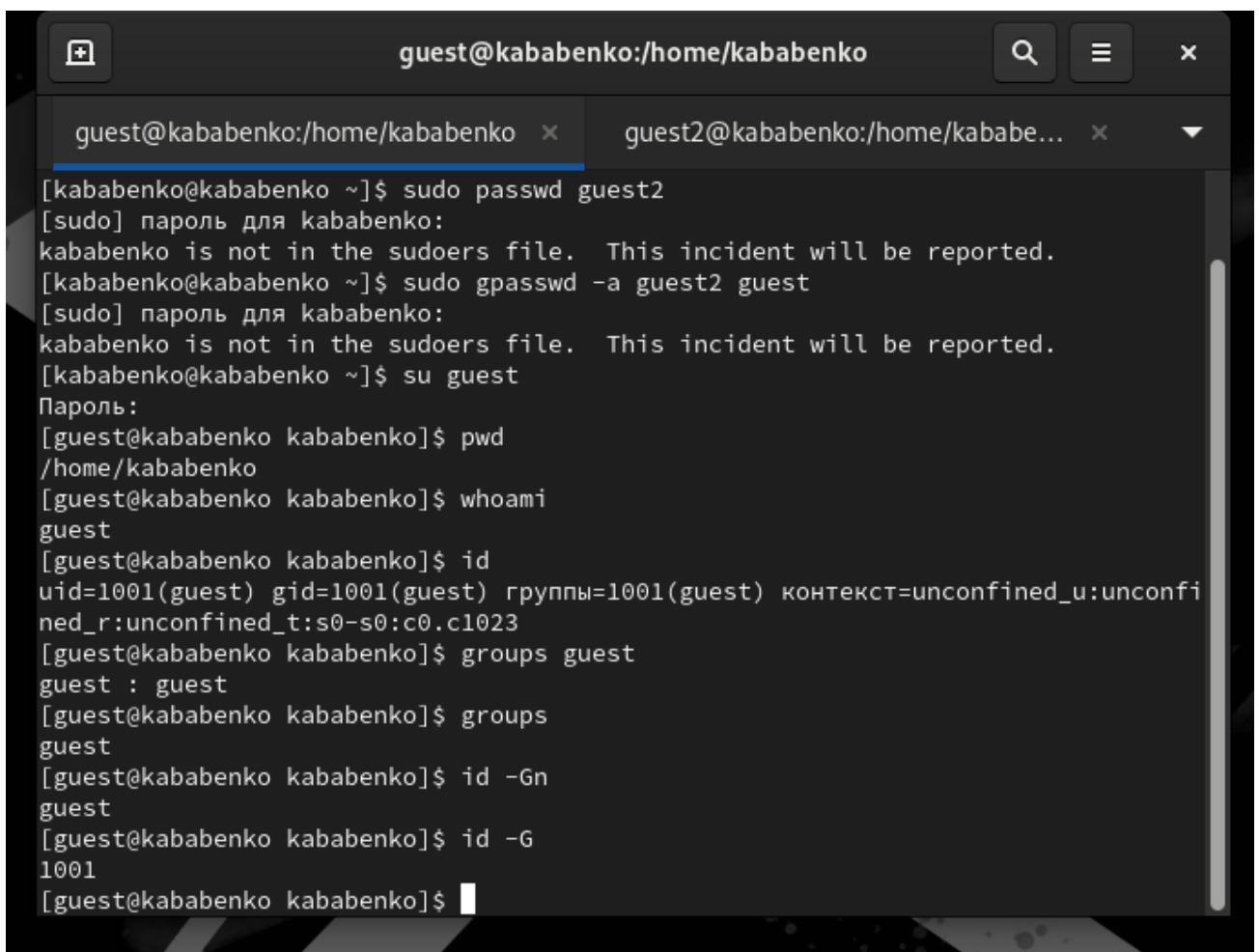


```
guest2@kababenko:/home/kababenko

[kababenko@kababenko ~]$ su guest2
Пароль:
[guest2@kababenko kababenko]$ pwd
/home/kababenko
[guest2@kababenko kababenko]$ whoami
guest2
[guest2@kababenko kababenko]$ id
uid=1002(guest2) gid=1002(guest2) группы=1002(guest2) контекст=unconfined_u:unco
nfinied_r:unconfined_t:s0-s0:c0.c1023
[guest2@kababenko kababenko]$ groups guest
guest : guest
[guest2@kababenko kababenko]$ groups
guest2
[guest2@kababenko kababenko]$ id -Gn
guest2
[guest2@kababenko kababenko]$ id -G
1002
[guest2@kababenko kababenko]$
```

Информация о пользователе `guest2`

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

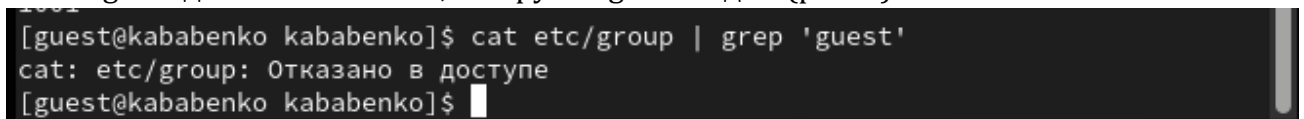


```
guest@kababenko:/home/kababenko
guest@kababenko:/home/kababenko x guest2@kababenko:/home/kababe... x
[kababenko@kababenko ~]$ sudo passwd guest2
[sudo] пароль для kababenko:
kababenko is not in the sudoers file. This incident will be reported.
[kababenko@kababenko ~]$ sudo gpasswd -a guest2 guest
[sudo] пароль для kababenko:
kababenko is not in the sudoers file. This incident will be reported.
[kababenko@kababenko ~]$ su guest
Пароль:
[guest@kababenko kababenko]$ pwd
/home/kababenko
[guest@kababenko kababenko]$ whoami
guest
[guest@kababenko kababenko]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@kababenko kababenko]$ groups guest
guest : guest
[guest@kababenko kababenko]$ groups
guest
[guest@kababenko kababenko]$ id -Gn
guest
[guest@kababenko kababenko]$ id -G
1001
[guest@kababenko kababenko]$
```

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.

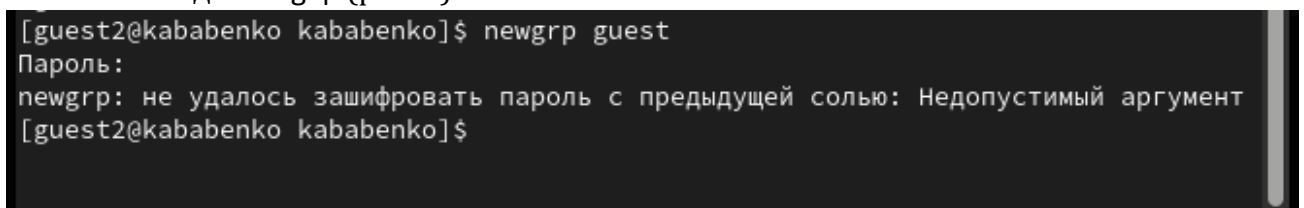
8. Вывел интересующее меня содержимое файла `etc/group`, видно, что в группе guest два пользователя, а в группе guest2 один (рис. 8).



```
[guest@kababenko kababenko]$ cat etc/group | grep 'guest'
cat: etc/group: Отказано в доступе
[guest@kababenko kababenko]$
```

Содержимое файла `etc/group`

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



```
[guest2@kababenko kababenko]$ newgrp guest
Пароль:
newgrp: не удалось зашифровать пароль с предыдущей солью: Недопустимый аргумент
[guest2@kababenko kababenko]$
```

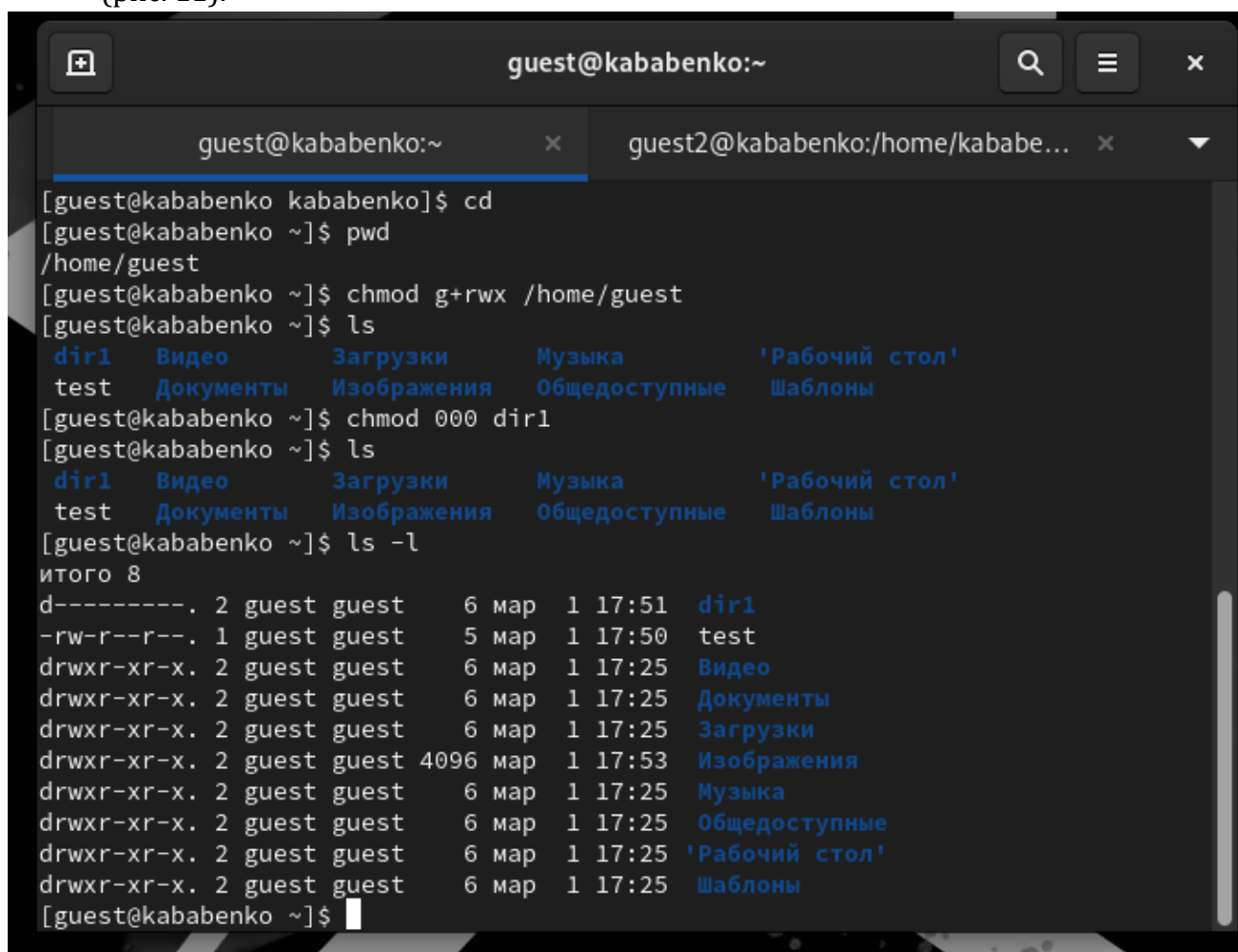
Регистрация пользователя в группе

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@kababenko kababenko]$ cd
[guest@kababenko ~]$ pwd
/home/guest
[guest@kababenko ~]$ chmod g+rwX /home/guest
[guest@kababenko ~]$
```

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).



The screenshot shows a terminal window with two tabs: 'guest@kababenko:~' and 'guest2@kababenko:/home/kababe...'. The active tab is 'guest@kababenko:~'. The terminal output is as follows:

```
[guest@kababenko kababenko]$ cd
[guest@kababenko ~]$ pwd
/home/guest
[guest@kababenko ~]$ chmod g+rwX /home/guest
[guest@kababenko ~]$ ls
dir1  Видео  Загрузки  Музыка  'Рабочий стол'
test  Документы  Изображения  Общедоступные  Шаблоны
[guest@kababenko ~]$ chmod 000 dir1
[guest@kababenko ~]$ ls
dir1  Видео  Загрузки  Музыка  'Рабочий стол'
test  Документы  Изображения  Общедоступные  Шаблоны
[guest@kababenko ~]$ ls -l
итого 8
d----- . 2 guest guest 6 map 1 17:51 dir1
-rw-r--r-- 1 guest guest 5 map 1 17:50 test
drwxr-xr-x 2 guest guest 6 map 1 17:25 Видео
drwxr-xr-x 2 guest guest 6 map 1 17:25 Документы
drwxr-xr-x 2 guest guest 6 map 1 17:25 Загрузки
drwxr-xr-x 2 guest guest 4096 map 1 17:53 Изображения
drwxr-xr-x 2 guest guest 6 map 1 17:25 Музыка
drwxr-xr-x 2 guest guest 6 map 1 17:25 Общедоступные
drwxr-xr-x 2 guest guest 6 map 1 17:25 'Рабочий стол'
drwxr-xr-x 2 guest guest 6 map 1 17:25 Шаблоны
[guest@kababenko ~]$
```

Изменение прав директории

Заполнение таблицы 3.1

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


```
guest@kababenko:~
[guest@kababenko kababenko]$ cd
[guest@kababenko ~]$ pwd
/home/guest
[guest@kababenko ~]$ chmod g+rwX /home/guest
[guest@kababenko ~]$ ls
dir1 Видео Загрузки Музыка 'Рабочий стол'
test Документы Изображения Общедоступные Шаблоны
[guest@kababenko ~]$ chmod 000 dir1
[guest@kababenko ~]$ ls
dir1 Видео Загрузки Музыка 'Рабочий стол'
test Документы Изображения Общедоступные Шаблоны
[guest@kababenko ~]$ ls -l
итого 8
d----- . 2 guest guest 6 мар 1 17:51 dir1
-rw-r--r-- 1 guest guest 5 мар 1 17:50 test
drwxr-xr-x 2 guest guest 6 мар 1 17:25 Видео
drwxr-xr-x 2 guest guest 6 мар 1 17:25 Документы
drwxr-xr-x 2 guest guest 6 мар 1 17:25 Загрузки
drwxr-xr-x 2 guest guest 4096 мар 1 17:53 Изображения
drwxr-xr-x 2 guest guest 6 мар 1 17:25 Музыка
drwxr-xr-x 2 guest guest 6 мар 1 17:25 Общедоступные
drwxr-xr-x 2 guest guest 6 мар 1 17:25 'Рабочий стол'
drwxr-xr-x 2 guest guest 6 мар 1 17:25 Шаблоны
[guest@kababenko ~]$
```

Пример заполнения таблицы 3.1

Права директо рии	Пра ва фай ла	Созда ние файла	Удале ние файла	Зап ись фай л	Чтен ие фай ла	Смена директо рии	Просмо тр файлов в директо рии	Переимено вание файл	Смена атрибу тов файла
d----- -- (000)	--- --- ---	-	-	-	-	-	-	-	-
d----- x-- (010)	--- --- ---	-	-	-	-	-	-	-	+
d----w- -- (020)	--- --- ---	-	-	-	-	-	-	-	-

Права директо рии	Пра ва фай ла	Созда ние файла	Удале ние файла	Зап ись в фай л	Чтен ие фай ла	Смена директо рии	Просмо тр файлов в директо рии	Переимено вание файл	Смена атрибу тов файла
	0)								
d----	---	+	+	-	-	+	-	+	+
wx--	---								
(030)	---								
	(00								
	0)								
d---r--	---	-	-	-	-	-	+	-	-
--	---								
(040)	---								
	(00								
	0)								
d---r-	---	-	-	-	-	+	+	-	+
x--	---								
(050)	---								
	(00								
	0)								
d---rw-	---	-	-	-	-	-	+	-	-
--	---								
(060)	---								
	(00								
	0)								
d---	---	+	+	-	-	+	+	+	+
rwx--	---								
(070)	---								
	(00								
	0)								
d-----	---	-	-	-	-	-	-	-	-
--	---								
(000)	x--								
	(01								
	0)								
d-----	---	-	-	-	-	-	-	-	+
x--	---								
(010)	x--								
	(01								
	0)								
d-----w-	---	-	-	-	-	-	-	-	-
--	---								
(020)	x--								
	(01								
	0)								
d----	---	+	+	-	-	+	-	+	+
wx--	---								

Права директо рии	Пра ва фай ла	Созда ние файла	Удале ние файла	Зап ись в фай л	Чтен ие фай ла	Смена директо рии	Просмо тр файлов в директо рии	Переимено вание файл	Смена атрибу тов файла
(030)	x-- (01 0)								
d---r-- --	---	-	-	-	-	-	+	-	-
(040)	x-- (01 0)								
d---r- x--	---	-	-	-	-	+	+	-	+
(050)	x-- (01 0)								
d---rw- --	---	-	-	-	-	-	+	-	-
(060)	x-- (01 0)								
d--- rwx--	---	+	+	-	-	+	+	+	+
(070)	x-- (01 0)								
d----- --	---	-	-	-	-	-	-	-	-
(000)	w-- -- (02 0)								
d----- x--	---	-	-	+	-	-	-	-	+
(010)	w-- -- (02 0)								
d----w- --	---	-	-	-	-	-	-	-	-
(020)	w-- -- (02 0)								
d---- wx--	---	+	+	+	-	+	-	+	+

Права директо рии	Пра ва фай ла	Созда ние файла	Удале ние файла	Зап ись в фай л	Чтен ие фай ла	Смена директо рии	Просмо тр файлов в директо рии	Переимено вание файл	Смена атрибу тов файла
(030)	w-- — (02 0)								
d---r-- --	---	-	-	-	-	-	+	-	-
(040)	w-- — (02 0)								
d---r- x--	---	-	-	+	-	+	+	-	+
(050)	w-- — (02 0)								
d---rw- --	---	-	-	-	-	-	+	-	-
(060)	w-- — (02 0)								
d--- rwx--	---	+	+	+	-	+	+	+	+
(070)	w-- — (02 0)								
d----- --	---	-	-	-	-	-	-	-	-
(000)	wx- — (03 0)								
d----- x--	---	-	-	+	-	-	-	-	+
(010)	wx- — (03 0)								
d----w- --	---	-	-	-	-	-	-	-	-
(020)	wx-								

Права директо рии	Пра ва фай ла	Созда ние файла	Удале ние файла	Зап ись в фай л	Чтен ие фай ла	Смена директо рии	Просмо тр файлов в директо рии	Переимено вание файл	Смена атрибу тов файла
	— (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)								

Права директо рии	Пра ва фай ла	Созда ние файла	Удале ние файла	Зап ись в фай л	Чтен ие фай ла	Смена директо рии	Просмо тр файлов в директо рии	Переимено вание файл	Смена атрибу тов файла
d----w- -- (020)	--- -r- --- (04 0)	-	-	-	-	-	-	-	-
d---- wx-- (030)	--- -r- --- (04 0)	+	+	-	+	+	-	+	+
d---r-- -- (040)	--- -r- --- (04 0)	-	-	-	-	-	+	-	-
d---r- x-- (050)	--- -r- --- (04 0)	-	-	-	+	+	+	-	+
d---rw- -- (060)	--- -r- --- (04 0)	-	-	-	-	-	+	-	-
d--- rwx-- (070)	--- -r- --- (04 0)	+	+	-	+	+	+	+	+
d----- -- (000)	--- -r- x-- (05 0)	-	-	-	-	-	-	-	-
d----- x-- (010)	--- -r- x-- (05 0)	-	-	-	+	+	-	-	+
d----w- -- (020)	--- -r- x--	-	-	-	-	-	-	-	-

Права директо рии	Пра ва фай ла	Созда ние файла	Удале ние файла	Зап ись в фай л	Чтен ие фай ла	Смена директо рии	Просмо тр файлов в директо рии	Переимено вание файл	Смена атрибу тов файла
	(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- --	-	-	-	-	-	-	-	-

Права директо рии	Пра ва фай ла	Созда ние файла	Удале ние файла	Зап ись в фай л	Чтен ие фай ла	Смена директо рии	Просмо тр файлов в директо рии	Переимено вание файл	Смена атрибу тов файла
	(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)	-	-	+	+	+	-	-	+

Права директо рии	Пра ва фай ла	Созда ние файла	Удале ние файла	Зап ись в фай л	Чтен ие фай ла	Смена директо рии	Просмо тр файлов в директо рии	Переимено вание файл	Смена атрибу тов файла
	0)								
d----w- -- (020)	--- - rwx -- (07 0)	-	-	-	-	-	-	-	-
d---- wx-- (030)	--- - rwx -- (07 0)	+	+	+	+	+	-	+	+
d---r-- -- (040)	--- - rwx -- (07 0)	-	-	-	-	-	+	-	-
d---r- x-- (050)	--- - rwx -- (07 0)	-	-	+	+	+	+	-	+
d---rw- -- (060)	--- - rwx -- (07 0)	-	-	-	-	-	+	-	-
d--- rwx-- (070)	--- - rwx -- (07 0)	+	+	+	+	+	+	+	+

Таблица 3.1 «Установленные права и разрешённые действия для групп»

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»

Выводы

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

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