

Основы информационной безопасности

**Лабораторная работа № 3. Дискреционное разграничение прав в Linux.
Два пользователя**

Сунгурова Мариян Мухсиновна

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
4	Выводы	15
	Список литературы	16

Список иллюстраций

3.1	Создание нового пользователя guest2 и добавление его в группу guest	7
3.2	Создание нового пользователя guest2 и добавление его в группу guest	7
3.3	Создание нового пользователя guest2 и добавление его в группу guest	8
3.4	Создание нового пользователя guest2 и добавление его в группу guest	9
3.5	Создание нового пользователя guest2 и добавление его в группу guest	9
3.6	Создание нового пользователя guest2 и добавление его в группу guest	9

Список таблиц

3.1	Установленные права и разрешённые действия	10
3.2	Минимальные права для совершения операций	13

1 Цель работы

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

2 Теоретическое введение

При работе с командой `chmod` важно понимать основные права доступа, которые назначают файлам или каталогам. В Linux используется три основных типа прав доступа[1]:

- Чтение (Read) — обозначается буквой «r». Предоставляет возможность просматривать содержимое файла или каталога.
- Запись (Write) — обозначается буквой «w». Позволяет создавать, изменять и удалять файлы внутри каталога, а также изменять содержимое файла.
- Выполнение (Execute) — обозначается буквой «x». Дает разрешение на выполнение файла или на вход в каталог.

Каждый из указанных выше типов прав доступа может быть назначен трем группам пользователей:

- Владелец (Owner) — пользователь, который является владельцем файла или каталога.
- Группа (Group) — группа пользователей, к которой принадлежит файл или каталог.
- Остальные пользователи (Others) — все остальные пользователи системы.

Комбинация этих базовых прав доступа для каждой из групп пользователей определяет полный набор прав доступа для файла или каталога.

3 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы ОС создадим учетную запись пользователя guest2 и добавляем его в группу guest (рис. fig. 3.1 – fig. 3.2)

```
[mmsungurova@mmsungurova ~]$ sudo useradd guest2
[sudo] пароль для mmsungurova:
[mmsungurova@mmsungurova ~]$ passwd guest2
passwd: только root может выбрать имя учетной записи.
[mmsungurova@mmsungurova ~]$ sudo passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[mmsungurova@mmsungurova ~]$
```

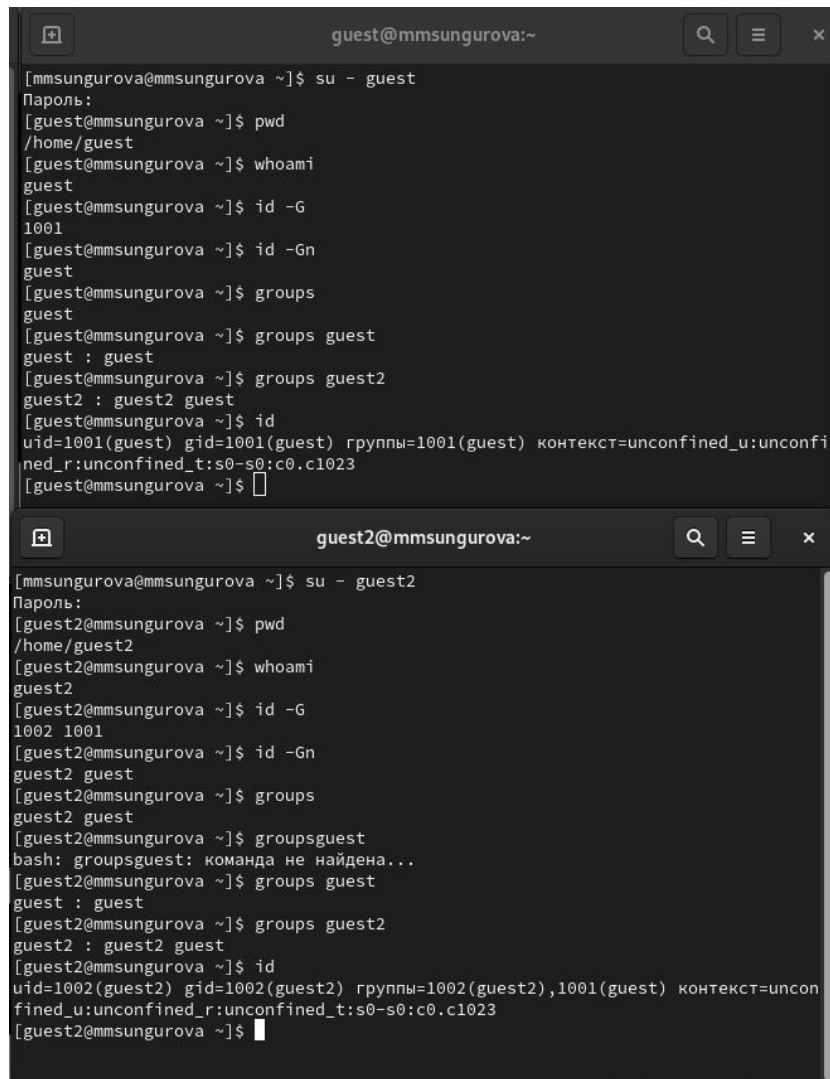
Рис. 3.1: Создание нового пользователя guest2 и добавление его в группу guest

```
[mmsungurova@mmsungurova ~]$ sudo gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[mmsungurova@mmsungurova ~]$
```

Рис. 3.2: Создание нового пользователя guest2 и добавление его в группу guest

1. Осуществим вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли. Далее для обоих пользователей командой pwd определим директорию, в которой находимся. Увидим, что она совпадает с приглашениями командной строки. Увидим, что guest принадлежит одной группе guet с id 2001, а двум группам guest и guest2 с id 1001 и 1002. С помощью команд id -Gn и id -G можно увидеть только id существующих групп и название соответственно

2. Уточним имя 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`. Увидим, что `guest` принадлежит одной группе `guet` с `ig 2001`, а двум группам `guest` и `guest2` с `id 1001` и `1002`. С помощью команд `id -Gn` и `id -G` можно увидеть только `id` существующих групп и название соответственно (рис. fig. 3.3)



```
guest@mmsungurova:~$ su - guest
Пароль:
[guest@mmsungurova ~]$ pwd
/home/guest
[guest@mmsungurova ~]$ whoami
guest
[guest@mmsungurova ~]$ id -G
1001
[guest@mmsungurova ~]$ id -Gn
guest
[guest@mmsungurova ~]$ groups
guest
[guest@mmsungurova ~]$ groups guest
guest : guest
[guest@mmsungurova ~]$ groups guest2
guest2 : guest2 guest
[guest@mmsungurova ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@mmsungurova ~]$

guest2@mmsungurova:~$ su - guest2
Пароль:
[guest2@mmsungurova ~]$ pwd
/home/guest2
[guest2@mmsungurova ~]$ whoami
guest2
[guest2@mmsungurova ~]$ id -G
1002 1001
[guest2@mmsungurova ~]$ id -Gn
guest2 guest
[guest2@mmsungurova ~]$ groups
guest2 guest
[guest2@mmsungurova ~]$ groupsguest
bash: groupsguest: команда не найдена...
[guest2@mmsungurova ~]$ groups guest
guest : guest
[guest2@mmsungurova ~]$ groups guest2
guest2 : guest2 guest
[guest2@mmsungurova ~]$ id
uid=1002(guest2) gid=1002(guest2) группы=1002(guest2),1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@mmsungurova ~]$
```

Рис. 3.3: Создание нового пользователя `guest2` и добавление его в группу `guest`

3. Сравним полученную информацию с содержимым файла `/etc/group`, просмотрев файл командой `cat /etc/group`


```
[guest2@mmsungurova ~]$ cat /etc/group | grep guest
guest:x:1001:guest2
guest2:x:1002:
[guest2@mmsungurova ~]$
```

Рис. 3.4: Создание нового пользователя guest2 и добавление его в группу guest

4. От имени пользователя guest2 выполним регистрацию пользователя guest2 в группе guest командой `newgrp guest`

```
[guest2@mmsungurova ~]$ newgrp guest
[guest2@mmsungurova ~]$
```

Рис. 3.5: Создание нового пользователя guest2 и добавление его в группу guest

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

```
[guest@mmsungurova ~]$ chmod 000 dir1
[guest@mmsungurova ~]$ ls -l dir1
ls: невозможно открыть каталог 'dir1': Отказано в доступе
[guest@mmsungurova ~]$ ls -l
итого 0
d-----, 2 guest guest 6 сен 11 21:14 dir1
[guest@mmsungurova ~]$
```

Рис. 3.6: Создание нового пользователя guest2 и добавление его в группу guest

В табл. 3.1 приведены данные о том, какие операции разрешены, а какие нет для владельца данных.

Таблица 3.1: Установленные права и разрешённые действия

Права дирек- тории	Права файла	Про- смотр							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- то- рии	фай- лов в ди- рек- то- рии	Пере- име- нова- ние фай- ла	Сме- на атри- бутов фай- ла
d(000)	(000)	-	-	-	-	-	-	-	-
d(010)	(000)	-	-	-	-	+	-	-	-
d(020)	(000)	-	-	-	-	-	-	-	-
d(030)	(000)	+	+	-	-	+	-	+	-
d(040)	(000)	-	-	-	-	-	+	-	-
d(050)	(000)	-	-	-	-	+	+	-	-
d(060)	(000)	-	-	-	-	-	+	-	-
d(070)	(000)	+	+	-	-	+	+	+	-
d(000)	(010)	-	-	-	-	-	-	-	-
d(010)	(010)	-	-	-	-	+	-	-	-
d(020)	(010)	-	-	-	-	-	-	-	-
d(030)	(010)	+	+	-	-	+	-	+	-
d(040)	(010)	-	-	-	-	-	+	-	-
d(050)	(010)	-	-	-	-	+	+	-	-
d(060)	(010)	-	-	-	-	-	+	-	-
d(070)	(010)	+	+	-	-	+	+	+	-
d(000)	(020)	-	-	-	-	-	-	-	-
d(010)	(020)	-	-	+	-	+	-	-	-
d(020)	(020)	-	-	-	-	-	-	-	-

		Про- смотр							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- то- рии	фай- лов в ди- рек- то- рии	Пере- име- нова- ние фай- ла	Сме- на атри- бутов фай- ла
Права дирек- тории	Права файла								
d(030)	(020)	+	+	+	-	+	-	+	-
d(040)	(020)	-	-	-	-	-	+	-	-
d(050)	(020)	-	-	+	-	+	+	-	-
d(060)	(020)	-	-	-	-	-	+	-	-
d(070)	(020)	+	+	+	-	+	+	+	-
d(000)	(030)	-	-	-	-	-	-	-	-
d(010)	(030)	-	-	+	-	+	-	-	-
d(020)	(030)	-	-	-	-	-	-	-	-
d(030)	(030)	+	+	+	-	+	-	+	-
d(040)	(030)	-	-	-	-	-	+	-	-
d(050)	(030)	-	-	+	-	+	+	-	-
d(060)	(030)	-	-	-	-	-	+	-	-
d(070)	(030)	+	+	+	-	+	+	+	-
d(000)	(040)	-	-	-	-	-	-	-	-
d(010)	(040)	-	-	-	+	+	-	-	-
d(020)	(040)	-	-	-	-	-	-	-	-
d(030)	(040)	+	+	-	+	+	-	+	-
d(040)	(040)	-	-	-	-	-	+	-	-
d(050)	(040)	-	-	-	+	+	+	-	-
d(060)	(040)	-	-	-	-	-	+	-	-
d(070)	(040)	+	+	-	+	+	+	+	-

		Про- смотр							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- то- рии	фай- лов в ди- рек- то- рии	Пере- име- нова- ние фай- ла	Сме- на атри- бутов фай- ла
Права дирек- тории	Права файла								
d(000)	(050)	-	-	-	-	-	-	-	-
d(010)	(050)	-	-	-	+	+	-	-	-
d(020)	(050)	-	-	-	-	-	-	-	-
d(030)	(050)	+	+	-	+	+	-	+	-
d(040)	(050)	-	-	-	-	-	+	-	-
d(050)	(050)	-	-	-	+	+	+	-	-
d(060)	(050)	-	-	-	-	-	+	-	-
d(070)	(050)	+	+	-	+	+	+	+	-
d(000)	(060)	-	-	-	-	-	-	-	-
d(010)	(060)	-	-	+	+	+	-	-	-
d(020)	(060)	-	-	-	-	-	-	-	-
d(030)	(060)	+	+	+	+	+	-	+	-
d(040)	(060)	-	-	-	-	-	+	-	-
d(050)	(060)	-	-	+	+	+	+	-	-
d(060)	(060)	-	-	-	-	-	+	-	-
d(070)	(060)	+	+	+	+	+	+	+	-
d(000)	(070)	-	-	-	-	-	-	-	-
d(010)	(070)	-	-	+	+	+	-	-	-
d(020)	(070)	-	-	-	-	-	-	-	-
d(030)	(070)	+	+	+	+	+	-	+	-
d(040)	(070)	-	-	-	-	-	+	-	-

						Про- смотр			
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- то- рии	фай- лов в ди- рек- то- рии	Пере- име- нова- ние фай- ла	Сме- на атри- бутов фай- ла
Права дирек- тории	Права файла								
d(050)	(070)	-	-	+	+	+	+	-	-
d(060)	(070)	-	-	-	-	-	+	-	-
d(070)	(070)	+	+	+	+	+	+	+	-

В табл. 3.2 приведены данные о том, какие минимальные права должны быть для совершения различных действий.

Таблица 3.2: Минимальные права для совершения операций

Операция	Минимальные	
	права на директорию	Минимальные права на файл
Создание файла	d(030)	(000)
Удаление файла	d(030)	(000)
Чтение файла	d(010)	(040)
Запись в файл	d(010)	(020)
Переименование файла	d(030)	(000)
Создание поддиректории	d(030)	(000)
Удаление поддиректории	d(030)	(000)

При сравнении с таблицей в лабораторной работе №2 можно увидеть, что отличие состоит только в том, что не владелец файла никогда не имеет прав на изме-

нение его атрибутов. Менять права может владелец файла или администратор[2]. Члены группы файла никаких особых прав на inode не имеют. Пользователь может отобрать у себя собственные права на чтение и запись в файл, но право на запись в inode (в т.ч. право на смену прав) сохраняется у владельца файла при любых обстоятельствах. Пользователь не может передать право собственности на файл другому пользователю и не может забрать право собственности на файл у другого пользователя.

4 Выводы

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

Список литературы

1. Граннеман С. Скотт Граннеман: Linux. Карманный справочник. 2-е изд. Вильямс, 2019. 464 с.
2. Параллельные вычисления в УрО РАН Параллельные вычисления в УрО РАН. Материалы к спецкурсу ОС (Unix). Inode и каталоги [Электронный ресурс]. Red Hat, Inc., 2020. URL: <https://parallel.uran.ru/node/382>.