

Информационная безопасность.

Лабораторная работа №2.

Алли Мохамед Заян.

Содержание

1	Цель работы.....	4
2	Задание.....	5
3	Выполнение лабораторной работы	6
3.1	Таблица 2.2	20
4	Выводы.....	20

Список иллюстраций

Рис. 3.1.: Создание учетной записи гостя	6
Рис. 3.2.:Учетная запись guest.....	7
Рис. 3.3.:Результат вывода команды pwd.....	8
Рис. 3.4.:Результат команды whoami	9
Рис. 3.5.: Результат команды id.....	10
Рис. 3.6.:Результат команды groups	10
Рис. 3.7.:Результат команды cat /etc/passwd.....	11
Рис. 3.8.: Результат команды cat /etc/passwd.....	12
Рис. 3.9.:Результат команды cat /etc/passwd grep guest.....	13
Рис. 3.10.: Результат команды ls -l /home/	14
Рис. 3.11.:Результат команды lsattr /home/	14
Рис. 3.12.: Результат команды mkdir dir1	15
Рис. 3.13.:Результат команды mkdir dir1 и ls -l	16
Рис. 3.14.: Результат команды echo "test" > /home/guest/dir1/file1.....	17

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 Задание

- 1) Выполнить пункты из по порядку выполнения работы
- 2) Заполнить таблицу с правами доступа размером 64 строк
- 3) Заполнить таблицу с минимальными правами для совершения операция

3 Выполнение лабораторной работы

С помощью команды `useradd guest` создал учетную запись гостя.

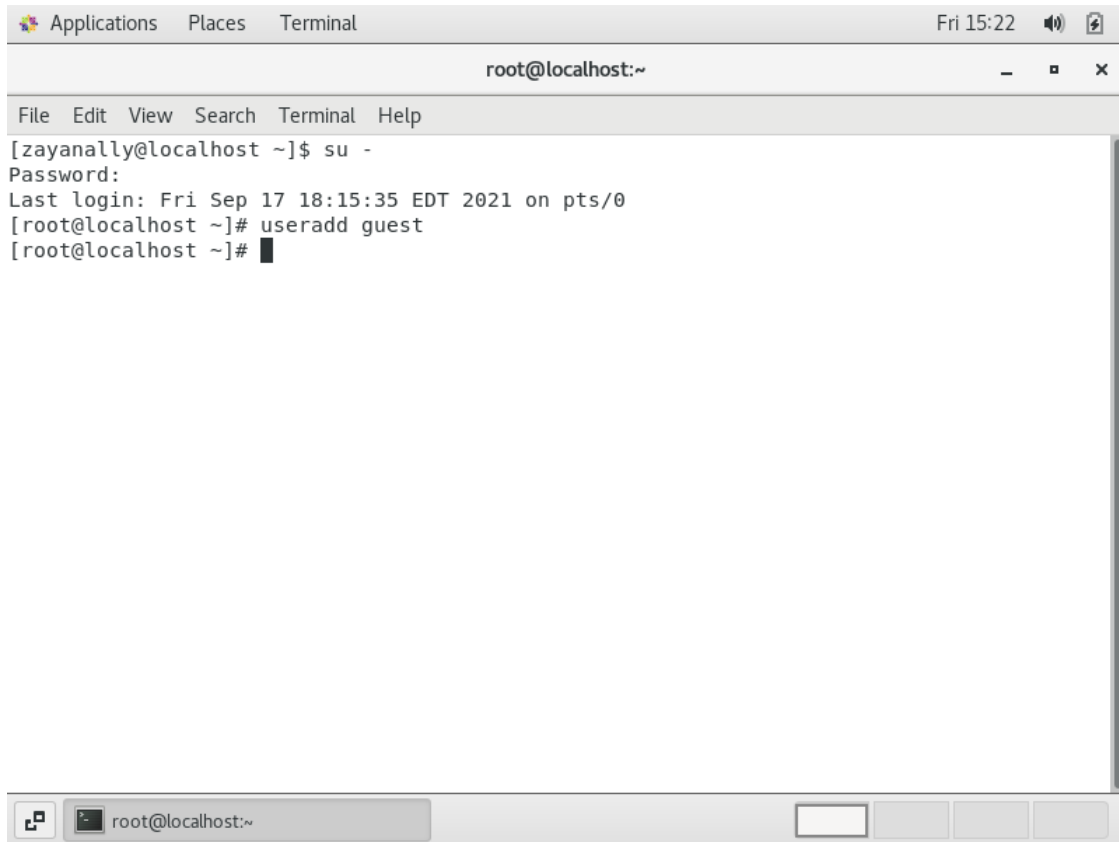


Рис. 3.1.: Создание учетной записи гостя

Задал пароль для пользователя `guest` командой `passwd guest` и зашёл от имени пользователя `guest`.

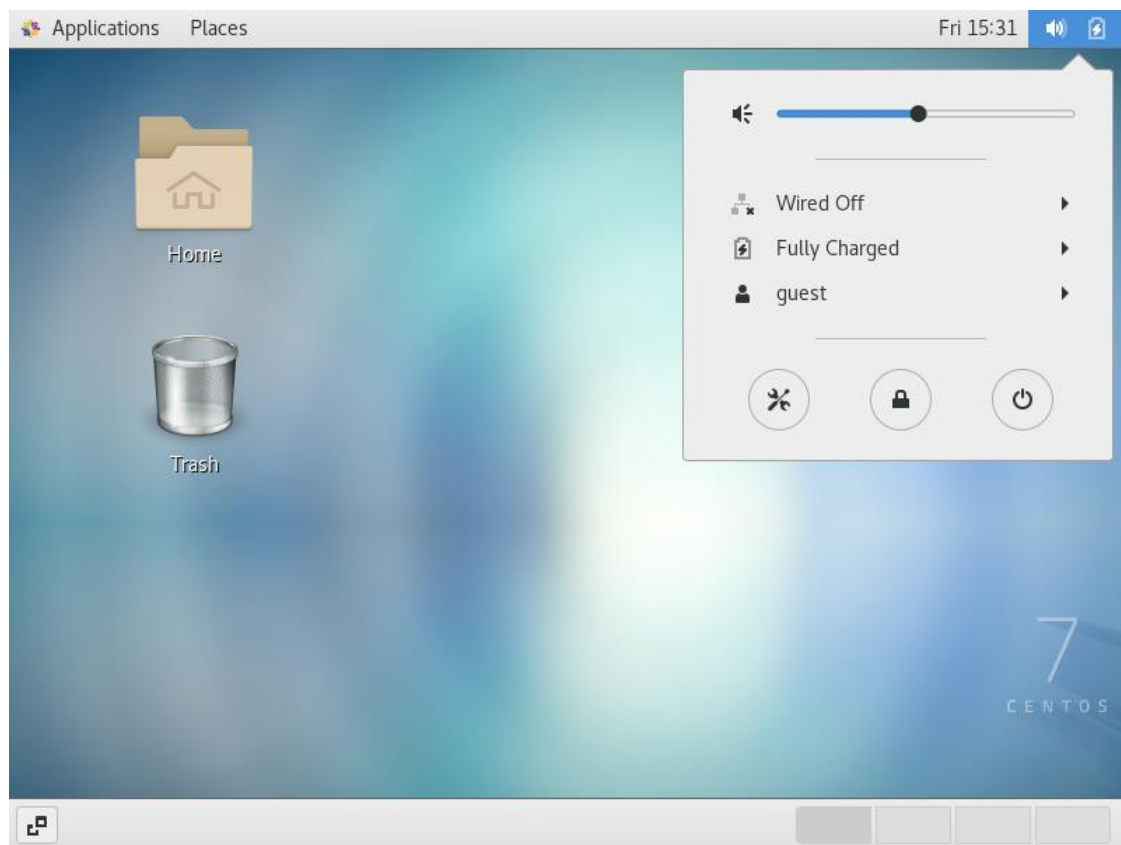


Рис. 3.2.:Учетная запись guest

Определил директорию командой `pwd`. Получил директорию `/home/guest`: да, она является домашней директорией пользователя `guest`.

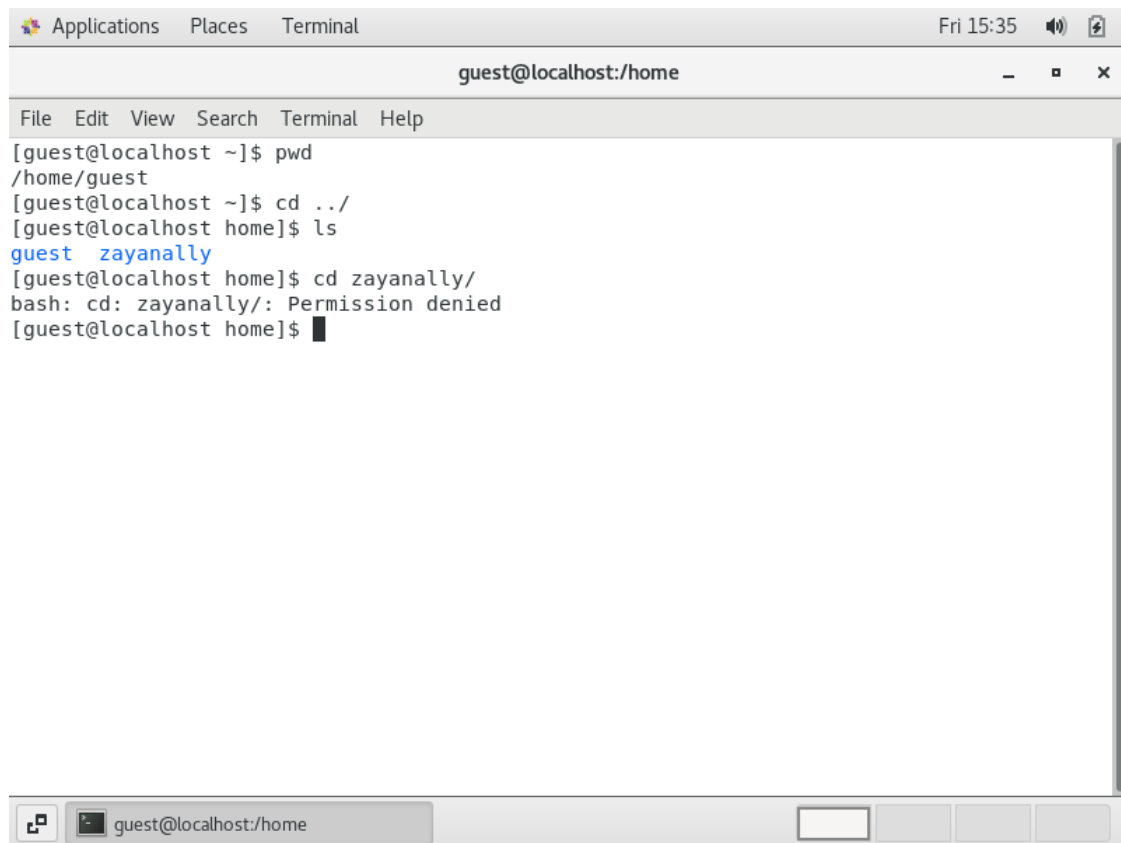
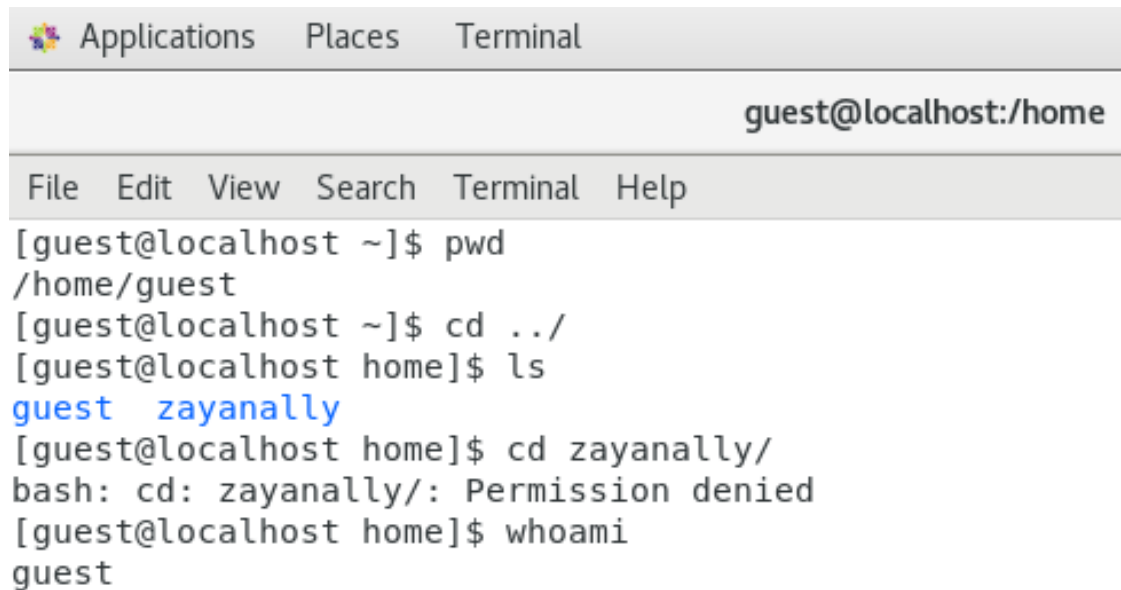


Рис. 3.3.:Результат вывода команды pwd

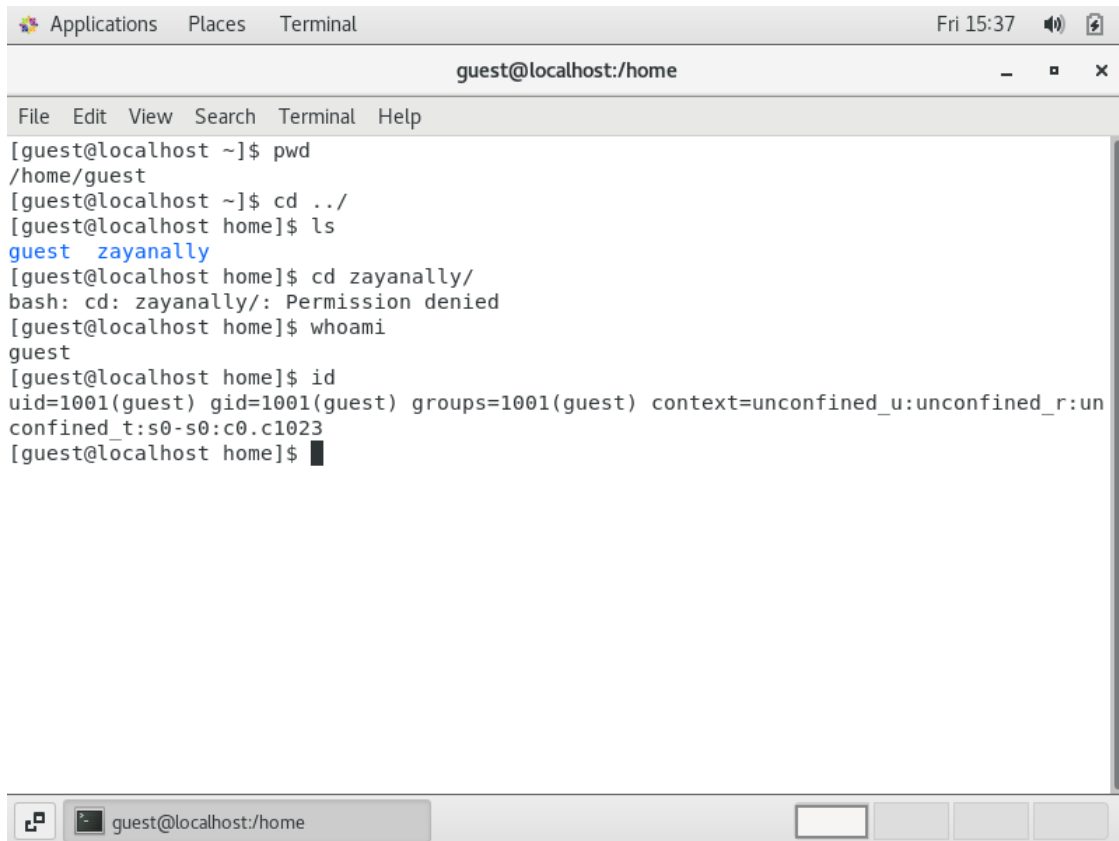
Уточнил имя пользователя командой whoami.

A terminal window with a title bar containing 'Applications', 'Places', and 'Terminal'. The window title is 'guest@localhost:/home'. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal content shows a series of commands and their outputs: 'pwd' returns '/home/guest', 'cd ../' changes the directory to '/home', 'ls' lists 'guest' and 'zayanally', 'cd zayanally/' results in a 'Permission denied' error, and 'whoami' returns 'guest'.

```
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ cd ../
[guest@localhost home]$ ls
guest  zayanally
[guest@localhost home]$ cd zayanally/
bash: cd: zayanally/: Permission denied
[guest@localhost home]$ whoami
guest
```

Рис. 3.4.:Результат команды `whoami`

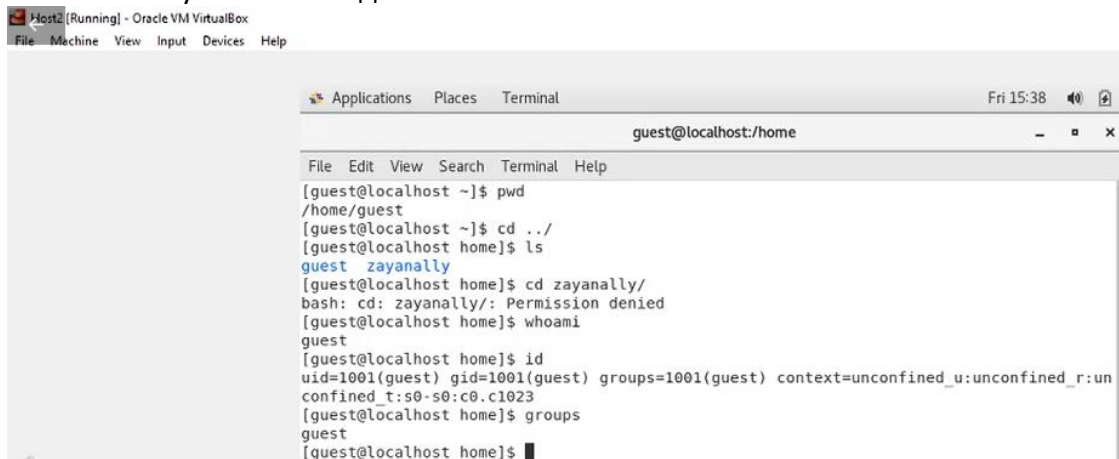
Уточнил имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Также выполнил команду `groups`. Последняя команда даёт лишь название группы, в то время как предыдущая команда даёт более расширенную информацию, в том числе номер и название группы.



A terminal window titled "guest@localhost:/home" with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (Fri 15:37). The terminal shows the following commands and output:

```
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ cd ../
[guest@localhost home]$ ls
guest  zayanally
[guest@localhost home]$ cd zayanally/
bash: cd: zayanally/: Permission denied
[guest@localhost home]$ whoami
guest
[guest@localhost home]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost home]$
```

Рис. 3.5.: Результат команды id



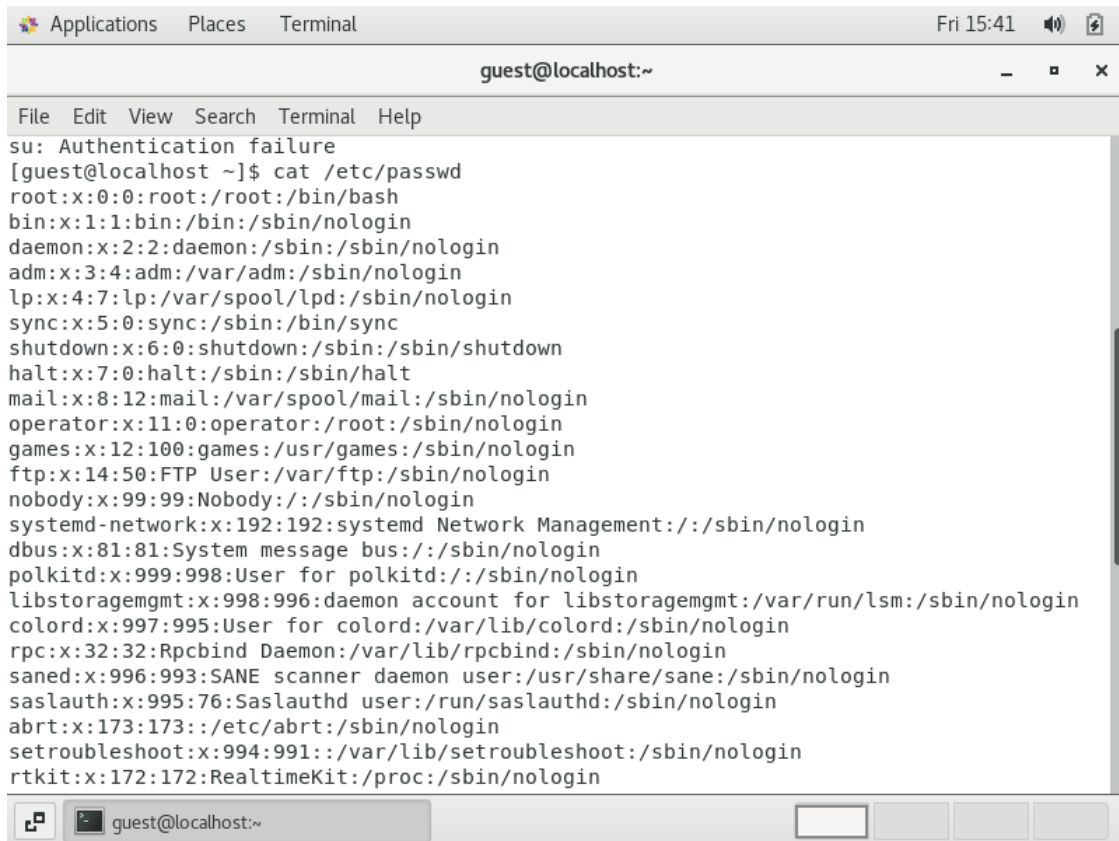
A terminal window titled "guest@localhost:/home" with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (Fri 15:38). The terminal shows the following commands and output:

```
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ cd ../
[guest@localhost home]$ ls
guest  zayanally
[guest@localhost home]$ cd zayanally/
bash: cd: zayanally/: Permission denied
[guest@localhost home]$ whoami
guest
[guest@localhost home]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost home]$ groups
guest
[guest@localhost home]$
```

Рис. 3.6.:Результат команды groups

Имя пользователя guest было получено с помощью предыдущих команд, также имя пользователя указано в приглашении командной строки, до знака @

Просмотрел файл /etc/passwd командой cat /etc/passwd. Нашёл в нём свою учетную запись, определил uid пользователя (1001) и gid пользователя (1001), эти значения совпадают со значениями, полученными ранее.



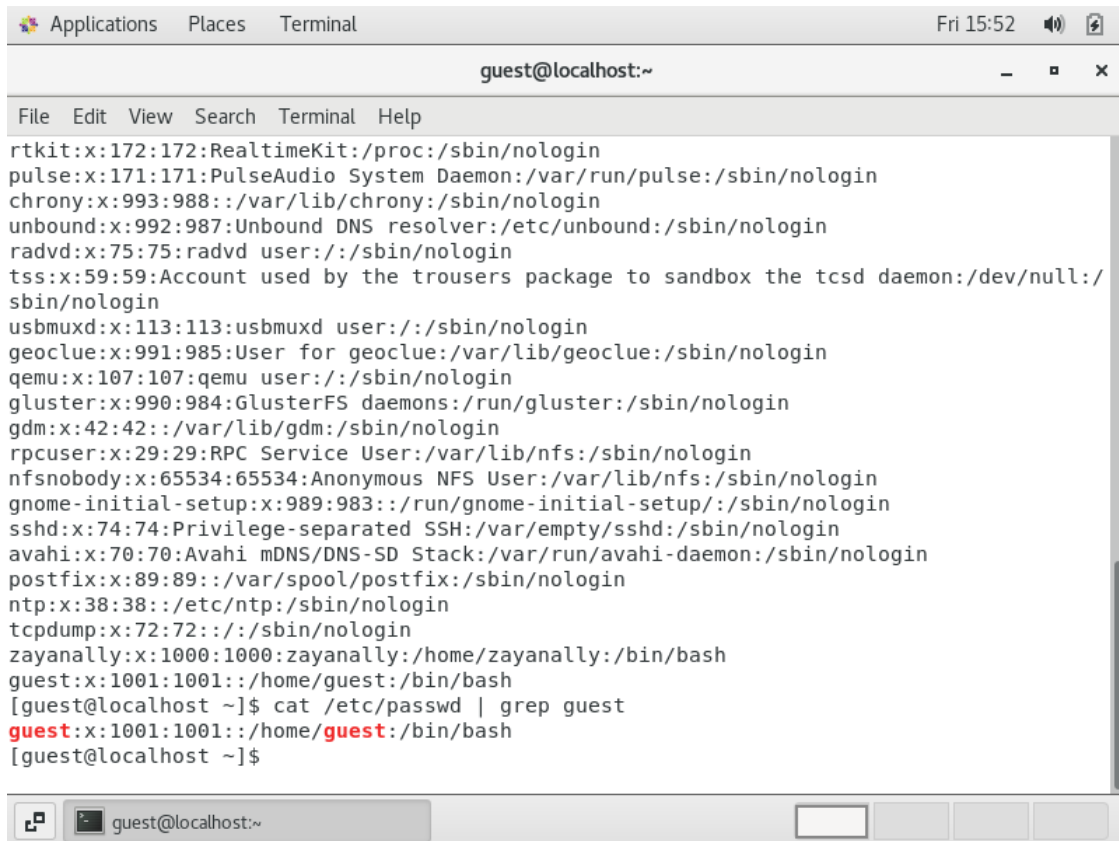
```
su: Authentication failure
[guest@localhost ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:./:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:./:/sbin/nologin
dbus:x:81:81:System message bus:./:/sbin/nologin
polkitd:x:999:998:User for polkitd:./:/sbin/nologin
libstoragemgmt:x:998:996:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
saned:x:996:993:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
sasauth:x:995:76:Sasauthd user:/run/sasauthd:/sbin/nologin
abrt:x:173:173:./etc/abrt:/sbin/nologin
setroubleshoot:x:994:991:./var/lib/setroubleshoot:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
```

Рис. 3.7.:Результат команды `cat /etc/passwd`

```
guest@localhost:~  
File Edit View Search Terminal Help  
libstoragemgmt:x:998:996:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin  
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin  
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin  
saned:x:996:993:SANE scanner daemon user:/usr/share/sane:/sbin/nologin  
saslauthd:x:995:76:Saslauthd user:/run/saslauthd:/sbin/nologin  
abrt:x:173:173:./etc/abrt:/sbin/nologin  
setroubleshoot:x:994:991:./var/lib/setroubleshoot:/sbin/nologin  
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin  
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
chrony:x:993:988:./var/lib/chrony:/sbin/nologin  
unbound:x:992:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin  
radvd:x:75:75:radvd user:/./sbin/nologin  
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin  
usbmuxd:x:113:113:usbmuxd user:/./sbin/nologin  
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin  
qemu:x:107:107:qemu user:/./sbin/nologin  
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/nologin  
gdm:x:42:42:./var/lib/gdm:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin  
gnome-initial-setup:x:989:983:./run/gnome-initial-setup:/./sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin  
postfix:x:89:89:./var/spool/postfix:/sbin/nologin  
ntp:x:38:38:./etc/ntp:/sbin/nologin
```

Рис. 3.8.: Результат команды `cat /etc/passwd`

Получил данные о пользователе с помощью команды `cat /etc/passwd | grep guest`

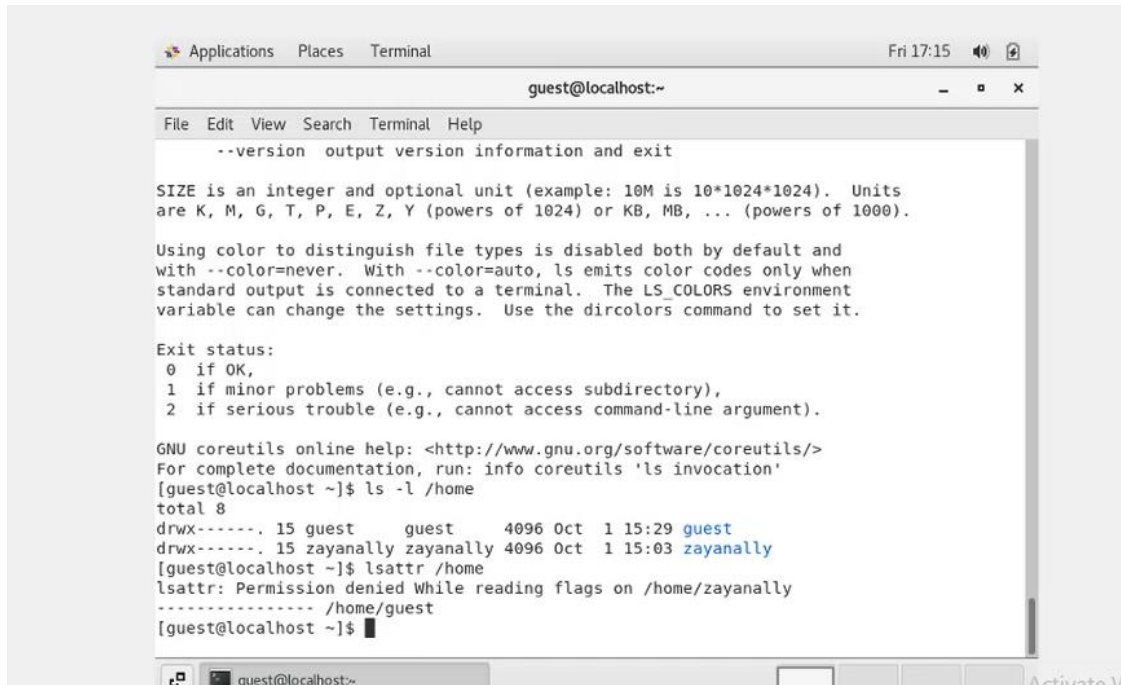


The screenshot shows a terminal window titled "guest@localhost:~". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output lists system users and their home directories. At the bottom, the command `cat /etc/passwd | grep guest` is executed, resulting in the output `guest:x:1001:1001:~/home/guest:/bin/bash`. The window's title bar indicates the time is "Fri 15:52".

```
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
chrony:x:993:988:~/var/lib/chrony:/sbin/nologin
unbound:x:992:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/nologin
gdm:x:42:42:~/var/lib/gdm:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
gnome-initial-setup:x:989:983:~/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
postfix:x:89:89:~/var/spool/postfix:/sbin/nologin
ntp:x:38:38:~/etc/ntp:/sbin/nologin
tcpdump:x:72:72:~/:/sbin/nologin
zayanally:x:1000:1000:zayanally:/home/zayanally:/bin/bash
guest:x:1001:1001:~/home/guest:/bin/bash
[guest@localhost ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:~/home/guest:/bin/bash
[guest@localhost ~]$
```

Рис. 3.9.:Результат команды `cat /etc/passwd | grep guest`

Определил существующие в системе директории командой `ls -l /home/`. Мне удалось получить список поддиректорий, в обеих директориях установлены все права только для владельца.



```
Applications  Places  Terminal  Fri 17:15  [Speaker Icon] [Refresh Icon]

guest@localhost:~

File Edit View Search Terminal Help

--version output version information and exit

SIZE is an integer and optional unit (example: 10M is 10*1024*1024). Units
are K, M, G, T, P, E, Z, Y (powers of 1024) or KB, MB, ... (powers of 1000).

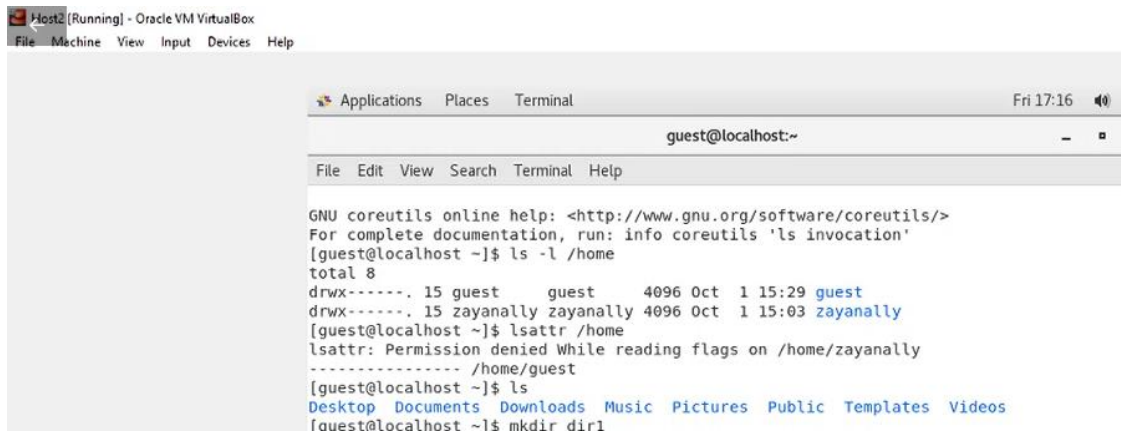
Using color to distinguish file types is disabled both by default and
with --color=never. With --color=auto, ls emits color codes only when
standard output is connected to a terminal. The LS_COLORS environment
variable can change the settings. Use the dircolors command to set it.

Exit status:
 0 if OK,
 1 if minor problems (e.g., cannot access subdirectory),
 2 if serious trouble (e.g., cannot access command-line argument).

GNU coreutils online help: <http://www.gnu.org/software/coreutils/>
For complete documentation, run: info coreutils 'ls invocation'
[guest@localhost ~]$ ls -l /home
total 8
drwx-----. 15 guest      guest      4096 Oct  1 15:29 guest
drwx-----. 15 zayanally zayanally 4096 Oct  1 15:03 zayanally
[guest@localhost ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/zayanally
----- /home/guest
[guest@localhost ~]$
```

Рис. 3.10.: Результат команды `ls -l /home/`

Проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home`. Для пользователя `iaprodmogiljnihy` я не получил результата, нет прав. Для пользователя `guest` был получен вывод.



```
Host2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Applications  Places  Terminal  Fri 17:16  [Speaker Icon]

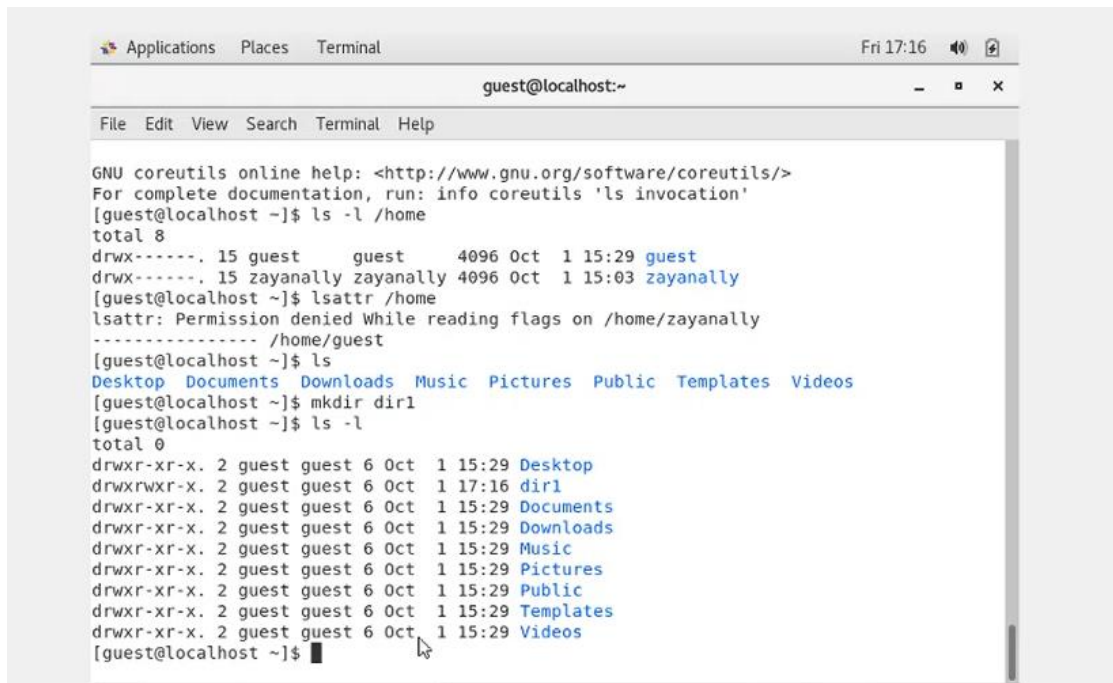
guest@localhost:~

File Edit View Search Terminal Help

GNU coreutils online help: <http://www.gnu.org/software/coreutils/>
For complete documentation, run: info coreutils 'ls invocation'
[guest@localhost ~]$ ls -l /home
total 8
drwx-----. 15 guest      guest      4096 Oct  1 15:29 guest
drwx-----. 15 zayanally zayanally 4096 Oct  1 15:03 zayanally
[guest@localhost ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/zayanally
----- /home/guest
[guest@localhost ~]$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
[guest@localhost ~]$ mkdir dir1
```

Рис. 3.11.:Результат команды `lsattr /home/`

Создал в домашней директории поддиректорию `dir1` командой `mkdir dir1`. Определил командой `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`



```
Applications  Places  Terminal  Fri 17:16
guest@localhost:~
File Edit View Search Terminal Help

GNU coreutils online help: <http://www.gnu.org/software/coreutils/>
For complete documentation, run: info coreutils 'ls invocation'
[guest@localhost ~]$ ls -l /home
total 8
drwx-----, 15 guest      guest      4096 Oct  1 15:29 guest
drwx-----, 15 zayanally  zayanally 4096 Oct  1 15:03 zayanally
[guest@localhost ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/zayanally
----- /home/guest
[guest@localhost ~]$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Oct  1 15:29 Desktop
drwxrwxr-x. 2 guest guest 6 Oct  1 17:16 dir1
drwxr-xr-x. 2 guest guest 6 Oct  1 15:29 Documents
drwxr-xr-x. 2 guest guest 6 Oct  1 15:29 Downloads
drwxr-xr-x. 2 guest guest 6 Oct  1 15:29 Music
drwxr-xr-x. 2 guest guest 6 Oct  1 15:29 Pictures
drwxr-xr-x. 2 guest guest 6 Oct  1 15:29 Public
drwxr-xr-x. 2 guest guest 6 Oct  1 15:29 Templates
drwxr-xr-x. 2 guest guest 6 Oct  1 15:29 Videos
[guest@localhost ~]$
```

Рис. 3.12.: Результат команды `mkdir dir1`

Снял с директории `dir1` все атрибуты командой `chmod 000 dir1`, и проверил её с помощью команды `ls -l`

```
Applications  Places  Terminal

guest@localhost:~/table

File Edit View Search Terminal Help

----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Desktop
d----- . 2 guest guest 6 Oct 1 17:16 dir1
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Documents
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Downloads
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Music
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Pictures
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Public
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Templates
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Videos
```

Рис. 3.13.:Результат команды `mkdir dir1` и `ls -l`

Попытался создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1`. Чтобы создать файл в директории `dir1` нужно иметь как минимум права чтения и исполнения команд (это было выяснено эмпирическим путём.). Командой `ls -l /home/guest/dir1` не удалось узнать, создан ли файл, потому что на папке установлены нулевые права.


```
Applications  Places  Terminal  Fri 18:50
guest@localhost:~/table
File Edit View Search Terminal Help
-----
./Documents
./Music
./Pictures
./Videos
./dir1
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Desktop
d----- . 2 guest guest 6 Oct 1 17:16 dir1
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Documents
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Downloads
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Music
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Pictures
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Public
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Templates
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Videos
[guest@localhost ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@localhost ~]$ ls -l /home/guest/dir1
ls: cannot open directory /home/guest/dir1: Permission denied
[guest@localhost ~]$ chmod u=rwx dir1
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Oct 1 15:29 Desktop
drwx----- . 2 guest guest 6 Oct 1 17:16 dir1
```

Рис. 3.14.: Результат команды echo "test" > /home/guest/dir1/file1

Заполнил таблицу 2.1. Я последовательно изменял права gwx для администратора, а затем gwx для группы. В итоге получил 70 строк в таблице (но я не претендую на правильность интерпритации задания). Последние 2 пачки строк не заполнены, потому что они являются лишь повторением последней заполненной пачки строк (от 010 до 700)

Пр дир	Пр ф	Созд ф	Уд ф	Зап в ф	Чт ф	Смена дир	Просм ф-в в дир	Переим ф	См атриб ф
000	000	-	-	-	-	-	-	-	-
100	000	-	-	-	-	+	-	-	+
300	000	+	+	-	-	+	-	+	+
700	000	+	+	-	-	+	+	+	+
010	000	-	-	-	-	-	-	-	-
030	000	-	-	-	-	-	-	-	-
070	000	-	-	-	-	-	-	-	-
710	000	+	+	-	-	+	+	+	+
730	000	+	+	-	-	+	+	+	+
770	000	+	+	-	-	+	+	+	+

000	100	-	-	-	-	-	-	-	-
100	100	-	-	-	-	+	-	-	+
300	100	+	+	-	-	+	-	+	+
700	100	+	+	-	-	+	+	+	+
010	100	-	-	-	-	-	-	-	-
030	100	-	-	-	-	-	-	-	-
070	100	-	-	-	-	-	-	-	-
710	100	+	+	-	-	+	+	+	+
730	100	+	+	-	-	+	+	+	+
770	100	+	+	-	-	+	+	+	+
000	300	-	-	-	-	-	-	-	-
300	300	+	+	+	-	+	-	+	+
100	300	-	-	+	-	+	-	-	+
700	300	+	+	+	-	+	+	+	+
010	300	-	-	-	-	-	-	-	-
030	300	-	-	-	-	-	-	-	-
070	300	-	-	-	-	-	-	-	-
710	300	+	+	+	-	+	+	+	+
730	300	+	+	+	-	+	+	+	+
770	300	+	+	+	-	+	+	+	+
000	700	-	-	-	-	-	-	-	-
100	700	-	-	+	+	+	-	-	+
300	700	+	+	+	+	+	-	+	+
700	700	+	+	+	+	+	+	+	+
010	700	-	-	-	-	-	-	-	-
030	700	-	-	-	-	-	-	-	-
070	700	-	-	-	-	-	-	-	-
710	700	+	+	+	+	+	+	+	+
730	700	+	+	+	+	+	+	+	+
770	700	+	+	+	+	+	+	+	+
000	710	-	-	-	-	-	-	-	-
100	710	-	-	+	+	+	-	-	+
300	710	+	+	+	+	+	-	+	+
700	710	+	+	+	+	+	+	+	+
010	710								

Заполнил таблицу 2.2 с минимальными правами для совершения операция.

3.1 Таблица 2.2

Операция	Мин пр на дир	Мин пр на ф
Создание файла	wx	rw (default when crating the file)
Удаление файла	wx	w
Чтение файла	x	r
Запись в файл	x	w
Переименование файла	wx	- - -
Создание поддиректории	wx	- - -
Удаление поддиректории	wx	- - -

4 Выводы

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