

Отчёт к лабораторной работе №3

Основы администрирования операционных систем

Борисенкова София Павловна

Содержание

1	Цель работы	5
2	Последовательность выполнения работы	6
3	Контрольные вопросы	12
4	Вывод	13

Список иллюстраций

2.1	Создание каталогов	7
2.2	Пользователь bob	8
2.3	Пользователь Alice	8
2.4	Пользователь bob №2	9
2.5	Пользователь Alice №2	10
2.6	Файлы	10
2.7	Новые файлы	11

Список таблиц

1 Цель работы

Целью данной работы является приобретение практических навыков работы с пользователями в Rocky Linux.

2 Последовательность выполнения работы

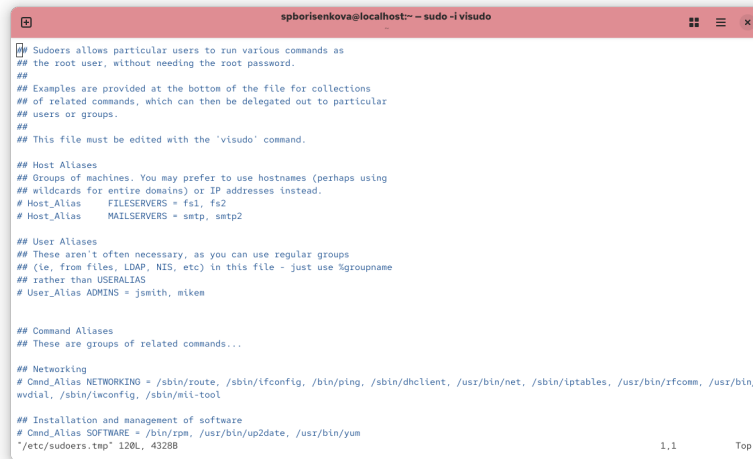
Открываем терминал с учётной записью root: `su -`. В корневом каталоге создаём каталоги `/data/main` и `/data/third` командой: `mkdir -p /data/main /data/third`. Посмотрим, кто является владельцем этих каталогов. Для этого используем: `ls -Al /data`. Владелец каталогов является суперпользователь. Прежде чем устанавливать разрешения, изменим владельцев этих каталогов с root на main и third соответственно: `chgrp main /data/main` и `chgrp third /data/third`. Теперь владельцем этих каталогов является main и third. Далее установим разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам: `chmod 770 /data/main` и `chmod 770 /data/third`. Проверим установленные права доступа

A terminal window titled 'root@localhost:~ - sudo -i' with a red header bar. The terminal shows a user 'spborisenkova' running 'whoami' and 'id' commands. The 'id' command output shows the user is 'spborisenkova' with UID 1000 and GID 1000, belonging to the 'spborisenkova' and 'wheel' groups. Then, the user runs 'sudo -i', enters a password, and becomes root. The root prompt shows the user is 'root' with UID 0 and GID 0, belonging to the 'root' group. Finally, the user runs 'ezit', which results in a 'bash: ezit: command not found...' error.

```
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. 2.1: Создание каталогов

В другом терминале перейдём под учётную запись пользователя bob: `su – bob`. Под пользователем bob попробуем перейти в каталог `/data/main` и создать файл `emptyfile` в этом каталоге: `cd /data/main` и `touch emptyfile`. Так как пользователь bob является владельцем каталога main, нам удалось перейти в этот каталог и создать в нём новый файл. Теперь под пользователем bob попробуем перейти в каталог `/data/third` и создать файл `emptyfile` в этом каталоге. Так как пользователь bob не является владельцем каталога third, нам не удалось перейти в этот каталог и создать в нём новый файл



```
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 USERALIASES
# User_Alias    ADMINS = jsmith, mikem

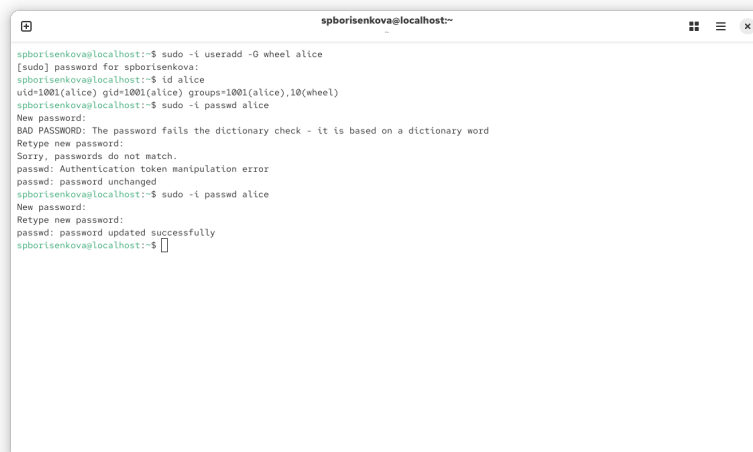
## Command Aliases
## These are groups of related commands...

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

## Installation and management of software
# Cmnd_Alias    SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum
"/etc/sudoers.tmp" 128L, 4328B                                     1,1                                     Top
```

Рис. 2.2: Пользователь bob

Откроем новый терминал под пользователем alice: `su - alice`. Перейдём в каталог `/data/main`: `cd /data/main`. В нём создадим два файла, владельцем которых является alice: `touch alice1` и `touch alice2`. Командой `ls` проверим корректность выполнения предыдущей команды



```
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. 2.3: Пользователь Alice

В другом терминале, под учётной записью пользователя bob (пользователь bob является членом группы main, как и alice) перейдём в каталог `/data/main`:

cd /data/main (данный каталог уже был открыт в нашем терминале) и в этом каталоге введём: ls. Мы увидим два файла, созданные пользователем alice. Теперь попробуем удалить файлы, принадлежащие пользователю alice командой: rm -f alice*. Убедимся, что файлы будут удалены пользователем bob. После проверки командой ls создадим два файла, которые принадлежат пользователю bob: touch bob1 и touch bob2.

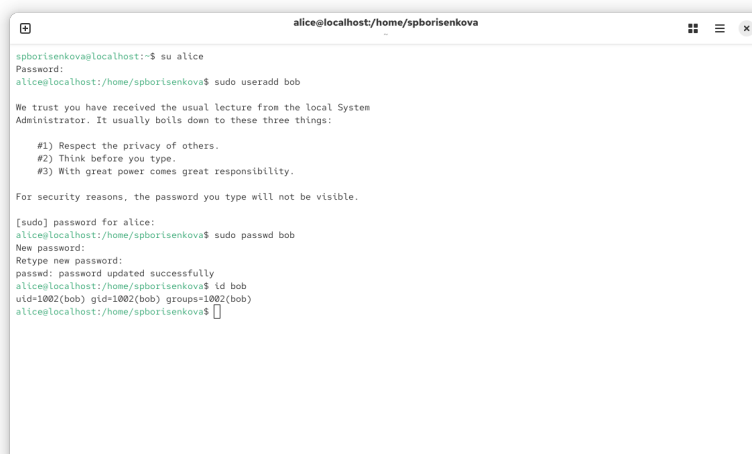
A terminal window titled 'alice@localhost/home/spborisenkova' showing the process of adding a new user 'bob'. The user 'spborisenkova' switches to 'alice' using 'su alice'. Then, 'alice' uses 'sudo useradd bob' to create the user. A standard Ubuntu-style warning message is displayed. Finally, 'alice' sets a password for 'bob' using 'sudo passwd bob', and the system confirms the password was updated successfully. The terminal ends with the command 'id bob' showing the user's identity as 'uid=1002(bob) gid=1002(bob) groups=1002(bob)'.

Рис. 2.4: Пользователь bob №2

Переходим в терминал под пользователем alice и создаём в каталоге /data/main файлы alice3 и alice4: touch alice3 и touch alice4. Теперь мы должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main: ls и ls -Al /data. В этом же терминале попробуем удалить файлы, принадлежащие пользователю bob: rm -rf bob*. Убедимся, что sticky-bit предотвратит удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов



Рис. 2.5: Пользователь Alice №2

Откроем терминал с учётной записью root и установим права на чтение и выполнение в каталоге /data/main для группы third и права на чтение и выполнение для группы main в каталоге /data/third: setfacl -m g:third:rx /data/main и setfacl -m g:main:rx /data/third. Теперь используем команду getfacl, чтобы убедиться в правильности установки разрешений: getfacl /data/main и getfacl /data/third

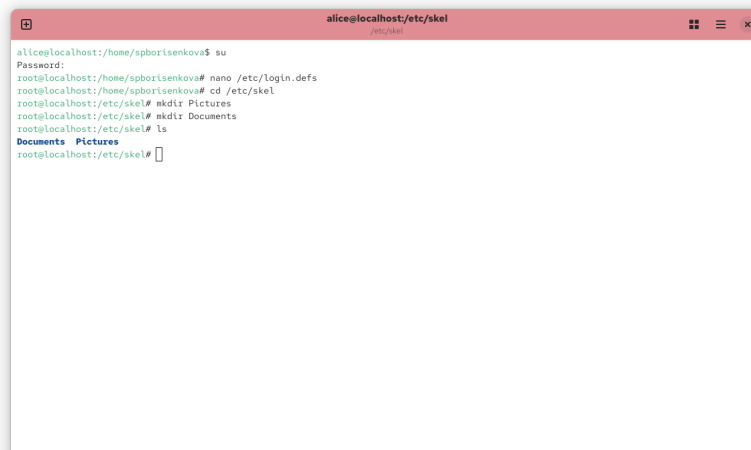
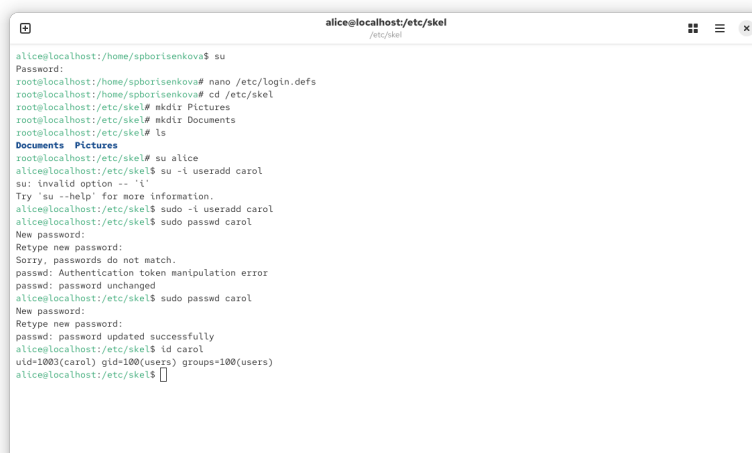


Рис. 2.6: Файлы

Далее создадим новый файл с именем newfile1 в каталоге /data/main: touch /data/main/newfile1. Используем getfacl /data/main/newfile1 для проверки текущих

назначений полномочий. У пользователя только чтение и запись, у группы и других только чтение.



```
alice@localhost:/home/spborisenkova$ su
Password:
root@localhost:/home/spborisenkova# nano /etc/login.defs
root@localhost:/home/spborisenkova# cd /etc/skel
root@localhost:/etc/skel# mkdir Pictures
root@localhost:/etc/skel# mkdir Documents
root@localhost:/etc/skel# ls
Documents  Pictures
root@localhost:/etc/skel# su alice
alice@localhost:/etc/skel$ su -i useradd carol
su: invalid option -- 'i'
Try 'su --help' for more information.
alice@localhost:/etc/skel$ sudo -i useradd carol
alice@localhost:/etc/skel$ sudo passwd carol
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
alice@localhost:/etc/skel$ sudo passwd carol
New password:
Retype new password:
passwd: password updated successfully
alice@localhost:/etc/skel$ id carol
uid=1003(carol) gid=100(users) groups=100(users)
alice@localhost:/etc/skel$
```

Рис. 2.7: Новые файлы

Для проверки полномочий группы third в каталоге /data/third войдём в другом терминале под учётной записью члена группы third: su – carol и проверим операции с файлами: rm /data/main/newfile1 и rm /data/main/newfile2. Система не даёт удалить данные файлы. Теперь проверим, возможно ли осуществить запись в файл: echo “Hello, world” » /data/main/newfile1 echo “Hello, world” » /data/main/newfile2 В файл newfile1 запись осуществить не получилось, а вот в newfile2 всё выполнилось

3 Контрольные вопросы

1. `chown bob:main data/third/newfile`
2. `find ~ -user bob -print`
3. `chmod 770`
4. `chmod +x file`
5. `getfacl "name"`
6. `chmod g+s,o+t path`
7. `setfacl -m g:group:dir path`
8. `setfacl -dm g:group:r parh`
9. `007`
10. `sudo chattr +i filename`

4 Вывод

В ходе работы были получены навыки обращения с пользователями и группами в Rocky Linux