

# Лабораторная работа №2

## Основы информационной безопасности

---

Феоктистов Владислав Сергеевич

17 сентября 2022

Российский университет дружбы народов, Москва, Россия

НПМбд-01-19

Целью данной работы является: приобретение практических навыков работы в консоли с правами и атрибутами файлов и каталогов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux, проверка необходимых наборов прав для выполнения различных действий над файлами и каталогами, получение навыков чтения выделенных прав через консоль.

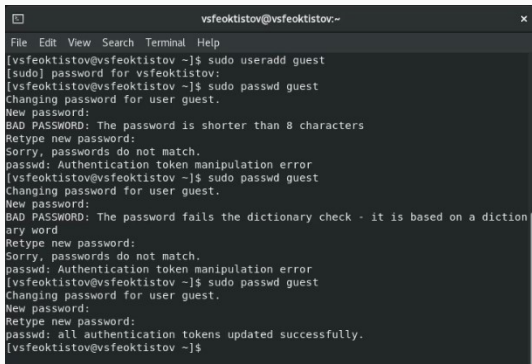
- Создать нового пользователя под именем guest с паролем;
- войти в систему от имени нового пользователя и получить о нем всю необходимую информацию через консоль;
- проверить и изменить права на существующие и созданные файлы и каталоги;
- проверить как снятие всех атрибутов с директории повлияло на возможности работы с ним.

## Ход выполнения лабораторной работы

---

## Создание нового пользователя и установка пароля

С помощью команды `useradd` создаем нового пользователя, а с помощью команды `passwd` устанавливаем для него пароль.

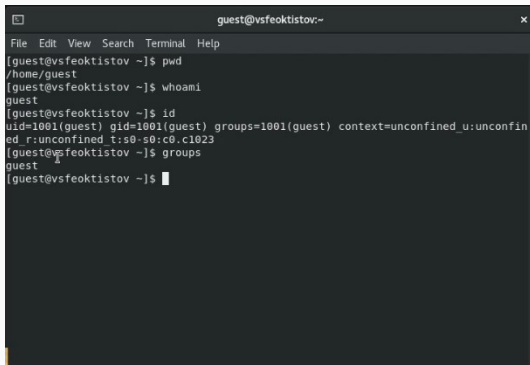
A terminal window titled 'vsfeoktistov@vsfeoktistov:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the execution of 'sudo useradd guest' followed by 'passwd guest'. The password setting process fails twice: first because the password is shorter than 8 characters, and second because it fails a dictionary check. After two successful password re-entries, the process completes with the message 'passwd: all authentication tokens updated successfully.'

```
vsfeoktistov@vsfeoktistov:~  
File Edit View Search Terminal Help  
[vsfeoktistov@vsfeoktistov ~]$ sudo useradd guest  
[sudo] password for vsfeoktistov:  
[vsfeoktistov@vsfeoktistov ~]$ sudo passwd guest  
Changing password for user guest.  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
Sorry, passwords do not match.  
passwd: Authentication token manipulation error  
[vsfeoktistov@vsfeoktistov ~]$ sudo passwd guest  
Changing password for user guest.  
New password:  
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word  
Retype new password:  
Sorry, passwords do not match.  
passwd: Authentication token manipulation error  
[vsfeoktistov@vsfeoktistov ~]$ sudo passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[vsfeoktistov@vsfeoktistov ~]$
```

Figure 1: Создание нового пользователя и пароля

## Получение информации о пользователе

Заходим в систему под созданным пользователем и получаем информацию о текущем каталоге [**cmd: pwd**] (домашняя директория); имя пользователя [**cmd: whoami**]; id,gip,groups [**cmd: id**]. Эту же информацию можно найти в файле */etc/passwd*.

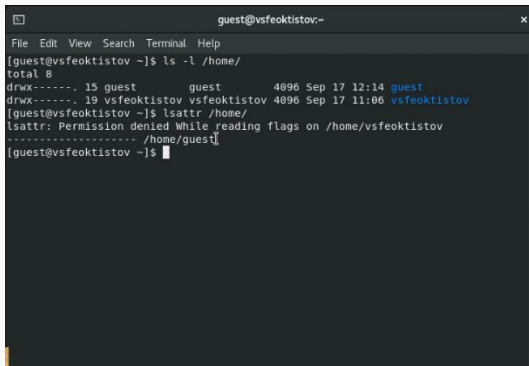
A terminal window titled 'guest@vsfeoktistov:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
[guest@vsfeoktistov ~]$ pwd
/home/guest
[guest@vsfeoktistov ~]$ whoami
guest
[guest@vsfeoktistov ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@vsfeoktistov ~]$ groups
guest
[guest@vsfeoktistov ~]$
```

Figure 2: Получение информации о пользователе

## Просмотр атрибутов

- Для просмотра прав доступа/атрибутов используется команда [cmd: `ls -l`]
- Для просмотра расширенных атрибутов используется команда [cmd: `lsattr`]

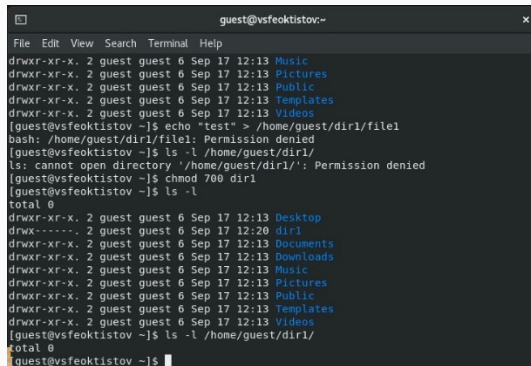


```
guest@vsfeoktistov:~  
File Edit View Search Terminal Help  
[guest@vsfeoktistov ~]$ ls -l /home/  
total 8  
drwx-----, 15 guest      guest      4096 Sep 17 12:14 guest  
drwx-----, 19 vsfeoktistov vsfeoktistov 4096 Sep 17 11:06 vsfeoktistov  
[guest@vsfeoktistov ~]$ lsattr /home/  
lsattr: Permission denied While reading flags on /home/vsfeoktistov  
----- /home/guest  
[guest@vsfeoktistov ~]$
```

Figure 3: Просмотр атрибутов

## Изменение прав

Изменение прав для файла/каталога осуществляется командой *chmod*. Только root, владелец файла или пользователь с привилегией *sudo* могут изменять права доступа к файлу или каталогу. Разрешения можно указывать с помощью символьного, числового или справочного режимов.



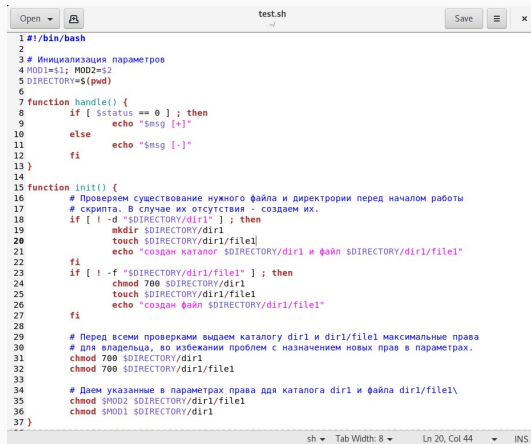
```
guest@vsfeoktistov:~  
File Edit View Search Terminal Help  
drwxr-xr-x. 2 guest guest 6 Sep 17 12:13 Music  
drwxr-xr-x. 2 guest guest 6 Sep 17 12:13 Pictures  
drwxr-xr-x. 2 guest guest 6 Sep 17 12:13 Public  
drwxr-xr-x. 2 guest guest 6 Sep 17 12:13 Templates  
drwxr-xr-x. 2 guest guest 6 Sep 17 12:13 Videos  
[guest@vsfeoktistov ~]$ echo "test" > /home/guest/dirl/file1  
bash: /home/guest/dirl/file1: Permission denied  
[guest@vsfeoktistov ~]$ ls -l /home/guest/dirl/  
ls: cannot open directory '/home/guest/dirl/': Permission denied  
[guest@vsfeoktistov ~]$ chmod 700 dirl  
[guest@vsfeoktistov ~]$ ls -l  
total 0  
drwxr-xr-x. 2 guest guest 6 Sep 17 12:13 Desktop  
drwx-----. 2 guest guest 6 Sep 17 12:20 dirl  
drwxr-xr-x. 2 guest guest 6 Sep 17 12:13 Documents  
drwxr-xr-x. 2 guest guest 6 Sep 17 12:13 Downloads  
drwxr-xr-x. 2 guest guest 6 Sep 17 12:13 Music  
drwxr-xr-x. 2 guest guest 6 Sep 17 12:13 Pictures  
drwxr-xr-x. 2 guest guest 6 Sep 17 12:13 Public  
drwxr-xr-x. 2 guest guest 6 Sep 17 12:13 Templates  
drwxr-xr-x. 2 guest guest 6 Sep 17 12:13 Videos  
[guest@vsfeoktistov ~]$ ls -l /home/guest/dirl/  
total 0  
[guest@vsfeoktistov ~]$
```

Figure 4: Изменение прав



# Автоматизация процесса проверки

Для заполнения таблицы “Установленные права и разрешенные действия” можно написать bash-скрипт, который будет создавать и выдавать права каталогу dir1 и файлу file1, чтобы потом проверить какие действия над ними можно будет совершать.



```
1 #!/bin/bash
2
3 # Инициализация параметров
4 MOD1=$1; MOD2=$2
5 DIRECTORY=$(pwd)
6
7 function handle() {
8     if [ $status == 0 ]; then
9         echo "msg [+]"
10    else
11        echo "msg [-]"
12    fi
13 }
14
15 function init() {
16     # Проверяем существование нужного файла и директории перед началом работы
17     # скрипта. В случае их отсутствия - создаем их.
18     if [ ! -d "$DIRECTORY/dir1" ]; then
19         mkdir $DIRECTORY/dir1
20         touch $DIRECTORY/dir1/file1
21         echo "создан каталог $DIRECTORY/dir1 и файл $DIRECTORY/dir1/file1"
22     fi
23     if [ ! -f "$DIRECTORY/dir1/file1" ]; then
24         chmod 700 $DIRECTORY/dir1
25         touch $DIRECTORY/dir1/file1
26         echo "создан файл $DIRECTORY/dir1/file1"
27     fi
28
29     # Перед всеми проверками выдаем каталогу dir1 и dir1/file1 максимальные права
30     # для владельца, во избежании проблем с назначением новых прав в параметрах.
31     chmod 700 $DIRECTORY/dir1
32     chmod 700 $DIRECTORY/dir1/file1
33
34     # Даем указанные в параметрах права для каталога dir1 и файла dir1/file1\
35     chmod $MOD2 $DIRECTORY/dir1/file1
36     chmod $MOD1 $DIRECTORY/dir1
37 }
```

## Разрешенные действия

После перебора всех атрибутов, используя `bash`-скрипт, можно заполнить такую таблицу:

		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
Права дирек- тории	Права файла								
d----	----	-	-	-	-	-	-	-	-
(000)	(000)								
d-x---	----	-	-	-	-	+	-	-	-
(100)	(000)								
...	...	...	...	...	...	...	...	...	...
drwx---	rwx---	+	+	+	+	+	+	+	+
(700)	(700)								

## Минимальные требования

На основе предыдущей таблицы можно определить минимально необходимые права для выполнения определенных действий над файлами и директориями.

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-wx (300)	— (000)
Удаление файла	d-wx (300)	— (000)
Чтение файла	d-x (100)	r- (400)
Запись в файл	d-x (100)	-w- (200)
Переименование файла	d-wx (300)	— (000)
Создание поддиректории	d-wx (300)	— (000)
Удаление поддиректории	d-wx (300)	— (000)

- Приобрел практические навыки работы в консоли с правами и атрибутами файлов и каталогов;
- закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux;
- проверил необходимый наборов прав для выполнения различных действий над файлами и каталогами;
- получил навыки чтения выделенных прав через консоль.