

# **Отчет по лабораторной работе №2**

**по предмету Информационная безопасность**

Алхимова Дарья Сергеевна

# Содержание

Цель работы	4
Задание	5
Выполнение лабораторной работы	7
Выводы	27
Список литературы	28

# Список иллюстраций

1	Создание пользователя . . . . .	7
2	Установка пароля для пользователя . . . . .	8
3	Название, тип ОС и размер памяти для ВМ . . . . .	8
4	Проверка текущей директории . . . . .	9
5	Имя пользователя . . . . .	10
6	Информация о пользователях командой id . . . . .	11
7	Сравнение id и приглашения командной строки . . . . .	12
8	Файл passwd 1/2 . . . . .	13
9	Файл passwd 2/2 . . . . .	13
10	Файл passwd 2/2 . . . . .	14
11	Определение существующих директорий . . . . .	14
12	Расширенные атрибуты директорий . . . . .	14
13	Создание поддиректории . . . . .	15
14	Снятие атрибутов директории . . . . .	15
15	Создание файла в директории . . . . .	16
16	Создание файла в директории . . . . .	16

## Цель работы

Целью данной работы является 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.

# Задание

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя `guest` (используя учётную запись администратора): `useradd guest`.
2. Задайте пароль для пользователя `guest` (используя учётную запись администратора): `passwd guest`.
3. Войдите в систему от имени пользователя `guest`.
4. Определите директорию, в которой вы находитесь, командой `pwd`. Сравните её с приглашением командной строки. Определите, является ли она вашей домашней директорией? Если нет, зайдите в домашнюю директорию.
5. Уточните имя вашего пользователя командой `whoami`.
6. Уточните имя вашего пользователя, его группу, а так же группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомните. Сравните вывод `id` с выводом команды `groups`.
7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки.
8. Просмотрите файл `/etc/passwd` командой `cat /etc/passwd` Найдите в нём свою учётную запись. Определите `uid` пользователя. Определите `gid` пользователя. Сравните найденные значения с полученными в предыдущих пунктах. Замечание: в случае, когда вывод команды не умещается на одном экране монитора, используйте прокрутку вверх–вниз (удерживая клавишу `shift`, нажимайте `page up` и `page down`) либо программу `grep` в

- качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания: `cat /etc/passwd | grep guest`.
9. Определите существующие в системе директории командой `ls -l /home/`. Удалось ли вам получить список поддиректорий директории `/home`? Какие права установлены на директориях?
  10. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home`. Удалось ли вам увидеть расширенные атрибуты директории? Удалось ли вам увидеть расширенные атрибуты директорий других пользователей?
  11. Создайте в домашней директории поддиректорию `dir1` командой `mkdir dir1`. Определите командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`.
  12. Снимите с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверьте с её помощью правильность выполнения команды `ls -l`.
  13. Попробуйте создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1` Объясните, почему вы получили отказ в выполнении операции по созданию файла? Оцените, как сообщение об ошибке отразилось на создании файла? Проверьте командой `ls -l /home/guest/dir1`, действительно ли файл `file1` не находится внутри директории `dir1`.
  14. Заполните таблицу «Установленные права и разрешённые действия» (см. табл. 2.1), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-».
  15. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории `dir1`, заполните табл. 2.2.

# Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создай учётную запись пользователя guest (используя учётную запись администратора):

`useradd guest` (рис. 1)

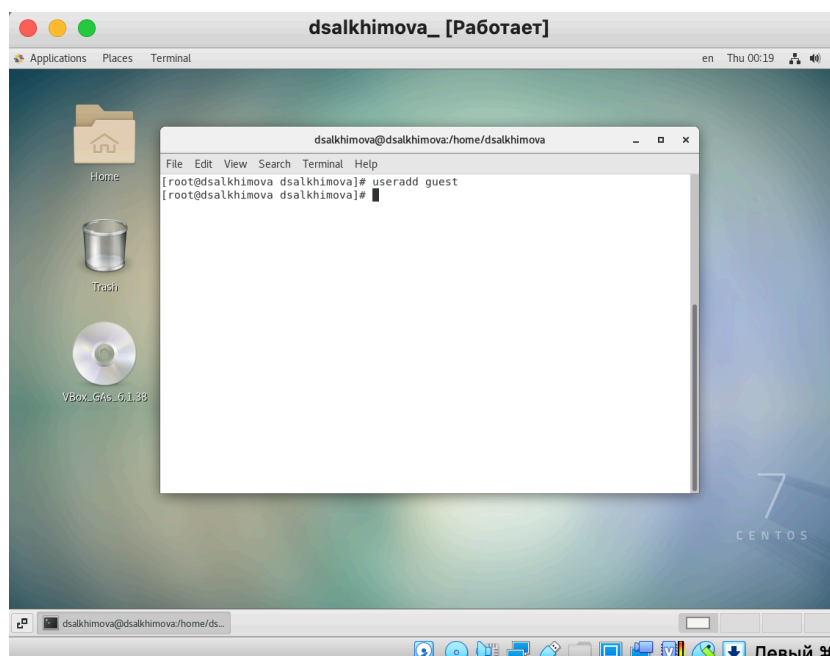


Рис. 1: Создание пользователя

2. Задала пароль для пользователя guest (используя учётную запись администратора): `passwd guest` (рис. 2)

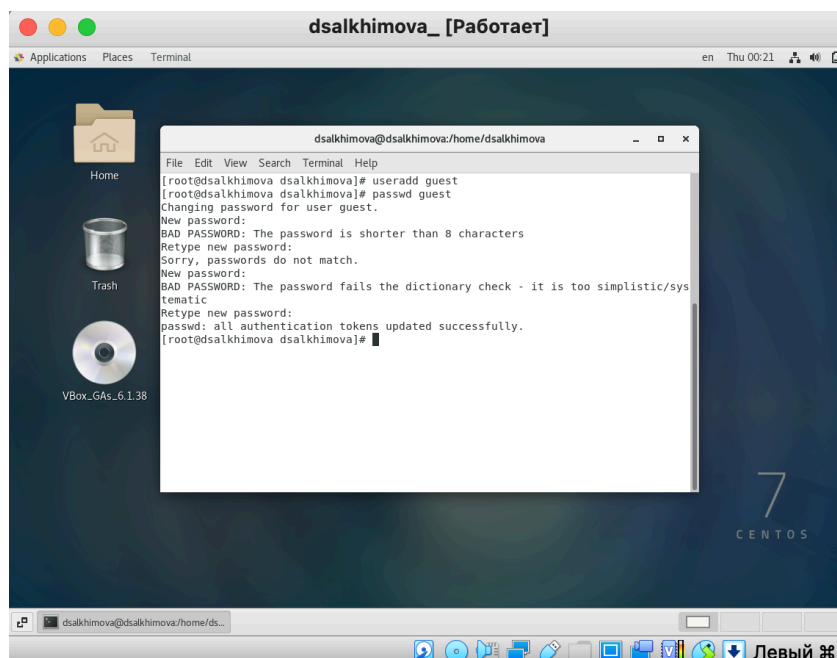


Рис. 2: Установка пароля для пользователя

3. Вошла в систему от имени пользователя guest. (рис. 3)

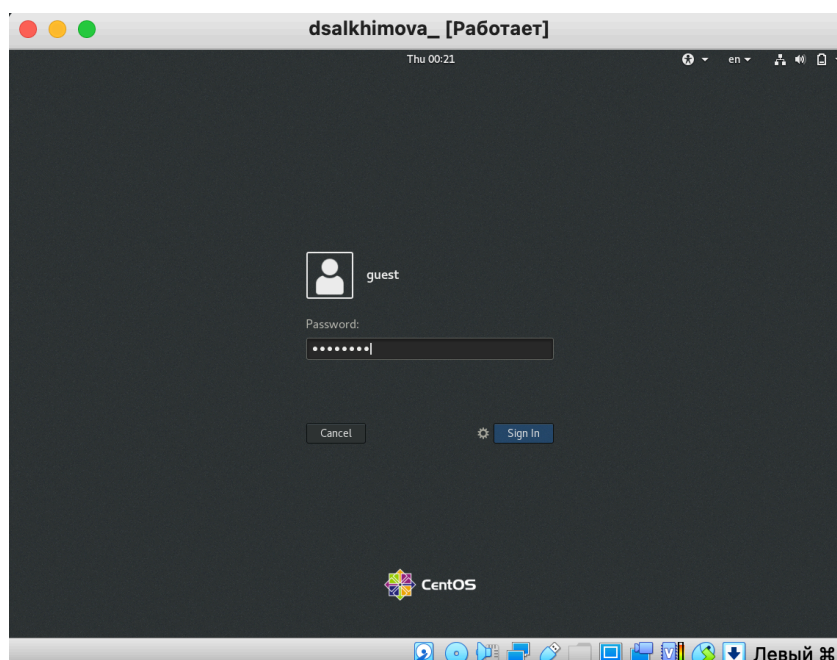


Рис. 3: Название, тип ОС и размер памяти для VM



4. Определила директорию, в которой я нахожусь, командой `pwd`. Данная директория является моей домашней директорией. (рис. 4)

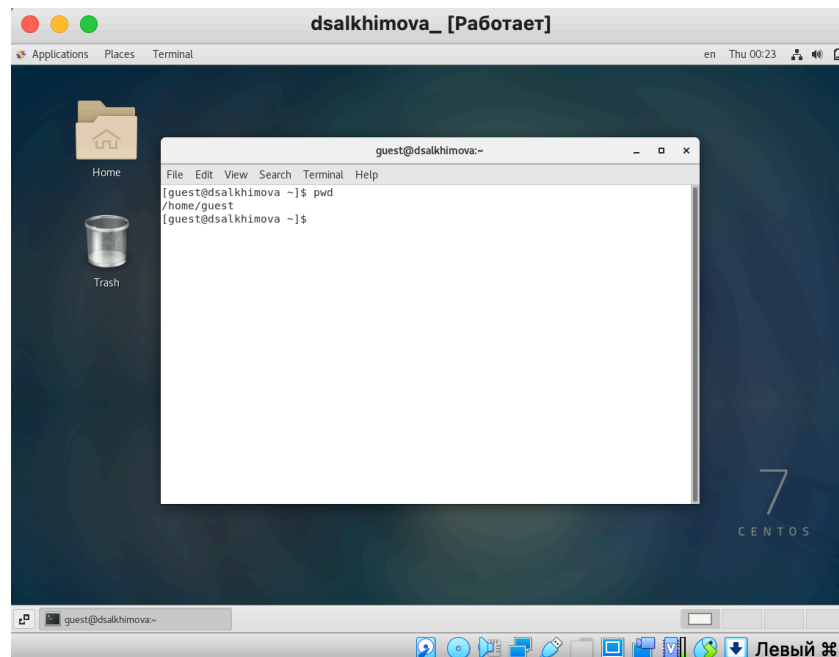


Рис. 4: Проверка текущей директории

5. Уточнила имя моего пользователя командой `whoami`. (рис. 5)

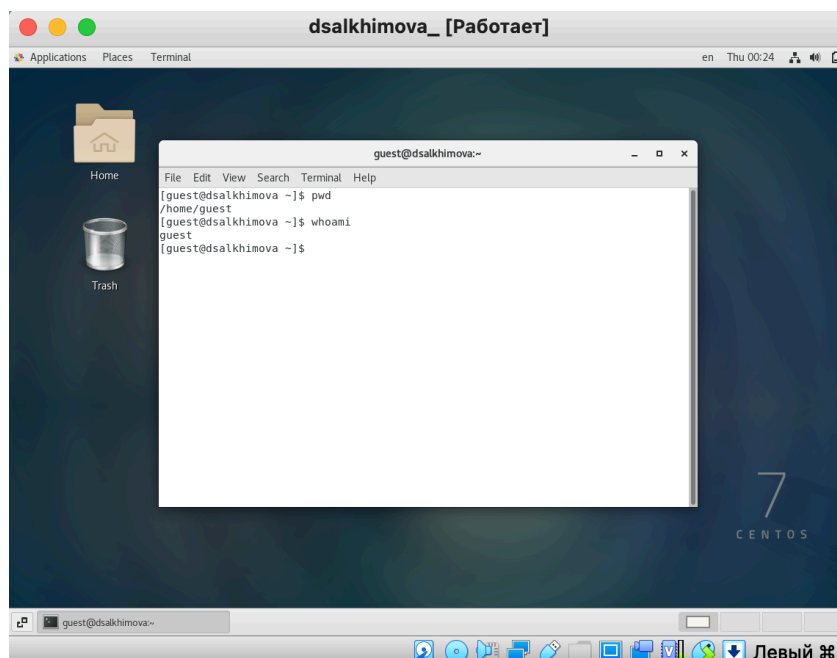


Рис. 5: Имя пользователя

6. Уточнила имя моего пользователя, его группу, а так же группы, куда входит пользователь, командой `id`. Вывод `id` содержит больше информации, чем вывод команды `groups`. (рис. 6)

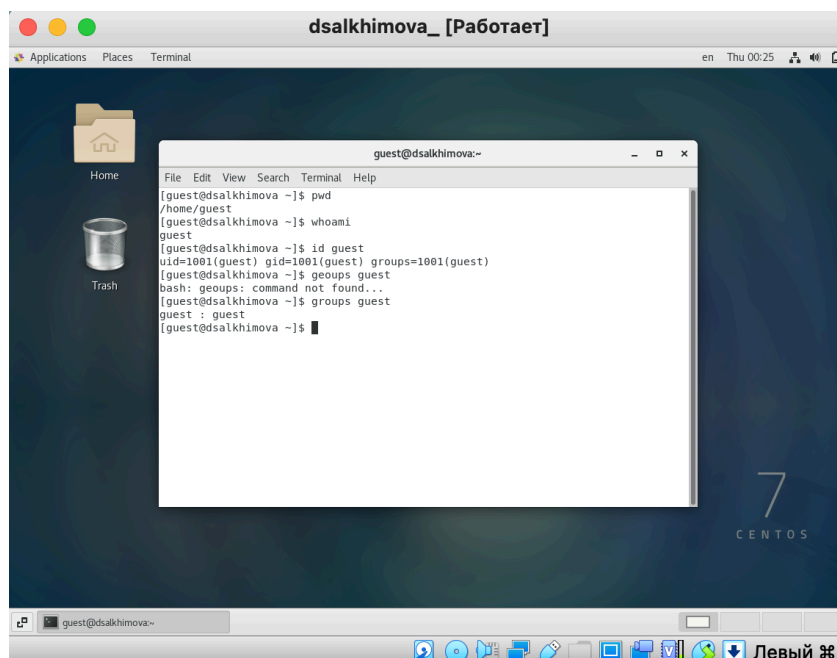


Рис. 6: Информация о пользователях командой id

7. Сравнила полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. (рис. 7)

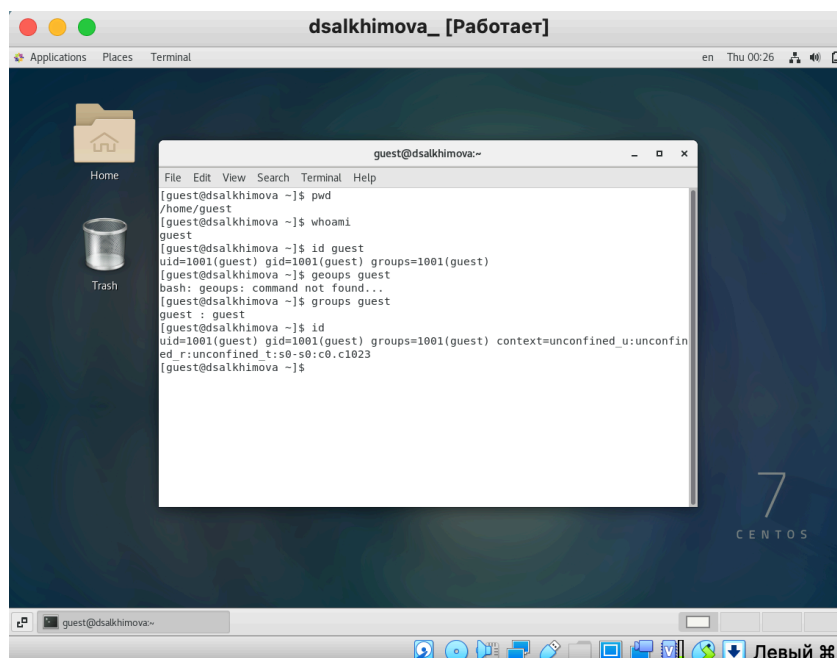


Рис. 7: Сравнение id и приглашения командной строки

8. Просмотрела файл `/etc/passwd` командой `cat /etc/passwd`. Нашла в нём свою учётную запись. Определила `uid` и `gid` пользователя: `1001(guest)`. Найденные значения совпадают с полученными в предыдущих пунктах. (рис. 8, рис. 9)

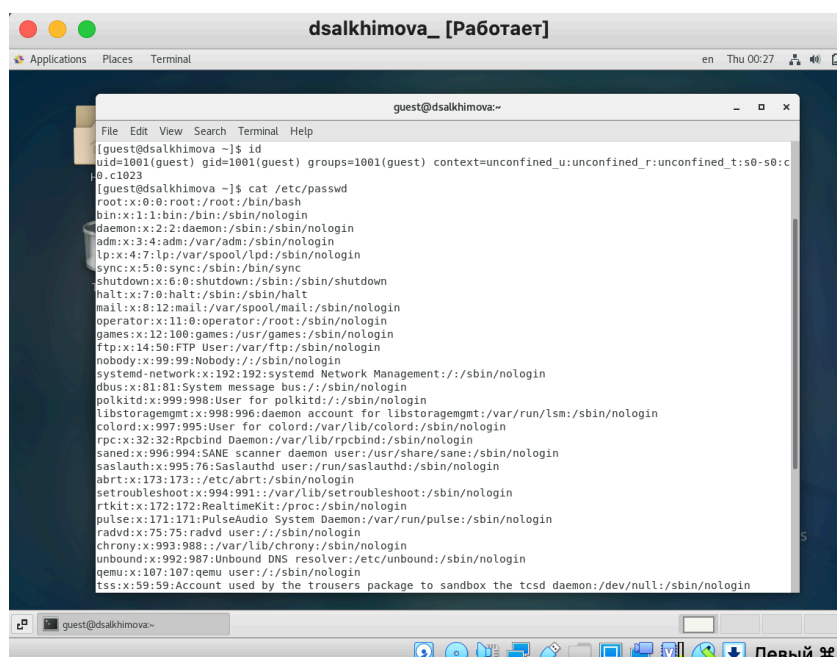


Рис. 8: Файл passwd 1/2

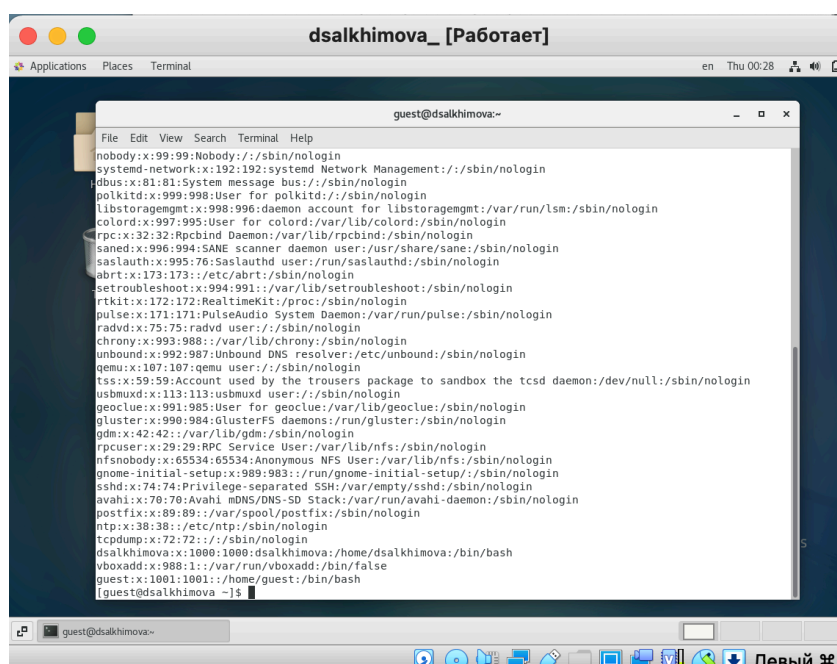


Рис. 9: Файл passwd 2/2

Использовала программу ggrep в качестве фильтра для вывода только строк,

содержащих определённые буквенные сочетания: `cat /etc/passwd | grep guest`. (рис. 10)

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

Рис. 10: Файл passwd 2/2

9. Определила существующие в системе директории командой `ls -l /home/`. Получить список поддиректорий директории `/home` не удалось, вывело только общее количество. На директориях установлены права на чтение, запись и исполнение есть только для владельцев (рис. 11)

```
[guest@dsalkhimova ~]$ ls -l /home/
total 8
drwx----- 15 dsalkhimova dsalkhimova 4096 Sep  8 08:00 dsalkhimova
drwx----- 15 guest          guest      4096 Sep 15 00:22 guest
[guest@dsalkhimova ~]$
```

Рис. 11: Определение существующих директорий

10. Проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой `lsattr /home`. Доступ к расширенным атрибутам директории, а также директорий других пользователей был запрещен. (рис. 12)

```
-----
[guest@dsalkhimova ~]$ lsattr /home
lsattr: Permission denied while reading flags on /home/dsalkhimova
-----
[guest@dsalkhimova ~]$
```

Рис. 12: Расширенные атрибуты директорий

11. Создала в домашней директории поддиректорию `dir1` командой `mkdir dir1`.  
Определила командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`. (рис. 13)

```
[guest@dsalkhimova ~]$ mkdir dir1
[guest@dsalkhimova ~]$ cd dir1
[guest@dsalkhimova dir1]$ ls -l
total 0
[guest@dsalkhimova dir1]$ cd ..
[guest@dsalkhimova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Desktop
drwxr-xr-x. 2 guest guest 6 Sep 15 00:34 dir1
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Documents
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Music
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Public
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Templates
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Videos
[guest@dsalkhimova ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@dsalkhimova ~]$
```

Рис. 13: Создание поддиректории

12. Сняла с директории dir1 все атрибуты командой `chmod 000 dir1` и проверила с её помощью правильность выполнения команды `ls -l`. Права стали удалены у всех пользователей. (рис. 14)

```
[guest@dsalkhimova ~]$ chmod 000 dir1
[guest@dsalkhimova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Desktop
d------. 2 guest guest 6 Sep 15 00:34 dir1
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Documents
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Music
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Public
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Templates
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Videos
[guest@dsalkhimova ~]$
```

Рис. 14: Снятие атрибутов директории

13. Попыталась создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1` и получила отказ в выполнении операции по созданию файла, поскольку на предыдущем шаге я убрала все права с директории dir1. Файл не был создан. (рис. 15)

```
[guest@dsalkhimova ~]$ chmod 000 dir1
[guest@dsalkhimova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Desktop
d-----.. 2 guest guest 6 Sep 15 00:34 dir1
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Documents
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Music
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Public
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Templates
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Videos
[guest@dsalkhimova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@dsalkhimova ~]$ ls -l /home/guest/dir1/file1
ls: cannot access /home/guest/dir1/file1: Permission denied
[guest@dsalkhimova ~]$ ls -l /home/guest/dir1
ls: cannot open directory /home/guest/dir1: Permission denied
[guest@dsalkhimova ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@dsalkhimova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Desktop
d-----.. 2 guest guest 6 Sep 15 00:34 dir1
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Documents
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Music
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Public
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Templates
drwxr-xr-x. 2 guest guest 6 Sep 15 00:22 Videos
[guest@dsalkhimova ~]$
```

Рис. 15: Создание файла в директории

Проверила командой `ls -l /home/guest/dir1`, что файл `file1` действительно не находится внутри директории `dir1`. (рис. 16)

```
[guest@dsalkhimova ~]$ chmod 777 dir1
[guest@dsalkhimova ~]$ cd dir1
[guest@dsalkhimova dir1]$ ls -l
total 0
[guest@dsalkhimova dir1]$
```

Рис. 16: Создание файла в директории

14. Заполнила 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, заносила в таблицу знак «+», если не разрешена, знак «-». [-@tbl:attr]



		Права							
		Соз- да- ние фай- ла		Уда- ле- ние фай- ла		Запись в файл		Чтение фай- ла	
		Смена дирек- то- рии		Смена лов в ди- рек- то- рии		Просмотр фай- лов		Пере- имено- ва- ние фай- ла	
Права дирек- тории	Права файла	фай- ла	фай- ла	фай- ла	фай- ла	фай- ла	фай- ла	фай- ла	фай- ла
d-----	-----	-	-	-	-	-	-	-	-
(000)	(000)								
d--x--	-----	-	-	-	-	+	-	-	+
(100)	(000)								
d-w---	-----	-	-	-	-	-	-	-	-
(200)	(000)								
d-wx--	-----	+	+	-	-	+	-	+	+
(300)	(000)								
dr----	-----	-	-	-	-	-	-	-	-
(400)	(000)								
dr-x--	-----	-	-	-	-	+	+	-	+
(500)	(000)								
drw---	-----	-	-	-	-	-	-	-	-
(600)	(000)								

		Права доступа								
		Просмотр		Передача		Смена дирек-		Смена атри-		
		фай-	имено-	лов в	ва-	атри-				
Права дирек-	Права файла	Соз-да-ние фай-ла	Уда-ле-ние фай-ла	Запись в файл	Чтение фай-ла	Смена дирек-рии	ди-рек-рии	не фай-ла	бутов фай-ла	
drwx--	-----	+	+	-	-	+	+	+	+	
----	----									
(700)	(000)									
d-----	---x--	-	-	-	-	-	-	-	-	
----	----									
(000)	(100)									
d--x--	---x--	-	-	-	-	+	-	-	+	
----	----									
(100)	(100)									
d-w---	---x--	-	-	-	-	-	-	-	-	
----	----									
(200)	(100)									
d-wx--	---x--	+	+	-	-	+	-	+	+	
----	----									
(300)	(100)									
dr----	---x--	-	-	-	-	-	-	-	-	
----	----									
(400)	(100)									
dr-x--	---x--	-	-	-	-	+	+	-	+	
----	----									
(500)	(100)									

		Просмотр							
		фай-				имено-			
		Соз-	Уда-			Смена	лов в		
		да-	ле-			дирек-	ди-	ва-	атри-
Права		ние	ние	Запись	Чтение		рек-	ние	бутов
дирек-	Права	фай-	фай-	в	фай-	то-	то-	фай-	фай-
тории	файла	ла	ла	файл	ла	рии	рии	ла	ла
drw---	---x--	-	-	-	-	-	-	-	-
----	----								
(600)	(100)								
drwx--	---x--	+	+	-	-	+	+	+	+
----	----								
(700)	(100)								
d-----	--w---	-	-	-	-	-	-	-	-
----	----								
(000)	(200)								
d--x--	--w---	-	-	+	-	+	-	-	+
----	----								
(100)	(200)								
d-w---	--w---	-	-	-	-	-	-	-	-
----	----								
(200)	(200)								
d-wx--	--w---	+	+	+	-	+	-	+	+
----	----								
(300)	(200)								
dr-----	--w---	-	-	-	-	-	-	-	-
----	----								
(400)	(200)								

		Права							
		Соз- да- ние фай- ла		Уда- ле- ние фай- ла		Запись в файл		Чтение фай- ла	
		Смена дирек- то- рии		Смена лов в ди- рек- то- рии		Просмотр фай- лов		Пере- имено- ва- ние фай- ла	
Права дирек- тории	Права файла	фай- ла	фай- ла	фай- ла	фай- ла	фай- ла	фай- ла	фай- ла	фай- ла
dr-x--	--w---	-	-	+	-	+	+	-	+
----	----								
(500)	(200)								
drw---	--w---	-	-	-	-	-	-	-	-
----	----								
(600)	(200)								
drwx--	--w---	+	+	+	-	+	+	+	+
----	----								
(700)	(200)								
d-----	--wx--	-	-	-	-	-	-	-	-
----	----								
(000)	(300)								
d--x--	--wx--	-	-	+	-	+	-	-	+
----	----								
(100)	(300)								
d-w---	--wx--	-	-	-	-	-	-	-	-
----	----								
(200)	(300)								
d-wx--	--wx--	+	+	+	-	+	-	+	+
----	----								
(300)	(300)								

		Просмотр							
		фай-				имено-			
		Соз-	Уда-			Смена	лов в		
		да-	ле-			дирек-	ди-	ва-	атри-
Права		ние	ние	Запись	Чтение		рек-	ние	бутов
дирек-	Права	фай-	фай-	в	фай-	то-	то-	фай-	фай-
тории	файла	ла	ла	файл	ла	рии	рии	ла	ла
dr----	--wx--	-	-	-	-	-	-	-	-
(400)	(300)								
dr-x--	--wx--	-	-	+	-	+	+	-	+
(500)	(300)								
drw---	--wx--	-	-	-	-	-	-	-	-
(600)	(300)								
drwx--	--wx--	+	+	+	-	+	+	+	+
(700)	(300)								
d-----	-r-----	-	-	-	-	-	-	-	-
(000)	(400)								
d--x--	-r-----	-	-	-	+	+	-	-	+
(100)	(400)								
d-w---	-r-----	-	-	-	-	-	-	-	-
(200)	(400)								

		Права							
		Соз- да- ние фай- ла		Уда- ле- ние фай- ла		Запись в файл		Чтение фай- ла	
		Смена дирек- то- рии		Смена лов в ди- рек- то- рии		Просмотр фай- лов		Пере- имено- вание фай- ла	
Права дирек- тории	Права файла	фай- ла	фай- ла	файл	фай- ла	то- рии	то- рии	фай- ла	фай- ла
d-wx--	-r----	+	+	-	+	+	-	+	+
----	----								
(300)	(400)								
dr----	-r----	-	-	-	-	-	-	-	-
----	----								
(400)	(400)								
dr-x--	-r----	-	-	-	+	+	+	-	+
----	----								
(500)	(400)								
drw---	-r----	-	-	-	-	-	-	-	-
----	----								
(600)	(400)								
drwx--	-r----	+	+	-	+	+	+	+	+
----	----								
(700)	(400)								
d-----	-r-x--	-	-	-	-	-	-	-	-
----	----								
(000)	(500)								
d--x--	-r-x--	-	-	-	+	+	-	-	+
----	----								
(100)	(500)								

		Права							
Права дирек- тории	Права файла	Соз- да- ние фай- ла		Уда- ле- ние фай- ла		Запись в файл		Чтение фай- ла	
		Просмо- тр фай- лов в ди- рек- то- рии		Пере- имено- ва- ние фай- ла		Смена дирек- то- рии		Смена атри- бутов фай- ла	
d-w---	-r-x--	-	-	-	-	-	-	-	-
----	----								
(200)	(500)								
d-wx--	-r-x--	+	+	-	+	+	-	+	+
----	----								
(300)	(500)								
dr----	-r-x--	-	-	-	-	-	-	-	-
----	----								
(400)	(500)								
dr-x--	-r-x--	-	-	-	+	+	+	-	+
----	----								
(500)	(500)								
drw---	-r-x--	-	-	-	-	-	-	-	-
----	----								
(600)	(500)								
drwx--	-r-x--	+	+	-	+	+	+	+	+
----	----								
(700)	(500)								
d-----	-rw---	-	-	-	-	-	-	-	-
----	----								
(000)	(600)								

		Права							
Права дирек- тории	Права файла	Соз- да- ние фай- ла		Уда- ле- ние фай- ла		Запись в файл		Чтение фай- ла	
		Просмо- тр фай- лов в ди- рек- то- рии		Пере- имено- ва- ние фай- ла		Смена дирек- то- рии		Смена атри- бутов фай- ла	
d--x--	-rw---	-	-	-	-	+	+	+	+
----	----								
(100)	(600)								
d-w---	-rw---	-	-	-	-	-	-	-	-
----	----								
(200)	(600)								
d-wx--	-rw---	+	+	+	+	+	-	+	+
----	----								
(300)	(600)								
dr----	-rw---	-	-	-	-	-	-	-	-
----	----								
(400)	(600)								
dr-x--	-rw---	-	-	+	+	+	+	-	+
----	----								
(500)	(600)								
drw---	-rw---	-	-	-	-	-	-	-	-
----	----								
(600)	(600)								
drwx--	-rw---	+	+	+	+	+	+	+	+
----	----								
(700)	(600)								



		Права							
		Соз- да- ние фай- ла		Уда- ле- ние фай- ла		Запись в файл		Чтение фай- ла	
		Смена дирек- то- рии		Смена лов в ди- ва- ние фай- ла		Смена атри- бутов фай- ла			
Права дирек- тории	Права файла	фай- ла	фай- ла	фай- ла	фай- ла	фай- ла	фай- ла	фай- ла	фай- ла
d-----	-rwx--	-	-	-	-	-	-	-	-
(000)	(700)								
d--x--	-rwx--	-	-	+	+	+	-	-	+
(100)	(700)								
d-w---	-rwx--	-	-	-	-	-	-	-	-
(200)	(700)								
d-wx--	-rwx--	+	+	+	+	+	-	+	+
(300)	(700)								
dr----	-rwx--	-	-	-	-	-	-	-	-
(400)	(700)								
dr-x--	-rwx--	-	-	+	+	+	+	-	+
(500)	(700)								
drw---	-rwx--	-	-	-	-	-	-	-	-
(600)	(700)								

		<div>Просмотр файла</div> <div>Переименование</div> <div>Смена атрибутов</div>							
Права дирек-	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Смена директории	Смена директории	Смена директории
drwx--	-rwx--	+	+	+	+	+	+	+	+
----	----								
(700)	(700)								

15. На основании заполненной таблицы определила минимально необходимые права для выполнения операций внутри директории dir1 и занесла данные в табл.2[#tbl:min].

Операция	Мин. права на директорию	Мин. 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)

## Выводы

В процессе выполнения данной лабораторной работы я получила практические навыки работы в консоли с атрибутами файлов, а также закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.

## Список литературы

1. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: <http://bugtraq.ru/library/books/attack1/index.html>
2. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. — Издательство ДМК, 1999. — URL: <http://bugtraq.ru/library/books/attack/index.html>
3. Запечников С. В. и др. Информационная безопасность открытых систем. Том 1. — М.: Горячая линия -Телеком, 2006.