

# **Лабораторная работа №2**

**Информационная безопасность**

НВЕ МАНГЕ ХОСЕ ХЕРСОН МИКО; НКАбд-03-22

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>17</b>

## Список иллюстраций

2.1	Создание и настройка нового пользователя . . . . .	6
2.2	pwd . . . . .	7
2.3	whoami . . . . .	7
2.4	id . . . . .	8
2.5	Файл passwd . . . . .	9
2.6	grep . . . . .	9
2.7	Существующие директории . . . . .	10
2.8	lsattr . . . . .	10
2.9	mkdir . . . . .	10
2.10	Атрибуты . . . . .	11
2.11	chmod . . . . .	12
2.12	echo . . . . .	13
2.13	Проверка создания файла . . . . .	13
2.14	chmod . . . . .	14

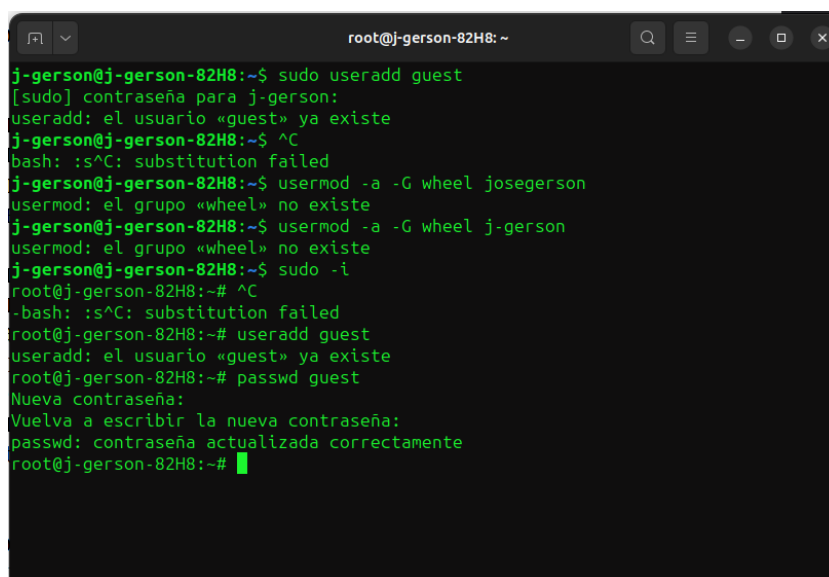
## **Список таблиц**

# 1 Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

## 2 Выполнение лабораторной работы

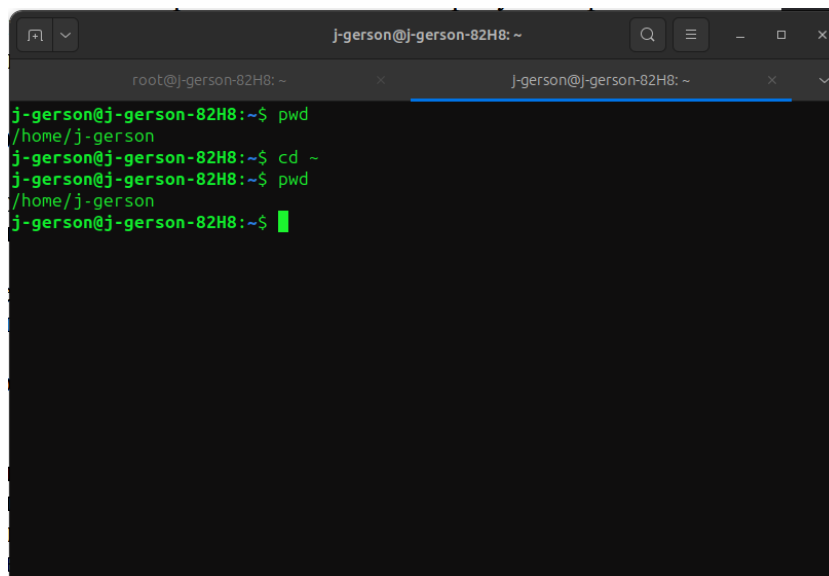
1. В установленной при выполнении предыдущей лабораторной работы операционной системе создаю учётную запись пользователя guest (через учётную запись администратора) и задаю пароль (рис. 2.1).



```
root@j-gerson-82H8: ~  
j-gerson@j-gerson-82H8:~$ sudo useradd guest  
[sudo] contraseña para j-gerson:  
useradd: el usuario «guest» ya existe  
j-gerson@j-gerson-82H8:~$ ^C  
bash: :s^C: substitution failed  
j-gerson@j-gerson-82H8:~$ usermod -a -G wheel josegerson  
usermod: el grupo «wheel» no existe  
j-gerson@j-gerson-82H8:~$ usermod -a -G wheel j-gerson  
usermod: el grupo «wheel» no existe  
j-gerson@j-gerson-82H8:~$ sudo -i  
root@j-gerson-82H8:~# ^C  
-bash: :s^C: substitution failed  
root@j-gerson-82H8:~# useradd guest  
useradd: el usuario «guest» ya existe  
root@j-gerson-82H8:~# passwd guest  
Nueva contraseña:  
Vuelva a escribir la nueva contraseña:  
passwd: contraseña actualizada correctamente  
root@j-gerson-82H8:~#
```

Рис. 2.1: Создание и настройка нового пользователя

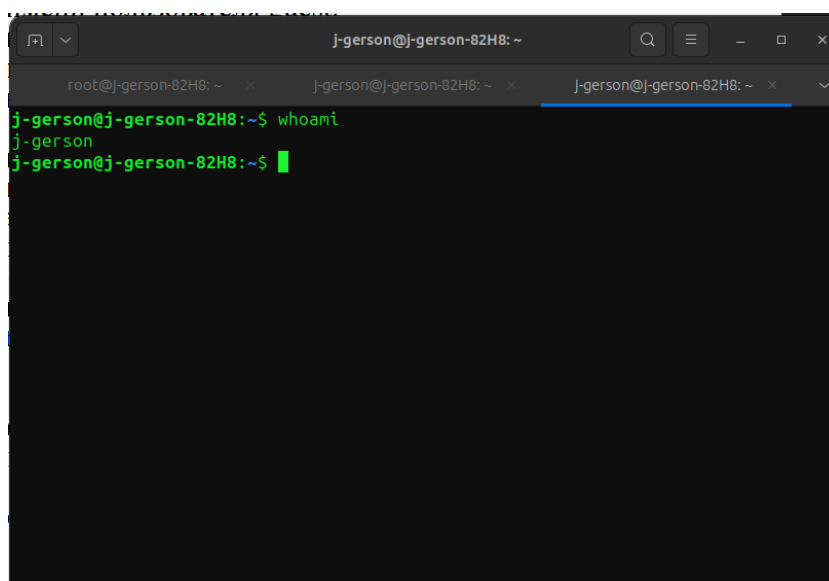
3. Вхожу в систему от имени пользователя guest.
4. Определяю директорию, в которой нахожусь. Это действительно домашняя директория (рис. 2.2).

A terminal window titled 'j-gerson@j-gerson-82H8: ~' with three tabs. The first tab is 'root@j-gerson-82H8: ~', the second is 'j-gerson@j-gerson-82H8: ~' (selected), and the third is 'j-gerson@j-gerson-82H8: ~'. The terminal shows the following commands and output:

```
j-gerson@j-gerson-82H8:~$ pwd
/home/j-gerson
j-gerson@j-gerson-82H8:~$ cd ~
j-gerson@j-gerson-82H8:~$ pwd
/home/j-gerson
j-gerson@j-gerson-82H8:~$
```

Рис. 2.2: pwd

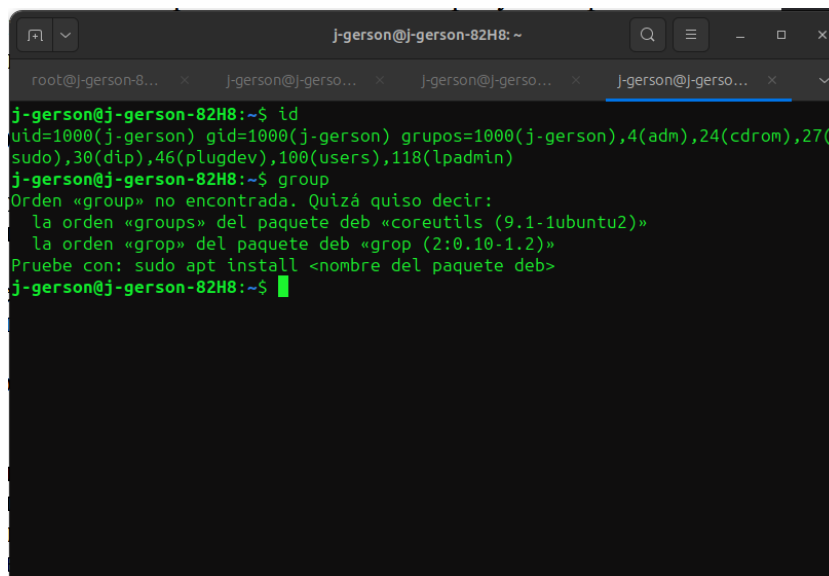
5. Уточняю имя пользователя через whoami (рис. 2.3).

A terminal window titled 'j-gerson@j-gerson-82H8: ~' with three tabs. The first tab is 'root@j-gerson-82H8: ~', the second is 'j-gerson@j-gerson-82H8: ~' (selected), and the third is 'j-gerson@j-gerson-82H8: ~'. The terminal shows the following commands and output:

```
j-gerson@j-gerson-82H8:~$ whoami
j-gerson
j-gerson@j-gerson-82H8:~$
```

Рис. 2.3: whoami

6. Уточняю имя пользователя, его группу, а также группы, куда входит пользователь, командой id. Данные совпадают (рис. 2.4).



```
j-gerson@j-gerson-82H8: ~  
root@j-gerson-8... x j-gerson@j-gerso... x j-gerson@j-gerso... x j-gerson@j-gerso... x  
j-gerson@j-gerson-82H8:~$ id  
uid=1000(j-gerson) gid=1000(j-gerson) grupos=1000(j-gerson),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users),118(lpadmin)  
j-gerson@j-gerson-82H8:~$ group  
Orden «group» no encontrada. Quizá quiso decir:  
  la orden «groups» del paquete deb «coreutils (9.1-1ubuntu2)»  
  la orden «grop» del paquete deb «grop (2:0.10-1.2)»  
Pruebe con: sudo apt install <nombre del paquete deb>  
j-gerson@j-gerson-82H8:~$
```

Рис. 2.4: id

7. Просматриваю файл /etc/passwd (рис. 2.5).



```
root@j-gerson-82H8: ~  
j-gerson@j-gerson-82H8:~$ cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailling List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin  
apt:x:42:65534::/nonexistent:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin  
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin  
messagebus:x:100:106::/nonexistent:/usr/sbin/nologin  
yslog:x:101:107::/nonexistent:/usr/sbin/nologin  
systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin  
uid:x:102:108::/run/uid:/usr/sbin/nologin  
tss:x:103:110:TPM software stack,,,:/var/lib/tpm:/bin/false  
systemd-oom:x:995:995:systemd Userspace OOM Killer:/:/usr/sbin/nologin  
cpdump:x:104:113::/nonexistent:/usr/sbin/nologin  
avahi-autoipd:x:105:114:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin  
usbmux:x:106:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin  
kernoops:x:107:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin  
hoopsie:x:108:115::/nonexistent:/bin/false  
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin  
avahi:x:110:116:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin  
cups-pk-helper:x:111:118:user for cups-pk-helper service,,,:/nonexistent:/usr/sbin/nologin  
rtkit:x:112:119:RealtimeKit,,,:/proc:/usr/sbin/nologin  
sssd:x:113:120:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin  
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false  
fwupd-refresh:x:115:122:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin  
n-ovpn:x:116:123:NetworkManager OpenVPN,,,:/var/lib/ovpn/chroot:/usr/sbin/nologin  
saned:x:117:125::/var/lib/saned:/usr/sbin/nologin  
colord:x:118:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin  
n-ovpn:x:119:127::/var/lib/ovpn:/usr/sbin/nologin
```

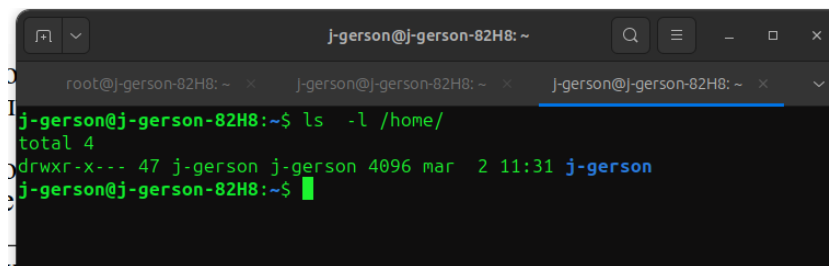
Рис. 2.5: Файл passwd

8. Нахожу в нём свою учётную запись через *grep*. Определяю *uid* и *gid* пользователя (рис. 2.6).

```
rtkit:x:112:119:RealtimeKit,,,:/proc:/usr/sbin/nologin  
sssd:x:113:120:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin  
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false  
fwupd-refresh:x:115:122:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin  
n-ovpn:x:116:123:NetworkManager OpenVPN,,,:/var/lib/ovpn/chroot:/usr/sbin/nologin  
saned:x:117:125::/var/lib/saned:/usr/sbin/nologin
```

Рис. 2.6: *grep*

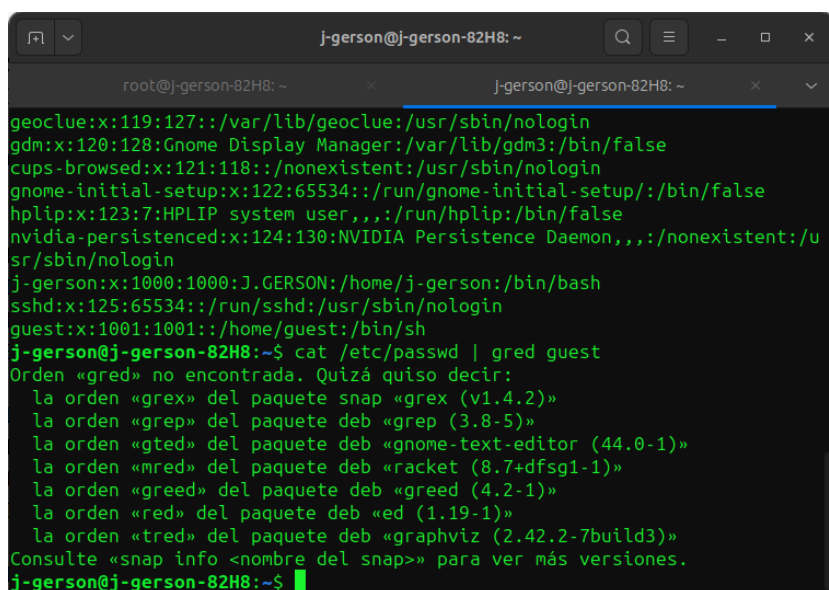
9. Определяю существующие в системе директории (рис. 2.7).



```
j-gerson@j-gerson-82H8: ~  
root@j-gerson-82H8: ~ x j-gerson@j-gerson-82H8: ~ x j-gerson@j-gerson-82H8: ~ x  
j-gerson@j-gerson-82H8:~$ ls -l /home/  
total 4  
drwxr-x--- 47 j-gerson j-gerson 4096 mar  2 11:31 j-gerson  
j-gerson@j-gerson-82H8:~$
```

Рис. 2.7: Существующие директории

10. Проверяю, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home. Мне отказано в доступе (рис. 2.8).



```
j-gerson@j-gerson-82H8: ~  
root@j-gerson-82H8: ~ x j-gerson@j-gerson-82H8: ~ x  
geoclue:x:119:127::/var/lib/geoclue:/usr/sbin/nologin  
gdm:x:120:128:Gnome Display Manager:/var/lib/gdm3:/bin/false  
cups-browsed:x:121:118::/nonexistent:/usr/sbin/nologin  
gnome-initial-setup:x:122:65534::/run/gnome-initial-setup:/bin/false  
hplip:x:123:7:HPLIP system user,,,:/run/hplip:/bin/false  
nvidia-persistenced:x:124:130:NVIDIA Persistence Daemon,,,:/nonexistent:/usr/sbin/nologin  
j-gerson:x:1000:1000:J.GERSON:/home/j-gerson:/bin/bash  
sshd:x:125:65534::/run/sshd:/usr/sbin/nologin  
guest:x:1001:1001::/home/guest:/bin/sh  
j-gerson@j-gerson-82H8:~$ cat /etc/passwd | gred guest  
Orden «gred» no encontrada. Quizá quiso decir:  
la orden «grex» del paquete snap «grex (v1.4.2)»  
la orden «grep» del paquete deb «grep (3.8-5)»  
la orden «gted» del paquete deb «gnome-text-editor (44.0-1)»  
la orden «mred» del paquete deb «racket (8.7+dfsg1-1)»  
la orden «greed» del paquete deb «greed (4.2-1)»  
la orden «red» del paquete deb «ed (1.19-1)»  
la orden «tred» del paquete deb «graphviz (2.42.2-7build3)»  
Consulte «snap info <nombre del snap>» para ver más versiones.  
j-gerson@j-gerson-82H8:~$
```

Рис. 2.8: lsattr

11. Создаю в домашней директории поддиректорию dir1 командой *mkdir dir1* (рис. 2.9).



```
j-gerson@j-gerson-82H8: ~  
root@j-gerson-82H8: ~ x j-gerson@j-gerson-82H8: ~ x j-gerson@j-gerson-82H8: ~ x j-gerson@j-gerson-82H8: ~ x  
j-gerson@j-gerson-82H8:~$ lsattr /home  
-----e----- /home/j-gerson  
j-gerson@j-gerson-82H8:~$
```

Рис. 2.9: mkdir

Определяю командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1` (рис. 2.10).

```
j-gereson@j-gereson-82H8:~$ ls -l
'2024-03-02 11-07-46.mkv'
'2024-03-02 11-18-30.mkv'
'2024-03-02 11-31-04.mkv'
Android
AndroidStudioProjects
Descargas
DESORDEN
dir1
Documentos
Escritorio
Imágenes
JP
linux_signing_key.pub
'mi primer programa.py'
Música
N2.odt
n3.odt
openvpn-install.sh
openvpn-install.sh.save
Plantillas
"PlayOnLinux's virtual drives"
programa1.cpp
Programa1.py
Público
SCORPION
snap
untitled
Untitled1.ipynb
Untitled2.ipynb
```

Рис. 2.10: Атрибуты

12. Снимаю с директории `dir1` все атрибуты командой `chmod 000 dir1` (рис. 2.11).

```
j-gerson@j-gerson-82H8:~$ ls -l
'2024-03-02 11-07-46.mkv'
'2024-03-02 11-18-30.mkv'
'2024-03-02 11-31-04.mkv'
'2024-03-02 12-24-18.mkv'
Android
AndroidStudioProjects
Descargas
DESORDEN
dir1
Documentos
Escritorio
Imágenes
JP
linux_signing_key.pub
'mi_primer programa.py'
Música
N2.odt
n3.odt
openvpn-install.sh
openvpn-install.sh.save
Plantillas
"PlayOnLinux's virtual drives"
programa1.cpp
Programa1.py
Público
SCORPION
snap
untitled
Untitled1.ipynb
Untitled2.ipynb
Untitled3.ipynb
Untitled4.ipynb
Untitled5.ipynb
Untitled6.ipynb
Untitled.ipynb
Videos
'VirtualBox VMs'
vpn
vpn.1
vpn.2
work
j-gerson@j-gerson-82H8:~$
```

Рис. 2.11: chmod

13. Пытаюсь создать в директории dir1 файл file1, но получаю отказ, так как я удалила права на доступ в прошлом пункте. Файл не был создан (рис. 2.12), (рис. 2.13).

```

j-gerson@j-gerson-82H8: ~
root@j-gerson-8... x j-gerson@j-gerso... x j-gerson@j-gerso... x j-gerson@j-gerso... x
j-gerson@j-gerson-82H8:~$ id
uid=1000(j-gerson) gid=1000(j-gerson) grupos=1000(j-gerson),4(adm),24(cdrom),27(
sudo),30(dip),46(plugdev),100(users),118(lpadmin)
j-gerson@j-gerson-82H8:~$ group
Orden «group» no encontrada. Quizá quiso decir:
  la orden «groups» del paquete deb «coreutils (9.1-1ubuntu2)»
  la orden «grop» del paquete deb «grop (2:0.10-1.2)»
Pruebe con: sudo apt install <nombre del paquete deb>
j-gerson@j-gerson-82H8:~$ █

```

Рис. 2.12: echo

```

j-gerson@j-gerson-82H8: ~
root@j-gerson... x j-gerson@j-ger... x j-gerson@j-ger... x j-gerson@j-ger... x
j-gerson@j-gerson-82H8:~$ lsattr /home
-----e----- /home/j-gerson
j-gerson@j-gerson-82H8:~$ █

```

Рис. 2.13: Проверка создания файла

#### 14. Минимальные права для совершения операций

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

15. Заполнение таблицы «Установленные права и разрешённые действия»

Пример проверки прав для заполнения таблицы (рис. 2.14).

```
j-gerson@j-gerson-82H8:~$ cat /etc/passwd | gred guest
Orden «gred» no encontrada. Quizá quiso decir:
  la orden «grex» del paquete snap «grex (v1.4.2)»
  la orden «grep» del paquete deb «grep (3.8-5)»
  la orden «gted» del paquete deb «gnome-text-editor (44.0-1)»
  la orden «mred» del paquete deb «racket (8.7+dfsg1-1)»
  la orden «greed» del paquete deb «greed (4.2-1)»
  la orden «red» del paquete deb «ed (1.19-1)»
  la orden «tred» del paquete deb «graphviz (2.42.2-7build3)»
Consulte «snap info <nombre del snap>» para ver más versiones.
j-gerson@j-gerson-82H8:~$
```

Рис. 2.14: chmod

Права ди- рек- то- рии	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	Смена ди- рек- то- рии	Просмотр фай- лов в ди- рек- то- рии	Переименование фай- ла	Создание атри- бутов фай- ла
d(000)	(000)	-	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(100)	(100)	-	-	-	-	+	-	-	+
d(100)	(200)	-	-	+	-	+	-	-	+
d(100)	(300)	-	-	+	-	+	-	-	+

---

d(100)	(400)	-	-	-	+	+	-	-	+
d(100)	(500)	-	-	-	+	+	-	-	+
d(100)	(600)	-	-	+	+	-	-	+	+
d(100)	(700)	-	-	+	+	-	-	+	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(200)	(100)	-	-	-	-	-	-	-	-
d(200)	(200)	-	-	-	-	-	-	-	-
d(200)	(300)	-	-	-	-	-	-	-	-
d(200)	(400)	-	-	-	-	-	-	-	-
d(200)	(500)	-	-	-	-	-	-	-	-
d(200)	(600)	-	-	-	-	-	-	-	-
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(000)	+	-	-	-	+	+	-	-
d(300)	(100)	+	-	-	-	+	+	-	-
d(300)	(200)	+	+	+	-	+	+	-	+
d(300)	(300)	+	+	+	-	+	+	-	+
d(300)	(400)	+	+	-	+	+	-	+	+
d(300)	(500)	+	+	-	+	+	-	+	+
d(300)	(600)	+	+	+	+	+	-	+	+
d(300)	(700)	+	+	+	+	+	-	+	+
d(400)	(000)	-	-	-	-	-	+	-	-
d(400)	(100)	-	-	-	-	-	+	-	-
d(400)	(200)	-	-	-	-	-	+	-	-
d(400)	(300)	-	-	-	-	-	+	-	-
d(400)	(400)	-	-	-	-	-	+	-	-
d(400)	(500)	-	-	-	-	-	+	-	-
d(400)	(600)	-	-	-	-	-	+	-	-
d(400)	(700)	-	-	-	-	-	+	-	-

---

d(500)	(000)	-	-	-	-	+	+	-	+
d(500)	(100)	-	-	-	-	+	+	-	+
d(500)	(200)	-	-	+	-	+	+	-	+
d(500)	(300)	-	-	+	-	+	+	-	+
d(500)	(400)	-	-	-	+	+	+	-	+
d(500)	(500)	-	-	-	+	+	+	-	+
d(500)	(600)	-	-	+	+	+	+	-	+
d(500)	(700)	-	-	+	+	+	+	-	+
d(600)	(000)	-	-	-	-	-	+	-	-
d(600)	(100)	-	-	-	-	-	+	-	-
d(600)	(200)	-	-	-	-	-	+	-	-
d(600)	(300)	-	-	-	-	-	+	-	-
d(600)	(400)	-	-	-	-	-	+	-	-
d(600)	(500)	-	-	-	-	-	+	-	-
d(600)	(600)	-	-	-	-	-	+	-	-
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(000)	+	-	-	-	+	+	+	+
d(700)	(100)	+	-	-	-	+	+	+	+
d(700)	(200)	+	+	-	-	+	+	+	+
d(700)	(300)	+	+	-	-	+	+	+	+
d(700)	(400)	+	+	+	-	+	+	+	+
d(700)	(500)	+	+	-	+	+	+	+	+
d(700)	(600)	+	+	-	+	+	+	+	+
d(700)	(700)	+	+	+	+	+	+	+	+

---



## 3 Выводы

Я получил практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

...