

# Лабораторная работа No 3

Дискреционное разграничение прав в Linux.  
Два пользователя

Выполнила: Белкина Анастасия Михайловна, НБИбд-01-18

Преподаватель: Кулябов Дмитрий Сергеевич

# Цель работы

---

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

## Задание

---

1. Добавить пользователя guest2
2. Создать пароль для пользователя guest2
3. Добавить guest2 в группу guest
4. Опытным путём заполнить таблицу "Установленные права и разрешённые действия"
5. На основании заполненной таблицы определить те или иные минимально необходимые права для выполнения операций внутри директории

## Теоретическое введение

---

В операционной системе Linux есть много отличных функций безопасности, но она из самых важных - это система прав доступа к файлам. Linux, как последователь идеологии ядра Linux в отличие от Windows, изначально проектировался как многопользовательская система, поэтому права доступа к файлам в linux продуманы очень хорошо.

И это очень важно, потому что локальный доступ к файлам для всех программ и всех пользователей позволил бы вирусам без проблем уничтожить систему. Но новым пользователям могут показаться очень сложными новые права на файлы в linux, которые очень сильно отличаются от того, что мы привыкли видеть в Windows. В этой статье мы попытаемся разобраться в том как работают права файлов в linux, а также как их изменять и устанавливать.

Изначально каждый файл имел три параметра доступа. Вот они:

Чтение - разрешает получать содержимое файла, но на запись нет. Для каталога позволяет получить список файлов и каталогов, расположенных в нем;

Запись - разрешает записывать новые данные в файл или изменять существующие, а также позволяет создавать и изменять файлы и каталоги;

Выполнение - вы не можете выполнить программу, если у нее нет флага выполнения. Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система может понять, что этот файл нужно запускать как программу.

Но все эти права были бы бессмысленными, если бы применялись сразу для всех пользователей. Поэтому каждый файл имеет три категории пользователей, для которых можно устанавливать различные сочетания прав доступа:

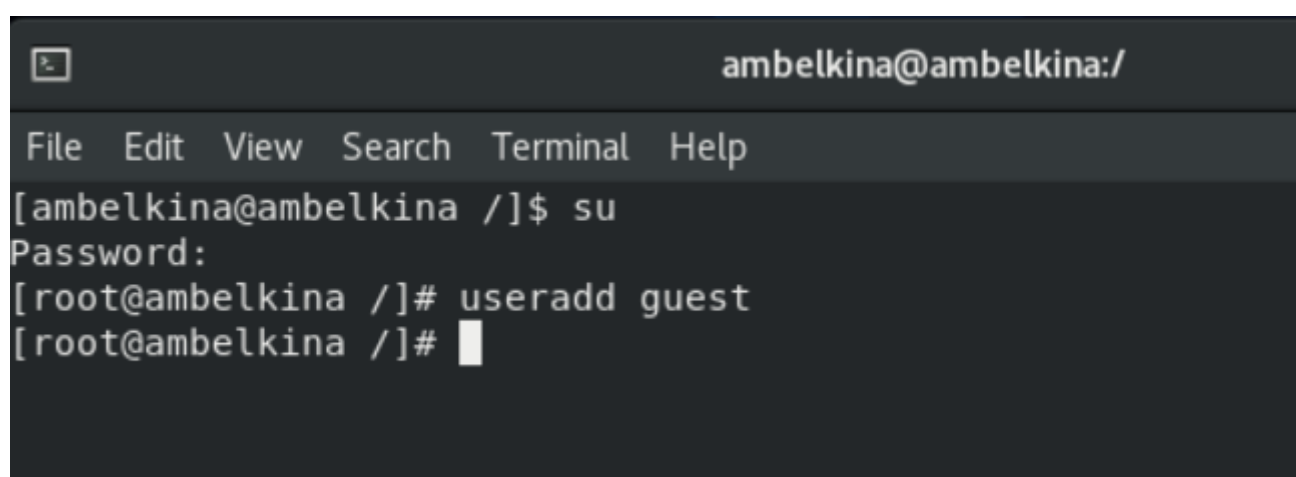
Владелец - набор прав для владельца файла, пользователя, который его создал или сейчас установлен его владельцем. Обычно владелец имеет все права, чтение, запись и выполнение. Группа - любая группа пользователей, существующая в системе и привязанная к файлу. Но это может быть только одна группа и обычно это группа владельца, хотя для файла можно назначить и другую группу. Остальные - все пользователи, кроме владельца и пользователей, входящих в группу файла. Именно с помощью

этих наборов полномочий устанавливаются права файлов в linux. Каждый пользователь может получить полный доступ только к файлам, владельцем которых он является или к тем, доступ к которым ему разрешен. Только пользователь Root может работать со всеми файлами независимо от их набора полномочий.

Но со временем такой системы стало не хватать и было добавлено еще несколько флагов, которые позволяют делать файлы не изменяемыми или же выполнять от имени суперпользователя

## Выполнение лабораторной работы

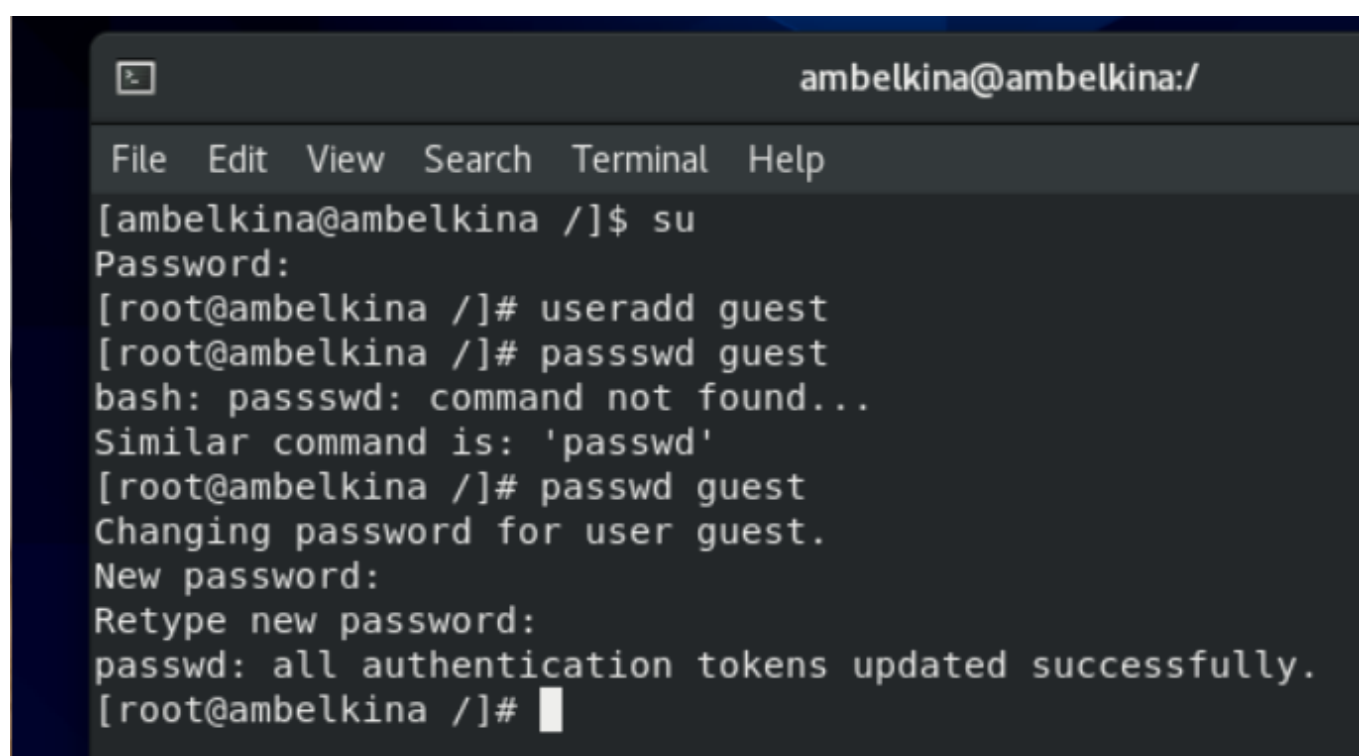
1. В установленной при выполнении предыдущей лабораторной работы операционной системе создала учётную запись пользователя guest (используя учётную запись администратора): `useradd guest`



```
ambelkina@ambelkina:/  
File Edit View Search Terminal Help  
[ambelkina@ambelkina /]$ su  
Password:  
[root@ambelkina /]# useradd guest  
[root@ambelkina /]#
```

Рис.1 Создался юзер guest

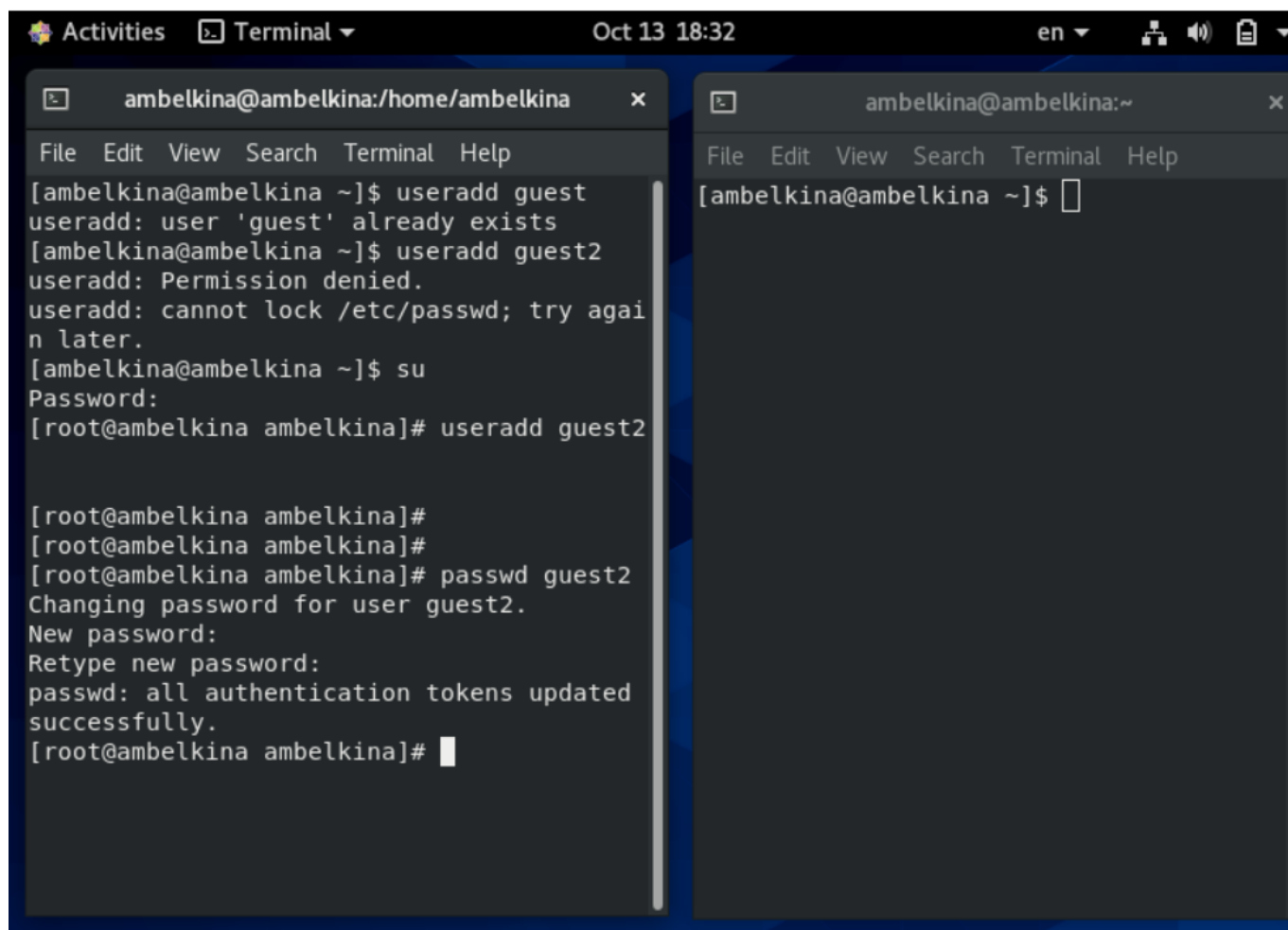
2. Задала пароль для пользователя guest (используя учётную запись администратора): `passwd guest`



```
ambelkina@ambelkina:/  
File Edit View Search Terminal Help  
[ambelkina@ambelkina /]$ su  
Password:  
[root@ambelkina /]# useradd guest  
[root@ambelkina /]# passwd guest  
bash: passwd: command not found...  
Similar command is: 'passwd'  
[root@ambelkina /]# passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@ambelkina /]#
```

Рис.2 Задала пароль

3. Аналогично создала второго пользователя guest2.



The image shows two terminal windows from the Ubuntu desktop environment. The left window, titled 'ambelkina@ambelkina:/home/ambelkina', shows the user 'ambelkina' attempting to create 'guest2' with 'useradd', which fails due to a permission error. The user then switches to root with 'su', successfully creates 'guest2' with 'useradd', and sets a password with 'passwd guest2'. The right window, titled 'ambelkina@ambelkina:~', shows the user 'ambelkina' at the prompt, waiting for input.

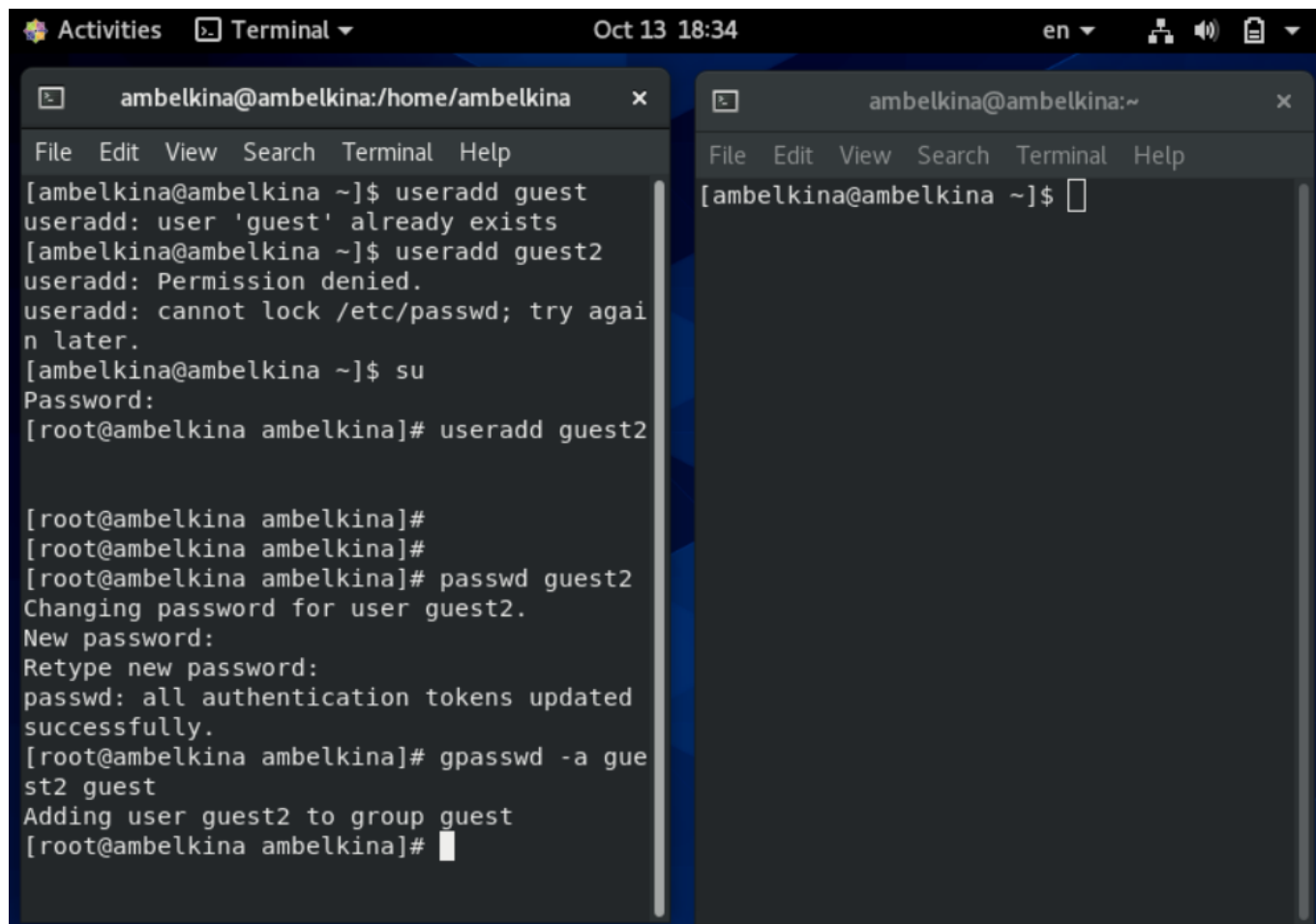
```
ambelkina@ambelkina:/home/ambelkina
File Edit View Search Terminal Help
[ambelkina@ambelkina ~]$ useradd guest
useradd: user 'guest' already exists
[ambelkina@ambelkina ~]$ useradd guest2
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
[ambelkina@ambelkina ~]$ su
Password:
[root@ambelkina ambelkina]# useradd guest2

[root@ambelkina ambelkina]#
[root@ambelkina ambelkina]#
[root@ambelkina ambelkina]# passwd guest2
Changing password for user guest2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ambelkina ambelkina]#

ambelkina@ambelkina:~
File Edit View Search Terminal Help
[ambelkina@ambelkina ~]$
```

Рис.3 Создался второй юзер

4. Добавила пользователя guest2 в группу guest: `gpasswd -a guest2 guest`



The screenshot shows two terminal windows. The left window, titled 'ambelkina@ambelkina:/home/ambelkina', shows the following commands and output:

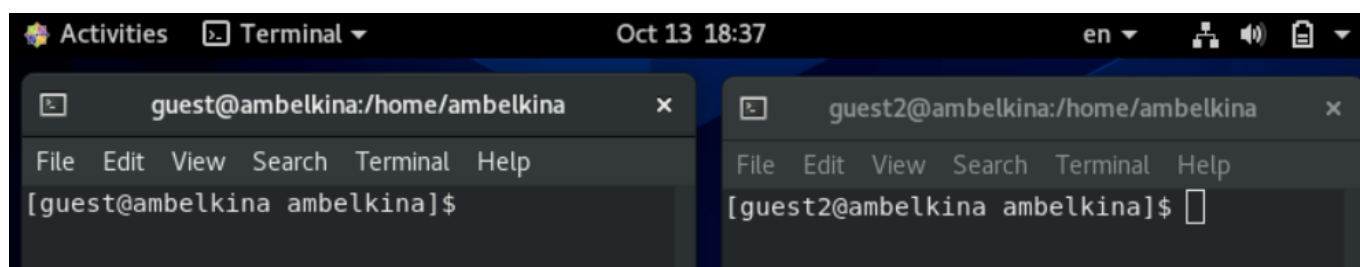
```
[ambelkina@ambelkina ~]$ useradd guest
useradd: user 'guest' already exists
[ambelkina@ambelkina ~]$ useradd guest2
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
[ambelkina@ambelkina ~]$ su
Password:
[root@ambelkina ambelkina]# useradd guest2

[root@ambelkina ambelkina]#
[root@ambelkina ambelkina]#
[root@ambelkina ambelkina]# passwd guest2
Changing password for user guest2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ambelkina ambelkina]# gpasswd -a guest2 guest
Adding user guest2 to group guest
[root@ambelkina ambelkina]#
```

The right window, titled 'ambelkina@ambelkina:~', shows the prompt [ambelkina@ambelkina ~]\$ and a cursor.

Рис.4 Добавление в группу

5. Осуществила вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли.

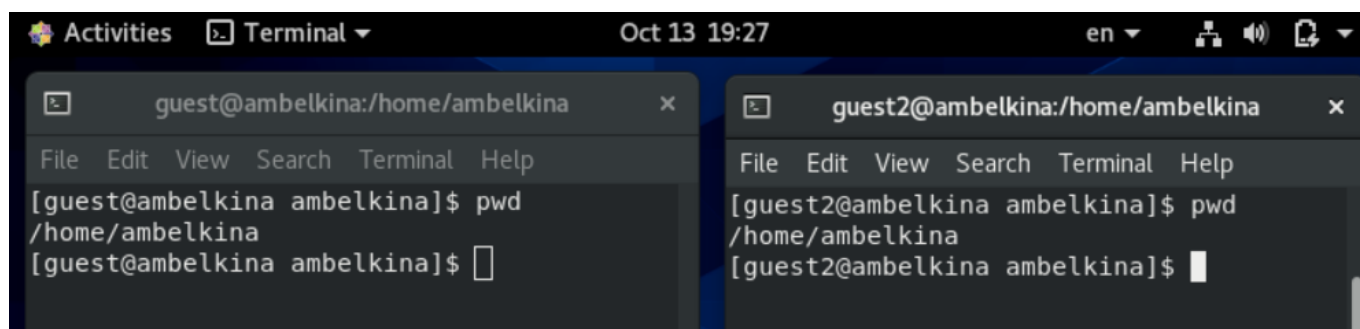


The screenshot shows two terminal windows. The left window, titled 'guest@ambelkina:/home/ambelkina', shows the prompt [guest@ambelkina ambelkina]\$.

The right window, titled 'guest2@ambelkina:/home/ambelkina', shows the prompt [guest2@ambelkina ambelkina]\$ and a cursor.

Рис.5 Две консоли

6. Для обоих пользователей командой pwd определила директорию, в которой нахожусь.



The screenshot shows two terminal windows. The left window, titled 'guest@ambelkina:/home/ambelkina', shows the following commands and output:

```
[guest@ambelkina ambelkina]$ pwd
/home/ambelkina
[guest@ambelkina ambelkina]$
```

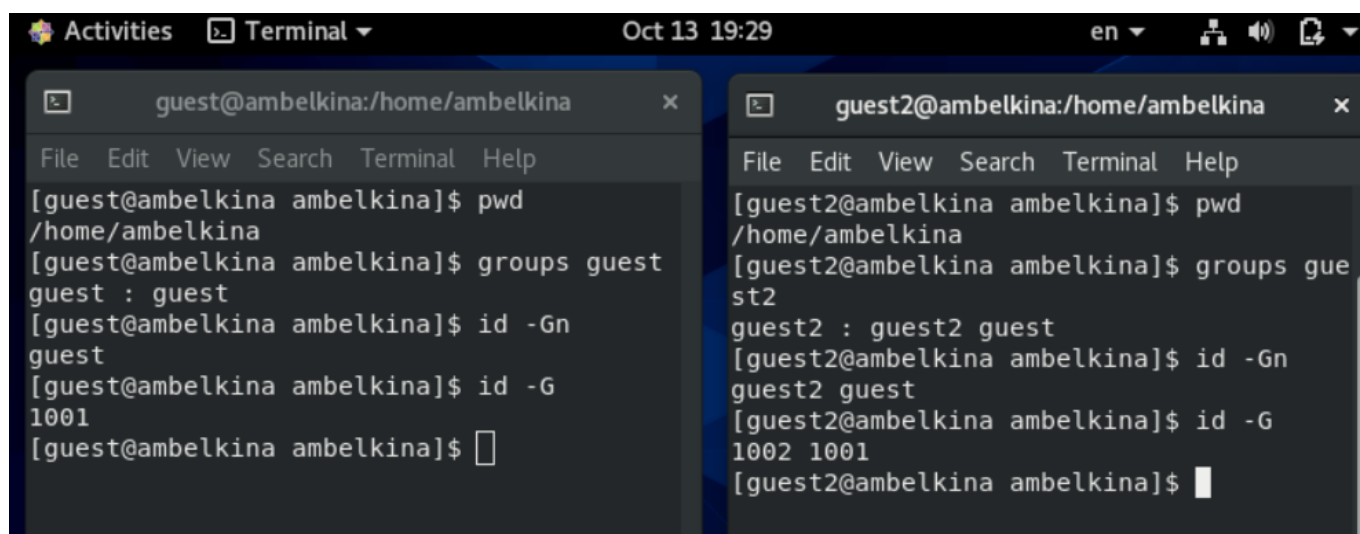
The right window, titled 'guest2@ambelkina:/home/ambelkina', shows the following commands and output:

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

Рис.6 Определенные директории

7. Уточнила имя 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`.



The image shows two terminal windows side-by-side. The left window is for user 'guest' and the right for 'guest2'. Both show the output of 'pwd', 'groups', 'id -Gn', and 'id -G' commands.

```
guest@ambelkina:/home/ambelkina
[guest@ambelkina ambelkina]$ pwd
/home/ambelkina
[guest@ambelkina ambelkina]$ groups guest
guest : guest
[guest@ambelkina ambelkina]$ id -Gn
guest
[guest@ambelkina ambelkina]$ id -G
1001
[guest@ambelkina ambelkina]$

guest2@ambelkina:/home/ambelkina
[guest2@ambelkina ambelkina]$ pwd
/home/ambelkina
[guest2@ambelkina ambelkina]$ groups guest2
guest2 : guest2 guest
[guest2@ambelkina ambelkina]$ id -Gn
guest2 guest
[guest2@ambelkina ambelkina]$ id -G
1002 1001
[guest2@ambelkina ambelkina]$
```

Рис.7 Имена пользователей и группы

8. Сравнила полученную информацию с содержимым файла `/etc/group`. Просмотрела файл командой `cat /etc/group`



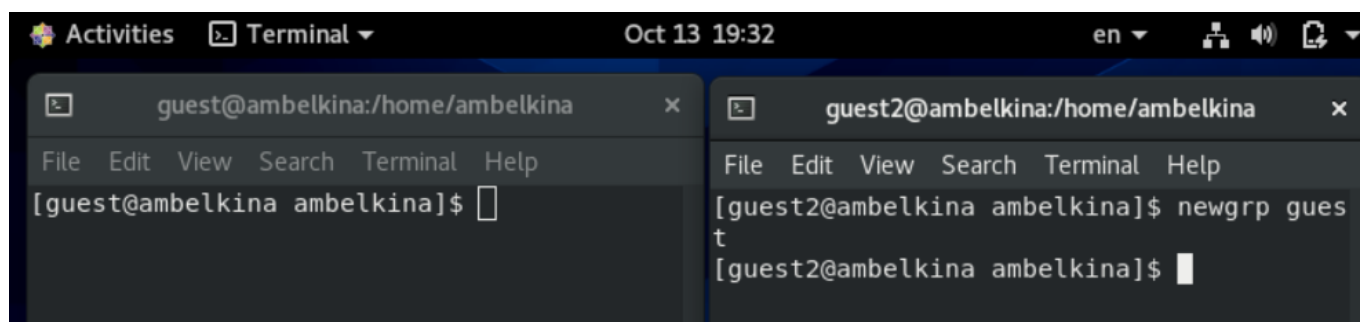
The image shows two terminal windows side-by-side, both displaying the output of the 'cat /etc/group' command.

```
ambelkina:x:1000:
guest:x:1001:guest2
guest2:x:1002:
[guest@ambelkina ambelkina]$

ambelkina:x:1000:
guest:x:1001:guest2
guest2:x:1002:
[guest2@ambelkina ambelkina]$
```

Рис.8 Данные из файла `etc/passwd`

9. От имени пользователя `guest2` выполнила регистрацию пользователя `guest2` в группе `guest` командой `newgrp guest`



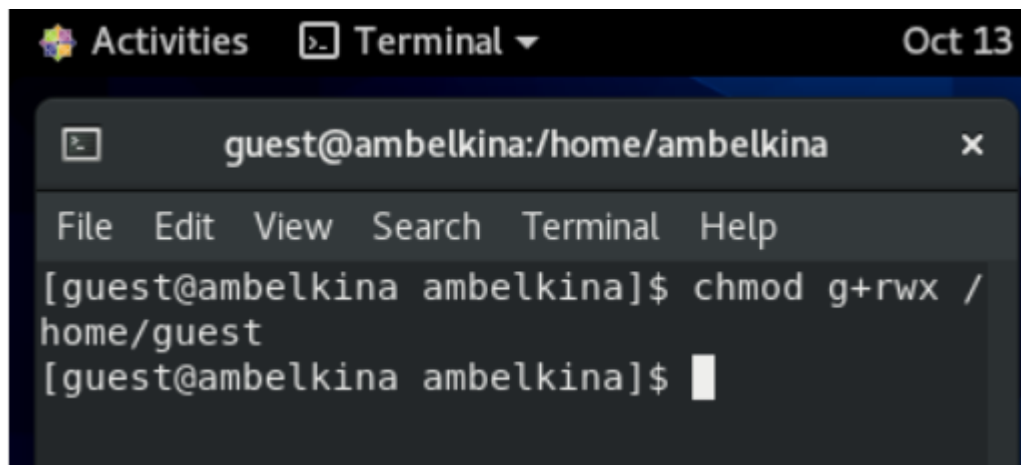
The image shows two terminal windows side-by-side. The left window is idle. The right window shows the execution of the 'newgrp guest' command by user 'guest2'.

```
guest@ambelkina:/home/ambelkina
[guest@ambelkina ambelkina]$

guest2@ambelkina:/home/ambelkina
[guest2@ambelkina ambelkina]$ newgrp guest
[guest2@ambelkina ambelkina]$
```

Рис.9 Зарегистрирован пользователь

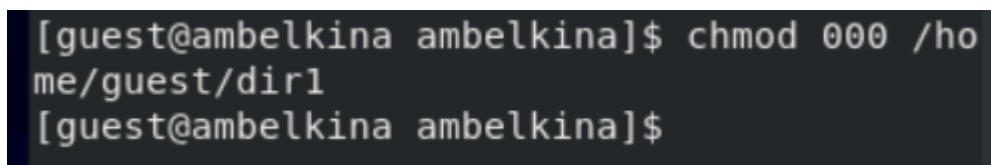
10. От имени пользователя `guest` изменила права директории `/home/guest`, разрешив все действия для пользователей группы: `chmod g+rx /home/guest`

A screenshot of a terminal window titled "Terminal" with a date "Oct 13" in the top right corner. The terminal shows the prompt "guest@ambelkina:/home/ambelkina" and a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The command "chmod g+rx /home/guest" has been entered and executed, resulting in a new prompt line "[guest@ambelkina ambelkina]\$".

```
guest@ambelkina:/home/ambelkina
File Edit View Search Terminal Help
[guest@ambelkina ambelkina]$ chmod g+rx /home/guest
[guest@ambelkina ambelkina]$
```

Рис.10 Измененные права директории

11. От имени пользователя guest сняла с директории /home/guest/dir1 все атрибуты командой `chmod 000 dir1` и проверила правильность снятия атрибутов.

A screenshot of a terminal window showing the command "chmod 000 /home/guest/dir1" being entered and executed. The prompt changes from "guest@ambelkina" to "guest2@ambelkina".

```
[guest@ambelkina ambelkina]$ chmod 000 /home/guest/dir1
[guest2@ambelkina ambelkina]$
```

Рис.11 Снятые права

12. Заполнила таблицу «Установленные права и разрешённые действия», выполняя действия от имени от имени пользователя guest и делая проверку от пользователя guest2, определив опытным путём, какие операции разрешены, а какие нет.

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d-----(000)	----- (0)	-	-	-	-	-	-	-	-
d--x----(100)	----- (0)	-	-	-	-	+	-	-	+
d-w-----(200)	----- (0)	-	-	-	-	-	-	-	-
d---wx--(300)	----- (0)	+	+	-	-	+	-	+	+
dr-----(400)	----- (0)	-	-	-	-	-	+	-	-
dr-x----(500)	----- (0)	-	-	-	-	+	+	-	+
drw-----(600)	----- (0)	-	-	-	-	-	+	-	-
drwx----(700)	----- (0)	+	+	-	-	+	+	+	+
d-----x(000)	--x----- (100)	-	-	-	-	-	-	-	-
d--x----- (100)	--x----- (100)	-	-	-	-	+	-	-	+
d-w-----x(200)	--x----- (100)	-	-	-	-	-	-	-	-
d---wx--x(300)	--x----- (100)	+	+	-	-	+	-	+	+
dr-----x(400)	--x----- (100)	-	-	-	-	-	+	-	-
dr-x-----x(500)	--x----- (100)	-	-	-	-	+	+	-	+
drw-----x(600)	--x----- (100)	-	-	-	-	-	+	-	-
drwx-----x(700)	--x----- (100)	+	+	-	-	+	+	+	+
d-----w(000)	-w----- (200)	-	-	-	-	-	-	-	-
d--x-----w(100)	-w----- (200)	-	-	+	-	+	-	-	+
d-w-----w(200)	-w----- (200)	-	-	-	-	-	-	-	-
d---wx--w(300)	-w----- (200)	+	+	+	-	+	-	+	+
d---r----- (040)	-w----- (200)	-	-	-	-	-	+	-	-
d---r-x-- (050)	-w----- (200)	-	-	+	-	+	+	-	+
d---rw-- (060)	-w----- (200)	-	-	-	-	-	+	-	-
d---rwx-- (070)	-w----- (200)	+	+	+	-	+	+	+	+
d-----wx(000)	-wx----- (300)	-	-	-	-	-	-	-	-
d--x-----wx(100)	-wx----- (300)	-	-	+	-	+	-	-	+
d-w-----wx(200)	-wx----- (300)	-	-	-	-	-	-	-	-
d---wx--wx(300)	-wx----- (300)	+	+	+	-	+	-	+	+
dr-----wx(400)	-wx----- (300)	-	-	-	-	-	+	-	-
dr-x-----wx(500)	-wx----- (300)	-	-	+	-	+	+	-	+
drw-----wx(600)	-wx----- (300)	-	-	-	-	-	+	-	-
drwx-----wx(700)	-wx----- (300)	+	+	+	-	+	+	+	+
d-----r(000)	r----- (400)	-	-	-	-	-	-	-	-
d--x-----r(100)	r----- (400)	-	-	-	+	+	-	-	+
d-w-----r(200)	r----- (400)	-	-	-	-	-	-	-	-
d---wx--r(300)	r----- (400)	+	+	-	+	+	-	+	+
dr-----r(400)	r----- (400)	-	-	-	-	-	+	-	-
dr-x-----r(500)	r----- (400)	-	-	-	+	+	+	-	+
drw-----r(600)	r----- (400)	-	-	-	-	-	+	-	-
drwx-----r(700)	r----- (400)	+	+	-	+	+	+	+	+
d-----rx(000)	r-x----- (500)	-	-	-	-	-	-	-	-
d--x-----rx(100)	r-x----- (500)	-	-	-	+	+	-	-	+
d-w-----rx(200)	r-x----- (500)	-	-	-	-	-	-	-	-
d---wx--rx(300)	r-x----- (500)	+	+	-	+	+	-	+	+
dr-----rx(400)	r-x----- (500)	-	-	-	-	-	+	-	-
dr-x-----rx(500)	r-x----- (500)	-	-	-	+	+	+	-	+
drw-----rx(600)	r-x----- (500)	-	-	-	-	-	+	-	-
drwx-----rx(700)	r-x----- (500)	+	+	-	+	+	+	+	+
d-----rw(000)	rw----- (600)	-	-	-	-	-	-	-	-
d--x-----rw(100)	rw----- (600)	-	-	+	+	+	-	-	+
d-w-----rw(200)	rw----- (600)	-	-	-	-	-	-	-	-
d---wx--rw(300)	rw----- (600)	+	+	+	+	+	-	+	+
dr-----rw(400)	rw----- (600)	-	-	-	-	-	+	-	-
dr-x-----rw(500)	rw----- (600)	-	-	+	+	+	+	-	+
drw-----rw(600)	rw----- (600)	-	-	-	-	-	+	-	-
drwx-----rw(700)	rw----- (600)	+	+	+	+	+	+	+	+
d-----rwx(000)	rw-x----- (700)	-	-	-	-	-	-	-	-
d--x-----rwx(100)	rw-x----- (700)	-	-	+	+	+	-	-	+
d-w-----rwx(200)	rw-x----- (700)	-	-	-	-	-	-	-	-
d---wx--rwx(300)	rw-x----- (700)	+	+	+	+	+	-	+	+
dr-----rwx(400)	rw-x----- (700)	-	-	-	-	-	+	-	-
dr-x-----rwx(500)	rw-x----- (700)	-	-	+	+	+	+	-	+
drw-----rwx(600)	rw-x----- (700)	-	-	-	-	-	+	-	-
drwx-----rwx(700)	rw-x----- (700)	+	+	+	+	+	+	+	+

Табл.1 Установленные права и разрешённые действия



13. На основании заполненной таблицы определила те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1, заполнила таблицу.

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---- (20)
Переименование файла	d----wx--- (030)	----- (000)
Создание поддиректории	d----wx--- (030)	----- (000)
Удаление поддиректории	d----wx--- (030)	----- (000)

Табл.2 Минимально необходимые права

## Выводы

---

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