

# report

## Отчет по лабораторной работе №3

### Основы информационной безопасности

Подъярова Ксения | НПМбд-02-21

## Цель работы

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

## Теоретическая часть

В операционной системе Linux есть много отличных функций безопасности, но одна из самых важных - это система прав доступа к файлам. Изначально каждый файл имел три параметра доступа. Вот они:

- Чтение - разрешает получать содержимое файла, но на запись нет. Для каталога позволяет получить список файлов и каталогов, расположенных в нем
- Запись - разрешает записывать новые данные в файл или изменять существующие, а также позволяет создавать и изменять файлы и каталоги
- Выполнение - невозможно выполнить программу, если у нее нет флага выполнения.

Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система может понять, что этот файл нужно запускать как программу. Каждый файл имеет три категории пользователей, для которых можно устанавливать различные сочетания прав доступа:

- Владелец - набор прав для владельца файла, пользователя, который его создал или сейчас установлен его владельцем. Обычно владелец имеет все права, чтение, запись и выполнение
- Группа - любая группа пользователей, существующая в системе и привязанная к файлу. Но это может быть только одна группа и обычно это группа владельца, хотя для файла можно назначить и другую группу
- Остальные - все пользователи, кроме владельца и пользователей, входящих в группу файла

Команды, которые могут понадобиться при работе с правами доступа:

- "ls -l" - для просмотра прав доступа к файлам и каталогам

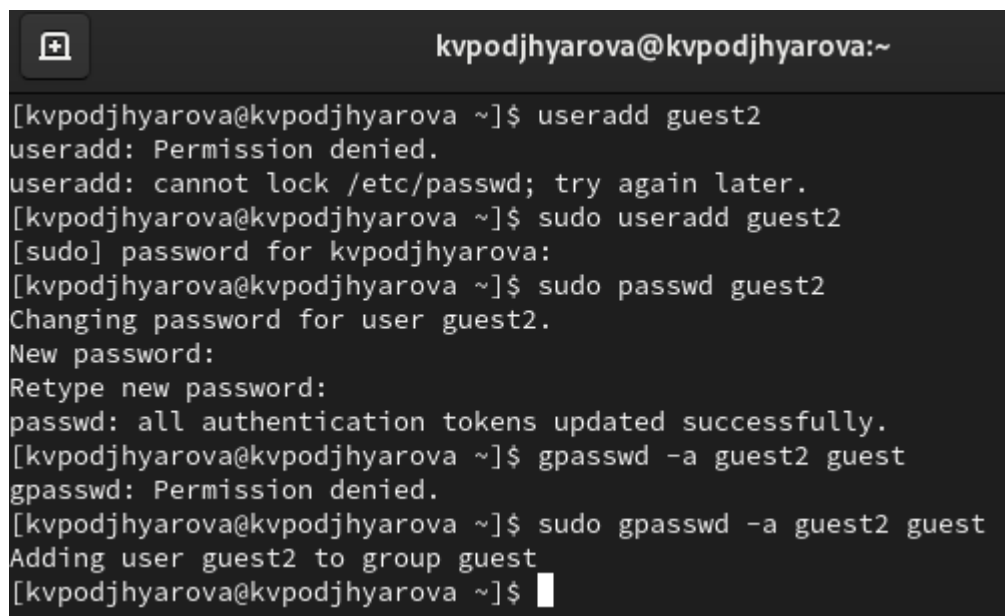
- “chmod категория действие флаг файл или каталог” - для изменения прав доступа к файлам и каталогам (категорию действие и флаг можно заменить на набор из трех цифр от 0 до 7)

Значения флагов прав:

- — - нет никаких прав
- —x - разрешено только выполнение файла, как программы, но не изменение и не чтение
- -w- - разрешена только запись и изменение файла
- -wx - разрешено изменение и выполнение, но в случае с каталогом, невозможно посмотреть его содержимое
- r— - права только на чтение
- r-x - только чтение и выполнение, без права на запись
- rw- - права на чтение и запись, но без выполнения
- rwx - все права

## Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы ОС создала учётную запись пользователя guest2 (т.к. пользователь guest уже был создан в прошлой лабораторной работе) с помощью команды “sudo useradd guest2” и задала пароль для этого пользователя командой “sudo passwd guest2”. Добавила пользователя guest2 в группу guest с помощью команды “sudo gpasswd -a guest2 guest”



```
kvpodjhyarova@kvpodjhyarova:~$ useradd guest2
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
[kvpodjhyarova@kvpodjhyarova ~]$ sudo useradd guest2
[sudo] password for kvpodjhyarova:
[kvpodjhyarova@kvpodjhyarova ~]$ sudo passwd guest2
Changing password for user guest2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[kvpodjhyarova@kvpodjhyarova ~]$ gpasswd -a guest2 guest
gpasswd: Permission denied.
[kvpodjhyarova@kvpodjhyarova ~]$ sudo gpasswd -a guest2 guest
Adding user guest2 to group guest
[kvpodjhyarova@kvpodjhyarova ~]$
```

2. Затем осуществила вход в систему от двух пользователей на двух разных консолях при помощи команд “su - guest” и “su - guest2”. Определила командой “pwd”, что оба

пользователя находятся в своих домашних директориях, что совпадает с приглашениями командной строки. Уточнила имена пользователей командой “whoami”, соответственно получила: guest и guest2. С помощью команд “groups guest” и “groups guest2” определила, что пользователь guest входит в группу guest, а пользователь guest2 в группы guest и guest2. Сравнила полученную информацию с выводом команд “id -Gn guest”, “id -Gn guest2”, “id -G guest” и “id -G guest2”: данные совпали, за исключением второй команды “id -G”, которая вывела номера групп 1001 и 1002, что также является верным

<pre>guest2 : guest2 guest [guest@kvpodjhyarova ~]\$ su - guest Password: [guest@kvpodjhyarova ~]\$ pwd /home/guest [guest@kvpodjhyarova ~]\$ whoami guest [guest@kvpodjhyarova ~]\$ groups guest guest : guest [guest@kvpodjhyarova ~]\$ id -Gn guest guest [guest@kvpodjhyarova ~]\$ id -G guest 1001 [guest@kvpodjhyarova ~]\$</pre>	<pre>[kvpodjhyarova@kvpodjhyarova ~]\$ su - guest2 Password: [guest2@kvpodjhyarova ~]\$ pwd /home/guest2 [guest2@kvpodjhyarova ~]\$ whoami guest2 [guest2@kvpodjhyarova ~]\$ groups guest2 guest2 : guest2 guest [guest2@kvpodjhyarova ~]\$ id -Gn guest2 guest2 guest [guest2@kvpodjhyarova ~]\$ id -G guest2 1002 1001 [guest2@kvpodjhyarova ~]\$</pre>
---	---

3. Просмотрела файл /etc/group командой “cat /etc/group”, данные этого файла совпадают с полученными ранее.

```
guest@kvpodjhyarova:~  
render:x:998:  
systemd-journal:x:190:  
systemd-coredump:x:997:  
dbus:x:81:  
polkitd:x:996:  
avahi:x:70:  
printadmin:x:995:  
ssh_keys:x:101:  
rtkit:x:172:  
pipewire:x:994:  
sssd:x:993:  
sgx:x:992:  
libstoragemgmt:x:991:  
brlapi:x:990:  
tss:x:59:clevis  
geoclue:x:989:  
cockpit-ws:x:988:  
cockpit-wsinstance:x:987:  
flatpak:x:986:  
colord:x:985:  
clevis:x:984:  
setroubleshoot:x:983:  
gdm:x:42:  
stapusr:x:156:  
stapsys:x:157:  
stapdev:x:158:  
pesign:x:982:  
gnome-initial-setup:x:981:  
sshd:x:74:  
slocate:x:21:  
chrony:x:980:  
dnsmasq:x:979:  
tcpdump:x:72:  
kvpodjhyarova:x:1000:  
guest:x:1001:guest2  
guest2:x:1002:  
[guest@kvpodjhyarova ~]$ S
```

4. От имени пользователя guest2 зарегистрировала этого пользователя в группе guest командой "newgrp guest". Далее от имени пользователя guest изменила права директории /home/guest, разрешив все действия для пользователей группы командой "chmod g+rwX /home/guest". От имени этого же пользователя сняла с директории /home/guest/dir1 все атрибуты командой "chmod 000 dir1" и проверила правильность снятия атрибутов командой "ls -l"

guest@kvpodjhyarova:~	guest2@kvpodjhyarova:~
<pre> stapdev:x:158: pesign:x:982: gnome-initial-setup:x:981: sshd:x:74: slocate:x:21: chrony:x:980: dnsmasq:x:979: tcpdump:x:72: kvpodjhyarova:x:1000: guest:x:1001:guest2 guest2:x:1002: [guest@kvpodjhyarova ~]\$ chmod g+rwX /home/guest [guest@kvpodjhyarova ~]\$ chmod 000 /home/guest/dir1 [guest@kvpodjhyarova ~]\$ ls -l total 0 drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Desktop d----- 2 guest guest 6 Sep  9 18:07 dir1 drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Documents drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Downloads drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Music drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Pictures drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Public drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Templates drwxr-xr-x. 2 guest guest 6 Sep  9 18:00 Videos [guest@kvpodjhyarova ~]\$ </pre>	<pre> [kvpodjhyarova@kvpodjhyarova ~]\$ su - guest2 Password: [guest2@kvpodjhyarova ~]\$ pwd /home/guest2 [guest2@kvpodjhyarova ~]\$ whoami guest2 [guest2@kvpodjhyarova ~]\$ groups guest2 guest2 : guest2 guest [guest2@kvpodjhyarova ~]\$ id -Gn guest2 guest2 guest [guest2@kvpodjhyarova ~]\$ id -G guest2 1002 1001 [guest2@kvpodjhyarova ~]\$ newgr guest bash: newgr: command not found... [guest2@kvpodjhyarova ~]\$ newgrp guest [guest2@kvpodjhyarova ~]\$ </pre>

Теперь заполним таблицу «Установленные права и разрешённые действия», меняя атрибуты у директории и файла от имени пользователя guest и делая проверку от пользователя guest2. Создание файла: “echo”text” > /home/guest/dir1/file2” Удаление файла: “rm -r /home/guest/dir1/file1” Запись в файл: “echo”textnew” > /home/guest/dir1/file1” Чтение файла: “cat /home/guest/dir1/file1” Смена директории: “cd /home/guest/dir1” Просмотр файлов в директории: “ls /home/guest/dir1” Переименование файла: “mv /home/guest/dir1/file1 filenew” Смена атрибутов файла: “chattr -a /home/guest/dir1/file1”

```

d
(000)
(000) -----
d -x
(100)
(000) ---- + ---
d -w-
(200)
(000) -----
d -wx
(300)
(000) ++ -- + - + -
d r-
(400)
(000) ----- + --

```

d r-x  
(500)  
(000) - - - - + + - -  
d rw-  
(600)  
(000) - - - - - + - -  
d rwx  
(700)  
(000) + + - - + + + -  
d  
(000)  
(100) - - - - - - - -  
d -x  
(100)  
(100) - - - - + - - -  
d -w-  
(200)  
(100) - - - - - - - -  
d -wx  
(300)  
(100) + + - - + - + -  
d r-  
(400)  
(100) - - - - - + - -  
d r-x  
(500)  
(100) - - - - + + - -  
d rw-  
(600)  
(100) - - - - - + - -  
d rwx  
(700)  
(100) + + - - + + + -  
d  
(000)  
(200) - - - - - - - -  
d -x  
(100)  
(200) - - + - + - - -  
d -w-

(200)  
(200) - - - - -  
d -wx  
(300)  
(200) + + + - + - + -  
d r-  
(400)  
(200) - - - - + - -  
d r-x  
(500)  
(200) - - + - + + - -  
d rw-  
(600)  
(200) - - - - + - -  
d rwx  
(700)  
(200) + + + - + + + -  
d  
(000)  
(300) - - - - -  
d -x  
(100)  
(300) - - + - + - - -  
d -w-  
(200)  
(300) - - - - -  
d -wx  
(300)  
(300) + + - + + - + -  
d r-  
(400)  
(300) - - - - + - -  
d r-x  
(500)  
(300) - - + - + + - -  
d rw-  
(600)  
(300) - - - - + - -  
d rwx  
(700)

(300) + + + - + + + -

d

(000)

(400) - - - - -

d -x

(100)

(400) - - - + + - - +

d -w-

(200)

(400) - - - - -

d -wx

(300)

(400) + + - + + - + +

d r-

(400)

(400) - - - - - + - -

d r-x

(500)

(400) - - - + + + - +

d rw-

(600)

(400) - - - - - + - -

d rwx

(700)

(400) + + - + + + + +

d

(000)

(500) - - - - -

d -x

(100)

(500) - - - + + - - +

d -w-

(200)

(500) - - - - -

d -wx

(300)

(500) + + - + + - + +

d r-

(400)

(500) - - - - - + - -



d r-x

(500)

(500) - - - + + + - +

d rw-

(600)

(500) - - - - - + - -

d rwx

(700)

(500) + + - + + + + +

d

(000)

(600) - - - - - - - -

d -x

(100)

(600) - - + + + - - +

d -w-

(200)

(600) - - - - - - - -

d -wx

(300)

(600) + + + + + - + +

d r-

(400)

(600) - - - - - + - -

d r-x

(500)

(600) - - + + + + - +

d rw-

(600)

(600) - - - - - + - -

d rwx

(700)

(600) + + + + + + + +

d

(000)

(700) - - - - - - - -

d -x

(100)

(700) - - + + + - - +

d -w-

(200)  
 (700) - - - - -  
 d -wx  
 (300)  
 (700) + + + + - + +  
 d r-  
 (400)  
 (700) - - - - + - -  
 d r-x  
 (500)  
 (700) - - + + + - +  
 d rw-  
 (600)  
 (700) - - - - + - -  
 d rwx  
 (700)  
 (700) + + + + + + +

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d -wd (300)	(000)
Удаление файла	d -wx (300)	(000)
Чтение файла	d --x (100)	(400)
Запись в файл	d --x (100)	(200)
Переименование файла	d -wx (300)	(000)
Создание поддиректории	d -wx (300)	(000)
Удаление поддиректории	d -wx (300)	(000)

## Выводы

В ходе выполнения данной лабораторной работы я получила практические навыки работы в консоли с атрибутами файлов для групп пользователей.