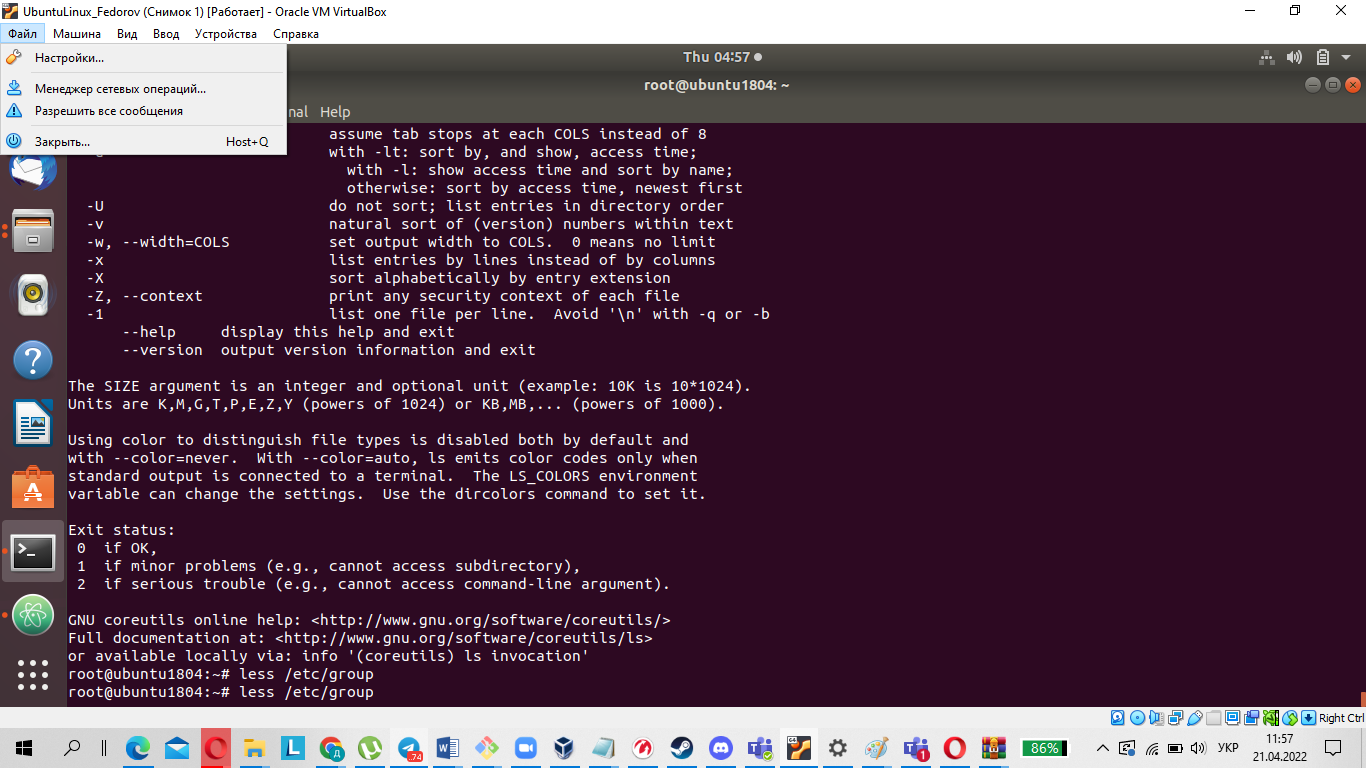
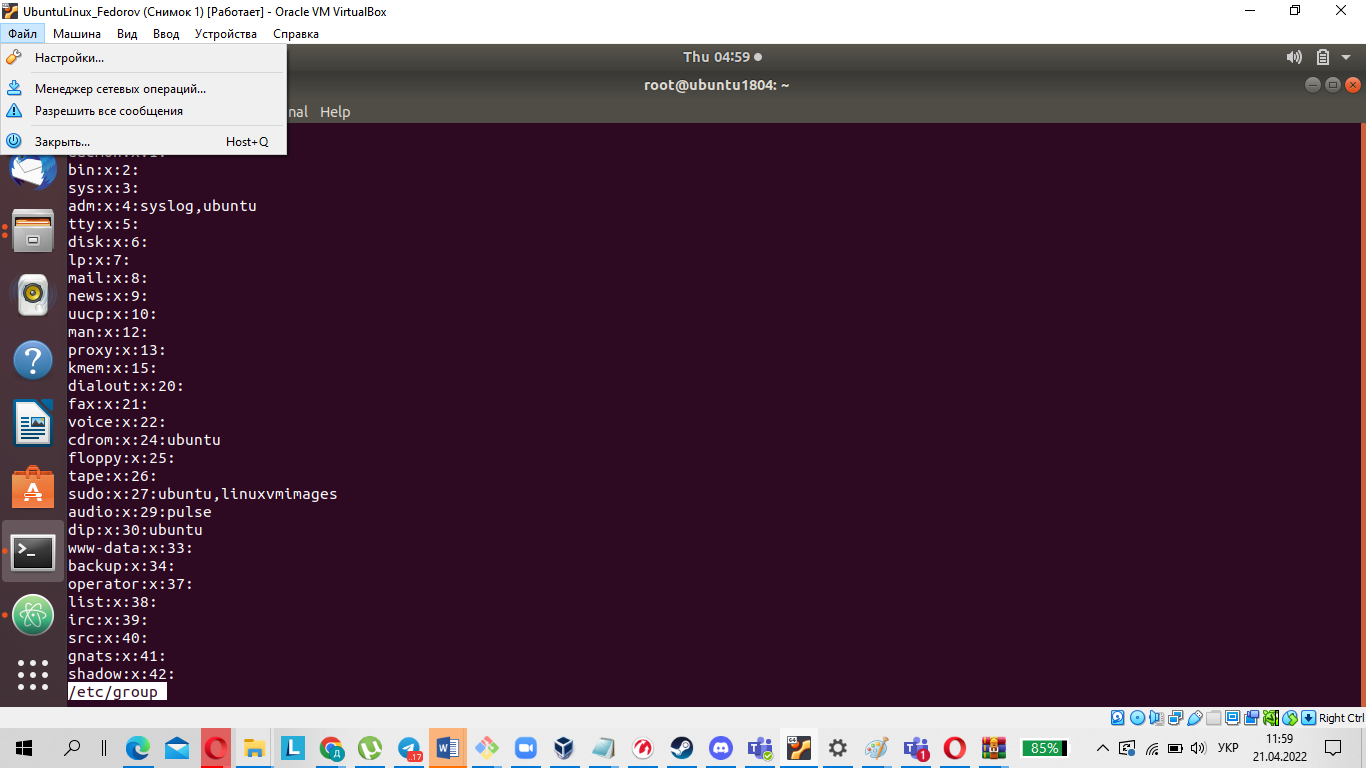
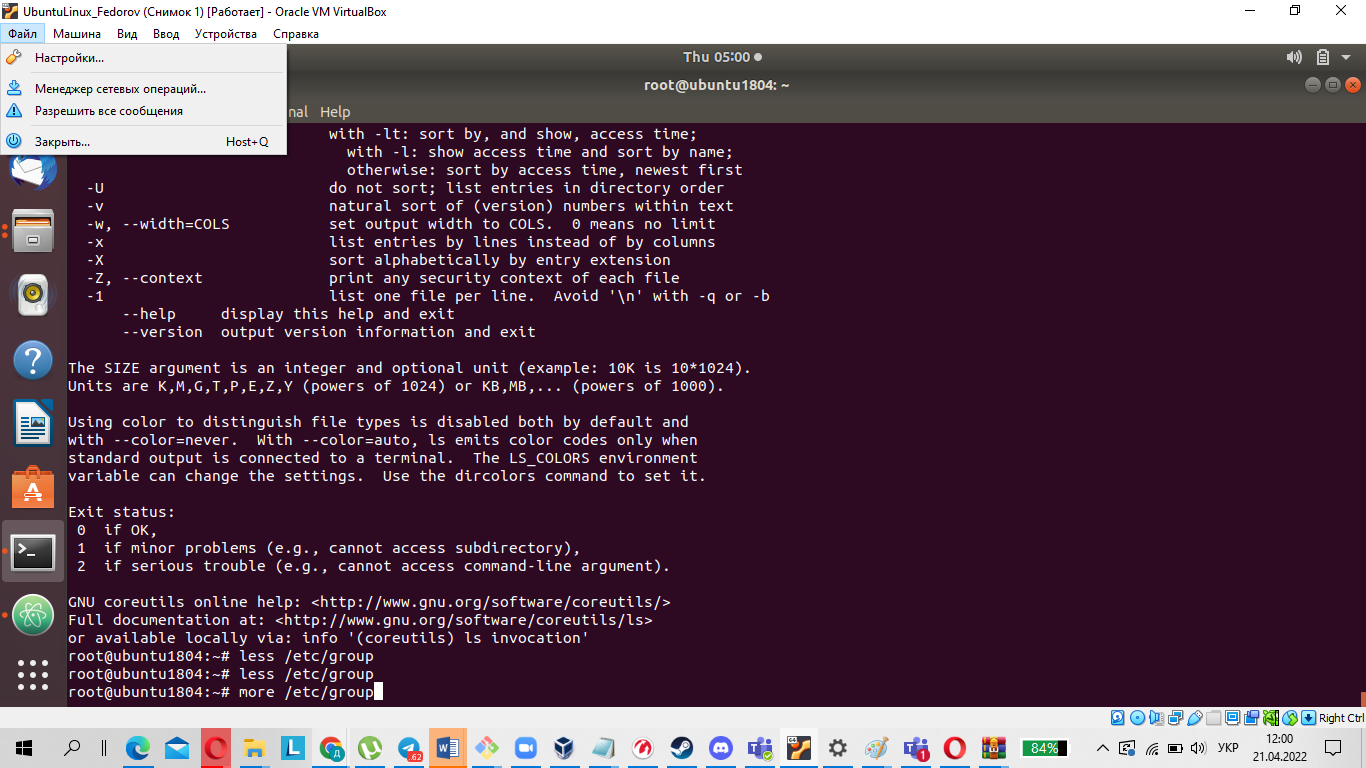
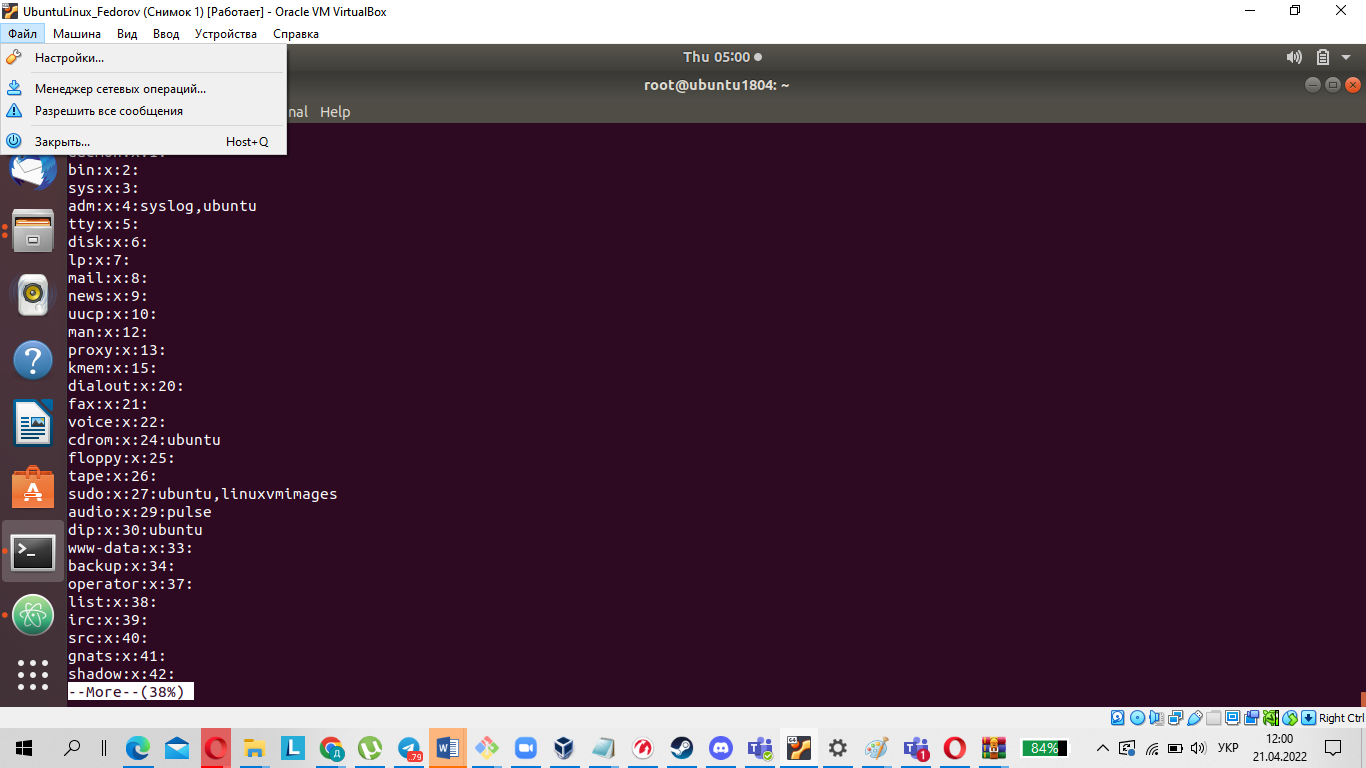
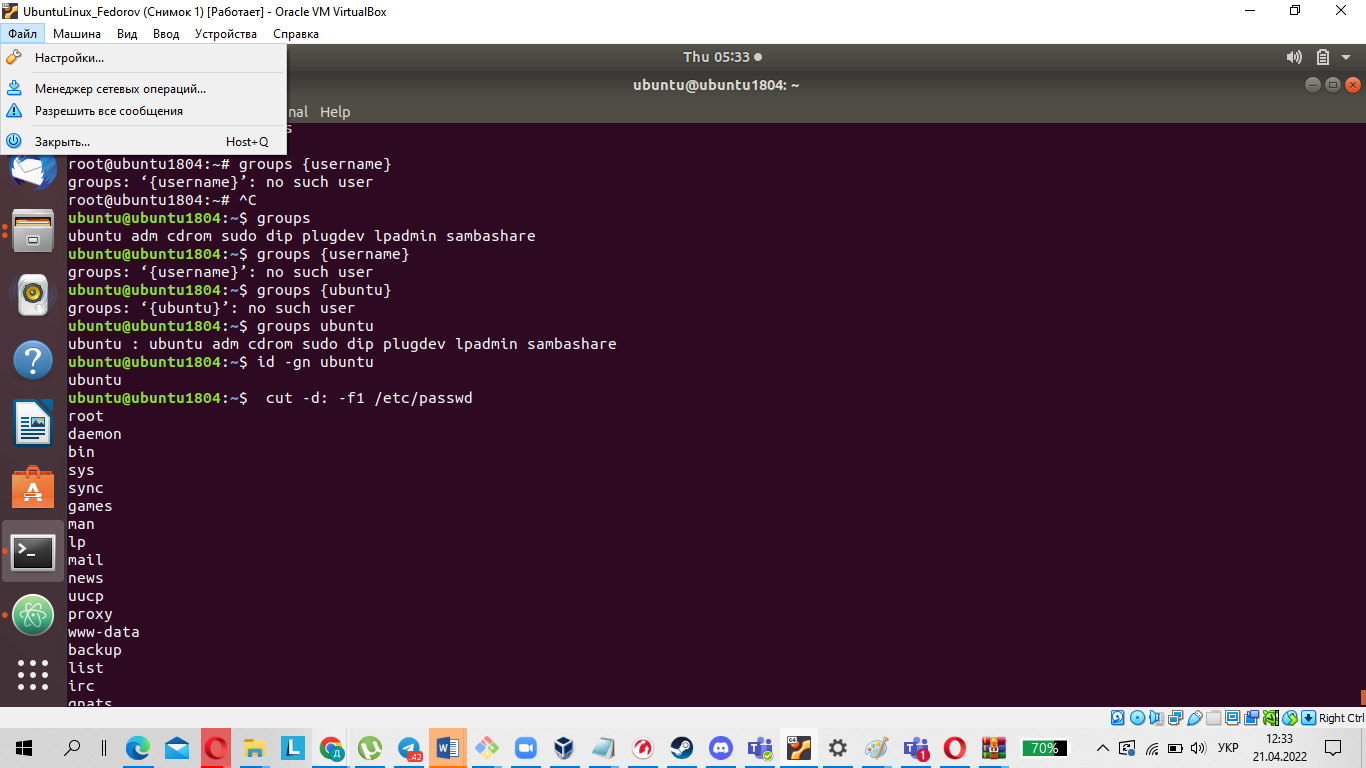
1.Analyze the structure of the /etc/passwd and /etc/group file, what fields are present in it, what users exist on the system? Specify several pseudo-users, how to define them?

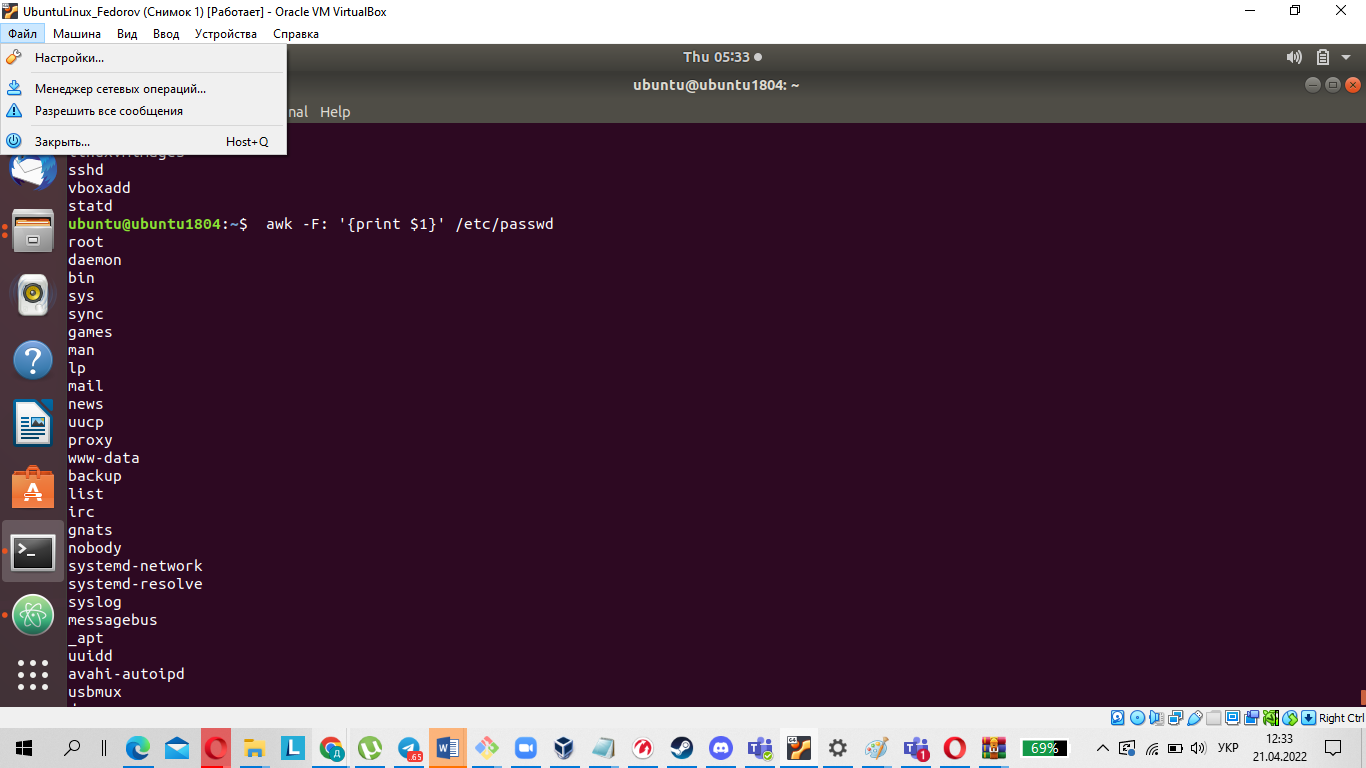


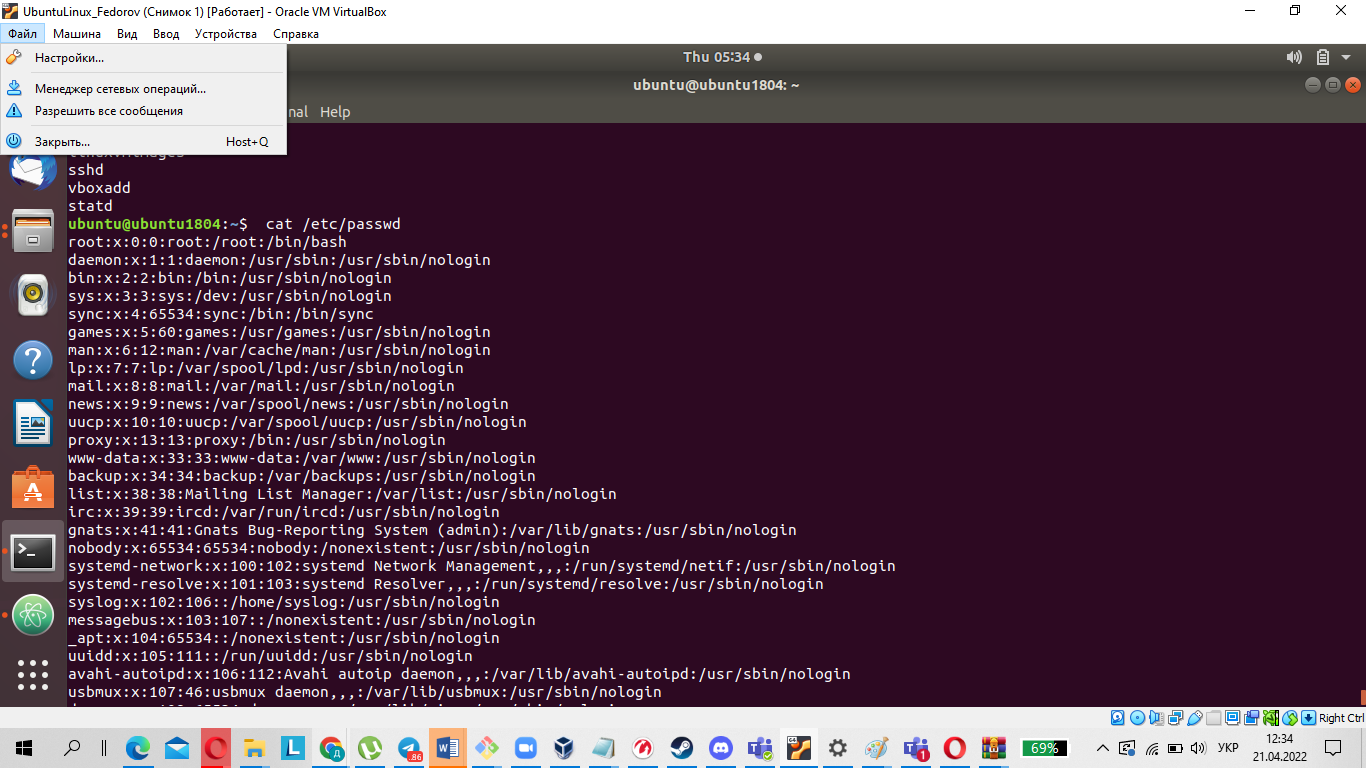














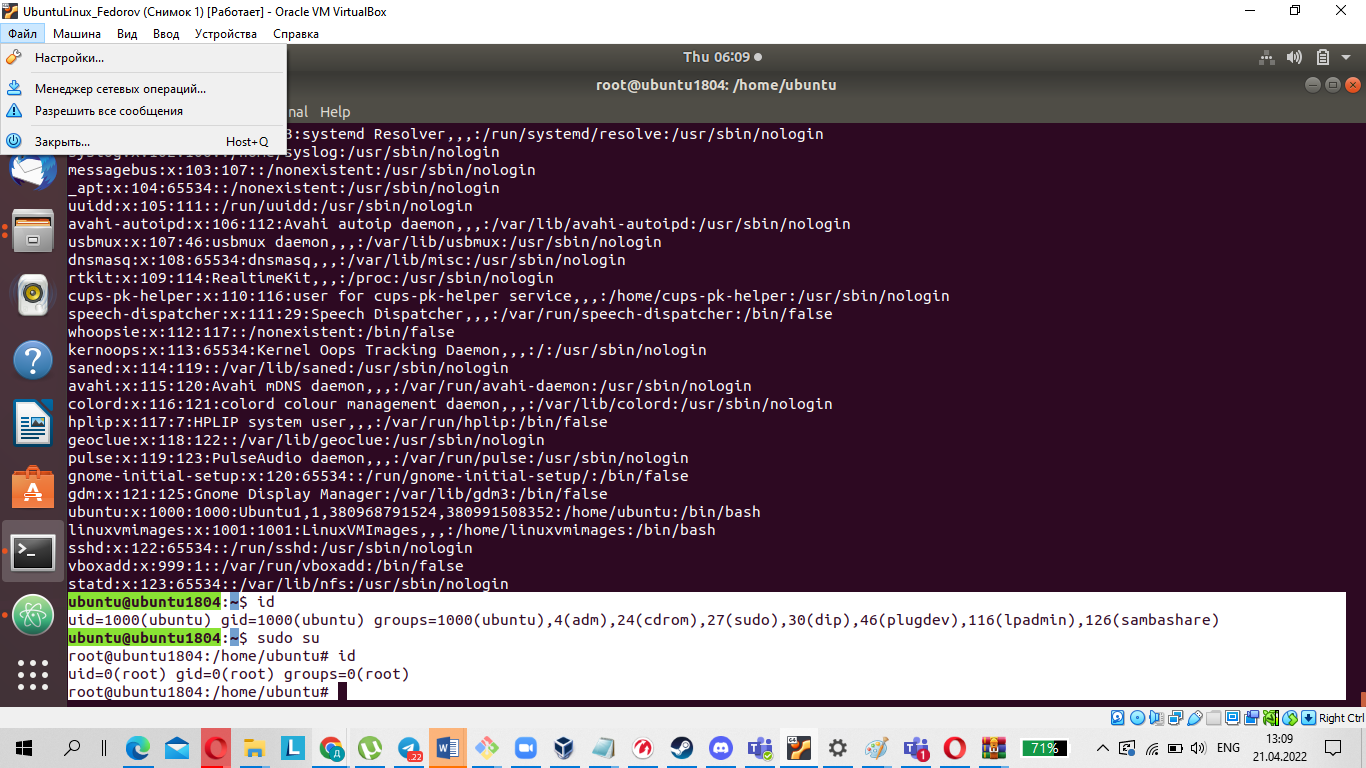
2.What are the uid ranges? What is UID? How to define it?

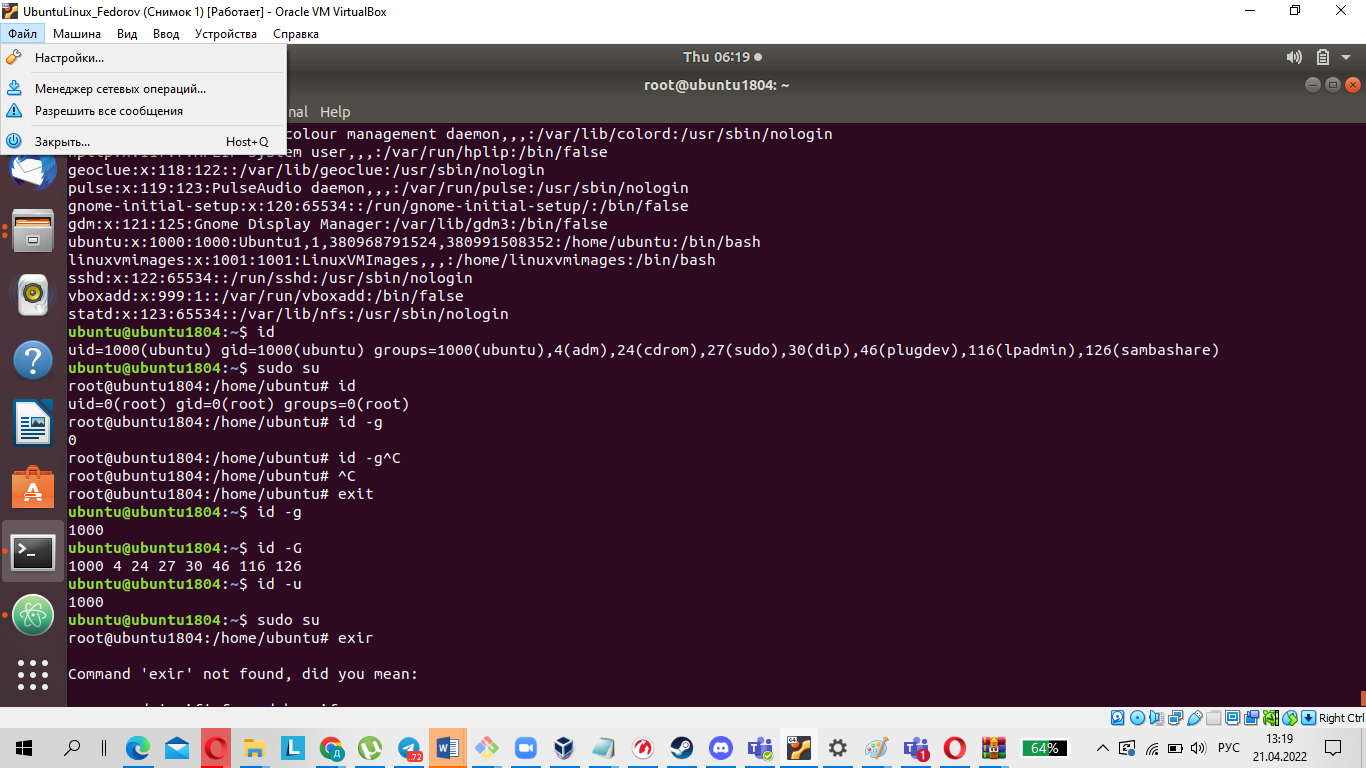
The system UIDs from 0 to 99 should be statically allocated by the system, and shall not be created by applications. The system UIDs from 100 to 499 should be reserved for dynamic allocation by system administrators and post install scripts using useradd.

A UID (user identifier) is a number assigned by Linux to each user on the system. This number is used to identify the user to the system and to determine which system resources the user can access.

The UID can be determined by the following commands:

id -u username





3.What is GID? How to define it?

Groups in Linux are defined by GIDs (group IDs).

GID 0 (zero) is reserved for the root group.

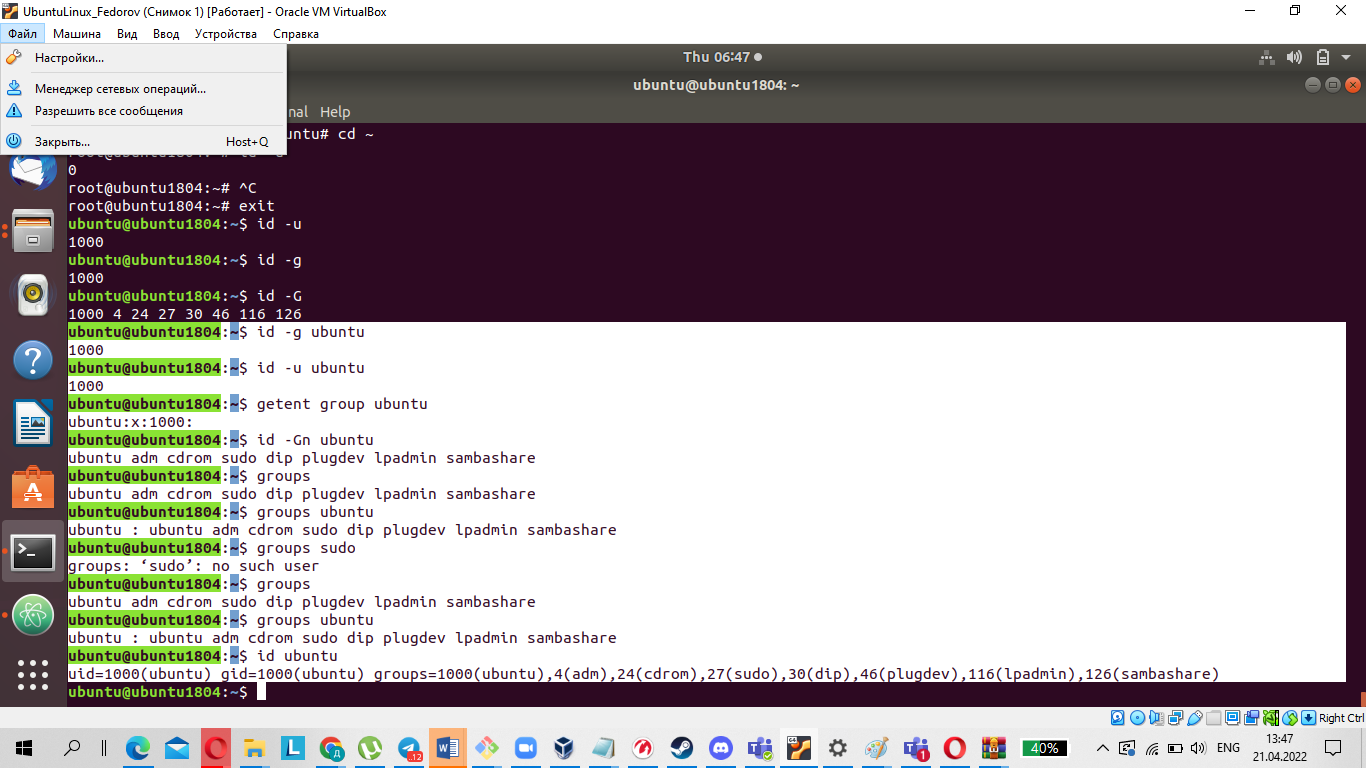
GID 1–99 are reserved for the system and application use.

GID 100+ allocated for the user’s group.

The UID can be determined by the following commands:

id -g username

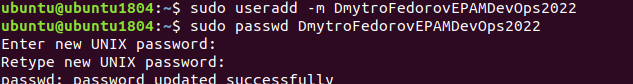
4.How to determine belonging of user to the specific group?



1. What are the commands for adding a user to the system? What are the basic parameters required to create a user?

The basic syntax of the useradd command is:

# useradd [options] username



Create a user with different home directory

sudo useradd -d /data/projects username

Create a user with a specific user id

sudo useradd -u id username

Create a user with a specific group id

sudo useradd -u id -g name group

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

Using the usermod -l login-name old-name command



7.What is skell\_dir? What is its structure?

skell\_dir - directory containing files to be copied to the newly created directory uid - unique user identifier.



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

To delete a user account named username using the userdel command you would run:

userdel username



Use the -r (--remove) option to force userdel to remove the user’s home directory and mail spool:

userdel -r username

Another option is to use the -f (--force) option that tells userdel to forcefully remove the user account, even if the user is still logged in or if there are running processes that belong to the user.

userdel -f username

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

Merhod1

passwd -l user\_name

passwd -u user\_name

Method2

usermod -L user\_name

usermod -U user\_name

Method3

chage -E 1 username

chage -E -1 username

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

Method1

passwd --delete username

Method2

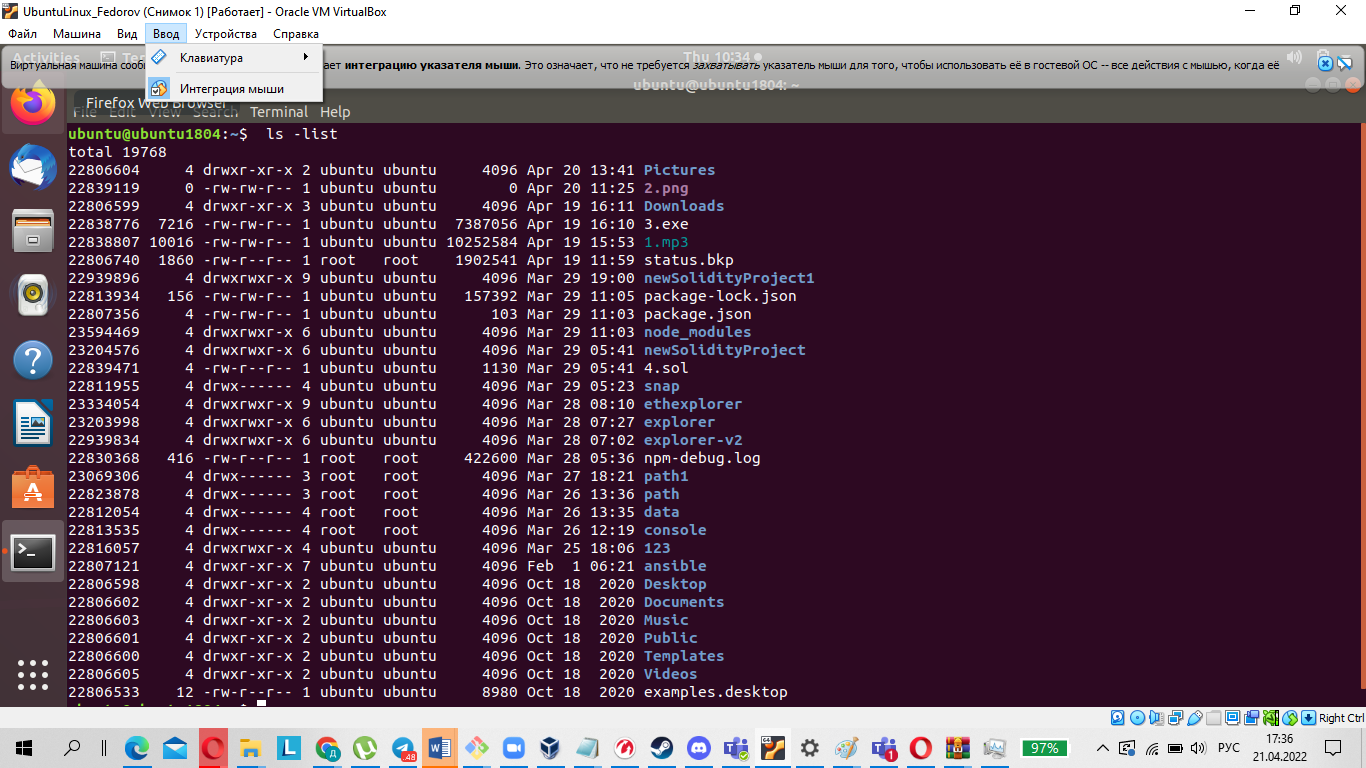
passwd -d username

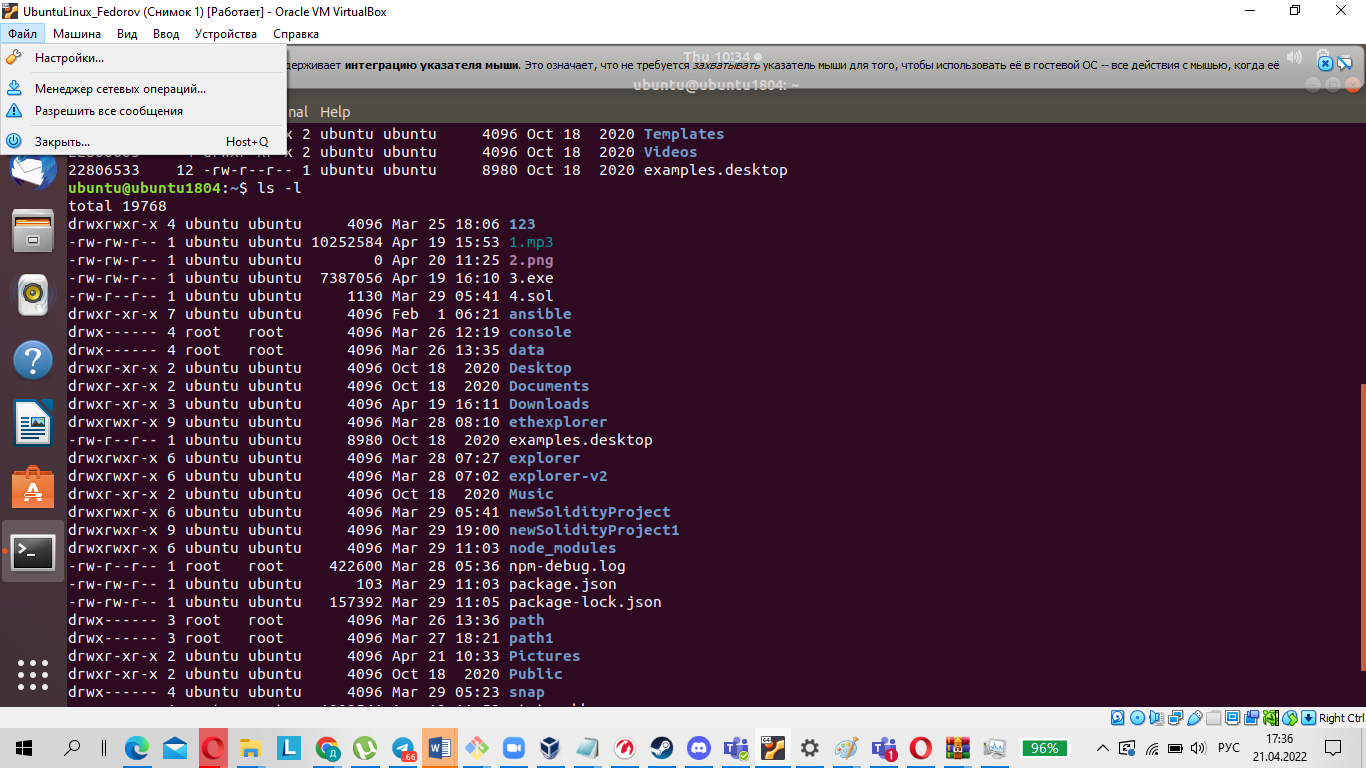
Method3

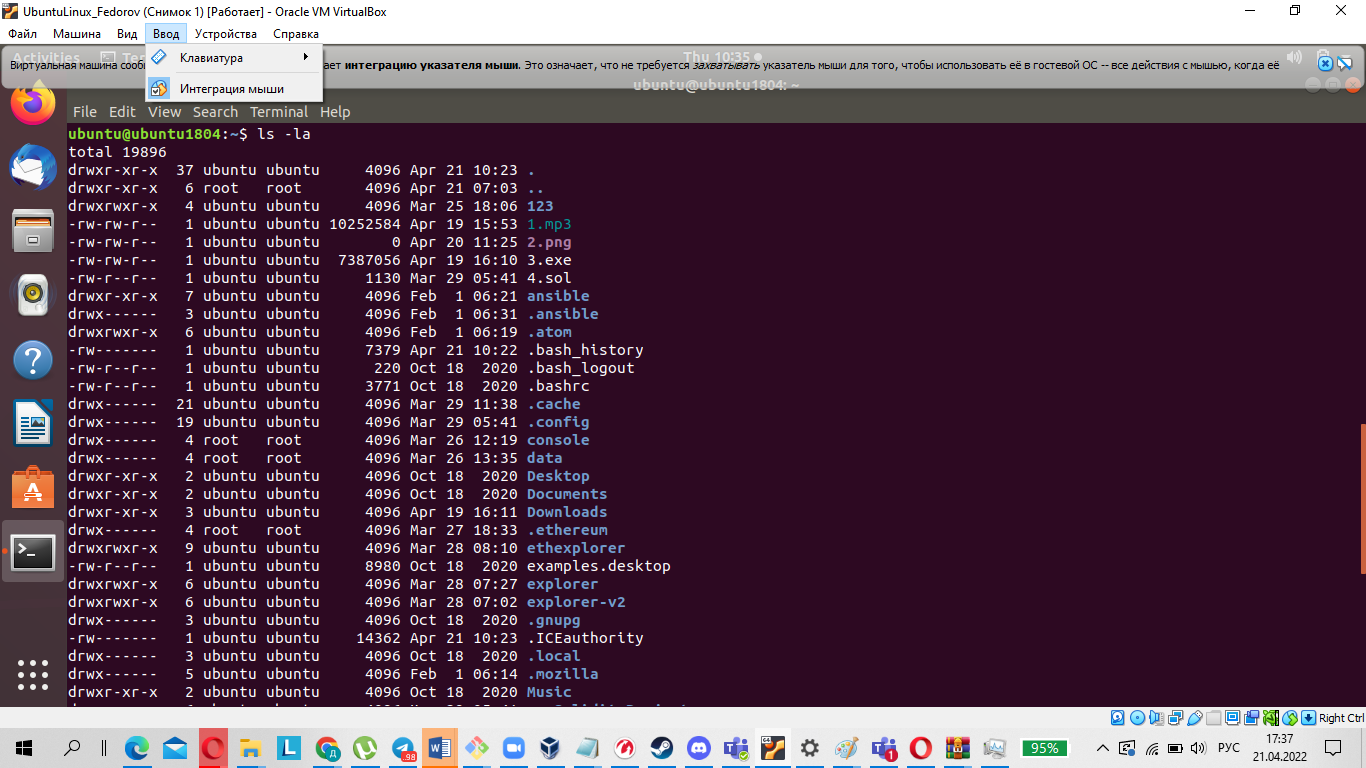
sudo passwd -d username



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







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

Read, write, execute and –

The ‘r’ means you can “read” the file’s contents.

The ‘w’ means you can “write”, or modify, the file’s contents.

The ‘x’ means you can “execute” the file. This permission is given only if the file is a program.

If any of the “rwx” characters is replaced by a ‘-‘, then that permission has been revoked.

User, group and others

user – The user permissions apply only the owner of the file or directory, they will not impact the actions of other users.

group – The group permissions apply only to the group that has been assigned to the file or directory, they will not effect the actions of other users.

others – The others permissions apply to all other users on the system, this is the permission group that you want to watch the most.

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

When figuring out the relationship between the file and the user who started the process, the role is defined as follows:

1.If the UID of the file matches the UID of the process, the user is the owner of the file.

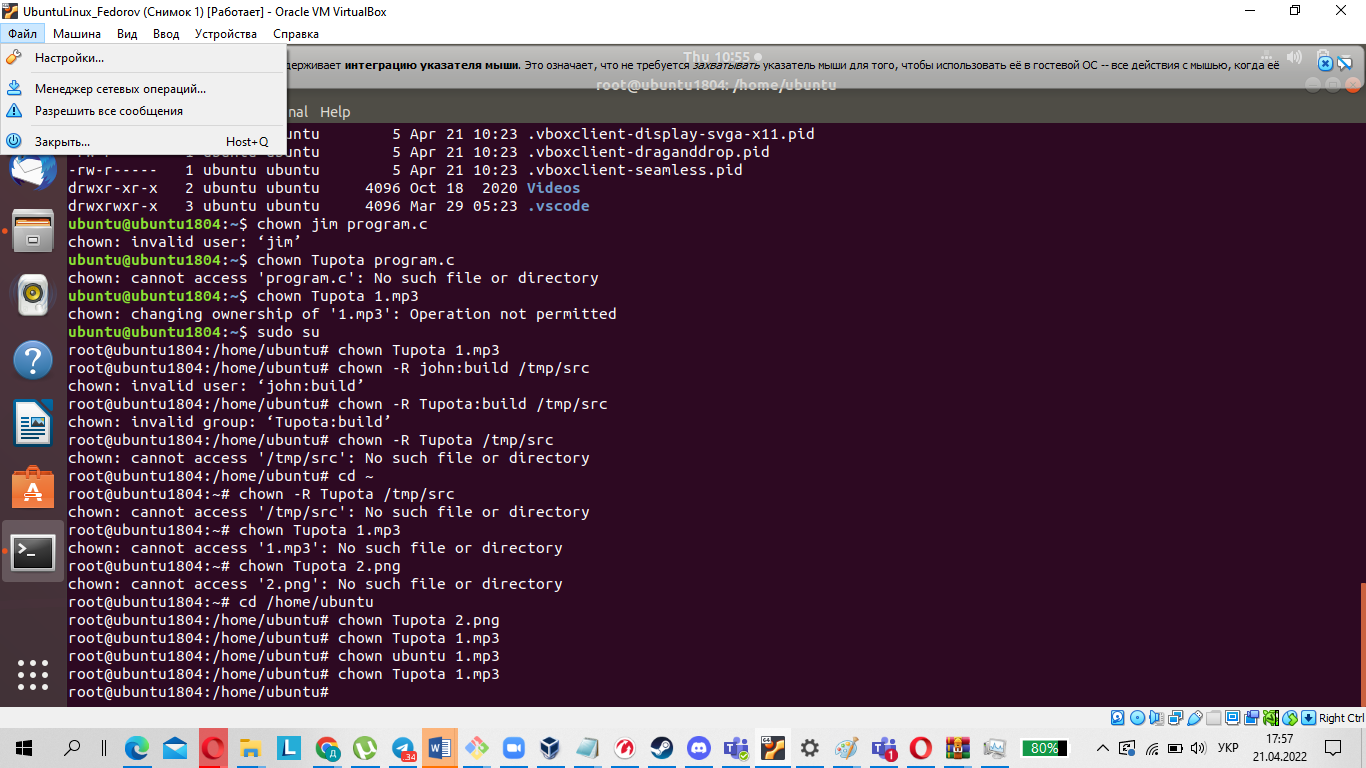
2.If the GID of the file matches the GID of any group the user belongs to, the user is a member of the group the file belongs to.

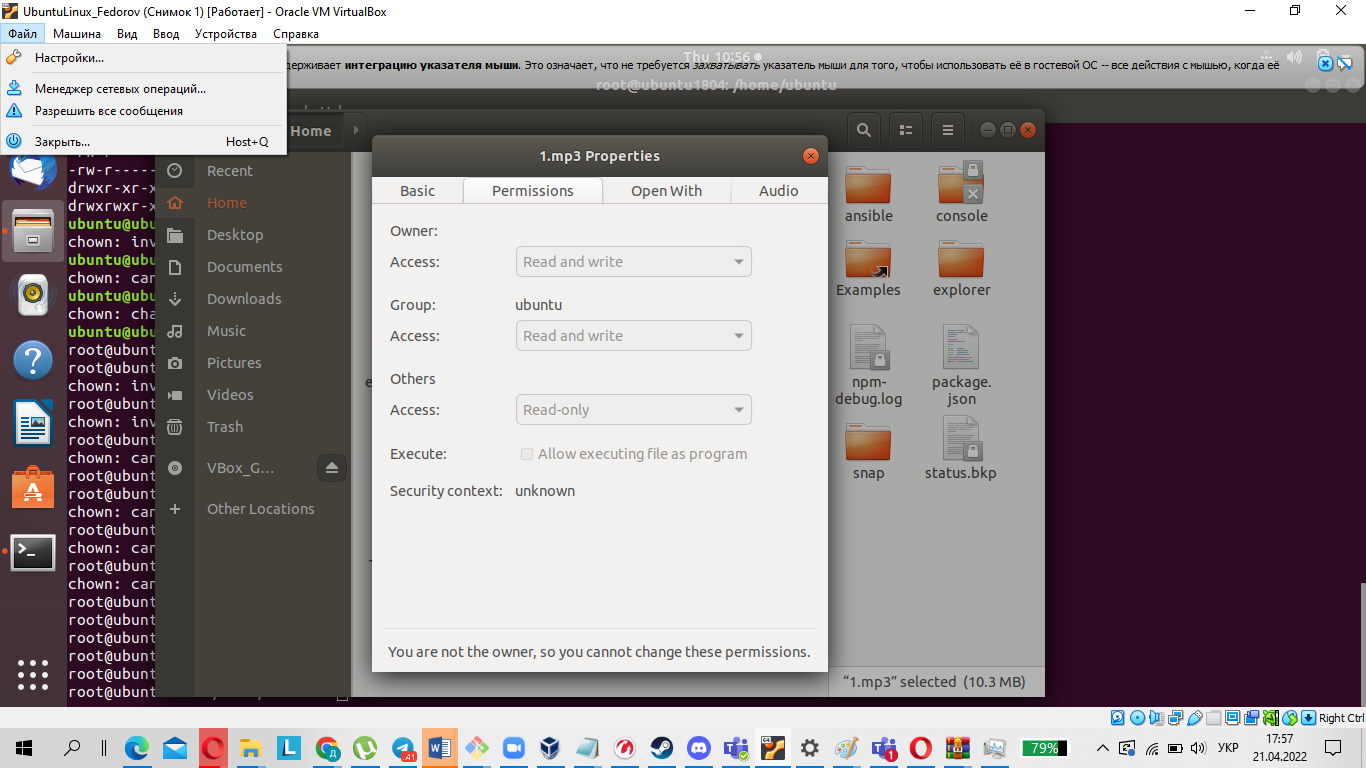
3.If neither the UID nor the GID of the file overlap with the process UID and the list of groups the user who started it belongs to, the user is an intruder.

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.

chown [ -f ] [ -h ] [ -R ] Owner [ :Group ] { File ... | Directory ... }

chown -R [ -f ] [ -H | -L | -P ] Owner [ :Group ] { File ... | Directory ... }





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

The octal number is the sum of the permission values, for example:

3 (1+2) – able to execute and write

6 (2+4) – able to write and read

On Linux and other Unix-like operating systems, new files are created with a default set of permissions. Specifically, a new file's permissions may be restricted in a specific way by applying a permissions "mask" called the umask. The umask command is used to set this mask, or to show you its current value.

Syntax

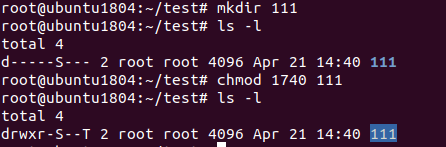
umask [-S] [mask]

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

The sticky bit is a permission bit that is set for a file or directory, which allows only the owner of the file/directory or the root user to delete or rename the file. No other user has permission to delete a file created by another user.

Command substitution allows you to use the command output stream as arguments to other commands. The command substitution mechanism has an alternative syntax inherited from older shells.





This command adds execution permission for all users:

chmod +x yourfile

This command adds write permission to the group and removes read permission for others:

chmod g+w,o-r yourfile

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

The following file attributes must be present in a script:

Read - designated as an "r"; allows a file to be read, but nothing can be written to or changed in the file.

Write - designated as a "w"; allows a file to be written to and changed.

Execute - designated as an "x"; allows a file to be executed by users or the operating system.