

Лабораторная работа № 2

Управление пользователями и группами

Жукова София Викторовна

Содержание

1 Цель работы	5
2 Выполнение лабораторной работы	6
2.0.1 1. Команды для получения информации о пользователе и группах	17
2.0.2 2. UID пользователя root и команда для его получения	17
2.0.3 3. Различие между командами su и sudo	17
2.0.4 4. Конфигурационный файл для sudo	18
2.0.5 5. Команда для безопасного изменения конфигурации sudo	18
2.0.6 6. Группа для администрирования через sudo	18
2.0.7 7. Файлы для настроек учетных записей	18
2.0.8 8. Хранение информации о группах пользователей	19
2.0.9 9. Команды для изменения информации о пароле	19
2.0.10 10. Команда для изменения информации в файле /etc/group	19
3 Выводы	21

Список иллюстраций

2.1 whoami	6
2.2 id	6
2.3 Переключение к учётной записи root	6
2.4 sudo -i visudo	7
2.5 Открывшийся файл	7
2.6 Стока присутствует	8
2.7 Закрываем	8
2.8 Создаем и убеждаемся	9
2.9 alice	9
2.10 Создадим	9
2.11 Пароль	9
2.12 Группы	10
2.13 root	10
2.14 Откроем файл конфигурации	10
2.15 Все верно	11
2.16 no	11
2.17 Создадим	12
2.18 Откроем	12
2.19 Изменим	12
2.20 Carol	13
2.21 Установим пароль	13
2.22 Посмотрим информацию о пользователе carol	13
2.23 Убедимся	14
2.24 alice	14
2.25 Стока записи о пароле	14
2.26 Изменим свойства пароля	14
2.27 /etc/shadow	15
2.28 Существует	15
2.29 Создадим	15
2.30 usermod	16
2.31 Убедимся	16
2.32 bob	16
2.33 alice	16

Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

Войдем в систему как обычный пользователь и откроем терминал. Определим, какую учётную запись пользователя мы используем, введя команду (рис. 2.1).

```
svzhukova@svzhukova:~$ whoami  
svzhukova
```

Рис. 2.1: whoami

Выведем на экран более подробную информацию, используя команду (рис. 2.2).

```
svzhukova@svzhukova:~$ id  
uid=1000(svzhukova) gid=1000(svzhukova) группы=1000(svzhukova),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 2.2: id

(UID – id пользователя равный 1000, GID – id группы равный 1000)

Используем команду su для переключения к учётной записи root. При запросе пароля введем пароль пользователя root (рис. 2.3).

```
svzhukova@svzhukova:~$ su  
Пароль:  
root@svzhukova:/home/svzhukova# id  
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
root@svzhukova:/home/svzhukova#  
exit
```

Рис. 2.3: Переключение к учётной записи root

(UID – id пользователя равный 0. GID – id группы равный 0)

Просмотрим в безопасном режиме файл /etc/sudoers, используя, например (рис. 2.4).

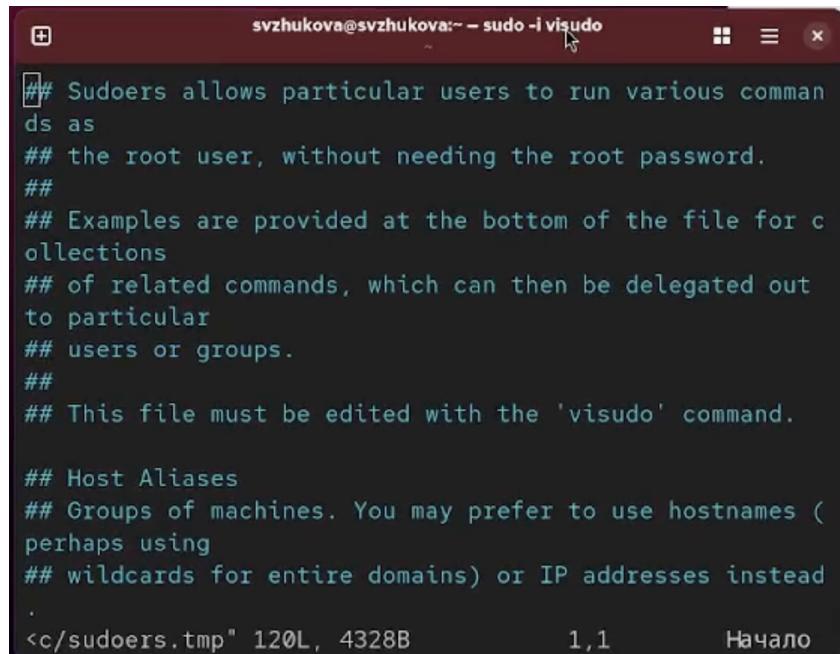


```
svzhukova@svzhukova:~$ sudo -i visudo
```

Рис. 2.4: sudo -i visudo

Использование visudo обеспечивает безопасность, надежность и правильность во время редактирования критически важного файла конфигурации, что минимизирует риск ошибок, которые могут негативно сказаться на управлении доступом в системе.

Файл (рис. 2.5).



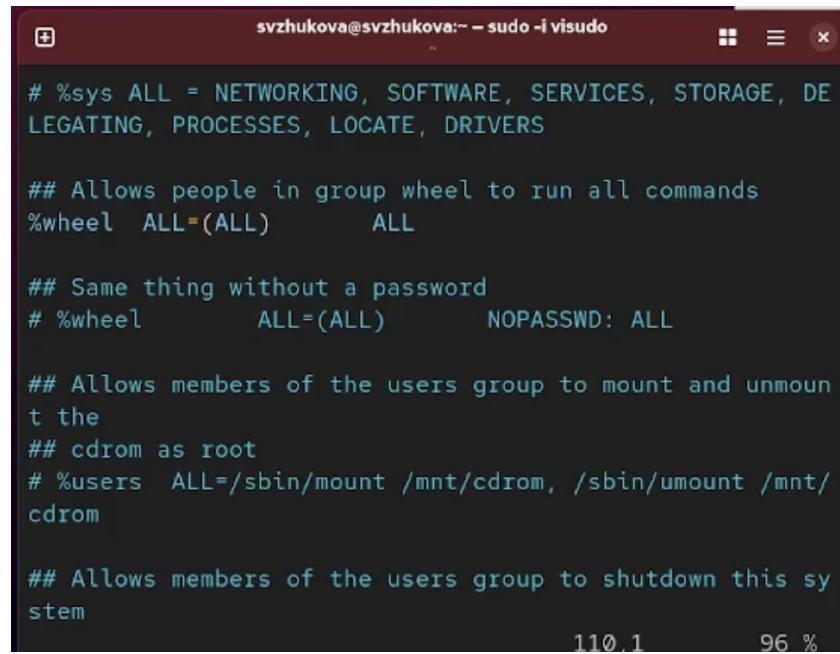
```
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
##
## Examples are provided at the bottom of the file for collections
## of related commands, which can then be delegated out to particular
## users or groups.
##
## This file must be 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

<c/sudoers.tmp" 120L, 4328B          1,1      Начало
```

Рис. 2.5: Открывшийся файл

Убедимся, что в открытом с помощью visudo файле присутствует строка %wheel ALL=(ALL) ALL (рис. 2.6).

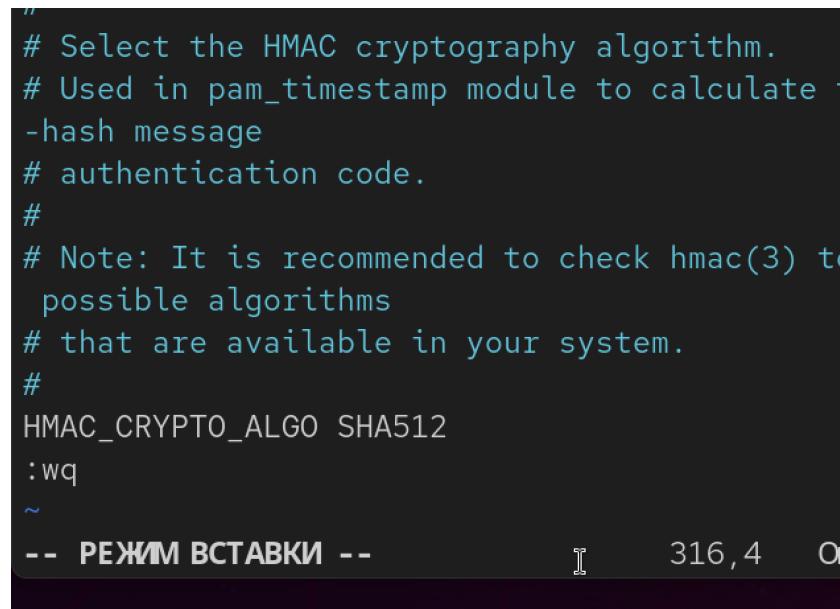


```
svzhukova@svzhukova:~ - sudo -i visudo
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS
## Allows people in group wheel to run all commands
%wheel    ALL=(ALL)        ALL
## Same thing without a password
# %wheel        ALL=(ALL)        NOPASSWD: ALL
## Allows members of the users group to mount and umount the
## cdrom as root
# %users    ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/
cdrom
## Allows members of the users group to shutdown this system
```

Рис. 2.6: Стока присутствует

Запись %wheel ALL=(ALL) ALL предоставляет членам группы wheel возможность использовать команды с повышенными привилегиями

Закрываем файл нажимая esc и вводя :wq (рис. 2.7).



```
"# Select the HMAC cryptography algorithm.
# Used in pam_timestamp module to calculate the
-hash message
# authentication code.
#
# Note: It is recommended to check hmac(3) to
#       see what possible algorithms
#       that are available in your system.
#
HMAC_CRYPTO_ALGO SHA512
:wq
~
-- РЕЖИМ ВСТАВКИ --
```

Рис. 2.7: Закрываем

Создадим пользователя alice, входящего в группу wheel и убедимся, что пользователь alice добавлен в группу wheel (рис. 2.8).

```
svzhukova@svzhukova:~$ sudo -i passwd alice
svzhukova@svzhukova:~$ id alice
uid=1001(alice) gid=1001(alice) группы=1001(alice),10
(wheel)
```

Рис. 2.8: Создаем и убеждаемся

Зададим пароль для пользователя alice, Переключимся на учётную запись пользователя alice (рис. 2.9).

```
svzhukova@svzhukova:~$ sudo -i passwd alice
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - слишком простой
Повторите ввод нового пароля:
passwd: пароль успешно обновлён
svzhukova@svzhukova:~$ su alice
Пароль:
alice@svzhukova:/home/svzhukova$ sudo useradd bob
```

Рис. 2.9: alice

Создадим пользователя bob (рис. 2.10).

```
alice@svzhukova:/home/svzhukova$ sudo useradd bob
```

Рис. 2.10: Создадим

Установим пароль для пользователя bob (рис. 2.11).

```
alice@svzhukova:/home/svzhukova$ id bob
uid=1002(bob) gid=1002(bob) группы=1002(bob)
```

Рис. 2.11: Пароль

Просмотрим, в какие группы входит пользователь bob (рис. 2.12).

```
alice@svzhukova:/home/svzhukova$ id bob  
uid=1002(bob) gid=1002(bob) группы=1002(bob)
```

Рис. 2.12: Группы

Создание учётных записей пользователей

Переключимся в терминале на учётную запись пользователя root (рис. 2.13).

```
alice@svzhukova:/home/svzhukova$ su  
Пароль:  
root@svzhukova:/home/svzhukova# █
```

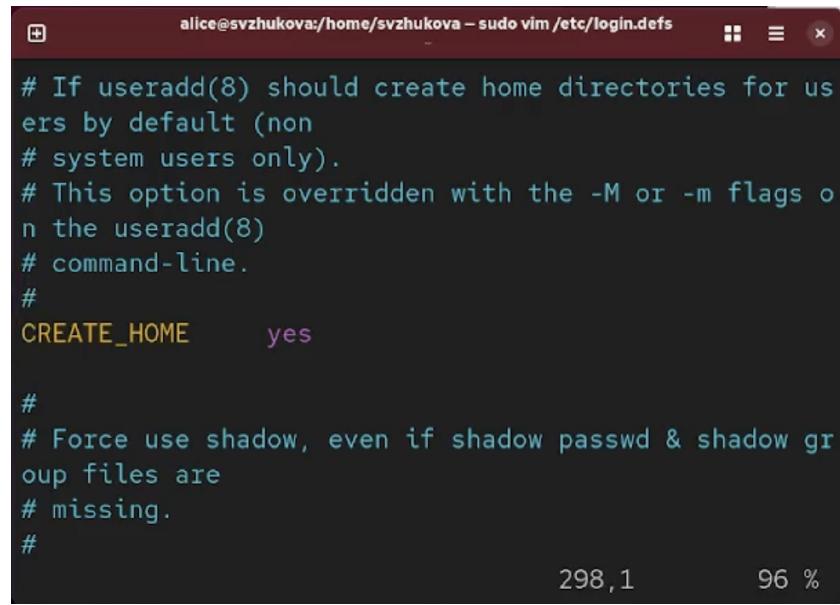
Рис. 2.13: root

Откроем файл конфигурации /etc/login.defs для редактирования, используя vim (рис. 2.14).

```
root@svzhukova:/home/svzhukova# sudo vim /etc/login.d  
efs
```

Рис. 2.14: Откроем файл конфигурации

Найдем параметр CREATE_HOME и убедимся, что он установлен в значение yes.(рис. 2.15).



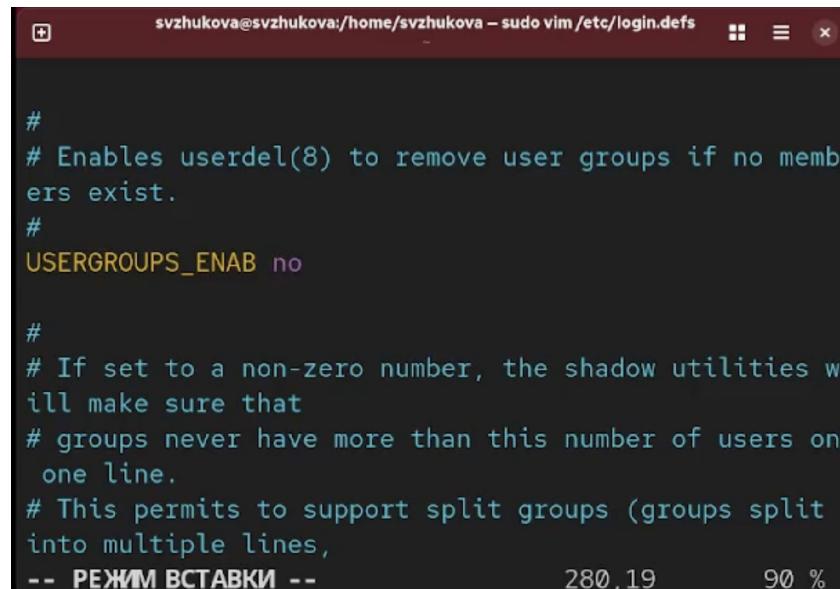
```
# If useradd(8) should create home directories for users by default (non
# system users only).
# This option is overridden with the -M or -m flags on the useradd(8)
# command-line.
#
CREATE_HOME      yes

#
# Force use shadow, even if shadow passwd & shadow group files are
# missing.
#

```

Рис. 2.15: Все верно

Также установим параметр USERGROUPS_ENAB no (рис. 2.16).



```
#
# 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,
-- РЕЖИМ ВСТАВКИ --
280,19          90 %
```

Рис. 2.16: no

Перейдем в каталог /etc/skel, создадим каталоги Pictures и Documents: (рис. 2.17).

```
root@svzhukova:/home/svzhukova# cd /etc/skel  
root@svzhukova:/etc/skel# mkdir Pictures  
root@svzhukova:/etc/skel# mkdir Documents  
root@svzhukova:/etc/skel# nano .bashrc
```

Рис. 2.17: Создадим

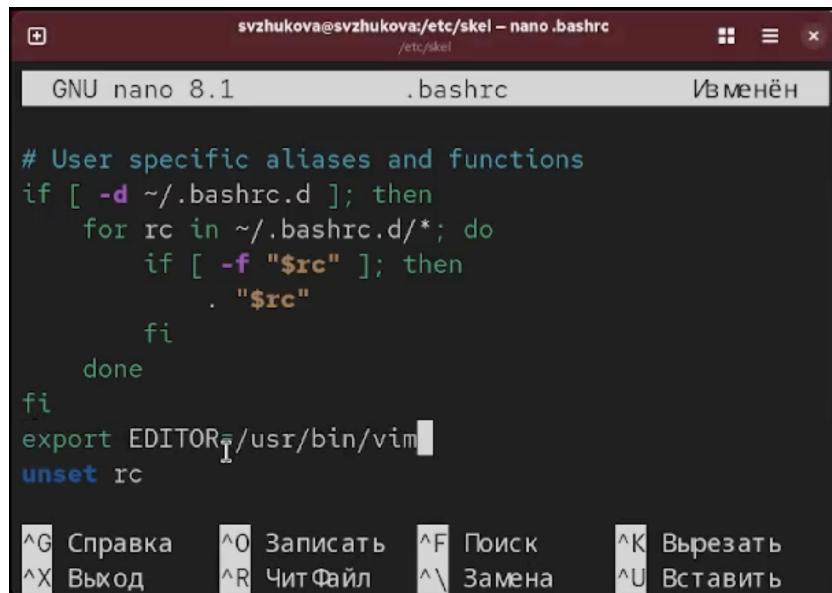
Это позволит добавить эти каталоги по умолчанию во все домашние каталоги пользователей.

Откроем файл .bashrc(рис. 2.18).

```
root@svzhukova:/etc/skel# nano .bashrc
```

Рис. 2.18: Откроем

Изменим содержимое файла .bashrc, добавив строку export EDITOR=/usr/bin/vim (рис. 2.19).



The screenshot shows a terminal window titled "svzhukova@svzhukova:/etc/skel – nano .bashrc". The file content is:

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

The cursor is positioned at the end of the line "export EDITOR=/usr/bin/vim". Below the editor window is a menu bar with Russian labels: Справка, Записать, Поиск, Вырезать, Выход, ЧитФайл, Замена, Вставить.

Рис. 2.19: Изменим

Эта запись означает, что текстовый редактор vim или редактор mceditor будет установлен по умолчанию для инструментов, которые нуждаются в изменении

текстовых файлов.

Переключимся в терминале на учётную запись пользователя alice, используя утилиту useradd, создадим пользователя carol(рис. 2.20).

```
root@svzhukova:/etc/skel# su alice
alice@svzhukova:/etc/skel$ sudo -i useradd carol
```

Рис. 2.20: Carol

Установим пароль для пользователя carol (рис. 2.21).

```
root@svzhukova:~# sudo passwd carol
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошёл проверку орфографии - слишком простой
Повторите ввод нового пароля:
passwd: пароль успешно обновлён
root@svzhukova:~#
```

Рис. 2.21: Установим пароль

Посмотрим информацию о пользователе carol, проверим, в какую первоначальную группу входит пользователь carol (рис. 2.22).

```
root@svzhukova:~# su carol
carol@svzhukova:/root$ id
uid=1003(carol) gid=100(users) группы=100(users) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
carol@svzhukova:/root$ cd
carol@svzhukova:~$
```

Рис. 2.22: Посмотрим информацию о пользователе carol

Убедимся, что каталоги Pictures и Documents были созданы в домашнем каталоге пользователя carol(рис. 2.23).

```
carol@svzhukova:~$ ls -Al
итого 12
-rw-r--r--. 1 carol users 18 окт 29 2024 .bash_logo
ut
-rw-r--r--. 1 carol users 144 окт 29 2024 .bash_profile
-rw-r--r--. 1 carol users 549 сен 11 20:03 .bashrc
drwxr-xr-x. 2 carol users 6 сен 11 20:00 Documents
drwxr-xr-x. 4 carol users 39 сен 6 13:33 .mozilla
drwxr-xr-x. 2 carol users 6 сен 11 20:00 Pictures
carol@svzhukova:~$
```

Рис. 2.23: Убедимся

Переключимся в терминале на учётную запись пользователя alice(рис. 2.24).

```
carol@svzhukova:~$ su alice
Пароль:
```

Рис. 2.24: alice

Строка записи о пароле пользователя carol в файле /etc/shadow (рис. 2.25).

```
alice@svzhukova:/home/carol$ sudo cat /etc/shadow | grep carol
[sudo] пароль для alice:
carol:$y$j9T$pRlW.167v18KKBm/htLVR0$hsDIspK5qtkC9FXwJ
ljKtJS152M3IDv2RRjtOsJQk70:20342:0:99999:7:::
```

Рис. 2.25: Страна записи о пароле

Сначала мы видим зашифрованный пароль, потом срок действия

Изменим свойства пароля пользователя carol следующим образом (рис. 2.26).

```
alice@svzhukova:/home/carol$ sudo passwd -n 30 -w 3 -x 90 carol
passwd: пароль изменён.
alice@svzhukova:/home/carol$ sudo cat /etc/shadow | grep carol
carol:$y$j9T$pRlW.167v18KKBm/htLVR0$hsDIspK5qtkC9FXwJ
ljKtJS152M3IDv2RRjtOsJQk70!20342:30:90:3:::
alice@svzhukova:/home/carol$
```

Рис. 2.26: Изменим свойства пароля

В этой записи срок действия пароля истекает через 90 дней (-x 90). За три дня до истечения срока действия пользователь получит предупреждение (-w 3). Пароль должен использоваться как минимум за 30 дней (-n 30) до того, как его можно будет изменить.

Убедимся в изменении в строке с данными о пароле пользователя carol в файле /etc/shadow:(рис. 2.27).

```
alice@svzhukova:/home/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:svzhukova,alice
/etc/group:alice:x:1001:
alice@svzhukova:/home/carol$
```

Рис. 2.27: /etc/shadow

Убедимся, что идентификатор carol существует не во всех трёх файлах:(рис. 2.28).

```
alice@svzhukova:/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$pRlw.167v18KKBm/htLVR0$hsDIspK5qtkC9FXwJljKtJS152M3IDv2RRjtQsJQk70:20342:30:90:::
::
alice@svzhukova:/home/carol$
```

Рис. 2.28: Существует

Работа с группами

В этом упражнении создадим две группы и добавим некоторых пользователей в эти группы. Находясь под учётной записью пользователя alice, создадим группы main и third:(рис. 2.29).

```
alice@svzhukova:/home/carol$ sudo groupadd main
alice@svzhukova:/home/carol$ sudo groupadd third
```

Рис. 2.29: Создадим

Используем usermod для добавления пользователей alice и bob в группу main, а carol, dan, dave и david – в группу third: (рис. 2.30).

```
alice@svzhukova:/home/carol$ sudo usermod -aG main al  
ice  
alice@svzhukova:/home/carol$ sudo usermod -aG main bo  
b  
alice@svzhukova:/home/carol$ sudo usermod -aG third c  
arol
```

Рис. 2.30: usermod

Убедимся, что пользователь carol правильно добавлен в группу third (рис. 2.31).

```
alice@svzhukova:/home/carol$ id carol  
uid=1003(carol) gid=100(users) группы=100(users),1004  
(third)  
alice@svzhukova:/home/carol$ id car
```

Рис. 2.31: Убедимся

Определим, участниками каких групп являются другие созданные нами пользователи (рис. 2.32). (рис. 2.33).

```
alice@svzhukova:/home/carol$ id bob  
uid=1002(bob) gid=1002(bob) группы=1002(bob),1003(mai  
n)
```

Рис. 2.32: bob

```
alice@svzhukova:/home/carol$ id alice  
uid=1001(alice) gid=1001(alice) группы=1001(alice),10  
(wheel),1003(main)  
alice@svzhukova:/home/carol$
```

Рис. 2.33: alice

Контрольные вопросы

2.0.1 1. Команды для получения информации о пользователе и группах

Для получения информации о номере (идентификаторе) пользователя и группах, в которые он включен, используйте команду:

```
id username
```

Эта команда выдает информацию о UID (идентификаторе пользователя) и GIDs (идентификаторы групп) для указанного пользователя.

2.0.2 2. UID пользователя root и команда для его получения

Пользователь root имеет UID 0. Узнать UID пользователя можно с помощью команды:

```
id root
```

или просто:

```
echo $UID
```

Эти команды выведут соответствующую информацию.

2.0.3 3. Различие между командами su и sudo

Команда su (switch user) позволяет переключаться на другого пользователя (по умолчанию на root), требуя его пароль. Команда sudo (superuser do) позволяет запускать команды с правами суперпользователя, используя при этом ваш собственный пароль. sudo более гибок и безопасен, особенно в многопользовательских системах.

2.0.4 4. Конфигурационный файл для sudo

Параметры для sudo определяются в конфигурационном файле:

`/etc/sudoers`

Этот файл можно редактировать с помощью команды `visudo`, что позволяет избежать синтаксических ошибок.

2.0.5 5. Команда для безопасного изменения конфигурации sudo

Для безопасного редактирования конфигурации sudo следует использовать команду:

`visudo`

Это предотвратит конфликт редактирования и проверит правильность синтаксиса.

2.0.6 6. Группа для администрирования через sudo

Чтобы предоставить пользователю доступ ко всем командам администрирования системы через sudo, он должен быть членом группы sudo или wheel (в зависимости от дистрибутива).

2.0.7 7. Файлы для настроек учетных записей

При создании учетных записей пользователей используются следующие файлы: - `/etc/login.defs` – содержит параметры для создания учетных записей, такие как минимальная длина пароля. - `/etc/default/useradd` – определяет параметры по умолчанию для команды useradd, например, домашний каталог.

2.0.8 8. Хранение информации о группах пользователей

Информация о первичных и дополнительных группах пользователей хранится в файле:

`/etc/passwd`

Запись для пользователя `alice` может выглядеть следующим образом:

`alice:x:1001:1001::/home/alice:/bin/bash`

Здесь `1001` – это `UID`, а `1001` после второго двоеточия – `GID` (идентификатор ее основной группы).

2.0.9 9. Команды для изменения информации о пароле

Для изменения информации о пароле пользователя, включая срок действия, можно использовать команды:

`passwd username`

и

`chage -l username`

Первая команда изменяет пароль, а вторая показывает параметры, связанные со сроками действия пароля.

2.0.10 10. Команда для изменения информации в файле /etc/group

Для изменения информации в файле `/etc/group` следует использовать команду:

`vigr /etc/group`

Это делается для обеспечения безопасности, так как `vigr` блокирует файл от одновременного доступа другими пользователями и проверяет синтаксис перед сохранением изменений.

3 Выводы

Мы получили 3 представление о работе с учётными записями пользователей и группами пользователей в операционной системе типа Linux.