

Информационная безопасность

**Л.3. Дискреционное разграничение прав в Linux. Два
пользователя**

Греков Максим Сергеевич

2021

Содержание

1	Цель работы	4
2	Ход работы	5
2.1	Новый пользователь	5
2.2	Добавление в группу	6
2.3	Два пользователя	6
2.4	Текущая директория	7
2.5	Группы пользователей	8
2.6	Файл /etc/group	8
2.7	Регистрация в группе	9
2.8	Права для группы	10
2.9	Снятие атрибутов	10
2.10	Таблицы	10
3	Вывод	14

List of Figures

2.1	Новый пользователь	5
2.2	Добавление в группу	6
2.3	Два пользователя	7
2.4	Текущая директория	7
2.5	Группы пользователей	8
2.6	Файл /etc/group	9
2.7	Регистрация в группе	9
2.8	Права для группы	10
2.9	Снятие атрибутов	10

1 Цель работы

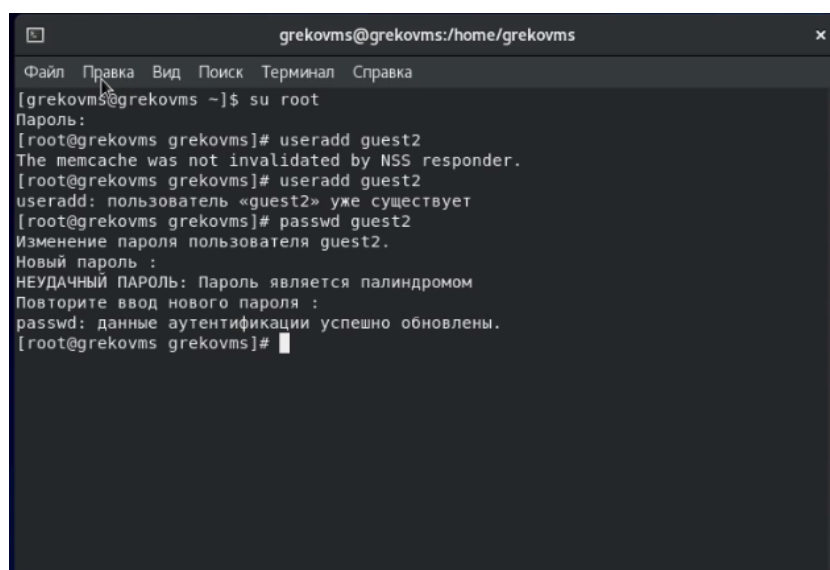
Целью данной лабораторной работы является получение практических навыков работы в консоли с атрибутами файлов для групп пользователей

2 Ход работы

2.1 Новый пользователь

В установленной операционной системе создали учётную запись пользователя guest2 (используя учётную запись администратора) с помощью команды `useradd guest`

Задали пароль для пользователя guest2 (используя учётную запись администратора) с помощью команды `passwd guest`

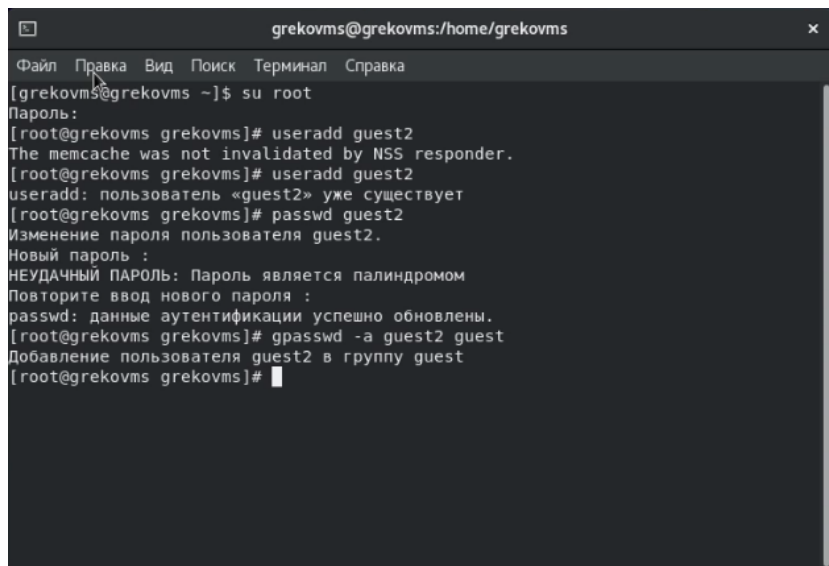


```
grekovms@grekovms:/home/grekovms
Файл Правка Вид Поиск Терминал Справка
[grekovms@grekovms ~]$ su root
Пароль:
[root@grekovms grekovms]# useradd guest2
The memcache was not invalidated by NSS responder.
[root@grekovms grekovms]# useradd guest2
useradd: пользователь «guest2» уже существует
[root@grekovms grekovms]# passwd guest2
Изменение пароля пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@grekovms grekovms]#
```

Figure 2.1: Новый пользователь

2.2 Добавление в группу

Добавили пользователя guest2 в группу guest с помощью команды `gpasswd -a guest2 guest`



```
grekovms@grekovms:/home/grekovms
Файл Правка Вид Поиск Терминал Справка
[grekovms@grekovms ~]$ su root
Пароль:
[root@grekovms grekovms]# useradd guest2
The memcache was not invalidated by NSS responder.
[root@grekovms grekovms]# useradd guest2
useradd: пользователь «guest2» уже существует
[root@grekovms grekovms]# passwd guest2
Изменение пароля пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@grekovms grekovms]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[root@grekovms grekovms]#
```

Figure 2.2: Добавление в группу

2.3 Два пользователя

Осуществили вход в систему от двух пользователей на двух разных консолях (вкладках): guest на первой консоли и guest2 на второй консоли

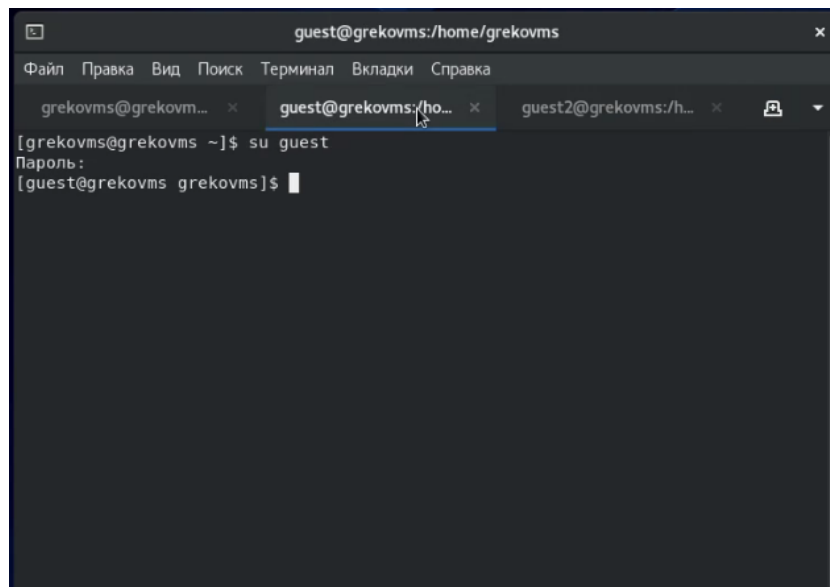


Figure 2.3: Два пользователя

2.4 Текущая директория

Для обоих пользователей командой `pwd` определили директорию, в которой находились. Сравнили её с приглашениями командной строки и получили идентичные значения

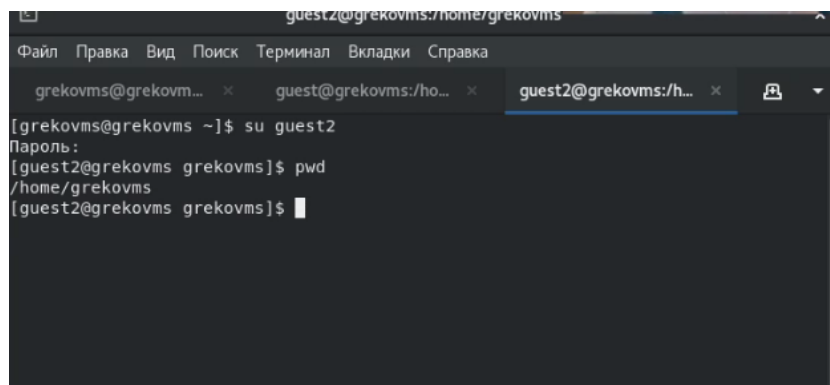


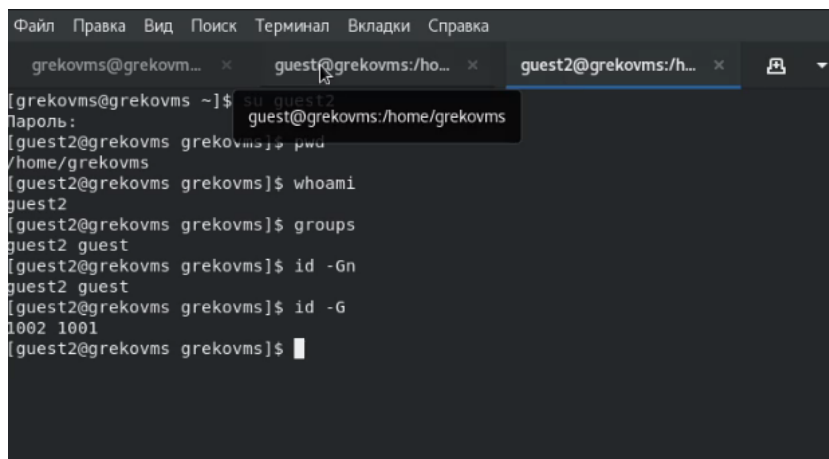
Figure 2.4: Текущая директория

2.5 Группы пользователей

Уточнили имя пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам.

Определили командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`.

Сравнили вывод команды `groups` с выводом команд `id -Gn` и `id -G`.

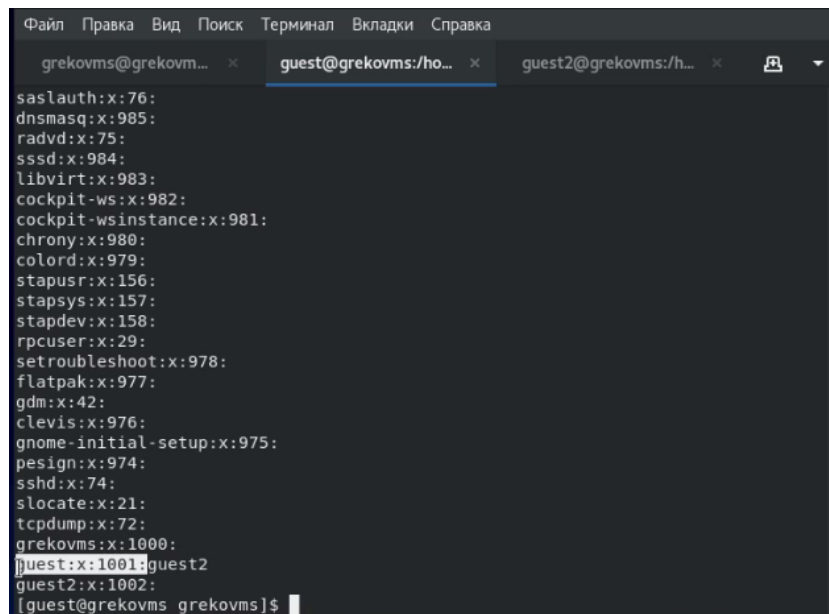


```
Файл  Правка  Вид  Поиск  Терминал  Вкладки  Справка
grekovms@grekovm...  x  guest@grekovms:/ho...  x  guest2@grekovms:/h...  x  [?]
[grekovms@grekovms ~]$ su guest2
Пароль:
[guest2@grekovms grekovms]$ pwd
/home/grekovms
[guest2@grekovms grekovms]$ whoami
guest2
[guest2@grekovms grekovms]$ groups
guest2 guest
[guest2@grekovms grekovms]$ id -Gn
guest2 guest
[guest2@grekovms grekovms]$ id -G
1002 1001
[guest2@grekovms grekovms]$
```

Figure 2.5: Группы пользователей

2.6 Файл `/etc/group`

Сравнили полученную информацию с содержимым файла `/etc/group`, посмотрели файл командой `cat /etc/group`

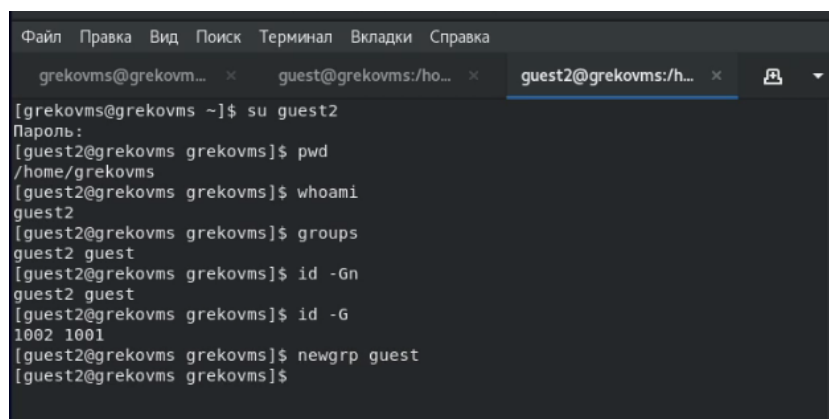


```
Файл Правка Вид Поиск Терминал Вкладки Справка
grekovms@grekovm... x guest@grekovms:/ho... x guest2@grekovms:/h... x
saslauth:x:76:
dnsmasq:x:985:
radvd:x:75:
sssd:x:984:
libvirt:x:983:
cockpit-ws:x:982:
cockpit-wsinstance:x:981:
chrony:x:980:
colord:x:979:
stapusr:x:156:
stapusr:x:157:
stapdev:x:158:
rpcuser:x:29:
setroubleshoot:x:978:
flatpak:x:977:
gdm:x:42:
clevis:x:976:
gnome-initial-setup:x:975:
pesign:x:974:
sshd:x:74:
slocate:x:21:
tcpdump:x:72:
grekovms:x:1000:
guest:x:1001:guest2
guest2:x:1002:
[guest@grekovms grekovms]$
```

Figure 2.6: Файл /etc/group

2.7 Регистрация в группе

От имени пользователя guest2 выполнили регистрацию пользователя guest2 в группе guest командой newgrp guest



```
Файл Правка Вид Поиск Терминал Вкладки Справка
grekovms@grekovm... x guest@grekovms:/ho... x guest2@grekovms:/h... x
[grekovms@grekovms ~]$ su guest2
Пароль:
[guest2@grekovms grekovms]$ pwd
/home/grekovms
[guest2@grekovms grekovms]$ whoami
guest2
[guest2@grekovms grekovms]$ groups
guest2 guest
[guest2@grekovms grekovms]$ id -gn
guest2 guest
[guest2@grekovms grekovms]$ id -G
1002 1001
[guest2@grekovms grekovms]$ newgrp guest
[guest2@grekovms grekovms]$
```

Figure 2.7: Регистрация в группе

2.8 Права для группы

От имени пользователя guest изменили права директории /home/guest, разрешив все действия для пользователей группы, применили команду `chmod g+rxw /home/guest`

```
clevis:x:976:
gnome-initial-setup:x:975:
pesign:x:974:
sshd:x:74:
slocate:x:21:
tcpdump:x:72:
grekovms:x:1000:
guest:x:1001:guest2
guest2:x:1002:
[guest@grekovms grekovms]$ ls
ls: невозможно открыть каталог '.': Отказано в доступе
[guest@grekovms grekovms]$ chmod g+rxw /home/guest
[guest@grekovms grekovms]$
```

Figure 2.8: Права для группы

2.9 Снятие атрибутов

От имени пользователя guest сняли с директории /home/guest/dir1 все атрибуты командой `chmod 000 dir1`, проверили правильность снятия атрибутов

```
chmod: невозможно получить доступ к 'dir1': Отказано в доступе
[guest@grekovms grekovms]$ chmod 000 /home/guest/dir1
[guest@grekovms grekovms]$ ls
ls: невозможно открыть каталог '.': Отказано в доступе
[guest@grekovms grekovms]$
```

Figure 2.9: Снятие атрибутов

2.10 Таблицы

Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполнили таблицу, определив опытным путём, какие операции разрешены, а какие нет.

На основании заполненной таблицы определили те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри

директории dir1 и заполнили вторую таблицу.

Установленные права и разрешённые действия для групп:

Права директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
d----- (000)	----- (000)	-	-	-	-	-	-	-	-
d----x--- (010)	----- (000)	-	-	-	-	+	-	-	+
d---w---- (020)	----- (000)	-	-	-	-	-	-	-	-
d---wx--- (030)	----- (000)	+	+	-	-	+	-	+	+
d---r----- (040)	----- (000)	-	-	-	-	-	+	-	-
d---r-x--- (050)	----- (000)	-	-	-	-	+	+	-	+
d---rw---- (060)	----- (000)	-	-	-	-	-	+	-	-
d---rwx--- (070)	----- (000)	+	+	-	-	+	+	+	+
d----- (000)	-----x--- (010)	-	-	-	-	-	-	-	-
d-----x--- (010)	-----x--- (010)	-	-	-	-	+	-	-	+
d---w---- (020)	-----x--- (010)	-	-	-	-	-	-	-	-
d---wx--- (030)	-----x--- (010)	+	+	-	-	+	-	+	+
d---r----- (040)	-----x--- (010)	-	-	-	-	-	+	-	-
d---r-x--- (050)	-----x--- (010)	-	-	-	-	+	+	-	+
d---rw---- (060)	-----x--- (010)	-	-	-	-	-	+	-	-
d---rwx--- (070)	-----x--- (010)	+	+	-	-	+	+	+	+
d----- (000)	-----w---- (020)	-	-	-	-	-	-	-	-
d-----x--- (010)	-----w---- (020)	-	-	+	-	+	-	-	+
d---w---- (020)	-----w---- (020)	-	-	-	-	-	-	-	-
d---wx--- (030)	-----w---- (020)	+	+	+	-	+	-	+	+
d---r----- (040)	-----w---- (020)	-	-	-	-	-	+	-	-
d---r-x--- (050)	-----w---- (020)	-	-	+	-	+	+	-	+
d---rw---- (060)	-----w---- (020)	-	-	-	-	-	+	-	-
d---rwx--- (070)	-----w---- (020)	+	+	+	-	+	+	+	+
d----- (000)	-----wx--- (030)	-	-	-	-	-	-	-	-

Права директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
d----x--- (010)	-----wx--- (030)	-	-	+	-	+	-	-	+
d----w---- (020)	-----wx--- (030)	-	-	-	-	-	-	-	-
d----wx--- (030)	-----wx--- (030)	+	+	+	-	+	-	+	+
d---r----- (040)	-----wx--- (030)	-	-	-	-	-	+	-	-
d---r-x--- (050)	-----wx--- (030)	-	-	+	-	+	+	-	+
d---rw---- (060)	-----wx--- (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)	-	-	-	+	+	+	-	+
d---rw---- (060)	----r----- (040)	-	-	-	-	-	+	-	-
d---rwx--- (070)	----r----- (040)	+	+	-	+	+	+	+	+
d----- (000)	----r-x--- (050)	-	-	-	-	-	-	-	-
d----x--- (010)	----r-x--- (050)	-	-	-	+	+	-	-	+
d----w---- (020)	----r-x--- (050)	-	-	-	-	-	-	-	-
d----wx--- (030)	----r-x--- (050)	+	+	-	+	+	-	+	+
d---r----- (040)	----r-x--- (050)	-	-	-	-	-	+	-	-
d---r-x--- (050)	----r-x--- (050)	-	-	-	+	+	+	-	+
d---rw---- (060)	----r-x--- (050)	-	-	-	-	-	+	-	-
d---rwx--- (070)	----r-x--- (050)	+	+	-	+	+	+	+	+
d----- (000)	----rw---- (060)	-	-	-	-	-	-	-	-
d----x--- (010)	----rw---- (060)	-	-	+	+	+	-	-	+
d----w---- (020)	----rw---- (060)	-	-	-	-	-	-	-	-
d----wx--- (030)	----rw---- (060)	+	+	+	+	+	-	+	+

Права директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
d---r----- (040)	----rw---- (060)	-	-	-	-	-	+	-	-
d---r-x--- (050)	----rw---- (060)	-	-	+	+	+	+	-	+
d---rw---- (060)	----rw---- (060)	-	-	-	-	-	+	-	-
d---rwx--- (070)	----rw---- (060)	+	+	+	+	+	+	+	+
d----- (000)	----rwx--- (070)	-	-	-	-	-	-	-	-
d-----x--- (010)	----rwx--- (070)	-	-	+	+	+	-	-	+
d-----w---- (020)	----rwx--- (070)	-	-	-	-	-	-	-	-
d----wx--- (030)	----rwx--- (070)	+	+	+	+	+	-	+	+
d---r----- (040)	----rwx--- (070)	-	-	-	-	-	+	-	-
d---r-x--- (050)	----rwx--- (070)	-	-	+	+	+	+	-	+
d---rw---- (060)	----rwx--- (070)	-	-	-	-	-	+	-	-
d---rwx--- (070)	----rwx--- (070)	+	+	+	+	+	+	+	+

Минимальные права для совершения операций:

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)

3 Вывод

В ходе лабораторной работы получили практические навыки работы в консоли с атрибутами файлов для групп пользователей