

Дискреционное разграничение прав в Linux. Основные атрибуты

Князьков Геннадий НБИ-01-19¹

19 сентября, 2022, Москва, Россия

¹Российский Университет Дружбы Народов

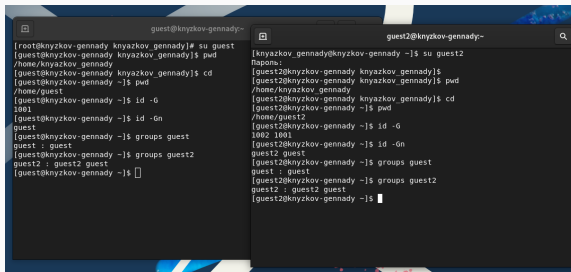
Цели и задачи работы

Цель лабораторной работы

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

Процесс выполнения лабораторной работы

Определяем UID и группу двух пользователей



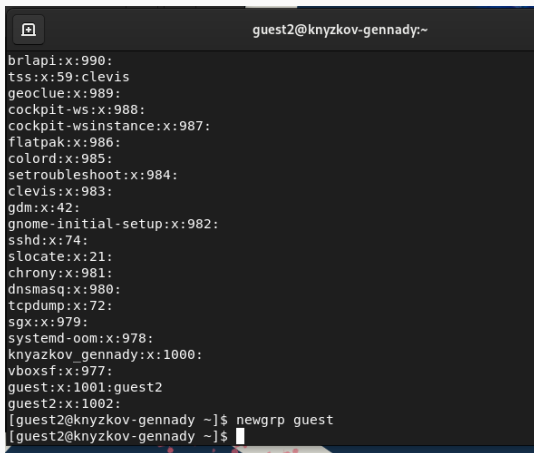
The image shows two terminal windows side-by-side. The left window is titled 'guest@knyzkov-gennady:-' and shows the process of switching to the 'guest' user and checking their details. The right window is titled 'guest2@knyzkov-gennady:-' and shows the process of switching to the 'guest2' user and checking their details.

```
guest@knyzkov-gennady:-  
[root@knyzkov-gennady knyazkov_gennady]# su guest  
[guest@knyzkov-gennady knyazkov_gennady]$ pwd  
/home/knyazkov_gennady  
[guest@knyzkov-gennady knyazkov_gennady]$ cd  
[guest@knyzkov-gennady ~]$ pwd  
/home/guest  
[guest@knyzkov-gennady ~]$ id -G  
1001  
[guest@knyzkov-gennady ~]$ id -Gn  
guest  
[guest@knyzkov-gennady ~]$ groups guest  
guest : guest  
[guest@knyzkov-gennady ~]$ groups guest2  
guest2 : guest2 guest  
[guest@knyzkov-gennady ~]$ █
```

```
guest2@knyzkov-gennady:-  
[knyazkov_gennady@knyzkov-gennady ~]$ su guest2  
Rafom:  
[guest2@knyzkov-gennady knyazkov_gennady]$  
[guest2@knyzkov-gennady knyazkov_gennady]$ pwd  
/home/knyazkov_gennady  
[guest2@knyzkov-gennady knyazkov_gennady]$ cd  
[guest2@knyzkov-gennady ~]$ pwd  
/home/guest2  
[guest2@knyzkov-gennady ~]$ id -G  
1002 1001  
[guest2@knyzkov-gennady ~]$ id -Gn  
guest2 guest  
[guest2@knyzkov-gennady ~]$ groups guest  
guest : guest  
[guest2@knyzkov-gennady ~]$ groups guest2  
guest2 : guest2 guest  
[guest2@knyzkov-gennady ~]$ █
```

Figure 1: Информация о пользователях

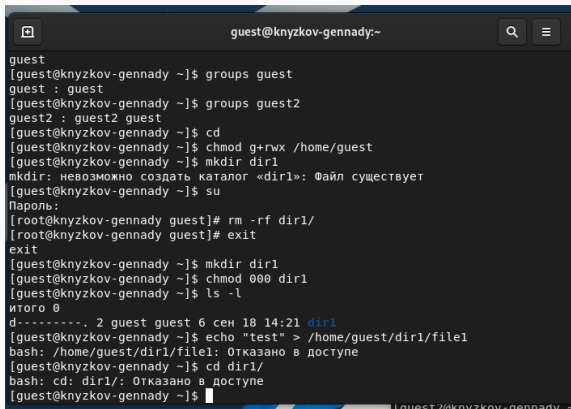
Файл с данными о пользователях

A terminal window with a dark background and light text. The title bar at the top reads "guest2@knyzkov-gennady:~". The terminal displays the output of a command, showing a list of system and user groups in the format "groupname:x:gid:groupmembers". The groups listed are: brlapi, tss, geoclue, cockpit-ws, cockpit-wsinstance, flatpak, colord, setroubleshoot, clevis, gdm, gnome-initial-setup, sshd, slocate, chrony, dnsmasq, tcpdump, sgx, systemd-oom, knyazkov_gennady, vboxsf, guest, and guest2. The last two lines show the execution of the "newgrp guest" command, resulting in a new shell prompt for the "guest" group.

```
guest2@knyzkov-gennady:~  
brlapi:x:990:  
tss:x:59:clevis  
geoclue:x:989:  
cockpit-ws:x:988:  
cockpit-wsinstance:x:987:  
flatpak:x:986:  
colord:x:985:  
setroubleshoot:x:984:  
clevis:x:983:  
gdm:x:42:  
gnome-initial-setup:x:982:  
sshd:x:74:  
slocate:x:21:  
chrony:x:981:  
dnsmasq:x:980:  
tcpdump:x:72:  
sgx:x:979:  
systemd-oom:x:978:  
knyazkov_gennady:x:1000:  
vboxsf:x:977:  
guest:x:1001:guest2  
guest2:x:1002:  
[guest2@knyzkov-gennady ~]$ newgrp guest  
[guest2@knyzkov-gennady ~]$
```

Figure 2: Содержимое файла /etc/group

Атрибуты директории



```
guest@knyzkov-gennady:~  
guest  
[guest@knyzkov-gennady ~]$ groups guest  
guest : guest  
[guest@knyzkov-gennady ~]$ groups guest2  
guest2 : guest2 guest  
[guest@knyzkov-gennady ~]$ cd  
[guest@knyzkov-gennady ~]$ chmod g+rwX /home/guest  
[guest@knyzkov-gennady ~]$ mkdir dir1  
mkdir: невозможно создать каталог «dir1»: Файл существует  
[guest@knyzkov-gennady ~]$ su  
Пароль:  
[root@knyzkov-gennady guest]# rm -rf dir1/  
[root@knyzkov-gennady guest]# exit  
exit  
[guest@knyzkov-gennady ~]$ mkdir dir1  
[guest@knyzkov-gennady ~]$ chmod 000 dir1  
[guest@knyzkov-gennady ~]$ ls -l  
итого 0  
d----- . 2 guest guest 6 сен 18 14:21 dir1  
[guest@knyzkov-gennady ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@knyzkov-gennady ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@knyzkov-gennady ~]$
```

Figure 3: Снятие атрибутов с директории

Права и разрешённые действия

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---- (020)
Переименование файла	d---wx--- (030)	----- (000)
Создание поддиректории	d---wx--- (030)	----- (000)
Удаление поддиректории	d---wx--- (030)	----- (000)

Figure 4: Минимальные права для совершения операций

Выводы по проделанной работе

В ходе выполнения работы, мы смогли приобрести практические навыки работы в консоли с атрибутами файлов для групп пользователей.