

Лабораторная работа №2

Управление пользователями и группами

Юсупова Ксения Равиловна

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Ответы на контрольные вопросы	15
5	Выводы	18

Список иллюстраций

3.1	Выполнили пункты 1-4 из раздела 2.4.1 (Переключение учётных записей пользователей)	8
3.2	Выполнили пункты 5 и 6 из раздела 2.4.1 (Переключение учётных записей пользователей)	9
3.3	Выполнили пункты 7-10 из раздела 2.4.1 (Переключение учётных записей пользователей)	9
3.4	Выполнили пункты 11-13 из раздела 2.4.1 (Переключение учётных записей пользователей)	10
3.5	Выполнили пункты 1 и 2 из раздела 2.4.2 (Создание учётных записей пользователей)	10
3.6	Выполнили пункт 2 из раздела 2.4.2 (Создание учётных записей пользователей)	11
3.7	Выполнили пункт 3 и 4 из раздела 2.4.2 (Создание учётных записей пользователей)	12
3.8	Выполнили пункт 5-8 из раздела 2.4.2 (Создание учётных записей пользователей)	13
3.9	Выполнили пункт 10-14 из раздела 2.4.2 (Создание учётных записей пользователей)	14
3.10	была выполнена работа с группами	14

Список таблиц

1 Цель работы

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

2 Задание

1. Прочитайте справочное описание man по командам ls, whoami, id, groups, su, sudo, passwd, vi, visudo, useradd, usermod, userdel, groupadd, groupdel.
2. Выполните действия по переключению между учётными записями пользователей, поуправлению учётными записями пользователей (раздел 2.4.1).
3. Выполните действия по созданию пользователей и управлению их учётными записями(раздел 2.4.2).
4. Выполните действия по работе с группами пользователей (раздел 2.4.3).

3 Выполнение лабораторной работы

Сначала вошли в систему как обычный пользователь и открыли терминал. Затем определили, какую учётную запись пользователя мы используем, введя команду `whoami`. Позже вывели на экран более подробную информацию, используя команду `id`. Пояснения по отображённой информации:

`uid=1000 (ksyusha):` вы работаете под обычным пользователем с ID 1000

`gid=1000 (ksyusha):` основная группа пользователя — ksyusha (ID 1000)

`группы=1000(ksyusha),10(wheel):` пользователь состоит в своей группе и в привилегированной группе wheel (дает право на повышение прав)

`контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023:` политика SELinux применяется в неограниченном режиме

Далее использовали команду `su` для переключения к учётной записи `root`. При запросе пароля ввели пароль пользователя `root`. Набрали `id`; пояснения по отображённой информации:

`uid=0(root):` вы стали суперпользователем (root) с ID 0.

`gid=0(root):` основная группа — root (ID 0).

`группы=0(root):` пользователь root состоит только в группе root.

`контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023:` контекст SELinux остался без изменений (неограниченный)

Затем мы вернулись к учётной записи своего пользователя. (рис. 3.1).

```

[ksyusha@yu ~]$ whoami
ksyusha
[ksyusha@yu ~]$ id
uid=1000(ksyusha) gid=1000(ksyusha) группы=1000(ksyusha),10(wheel) контекст
=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[ksyusha@yu ~]$ su
Пароль:
[root@yu ksyusha]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:u
nconfined_t:s0-s0:c0.c1023
[root@yu ksyusha]# su ksyusha
[ksyusha@yu ~]$

```

Рис. 3.1: Выполнили пункты 1-4 из раздела 2.4.1 (Переключение учётных записей пользователей)

Просмотрели в безопасном режиме файл `/etc/sudoers`, используя, `sudo -i visudo`. `visudo` используется вместо любого редактора, потому что он проверяет синтаксис перед сохранением. Ошибка в `/etc/sudoers`, допущенная в обычном редакторе, полностью отключает `sudo`, исправить её будет невозможно без доступа `root` другими способами. Например `sudo EDITOR=mcedit visudo` — меняет редактор, но сохраняет проверку синтаксиса.

Убедились, что в открытом с помощью `visudo` файле присутствует строка `%wheel ALL=(ALL) ALL`

Строка `wheel`— ключевой механизм делегирования прав администратора в системе. Пользователь, добавленный в группу `wheel`, может получить полный контроль над системой через `sudo`, что безопаснее, чем работа напрямую из-под `root`.(рис. 3.2).


```
ksyusha@yu:~ — sudo -i visudo
# commands via sudo.
#
# Defaults    env_keep += "HOME"

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
```

Рис. 3.2: Выполнили пункты 5 и 6 из раздела 2.4.1 (Переключение учётных записей пользователей)

Создали пользователя alice, входящего в группу wheel: `sudo -i useradd -G wheel alice`

Убедились, что пользователь alice добавлен в группу wheel, введя `id alice`

Задали пароль для пользователя alice, набрав `sudo -i passwd alice`. Позже переключились на учётную запись пользователя alice: `su alice`(рис. 3.3).

```
[ksyusha@yu ~]$ sudo -i useradd -G wheel alice
[ksyusha@yu ~]$ id alice
uid=1001(alice) gid=1001(alice) группы=1001(alice),10(wheel)
[ksyusha@yu ~]$ sudo -i passwd alice
Изменение пароля пользователя alice.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
Извините, но пароли не совпадают.
passwd: Ошибка при операциях с маркером проверки подлинности
[ksyusha@yu ~]$ sudo -i passwd alice
Изменение пароля пользователя alice.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[ksyusha@yu ~]$ su alice
Пароль:
```

Рис. 3.3: Выполнили пункты 7-10 из раздела 2.4.1 (Переключение учётных записей пользователей)

Создали пользователя bob: `sudo useradd bob`. Затем ввели пароль при запросе. Проверили, что пользователь bob создан. Установили пароль для пользователя bob: `sudo passwd bob`. Просмотрели, в какие группы входит пользователь bob: `id bob` (рис. 3.4).

```
[alice@yu ksyusha]$ sudo useradd bob
Мы полагаем, что ваш системный администратор изложил вам основы
безопасности. Как правило, всё сводится к трём следующим правилам:

№1) Уважайте частную жизнь других.
№2) Думайте, прежде что-то вводить.
№3) С большой властью приходит большая ответственность.

[sudo] пароль для alice:
[alice@yu ksyusha]$ sudo useradd bob
useradd: пользователь «bob» уже существует
[alice@yu ksyusha]$ sudo passwd bob
Изменение пароля пользователя bob.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[alice@yu ksyusha]$ id bob
uid=1002(bob) gid=1002(bob) группы=1002(bob)
```

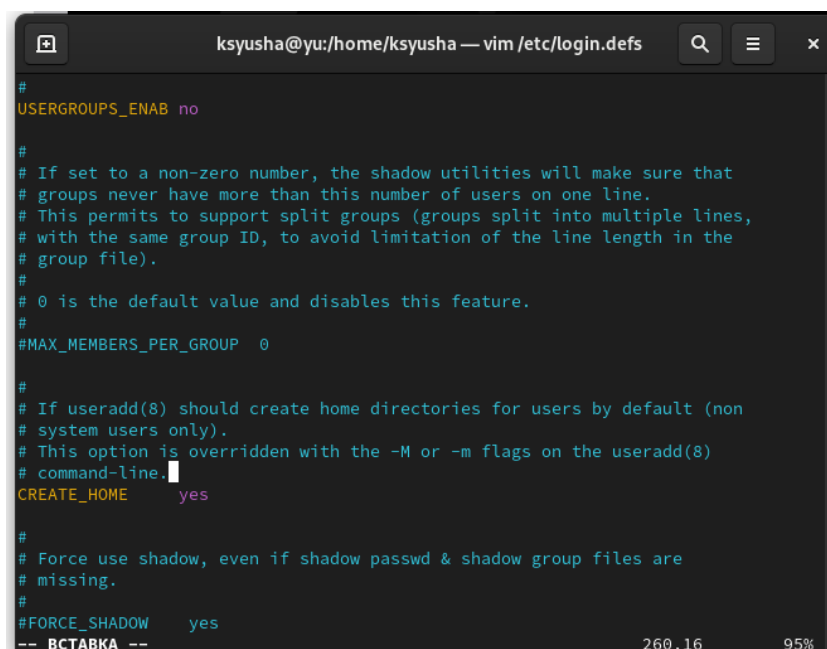
Рис. 3.4: Выполнили пункты 11-13 из раздела 2.4.1 (Переключение учётных записей пользователей)

Переключились в терминале на учётную запись пользователя root: `su` и открыли файл конфигурации `/etc/login.defs` (рис. 3.5).

```
[alice@yu ksyusha]$ su
Пароль:
[root@yu ksyusha]#
[root@yu ksyusha]# vim /etc/login.defs
```

Рис. 3.5: Выполнили пункты 1 и 2 из раздела 2.4.2 (Создание учётных записей пользователей)

Открыли файл конфигурации `/etc/login.defs` для редактирования: `vim /etc/login.defs`. Изменили несколько параметров. Например, нашли параметр `CREATE_HOME` и убедились, что он установлен в значение `yes`. Также установили параметр `USERGROUPS_ENAB` но Это позволит не добавлять нового пользователя в группу с тем же именем, что и пользователь, а использовать группу `users` (рис. 3.6).



```
#
USERGROUPS_ENAB no

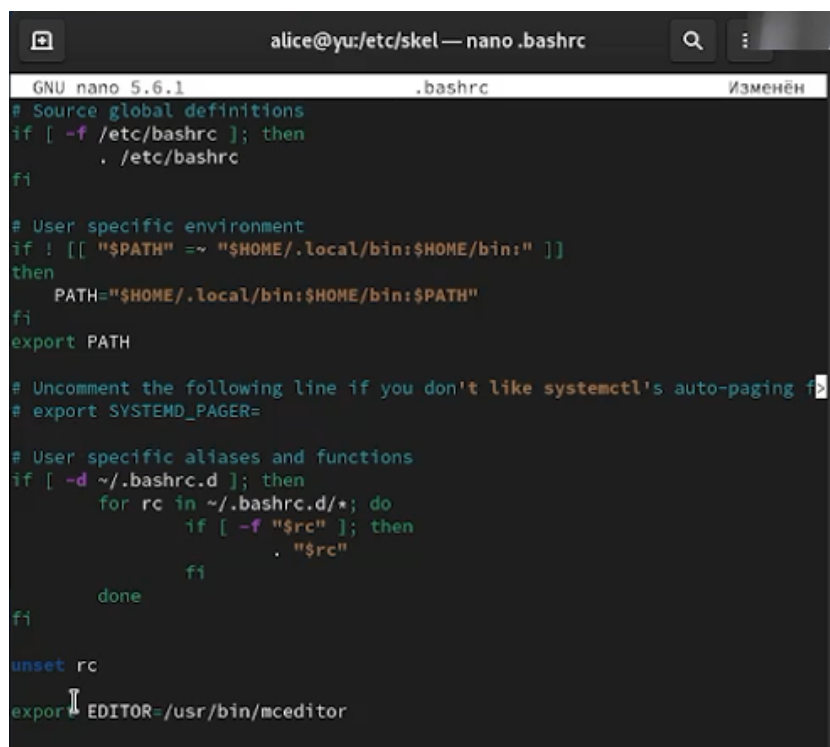
#
# If set to a non-zero number, the shadow utilities will make sure that
# groups never have more than this number of users on one line.
# This permits to support split groups (groups split into multiple lines,
# with the same group ID, to avoid limitation of the line length in the
# group file).
#
# 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.
#
#FORCE_SHADOW yes
-- ВСТАВКА --
```

Рис. 3.6: Выполнили пункт 2 из раздела 2.4.2 (Создание учётных записей пользователей)

Перешли в каталог `/etc/skel`: `cd /etc/skel`. Создали каталоги `Pictures` и `Documents`. Затем изменили содержимое файла `.bashrc`, добавив строку `export EDITOR=/usr/bin/mceditor` Эта запись означает, что редактор `mceditor` будет установлен по умолчанию для инструментов, которые нуждаются в изменении текстовых файлов (рис. 3.7).



```
alice@yu:/etc/skel — nano .bashrc
GNU nano 5.6.1 .bashrc Изменён
# 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
# 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/mceditor
```

Рис. 3.7: Выполнили пункт 3 и 4 из раздела 2.4.2 (Создание учётных записей пользователей)

Переключились в терминале на учётную запись пользователя alice. Используя утилиту useradd, создали пользователя carol. Установили пароль для пользователя carol.

Пользователь carol имеет базовые права для работы в своей домашней директории и с файлами, к которым у группы users есть доступ. Она не может повышать свои привилегии до root. Её основная группа — users (gid=100);

также убедились, что каталоги Pictures и Documents были созданы в домашнем каталоге пользователя carol(рис. 3.8).

```

[root@yu skel]# su alice
[alice@yu skel]$ sudo -i useradd carol
[sudo] пароль для alice:
[alice@yu skel]$ sudo passwd carol
Изменение пароля пользователя carol.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[alice@yu skel]$ su carol
Пароль:
[carol@yu skel]$ id
uid=1003(carol) gid=100(users) группы=100(users) контекст=unconfined_u:unco
nfinied_r:unconfined_t:s0-s0:c0.c1023
[carol@yu skel]$ cd
[carol@yu ~]$ ls -Al
итого 12
-rw-r--r--. 1 carol users 18 апр 30 2024 .bash_logout
-rw-r--r--. 1 carol users 141 апр 30 2024 .bash_profile
-rw-r--r--. 1 carol users 525 сен 12 16:14 .bashrc
drwxr-xr-x. 2 carol users 6 сен 12 16:08 Documents
drwxr-xr-x. 4 carol users 39 сен 5 22:42 .mozilla
drwxr-xr-x. 2 carol users 6 сен 12 16:07 Pictures

```

Рис. 3.8: Выполнили пункт 5-8 из раздела 2.4.2 (Создание учётных записей пользователей)

Переключились в терминале на учётную запись пользователя alice

Пароль пользователя carol надёжно защищен современным алгоритмом хеширования SHA-512 с использованием 100000 раундов шифрования. Политика паролей для этой учетной записи настроена так: пароль можно менять когда угодно, его срок действия практически не ограничен, но система будет напоминать о смене за 7 дней, если срок все же истечет. Позже изменили свойства пароля пользователя carol следующим образом: `sudo passwd -n 30 -w 3 -x 90 carol`. В этой записи срок действия пароля истекает через 90 дней (-x 90). За три дня до истечения срока действия пользователь получит предупреждение (-w 3). Убедились в изменении в строке с данными о пароле пользователя carol в файле `/etc/shadow`. Убедились, что идентификатор alice существует во всех трёх файлах, и что идентификатор carol существует не во всех трёх файлах (рис. 3.9).

```

[carol@yu ~]$ su alice
Пароль:
[alice@yu carol]$ sudo cat /etc/shadow | grep carol
carol:$6$rounds=100000$41G0VFkAdH6ub81e$SH3gbcPDqB5cAr/FK8c3oX/4bq3vNcM6oWm
v.57k/.1SAHMaR5PaIPvkaUH0oFIsyKvCF9hJfFBbUxmFe1xX0:20343:0:99999:7:::
[alice@yu carol]$ sudo passwd -n 30 -w 3 -x 90 carol
Устанавливаются параметры истечения срока действия для пользователя carol.
passwd: Успешно
[alice@yu carol]$ sudo cat /etc/shadow | grep carol
carol:$6$rounds=100000$41G0VFkAdH6ub81e$SH3gbcPDqB5cAr/FK8c3oX/4bq3vNcM6oWm
v.57k/.1SAHMaR5PaIPvkaUH0oFIsyKvCF9hJfFBbUxmFe1xX0:20343:30:90:3:::
[alice@yu carol]$ grep alice /etc/passwd /etc/shadow /etc/group
/etc/passwd:alice:x:1001:1001::/home/alice:/bin/bash
grep: /etc/shadow: Отказано в доступе
/etc/group:wheel:x:10:ksyusha,alice
/etc/group:alice:x:1001:
[alice@yu 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$41G0VFkAdH6ub81e$SH3gbcPDqB5cAr/FK8c3oX/
4bq3vNcM6oWm.v.57k/.1SAHMaR5PaIPvkaUH0oFIsyKvCF9hJfFBbUxmFe1xX0:20343:30:90
:3:::

```

Рис. 3.9: Выполнили пункт 10-14 из раздела 2.4.2 (Создание учётных записей пользователей)

Находясь под учётной записью пользователя alice, создали группы main и third. Далее использовали usermod для добавления пользователей alice и bob в группу main, а carol, dan, dave и david — в группу third. Убедились, что пользователь carol правильно добавлен в группу third. Пользователю carol была назначена основная группа с идентификатором gid = 100 (users), а также он входит во вторичную группу third (GID=1004). Пользователь bob имеет основную группу bob (GID=1002) и входит во вторичную группу main (GID=1003). Пользователь alice, чья основная группа — alice (GID=1001), является участником двух вторичных групп: wheel (GID=10) и main (GID=1003). Таким образом, среди анализируемых пользователей только alice обладает административными полномочиями.([рис.@fig:010]).

```

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

```

Рис. 3.10: была выполнена работа с группами

4 Ответы на контрольные вопросы

1. Команды для получения информации о пользователе и группах:

- `id` - показывает UID, GID и список групп текущего пользователя
- `id <username>` - показывает информацию для указанного пользователя
- `groups <username>` - отображает группы пользователя
- `cat /etc/passwd | grep <username>` - показывает запись пользователя
- `cat /etc/group | grep <username>` - показывает группы пользователя

2. UID пользователя root:

Пользователь root имеет UID=0. Узнать можно командами:

- `id root` → `uid=0(root)`
- `cat /etc/passwd | grep root` → `root:x:0:0:root:/root:/bin/bash`

3. Различие между su и sudo:

- `su` - переключение на другого пользователя (требуется пароль целевого пользователя)
- `sudo` - выполнение команды с правами другого пользователя (обычно root) с проверкой прав через `/etc/sudoers`

4. Конфигурационный файл sudo:

Параметры sudo определяются в файле /etc/sudoers

5. Безопасное изменение конфигурации sudo:

Команда visudo - открывает /etc/sudoers с проверкой синтаксиса перед сохранением

6. Группа для полного администрирования:

Пользователь должен быть членом группы wheel (в RHEL/CentOS) или sudo (в Debian/Ubuntu)

7. Файлы параметров создания учётных записей:

- /etc/login.defs - настройки паролей, UID/GID диапазоны
- /etc/default/useradd - параметры по умолчанию
- /etc/skel/ - шаблоны файлов для домашних каталогов

8. Хранение информации о группах:

Информация хранится в:

- /etc/passwd - первичная группа (4 поле)
- /etc/group - дополнительные группы

Пример для alice:

alice:x:1001:1001:Alice:/home/alice:/bin/bash - первичная группа 1001 (alice)

В /etc/group: wheel:x:10:alice и main:x:1003:alice - дополнительные группы

9. Команды для изменения информации о пароле:

- chage - изменение параметров старения пароля
- passwd - изменение пароля
- usermod - изменение параметров пользователя

10. Команда для изменения `/etc/group`:

Прямое редактирование не рекомендуется. Следует использовать:

- `groupadd`, `groupmod`, `groupdel` - для безопасного управления группами
- `usermod -G` - для изменения членства в группах

Причина: системные утилиты обеспечивают корректность формата файла и предотвращают ошибки синтаксиса.

5 Выводы

В ходе лабораторной работы мы получили представление о работе с учётными записями пользователей и группами пользователей в операционной системе типа Linux.