

Информационная безопасность.

Лабораторная работа №2.

Подмогильный Иван Александрович.

Содержание

1. Цель работы	5
2. Задание	6
3. Выполнение лабораторной работы	7
3.1. Таблица 2.2	19
4. Выводы	21

Список таблиц

Список иллюстраций

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

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.

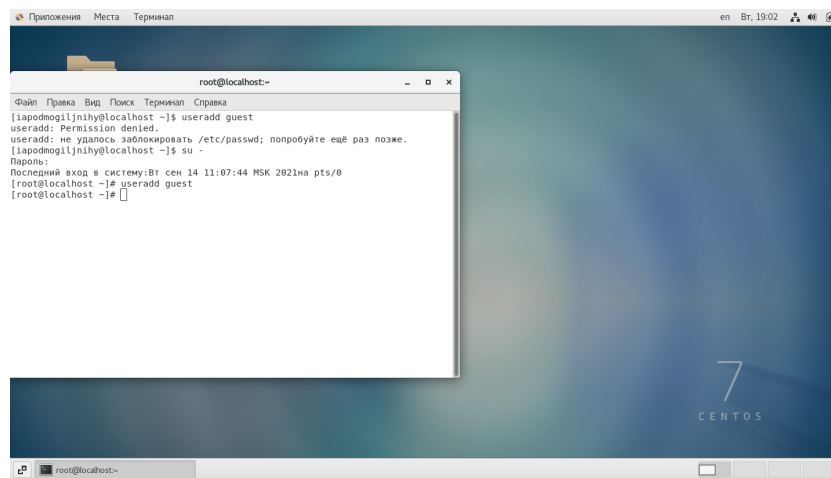


Рис. 3.1.: Создание учетной записи гостя

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

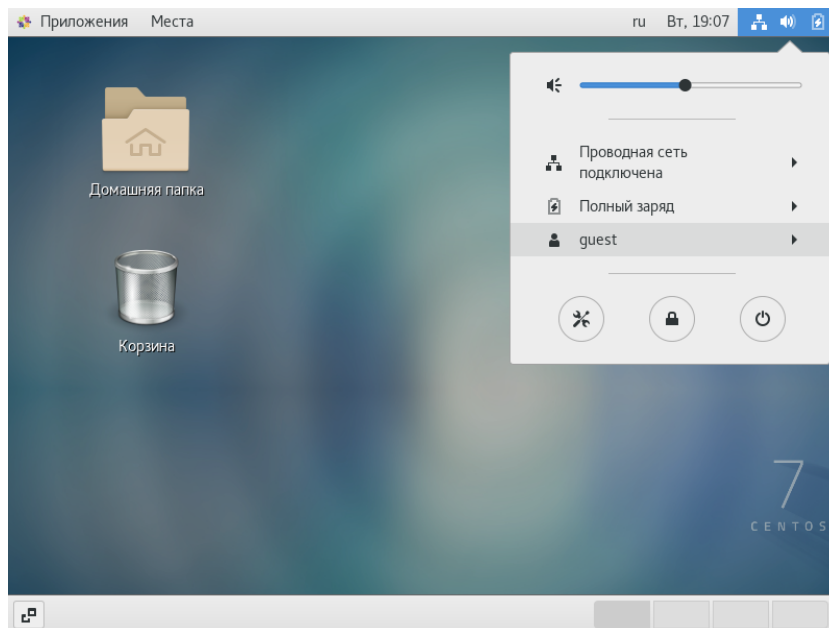


Рис. 3.2.: Учетная запись guest

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

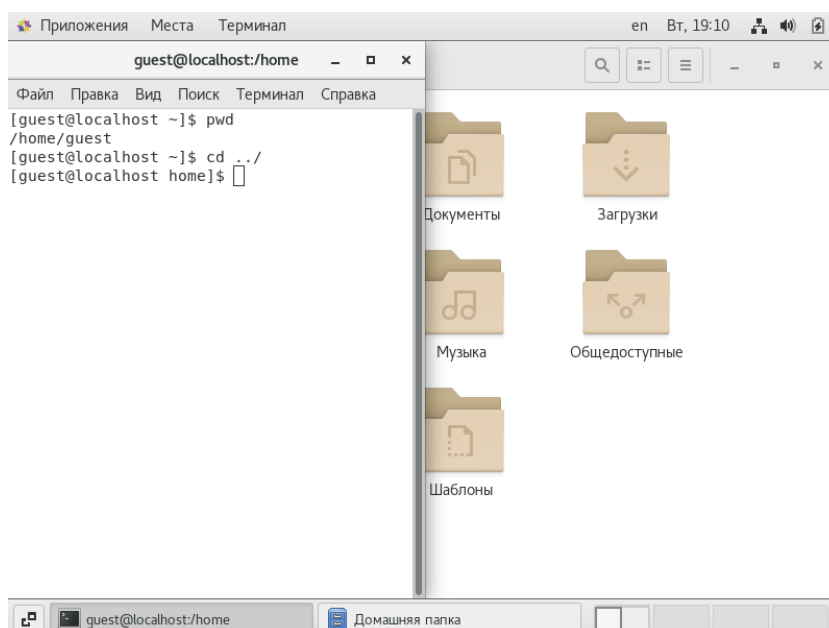


Рис. 3.3.: Результат вывода команды `pwd`

Уточнил имя пользователя командой `whoami`.

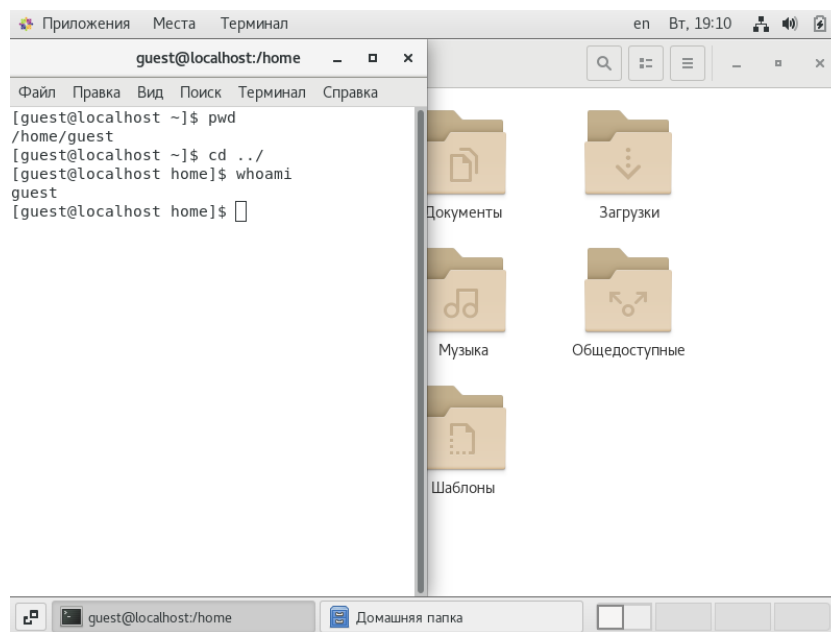


Рис. 3.4.: Результат команды `whoami`

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.

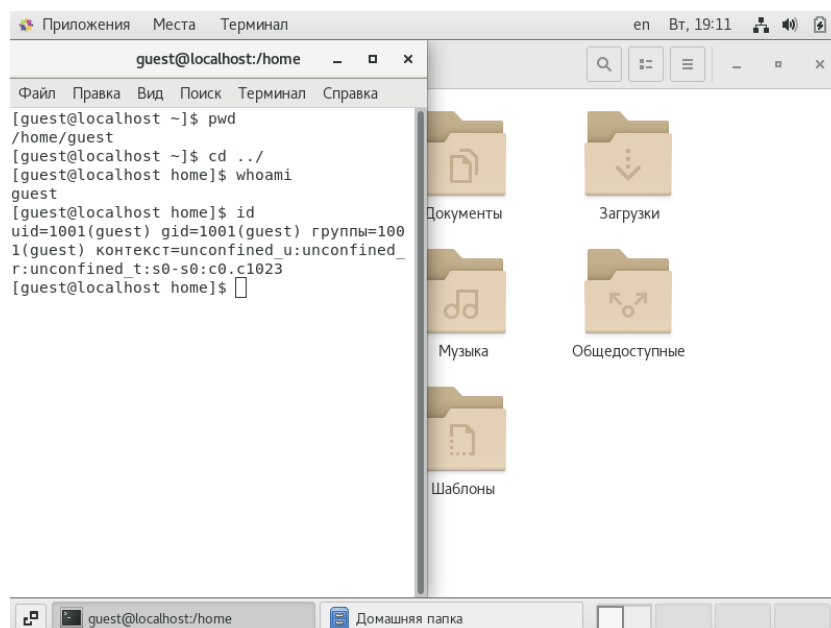


Рис. 3.5.: Результат команды id

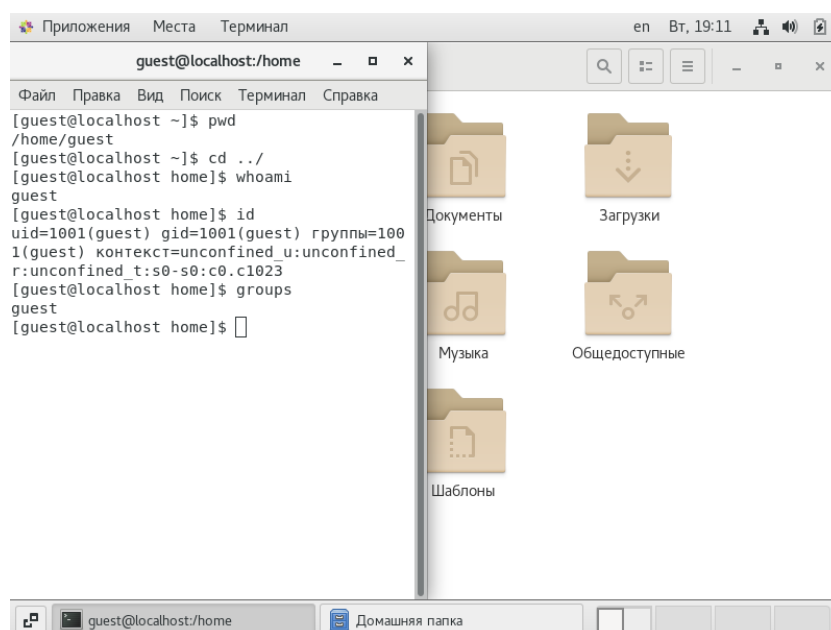
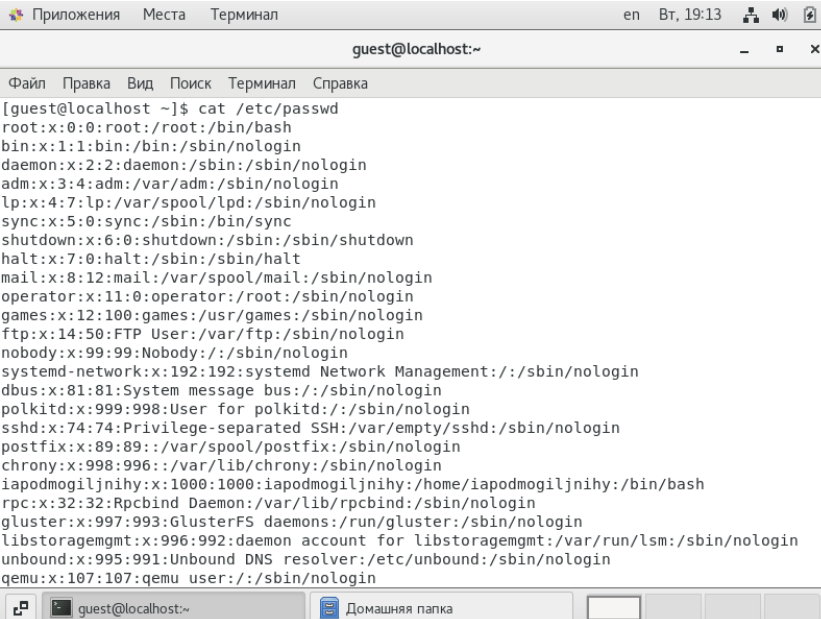


Рис. 3.6.: Результат команды groups

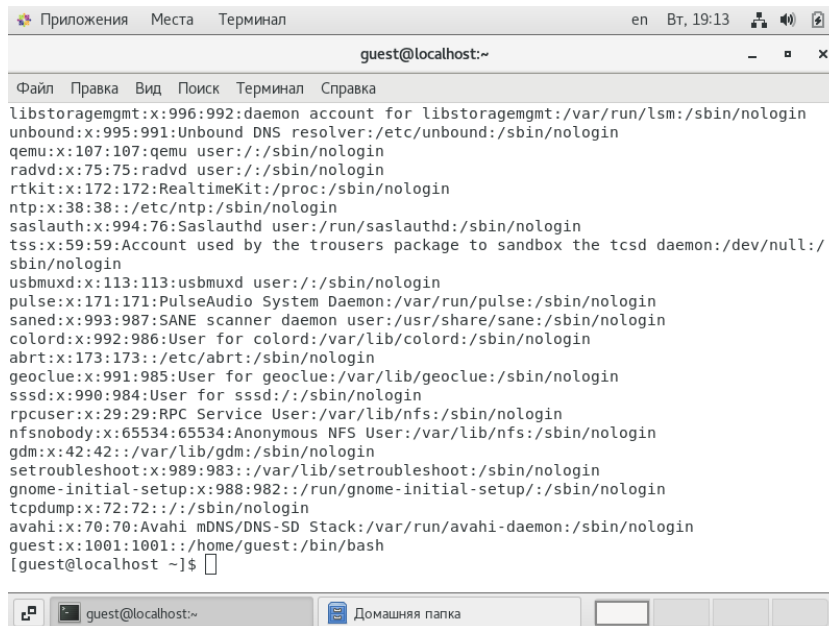
Имя пользователя guest было получено с помощью предыдущих команд, также имя пользователя указано в приглашении командной строки, до знака @

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.



```
guest@localhost:~  
[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  
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin  
postfix:x:89:89:/:/var/spool/postfix:/sbin/nologin  
chrony:x:998:996:/:/var/lib/chrony:/sbin/nologin  
iapodmogiljniy:x:1000:1000:iapodmogiljniy:/home/iapodmogiljniy:/bin/bash  
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin  
gluster:x:997:993:GlusterFS daemons:/run/gluster:/sbin/nologin  
libstoragemgmt:x:996:992:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin  
unbound:x:995:991:Unbound DNS resolver:/etc/unbound:/sbin/nologin  
qemu:x:107:107:qemu user:/:/sbin/nologin
```

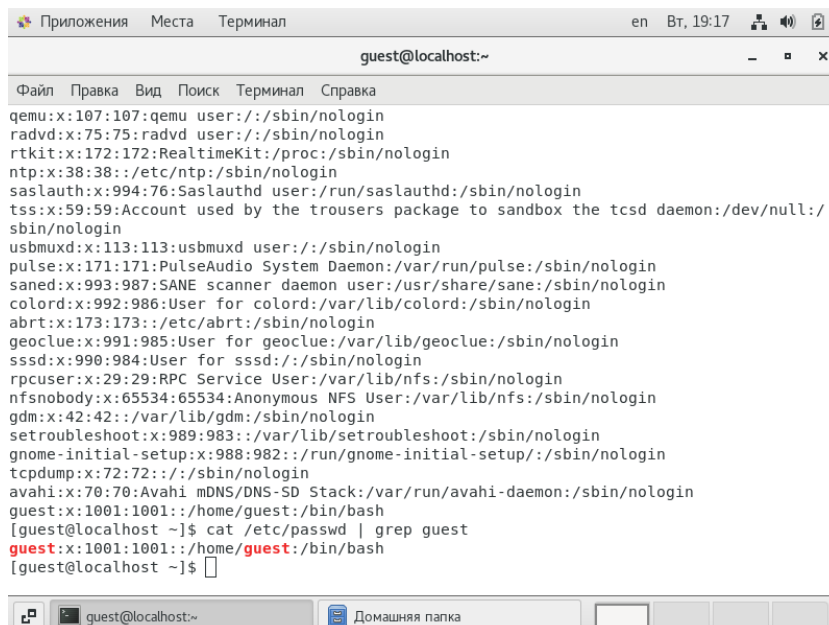
Рис. 3.7.: Результат команды `cat /etc/passwd`



```
libstorage:x:996:992:daemon account for libstorage:/var/run/lsm:/sbin/nologin
unbound:x:995:991:Unbound DNS resolver:/etc/unbound:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
ntp:x:38:38:/etc/ntp:/sbin/nologin
saslauth:x:994:76:Saslauthd user:/run/saslauthd:/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
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
saned:x:993:987:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
colord:x:992:986:User for colord:/var/lib/colord:/sbin/nologin
abrt:x:173:173:/etc/abrt:/sbin/nologin
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin
sssd:x:990:984:User for sssd:/:/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
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
setroubleshoot:x:989:983:/var/lib/setroubleshoot:/sbin/nologin
gnome-initial-setup:x:988:982:/run/gnome-initial-setup:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
guest:x:1001:1001:/home/guest:/bin/bash
[guest@localhost ~]$
```

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

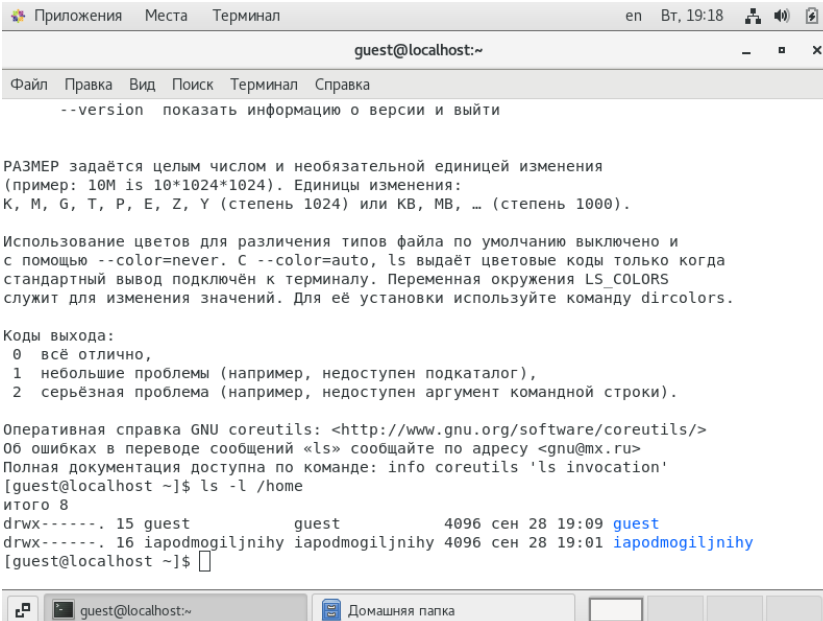
Получил данные о пользователе с помощью команды `cat /etc/passwd | grep guest`



```
qemu:x:107:107:qemu user:/:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
ntp:x:38:38:/etc/ntp:/sbin/nologin
saslauth:x:994:76:Saslauthd user:/run/saslauthd:/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
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
saned:x:993:987:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
colord:x:992:986:User for colord:/var/lib/colord:/sbin/nologin
abrt:x:173:173:/etc/abrt:/sbin/nologin
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin
sssd:x:990:984:User for sssd:/:/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
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
setroubleshoot:x:989:983:/var/lib/setroubleshoot:/sbin/nologin
gnome-initial-setup:x:988:982:/run/gnome-initial-setup:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
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.



```
Приложения Места Терминал en Вт, 19:18
guest@localhost:~
Файл Правка Вид Поиск Терминал Справка
--version показать информацию о версии и выйти

РАЗМЕР задаётся целым числом и необязательной единицей изменения
(пример: 10M is 10*1024*1024). Единицы изменения:
K, M, G, T, P, E, Z, Y (степень 1024) или KB, MB, ... (степень 1000).

Использование цветов для различения типов файла по умолчанию выключено и
с помощью --color=never. С --color=auto, ls выдаёт цветовые коды только когда
стандартный вывод подключён к терминалу. Переменная окружения LS_COLORS
служит для изменения значений. Для её установки используйте команду dircolors.

Коды выхода:
0 всё отлично,
1 небольшие проблемы (например, недоступен подкаталог),
2 серьёзная проблема (например, недоступен аргумент командной строки).

Оперативная справка GNU coreutils: <http://www.gnu.org/software/coreutils/>
Об ошибках в переводе сообщений «ls» сообщайте по адресу <gnu@mx.ru>
Полная документация доступна по команде: info coreutils 'ls invocation'
[guest@localhost ~]$ ls -l /home
итого 8
drwx-----. 15 guest      guest      4096 сен 28 19:09 guest
drwx-----. 16 iapodmogiljniy iapodmogiljniy 4096 сен 28 19:01 iapodmogiljniy
[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 `iapodmogiljniy` я не получил результата, нет прав. Для пользователя `guest` был получен вывод.

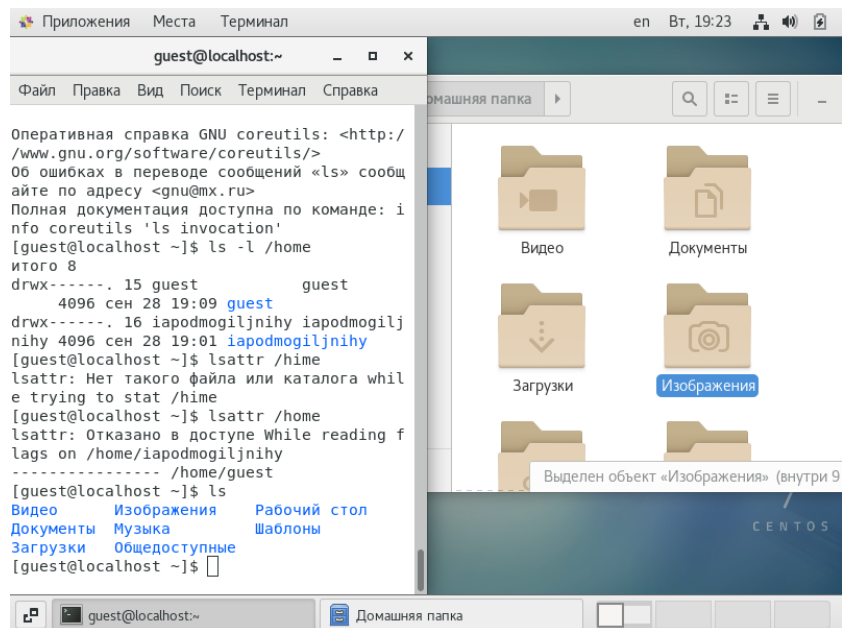


Рис. 3.11.: Результат команды `lsattr /home/`

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`

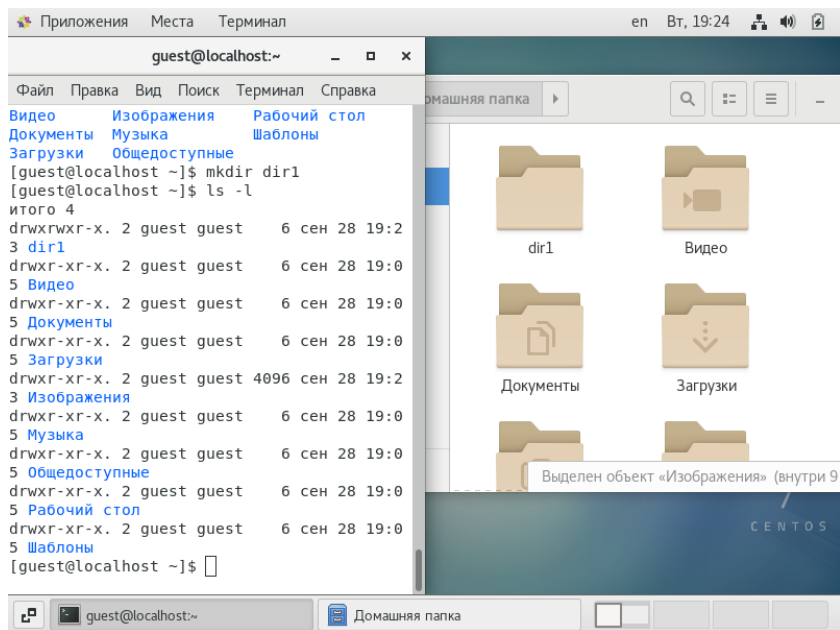


Рис. 3.12.: Результат команды `mkdir dir1`

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

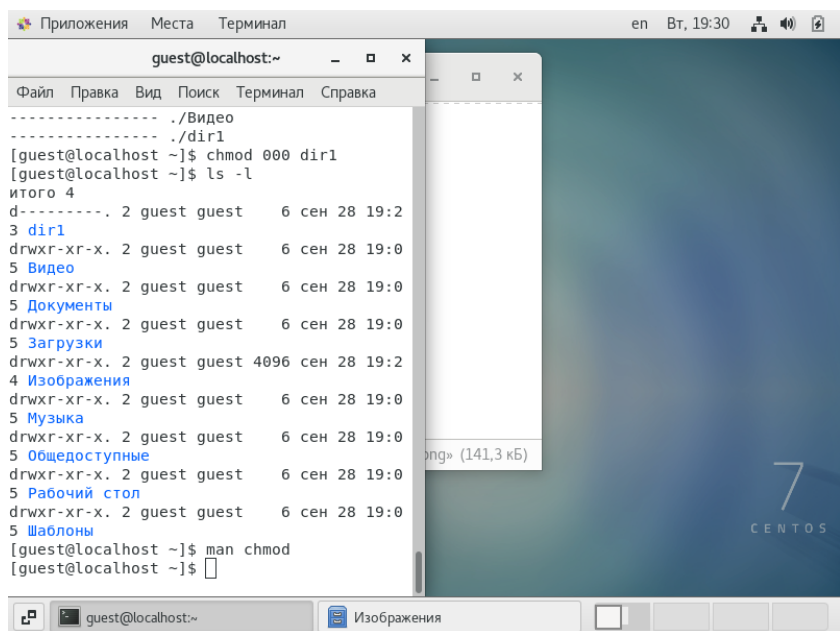


Рис. 3.13.: Результат команды `mkdir dir1` и `ls -l`

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, созданся ли файл, потому что на папке установлены нулевые права.

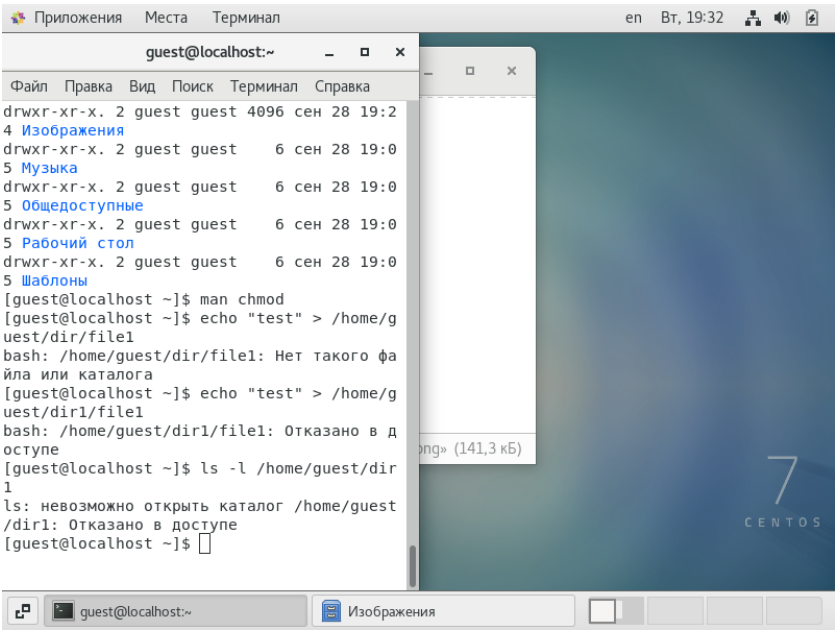


Рис. 3.14.: Результат команды echo "test" > /home/guest/dir1/file1

Заполнил таблицу 2.1. Я последовательно изменял права rwx для администратора, а затем rwx 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	-	-	-	-	-	-	-	-

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
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	-	-	-	-	-	-	-	-

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
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								
030	710								
070	710								
710	710								
730	710								
770	710								
000	730								

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

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.