

Task2(Part2)

1) Analyze the structure of the /etc/passwd and /etc/group file, what fields are present in it, what users exist on the system? Specify several pseudo-users, how to define them?

The /etc/passwd file contains a list of users known to the system. During the user registration process, the system accesses this file in search of the user ID and home directory. Each line of the file describes one user and 7 fields separated by colons:

1 username – registration names must be unique and contain no more than 32 characters.

2 pswd – password or password "filler".

3 UID is a 32-bit integer that uniquely identifies a user on the system.

4 GID. Like the user ID, the group ID (GID) is a 32-bit integer.

5 UID comments/ The GECOS field is mainly used to store personal information about each user. It does not have a well-defined syntax.

6 Home directory. Upon logging in, the user is taken to their home directory.

7 Shell – program name the user's command interpreter

```
student@CsnKhai:~$ cat /etc/group
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:/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:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
student:x:1000:1000:Student KhAI,,,:/home/student:/bin/bash
nureshnik:x:1001:1001:Dmitriy Korkhov,12,+380990167617,,ato201588@gmail.com:/home/nureshnik:/bin/bash
student@CsnKhai:~$ _
```

The /etc/group file contains the names of the groups present in the Linux OS and lists the members of each group. Each entry in the /etc/group file represents one group and contains 4 fields:

- 1 Group_name. By default, when a new user is created, its group is also created with the same name as the user's login name.
- 2 Password or character x indicating use of the /etc/gshadow file;
- 3 Group_ID. (number)
- 4 List of members separated by commas without spaces

Pseudo users Each of the UNIX variants contains pseudo user description lines in the password file These descriptions are never edited Users of these names are not registered in the system and are only needed to confirm ownership of the processes The most used are

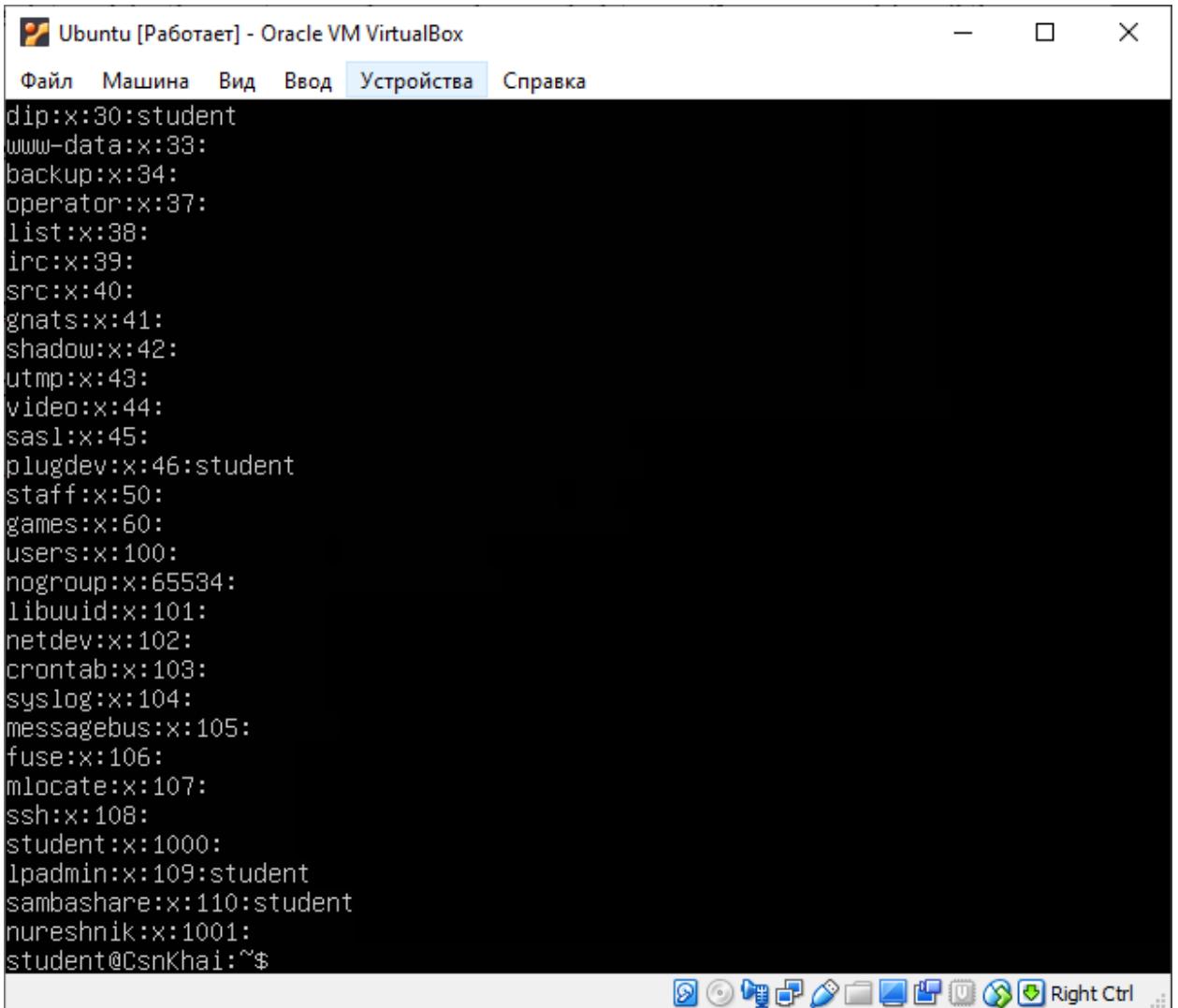
daemon – Used by system service processes

bin – Gives ownership of executables command

adm – Owns registration files

nobody – Used by many services

sshd – used by the secure shell server



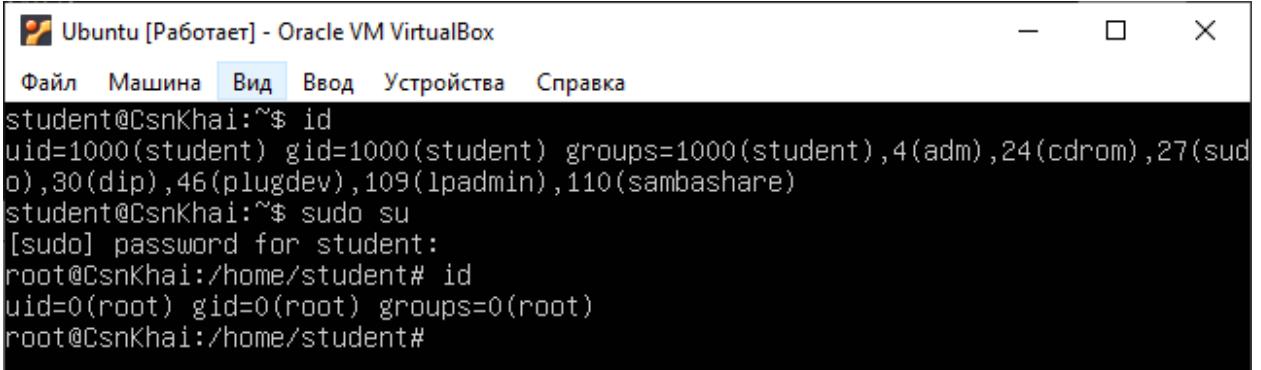
The screenshot shows a terminal window titled "Ubuntu [Работает] - Oracle VM VirtualBox". The window has a menu bar with Russian labels: Файл, Машина, Вид, Ввод, Устройства (Devices), and Справка. The "Устройства" tab is currently selected. The main area of the terminal displays a list of pseudo users from the /etc/passwd file. The output is as follows:

```
dip:x:30:student
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:student
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
libuuid:x:101:
netdev:x:102:
crontab:x:103:
syslog:x:104:
messagebus:x:105:
fuse:x:106:
mlocate:x:107:
ssh:x:108:
student:x:1000:
lpadmin:x:109:student
sambashare:x:110:student
nureshnik:x:1001:
student@CsnKhai:~$
```

The terminal window includes a toolbar at the bottom with various icons for file operations like copy, paste, and search.

2) What are the uid ranges? What is UID? How to define it?

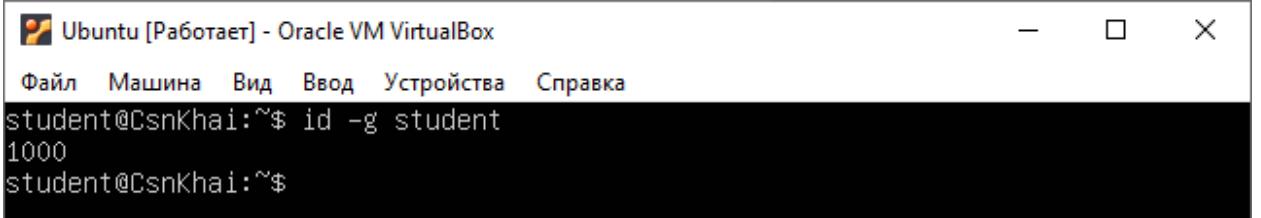
UID – unique identifier of the user within the system. UID is a simple numeric designation for an individual user. This is usually a positive number not more than 65535 (sometimes 32 bit). Some identifiers are reserved for special use. These include 0 (root), 1 999(daemons, pseudo users, system and reserved users), 1000+ (regular users).



```
Ubuntu [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
student@CsnKhai:~$ id
uid=1000(student) gid=1000(student) groups=1000(student),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),109(lpadmin),110(sambashare)
student@CsnKhai:~$ sudo su
[sudo] password for student:
root@CsnKhai:/home/student# id
uid=0(root) gid=0(root) groups=0(root)
root@CsnKhai:/home/student#
```

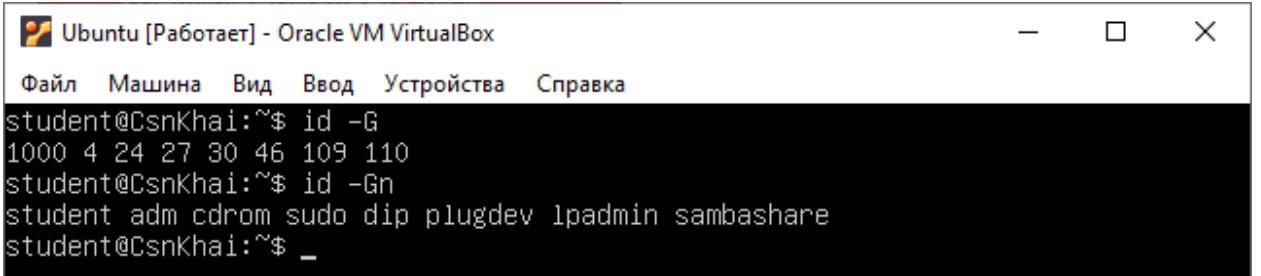
3) What is GID? How to define it?

GID – unique identifier of the group within the system to which the user belongs.



```
Ubuntu [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
student@CsnKhai:~$ id -g student
1000
student@CsnKhai:~$
```

4) How to determine belonging of user to the specific group?



```
Ubuntu [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
student@CsnKhai:~$ id -G
1000 4 24 27 30 46 109 110
student@CsnKhai:~$ id -Gn
student adm cdrom sudo dip plugdev lpadmin sambashare
student@CsnKhai:~$ _
```

5) What are the commands for adding a user to the system? What are the basic parameters required to create a user?

```
Ubuntu [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
student@CsnKhai:~$ sudo useradd -m User
student@CsnKhai:~$ sudo passwd User
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
student@CsnKhai:~$ su User
Password:
User@CsnKhai:/home/student$ pwd
/home/student
User@CsnKhai:/home/student$
```

```
Ubuntu [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Ubuntu 14.04.6 LTS CsnKhai tty1
CsnKhai login: User
Password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 3.13.0-63-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

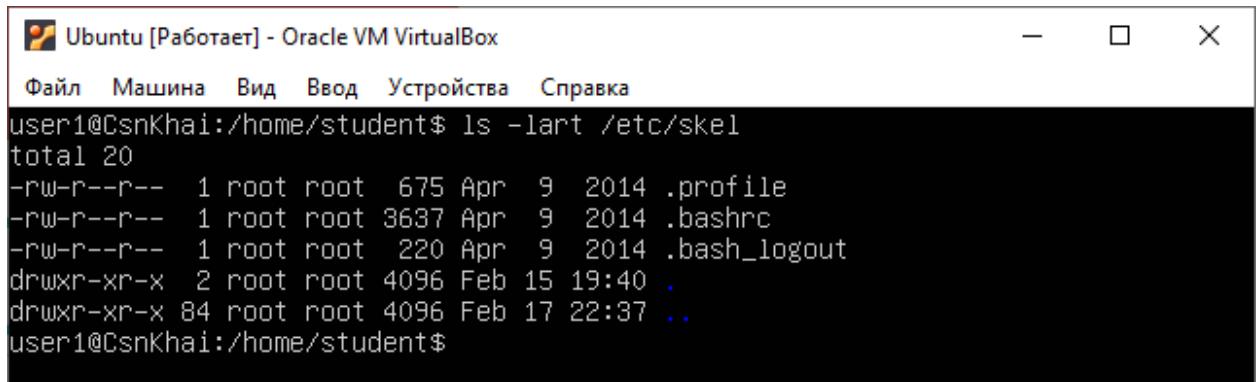
User@CsnKhai:~$ pwd
/home/User
User@CsnKhai:~$ _
```

6) How do I change the name (account name) of an existing user?

```
Ubuntu [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
student@CsnKhai:~$ sudo usermod -l user1 User
student@CsnKhai:~$ su user1
Password:
user1@CsnKhai:/home/student$ _
```

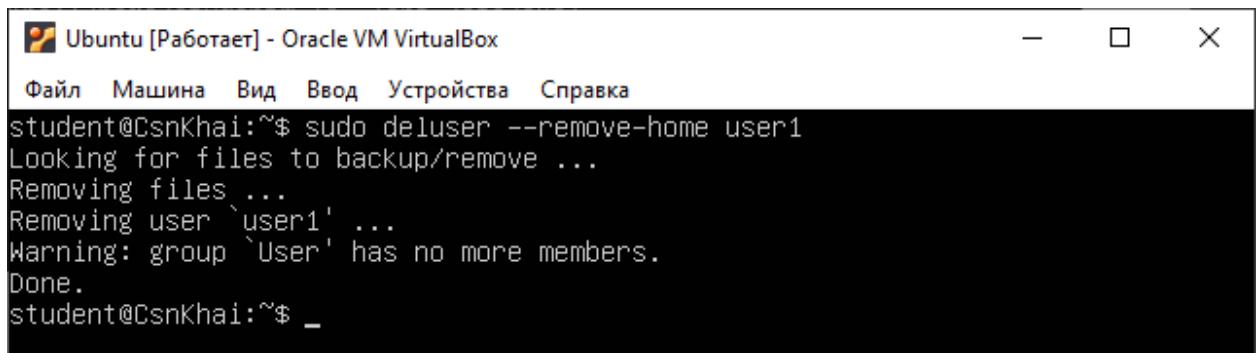
7) What is skell_dir? What is its structure?

skell_dir is the directory containing the files to copy to the newly created own directory.



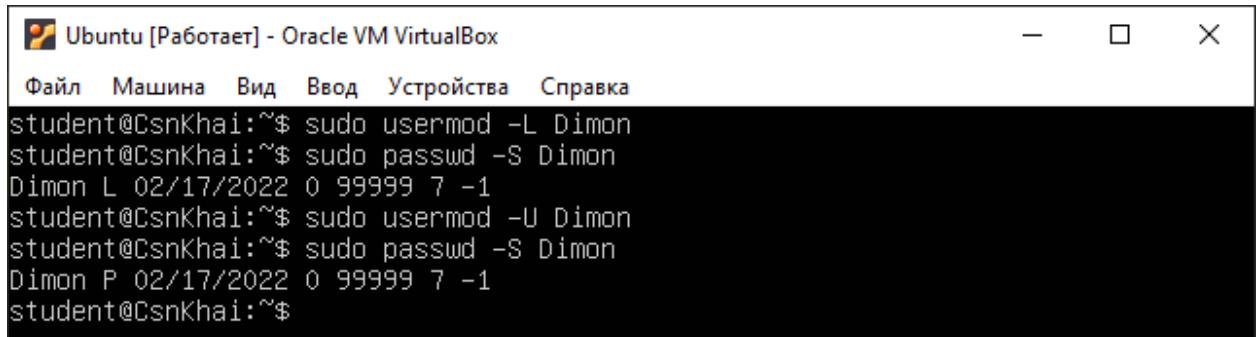
```
Ubuntu [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
user1@CsnKhai:/home/student$ ls -lart /etc/skel
total 20
-rw-r--r-- 1 root root 675 Apr  9 2014 .profile
-rw-r--r-- 1 root root 3637 Apr  9 2014 .bashrc
-rw-r--r-- 1 root root 220 Apr  9 2014 .bash_logout
drwxr-xr-x 2 root root 4096 Feb 15 19:40 .
drwxr-xr-x 84 root root 4096 Feb 17 22:37 ..
user1@CsnKhai:/home/student$
```

8) How to remove a user from the system (including his mailbox)?



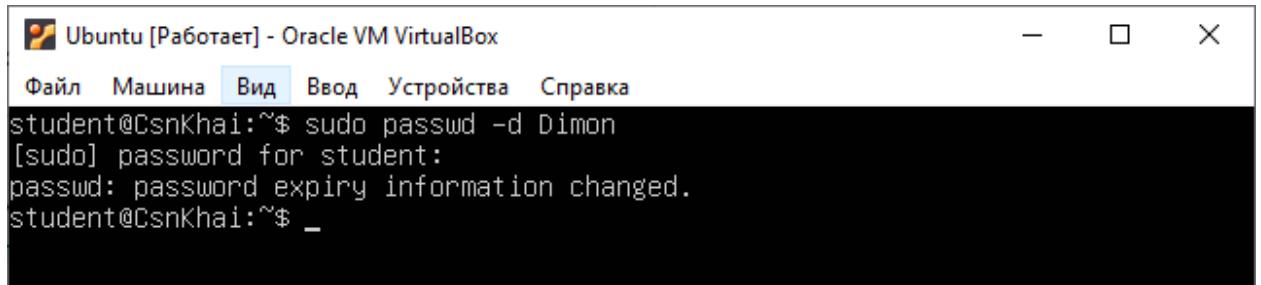
```
Ubuntu [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
student@CsnKhai:~$ sudo deluser --remove-home user1
Looking for files to backup/remove ...
Removing files ...
Removing user `user1' ...
Warning: group `User' has no more members.
Done.
student@CsnKhai:~$ _
```

9) What commands and keys should be used to lock and unlock a user account?



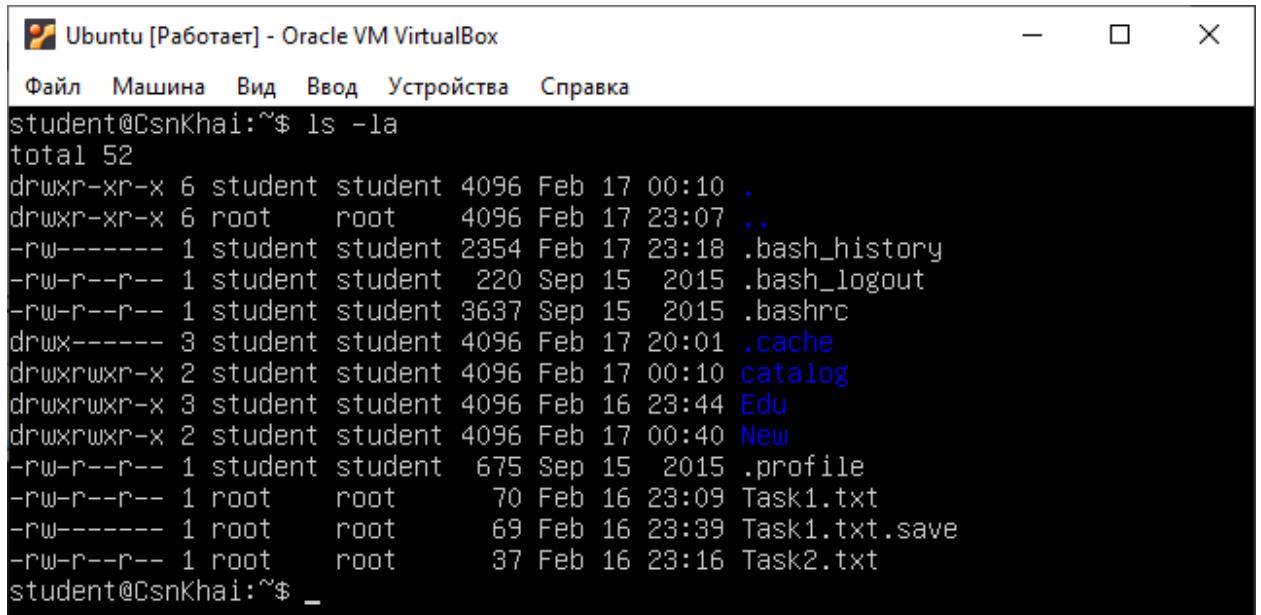
```
Ubuntu [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
student@CsnKhai:~$ sudo usermod -L Dimon
student@CsnKhai:~$ sudo passwd -S Dimon
Dimon L 02/17/2022 0 99999 7 -1
student@CsnKhai:~$ sudo usermod -U Dimon
student@CsnKhai:~$ sudo passwd -S Dimon
Dimon P 02/17/2022 0 99999 7 -1
student@CsnKhai:~$
```

10) How to remove a user's password and provide him with a password-free login for subsequent password change?



```
Ubuntu [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
student@CsnKhai:~$ sudo passwd -d Dimon
[sudo] password for student:
passwd: password expiry information changed.
student@CsnKhai:~$ _
```

11) Display the extended format of information about the directory, tell about the information columns displayed on the terminal.



```
Ubuntu [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
student@CsnKhai:~$ ls -la
total 52
drwxr-xr-x 6 student student 4096 Feb 17 00:10 .
drwxr-xr-x 6 root root 4096 Feb 17 23:07 ..
-rw----- 1 student student 2354 Feb 17 23:18 .bash_history
-rw-r--r-- 1 student student 220 Sep 15 2015 .bash_logout
-rw-r--r-- 1 student student 3637 Sep 15 2015 .bashrc
drwx----- 3 student student 4096 Feb 17 20:01 .cache
drwxrwxr-x 2 student student 4096 Feb 17 00:10 catalog
drwxrwxr-x 3 student student 4096 Feb 16 23:44 Edu
drwxrwxr-x 2 student student 4096 Feb 17 00:40 New
-rw-r--r-- 1 student student 675 Sep 15 2015 .profile
-rw-r--r-- 1 root root 70 Feb 16 23:09 Task1.txt
-rw----- 1 root root 69 Feb 16 23:39 Task1.txt.save
-rw-r--r-- 1 root root 37 Feb 16 23:16 Task2.txt
student@CsnKhai:~$ _
```

12) What access rights exist and for whom (i. e., describe the main roles)? Briefly describe the acronym for access rights.

Dashes are responsible for file permissions in linux. The first is the file type, followed by groups of rights, first for the owner, for the group, and for everyone else. Only nine dashes for rights and one for type.

--- - no rights at all;

--x - only file execution is allowed, as a program, but not changing or reading;

-w- - only writing and modifying the file is allowed;

-wx - allow modification and execution, but in the case of a directory, you cannot see its contents;

r-- - read-only rights;

r-x - read and execute only, no write access;

rw- - read and write permissions, but no execution;

rxw - all rights;

--s - SUID or SGID bit is set, the first is displayed in the field for the owner, the second for the group;

--t - sticky-bit is set, which means users cannot delete this file.

13) What is the sequence of defining the relationship between the file and the user?

When the relationship between the file and the user who started the process, the role is determined as follows If the UID of the file is the same as the UID of the process, the user is the owner of the file If the GID of the file matches the GID of any group the user belongs to, he is a member of the group to which the file belongs If neither the UID nor the GID of a file overlaps with the UID of the process and the list of groups that the user running it belongs to, that user is an outsider.

14) What commands are used to change the owner of a file (directory), as well as the mode of access to the file? Give examples, demonstrate on the terminal.

```

student@CsnKhai:~$ chown Dimon Task1.txt
chown: changing ownership of 'Task1.txt': Operation not permitted
student@CsnKhai:~$ ls -l Task1.txt
-rw-r--r-- 1 root root 70 Feb 16 23:09 Task1.txt
student@CsnKhai:~$ sudo chown Dimon Task1.txt
[sudo] password for student:
student@CsnKhai:~$ ls -l Task1.txt
-rw-r--r-- 1 Dimon root 70 Feb 16 23:09 Task1.txt
student@CsnKhai:~$ chmod o+wx Task1.txt
chmod: changing permissions of 'Task1.txt': Operation not permitted
student@CsnKhai:~$ sudo chmod o+wx Task1.txt
student@CsnKhai:~$ ls -l Task1.txt
-rw-r--rwx 1 Dimon root 70 Feb 16 23:09 Task1.txt
student@CsnKhai:~$ sudo chmod u-x Task1.txt
student@CsnKhai:~$ ls -l Task1.txt
-rw-r--rwx 1 Dimon root 70 Feb 16 23:09 Task1.txt
student@CsnKhai:~$ sudo chmod 7 Task1.txt
student@CsnKhai:~$ ls -l Task1.txt
-----rwx 1 Dimon root 70 Feb 16 23:09 Task1.txt

```

15) What is an example of octal representation of access rights? Describe the umask command.

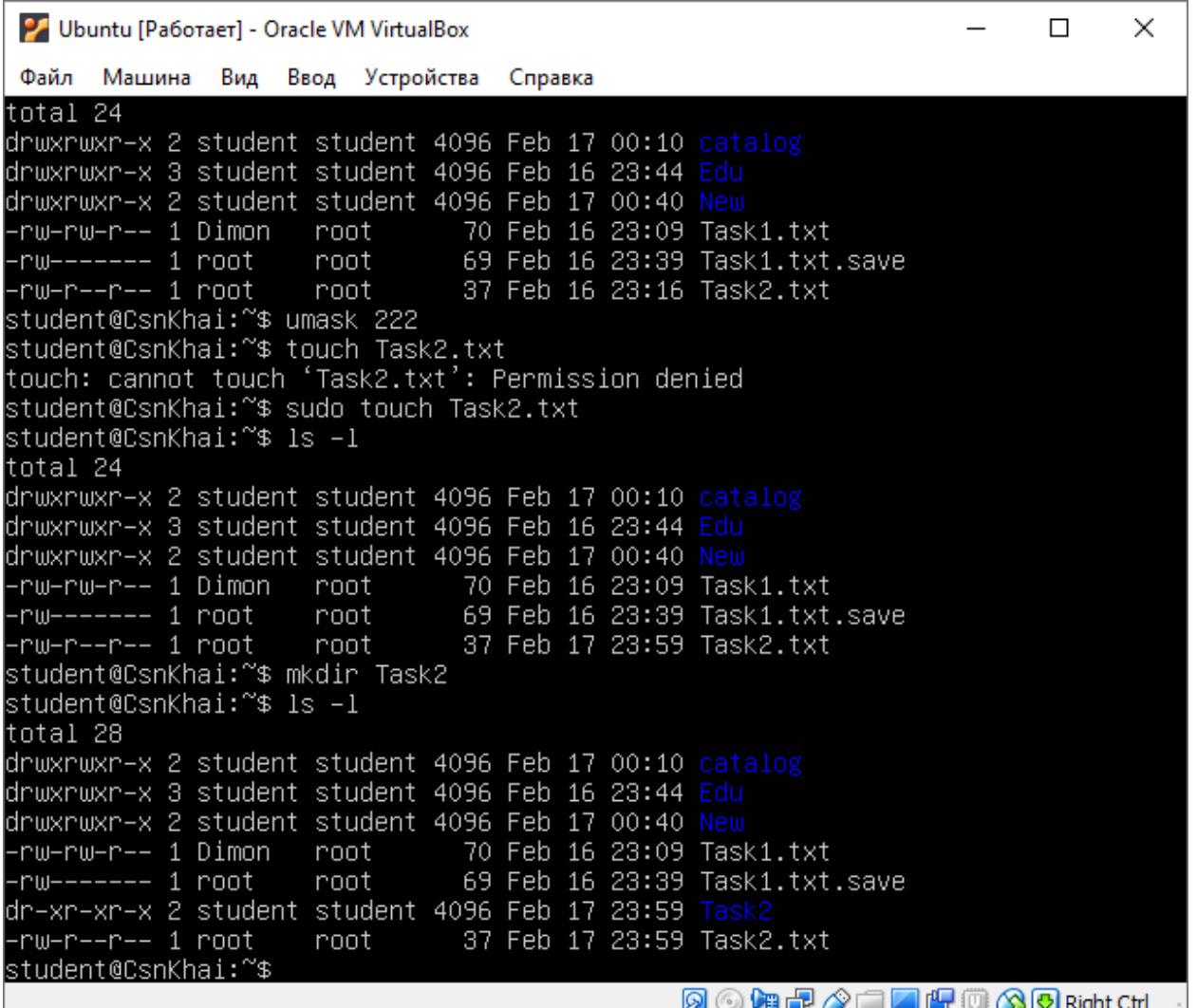
```

student@CsnKhai:~$ sudo chmod 664 Task1.txt
student@CsnKhai:~$ ls -l Task1.txt
-rw-rw-r-- 1 Dimon root 70 Feb 16 23:09 Task1.txt
student@CsnKhai:~$ _

```

Octal representation	Access rights
0	---
1	--x
2	-w-
3	-wx
4	r--
5	r-x
6	rw-
7	rwx

The umask command sets the permissions mask for new files and directories. When creating any file, the operating system requests a permissions mask and calculates the mask based on it. The default mask is 0002.

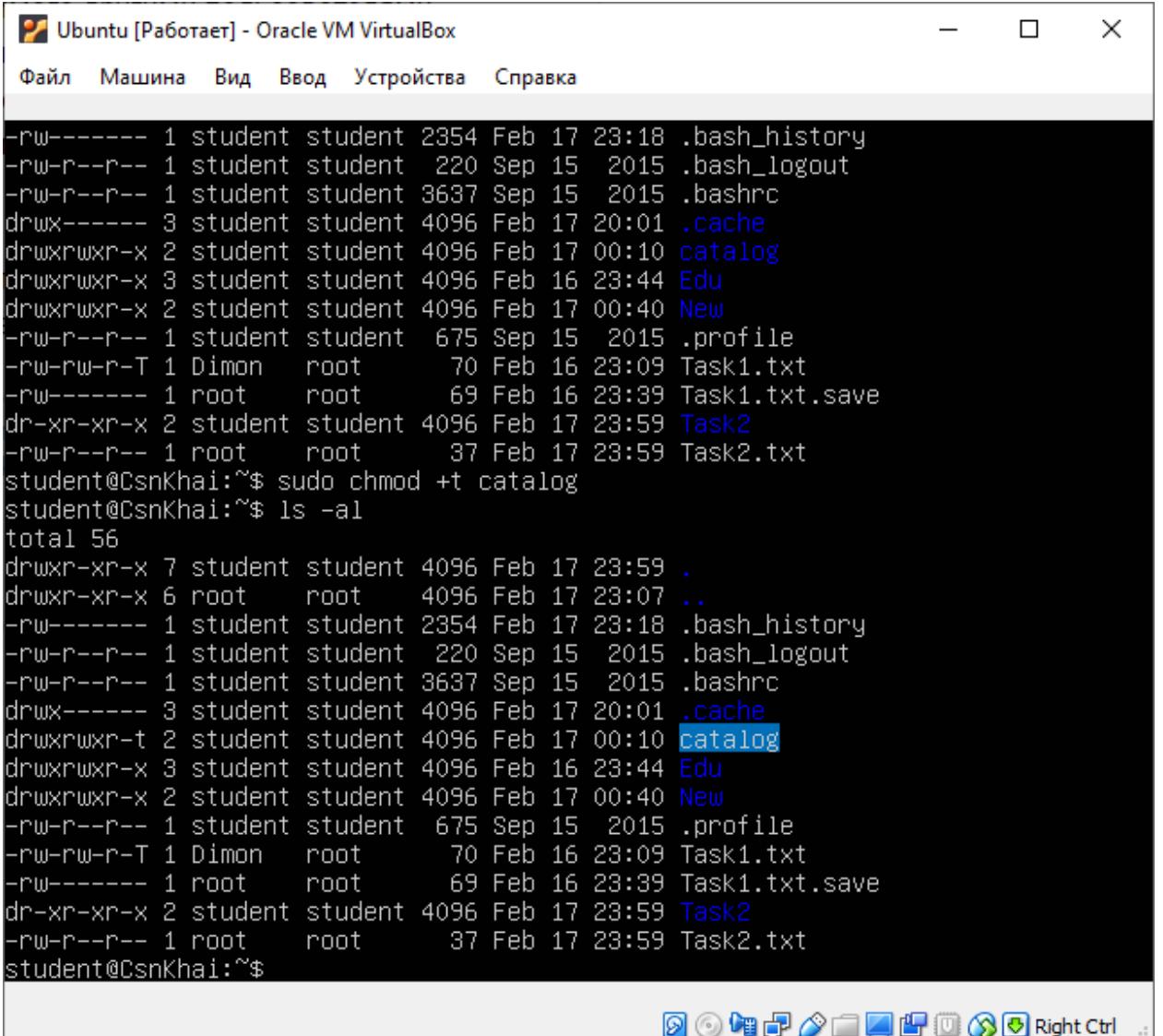


```
Ubuntu [Работает] - Oracle VM VirtualBox
Файл Машине Вид Ввод Устройства Справка
total 24
drwxrwxr-x 2 student student 4096 Feb 17 00:10 catalog
drwxrwxr-x 3 student student 4096 Feb 16 23:44 Edu
drwxrwxr-x 2 student student 4096 Feb 17 00:40 New
-rw-rw-r-- 1 Dimon root 70 Feb 16 23:09 Task1.txt
-rw----- 1 root root 69 Feb 16 23:39 Task1.txt.save
-rw-r--r-- 1 root root 37 Feb 16 23:16 Task2.txt
student@CsnKhai:~$ umask 222
student@CsnKhai:~$ touch Task2.txt
touch: cannot touch 'Task2.txt': Permission denied
student@CsnKhai:~$ sudo touch Task2.txt
student@CsnKhai:~$ ls -l
total 24
drwxrwxr-x 2 student student 4096 Feb 17 00:10 catalog
drwxrwxr-x 3 student student 4096 Feb 16 23:44 Edu
drwxrwxr-x 2 student student 4096 Feb 17 00:40 New
-rw-rw-r-- 1 Dimon root 70 Feb 16 23:09 Task1.txt
-rw----- 1 root root 69 Feb 16 23:39 Task1.txt.save
-rw-r--r-- 1 root root 37 Feb 17 23:59 Task2.txt
student@CsnKhai:~$ mkdir Task2
student@CsnKhai:~$ ls -l
total 28
drwxrwxr-x 2 student student 4096 Feb 17 00:10 catalog
drwxrwxr-x 3 student student 4096 Feb 16 23:44 Edu
drwxrwxr-x 2 student student 4096 Feb 17 00:40 New
-rw-rw-r-- 1 Dimon root 70 Feb 16 23:09 Task1.txt
-rw----- 1 root root 69 Feb 16 23:39 Task1.txt.save
dr-xr-xr-x 2 student student 4096 Feb 17 23:59 Task2
-rw-r--r-- 1 root root 37 Feb 17 23:59 Task2.txt
student@CsnKhai:~$
```

- 16) Give definitions of sticky bits and mechanism of identifier substitution. Give an example of files and directories with these attributes.

Sticky Bit is mainly used on folders in order to avoid deletion of a folder and its content by other users though they having write permissions on the folder contents If Sticky bit is enabled on a folder, the folder contents are deleted by only owner who created them and the root user No one else can delete other users data in

this folder(Where sticky bit is set) This is a security measure to avoid deletion of critical folders and their content(sub folders and files), though other users have full permissions.



```
-rw----- 1 student student 2354 Feb 17 23:18 .bash_history
-rw-r--r-- 1 student student 220 Sep 15 2015 .bash_logout
-rw-r--r-- 1 student student 3637 Sep 15 2015 .bashrc
drwx----- 3 student student 4096 Feb 17 20:01 .cache
drwxrwxr-x 2 student student 4096 Feb 17 00:10 catalog
drwxrwxr-x 3 student student 4096 Feb 16 23:44 Edu
drwxrwxr-x 2 student student 4096 Feb 17 00:40 New
-rw-r--r-- 1 student student 675 Sep 15 2015 .profile
-rw-rw-r-T 1 Dimon root 70 Feb 16 23:09 Task1.txt
-rw----- 1 root root 69 Feb 16 23:39 Task1.txt.save
dr-xr-xr-x 2 student student 4096 Feb 17 23:59 Task2
-rw-r--r-- 1 root root 37 Feb 17 23:59 Task2.txt
student@CsnKhai:~$ sudo chmod +t catalog
student@CsnKhai:~$ ls -al
total 56
drwxr-xr-x 7 student student 4096 Feb 17 23:59 .
drwxr-xr-x 6 root root 4096 Feb 17 23:07 ..
-rw----- 1 student student 2354 Feb 17 23:18 .bash_history
-rw-r--r-- 1 student student 220 Sep 15 2015 .bash_logout
-rw-r--r-- 1 student student 3637 Sep 15 2015 .bashrc
drwx----- 3 student student 4096 Feb 17 20:01 .cache
drwxrwxr-t 2 student student 4096 Feb 17 00:10 catalog
drwxrwxr-x 3 student student 4096 Feb 16 23:44 Edu
drwxrwxr-x 2 student student 4096 Feb 17 00:40 New
-rw-r--r-- 1 student student 675 Sep 15 2015 .profile
-rw-rw-r-T 1 Dimon root 70 Feb 16 23:09 Task1.txt
-rw----- 1 root root 69 Feb 16 23:39 Task1.txt.save
dr-xr-xr-x 2 student student 4096 Feb 17 23:59 Task2
-rw-r--r-- 1 root root 37 Feb 17 23:59 Task2.txt
student@CsnKhai:~$
```

17) What file attributes should be present in the command script?

For this file to become a script, you must set the right to execute this file. Execution attribute (x)