

# **Отчёт по лабораторной работе №2**

**Управление пользователями и группами**

Тукаев Тимур

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Выполнение</b>	<b>6</b>
2.1 Переключение учётных записей пользователей . . . . .	6
2.2 Просмотр и анализ файла /etc/sudoers . . . . .	7
2.3 Создание пользователей alice и bob . . . . .	8
2.4 Настройка общих параметров создания пользователей . . . . .	10
2.5 Создание и анализ учётной записи carol . . . . .	13
2.6 Работа с файлом /etc/shadow и параметрами паролей . . . . .	14
2.7 Работа с группами . . . . .	16
<b>3 Контрольные вопросы</b>	<b>18</b>
<b>4 Заключение</b>	<b>20</b>

# **Список иллюстраций**

2.1	Определение пользователя и его групп . . . . .	6
2.2	Файл sudoers, открытый через visudo . . . . .	7
2.3	Создание пользователей alice и bob . . . . .	10
2.4	Редактирование файла /etc/login.defs . . . . .	11
2.5	Настройка EDITOR и .bashrc . . . . .	12
2.6	Домашний каталог и информация о carol . . . . .	14
2.7	Просмотр и изменение записи carol в /etc/shadow . . . . .	14
2.8	Создание групп и проверка их состава . . . . .	17

# **Список таблиц**

# **1 Цель работы**

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

## 2 Выполнение

### 2.1 Переключение учётных записей пользователей

1. В системе выполнен вход под обычным пользователем и открыт терминал.

Для определения активной учётной записи использована команда `whoami`, которая показала, что текущий пользователь – `titukaev`.

Затем выполнена команда `id`. Отображены следующие данные:

- `uid=1000(titukaev)` – уникальный идентификатор пользователя;
- `gid=1000(titukaev)` – идентификатор основной группы пользователя;
- `groups=1000(titukaev),10(wheel)` – пользователь состоит в собственной группе и в группе `wheel`, что даёт возможность получать административные права;
- также показан SELinux-контекст текущего процесса.

---

```
titukaev@titukaev:~$ whoami
titukaev
titukaev@titukaev:~$ id
uid=1000(titukaev) gid=1000(titukaev) groups=1000(titukaev),10(wheel) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
titukaev@titukaev:~$ su
Password:
root@titukaev:/home/titukaev# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
root@titukaev:/home/titukaev#
exit
titukaev@titukaev:~$
```

Рис. 2.1: Определение пользователя и его групп

2. Для переключения к учётной записи суперпользователя использована команда `su`.

После ввода пароля `root` выполнен переход в контекст суперпользователя, что подтверждено приглашением командной строки.

Команда `id`, выполненная под root, показала:

- `uid=0(root)` – идентификатор суперпользователя;
- `gid=0(root)` – основная группа root;
- группы, к которым относится root;
- SELinux-контекст для пользователя root.

Возврат к обычному пользователю выполнен с помощью команды `exit`.

## 2.2 Просмотр и анализ файла `/etc/sudoers`

3. Для безопасного редактирования конфигурации прав sudo использована команда `sudo -i visudo`.

В результате был открыт файл `/etc/sudoers` в редакторе, настроенном по умолчанию (vim).

```
Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## 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)
```

Рис. 2.2: Файл sudoers, открытый через visudo

## **Почему требуется использовать visudo, а не произвольный редактор?**

Файл `/etc/sudoers` критически важен для работы механизма `sudo`. Если при редактировании допустить синтаксическую ошибку, система может полностью потерять возможность выдавать административные права через `sudo`.

Утилита `visudo`:

- блокирует файл от одновременного редактирования несколькими пользователями;
- проверяет синтаксис файла перед сохранением;
- в случае ошибки не перезаписывает рабочую конфигурацию.

Поэтому для работы с `/etc/sudoers` необходимо пользоваться именно `visudo`.

4. В файле `/etc/sudoers` найдена строка:

```
%wheel ALL=(ALL) ALL
```

Эта запись означает, что **все пользователи, входящие в группу wheel**, имеют право выполнять через `sudo` **любые команды** от имени **любого пользователя** (в том числе `root`) на любой машине, где действует данная конфигурация.

Группа `wheel` используется как механизм ограниченного делегирования административных привилегий: достаточно добавить пользователя в эту группу, чтобы он получил возможность выполнять команды от имени суперпользователя через `sudo`.

## **2.3 Создание пользователей alice и bob**

5. Пользователь `alice` был создан с включением в группу `wheel` командой  
`sudo -i useradd -G wheel alice`.

Далее выполнена команда `id alice`, подтвердившая:

- наличие пользователя `alice` с собственным `uid`;
  - принадлежность к основной группе `alice`;
  - принадлежность к дополнительной группе `wheel`.
6. Для пользователя `alice` установлен пароль с помощью `sudo -i passwd alice`.  
Пароль вводился дважды, после чего система сообщила об успешном обновлении.
7. Затем выполнено переключение на учётную запись `alice` командой `su alice`.
8. Находясь под пользователем `alice`, создан пользователь `bob` командой `sudo useradd bob`.  
При этом система запросила пароль от `alice` для выполнения команды с повышенными привилегиями.
9. Для пользователя `bob` установлен пароль командой `sudo passwd bob`.  
После ввода и подтверждения пароля система сообщила об успешной смене пароля.
10. Командой `id bob` проверены параметры новой учётной записи:

```

titukaev@titukaev:~$ sudo -i useradd -G wheel alice
titukaev@titukaev:~$ id alice
uid=1001(alice) gid=1001(alice) groups=1001(alice),10(wheel)
titukaev@titukaev:~$ sudo -i passwd alice
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
titukaev@titukaev:~$ su alice
Password:
alice@titukaev:/home/titukaev$ 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@titukaev:/home/titukaev$ sudo passwd bob
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
alice@titukaev:/home/titukaev$ id bob
uid=1002(bob) gid=1002(bob) groups=1002(bob)
alice@titukaev:/home/titukaev$ █

```

Рис. 2.3: Создание пользователей alice и bob

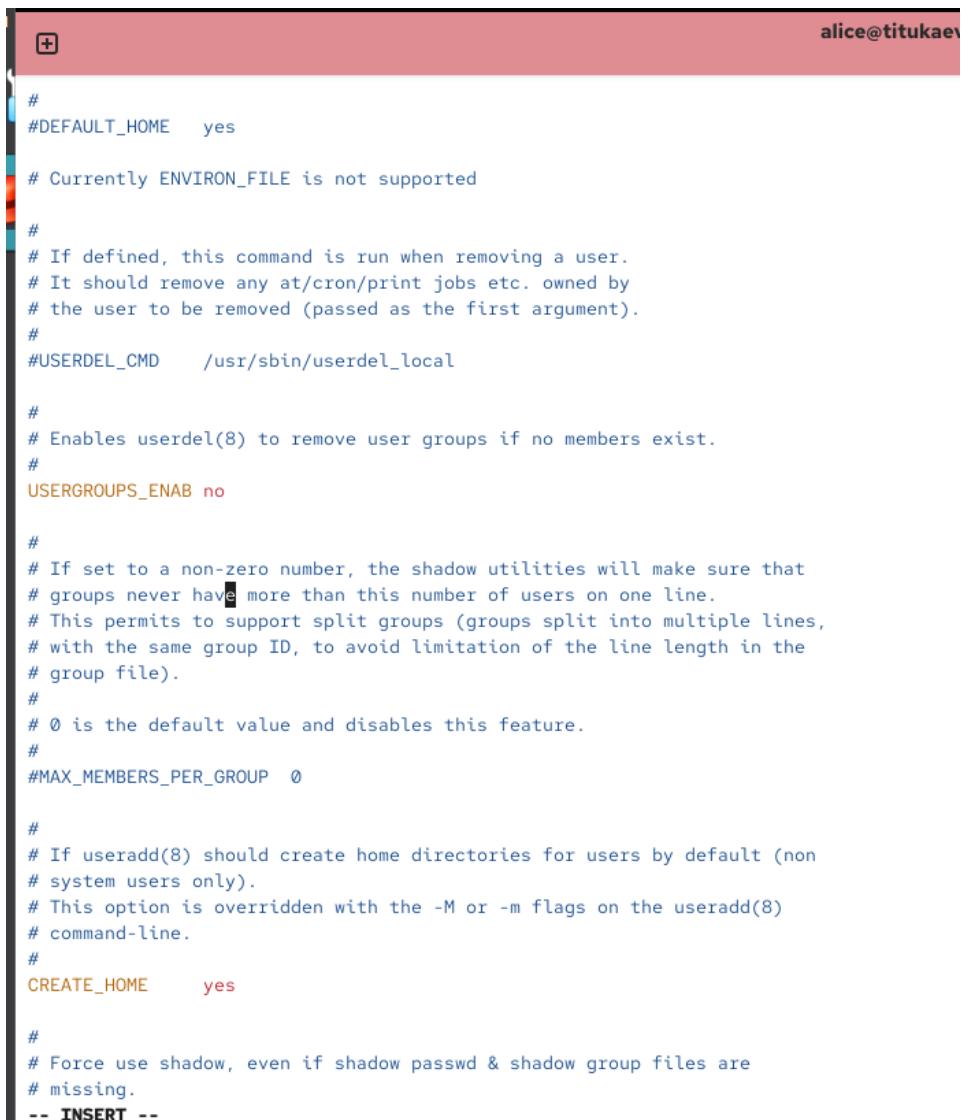
Из вывода видно:

- `uid=1002(bob)` — идентификатор пользователя bob;
- `gid=1002(bob)` — основная группа с тем же именем;
- `groups=1002(bob)` — вторичных групп пока нет.

## 2.4 Настройка общих параметров создания пользователей

11. Выполнено переключение в контекст root командой `su`.
12. Открыт для редактирования файл конфигурации `/etc/login.defs` (редак-

top vim).



```
#  
#DEFAULT_HOME yes  
  
# Currently ENVIRON_FILE is not supported  
  
#  
# If defined, this command is run when removing a user.  
# It should remove any at/cron/print jobs etc. owned by  
# the user to be removed (passed as the first argument).  
#  
#USERDEL_CMD /usr/sbin/userdel_local  
  
#  
# Enables userdel(8) to remove user groups if no members exist.  
#  
USERGROUPS_ENAB no  
  
#  
# If set to a non-zero number, the shadow utilities will make sure that  
# groups never have more than this number of users on one line.  
# This permits to support split groups (groups split into multiple lines,  
# with the same group ID, to avoid limitation of the line length in the  
# group file).  
#  
# 0 is the default value and disables this feature.  
#  
#MAX_MEMBERS_PER_GROUP 0  
  
#  
# If useradd(8) should create home directories for users by default (non  
# system users only).  
# This option is overridden with the -M or -m flags on the useradd(8)  
# command-line.  
#  
CREATE_HOME yes  
  
#  
# Force use shadow, even if shadow passwd & shadow group files are  
# missing.  
-- INSERT --
```

Рис. 2.4: Редактирование файла /etc/login.defs

В файле проверены и изменены следующие параметры:

- **CREATE\_HOME yes** — при создании нового пользователя (`useradd`) автоматически создаётся его домашний каталог.
- **USERGROUPS\_ENAB no** — новые пользователи не получают отдельную однолинейную группу; вместо этого используется общая группа `users`. Это

влияет на то, какая группа будет назначена пользователю по умолчанию.

#### 13. Выполнен переход в каталог /etc/skel.

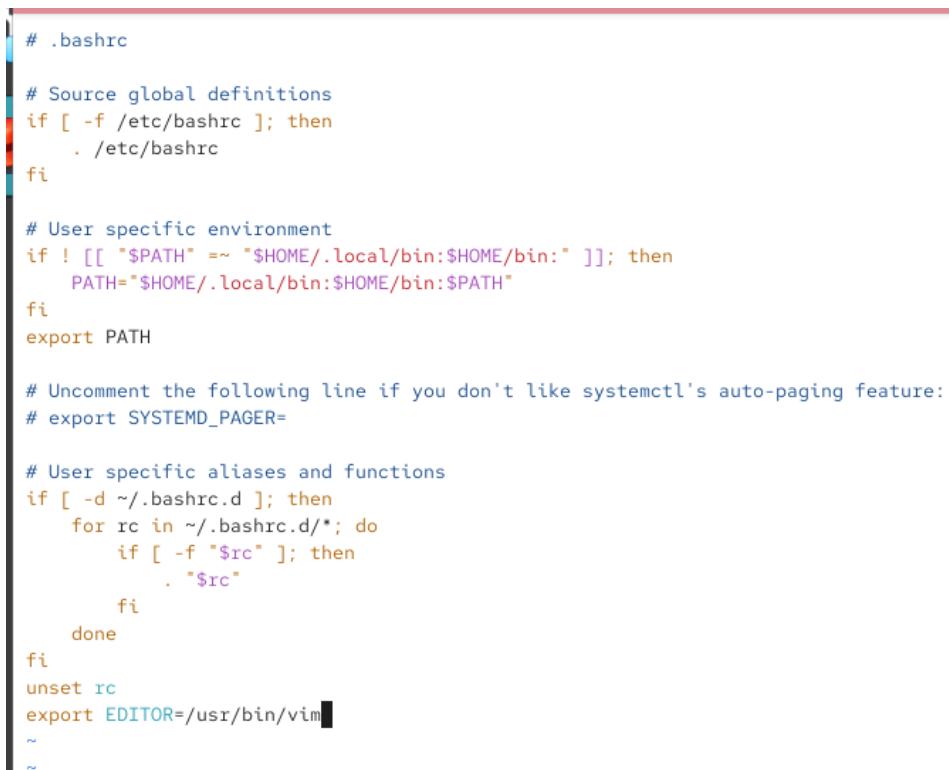
В этом каталоге находятся файлы и папки, которые автоматически копируются в домашний каталог каждого нового пользователя.

Созданы каталоги Pictures и Documents командами `mkdir Pictures` и `mkdir Documents`.

Теперь при создании новой учётной записи эти каталоги будут появляться в домашнем каталоге пользователя по умолчанию.

#### 14. В файле /etc/skel/.bashrc добавлена строка:

```
export EDITOR=/usr/bin/vim
```



```
# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
    . /etc/bashrc
fi

# User specific environment
if ! [[ "$PATH" =~ "$HOME/.local/bin:$HOME/bin:" ]]; then
    PATH="$HOME/.local/bin:$HOME/bin:$PATH"
fi
export PATH

# Uncomment the following line if you don't like systemctl's auto-paging feature:
# export SYSTEMD_PAGER=

# User specific aliases and functions
if [ -d ~/.bashrc.d ]; then
    for rc in ~/.bashrc.d/*; do
        if [ -f "$rc" ]; then
            . "$rc"
        fi
    done
fi
unset rc
export EDITOR=/usr/bin/vim
~
```

Рис. 2.5: Настройка EDITOR и .bashrc

Это означает, что переменная окружения EDITOR будет автоматически за-

даваться для всех новых пользователей. Многие консольные утилиты (например, `crontab`, `visudo` при определённых настройках и др.) используют переменную `EDITOR`, чтобы узнать, какой текстовый редактор запускать для редактирования файлов.

В данном случае по умолчанию будет использоваться редактор `vim`.

## 2.5 Создание и анализ учётной записи carol

15. В терминале выполнено переключение на учётную запись `alice` командой `su alice`.

16. Находясь под пользователем `alice`, с использованием прав `sudo` создан пользователь `carol`:

```
sudo -i useradd carol
```

17. Для пользователя `carol` задан пароль командой `sudo passwd carol`.

18. Далее выполнено переключение на `carol` (команда `su carol`) и просмотр информации о нём:

- команда `id` показала:
  - `uid=1003(carol)` – идентификатор пользователя;
  - `gid=100(users)` – основной группой назначена `users` (как и задавалось параметром `USERGROUPS_ENAB no`);
  - перечислены вторичные группы (на данном этапе только `users`).
- переход в домашний каталог (`cd`) и просмотр его содержимого (`ls -Al`) показали наличие файлов и каталогов:
  - стандартные файлы инициализации: `.bash_logout`, `.bash_profile`, `.bashrc`;
  - каталоги `Documents` и `Pictures`, скопированные из `/etc/skel`.

```

root@titukaev:/etc/skel# su alice
alice@titukaev:/etc/skel$ sudo -i useradd carol
alice@titukaev:/etc/skel$ sudo passwd carol
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
alice@titukaev:/etc/skel$ su carol
Password:
carol@titukaev:/etc/skel$ id
uid=1003(carol) gid=100(users) groups=100(users) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
carol@titukaev:/etc/skel$ cd
carol@titukaev:~$ ls -Al
total 12
-rw-r--r--. 1 carol users 18 Oct 29 2024 .bash_logout
-rw-r--r--. 1 carol users 144 Oct 29 2024 .bash_profile
-rw-r--r--. 1 carol users 549 Dec 9 11:36 .bashrc
drwxr-xr-x. 2 carol users 6 Dec 9 11:35 Documents
drwxr-xr-x. 4 carol users 39 Oct 9 13:36 .mozilla
drwxr-xr-x. 2 carol users 6 Dec 9 11:35 Pictures
carol@titukaev:~$
```

Рис. 2.6: Домашний каталог и информация о carol

## 2.6 Работа с файлом /etc/shadow и параметрами паролей

- Находясь под пользователем `alice`, выполнен просмотр строки пароля пользователя `carol` в файле `/etc/shadow`:

Использована команда вида `sudo cat /etc/shadow | grep carol`.

```

carol@titukaev:~$ 
carol@titukaev:~$ su alice
Password:
alice@titukaev:/home/carol$ sudo cat /etc/shadow | grep carol
carol:$j9TSL4RldJ2uzjpfI02/0u85D0$8veS3dSXow4kcGLQ5Sd.1dFEPLnLICbi5hvPa0zBT.:20431:0:99999:7:::
alice@titukaev:/home/carol$ sudo passwd -n 30 -w 3 -x 90 carol
passwd: password changed.
alice@titukaev:/home/carol$ sudo cat /etc/shadow | grep carol
carol:$j9TSL4RldJ2uzjpfI02/0u85D0$8veS3dSXow4kcGLQ5Sd.1dFEPLnLICbi5hvPa0zBT.:20431:30:90:3:::
alice@titukaev:/home/carol$ sudo grep alice /etc/passwd /etc/shadow /etc/group
/etc/passwd:alice:x:1001:1001::/home/alice:/bin/bash
/etc/shadow:alice:$j9TSL4RldJ2uzjpfI02/0u85D0$8veS3dSXow4kcGLQ5Sd.1dFEPLnLICbi5hvPa0zBT.:20431:30:90:3:::
/etc/group:wheel:x:10:titukaev,alice
/etc/group:alice:x:1001:
alice@titukaev:/home/carol$ sudo grep carol /etc/passwd /etc/shadow /etc/group
/etc/passwd:carol:x:1003:100::/home/carol:/bin/bash
/etc/shadow:carol:$j9TSL4RldJ2uzjpfI02/0u85D0$8veS3dSXow4kcGLQ5Sd.1dFEPLnLICbi5hvPa0zBT.:20431:30:90:3:::
alice@titukaev:/home/carol$
```

Рис. 2.7: Просмотр и изменение записи carol в /etc/shadow

Строка имеет вид (обобщённо):

`carol:xэш_пароля:20431:0:99999:7:::`

Поля строки означают:

- имя учётной записи (carol);
- зашифрованный пароль (хэш);
- число дней от 1 января 1970 года до даты последней смены пароля;
- минимальное число дней до разрешения смены пароля;
- максимальное число дней действия пароля;
- количество дней предупреждения пользователя до истечения срока действия пароля;
- число дней после истечения срока действия до блокировки;
- дата окончательного отключения учётной записи (если задана).

20. Изменены свойства пароля пользователя carol командой вида

```
sudo passwd -n 30 -w 3 -x 90 carol.
```

Параметры означают:

- **-n 30** — минимальный срок использования пароля 30 дней (до истечения этого срока сменить пароль нельзя);
- **-w 3** — за 3 дня до истечения срока действия пароля пользователь начнёт получать предупреждения;
- **-x 90** — максимальный срок действия пароля 90 дней (после этого потребуется смена пароля).

21. Повторный вывод строки пользователя carol из /etc/shadow показал изменение соответствующих полей (минимальный срок, максимальный срок, период предупреждения).

22. Проверено наличие идентификатора alice во всех трёх файлах:

```
grep alice /etc/passwd /etc/shadow /etc/group
```

Пользователь alice присутствует:

- в /etc/passwd — общая информация (uid, gid, shell, домашний каталог);
- в /etc/shadow — данные о пароле;
- в /etc/group — членство в группах.

23. Для carol выполнена команда `sudo grep carol /etc/passwd /etc/shadow /etc/group`.

Пользователь присутствует в `/etc/passwd` и `/etc/shadow`, а в `/etc/group` отображается только в качестве члена групп, где он явно добавлен (по умолчанию – группа `users`). Это демонстрирует разделение информации о пользователе и его пароле (`passwd/shadow`) и о группах (`group`).

## 2.7 Работа с группами

24. Находясь под учётной записью `alice`, были созданы две новые группы:

- `main`
- `third`

Для этого использованы команды `sudo groupadd main` и `sudo groupadd third`.

25. После этого пользователи были добавлены в группы с помощью `usermod`:

- `alice` добавлена в группу `main` (`sudo usermod -aG main alice`);
- `bob` добавлен в группу `main` (`sudo usermod -aG main bob`);
- `carol` добавлена в группу `third` (`sudo usermod -aG third carol`).

26. Командой `id carol` проверено, что пользователь `carol` корректно добавлен в группу `third`:

- основная группа: `gid=100(users)`;
- вторичная группа: `third` (с собственным `gid`).

Таким образом, `users` остаётся основной группой, а `third` – вторичной.

27. Аналогично выполнены команды `id alice` и `id bob` для анализа их членства в группах:

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

Рис. 2.8: Создание групп и проверка их состава

В результате получено:

- **alice:**

- основная группа – **alice**;
- вторичные группы – **wheel**, **main** (и, возможно, другие стандартные группы).

- **bob:**

- основная группа – **bob**;
- вторичная группа – **main**.

- **carol:**

- основная группа – **users**;
- вторичная группа – **third**.

## 3 Контрольные вопросы

1. Информацию о UID пользователя и его принадлежности к группам можно получить с помощью команд `id`, `whoami`, а также просмотром файлов `/etc/passwd` и `/etc/group`.
2. Пользователь `root` имеет UID 0.  
Узнать UID любого пользователя можно командой `id имя_пользователя` или просмотром файла `/etc/passwd`, где UID хранится в третьем поле каждой записи.
3. Команда `su` переключает контекст на другой аккаунт, полностью изменяя пользователя, тогда как `sudo` позволяет выполнять отдельные команды от имени суперпользователя, не покидая текущую учётную запись.  
`su` требует пароль целевой учётной записи, `sudo` — пароль текущего пользователя, имеющего соответствующие права.
4. Параметры работы `sudo` определяются в конфигурационном файле `/etc/sudoers`, а также в дополнительных файлах каталога `/etc/sudoers.d`.
5. Для безопасного изменения конфигурации `sudo` используется команда `visudo`, поскольку она проверяет файл на синтаксические ошибки перед сохранением.
6. Чтобы предоставить пользователю доступ ко всем командам администрирования через `sudo`, его необходимо включить в группу `wheel` (или `sudo` — в зависимости от дистрибутива).

7. Для задания параметров, используемых при создании новых учётных записей, применяются:

- файл конфигурации `/etc/login.defs` (например, параметры `CREATE_HOME`, `USERGROUPS_ENAB`);
- каталог `/etc/skel`, содержащий файлы и настройки, копируемые в домашний каталог нового пользователя (`.bashrc`, каталоги `Documents` и `Pictures`).

8. Информация о первичной и дополнительных группах пользователей хранится в файлах `/etc/passwd` и `/etc/group`.

У пользователя `alice` запись в `/etc/passwd` содержит указание основной группы, а в `/etc/group` отображаются группы, в которых `alice` состоит как член.

9. Для изменения параметров пароля пользователя применяются команды `passwd` (например: минимальный, максимальный срок действия, предупреждения) и `chage`, позволяющие управлять сроками действия пароля более детально.

10. Для прямого изменения информации в файле `/etc/group` следует использовать команду `vigr`.

Она блокирует файл от одновременного редактирования и проверяет корректность структуры, что предотвращает повреждение системной конфигурации.

## **4 Заключение**

В ходе лабораторной работы были изучены механизмы управления учётными записями и группами в операционной системе Linux.

Были рассмотрены способы переключения между пользователями, принципы работы команд `su` и `sudo`, а также правила безопасного редактирования файла конфигурации `/etc/sudoers`.

На практике были созданы новые пользователи и группы, настроены параметры паролей и изучена структура системных файлов `/etc/passwd`, `/etc/shadow` и `/etc/group`.

Особое внимание уделялось настройкам, влияющим на автоматическое создание домашнего каталога и применение шаблонов из `/etc/skel`.