

Отчёт по лабораторной работе №3

Установка и конфигурация ОС

Борисенкова София Павловна

1 сентября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Целью данной работы является получение навыков настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.



```
root@localhost:~ - sudo -i

spborisenkova@localhost:~$ whoami
spborisenkova
spborisenkova@localhost:~$ id
uid=1000(spborisenkova) gid=1000(spborisenkova) groups=1000(spborisenkova),10(wheel) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
spborisenkova@localhost:~$ sudo -i
[sudo] password for spborisenkova:
root@localhost:~# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
root@localhost:~# ezit
bash: ezit: command not found...
root@localhost:~#
```

Рис. 1: root

Работа в учётной записи пользователя bob



```
spborisenkova@localhost:~ - sudo -i visudo

## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
##
## Examples are provided at the bottom of the file for collections
## of related commands, which can then be delegated out to particular
## users or groups.
##
## This file must be edited with the 'visudo' command.

## Host Aliases
## Groups of machines. You may prefer to use hostnames (perhaps using
## wildcards for entire domains) or IP addresses instead.
# Host_Alias    FILESERVERS = fs1, fs2
# Host_Alias    MAILSERVERS = smtp, smtp2

## User Aliases
## These aren't often necessary, as you can use regular groups
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname
## rather than USERALIAS
# User_Alias ADMINS = jsmith, mikem

## Command Aliases
## These are groups of related commands...

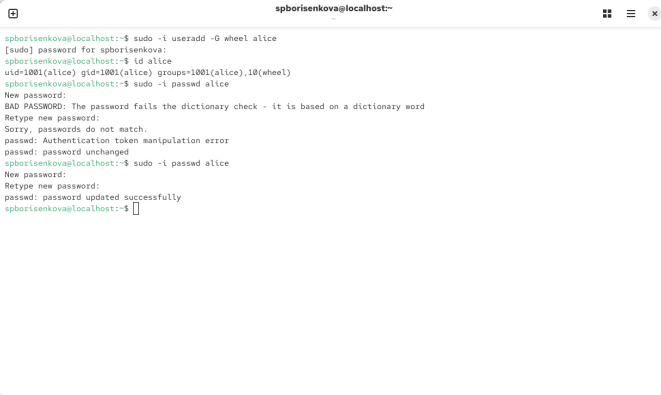
## Networking
# Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient, /usr/bin/net, /sbin/iptables, /usr/bin/rfcomm, /usr/bin/wvdial, /sbin/twconfig, /sbin/mii-tool

## Installation and management of software
# Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum
"/etc/sudoers.tmp" 120L, 432BB

1,1 Top
```

Рис. 2: bob

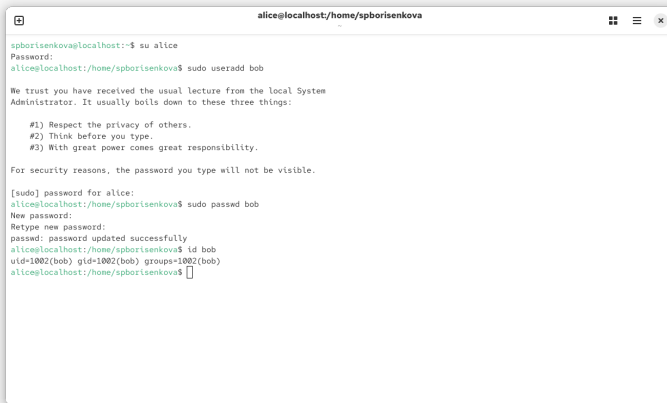
Работа в учётной записи пользователя alice



```
spborisenkova@localhost:~  
spborisenkova@localhost:~$ sudo -i useradd -G wheel alice  
[sudo] password for spborisenkova:  
spborisenkova@localhost:~$ id alice  
uid=1001(alice) gid=1001(alice) groups=1001(alice),10(wheel)  
spborisenkova@localhost:~$ sudo -i passwd alice  
New password:  
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word  
Retype new password:  
Sorry, passwords do not match.  
passwd: Authentication token manipulation error  
passwd: password unchanged  
spborisenkova@localhost:~$ sudo -i passwd alice  
New password:  
Retype new password:  
passwd: password updated successfully  
spborisenkova@localhost:~$
```

Рис. 3: alice

Возвращение в терминал



```
alice@localhost:/home/spborisenkova

spborisenkova@localhost:~$ su alice
Password:
alice@localhost:/home/spborisenkova$ sudo useradd bob

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

For security reasons, the password you type will not be visible.

[sudo] password for alice:
alice@localhost:/home/spborisenkova$ sudo passwd bob
New password:
Retype new password:
passwd: password updated successfully
alice@localhost:/home/spborisenkova$ id bob
uid=1002(bob) gid=1002(bob) groups=1002(bob)
alice@localhost:/home/spborisenkova$
```

Рис. 4: Терминал

Терминал под пользователем root



```
alice@localhost:/home/spborisenkova - nano /etc/login.defs
GNU nano 2.8.1 /etc/login.defs
# Please note that the parameters in this configuration file control the
# behavior of the tools from the shadow-utils component. None of these
# tools uses the PAM mechanism, and the utilities that use PAM (such as the
# passwd command) should therefore be configured elsewhere. Refer to
# /etc/pam.d/system-auth for more information.
#
#
# Delay in seconds before being allowed another attempt after a login failure
# Note: When PAM is used, some modules may enforce a minimum delay (e.g.
#       pam_unix(8) enforces a 2s delay)
#
#FAIL_DELAY          3
#
# Currently FAILLOG_ENAB is not supported
#
# Enable display of unknown usernames when login(1) failures are recorded.
#
#LOG_UNKFAIL_ENAB    no
#
# Currently LOG_OK_LOGINS is not supported
#
# Currently LASTLOG_ENAB is not supported
#
# Limit the highest user ID number for which the lastlog entries should
[ Read 315 lines ]
^G Help      ^O Write Out  ^R Where Is   ^K Cut        ^J Execute    ^C Location   ^M Undo       ^_ Set Mark
^X Exit      ^W Read File  ^I Replace    ^U Paste      ^_ Justify    ^_ Go To Line ^B Redo       ^- Copy
```

Рис. 5: root

В ходе выполнения лабораторной работы были получены представление о работе с учётными записями пользователей и группами пользователей в операционной системе типа Linux.