

Отчёт по лабораторной работе №2

Управление пользователями и группами

Анна Саенко

Содержание

1	Цель работы	5
2	Ход выполнения работы	6
2.1	Переключение между пользователями	6
2.2	Создание учётных записей	8
2.3	Работа с группами	11
3	Контрольные вопросы	12
4	Заключение	15

Список иллюстраций

2.1	Определение текущего пользователя и вход под root	6
2.2	Просмотр файла sudoers	7
2.3	Создание пользователей alice и bob	8
2.4	Изменение файла login.defs	9
2.5	Изменение .bashrc в /etc/skel	10
2.6	Создание пользователя carol	10
2.7	Настройка параметров пароля carol	11
2.8	Добавление пользователей в группы и проверка членства	11

Список таблиц

1 Цель работы

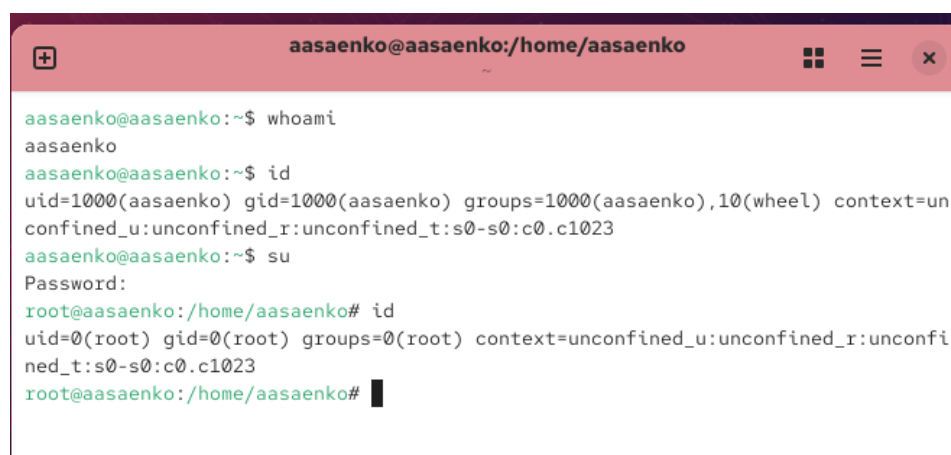
Закрепить навыки администрирования в Linux: научиться создавать и настраивать учётные записи пользователей и групп, управлять правами доступа и политикой паролей, а также работать с основными системными файлами конфигурации.

2 Ход выполнения работы

2.1 Переключение между пользователями

Сначала я проверила, под какой учётной записью выполняется работа, используя команду `whoami`, а затем уточнила информацию о пользователе через команду `id`.

После этого я перешла под суперпользователя `root`, выполнив команду `su`. На скриншоте ниже показаны результаты.

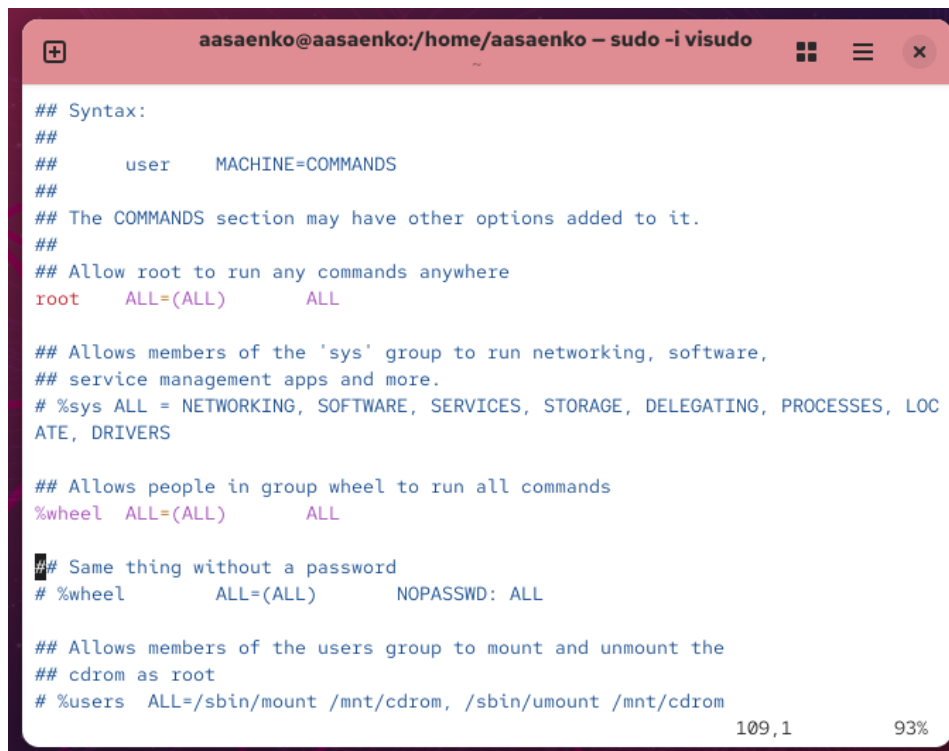


```
aasaenko@aasaenko:~/home/aasaenko
aasaenko@aasaenko:~$ whoami
aasaenko
aasaenko@aasaenko:~$ id
uid=1000(aasaenko) gid=1000(aasaenko) groups=1000(aasaenko),10(wheel) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
aasaenko@aasaenko:~$ su
Password:
root@aasaenko:~/home/aasaenko# id
uid=0(root)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

Рис. 2.1: Определение текущего пользователя и вход под root

Затем я открыла файл `/etc/sudoers` с помощью утилиты `visudo`, чтобы посмотреть настройки доступа.

Содержимое файла видно на скриншоте.



```
## 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, LOC
ATE, 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
```

109,1 93%

Рис. 2.2: Просмотр файла sudoers

После этого я создала пользователя **alice**, добавила её в группу `wheel` и назначила пароль. Проверив вход, убедилась, что всё работает. Аналогично я завела пользователя **bob** и тоже задала ему пароль. Проверку можно увидеть на скриншоте.

```

root@aasaenko:/home/aasaenko# sudo -i useradd -G wheel alice
root@aasaenko:/home/aasaenko# sudo -i passwd alice
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
root@aasaenko:/home/aasaenko# su alice
alice@aasaenko:/home/aasaenko$ 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.

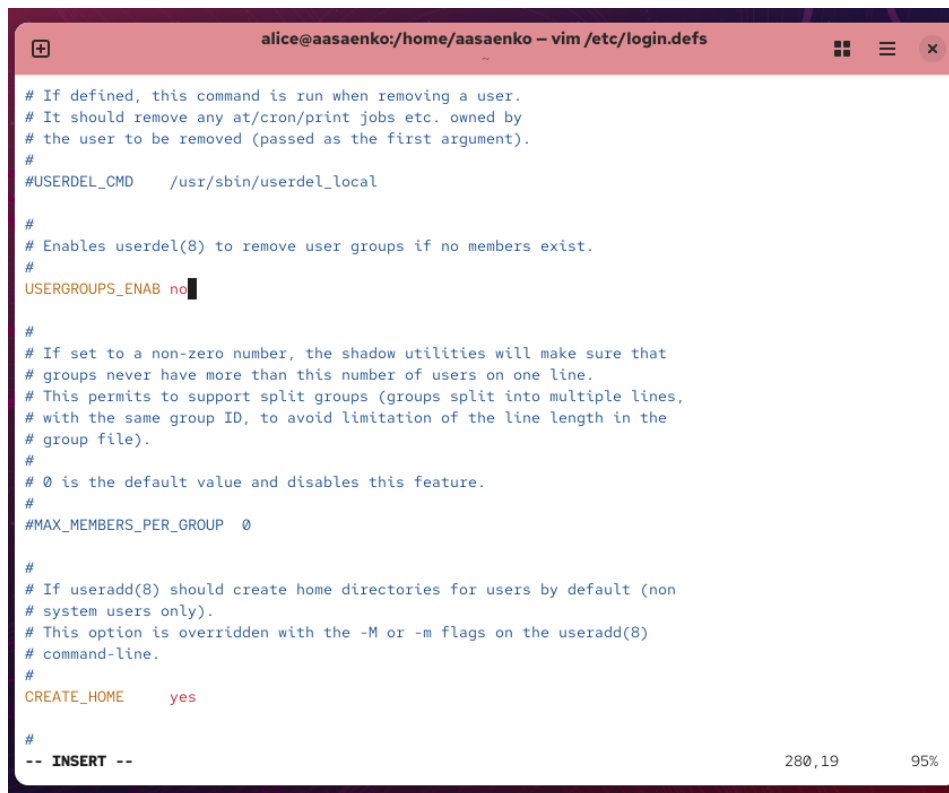
[sudo] password for alice:
alice@aasaenko:/home/aasaenko$ sudo passwd bob
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
alice@aasaenko:/home/aasaenko$ id bob
uid=1002(bob) gid=1002(bob) groups=1002(bob)
alice@aasaenko:/home/aasaenko$ id alice
uid=1001(alice) gid=1001(alice) groups=1001(alice),10(wheel)
alice@aasaenko:/home/aasaenko$

```

Рис. 2.3: Создание пользователей alice и bob

2.2 Создание учётных записей

Чтобы при добавлении новых пользователей автоматически создавались домашние каталоги, я изменила параметры в файле `/etc/login.defs`: включила `CREATE_HOME yes` и отключила `USERGROUPS_ENAB no`.



```
alice@aasaenko:/home/aasaenko - vim /etc/login.defs

# 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

#
-- INSERT --                                     280,19      95%
```

Рис. 2.4: Изменение файла login.defs

Кроме того, я изменила содержимое каталога `/etc/skel`: добавила стандартные директории и отредактировала файл `.bashrc`, где указала редактор по умолчанию.



```
alice@aasaenko:/etc/skel - vim .bashrc
# .bashrc

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

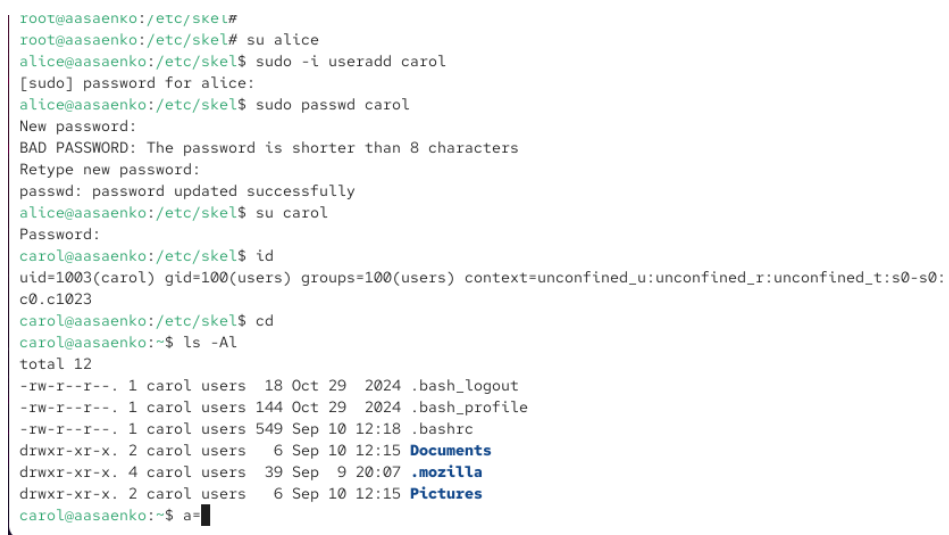
# User specific environment
if ! [[ "$PATH" =~ "$HOME/.local/bin:$HOME/bin:" ]]; then
    PATH="$HOME/.local/bin:$HOME/bin:$PATH"
fi
export PATH

# 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/vi
```

Рис. 2.5: Изменение .bashrc в /etc/skel

Далее я создала пользователя **carol**, задала ей пароль и настроила параметры действия пароля: минимальный срок — 30 дней, максимальный — 90 дней, предупреждение за 3 дня до истечения.



```
root@aasaenko:/etc/skel#
root@aasaenko:/etc/skel# su alice
alice@aasaenko:/etc/skel$ sudo -i useradd carol
[sudo] password for alice:
alice@aasaenko:/etc/skel$ sudo passwd carol
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
alice@aasaenko:/etc/skel$ su carol
Password:
carol@aasaenko:/etc/skel$ id
uid=1003(carol) gid=100(users) groups=100(users) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
carol@aasaenko:/etc/skel$ cd
carol@aasaenko:~$ 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 Sep 10 12:18 .bashrc
drwxr-xr-x. 2 carol users 6 Sep 10 12:15 Documents
drwxr-xr-x. 4 carol users 39 Sep 9 20:07 .mozilla
drwxr-xr-x. 2 carol users 6 Sep 10 12:15 Pictures
carol@aasaenko:~$ a=
```

Рис. 2.6: Создание пользователя carol

```

carol@aasaenko:~$ su alice
Password:
alice@aasaenko:/home/carol$ sudo cat /etc/shadow | grep carol
carol:$y$j9T$KjPjPtdy3SLQN8E7PvGDW.$pDM94vE/SrDVWt6a2VjyoQQ25Z7afE/AmjTPXyV/CP6:20341:0:99999:7:::
alice@aasaenko:/home/carol$ sudo passwd -n 30 -w 3 -x 90 carol
passwd: password changed.
alice@aasaenko:/home/carol$ sudo cat /etc/shadow | grep carol
carol:$y$j9T$KjPjPtdy3SLQN8E7PvGDW.$pDM94vE/SrDVWt6a2VjyoQQ25Z7afE/AmjTPXyV/CP6:20341:30:90:3:::
alice@aasaenko:/home/carol$ sudo grep alice /etc/passwd /etc/shadow /etc/group
/etc/passwd:alice:x:1001:1001::/home/alice:/bin/bash
/etc/shadow:alice:$y$j9T$EKVkmFXn0UQFBUQNBmb10$6UaJEB6qudo3iQGhn/vQ0jbJDLWQH1M87dynpd4Q.87:20341:0:99
999:7:::
/etc/group:wheel:x:10:aasaenko,alice
/etc/group:alice:x:1001:
alice@aasaenko:/home/carol$ sudo grep carol /etc/passwd /etc/shadow /etc/group
/etc/passwd:carol:x:1003:100::/home/carol:/bin/bash
/etc/shadow:carol:$y$j9T$KjPjPtdy3SLQN8E7PvGDW.$pDM94vE/SrDVWt6a2VjyoQQ25Z7afE/AmjTPXyV/CP6:20341:30:9
0:3:::
alice@aasaenko:/home/carol$ █

```

Рис. 2.7: Настройка параметров пароля carol

2.3 Работа с группами

Я создала группы `main` и `third`, после чего добавила `alice` и `bob` в группу `main`, а `carol` — в группу `third`. Затем проверила принадлежность пользователей к группам через команду `id`.

```

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

```

Рис. 2.8: Добавление пользователей в группы и проверка членства

3 Контрольные вопросы

1. Как определить UID и группы пользователя?

Для этого можно использовать несколько команд:

- `id` — выводит UID, GID и список всех групп пользователя;
- `id -u` — показывает только UID;
- `id -G` — отображает идентификаторы групп;
- `groups` — выводит названия групп, в которых состоит пользователь.

2. Какой UID у пользователя root?

У суперпользователя `root` всегда UID равен 0. Проверить это можно командой `id root`.

3. В чём различие между `su` и `sudo`?

- `su` (substitute user) полностью переключает с текущего пользователя на другого, чаще всего на `root`, и открывает его окружение.
- `sudo` (superuser do) выполняет отдельные команды от имени администратора или другого пользователя, при этом оставаясь в текущей сессии.

4. Где задаются параметры работы `sudo`?

Настройки определяются в конфигурационном файле `/etc/sudoers`.

5. Как безопасно редактировать файл `sudoers`?

Для этого применяется команда `visudo`. Она блокирует одновременное редактирование файла и проверяет синтаксис перед сохранением.

6. Какая группа предоставляет полный доступ через `sudo`?

В большинстве дистрибутивов Linux это группа `wheel` (в Debian/Ubuntu часто используется группа `sudo`).

7. Какие файлы отвечают за параметры новых пользователей?

- `/etc/login.defs` — глобальные параметры (создание домашнего каталога, политика паролей и т.д.);
- `/etc/default/useradd` — настройки по умолчанию для команды `useradd`;
- `/etc/skel/` — шаблон содержимого домашнего каталога для новых пользователей.

8. Где хранится информация о пользователях и группах?

- `/etc/passwd` — содержит сведения о пользователях и их основных группах;
- `/etc/shadow` — хранит зашифрованные пароли и параметры их действия;
- `/etc/group` — описывает дополнительные группы и список участников.

9. Какие команды позволяют управлять сроком действия паролей?

- `passwd` — изменение пароля пользователя;

- `chage` — настройка срока действия пароля (минимальный, максимальный срок, дата истечения, предупреждение о смене).

10. Можно ли вручную редактировать файл `/etc/group`?

Напрямую вносить изменения в `/etc/group` не рекомендуется, так как это может привести к ошибкам. Корректнее использовать утилиты:

- `groupadd` — добавление новой группы;
- `groupdel` — удаление группы;
- `usermod` — изменение членства пользователей в группах.

4 Заключение

В ходе выполнения лабораторной работы я научилась администрировать учётные записи пользователей и управлять группами в Linux.

Были выполнены следующие действия:

- определение текущего пользователя и вход под root;
- создание новых пользователей и настройка паролей;
- изменение системных параметров для автоматического формирования домашнего каталога;
- редактирование шаблонных файлов в `/etc/skel`;
- настройка политики паролей с помощью `chage`;
- создание групп и распределение пользователей между ними.

В процессе работы я закрепила знания о назначении файлов `/etc/passwd`, `/etc/shadow`, `/etc/group` и `/etc/sudoers`. Полученный опыт показал, как с помощью командной строки можно управлять многопользовательской системой, обеспечивать контроль доступа и повышать её безопасность.