Task2

1) Analyze the structure of the /etc/passwd and /etc/group file, what fields are present in it, what users exist on the system?
   The /etc/passwd contains username, password, uid, gid, uid comments, directory and shell.
   The /etc/group file contains group name, password, group id, list of users.

Specify several pseudo-users, how to define them?

-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?
   This is unique identifier:
   0 (root), 1-999(daemons, pseudo-users, system and reserved users), 1000+(regular users).

What is UID?

Unique identifier of user within the system.

How to define it? From /etc/passwd (username: pswd: uid: gid: uid comments: directory: shell)

3) What is GID?

Unique identifier of the group within the system where user belongs.

How to define it?

From /etc/passwd (username: pswd: uid: gid: uid comments: directory: shell)

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

In /etc/group there should be a list of groups, each of them contains a list of users what belongs there.

group_name :password :group_id :list

5) What are the commands for adding a user to the system?
   useradd [-c uid comment] [-d dir] [-e expire] [-f inactive] [-g gid] [-m [-k skel_dir]] [-s shell] [-u uid [-o]] username

What are the basic parameters required to create a user? Username. Additional parameters are: uid, dir (directory), expire, gid (ir or name of group) etc

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

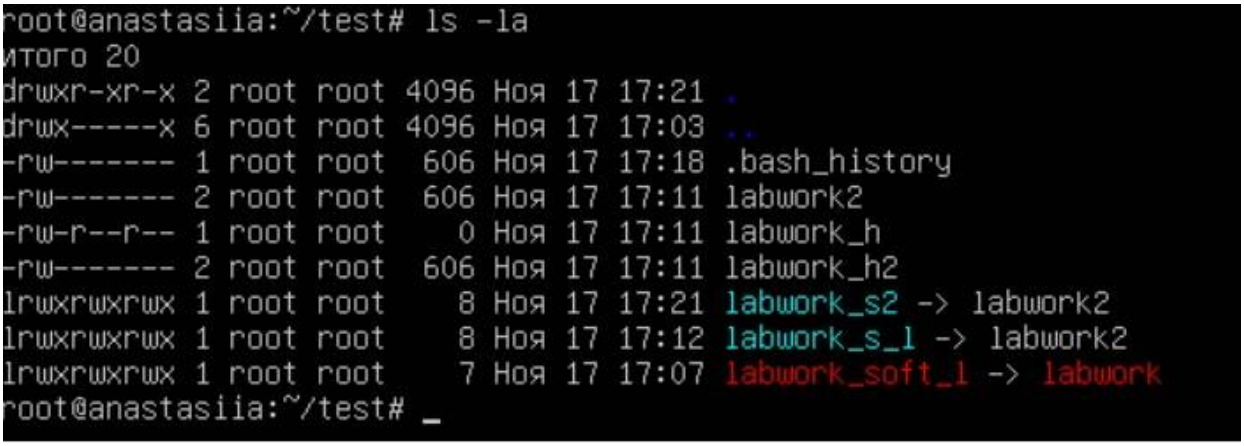
Using command Usermod -l <new username> <old username>

7) What is skell_dir? This is the directory that using for running the home directory when creating the user the first time. “skeleton” directory is defined in /etc/default/useradd file.

What is its structure?

```
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

8) How to remove a user from the system (including his mailbox)?
   Using command userdel -r <username>
9) What commands and keys should be used to lock and unlock a user account?
   Block user: passwd -l <username> .Performing by adding the ! prefix to the password
   Unblock: passwd -u <username> and remove prefix ! from password.
10) How to remove a user's password and provide him with a password-free login for subsequent password change?
   Passwd -d <username>
11) Display the extended format of information about the directory, tell about the information columns displayed on the terminal.



The first character indicates the file type:
- - regular file;

d - directory;
b - block device;
c - character device;
l - symbolic link;
p - pipe (pipe, fifo);
s - socket.

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

There are 3 type of users: owner, member of the group and outsider.

Permission types: read (r), write(w) and execute(x).

Briefly describe the acronym for access rights. Depending on the file the access rights to the defferents type of users can be modified.

Access Rights are the permissions an individual user or a computer application holds to read, write, modify files.

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?

Command chown is used to change the owner of file, and chmod with extended parameter format:

- **chmod +rwx filename** to add permissions.
- **chmod -rwx directoryname** to remove permissions.
- **chmod +x filename** to allow executable permissions.
- **chmod -wx filename** to take out write and executable permissions.

Give examples, demonstrate on the terminal.

```
root@anastasiia:~# chown student info.txt
root@anastasiia:~# ls -la
итого 44
drwx------x  6 root    root 4096 Ноя 17 17:03 .
drwxr-xr-x 24 root    root 4096 Ноя 17 14:40 ..
drwxr-xr-x  6 root    root 4096 Ноя 17 12:55 1
drwxr-xr-x  2 root    root 4096 Ноя 17 12:53 2
drwxr-xr-x  2 root    root 4096 Ноя 17 12:53 3
-rw-------  1 root    root  606 Ноя 17 16:56 .bash_history
-rw-r--r--  1 root    root 3106 Окт 22  2015 .bashrc
-rw-r--r--  1 student root  470 Ноя 17 14:20 info.txt
-rw-------  1 root    root    0 Ноя 17 17:04 labwork2
-rw-r--r-x  1 root    root   29 Ноя 17 14:41 .plan
-rw-r--r--  1 root    root  148 Авг 17  2015 .profile
drwxr-xr-x  2 root    root 4096 Ноя 17 17:21 test
root@anastasiia:~#
```

```
root@anastasiia:~# chmod +rwx info.txt
root@anastasiia:~# ls -la
итого 44
drwx------x  6 root    root 4096 Ноя 17 17:03 .
drwxr-xr-x 24 root    root 4096 Ноя 17 14:40 ..
drwxr-xr-x  6 root    root 4096 Ноя 17 12:55 1
drwxr-xr-x  2 root    root 4096 Ноя 17 12:53 2
drwxr-xr-x  2 root    root 4096 Ноя 17 12:53 3
-rw-------  1 root    root  606 Ноя 17 16:56 .bash_history
-rw-r--r--  1 root    root 3106 Окт 22  2015 .bashrc
-rwxr-xr-x  1 student root  470 Ноя 17 14:20 info.txt
-rw-------  1 root    root    0 Ноя 17 17:04 labwork2
-rw-r--r-x  1 root    root   29 Ноя 17 14:41 .plan
-rw-r--r--  1 root    root  148 Авг 17  2015 .profile
drwxr-xr-x  2 root    root 4096 Ноя 17 17:21 test
root@anastasiia:~#
```

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

We can use the `chmod` command to set permissions in either of two modes:

- Absolute Mode - Use numbers to represent file permissions (the method most commonly used to set permissions). When you change permissions by using the absolute mode, represent permissions for each triplet by an octal mode number.
- Symbolic Mode - Use combinations of letters and symbols to add or remove permissions.

Each number in octal value represents file permission set:

0 – no permission , 1-x (execute), 2-w(write), 3 -wx, 4-r (read), 5 -rx, 6 -rw, 7-rwx.

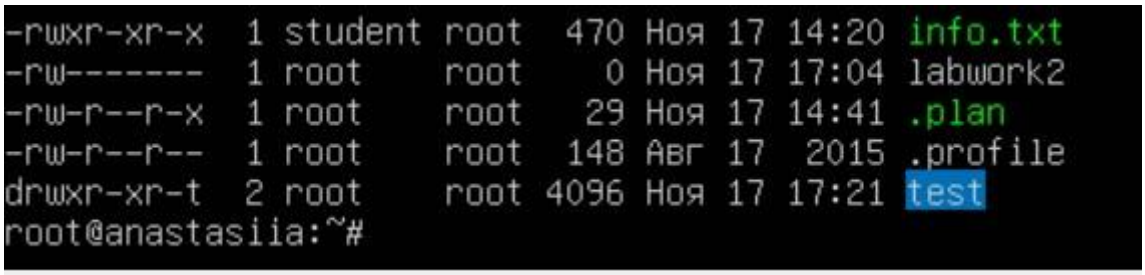
This is done using the umask command. For example, unmask 011 will cause no permission to execute for everyone except the owner.

16) Give definitions of sticky bits and mechanism of identifier substitution.

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. Stiky bit had "t" in the end of its indetifier.

To create sticky bit use command chmod +t <directory>

Give an example of files and directories with these attributes.



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

There are three main file attributes: **read (r), write (w), execute (x)**.