

Основы информационной безопасности

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

Демидова Екатерина Алексеевна

Содержание

1	Цель работы	4
2	Теоретические сведения	5
3	Выполнение лабораторной работы	6
4	Выводы	14
	Список литературы	15

Список иллюстраций

3.1	Создание нового пользователя guest2 и добавление его в группу guest	6
3.2	Просмотр информации о группах пользователей	7
3.3	Просмотр информации о группах пользователей в файле /etc/group	7
3.4	Изменение прав доступа	8
3.5	Изменение прав доступа	8

1 Цель работы

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

2 Теоретические сведения

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.

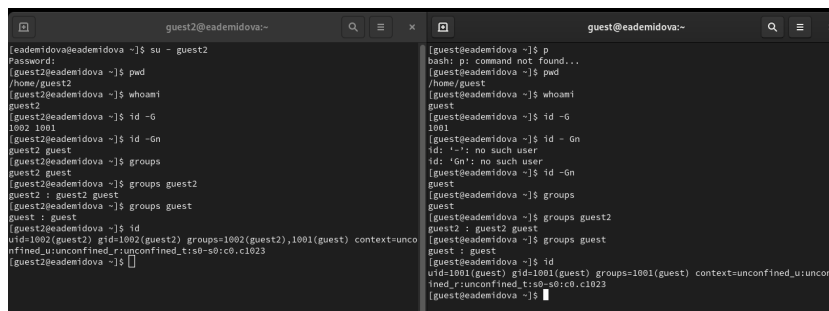
3 Выполнение лабораторной работы

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

```
[eademidova@eademidova ~]$ su -  
Password:  
[root@eademidova ~]# useradd guest2  
[root@eademidova ~]# passwd guest2  
Changing password for user guest2.  
New password:  
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@eademidova ~]# gpasswd -a guest2 guest  
Adding user guest2 to group guest  
[root@eademidova ~]#
```

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

Осуществим вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли. Для обоих пользователей командой pwd определим директорию, в которой находимся, увидим, что она совпадает с приглашениями командной строки. Уточните 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. 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(рис. 3.2)

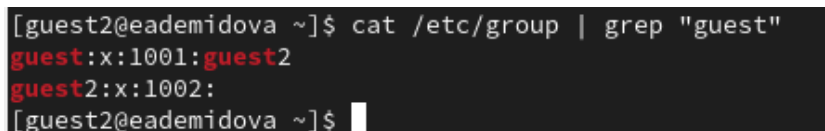


The image shows two terminal windows side-by-side. The left window is titled 'guest2@eademidova:~' and shows the following commands and output:
eadeimidova@eadeimidova ~\$ su - guest2
password:
guest2@eadeimidova ~\$ pwd
/home/guest2
guest2@eadeimidova ~\$ whoami
guest2
guest2@eadeimidova ~\$ id -G
1002 1001
guest2@eadeimidova ~\$ id -Gn
guest2 : guest
guest2@eadeimidova ~\$ groups guest2
guest2 : guest2 guest
guest2@eadeimidova ~\$ groups guest
guest : guest
guest2@eadeimidova ~\$ id
uid=1002(guest2) gid=1002(guest2) groups=1002(guest2),1001(guest) context=unconfined_u:unconfined_t:unconfined_t:s0-s0:c0.c1023
guest2@eadeimidova ~\$

The right window is titled 'guest@eadeimidova:~' and shows the following commands and output:
[guest@eadeimidova ~]\$ p
bash: p: command not found...
[guest@eadeimidova ~]\$ pwd
/home/guest
[guest@eadeimidova ~]\$ whoami
guest
[guest@eadeimidova ~]\$ id -G
1001
[guest@eadeimidova ~]\$ id -Gn
id: 'Gn': no such user
id: 'Gn': no such user
[guest@eadeimidova ~]\$ id -Gn
guest
[guest@eadeimidova ~]\$ groups guest
guest
[guest@eadeimidova ~]\$ groups guest2
guest2 : guest2 guest
[guest@eadeimidova ~]\$ groups guest
guest : guest
[guest@eadeimidova ~]\$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_t:unconfined_t:s0-s0:c0.c1023
[guest@eadeimidova ~]\$

Рис. 3.2: Просмотр информации о группах пользователей

Посмотрев информацию о группах этих пользователей в файле `/etc/group` получим аналогичную информацию(рис. 3.3)



The image shows a terminal window with the following command and output:
[guest2@eadeimidova ~]\$ cat /etc/group | grep "guest"
guest:x:1001:guest2
guest2:x:1002:
[guest2@eadeimidova ~]\$

Рис. 3.3: Просмотр информации о группах пользователей в файле `/etc/group`

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

От имени пользователя `guest` изменим права директории `/home/guest`, разрешив все действия для пользователей группы и снимем с директории `/home/guest/dir1` все атрибуты, затем проверим правильность атрибутов(рис. 3.4, 3.5).

```

[guest@eademidova ~]$ chmod g+rwX /home/guest
[guest@eademidova ~]$ chmod 000 dir1
[guest@eademidova ~]$ ls -l dir1/
ls: cannot open directory 'dir1/': Permission denied
[guest@eademidova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Desktop
d------. 2 guest guest 34 Jun 30 22:01 dir1
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Documents
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Downloads
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Music
drwxr-xr-x. 2 guest guest 53 Jun 30 18:41 Pictures
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Public
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Templates
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Videos
[guest@eademidova ~]$

```

Рис. 3.4: Изменение прав доступа

```

[guest@eademidova ~]$ ls -l /home/guest
[guest@eademidova ~]$ ls -l /home/guest
total 0
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Desktop
d---rwx---. 3 guest guest 31 Jul 3 23:16 dir1
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Documents
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Downloads
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Music
drwxr-xr-x. 2 guest guest 53 Jun 30 18:41 Pictures
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Public
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Templates
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Videos
[guest@eademidova ~]$

```

Рис. 3.5: Изменение прав доступа

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

		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)	(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 изменение его атрибутов. Менять права доступа (записывать в inode) 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 работы были приобретены 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>.