

# Дискреционное разграничение прав в Linux. Два пользователя

## Содержание

Цель работы .....	1
Теоретическое введение .....	1
Выполнение лабораторной работы .....	2
Атрибуты файлов .....	2
Заполнение таблицы 3.1 .....	4
Заполнение таблицы 3.2 .....	13
Вывод .....	14
Список литературы. Библиография.....	14

## Цель работы

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

## 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/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

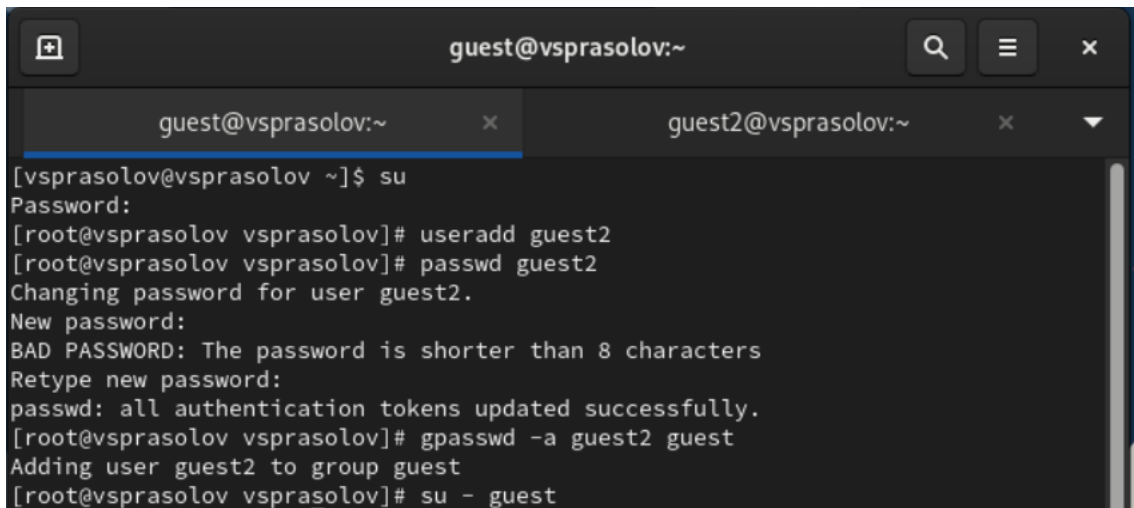
## Выполнение лабораторной работы

### Атрибуты файлов

1. В установленной операционной системе создайте учётную запись пользователя guest2 (используя учётную запись администратора)

guest1 был создан в предыдущей лабораторной.

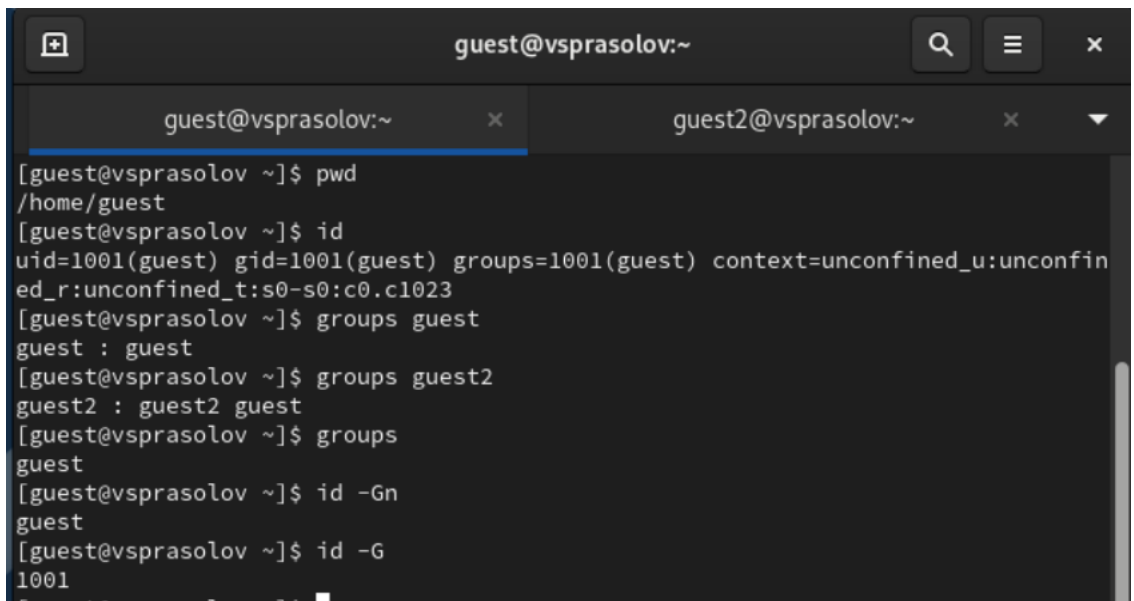
2. Задайте пароль для пользователя guest2
3. Добавьте пользователя guest2 в группу guest:



```
guest@vsprasolov:~  
[vsprasolov@vsprasolov ~]$ su  
Password:  
[root@vsprasolov vsprasolov]# useradd guest2  
[root@vsprasolov vsprasolov]# passwd guest2  
Changing password for user guest2.  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@vsprasolov vsprasolov]# gpasswd -a guest2 guest  
Adding user guest2 to group guest  
[root@vsprasolov vsprasolov]# su - guest
```

(рис. 1. 1-4 пункты задания лабораторной)

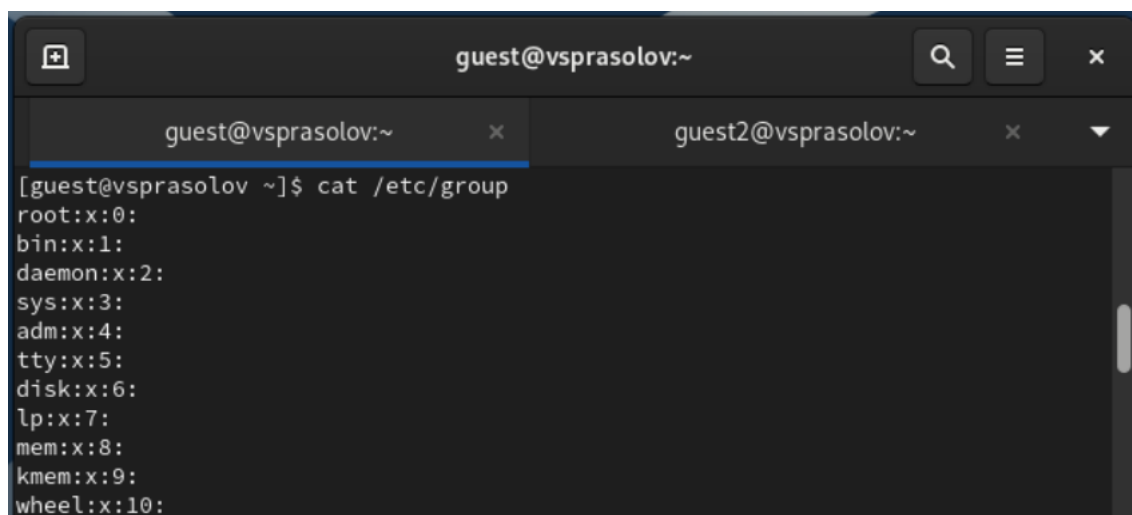
4. Осуществите вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли
5. Для обоих пользователей командой pwd определите директорию, в которой вы находитесь. Сравните её с приглашениями командной строки
6. Уточните имя вашего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определите командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2. Сравните вывод команды groups с выводом команд id -Gn и id -G :



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

(рис. 2. 5-7 пункты задания лабораторной)

7. Сравните полученную информацию с содержимым файла /etc/group :



(рис. 3. 8 пункт задания лабораторной)

8. От имени пользователя guest2 выполните регистрацию пользователя guest2 в группе guest командой `newgrp guest` :
9. От имени пользователя guest измените права директории `/home/guest`, разрешив все действия для пользователей группы: `chmod g+rwX /home/guest`
10. От имени пользователя guest снимите с директории `/home/guest/dir1` все атрибуты командой `chmod 000 dir1` :

### Заполнение таблицы 3.1

11. 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 файла	Смена атрибутов файла
d----- --- (000)	--- --- ---	-	-	-	-	-	-	-	-
d----- x--- (010)	--- --- ---	-	-	-	-	+	-	-	+

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)	--- --- --- - (00 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-----	---	-	-	-	-	+	-	-	+

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
x--- (010)	--- x-- - (01 0)								
d----w- --- (020)	--- --- x-- - (01 0)	-	-	-	-	-	-	-	-
d---- wx--- (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----- ---	--- --	-	-	-	-	-	-	-	-

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
(000)	w-- -- (02 0)								
d----- x--- (010)	--- -- w-- -- (02 0)	-	-	+	-	+	-	-	+
d----w- --- (020)	--- -- w-- -- (02 0)	-	-	-	-	-	-	-	-
d---- wx--- (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--	+	+	+	-	+	+	+	+

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
	-- (02 0)								
d----- --- (000)	--- -- wx-	-	-	-	-	-	-	-	-
	-- (03 0)								
d----- x--- (010)	--- -- wx-	-	-	+	-	+	-	-	+
	-- (03 0)								
d----w- --- (020)	--- -- wx-	-	-	-	-	-	-	-	-
	-- (03 0)								
d---- wx--- (030)	--- -- wx-	+	+	+	-	+	-	+	+
	-- (03 0)								
d---r-- --- (040)	--- -- wx-	-	-	-	-	-	+	-	-
	-- (03 0)								
d---r- x--- (050)	--- -- wx-	-	-	+	-	+	+	-	+
	-- (03 0)								
d---rw- --- (060)	--- -- 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--- 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)	-	-	-	+	+	+	-	+

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---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-- - (05 0)	-	-	-	-	-	-	-	-
d---- wx--- (030)	--- -r- x-- - (05 0)	+	+	-	+	+	-	+	+
d---r-- --- (040)	--- -r- x-- - (05 0)	-	-	-	-	-	+	-	-

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---r- x--- (050)	--- -r- x-- - (05 0)	-	-	-	+	+	+	-	+
d---rw- --- (060)	--- -r- x-- - (05 0)	-	-	-	-	-	+	-	-
d--- rwx--- (070)	--- -r- x-- - (05 0)	+	+	-	+	+	+	+	+
d----- --- (000)	--- - rw- --- (06 0)	-	-	-	-	-	-	-	-
d----- x--- (010)	--- - rw- --- (06 0)	-	-	+	+	+	-	-	+
d----w- --- (020)	--- - rw- --- (06 0)	-	-	-	-	-	-	-	-
d---- wx--- (030)	--- - rw- --- (06 0)	+	+	+	+	+	-	+	+
d---r--	---	-	-	-	-	-	+	-	-

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
---	-								
(040)	rw-								
	---								
	(060)								
d---r-	---	-	-	+	+	+	+	-	+
x---	-								
(050)	rw-								
	---								
	(060)								
d---rw-	---	-	-	-	-	-	+	-	-
---	-								
(060)	rw-								
	---								
	(060)								
d---	---	+	+	+	+	+	+	+	+
rw---	-								
(070)	rw-								
	---								
	(060)								
d-----	---	-	-	-	-	-	-	-	-
---	-								
(000)	rwX								
	---								
	(070)								
d-----	---	-	-	+	+	+	-	-	+
x---	-								
(010)	rwX								
	---								
	(070)								
d----w-	---	-	-	-	-	-	-	-	-
---	-								
(020)	rwX								
	---								
	(070)								
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)	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»

### Заполнение таблицы 3.2

12. 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)

Операция	Права на директорию	Права на файл
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.

## Вывод

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#%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](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)