

Лабораторная работа №2. Управление пользователями и группами

Отчёт

Сергеев Даниил Олегович

Содержание

1	Цель работы	5
2	Задание	6
3	Ход выполнения лабораторной работы	7
3.1	Переключение учётных записей пользователей	7
3.2	Создание учётных записей пользователей	10
3.3	Работа с группами	13
4	Ответы на контрольные вопросы	15
5	Вывод	18
	Список литературы	19

Список иллюстраций

3.1	Вывод команд <code>whoami</code> и <code>id</code> для пользователя <code>dosergeev</code>	7
3.2	Вывод команд <code>id</code> для <code>root</code>	8
3.3	Файл <code>/etc/sudoers</code>	8
3.4	Создание пользователя <code>alice</code>	9
3.5	Создание пользователя <code>bob</code>	9
3.6	Задание пароля и проверка групп <code>bob</code> 'а	9
3.7	Редактирование <code>/etc/login.defs</code>	10
3.8	Создание каталогов по умолчанию	11
3.9	Редактирование <code>.bashrc</code>	11
3.10	Создание пользователя <code>carol</code>	12
3.11	Информация о пользователе <code>carol</code>	12
3.12	Информация о пароле <code>carol</code>	13
3.13	Проверка идентификатора <code>alice</code>	13
3.14	Проверка идентификатора <code>carol</code>	13
3.15	Задание по работе с группами	13
4.1	Пример команд	15
4.2	Пример для <code>alice</code>	17

Список таблиц

1 Цель работы

Получить представление о работе с учётными записями пользователей и группами пользователей в операционной системе типа Linux. [1]

2 Задание

- Прочитать справочное описание man по командам ls, whoami, id, groups, su, sudo, passwd, vi, visudo, useradd, usermod, userdel, groupadd, groupdel.
- Выполнить действия по переключению между учётными записями пользователей, по управлению учётными записями пользователей.
- Выполнить действия по созданию пользователей и управлению их учётными записями.
- Выполнить действия по работе с группами пользователей.

3 Ход выполнения лабораторной работы

3.1 Переключение учётных записей пользователей

Войдем в систему и откроем терминал. Проверим какая учётная запись используется на данный момент командой `whoami`. Выведем более подробную информацию с помощью `id`. Данная команда выводит:

- `uid=1000` - уникальный номер пользователя
- `gid=1000` - уникальный номер основной группы пользователя
- `groups=1000,10` - список групп (основной и дополнительных), в которых состоит пользователь
- `context=...` - контекст безопасности пользователя SELinux



```
[dosergeev@dosergeev ~]$ whoami
dosergeev
[dosergeev@dosergeev ~]$ id
uid=1000(dosergeev) gid=1000(dosergeev) groups=1000(dosergeev),10(wheel) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[dosergeev@dosergeev ~]$
```

Рис. 3.1: Вывод команд `whoami` и `id` для пользователя `dosergeev`

Перейдем в учётную запись `root` и также напишем команду `id`. На этот раз получим такую информацию:

- `uid=0`

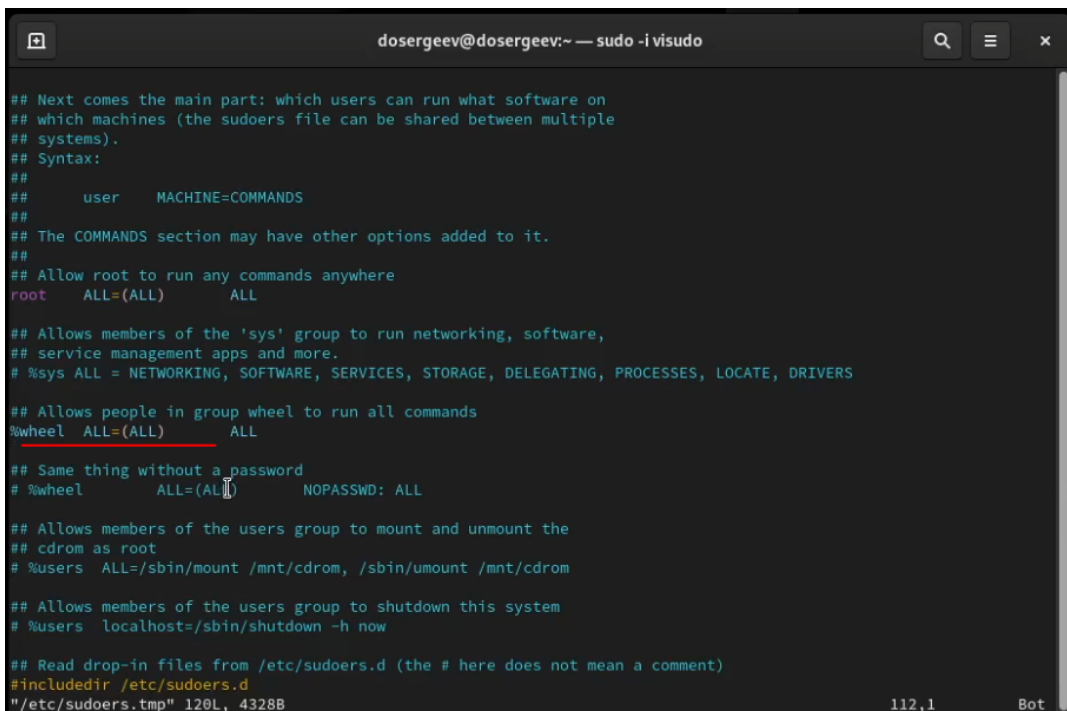
- gid=0
- groups=0

То есть для пользователя root и его основной группы предназначен специальный идентификатор 0, одинаковый для каждой системы.

```
[dosergeev@dosergeev ~]$ su root
Password:
[root@dosergeev dosergeev]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@dosergeev dosergeev]#
exit
[dosergeev@dosergeev ~]$
```

Рис. 3.2: Вывод команд id для root

Вернемся к своей учётной записи и откроем файл /etc/sudoers в безопасном режиме с помощью visudo. Это нужно для того чтобы измененные строки были проверены на синтаксис, иначе ошибка в файле может привести к полной блокировке доступа к sudo для всех пользователей. Убедимся что в открытом файле присутствует нужная строка



```
## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)        ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)        ALL

## Same thing without a password
# %wheel    ALL=(ALL)        NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users    ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users    localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
"/etc/sudoers.tmp" 120L, 4328B
```

Рис. 3.3: Файл /etc/sudoers

Эта строка означает, что все пользователи, входящие в специальную группу wheel, предназначенную для администраторов, смогут использовать команду sudo для получения доступа к root-правам.

Теперь создадим пользователя alice и добавим его в группу wheel. Проверим что он добавлен в группу и зададим пароль. Переключимся на учётную запись alice.

```
[dosergeev@dosergeev ~]$ sudo -i useradd -G wheel alice
[dosergeev@dosergeev ~]$ id alice
uid=1001(alice) gid=1001(alice) groups=1001(alice),10(wheel)
[dosergeev@dosergeev ~]$ sudo -i passwd alice
Changing password for user alice.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[dosergeev@dosergeev ~]$ su alice
```

Рис. 3.4: Создание пользователя alice

Создадим пользователя bob и снова установим пароль. Проверим группы в которые он входит - только в основную 1002.

```
[alice@dosergeev dosergeev]$ 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.

[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
[alice@dosergeev dosergeev]$ id bob
uid=1002(bob) gid=1002(bob) groups=1002(bob)
[alice@dosergeev dosergeev]$
```

Рис. 3.5: Создание пользователя bob

```
[alice@dosergeev dosergeev]$
[alice@dosergeev dosergeev]$ sudo passwd bob
Changing password for user bob.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[alice@dosergeev dosergeev]$ id bob
uid=1002(bob) gid=1002(bob) groups=1002(bob)
[alice@dosergeev dosergeev]$
```

Рис. 3.6: Задание пароля и проверка групп bob'a

3.2 Создание учётных записей пользователей

Переключимся на учётную запись root и откроем файл конфигурации /etc/login.defs с помощью mc. Найдем параметры CREATE_HOME и USERGROUPS_ENAB. Убедимся что первый из них установлен в значении yes, а второй установим в значении no.

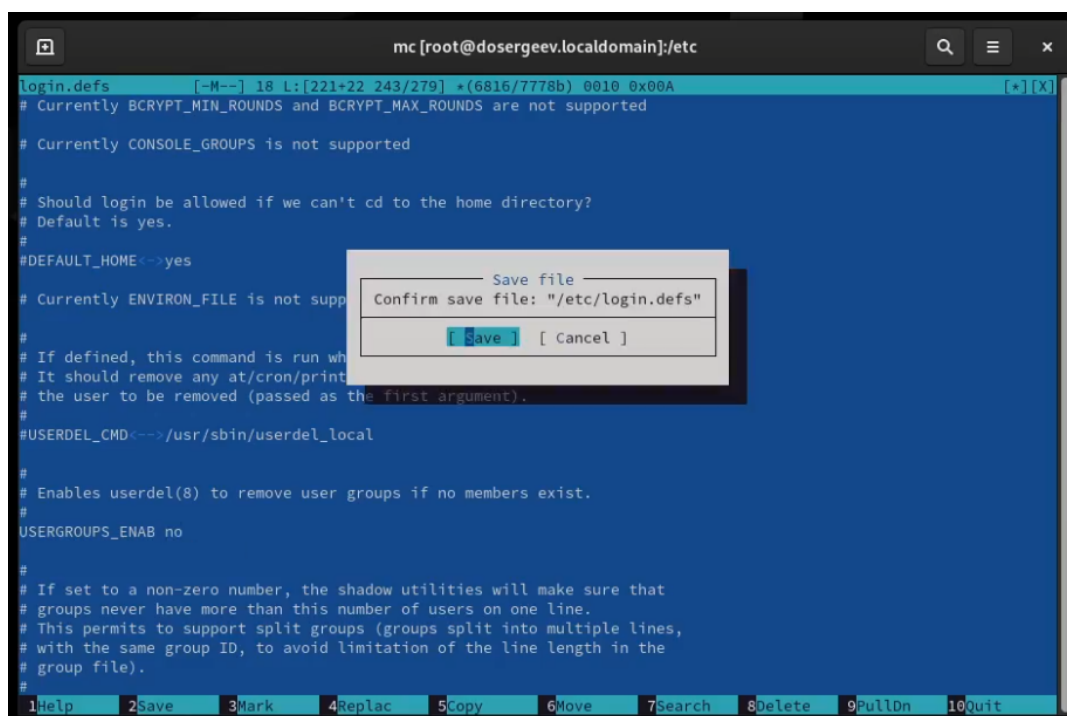


Рис. 3.7: Редактирование /etc/login.defs

Перейдем в каталог /etc/skel и создадим каталоги Pictures и Documents. Изменим содержимое файла .bashrc, добавив две строки.

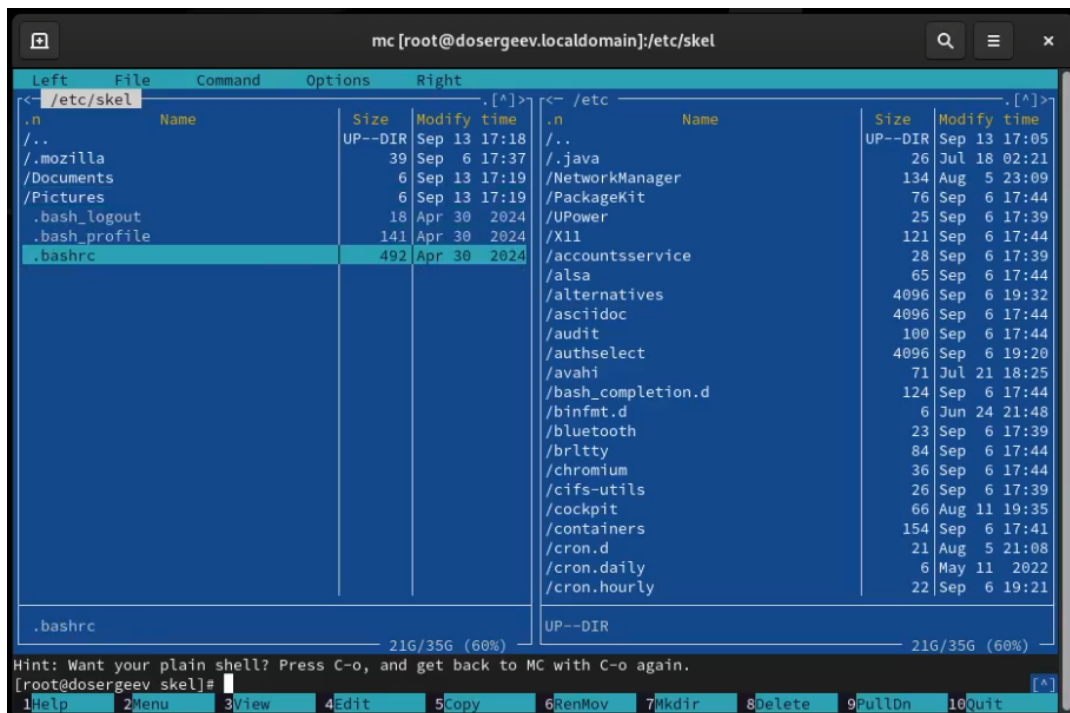


Рис. 3.8: Создание каталогов по умолчанию

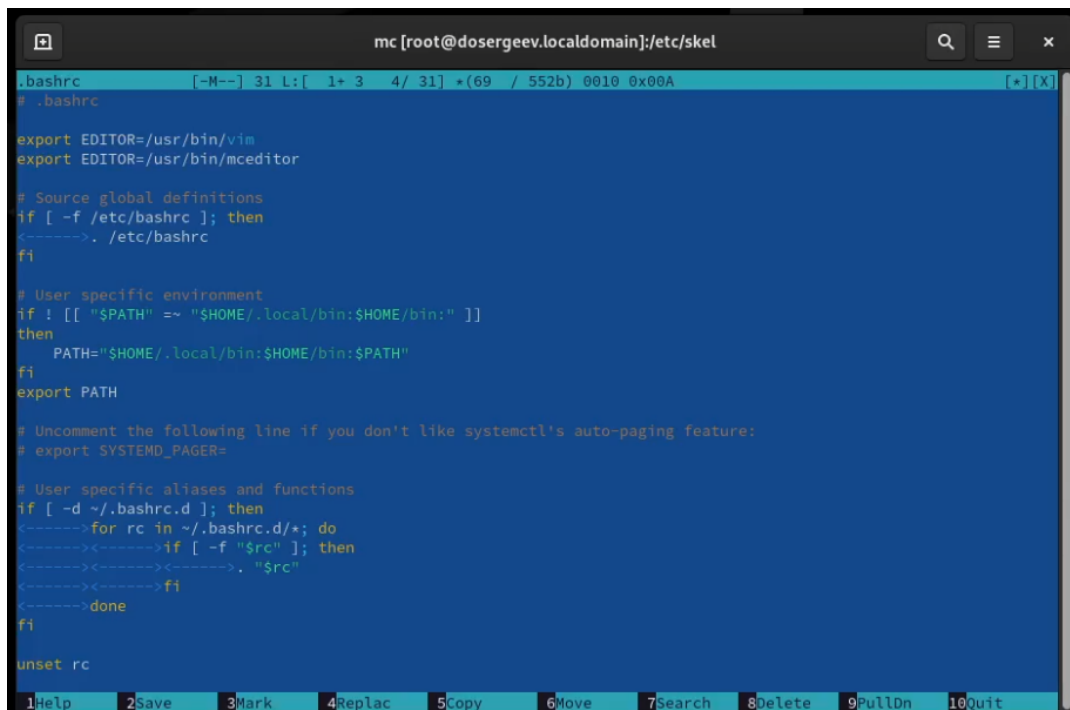


Рис. 3.9: Редактирование .bashrc

Переключимся на пользователя alice и создадим нового с именем carol, уста-

новим пароль. С помощью команды `id` узнаем, что вместо основной группы с именем пользователя, `carol` состоит только в группе `100(users)`. Проверим наличие созданных каталогов по умолчанию.

```
[alice@dosergeev dosergeev]$ sudo -i useradd carol
[alice@dosergeev dosergeev]$ sudo passwd carol
Changing password for user carol.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[alice@dosergeev dosergeev]$ su carol
Password: 
```

Рис. 3.10: Создание пользователя `carol`

```
[carol@dosergeev dosergeev]$
[carol@dosergeev dosergeev]$ id
uid=1003(carol) gid=100(users) groups=100(users) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[carol@dosergeev dosergeev]$ cd
[carol@dosergeev ~]$ ls
Documents Pictures
[carol@dosergeev ~]$ ls -Al
total 16
-rw-r--r--. 1 carol users 18 Apr 30 2024 .bash_logout
-rw-r--r--. 1 carol users 141 Apr 30 2024 .bash_profile
-rw-r--r--. 1 carol users 552 Sep 13 17:19 .bashrc
drwxr-xr-x. 2 carol users 6 Sep 13 17:19 Documents
drwxr-xr-x. 4 carol users 39 Sep 6 17:37 .mozilla
drwxr-xr-x. 2 carol users 6 Sep 13 17:19 Pictures
-rw-----. 1 carol users 130 Sep 13 17:20 .xauthEZRMH3
[carol@dosergeev ~]$
```

Рис. 3.11: Информация о пользователе `carol`

Откроем строку записи о пароле пользователя `carol` в файле `/etc/shadow`. В нем мы можем увидеть следующую информацию: `carol:(хеш-код пароля):20344:0:99999:7:::`

- `carol` - имя пользователя
- хеш-код пароль - пароль в зашифрованном виде
- 20344 - количество дней с 1 января 1970 года, когда пароль был изменен в последний раз
- 0 - минимальное число дней между сменами пароля
- 99999 - максимальное число дней, в течение которых пароль будет работать
- 7 - количество дней, за которое пользователь будет предупрежден о конце срока действия пароля

Изменим свойства пароля пользователя `carol` так, как сказано в лабораторной работе. Проверим изменения.

```
[alice@dosergeev carol]$ sudo cat /etc/shadow | grep carol
carol:$6$rounds=100000$ljY0tKfKJP4v4eL/$wTua/FX5yIwL/0IBhrnSUv/R.2SpXZM3In92Y7sSjTpK0Q5KX/3hBp0MEaVGiv/v/5pXwnZ7wM
mJS1Jzd/zeb/:20344:0:99999:7:::
[alice@dosergeev carol]$ sudo passwd -n 30 -w 3 -x 90 carol
Adjusting aging data for user carol.
passwd: Success
[alice@dosergeev carol]$ sudo cat /etc/shadow | grep carol
carol:$6$rounds=100000$ljY0tKfKJP4v4eL/$wTua/FX5yIwL/0IBhrnSUv/R.2SpXZM3In92Y7sSjTpK0Q5KX/3hBp0MEaVGiv/v/5pXwnZ7wM
mJS1Jzd/zeb/:20344:30:90:3:::
[alice@dosergeev carol]$
```

Рис. 3.12: Информация о пароле carol

Убедимся что идентификатор alice существует во всех трёх файлах и что идентификатор carol существует не во всех трёх файлах.

```
[alice@dosergeev carol]$ grep alice /etc/passwd /etc/shadow /etc/group
/etc/passwd:alice:x:1001:1001::/home/alice:/bin/bash
grep: /etc/shadow: Permission denied
/etc/group:wheel:x:10:dosergeev,alice
/etc/group:alice:x:1001:
[alice@dosergeev carol]$
```

Рис. 3.13: Проверка идентификатора alice

```
[alice@dosergeev carol]$ sudo grep carol /etc/passwd /etc/shadow /etc/group
/etc/passwd:carol:x:1003:100::/home/carol:/bin/bash
/etc/shadow:carol:$6$rounds=100000$ljY0tKfKJP4v4eL/$wTua/FX5yIwL/0IBhrnSUv/R.2SpXZM3In92Y7sSjTpK0Q5KX/3hBp0MEaVGiv
/v/5pXwnZ7wMmJS1Jzd/zeb/:20344:30:90:3:::
[alice@dosergeev carol]$
```

Рис. 3.14: Проверка идентификатора carol

3.3 Работа с группами

Находясь в учётной записи пользователя alice, создадим группы main и third. Используем usermod для добавления alice и bob в группу main, а carol в группу third. Убедимся что carol правильно добавлен в группу.

```
[alice@dosergeev carol]$ sudo groupadd main
[alice@dosergeev carol]$ sudo groupadd third
[alice@dosergeev carol]$ sudo usermod -aG main alice
[alice@dosergeev carol]$ sudo usermod -aG main bob
[alice@dosergeev carol]$ sudo usermod -aG third carol
[alice@dosergeev carol]$ id carol
uid=1003(carol) gid=100(users) groups=100(users),1004(third)
[alice@dosergeev carol]$ id alice
uid=1001(alice) gid=1001(alice) groups=1001(alice),10(wheel),1003(main)
[alice@dosergeev carol]$ id bob
uid=1002(bob) gid=1002(bob) groups=1002(bob),1003(main)
[alice@dosergeev carol]$
```

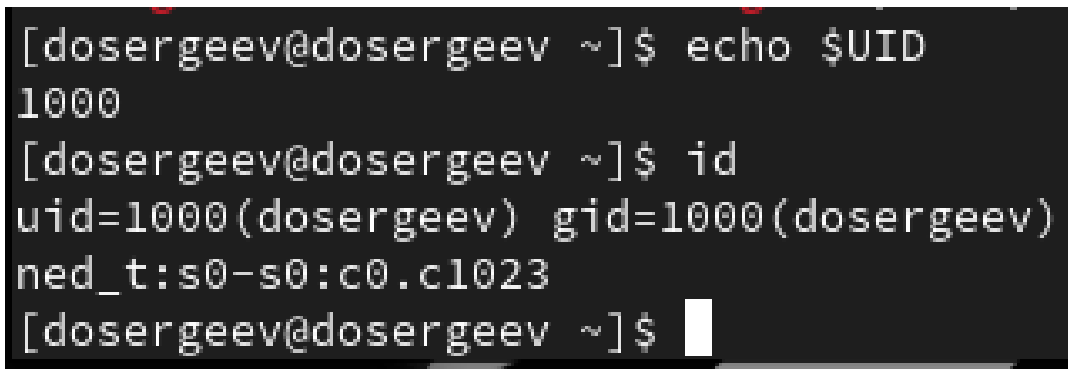
Рис. 3.15: Задание по работе с группами

Определим, участниками каких групп являются другие пользователи, созданные в ходе лабораторной работы.

- alice: groups=1001(alice),10(wheel),1003(main)
- bob: groups=1002(bob),1003(main)

4 Ответы на контрольные вопросы

1. При помощи каких команд можно получить информацию о номере(идентификаторе), назначенном пользователю Linux, о группах, в которые включён пользователь?
 - Информация о номере: `id`
 - Информация о группах: `groups`
2. Какой UID имеет пользователь `root`? При помощи какой команды можно узнать UID пользователя? Приведите примеры.
 - Пользователь `root` имеет UID под номером 0. UID можно узнать с помощью команды `id` или `echo $UID`.



```
[dosergeev@dosergeev ~]$ echo $UID
1000
[dosergeev@dosergeev ~]$ id
uid=1000(dosergeev) gid=1000(dosergeev)
ned_t:s0-s0:c0.c1023
[dosergeev@dosergeev ~]$
```

Рис. 4.1: Пример команд

3. В чём состоит различие между командами `su` и `sudo`?
 - Команда `su` позволяет переключиться на другого пользователя(включая `root`), а `sudo` позволяет выполнить текущую команду от прав `root`.

4. В каком конфигурационном файле определяются параметры sudo?
- В файле `/etc/sudoers`
5. Какую команду следует использовать для безопасного изменения конфигурации sudo?
- Стоит использовать команду `visudo`
6. Если вы хотите предоставить пользователю доступ ко всем командам администрирования системы через sudo, членом какой группы он должен быть?
- Он должен быть членом группы `wheel`
7. Какие файлы/каталоги можно использовать для определения параметров, которые будут использоваться при создании учётных записей пользователей? Приведите примеры настроек.
- Можно использовать:
 - `/etc/skel` - каталог-шаблон для новых пользователей, содержит конфигурационный файл `.bashrc`
 - `/etc/login.defs` - файл, содержит такие настройки как `USERGROUPS_ENAB` (Указывает, создавать ли частную группу для новых пользователей с таким же именем), `CREATE_HOME` (Указывает, следует ли создавать домашний каталог для новых пользователей)
8. Где хранится информация о первичной и дополнительных группах пользователей ОС типа Linux?
- Информация о первичной группе содержится в файле `/etc/passwd` (идентификатор вслед за идентификатором пользователя), а о дополнительных в файле `/etc/group`


```
[dosergeev@dosergeev ~]$ cat /etc/passwd | grep alice
alice:x:1001:1001:~/home/alice:/bin/bash
[dosergeev@dosergeev ~]$ cat /etc/group | grep alice
wheel:x:10:dosergeev,alice
alice:x:1001:
main:x:1003:alice,bob
[dosergeev@dosergeev ~]$
```

Рис. 4.2: Пример для alice

9. Какие команды вы можете использовать для изменения информации о пароле пользователя (например о сроке действия пароля)?
 - Можно использовать команду `passwd` для изменения пароля и `chage` для изменения срока действия пароля.
10. Какую команду следует использовать для прямого изменения информации в файле `/etc/group` и почему?
 - Следует использовать команду `vi` -g. Она нужна для безопасного редактирования файла `/etc/group` (с опцией -g). В отличие от стандартных текстовых редакторов, `vi` будет блокировать файлы на время редактирования, предотвращая одновременные изменения, которые могут повредить системный файл.

5 Вывод

В результате выполнения лабораторной работы я получил представление о работе с учётными записями и группами пользователей и изучил как работает управление доступом в операционной системе типа Linux.

Список литературы

1. Kulyabov, Korolykova. Лабораторная работа №2. Управление пользователями и группами. https://esystem.rudn.ru/pluginfile.php/2843451/mod_resource/content/4/003-user_management.pdf; RUDN.