

# **Отчёт по лабораторной работе №2**

**Дискреционное разграничение прав в Linux. Основные атрибуты**

Ханина Ирина Владимировна, НБИбд-02-18

# Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	23
	Список литературы	24

## List of Tables

4.1	Установленные права и разрешённые действия . . . . .	18
4.2	Минимальные права для совершения операций . . . . .	21

# List of Figures

4.1	Рис 1. Команда <code>useradd guest1</code> . . . . .	9
4.2	Рис 2. Команда <code>passwd guest1</code> . . . . .	10
4.3	Рис 3. Вход в систему от имени пользователя <code>guest1</code> . . . . .	10
4.4	Рис 4. Команда <code>pwd</code> . . . . .	11
4.5	Рис 5. Команда <code>whoami</code> . . . . .	12
4.6	Рис 6. Команда <code>id</code> . . . . .	13
4.7	Рис 7. Команда <code>groups</code> . . . . .	13
4.8	Рис 8. Команда <code>cat /etc/passwd</code> . . . . .	14
4.9	Рис 9. Содержимое файла <code>/etc/passwd</code> . . . . .	15
4.10	Рис 10. Список поддиректорий директории <code>/home</code> . . . . .	15
4.11	Рис 11. Расширенные атрибуты, установленные на поддиректориях, находящихся в директории <code>/home</code> . . . . .	16
4.12	Рис 12. Команды <code>mkdir dir1</code> и <code>ls -l</code> . . . . .	16
4.13	Рис 13. Команда <code>lsattr</code> . . . . .	16
4.14	Рис 14. Команда <code>chmod 000 dir1</code> . . . . .	16
4.15	Рис 15. Попытка создания в директории <code>dir1</code> файла <code>file1</code> . . . . .	17
4.16	Рис 16. Создание в директории <code>dir1</code> тестового файла <code>file1</code> . . . . .	17
4.17	Рис 17. Заполнение таблицы и проверка разрешённых действий .	18
4.18	Рис 17. Минимальные права для создания и удаления поддиректорий	21

# 1 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 Linux.

## 2 Задание

Получить практические навыки работы в консоли с атрибутами файлов и закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

### 3 Теоретическое введение

Операционные системы семейства Unix, такие как Linux, отличаются от большинства остальных тем, что они не только многозадачные, но и многопользовательские. Возможность многопользовательской работы глубоко интегрирована в архитектуру операционной системы Linux. В Linux, как и в любой многопользовательской системе, возникает задача разграничения доступа субъектов к объектам. Один из подходов к разграничению доступа — дискреционный. Он предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов к объектам, которыми владеют. [2]

В операционной системе Linux каждому файлу и директории заданы разрешения доступа для владельца файла, членов группы владельца файла и всех остальных пользователей. Права могут быть заданы на:

- чтение (r);
- запись (w);
- выполнение (x).[1]

Информация о разрешениях в выводе прав доступа содержит символ, определяющий тип файла (-, если обычный файл, d, если директория). Далее идет три набора из трех символов, которые представляют права доступа. Первый набор из трех символов указывает права доступа владельца файла, второй — права группы файла, а последний указывает права доступа файла для всех остальных пользователей. [1]

Сменить разрешения доступа к файлу или директории можно с помощью

команды `chmod`. Для этого нужно указать желаемые настройки прав доступа для файла, файлов или директории, которые нужно изменить.



## 4 Выполнение лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе с помощью команды `useradd guest1`, используя учётную запись администратора, я создала учётную запись пользователя `guest1`. (рис. 1)

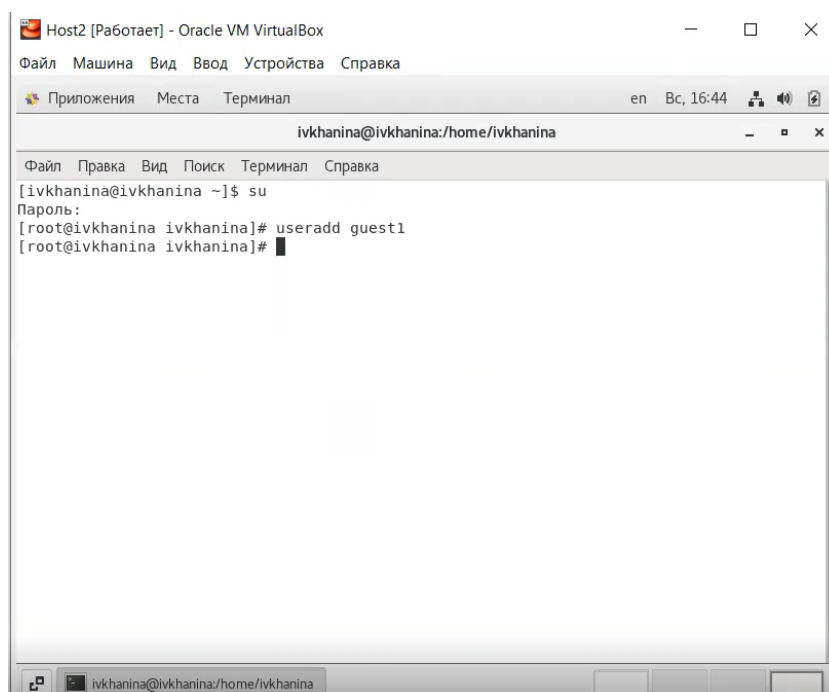


Figure 4.1: Рис 1. Команда `useradd guest1`

Далее, используя учётную запись администратора, я задала пароль для пользователя `guest1` с помощью команды `passwd guest1`. (рис. 2)

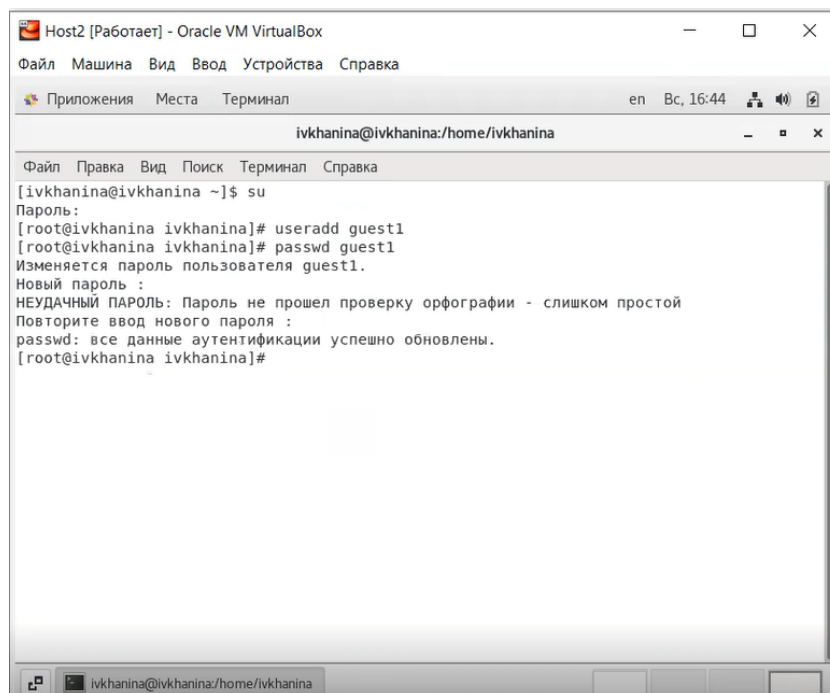


Figure 4.2: Рис 2. Команда passwd guest1

Я вошла в систему от имени пользователя guest1. (рис. 3)

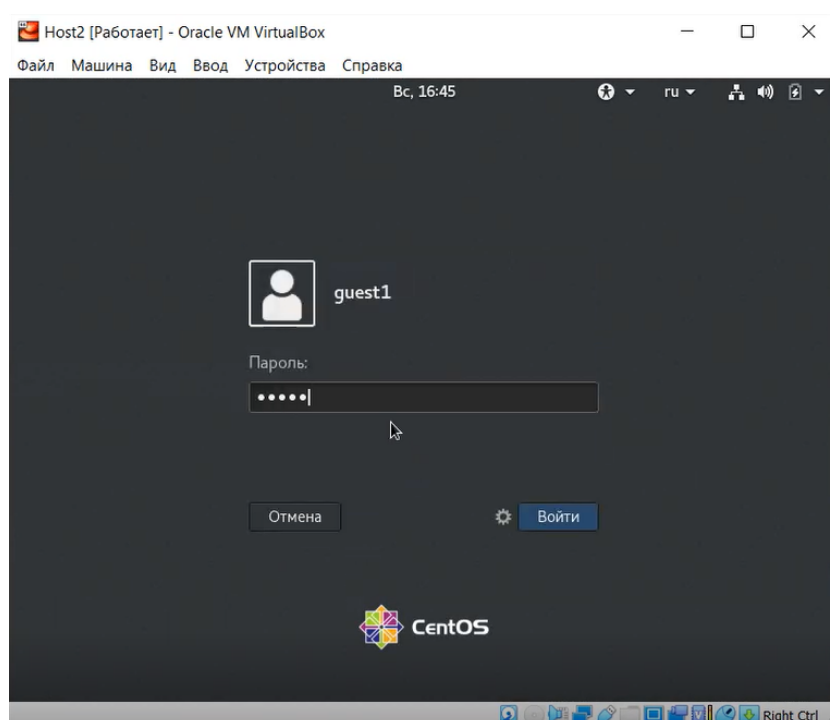


Figure 4.3: Рис 3. Вход в систему от имени пользователя guest1

Запустила терминал, командой `pwd` определила директорию, в которой я находилась, и сравнила её с приглашением командной строки. Она являлась моей домашней директорией. (рис. 4)

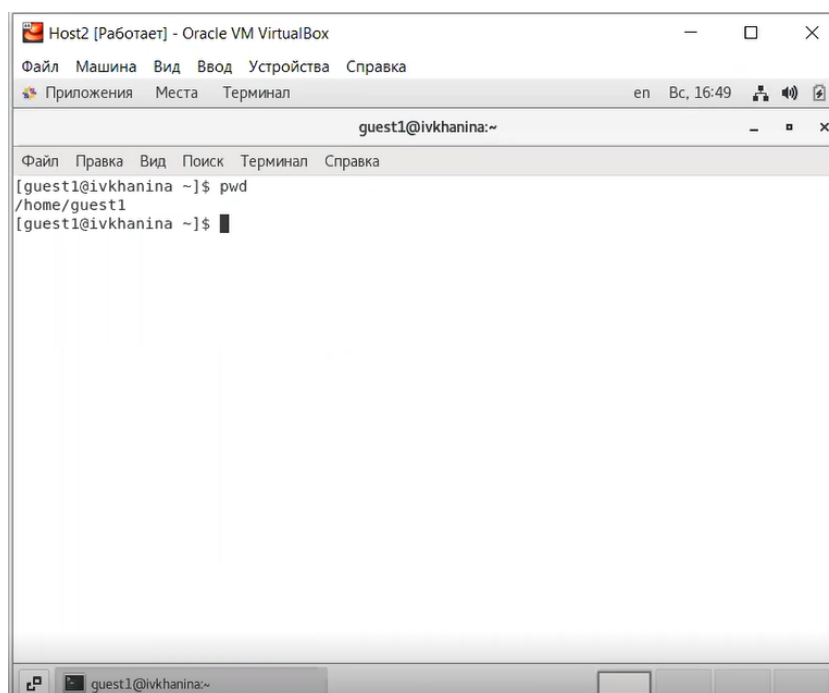


Figure 4.4: Рис 4. Команда `pwd`

Я уточнила имя пользователя, введя команду `whoami`. (рис. 5)

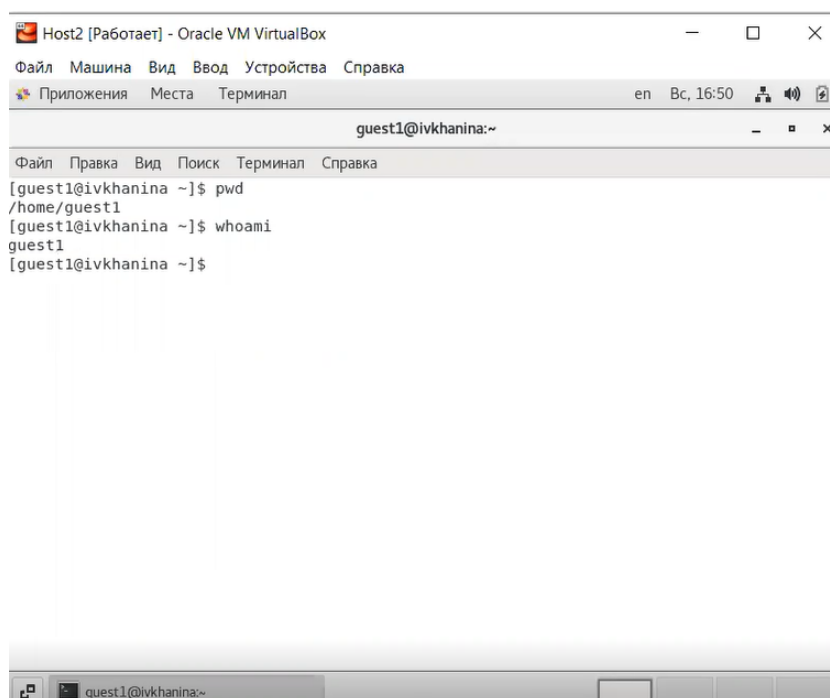
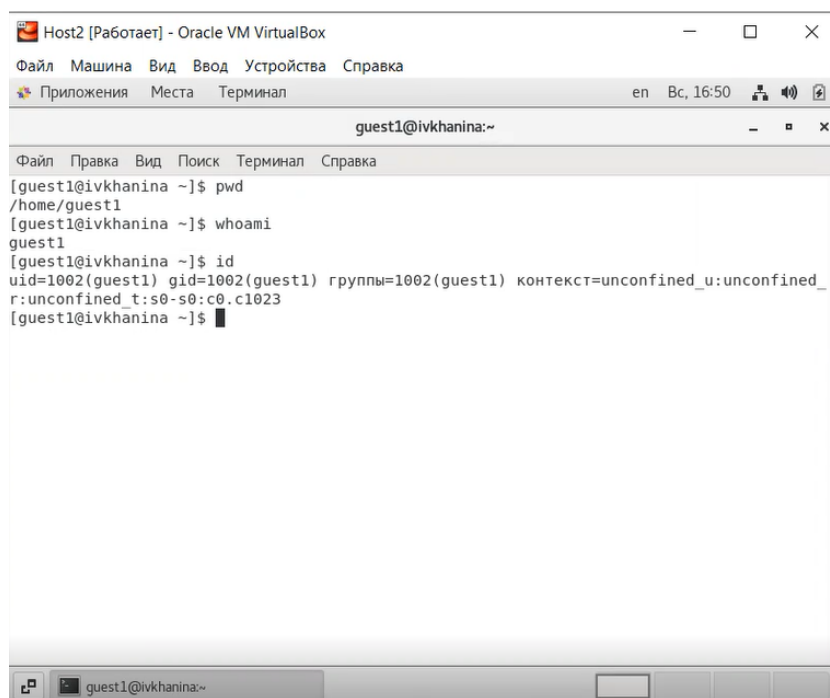


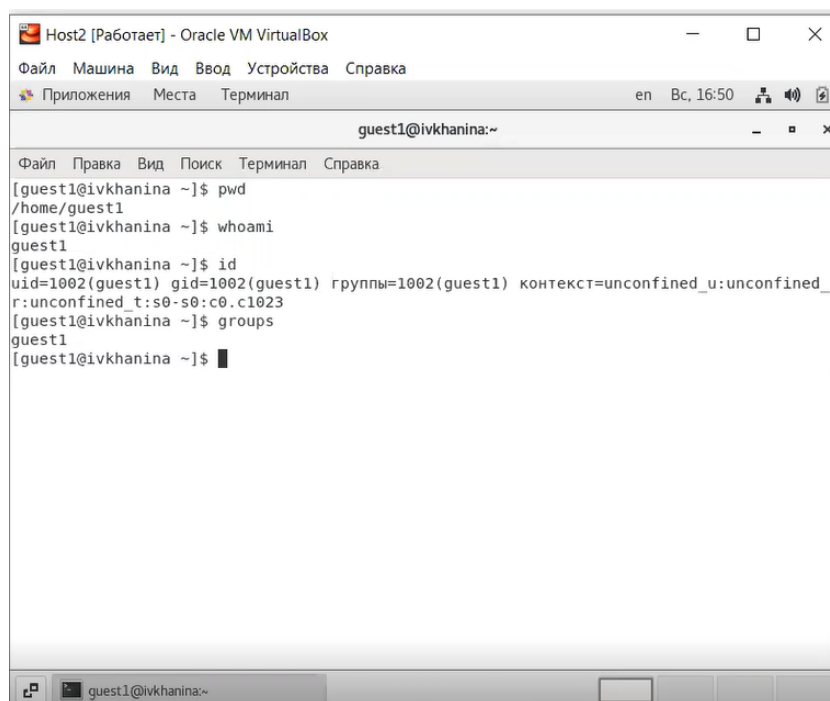
Figure 4.5: Рис 5. Команда whoami

Я уточнила имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. (рис. 6). Выведенные значения `uid`, `gid` и др. запомнила. Сравнила вывод `id` с выводом команды `groups`: команда `id` выводит `id` пользователя, `id` его группы, а также имя группы, куда входит пользователь, а команда `groups` выводит только имя группы, куда входит пользователь. (рис. 7). Затем я сравнила полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки.



```
Host2 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Приложения Места Терминал en Вс, 16:50
guest1@ivkhanina:~
Файл Правка Вид Поиск Терминал Справка
[guest1@ivkhanina ~]$ pwd
/home/guest1
[guest1@ivkhanina ~]$ whoami
guest1
[guest1@ivkhanina ~]$ id
uid=1002(guest1) gid=1002(guest1) группы=1002(guest1) контекст=unconfined_u:unconfined_
r:unconfined_t:s0-s0:c0.c1023
[guest1@ivkhanina ~]$
```

Figure 4.6: Рис 6. Команда id

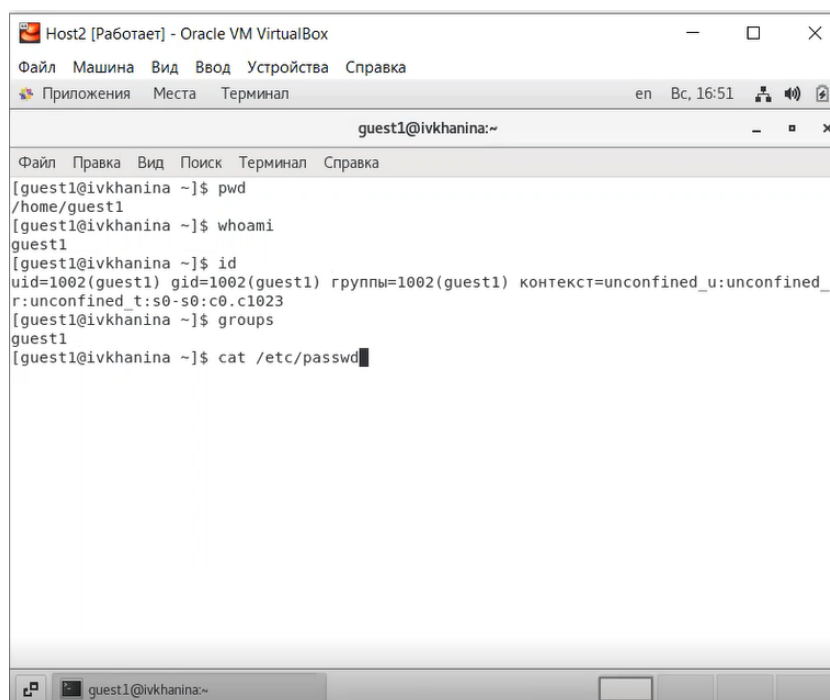


```
Host2 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Приложения Места Терминал en Вс, 16:50
guest1@ivkhanina:~
Файл Правка Вид Поиск Терминал Справка
[guest1@ivkhanina ~]$ pwd
/home/guest1
[guest1@ivkhanina ~]$ whoami
guest1
[guest1@ivkhanina ~]$ id
uid=1002(guest1) gid=1002(guest1) группы=1002(guest1) контекст=unconfined_u:unconfined_
r:unconfined_t:s0-s0:c0.c1023
[guest1@ivkhanina ~]$ groups
guest1
[guest1@ivkhanina ~]$
```

Figure 4.7: Рис 7. Команда groups

Затем я просмотрела файл /etc/passwd командой cat /etc/passwd (рис. 8), нашла

в нём свою учётную запись (рис. 9). Uid пользователя = 1002, gid пользователя = 1002. Эти значения совпадают с полученными в предыдущих пунктах.



```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Места  Терминал  en  Вс, 16:51
guest1@ivkhanina:~
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest1@ivkhanina ~]$ pwd
/home/guest1
[guest1@ivkhanina ~]$ whoami
guest1
[guest1@ivkhanina ~]$ id
uid=1002(guest1) gid=1002(guest1) группы=1002(guest1) контекст=unconfined_u:unconfined_
r:unconfined_t:s0-s0:c0.c1023
[guest1@ivkhanina ~]$ groups
guest1
[guest1@ivkhanina ~]$ cat /etc/passwd
```

Figure 4.8: Рис 8. Команда cat /etc/passwd

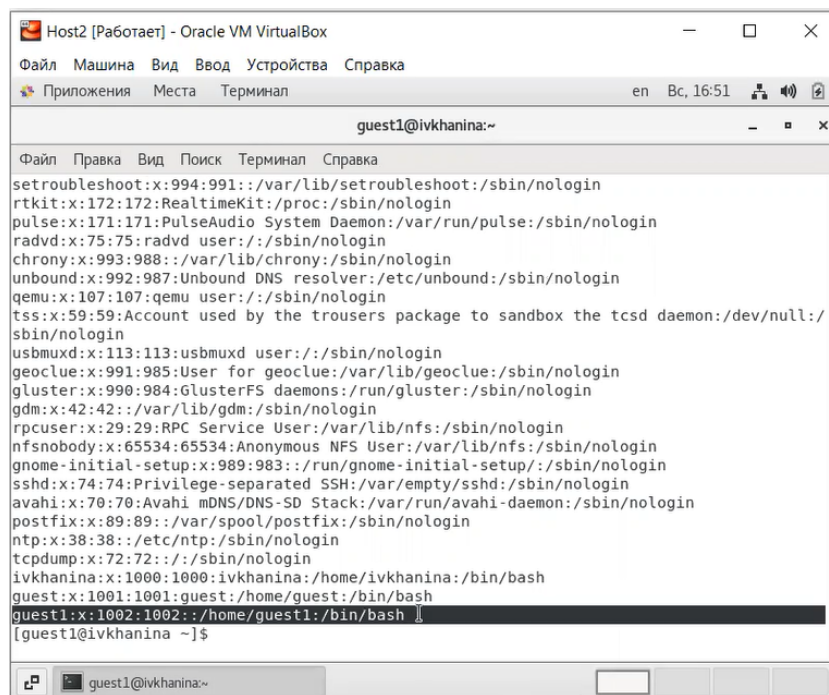


Figure 4.9: Рис 9. Содержимое файла /etc/passwd

Я определила существующие в системе директории командой `ls -l /home/` (рис. 10) и получила список поддиректорий директории /home. На обеих директориях установлены следующие права: владелец директорий обладает всеми правами (rwx), его группа и остальные пользователи не имеют никаких прав (— и —).

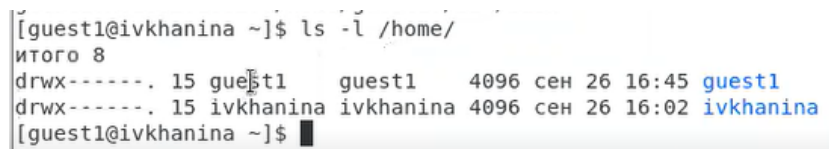


Figure 4.10: Рис 10. Список поддиректорий директории /home

С помощью команды `lsattr /home` проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home. Мне удалось увидеть расширенные атрибуты директории, но я не смогла увидеть расширенные атрибуты директорий других пользователей. (рис. 11)

```
[guest1@ivkhanina ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/ivkhanina
----- /home/guest1
[guest1@ivkhanina ~]$
```

Figure 4.11: Рис 11. Расширенные атрибуты, установленные на поддиректориях, находящихся в директории /home

Далее я создала в домашней директории поддиректорию dir1, используя команду mkdir dir1. Определила командами ls -l (рис. 12) и lsattr (рис. 13), какие права доступа и расширенные атрибуты были выставлены на директорию dir1. Владелец директории так же, как и его группа имеют все права (rwx), остальные пользователи имеют только права на чтение и исполнение (r-x).

```
[guest1@ivkhanina ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/ivkhanina
----- /home/guest1
[guest1@ivkhanina ~]$
```

Figure 4.12: Рис 12. Команды mkdir dir1 и ls -l

```
[guest1@ivkhanina ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/ivkhanina
----- /home/guest1
[guest1@ivkhanina ~]$
```

Figure 4.13: Рис 13. Команда lsattr

Сняла с директории dir1 все атрибуты командой chmod 000 dir1 и проверила правильность выполнения команды с помощью команды ls -l. (рис. 14)

```
[guest1@ivkhanina ~]$ chmod 000 dir1
[guest1@ivkhanina ~]$ ls -l
итого 0
d----- . 2 guest1 guest1 6 сен 26 16:54 dir1
drwxr-xr-x. 2 guest1 guest1 6 сен 26 16:45 Видео
drwxr-xr-x. 2 guest1 guest1 6 сен 26 16:45 Документы
drwxr-xr-x. 2 guest1 guest1 6 сен 26 16:45 Загрузки
drwxr-xr-x. 2 guest1 guest1 6 сен 26 16:45 Изображения
drwxr-xr-x. 2 guest1 guest1 6 сен 26 16:45 Музыка
drwxr-xr-x. 2 guest1 guest1 6 сен 26 16:45 Общедоступные
drwxr-xr-x. 2 guest1 guest1 6 сен 26 16:45 Рабочий стол
drwxr-xr-x. 2 guest1 guest1 6 сен 26 16:45 Шаблоны
[guest1@ivkhanina ~]$
```

Figure 4.14: Рис 14. Команда chmod 000 dir1



Я попыталась создать в директории dir1 файл file1 командой echo "test" > /home/guest1/dir1/file1. Я получила отказ в выполнении операции по созданию файла, потому что на предыдущем шаге я лишила владельца директории всех прав, включая право на запись (—). Я не смогла создать файл. Проверила командой ls -l /home/guest1/dir1, файл file1 действительно не находится внутри директории dir1. (рис. 15)

```
[guest1@ivkhanina ~]$ echo "test" > /home/guest1/dir1/file1
bash: /home/guest1/dir1/file1: Отказано в доступе
[guest1@ivkhanina ~]$ ls -l /home/guest1/dir1
ls: невозможно открыть каталог /home/guest1/dir1: Отказано в доступе
[guest1@ivkhanina ~]$
```

Figure 4.15: Рис 15. Попытка создания в директории dir1 файла file1

Для заполнения таблицы в следующем пункте я создала тестовой файл file1 в директории dir1 для того, чтобы был файл для тестирования некоторых действий. (рис. 16)

```
[guest1@ivkhanina ~]$ chmod 700 dir1
[guest1@ivkhanina ~]$ cd /home/guest1/dir1
[guest1@ivkhanina dir1]$ ls
[guest1@ivkhanina dir1]$ echo "test" > /home/guest1/dir1/file1
[guest1@ivkhanina dir1]$ ls
file1
[guest1@ivkhanina dir1]$ cat /home/guest1/dir1/file1
test
[guest1@ivkhanina dir1]$ cd /home/guest1
[guest1@ivkhanina ~]$ chmod 000 dir1
[guest1@ivkhanina ~]$ ls -l
итого 0
d----- 2 guest1 guest1 19 сен 26 17:00 dir1
drwxr-xr-x 2 guest1 guest1 6 сен 26 16:45 Видео
drwxr-xr-x 2 guest1 guest1 6 сен 26 16:45 Документы
drwxr-xr-x 2 guest1 guest1 6 сен 26 16:45 Загрузки
drwxr-xr-x 2 guest1 guest1 6 сен 26 16:45 Изображения
drwxr-xr-x 2 guest1 guest1 6 сен 26 16:45 Музыка
drwxr-xr-x 2 guest1 guest1 6 сен 26 16:45 Общедоступные
drwxr-xr-x 2 guest1 guest1 6 сен 26 16:45 Рабочий стол
drwxr-xr-x 2 guest1 guest1 6 сен 26 16:45 Шаблоны
[guest1@ivkhanina ~]$
```

Figure 4.16: Рис 16. Создание в директории dir1 тестового файла file1

Заполнила таблицу «Установленные права и разрешённые действия» 4.1, выполняя действия от имени владельца директории (файлов), определив опытным

заносила в таблицу знак «+», если не разрешена, знак «-». (рис. 17)

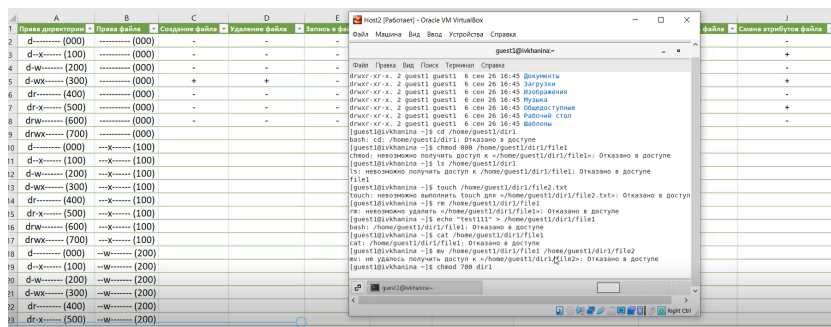


Figure 4.17: Рис 17. Заполнение таблицы и проверка разрешённых действий

Обозначения в таблице:

- (a) Создание файла
- (b) Удаление файла
- (c) Запись в файл
- (d) Чтение файла
- (e) Смена директории
- (f) Просмотр файлов в директории
- (g) Переименование файл
- (h) Смена атрибутов файла

Table 4.1: Установленные права и разрешённые действия

Права директории	Права файла	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
d----- (000)	----- (000)	-	-	-	-	-	-	-	-
d--x----- (100)	----- (000)	-	-	-	-	+	-	-	+
d-w----- (200)	----- (000)	-	-	-	-	-	-	-	-
d-wx----- (300)	----- (000)	+	+	-	-	+	-	+	+
dr----- (400)	----- (000)	-	-	-	-	-	-	-	-
dr-x----- (500)	----- (000)	-	-	-	-	+	+	-	+

Права директории	Права файла	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
drw----- (600)	----- (000)	-	-	-	-	-	-	-	-
drwx----- (700)	----- (000)	+	+	-	-	+	+	+	+
d----- (000)	---x----- (100)	-	-	-	-	-	-	-	-
d--x----- (100)	---x----- (100)	-	-	-	-	+	-	-	+
d-w----- (200)	---x----- (100)	-	-	-	-	-	-	-	-
d-wx----- (300)	---x----- (100)	+	+	-	-	+	-	+	+
dr----- (400)	---x----- (100)	-	-	-	-	-	-	-	-
dr-x----- (500)	---x----- (100)	-	-	-	-	+	+	-	+
drw----- (600)	---x----- (100)	-	-	-	-	-	-	-	-
drwx----- (700)	---x----- (100)	+	+	-	-	+	+	+	+
d----- (000)	--w----- (200)	-	-	-	-	-	-	-	-
d--x----- (100)	--w----- (200)	-	-	+	-	+	-	-	+
d-w----- (200)	--w----- (200)	-	-	-	-	-	-	-	-
d-wx----- (300)	--w----- (200)	+	+	+	-	+	-	+	+
dr----- (400)	--w----- (200)	-	-	-	-	-	-	-	-
dr-x----- (500)	--w----- (200)	-	-	+	-	+	+	-	+
drw----- (600)	--w----- (200)	-	-	-	-	-	-	-	-
drwx----- (700)	--w----- (200)	+	+	+	-	+	+	+	+
d----- (000)	--wx----- (300)	-	-	-	-	-	-	-	-
d--x----- (100)	--wx----- (300)	-	-	+	-	+	-	-	+
d-w----- (200)	--wx----- (300)	-	-	-	-	-	-	-	-
d-wx----- (300)	--wx----- (300)	+	+	+	-	+	-	+	+
dr----- (400)	--wx----- (300)	-	-	-	-	-	-	-	-
dr-x----- (500)	--wx----- (300)	-	-	+	-	+	+	-	+
drw----- (600)	--wx----- (300)	-	-	-	-	-	-	-	-
drwx----- (700)	--wx----- (300)	+	+	+	-	+	+	+	+
d----- (000)	-r----- (400)	-	-	-	-	-	-	-	-

Права директории	Права файла	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
d--x----- (100)	-r----- (400)	-	-	-	+	+	-	-	+
d-w----- (200)	-r----- (400)	-	-	-	-	-	-	-	-
d-wx----- (300)	-r----- (400)	+	+	-	+	+	-	+	+
dr----- (400)	-r----- (400)	-	-	-	-	-	-	-	-
dr-x----- (500)	-r----- (400)	-	-	-	+	+	+	-	+
drw----- (600)	-r----- (400)	-	-	-	-	-	-	-	-
drwx----- (700)	-r----- (400)	+	+	-	+	+	+	+	+
d----- (000)	-r-x----- (500)	-	-	-	-	-	-	-	-
d--x----- (100)	-r-x----- (500)	-	-	-	+	+	-	-	+
d-w----- (200)	-r-x----- (500)	-	-	-	-	-	-	-	-
d-wx----- (300)	-r-x----- (500)	+	+	-	+	+	-	+	+
dr----- (400)	-r-x----- (500)	-	-	-	-	-	-	-	-
dr-x----- (500)	-r-x----- (500)	-	-	-	+	+	+	-	+
drw----- (600)	-r-x----- (500)	-	-	-	-	-	-	-	-
drwx----- (700)	-r-x----- (500)	+	+	-	+	+	+	+	+
d----- (000)	-rw----- (600)	-	-	-	-	-	-	-	-
d--x----- (100)	-rw----- (600)	-	-	+	+	+	-	-	+
d-w----- (200)	-rw----- (600)	-	-	-	-	-	-	-	-
d-wx----- (300)	-rw----- (600)	+	+	+	+	+	-	+	+
dr----- (400)	-rw----- (600)	-	-	-	-	-	-	-	-
dr-x----- (500)	-rw----- (600)	-	-	+	+	+	+	-	+
drw----- (600)	-rw----- (600)	-	-	-	-	-	-	-	-
drwx----- (700)	-rw----- (600)	+	+	+	+	+	+	+	+
d----- (000)	-rwx----- (700)	-	-	-	-	-	-	-	-
d--x----- (100)	-rwx----- (700)	-	-	+	+	+	-	-	+
d-w----- (200)	-rwx----- (700)	-	-	-	-	-	-	-	-
d-wx----- (300)	-rwx----- (700)	+	+	+	+	+	-	+	+

Права директории	Права файла	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
dr----- (400)	-rwx----- (700)	-	-	-	-	-	-	-	-
dr-x----- (500)	-rwx----- (700)	-	-	+	+	+	+	-	+
drw----- (600)	-rwx----- (700)	-	-	-	-	-	-	-	-
drwx----- (700)	-rwx----- (700)	+	+	+	+	+	+	+	+

На основании заполненной таблицы определила те или иные минимально необходимые права для выполнения операций внутри директории dir1 и заполнила таблицу 4.2. Для заполнения последних двух строк опытным путем проверила минимальные права. (рис. 18)

```
[guest1@ivkhanina ~]$ chmod 000 dir1
[guest1@ivkhanina ~]$ cd /home/guest1/dir1
bash: cd: /home/guest1/dir1: Отказано в доступе
[guest1@ivkhanina ~]$ chmod 100 dir1
[guest1@ivkhanina ~]$ cd /home/guest1/dir1
[guest1@ivkhanina dir1]$ mkdir dir2
mkdir: невозможно создать каталог «dir2»: Отказано в доступе
[guest1@ivkhanina dir1]$ rmdir dir2
rmdir: не удалось удалить «dir2»: Нет такого файла или каталога
[guest1@ivkhanina dir1]$ cd /home/guest1
[guest1@ivkhanina ~]$ chmod 200 dir1
[guest1@ivkhanina ~]$ cd /home/guest1/dir1
bash: cd: /home/guest1/dir1: Отказано в доступе
[guest1@ivkhanina ~]$ chmod 300 dir1
[guest1@ivkhanina ~]$ cd /home/guest1/dir1
[guest1@ivkhanina dir1]$ mkdir dir2
[guest1@ivkhanina dir1]$ rmdir dir2
[guest1@ivkhanina dir1]$ cd /home/guest1
[guest1@ivkhanina ~]$
```



Figure 4.18: Рис 17. Минимальные права для создания и удаления поддиректорий

Table 4.2: Минимальные права для совершения операций

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)

Операция	Минимальные права на директорию	Минимальные права на файл
Переименование файла	d-wx— (300)	— — — — (000)
Создание поддиректории	d-wx— (300)	— — — — (000)
Удаление поддиректории	d-wx— (300)	— — — — (000)

## 5 Выводы

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 Linux.

# Список литературы

1. Разрешения доступа к файлам
2. Дискреционное разграничение доступа Linux