

Отчёт по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Виноградова Варвара Станиславовна НФИбд-01-18

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Вывод	15

List of Figures

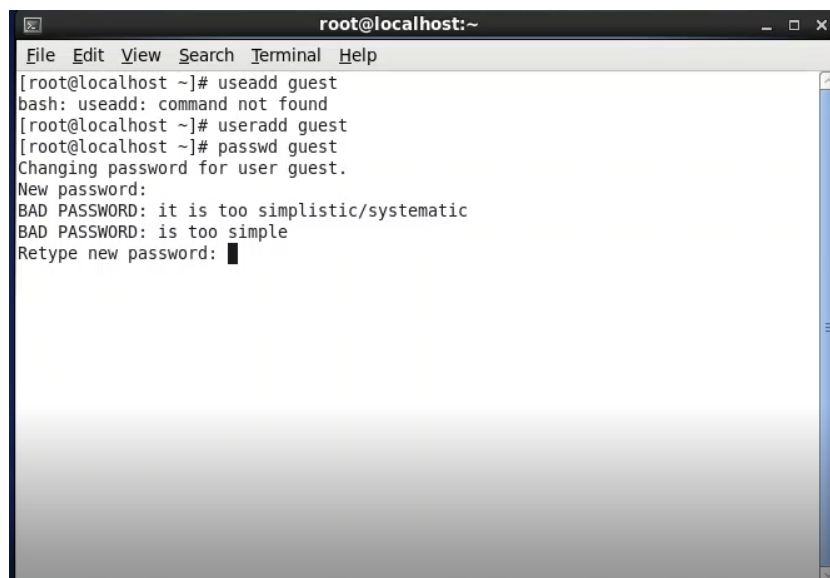
2.1	Создала пользователя guest	5
2.2	Рабочий экран guest	6
2.3	Команда pwd и cd	6
2.4	Команда whoami	7
2.5	Команда id и groups	7
2.6	Информация о пользователе guest	8
2.7	Содержимое файла /etc/passwd	9
2.8	Команда ls -l /home/	9
2.9	Расширенные атрибуты	10
2.10	Снятие атрибутов с директории	11

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 Linux1.

2 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создали учётную запись пользователя guest (используя учётную запись администратора) и задали пароль для пользователя guest (используя учётную запись администратора)



```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# useadd guest  
bash: useadd: command not found  
[root@localhost ~]# useradd guest  
[root@localhost ~]# passwd guest  
Changing password for user guest.  
New password:  
BAD PASSWORD: it is too simplistic/systematic  
BAD PASSWORD: is too simple  
Retype new password: █
```

Figure 2.1: Создала пользователя guest

2. Вошли в систему от имени пользователя guest

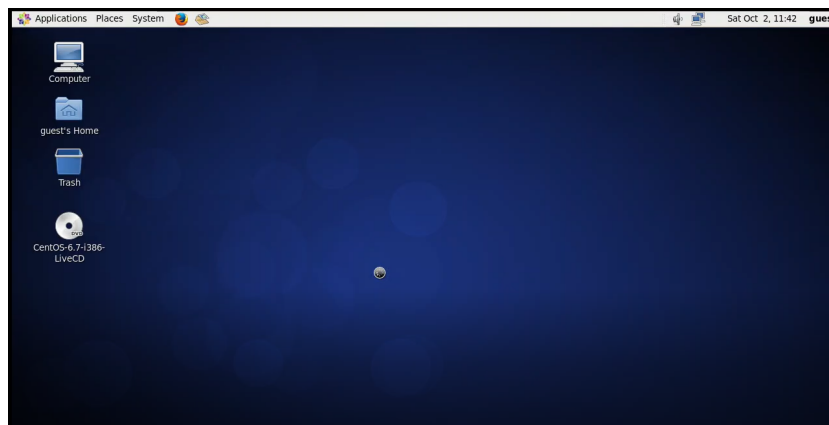


Figure 2.2: Рабочий экран guest

3. Командой `pwd` определили директорию, в которой находимся и определили является ли она домашней директорией

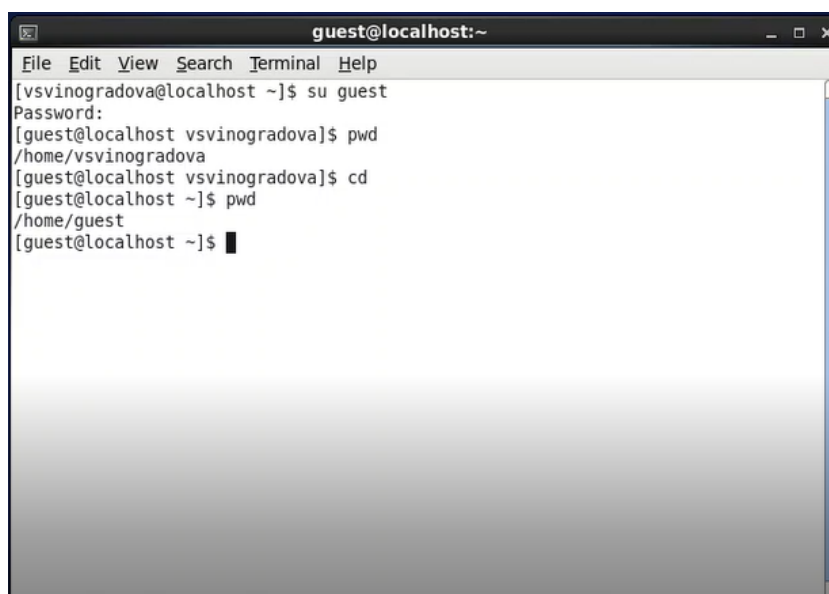
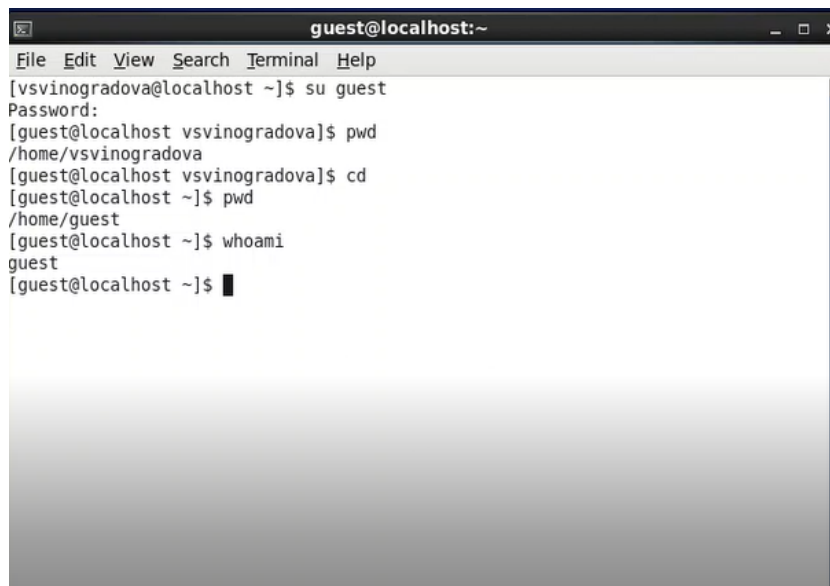


Figure 2.3: Команда `pwd` и `cd`

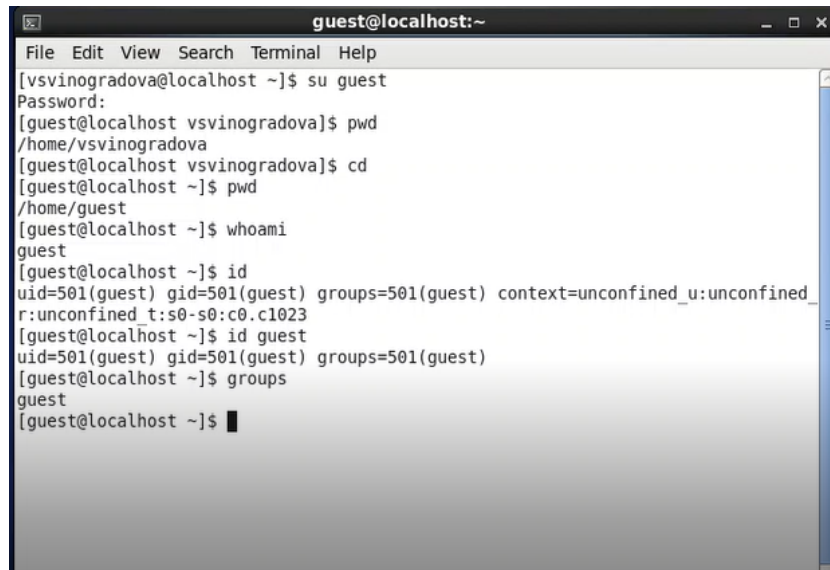
4. Уточнили имя нашего пользователя командой `whoami`:

A terminal window titled 'guest@localhost:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command history shows: [vsvinogradova@localhost ~]\$ su guest, Password:, [guest@localhost vsvinogradova]\$ pwd, /home/vsvinogradova, [guest@localhost vsvinogradova]\$ cd, [guest@localhost ~]\$ pwd, /home/guest, [guest@localhost ~]\$ whoami, guest, [guest@localhost ~]\$.

```
guest@localhost:~
File Edit View Search Terminal Help
[vsvinogradova@localhost ~]$ su guest
Password:
[guest@localhost vsvinogradova]$ pwd
/home/vsvinogradova
[guest@localhost vsvinogradova]$ cd
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ whoami
guest
[guest@localhost ~]$
```

Figure 2.4: Команда whoami

- Уточнили имя пользователя, его группу, а также группы, куда входит пользователь, командой id. Выведенные значения uid, gid и др. Сравнили вывод id с выводом команды groups. Видим, что gid и группы = 501(guest)

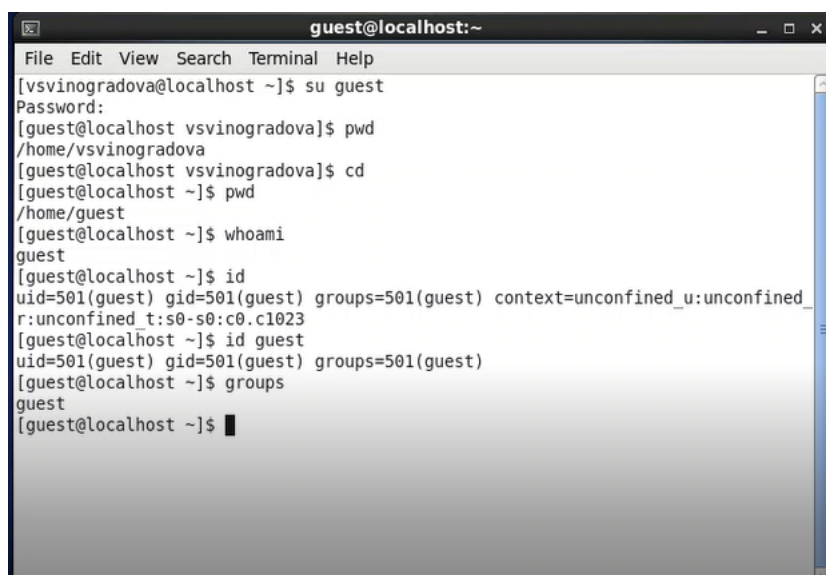
A terminal window titled 'guest@localhost:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command history shows: [vsvinogradova@localhost ~]\$ su guest, Password:, [guest@localhost vsvinogradova]\$ pwd, /home/vsvinogradova, [guest@localhost vsvinogradova]\$ cd, [guest@localhost ~]\$ pwd, /home/guest, [guest@localhost ~]\$ whoami, guest, [guest@localhost ~]\$ id, uid=501(guest) gid=501(guest) groups=501(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023, [guest@localhost ~]\$ id guest, uid=501(guest) gid=501(guest) groups=501(guest), [guest@localhost ~]\$ groups, guest, [guest@localhost ~]\$.

```
guest@localhost:~
File Edit View Search Terminal Help
[vsvinogradova@localhost ~]$ su guest
Password:
[guest@localhost vsvinogradova]$ pwd
/home/vsvinogradova
[guest@localhost vsvinogradova]$ cd
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ whoami
guest
[guest@localhost ~]$ id
uid=501(guest) gid=501(guest) groups=501(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost ~]$ id guest
uid=501(guest) gid=501(guest) groups=501(guest)
[guest@localhost ~]$ groups
guest
[guest@localhost ~]$
```

Figure 2.5: Команда id и groups

- Сравним полученную информацию об имени пользователя с данными,

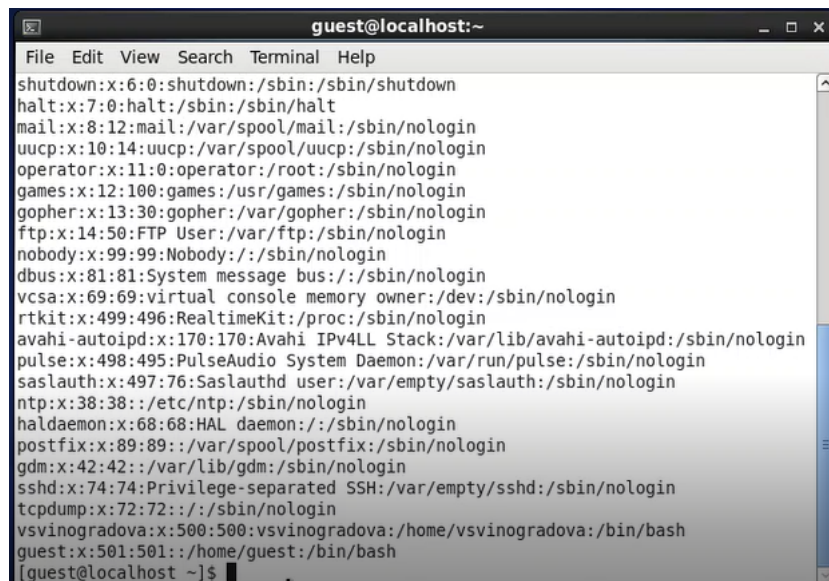
выводимыми в приглашении командной строки и убедимся, что они совпадают



```
guest@localhost:~  
File Edit View Search Terminal Help  
[vsvinogradova@localhost ~]$ su guest  
Password:  
[guest@localhost vsvinogradova]$ pwd  
/home/vsvinogradova  
[guest@localhost vsvinogradova]$ cd  
[guest@localhost ~]$ pwd  
/home/guest  
[guest@localhost ~]$ whoami  
guest  
[guest@localhost ~]$ id  
uid=501(guest) gid=501(guest) groups=501(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@localhost ~]$ id guest  
uid=501(guest) gid=501(guest) groups=501(guest)  
[guest@localhost ~]$ groups  
guest  
[guest@localhost ~]$
```

Figure 2.6: Информация о пользователе guest

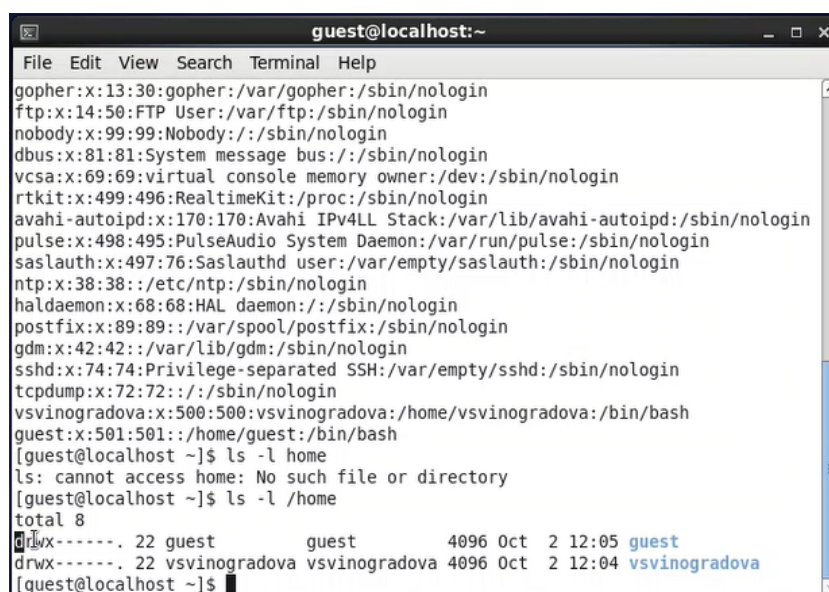
7. Просмотрим файл `/etc/passwd` Командой: `cat /etc/passwd`. Найдём в нём свою учётную запись. Определим `uid` пользователя. Определим `gid` пользователя. Сравним найденные значения с полученными в предыдущих пунктах. Guest имеет те же идентификаторы 501, наш пользователь под идентификатором 500.

A terminal window titled 'guest@localhost:~' showing the output of the 'cat /etc/passwd' command. The output lists system users and regular users with their usernames, UIDs, GIDs, names, home directories, and shell programs. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'.

```
guest@localhost:~  
File Edit View Search Terminal Help  
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
halt:x:7:0:halt:/sbin:/sbin/halt  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin  
games:x:12:100:games:/usr/games:/sbin/nologin  
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
nobody:x:99:99:Nobody:./:/sbin/nologin  
dbus:x:81:81:System message bus:./:/sbin/nologin  
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin  
rtkit:x:499:496:RealtimeKit:/proc:/sbin/nologin  
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin  
pulse:x:498:495:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
saslauth:x:497:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin  
ntp:x:38:38:./etc/ntp:/sbin/nologin  
haldaemon:x:68:68:HAL daemon:./:/sbin/nologin  
postfix:x:89:89:./var/spool/postfix:/sbin/nologin  
gdm:x:42:42:./var/lib/gdm:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
tcpdump:x:72:72:./:/sbin/nologin  
vsvinogradova:x:500:500:vsvinogradova:/home/vsvinogradova:/bin/bash  
guest:x:501:501:./home/guest:/bin/bash  
[guest@localhost ~]$
```

Figure 2.7: Содержимое файла /etc/passwd

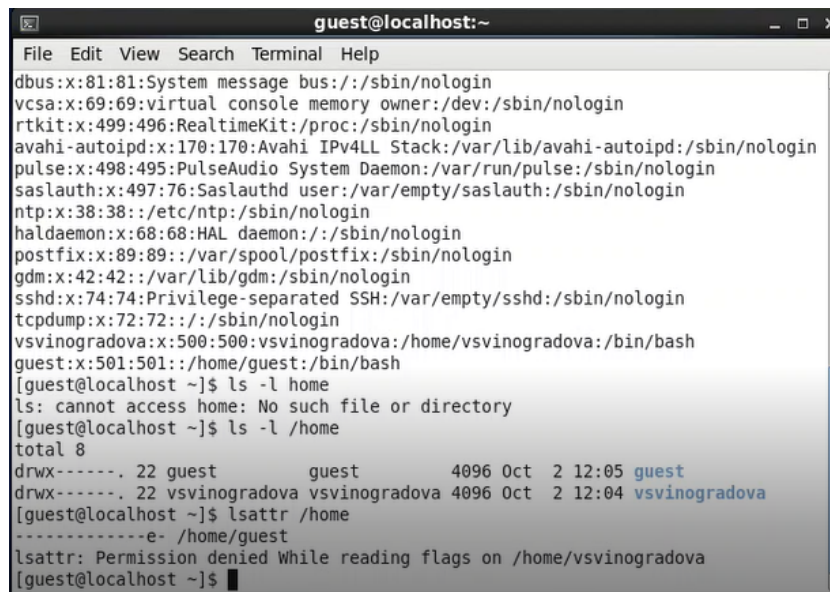
8. Определим существующие в системе директории командой `ls -l /home/`

A terminal window titled 'guest@localhost:~' showing the output of the 'ls -l /home' command. The output shows the permissions, owner, group, size, date, and name of the files in the /home directory. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'.

```
guest@localhost:~  
File Edit View Search Terminal Help  
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
nobody:x:99:99:Nobody:./:/sbin/nologin  
dbus:x:81:81:System message bus:./:/sbin/nologin  
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin  
rtkit:x:499:496:RealtimeKit:/proc:/sbin/nologin  
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin  
pulse:x:498:495:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
saslauth:x:497:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin  
ntp:x:38:38:./etc/ntp:/sbin/nologin  
haldaemon:x:68:68:HAL daemon:./:/sbin/nologin  
postfix:x:89:89:./var/spool/postfix:/sbin/nologin  
gdm:x:42:42:./var/lib/gdm:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
tcpdump:x:72:72:./:/sbin/nologin  
vsvinogradova:x:500:500:vsvinogradova:/home/vsvinogradova:/bin/bash  
guest:x:501:501:./home/guest:/bin/bash  
[guest@localhost ~]$ ls -l /home  
ls: cannot access /home: No such file or directory  
[guest@localhost ~]$ ls -l /home  
total 8  
drwx-----. 22 guest      guest      4096 Oct  2 12:05 guest  
drwx-----. 22 vsvinogradova vsvinogradova 4096 Oct  2 12:04 vsvinogradova  
[guest@localhost ~]$
```

Figure 2.8: Команда `ls -l /home/`

9. Проверили, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home`. Нам не удалось увидеть расширенные атрибуты директорий других пользователей, только своей домашней директории.

A terminal window titled 'guest@localhost:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal output shows the status of various system services like dbus, vcsa, rtkit, avahi-autoipd, pulse, saslauthd, ntp, haldaemon, postfix, gdm, sshd, tcpdump, and vsvinogradova. It then shows the output of 'ls -l /home' and 'lsattr /home', indicating that permissions have been removed from the /home directory.

```
guest@localhost:~  
File Edit View Search Terminal Help  
dbus:x:81:81:System message bus:/:/sbin/nologin  
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin  
rtkit:x:499:496:RealtimeKit:/proc:/sbin/nologin  
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin  
pulse:x:498:495:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
saslauthd:x:497:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin  
ntp:x:38:38::/etc/ntp:/sbin/nologin  
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin  
postfix:x:89:89::/var/spool/postfix:/sbin/nologin  
gdm:x:42:42::/var/lib/gdm:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
tcpdump:x:72:72::/sbin/nologin  
vsvinogradova:x:500:500:vsvinogradova:/home/vsvinogradova:/bin/bash  
guest:x:501:501::/home/guest:/bin/bash  
[guest@localhost ~]$ ls -l /home  
ls: cannot access /home: No such file or directory  
[guest@localhost ~]$ ls -l /home  
total 8  
drwx-----. 22 guest      guest      4096 Oct  2 12:05 guest  
drwx-----. 22 vsvinogradova vsvinogradova 4096 Oct  2 12:04 vsvinogradova  
[guest@localhost ~]$ lsattr /home  
-----e- /home/guest  
lsattr: Permission denied While reading flags on /home/vsvinogradova  
[guest@localhost ~]$
```

Figure 2.9: Расширенные атрибуты

10. Создали в домашней директории поддиректорию dir1 командой `mkdir dir1`.
Определим командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию dir1.
11. Сняли с директории dir1 все атрибуты командой `chmod 000 dir1` и проверили с `ls -l` помощью правильность выполнения команды `chmod`.
12. Создали в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`.
Поскольку ранее мы отозвали все атрибуты, то тем самым лишили всех прав на взаимодействие с dir1.

```

guest@localhost:~
File Edit View Search Terminal Help
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls -l
total 36
drwxr-xr-x. 2 guest guest 4096 Oct  2 11:42 Desktop
drwxrwxr-x. 2 guest guest 4096 Oct  2 12:19 dir1
drwxr-xr-x. 2 guest guest 4096 Oct  2 11:42 Documents
drwxr-xr-x. 2 guest guest 4096 Oct  2 11:42 Downloads
drwxr-xr-x. 2 guest guest 4096 Oct  2 11:42 Music
drwxr-xr-x. 2 guest guest 4096 Oct  2 11:42 Pictures
drwxr-xr-x. 2 guest guest 4096 Oct  2 11:42 Public
drwxr-xr-x. 2 guest guest 4096 Oct  2 11:42 Templates
drwxr-xr-x. 2 guest guest 4096 Oct  2 11:42 Videos
[guest@localhost ~]$ lsattr
-----e- ./Documents
-----e- ./Videos
-----e- ./Templates
-----e- ./Public
-----e- ./Desktop
-----e- ./Pictures
-----e- ./Music
-----e- ./Downloads
-----e- ./dir1
[guest@localhost ~]$ chmod 000 dir1/
[guest@localhost ~]$

```

Figure 2.10: Снятие атрибутов с директории

13. Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определим опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносим в таблицу знак «+», если не разрешена, знак «-».

- 1 - Создание файла
- 2- Удаление файла
- 3- Запись в файл
- 4- Чтение файла
- 5- Смена директории
- 6- Просмотр файлов в директории
- 7 - Переименование файла
- 8- Смена атрибутов файла

Table 2.1: Установленные права и разрешённые действия

Права директории	Права файла	1	2	3	4	5	6	7	8
d----- (000)	----- (000)	-	-	-	-	-	-	-	-

Права директории	Права файла	1	2	3	4	5	6	7	8
d--x------(100)	------(000)	-	-	-	-	+	-	-	+
d-w------(200)	------(000)	-	-	-	-	-	-	-	-
d-wx------(300)	------(000)	+	+	-	-	+	-	+	+
dr------(400)	------(000)	-	-	-	-	-	-	-	-
dr-x------(500)	------(000)	-	-	-	-	+	+	-	+
drw------(600)	------(000)	-	-	-	-	-	-	-	-
drwx------(700)	------(000)	+	+	-	-	+	+	+	+
d------(000)	---x------(100)	-	-	-	-	-	-	-	-
d--x------(100)	---x------(100)	-	-	-	-	+	-	-	+
d-w------(200)	---x------(100)	-	-	-	-	-	-	-	-
d-wx------(300)	---x------(100)	+	+	-	-	+	-	+	+
dr------(400)	---x------(100)	-	-	-	-	-	-	-	-
dr-x------(500)	---x------(100)	-	-	-	-	+	+	-	+
drw------(600)	---x------(100)	-	-	-	-	-	-	-	-
drwx------(700)	---x------(100)	+	+	-	-	+	+	+	+
d------(000)	--w------(200)	-	-	-	-	-	-	-	-
d--x------(100)	--w------(200)	-	-	+	-	+	-	-	+
d-w------(200)	--w------(200)	-	-	-	-	-	-	-	-
d-wx------(300)	--w------(200)	+	+	+	-	+	-	+	+
dr------(400)	--w------(200)	-	-	-	-	-	-	-	-
dr-x------(500)	--w------(200)	-	-	+	-	+	+	-	+
drw------(600)	--w------(200)	-	-	-	-	-	-	-	-
drwx------(700)	--w------(200)	+	+	+	-	+	+	+	+
d------(000)	--wx------(300)	-	-	-	-	-	-	-	-
d--x------(100)	--wx------(300)	-	-	+	-	+	-	-	+
d-w------(200)	--wx------(300)	-	-	-	-	-	-	-	-
d-wx------(300)	--wx------(300)	+	+	+	-	+	-	+	+

Права директории	Права файла	1	2	3	4	5	6	7	8
dr------(400)	--wx------(300)	-	-	-	-	-	-	-	-
dr-x------(500)	--wx------(300)	-	-	+	-	+	+	-	+
drw------(600)	--wx------(300)	-	-	-	-	-	-	-	-
drwx------(700)	--wx------(300)	+	+	+	-	+	+	+	+
d------(000)	-r------(400)	-	-	-	-	-	-	-	-
d--x------(100)	-r------(400)	-	-	-	+	+	-	-	+
d-w------(200)	-r------(400)	-	-	-	-	-	-	-	-
d-wx------(300)	-r------(400)	+	+	-	+	+	-	+	+
dr------(400)	-r------(400)	-	-	-	-	-	-	-	-
dr-x------(500)	-r------(400)	-	-	-	+	+	+	-	+
drw------(600)	-r------(400)	-	-	-	-	-	-	-	-
drwx------(700)	-r------(400)	+	+	-	+	+	+	+	+
d------(000)	-r-x------(500)	-	-	-	-	-	-	-	-
d--x------(100)	-r-x------(500)	-	-	-	+	+	-	-	+
d-w------(200)	-r-x------(500)	-	-	-	-	-	-	-	-
d-wx------(300)	-r-x------(500)	+	+	-	+	+	-	+	+
dr------(400)	-r-x------(500)	-	-	-	-	-	-	-	-
dr-x------(500)	-r-x------(500)	-	-	-	+	+	+	-	+
drw------(600)	-r-x------(500)	-	-	-	-	-	-	-	-
drwx------(700)	-r-x------(500)	+	+	-	+	+	+	+	+
d------(000)	-rw------(600)	-	-	-	-	-	-	-	-
d--x------(100)	-rw------(600)	-	-	+	+	+	-	-	+
d-w------(200)	-rw------(600)	-	-	-	-	-	-	-	-
d-wx------(300)	-rw------(600)	+	+	+	+	+	-	+	+
dr------(400)	-rw------(600)	-	-	-	-	-	-	-	-
dr-x------(500)	-rw------(600)	-	-	+	+	+	+	-	+
drw------(600)	-rw------(600)	-	-	-	-	-	-	-	-

Права директории	Права файла	1	2	3	4	5	6	7	8
drwx----- (700)	-rw----- (600)	+	+	+	+	+	+	+	+
d----- (000)	-rwx----- (700)	-	-	-	-	-	-	-	-
d--x----- (100)	-rwx----- (700)	-	-	+	+	+	-	-	+
d-w----- (200)	-rwx----- (700)	-	-	-	-	-	-	-	-
d-wx----- (300)	-rwx----- (700)	+	+	+	+	+	-	+	+
dr----- (400)	-rwx----- (700)	-	-	-	-	-	-	-	-
dr-x----- (500)	-rwx----- (700)	-	-	+	+	+	+	-	+
drw----- (600)	-rwx----- (700)	-	-	-	-	-	-	-	-
drwx----- (700)	-rwx----- (700)	+	+	+	+	+	+	+	+

На основании таблицы выше определили минимально необходимые права для выполнения операций внутри директории dir1 и заполнили таблицу 2.2. Для заполнения последних двух строк опытным путем проверили минимальные права.

Table 2.2: Минимальные права для совершения операций

Операция	Права на директорию	Права на файл
Создание файла	d-wx----- (300)	----- (000)
Удаление файла	d-wx----- (300)	----- (000)
Чтение файла	d--x----- (100)	-r----- (400)
Запись в файл	d--x----- (100)	--w----- (200)
Переименование файла	d-wx----- (300)	----- (000)
Создание поддиректории	d-wx----- (300)	----- (000)
Удаление поддиректории	d-wx----- (300)	----- (000)

3 Вывод

В ходе выполнения лабораторной работы были получены навыки работы с атрибутами файлов и сведения о разграничении доступа.