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".

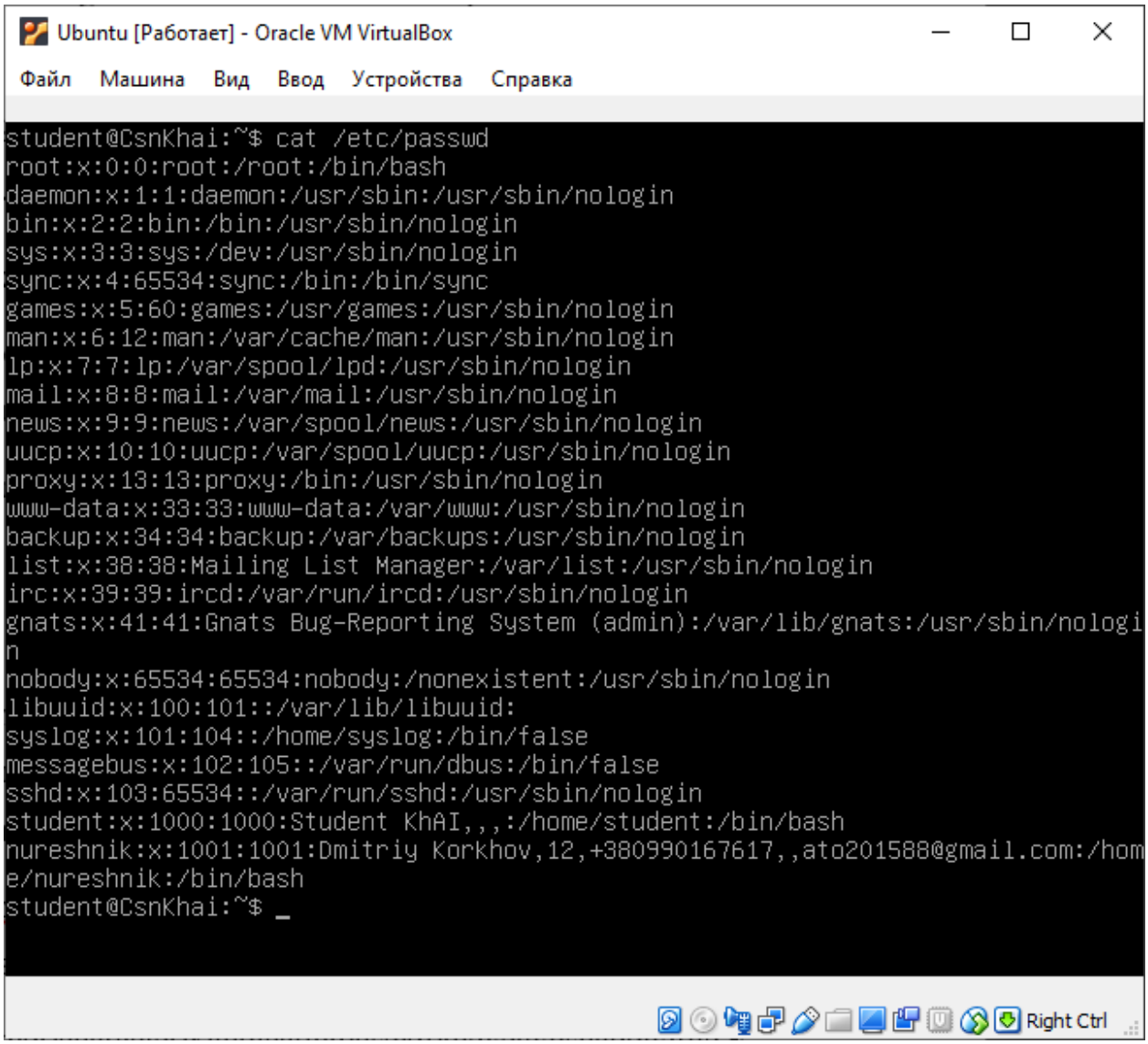
3 UID is a 32-bit integer that uniquely identifies a user on the system.

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



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

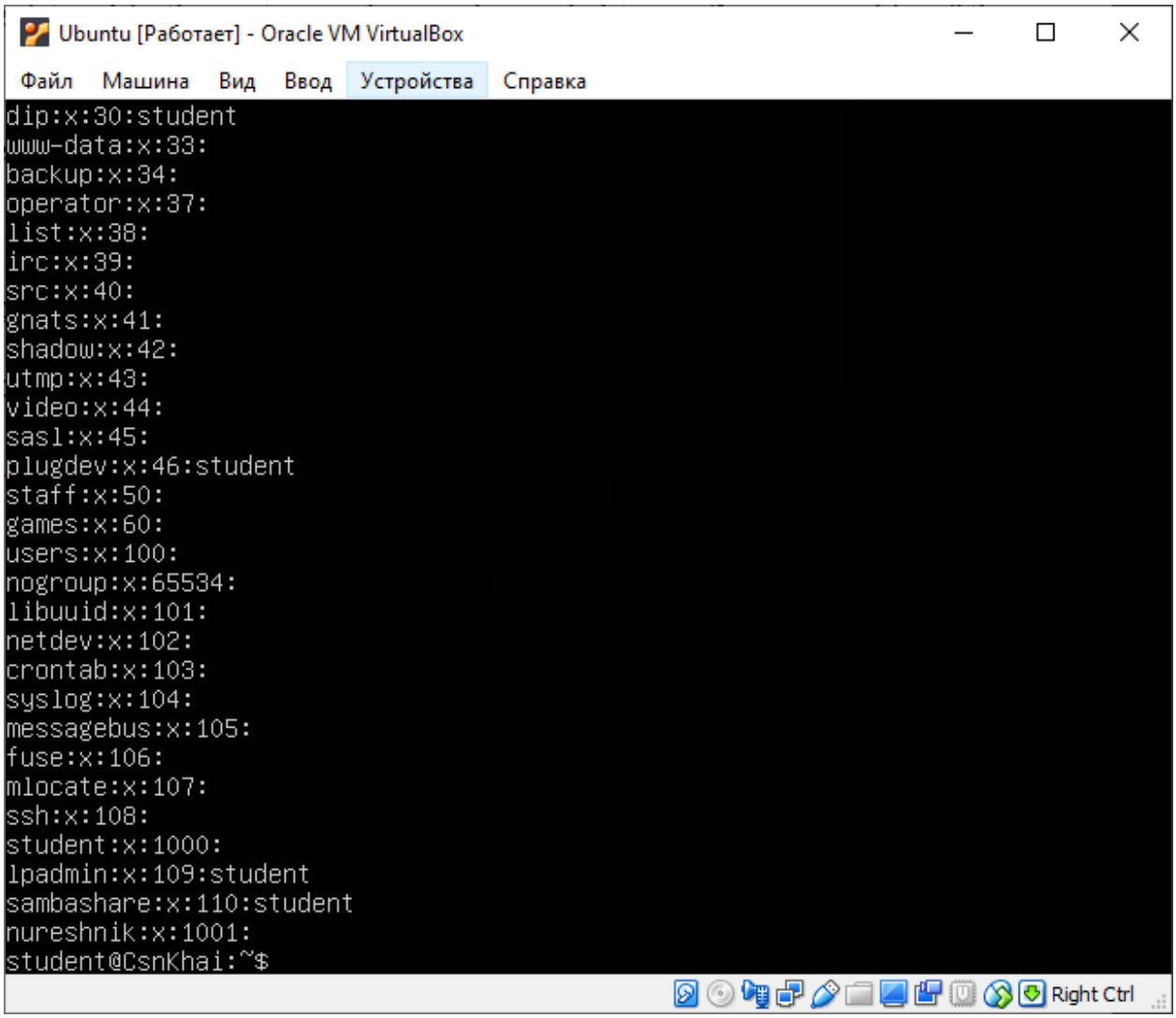
daemon – Used by system service processes

bin – Gives ownership of executables command

adm – Owns registration files

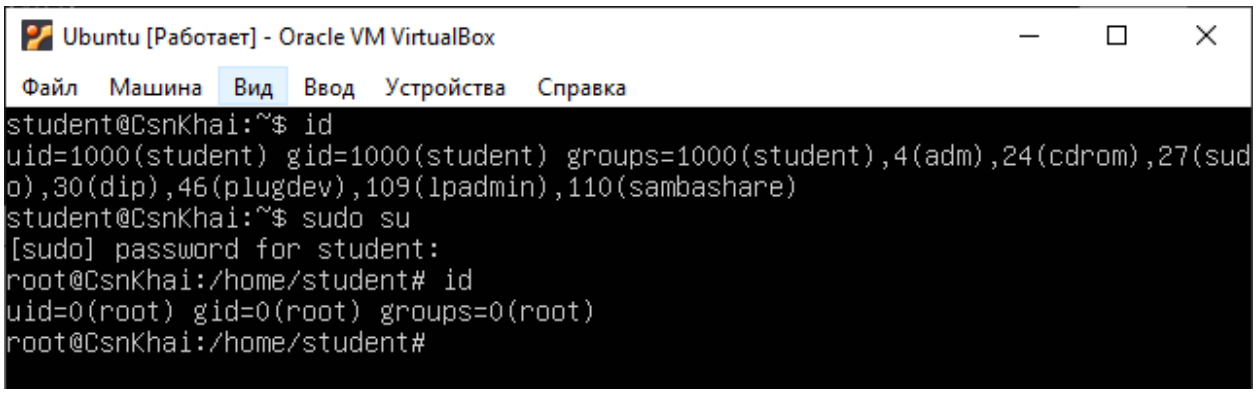
nobody – Used by many services

sshd – used by the secure shell server



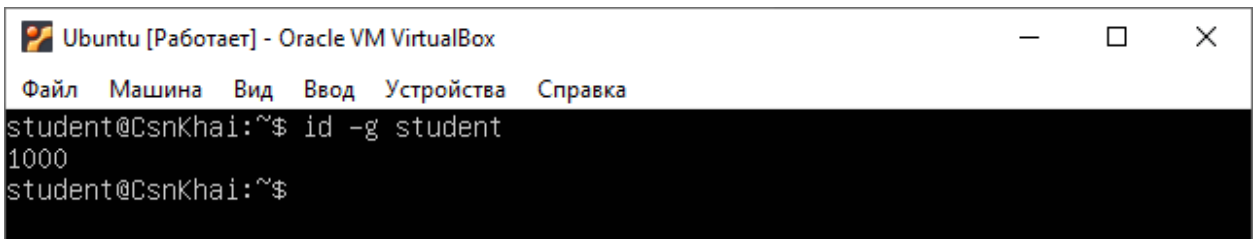
2) What are the uid ranges? What is UID? How to define it?

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).

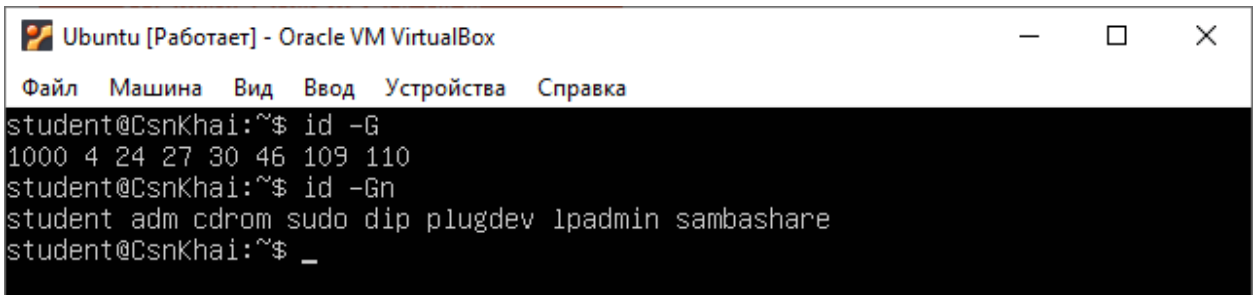


3) What is GID? How to define it?

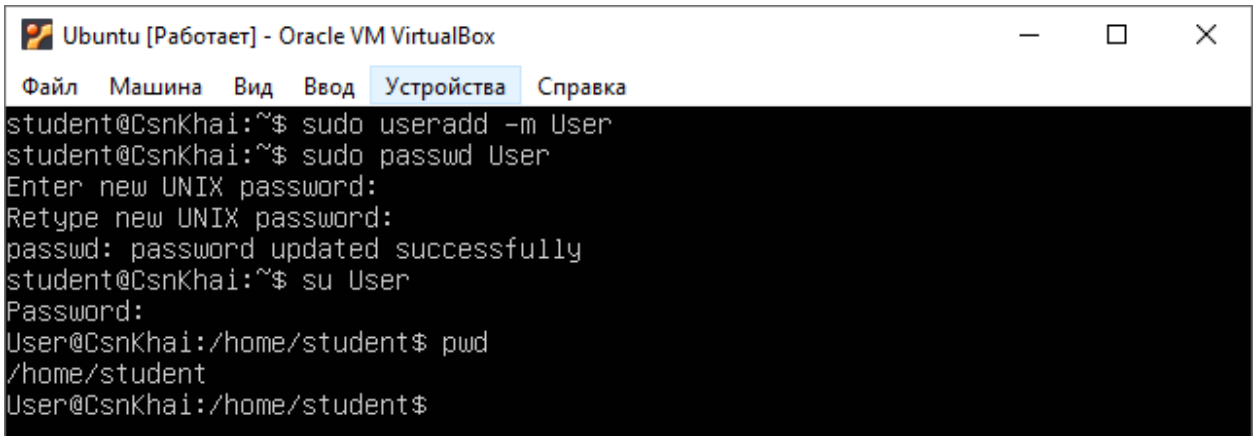
GID – unique identifier of the group within the system to which the user belongs.

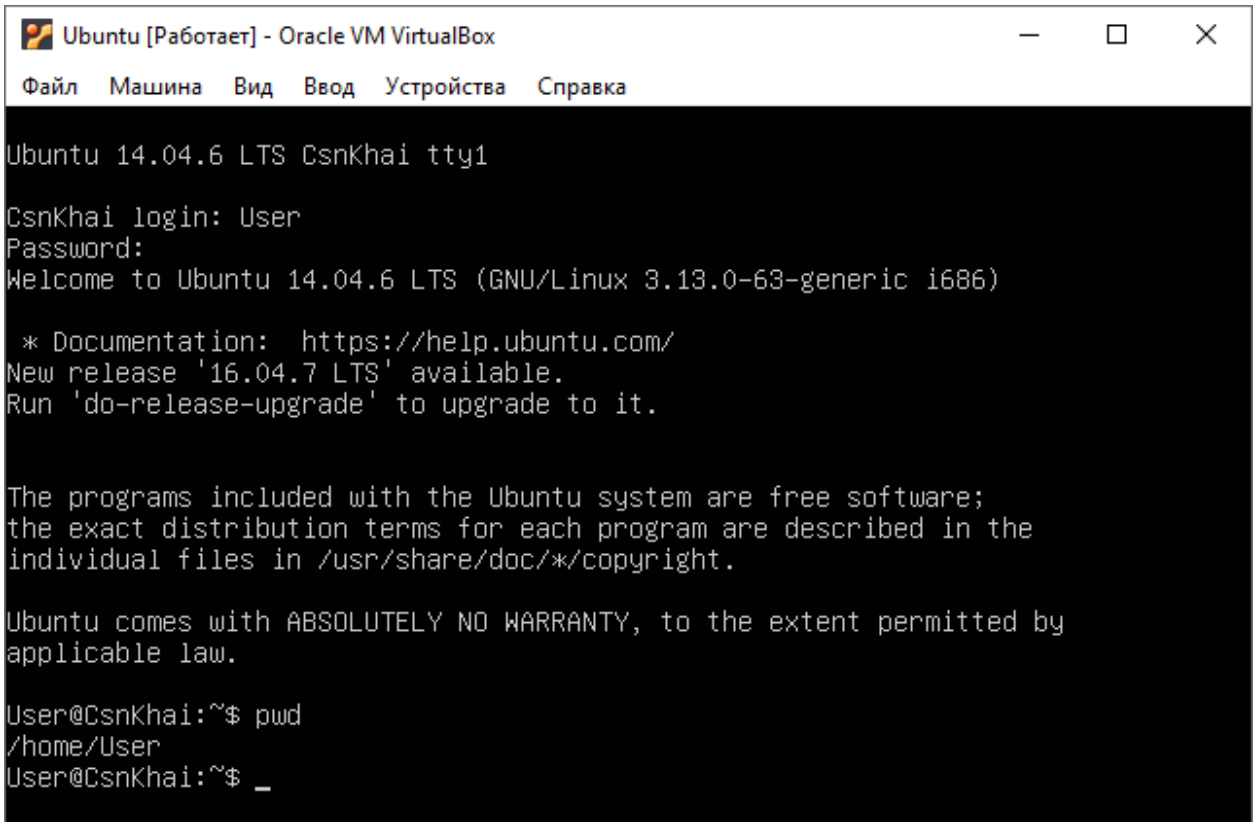


4) How to determine belonging of user to the specific group?

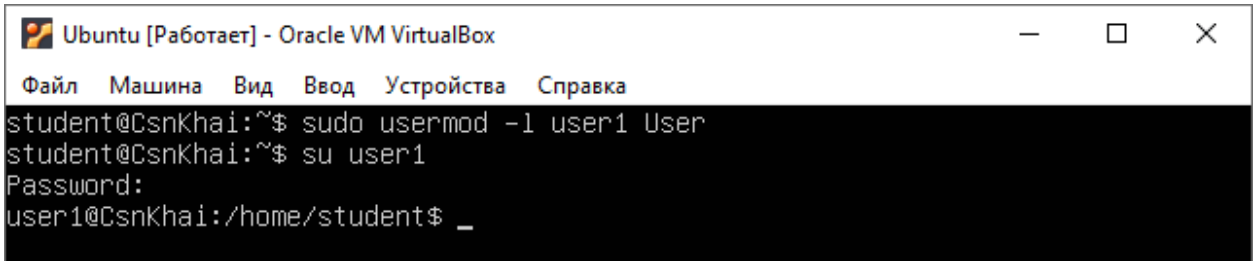


5) What are the commands for adding a user to the system? What are the basic parameters required to create a user?



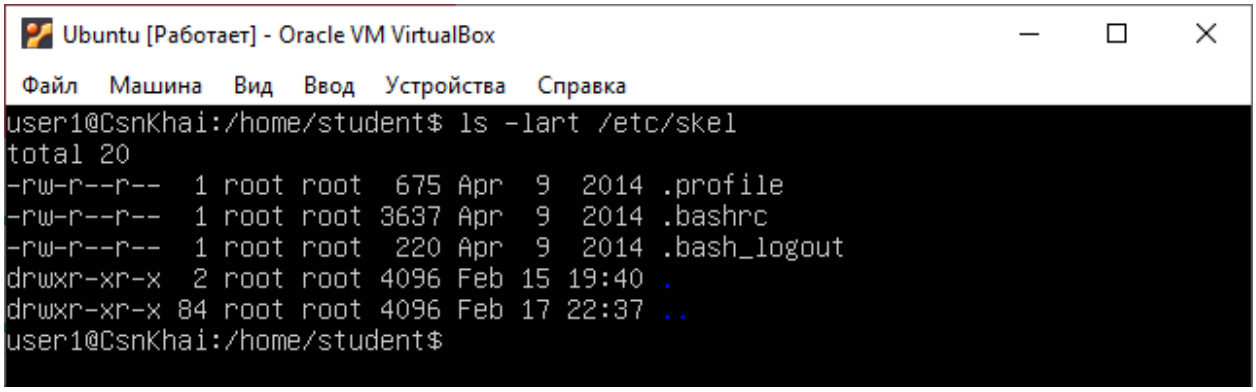


6) How do I change the name (account name) of an existing user?

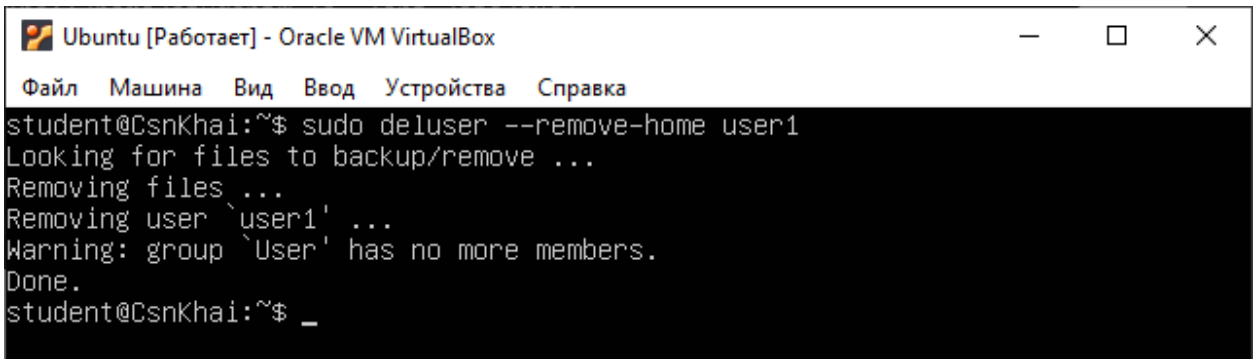


7) What is skell_dir? What is its structure?

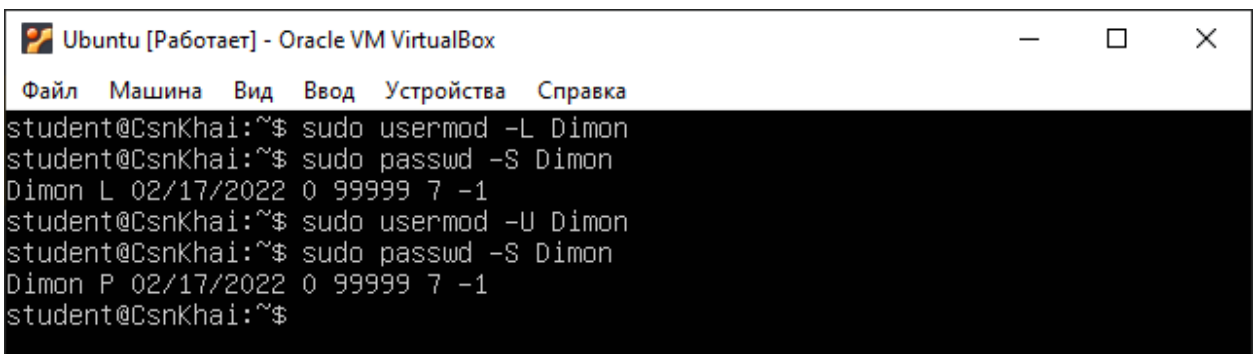
skell_dir is the directory containing the files to copy to the newly created own directory.



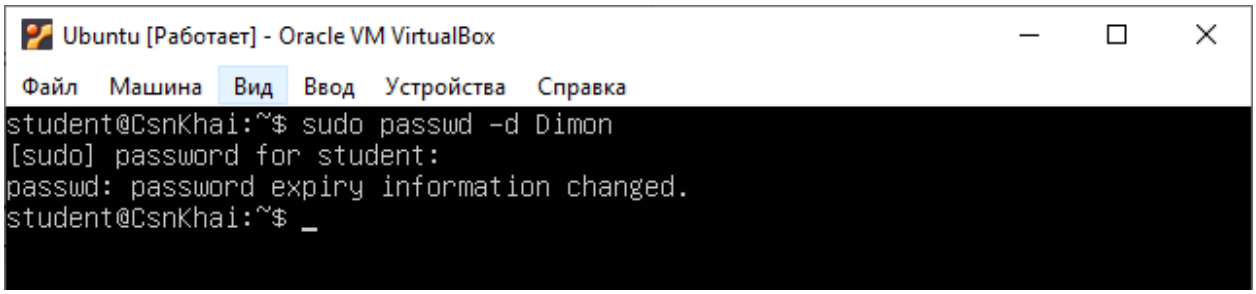
8) How to remove a user from the system (including his mailbox)?



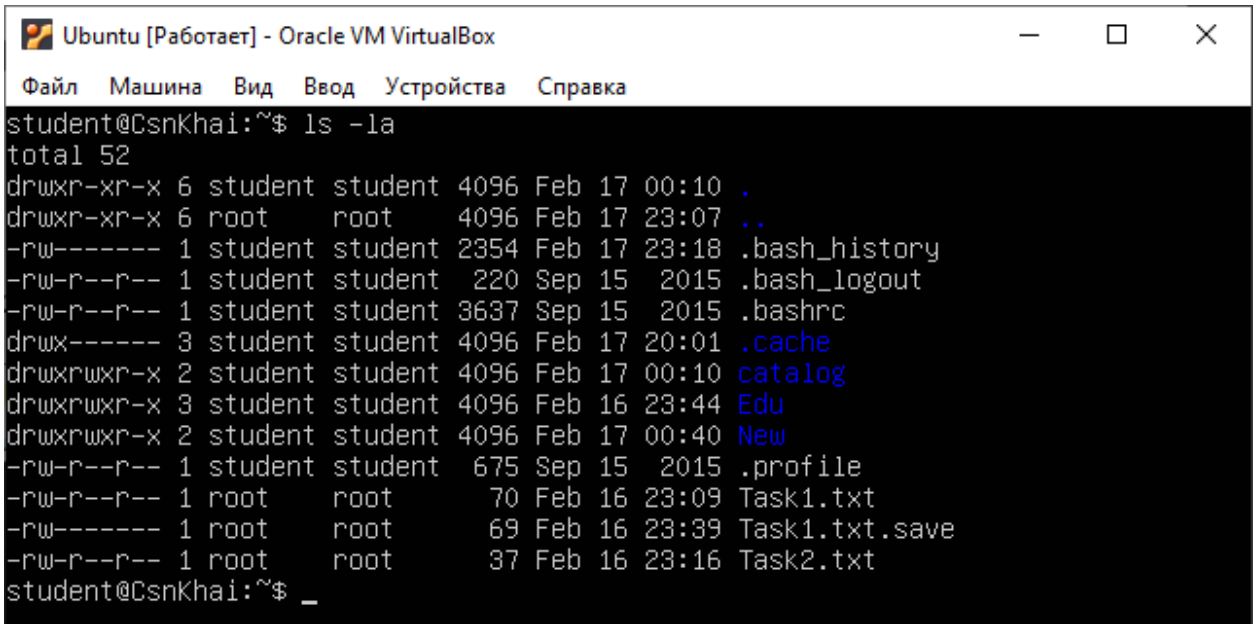
9) What commands and keys should be used to lock and unlock a user account?



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



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



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;

rwx - all rights;

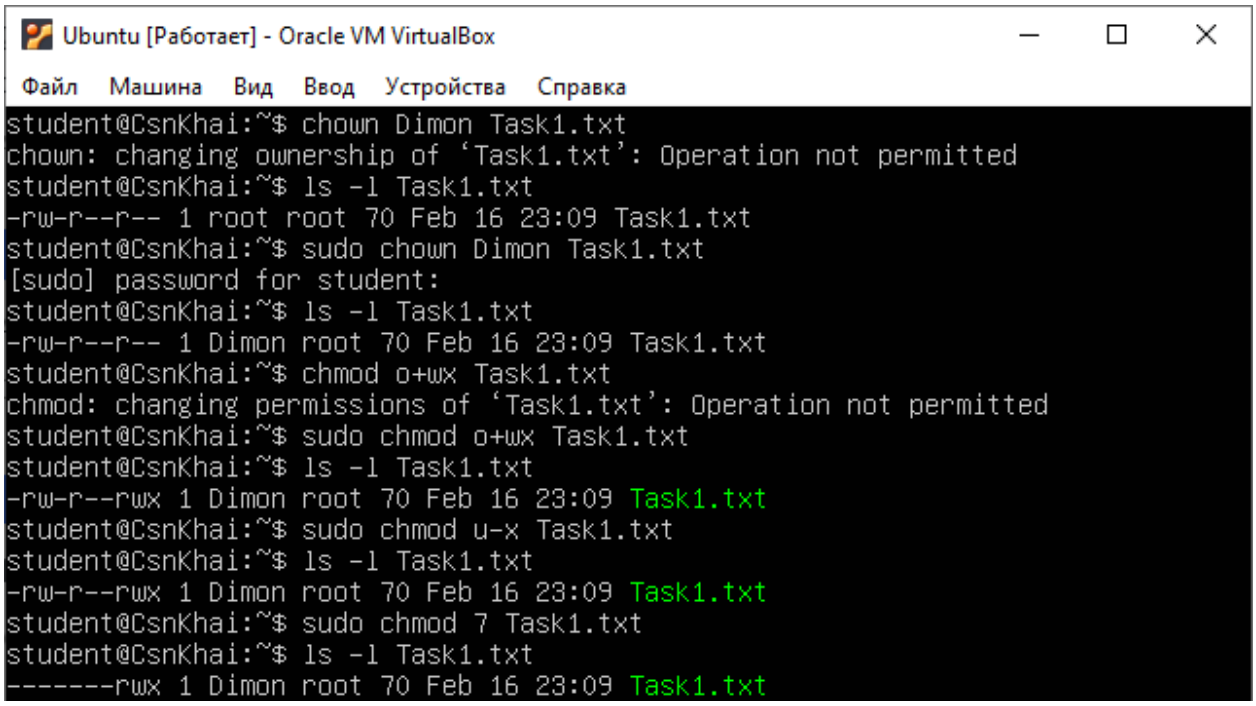
--s - SUID or SGID bit is set, the first is displayed in the field for the owner, the second for the group;

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

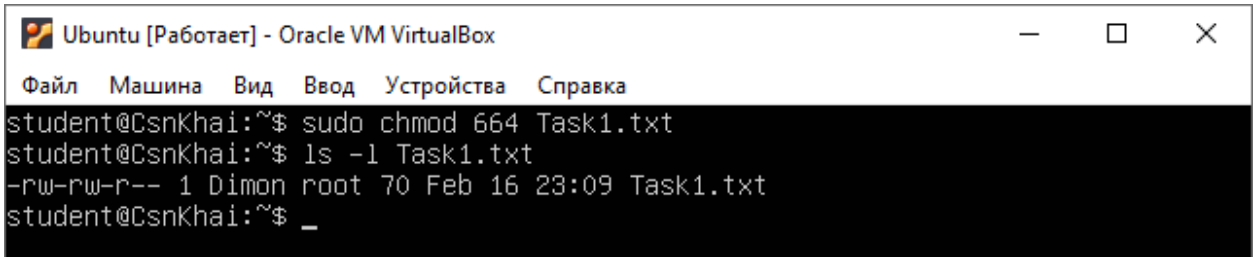
13) What is the sequence of defining the relationship between the file and the user?

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 no 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.

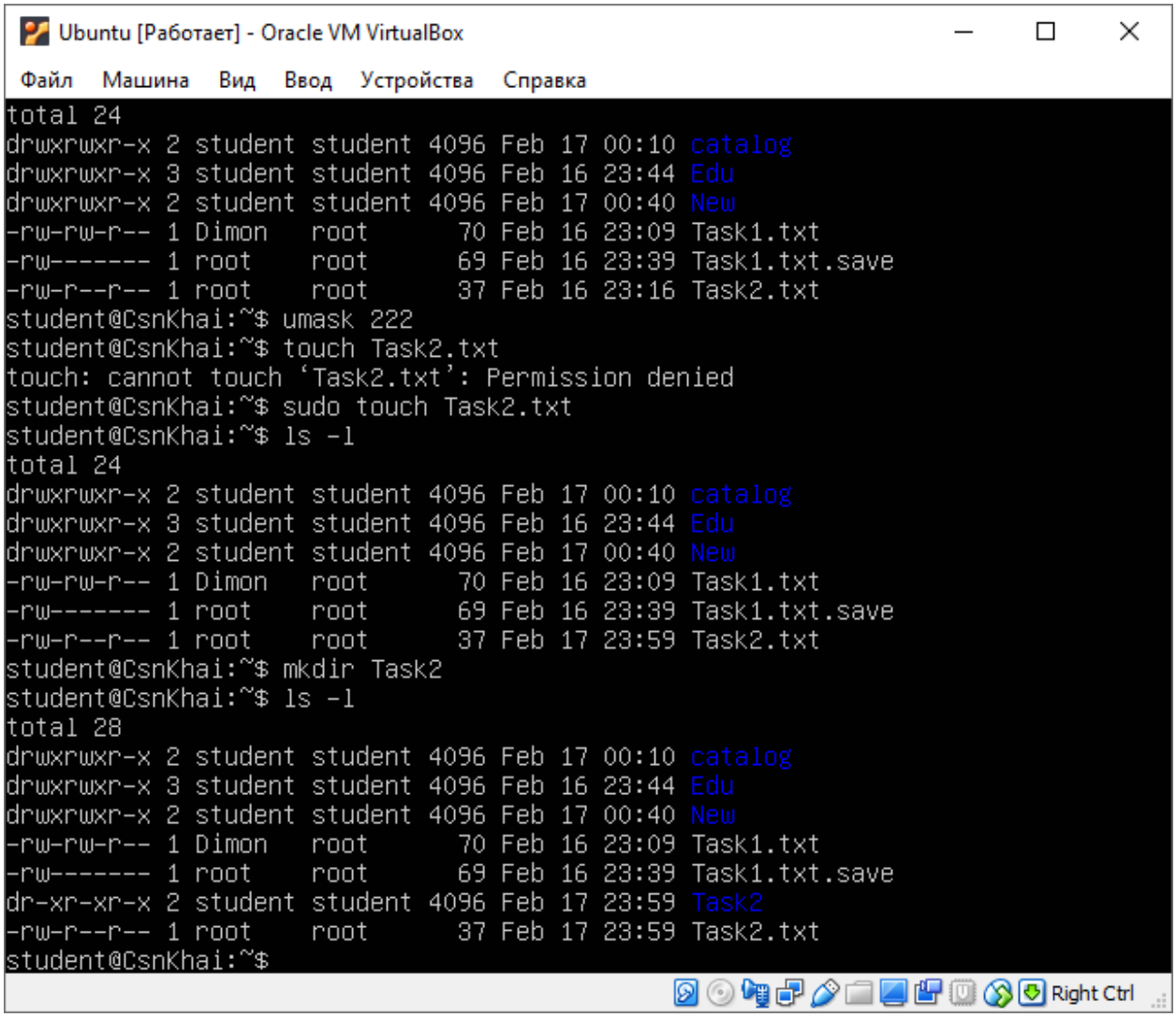


15) What is an example of octal representation of access rights? Describe the umask command.



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

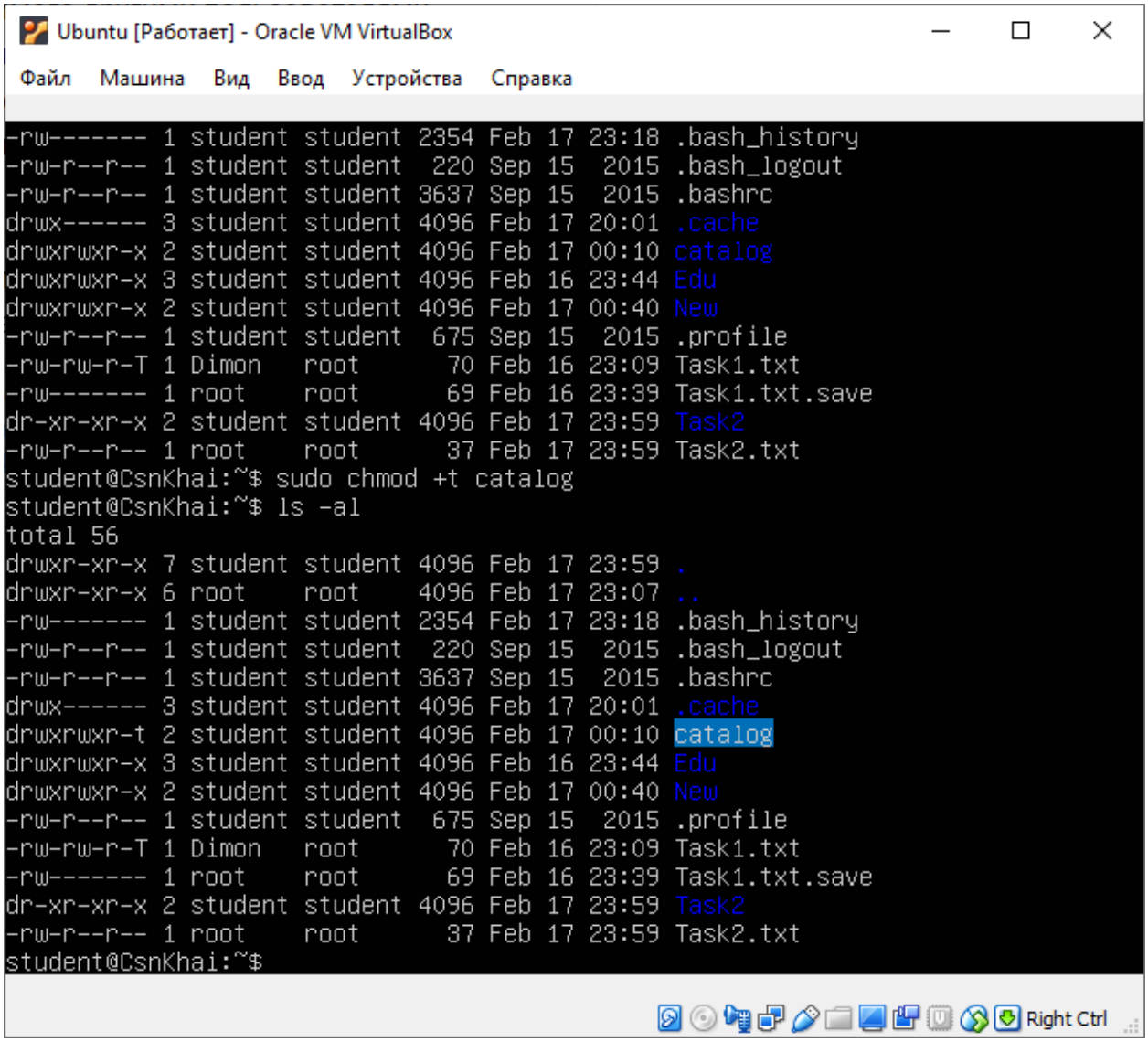
The umask command sets the permissions mask for new files and directories. When creating any file, the operating system requests a permissions mask and calculates the mask based on it. The default mask is 0002.



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 it's 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.



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)