

---

## Информационная безопасность

### Лабораторная работа №2

Кузнецов Юрий Владимирович

#### Цель работы:

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.

#### Ход работы:

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя **guest** (используя учётную запись администратора: **useradd guest**

```
[root@vm571215 ~]# sudo su
[root@vm571215 ~]# useradd guest
```

2. Зададим пароль для пользователя **guest**: **passwd guest**

```
[root@vm571215 ~]# passwd guest
Изменяется пароль пользователя guest.
Новый пароль : █
```

3. Войдите в систему от имени пользователя **guest**:

```
(base) uvkuznetsov@MacBook-Air-Urij Desktop % ssh guest@95.142.39.209
guest@95.142.39.209's password: █
```

4. Определим директорию, в которой находимся, командой **pwd**. Сравним её с приглашением командной строки. Определим, является ли она домашней директорией:

```
[guest@vm571215 ~]$ pwd
/home/guest
```

5. Уточним имя пользователя командой **whoami**:

```
[guest@vm571215 ~]$ whoami
guest
```

6. Уточним имя пользователя, его группу, а также группы, куда входит пользователь, командой **id**. Выведенные значения **uid**, **gid** и др. Сравним вывод **id** с выводом команды **groups**:

```
[guest@vm571215 ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest)
[guest@vm571215 ~]$ groups
guest
[guest@vm571215 ~]$
```

7. Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки:

```
[guest@vm571215 ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89:/:/var/spool/postfix:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
user1:x:1000:1000:/:/home/user1:/bin/bash
guest:x:1001:1001:/:/home/guest:/bin/bash
[guest@vm571215 ~]$
```

8. Просмотрим файл **/etc/passwd** командой **cat /etc/passwd**. Найдём в нём свою учётную запись. Определим **uid** пользователя. Определим **gid** пользователя. Сравним найденные значения с полученными в предыдущих пунктах:

```
[guest@vm571215 ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:/:/home/guest:/bin/bash
[guest@vm571215 ~]$
```

9. Определим существующие в системе директории командой **ls -l /home/**:

```
[guest@vm571215 ~]$ ls -l /home/
итого 8
drwx----- 2 guest guest 4096 сен 16 21:07 guest
drwx----- 2 user1 user1 4096 сен 16 20:57 user1
[guest@vm571215 ~]$
```

10. Проверим какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой **lsattr /home**:

```
[guest@vm571215 ~]$ lsattr /home
-----e-- /home/guest
lsattr: Отказано в доступе While reading flags on /home/user1
[guest@vm571215 ~]$
```

11. Создадим в домашней директории поддиректорию dir1 командой **mkdir dir1**  
Определим командами **ls -l** и **lsattr**, какие права доступа и расширенные атрибуты были выставлены на директорию dir1:

```
[guest@vm571215 ~]$ mkdir dir1
[guest@vm571215 ~]$ ls
dir1
[guest@vm571215 ~]$ ls -l
итого 4
drwxrwxr-x 2 guest guest 4096 сен 16 21:15 dir1
[guest@vm571215 ~]$ lsattr
-----e-- ./dir1
[guest@vm571215 ~]$
```

12. Снимем с директории dir1 все атрибуты командой **chmod 000 dir1** и проверим с её помощью правильность выполнения команды **ls -l**:

```
[guest@vm571215 ~]$ chmod 000 dir1
[guest@vm571215 ~]$ ls -l
итого 4
d----- 2 guest guest 4096 сен 16 21:15 dir1
[guest@vm571215 ~]$
```

13. Попытаемся создать в директории dir1 файл file1 командой **echo "test" > /home/guest/dir1/file1** Проверим командой **ls -l /home/guest/dir1**:

```
[guest@vm571215 ~]$ cd dir1
-bash: cd: dir1: Отказано в доступе
[guest@vm571215 ~]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Отказано в доступе
[guest@vm571215 ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest@vm571215 ~]$
```

14. Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, знак «+», если не разрешена, знак «-». На основании заполненной таблицы определим те или иные минимально необходимые права для выполнения операций внутри директории dir1:

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
0	0	-	-	-	-	-	-	-	-
100	0	-	-	-	-	-	-	-	-
200	0	-	-	-	-	-	-	-	-
300	0	+	+	-	-	+	-	+	+
400	0	-	-	-	-	-	-	-	-
500	0	-	-	-	-	+	+	-	+
600	0	-	-	-	-	-	+	-	-
700	0	+	+	-	-	+	+	+	+
0	100	-	-	-	-	-	-	-	-
100	100	-	-	-	-	+	-	-	+
200	100	-	-	-	-	-	-	-	-
300	100	+	+	-	-	+	-	+	+
400	100	-	-	-	-	-	+	-	-
500	100	-	-	-	-	+	+	-	+
600	100	-	-	-	-	-	+	-	-
700	100	+	+	-	-	+	+	+	+
0	200	-	-	-	-	-	-	-	-
100	200	-	-	+	-	+	-	-	+
200	200	-	-	-	-	-	-	-	-
300	200	+	+	-	-	+	-	-	+
400	200	-	-	-	-	-	+	-	-
500	200	-	-	+	-	+	+	-	+
600	200	-	-	-	-	-	+	-	-
700	200	+	+	+	-	+	+	+	+
0	300	-	-	-	-	-	-	-	-
100	300	-	-	-	-	+	-	-	+
200	300	-	-	-	-	-	-	-	-
300	300	+	+	+	-	+	-	+	+
400	300	-	-	-	-	-	+	-	-
500	300	-	-	-	-	+	+	-	+
600	300	-	-	-	-	-	+	-	-
700	300	+	+	+	-	+	+	+	+
0	400	-	-	-	-	-	-	-	-
100	400	-	-	-	+	+	-	-	+
200	400	-	-	-	-	-	-	-	-
300	400	+	+	-	+	+	-	+	+
400	400	-	-	-	-	+	-	-	-
500	400	-	-	-	+	+	-	-	+
600	400	-	-	-	-	-	+	-	-
700	400	+	+	-	-	+	+	+	+
0	500	-	-	-	-	-	-	-	-
100	500	-	-	-	-	-	-	-	-
200	500	-	-	-	-	-	-	-	-
300	500	+	+	-	+	+	-	+	+
400	500	-	-	-	-	-	+	-	-
500	500	-	-	-	-	-	+	-	+
600	500	-	-	-	-	-	-	-	-
700	500	+	+	-	+	+	+	+	+
0	600	-	-	-	-	-	-	-	-
100	600	-	-	-	+	+	-	-	+
200	600	-	-	-	-	-	-	-	-
300	600	+	+	+	+	+	-	+	+
400	600	-	-	-	-	-	-	-	-
500	600	-	-	+	+	+	-	-	+
600	600	-	-	-	-	-	+	-	-
700	600	+	+	+	+	+	+	+	+
0	700	-	-	-	-	-	-	-	-
100	700	-	-	+	+	+	-	-	+
200	700	-	-	-	-	-	-	-	-
300	700	+	+	+	+	+	-	+	+
400	700	-	-	-	-	-	+	-	-
500	700	-	-	-	-	+	-	-	+
600	700	-	-	-	-	-	+	-	-
700	700	+	+	+	+	+	+	+	+

Таблица 2.1

Минимальные права для совершения операций		
Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	"300"	"000"
Удаление файла	"300"	"000"
Чтение файла	"100"	"400"
Запись в файл	"100"	"200"
Переименование файла	"300"	"000"
Создание поддиректории	"300"	"000"
Удаление поддиректории	"300"	"000"

Таблица 2.2

### Вывод:

В ходе выполнения лабораторной работы были приобретены практические навыки работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.