

Отчёта по лабораторной работе 2

Управление пользователями и группами

Накова Амина Михайловна

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
4	Выводы	14
	Список литературы	15

Список иллюстраций

3.1	рис. 1	7
3.2	рис. 2	8
3.3	рис. 3	8
3.4	рис. 4	9
3.5	рис. 5	9
3.6	рис. 6	10
3.7	рис. 7	10
3.8	рис. 8	11
3.9	рис. 9	11
3.10	рис. 10	12
3.11	рис. 11	12

Список таблиц

1 Цель работы

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

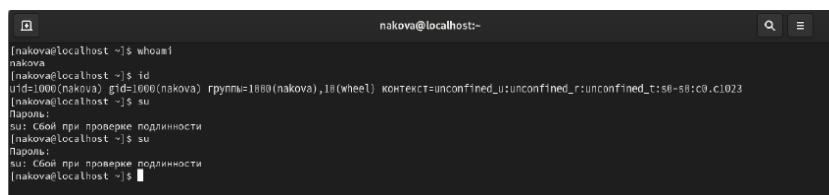
Здесь приводится описание задания в соответствии с рекомендациями методического пособия и выданным вариантом.

2 Теоретическое введение

В операционных системах типа Linux чаще всего применяется дискреционное управление доступом субъектов к объектам системы. В качестве субъектов системы чаще всего выступают пользователи или группы пользователей, а в качестве объектов — файлы (в том числе системные), каталоги, устройства и т.п. В качестве особого субъекта выделяется суперпользователь (пользователь root), имеющий право устанавливать права владения для всех остальных субъектов системы. Под доступом к ресурсу системы понимают чтение (read), запись (write) и выполнение (execute). Тот или иной тип доступа может быть применён к пользователю и/или группе, владеющими тем или иным ресурсом операционной системы, а также ко всем остальным субъектам, не являющимся владельцами ресурса. Механизм пользователей был разработан по соображениям безопасности, для ограничения доступа к различным частям системы. Суперпользователь (root) имеет полный доступ к операционной системе и её настройкам и используется только для целей системного администрирования. Обычные пользователи работают с ограниченными правами, т.е. сокращается их влияние на их собственную среду и на операционную систему в целом. Один из способов изменения прав доступа пользователя к ресурсам системы — добавление пользователя в определённую группу. Например, члены группы wheel используют административные привилегии пользователя root, в частности, они могут использовать команду sudo, чтобы не входить в систему как пользователь root, но при этом выполнять административные задачи в операционной системе.

3 Выполнение лабораторной работы

Войдём в систему как обычный пользователь и откроем терминал. Определим, какую учётную запись пользователя мы используем, введя команду `whoami` (используем учётную запись `ismakhorin`). Выведем на экран более подробную информацию, используя команду `id` (UID – id пользователя равный 1000. GID – id группы равный 1000). Используем команду `su` для переключения к учётной записи `root`. При запросе пароля вводим пароль пользователя `root`. Наберём `id` (UID – id пользователя равный 0. GID – id группы равный 0). Далее просмотрим в безопасном режиме файл `/etc/sudoers`. Мы хотим использовать `mcedit`, поэтому в терминале для запуска `visudo` указываем: `EDITOR=mcedit visudo` (Рис. 1):



```
nakova@localhost:~$ whoami
nakova
nakova@localhost:~$ id
uid=1000(nakova) gid=1000(nakova) группы=1000(nakova),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
nakova@localhost:~$ su
Пароль:
su: Сбой при проверке подлинности
nakova@localhost:~$ su
Пароль:
su: Сбой при проверке подлинности
nakova@localhost:~$
```

Рис. 3.1: рис. 1

После мы должны убедиться, что в открытом с помощью `visudo` файле присутствует строка `%wheel ALL=(ALL) ALL` (данная строка присутствует) (Рис. 2):

```
nakova@localhost:~$ sudo -i visudo
## 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
```

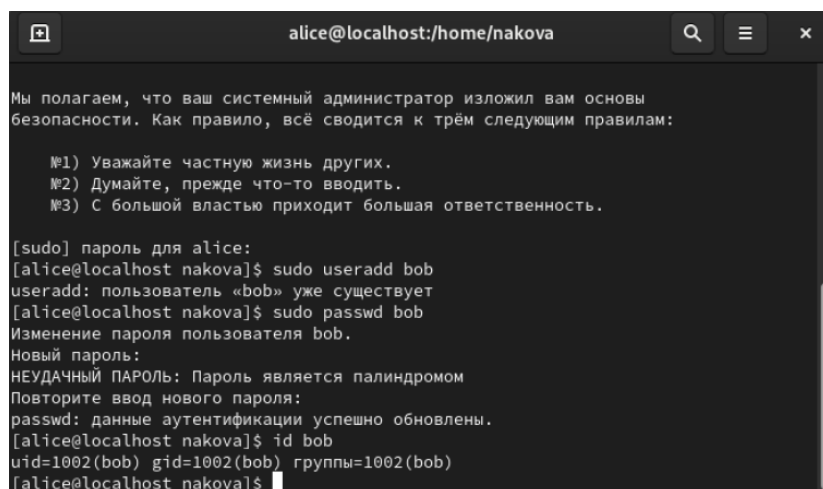
Рис. 3.2: рис. 2

По закрытию файла создаём пользователя alice, входящего в группу wheel с помощью команды: `useradd -G wheel alice`. Нужно убедиться, что пользователь alice добавлен в группу wheel. Для этого введём команду `id alice` (Groups = 1001(alice),10(wheel)). Следующим шагом зададим пароль для пользователя alice, набрав `passwd alice`. Пароль требуется ввести дважды (Рис. 3).

```
nakova@localhost:~$ sudo -i useradd -G wheel alice
[sudo] пароль для nakova:
[nakova@localhost ~]$ id alice
uid=1001(alice) gid=1001(alice) группы=1001(alice),10(wheel)
[nakova@localhost ~]$
```

Рис. 3.3: рис. 3

Переключаемся на учётную запись пользователя alice командой: `su alice`. Создаём пользователя bob: `sudo useradd bob`. При запросе вводим пароль пользователя. Проверяем, что пользователь bob создан (`id bob`) и устанавливаем пароль для пользователя: `sudo passwd bob` (Рис. 4).

A terminal window titled 'alice@localhost:/home/nakova' with search, menu, and close icons. It displays a security notice in Russian, followed by three rules. Then, it shows the execution of 'sudo useradd bob' (which fails because 'bob' already exists) and 'sudo passwd bob' (which succeeds after a password is set). Finally, it shows the output of 'id bob', indicating that 'bob' is a user with UID 1002 and belongs to the 'bob' group.

```
alice@localhost:/home/nakova

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@localhost nakova]$ sudo useradd bob
useradd: пользователь «bob» уже существует
[alice@localhost nakova]$ sudo passwd bob
Изменение пароля пользователя bob.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[alice@localhost nakova]$ id bob
uid=1002(bob) gid=1002(bob) группы=1002(bob)
[alice@localhost nakova]$
```

Рис. 3.4: рис. 4

Теперь применим общие решения для создания учётных записей пользователей. Для этого переключимся в терминале на учётную запись пользователя root: su. Далее открываем файл конфигурации /etc/login.defs для редактирования, используя: vim /etc/login.defs (Рис. 5).

A terminal window showing the execution of 'su' to switch to root and then 'vim /etc/login.defs' to open the configuration file for editing.

```
$ su
vim /etc/login.defs
```

Рис. 3.5: рис. 5

В файле требуется изменить несколько параметров. Для начала найдём параметр CREATE_HOME и убедимся, что он установлен в значение yes. Теперь установим параметр USERGROUPS_ENAB no. Это позволит не добавлять нового пользователя в группу с тем же именем, что и пользователь, а использовать группу users. (Рис. 6).

```
root@localhost:~  
#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
```

Рис. 3.6: рис. 6

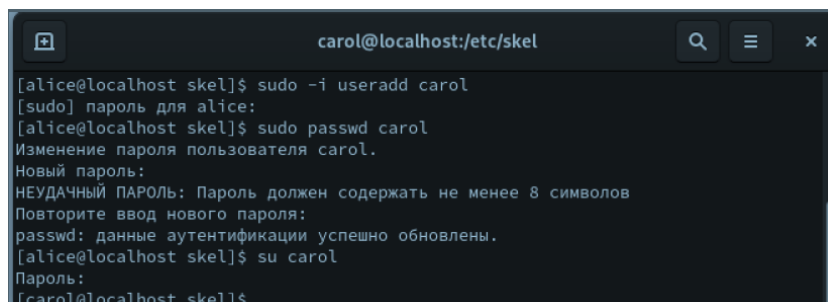
После закрытия файла перейдём в каталог /etc/skel: `cd /etc/skel`. В этом каталоге создаём подкаталоги Pictures и Documents: `mkdir Pictures Documents` (это позволит добавить эти каталоги по умолчанию во все домашние каталоги пользователей). Выполняем проверку создания командой: `ls` (Рис. 7.1). Теперь нам нужно изменить содержимое файла `.bashrc`, добавив строку: `export EDITOR=/usr/bin/vim` (Рис. 7.2). (эта запись означает, что текстовый редактор `vim` будет установлен по умолчанию для инструментов, которые нуждаются в изменении текстовых файлов).

```
root@localhost:/etc/skel  
[nakova@localhost ~]$ cd /etc/skel  
[nakova@localhost skel]$ mkdir Pictures  
mkdir: невозможно создать каталог «Pictures»: Отказано в доступе  
[nakova@localhost skel]$ su  
Пароль:  
su: Сбой при проверке подлинности  
[nakova@localhost skel]$ sudo su  
[sudo] пароль для nakova:  
[root@localhost skel]# mkdir Pictures  
[root@localhost skel]# mkdir Documents  
[root@localhost skel]# nano .bashrc
```

Рис. 3.7: рис. 7

Используя утилиту `useradd`, создаём пользователя `carol`: `useradd carol` и установим пароль для пользователя `carol`: `passwd carol`. Посмотрим информацию о пользователе `carol`: `id carol` (`carol` находится в группе `users`). Теперь нам нужно

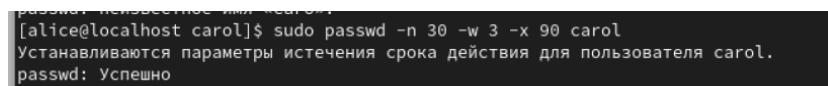
убедитесь, что каталоги Pictures и Documents были созданы в домашнем каталоге пользователя carol: su carol и ls (Рис. 8).

A terminal window titled 'carol@localhost:/etc/skel' with search, menu, and close icons. The terminal shows the following commands and output:

```
[alice@localhost skel]$ sudo -i useradd carol
[sudo] пароль для alice:
[alice@localhost skel]$ sudo passwd carol
Изменение пароля пользователя carol.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[alice@localhost skel]$ su carol
Пароль:
[carol@localhost skel]$
```

Рис. 3.8: рис. 8

Изменим свойства пароля пользователя carol следующим образом: 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). Пароль должен использоваться как минимум за 30 дней (-n 30) до того, как его можно будет изменить) (Рис. 9).

A terminal window showing the following commands and output:

```
[alice@localhost carol]$ sudo passwd -n 30 -w 3 -x 90 carol
Устанавливаются параметры истечения срока действия для пользователя carol.
passwd: Успешно
```

Рис. 3.9: рис. 9

Создаём ещё несколько пользователей: dan, dave, david, используя скрипт: for i in dan dave david; do useradd \$i; done. Для этого создадим файл script.sh: touch script.sh. Командой mcedit открываем файл в редакторе. Теперь вносим скрипт в наш файл и выполняем сохранение. Переходим к запуску нашего скрипта командой bash. После успешного выполнения нам нужно убедиться, что идентификатор alice существует во всех трёх файлах: grep alice /etc/passwd /etc/shadow /etc/group и то, что идентификатор carol существует не во всех трёх файлах: grep carol /etc/passwd /etc/shadow /etc/group (Рис. 10).

```

[alice@localhost carol]$ sudo cat /etc/shadow | grep carol
carol:$6$skzBTLcU0GxLM0ZCZ$aRDIVlxZSeqbg5jP1SgCMrvf5JNMT4ZMK5zakT4CzxUwr0TKXdRlti
rNtlwTa8oVzr0sjq2uYVjIm1.TkmA8V.:20078:30:90:3::
[alice@localhost carol]$ 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:nakova,alice
/etc/group:alice:x:1001:
[alice@localhost carol]$ sudo grep carol /etc/passwd /etc/shadow /etc/group
/etc/passwd:carol:x:1003:1003::/home/carol:/bin/bash
/etc/shadow:carol:$6$skzBTLcU0GxLM0ZCZ$aRDIVlxZSeqbg5jP1SgCMrvf5JNMT4ZMK5zakT4Czx
Uwr0TKXdRltirNtlwTa8oVzr0sjq2uYVjIm1.TkmA8V.:20078:30:90:3::
/etc/group:carol:x:1003:
[alice@localhost carol]$

```

Рис. 3.10: рис. 10

На данном этапе требуется создать две группы и добавить некоторых пользователей в эти группы. Находясь под учётной записью пользователя root, создаём группы main и third: `groupadd main`, `groupadd third`. Затем, используем `usermod` для добавления пользователей alice и bob в группу main, а carol, dan, dave и david - в группу third: `usermod -aG main alice`, `usermod -aG main bob`, `usermod -aG third carol`, `usermod -aG third dan`, `usermod -aG third dave`, `usermod -aG third david` 9 Убеждаемся, что пользователь carol правильно добавлен в группу third: `id carol` (пользователю carol должна быть назначена основная группа с идентификатором `gid = 100` (users)) (Рис. 11).

```

/etc/group:carol:x:1003:
[alice@localhost carol]$ sudo groupadd main
[alice@localhost carol]$ sudo groupadd third
[alice@localhost carol]$ sudo usermod -aG main alice
[alice@localhost carol]$ sudo usermod -aG main bob
[alice@localhost carol]$ sudo usermod -aG third carol
[alice@localhost carol]$ id carol
uid=1003(carol) gid=1003(carol) группы=1003(carol),1005(third)
[alice@localhost carol]$

```

Рис. 3.11: рис. 11

Ответы на контрольные вопросы 1. При помощи какой команды можно получить информацию о номере, назначенном пользователю Linux, о группах, в которые включён пользователь? `id`. 2. Какой UID имеет пользователь root? `UID=0`. 3. В чём состоит различие между командами `su` и `sudo`? Основное различие между ними заключается в пароле, который им требуется: в то время как “`sudo`” требует пароля текущего пользователя, “`su`” требует ввода пароля пользователя root. Совершенно очевидно, что “`sudo`” является лучшей альтернативой между ними с

точки зрения безопасности. 4. В каком конфигурационном файле определяются параметры sudo? `/etc/sudoers`. 5. Какую команду следует использовать для безопасного изменения конфигурации sudo? `visudo`. 10 6. Если вы хотите предоставить пользователю доступ ко всем командам администратора через sudo, членом какой группы он должен быть? `Admin`. 7. Какие файлы/каталоги можно использовать для определения параметров, которые будут использоваться при создании учётных записей пользователей? `/etc/login.defs` и `/etc/default/useradd`. 8. В каких файлах хранятся пароли пользователей, учётные записи групп? `/etc/shadow` `/etc/group`. 9. Какие команды вы можете использовать для изменения информации о пароле пользователя? `passwd` и `grpasswd`. 10. Сколько групп вы можете создать в файле `/etc/passwd`? Поясните свой ответ. Любое количество. 11. Какую команду следует использовать для изменения файла `/etc/group` вручную? `emacs /etc/group` или `vim /etc/group`.

4 Выводы

В ходе выполнения лабораторной работы были получены представление о работе с учётными записями пользователей и группами пользователей в операционной системе типа Linux.

Список литературы