

## ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 9. «ВЫПОЛНЕНИЕ СЦЕНАРИЕВ В UNIX»

### Теоретическая часть

#### Сценарий: Вход в систему и завершение сеанса

Для входа в систему необходимо ввести логин и пароль пользователя. При этом символы вводимого пароля не отображаются.

```
Welcome to desktop / tty1
desktop login: user
Password:
Last login: Wed Dec 07 00:20:09 2006 from tty1
user@desktop ~ $
```

При входе в систему в графическом режиме (через X11), пользователю вместо командной строки предоставляется графический десктоп.

Для завершения сеанса работы в командной строке необходимо ввести команду `exit`:

```
user@desktop ~ $ exit.
```

#### Сценарий: Изучение базовых прав доступа

Для просмотра прав доступа можно использовать команду `ls` с ключом вывода расширенной информации: **`ls -l`**.

```
user@desktop ~ $ ls -l
drwxr-xr-x  1 user users  22 Дек 19 11:18 test/
-rw-r--r--  1 user users  90 Сен 19 00:20 test.txt
```

Особый интерес представляют: первая колонка (права доступа), третья и четвёртая – владелец и группа владельцев соответственно.

Рассмотрим исполняемый файл **`ls -l /bin/bash`**.

```
user@desktop ~ $ ls -l /bin/bash
-rwxr-xr-x  1 root root 746544 Дек 21 13:40 /bin/bash*
```

Исполняемые файлы в UNIX определяются наличием специального бита прав доступа.

Для директории права на исполнения трактуются по-другому. Рассмотрим права директории `/tmp` **`ls -ld /tmp`**:

```
user@desktop ~ $ ls -ld /tmp
drwxrwxrwt  26 root root 5168 Дек 22 20:04 /tmp/
```

Директория имеет дополнительный `sticky-bit`, определяю-

щий права на создание и удаление файлов в директории.

Изменение файла с недостатком прав приводит к ошибке доступа. Например, команда: **rm /bin/bash**.

```
user@desktop ~ $ rm /bin/bash
rm: удалить защищенный от записи обычный файл
`/bin/bash'? y
rm: невозможно удалить `/bin/bash': Permission denied.
```

Для всех файлов, на которые данный пользователь не имеет прав записи, команда `rm` выведет предупреждение об удалении.

Изменение прав доступа производится с помощью команды `chmod`. Для задания файлу прав только для чтения воспользуемся командой: **chmod a=r test.txt**.

Для лишения всех прав группы владельцев и остальных пользователей воспользуемся командой: **chmod go-rwx test.txt**.

### Сценарий: Переход в режим суперпользователя

Некоторые исполняемые программы обладают специальным `suid`-битом, например, программа `passwd`. Рассмотрим права доступа к этому исполняемому файлу: **ls -l /bin/passwd**.

```
user@desktop ~ $ ls -l /bin/passwd
-rws--x--x 1 root root 28660 Янв  8 13:05 /bin/passwd*
```

Запускаются `suid`-программы от имени владельца файла. В этом можно убедиться, если запустить команду **passwd**, а затем на другом терминале сделать **ps aux | grep passwd**:

```
user@desktop ~ $ passwd
Changing password for user
(current) UNIX password:
user@desktop ~ $ ps aux | grep passwd
root 12937 0.0 0.1 3228 1012 pts/2 S+ 23:28 0:00 passwd
user 12989 0.0 0.1 2740 748 pts/3 R+ 23:28 0:00 grep passwd
```

Для длительной работы в режиме суперпользователя обычно используют команду `su`. Используем параметр `-`, чтобы проинициализировать окружение суперпользователя: **su -**. Для того, чтобы перейти в режим суперпользователя, необходимо знать его пароль.

```
user@desktop ~ $ su -
Password:
desktop ~ #
```

При этом запускается новая командная оболочка, уже с новыми привилегиями.

Для завершения сеанса суперпользователя необходимо

воспользоваться командой **exit**:

```
desktop ~ # exit
logout
user@desktop ~ $
```

### Сценарий: Изучение базы данных пользователей

Данные о зарегистрированных в системе пользователях хранятся в файле `/etc/passwd`. Рассмотрим его содержимое **cat /etc/passwd**:

```
user@desktop ~ $ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
adm:x:3:4:adm:/var/adm:/bin/false
```

Аналогичным образом данные о группах хранятся в файле `/etc/group`. Рассмотрим его содержимое **cat /etc/group**:

```
user@desktop ~ $ cat /etc/group
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm.
```

### Сценарий: Добавление и удаление пользователей

Изменения учётных записей пользователей доступны только суперпользователю.

Для добавления новых пользователей используется команда `useradd`. При этом в качестве параметров можно указать домашнюю директорию и командную оболочку пользователя: **useradd testuser -d /home/users/testuser -s /bin/sh**, результат можно увидеть следующим образом: **cat /etc/passwd | grep testuser**.

```
desktop ~ # cat /etc/passwd
testuser:x:1003:1003:~/home/users/testuser:/bin/sh
```

С помощью команды `passwd` можно задать пароль для нового пользователя: **passwd testuser**.

```
desktop ~ # passwd testuser
New UNIX password:
Retype new UNIX password:
passwd: пароль успешно обновлён
```

Для изменения параметров учётной записи можно отредактировать файл `/etc/passwd`, однако более корректным способом

является использование команды `usermod`. Например, для изменения командной оболочки пользователя на `/bin/false` приведёт к невозможности его входа в систему: **`usermod -s /bin/false testuser`**.

Удаление пользователя производится с помощью команды `userdel`: **`userdel testuser`**.

### Задания для самостоятельной работы

1. Выясните, чем отличается реакция операционной системы на различные ошибки аутентификации.

2. Сравните права доступа к директориям `/bin` и `/tmp`. Какие операции сможет совершать в них простой пользователь?

3. Создайте текстовый файл и задайте права на него таким образом, чтобы он мог просматриваться только владельцем и никем не мог редактироваться.

4. Что смогут делать другие пользователи с файлами в домашней директории пользователя, если он задаст всем остальным пользователям право на запись в директорию, но удалит право исполнения на неё?

5. Найдите все исполняемые файлы с установленным `suid`-битом.

6. Получите имена всех пользователей системы, у которых в качестве командной оболочки используется программа `/bin/false`.

### Контрольные вопросы

1. Что необходимо ввести для входа в систему?
2. Для чего нужна команда `rm`?
3. С помощью какой команды производится изменение прав доступа?
4. Как перейти в режим суперпользователя?
5. Какая команда используется для добавления новых пользователей?
6. Какая команда используется для удаления пользователей?