

Лабораторная работа 2

Права доступа

Бешкуров Михаил Борисович

Содержание

1	Цель работы	3
2	Задание	4
3	Выполнение лабораторной работы	5
4	Выводы	19
5	Список литературы	20

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

1. Создать учетную запись пользователя guest.
2. Войти в терминал, используя созданную учетную запись, и выполнить ряд команд.
3. Заполнить таблицу “Установленные права и разрешенные действия”
4. Заполнить таблицу “Минимальные права для совершения операций”

3 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создал учётную запись пользователя guest (использовал учётную запись администратора) (рис - @fig:001). Для этого использовал команду `user add guess`

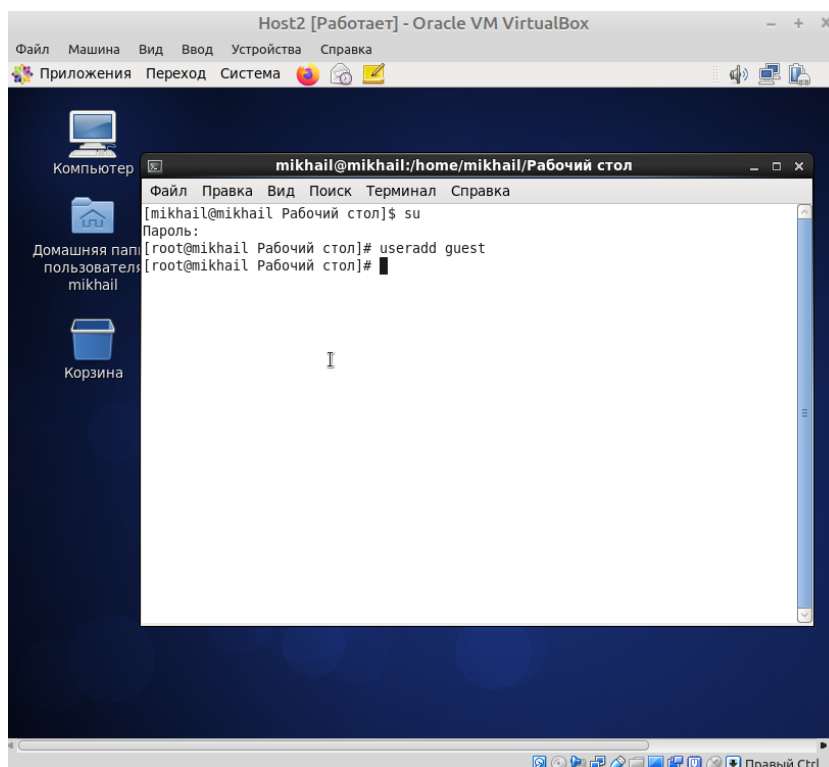


Рис. 3.1: Создание учетной записи guest

Задал пароль для пользователя guest (использовал учётную запись администратора) (рис @fig:002). Для этого использовал команду `passwd guest`

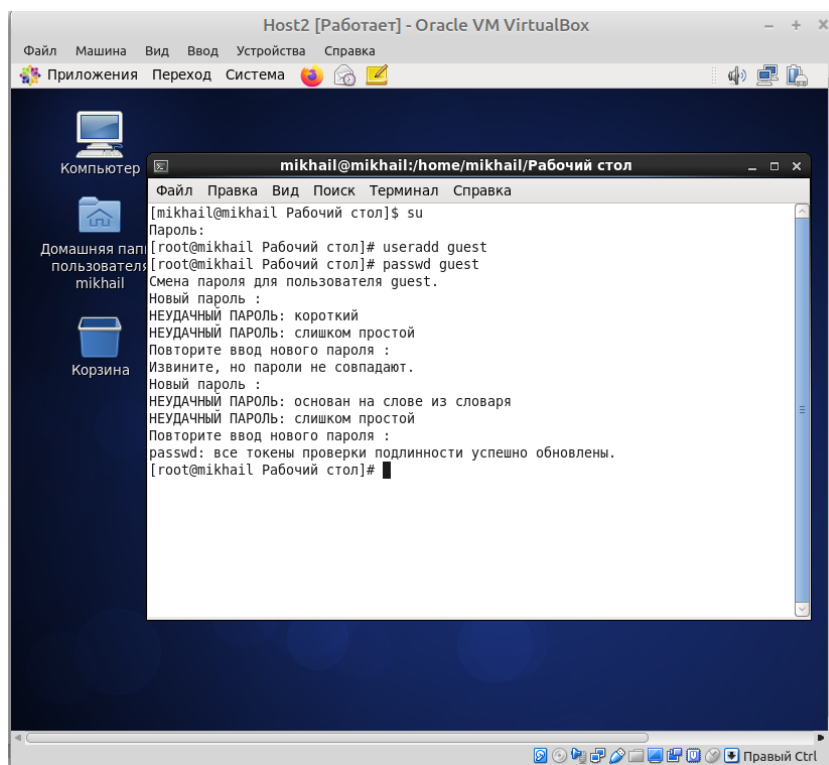


Рис. 3.2: Задание пароля для учетной записи

Вошел в систему от имени пользователя guest.

2. Определил директорию, в которой я нахожусь, командой `pwd`. Она совпадает с приглашением командной строки. Определил, что она не является моей домашней директорией. Перешл в свою домашнюю директорию. (рис @fig:004)

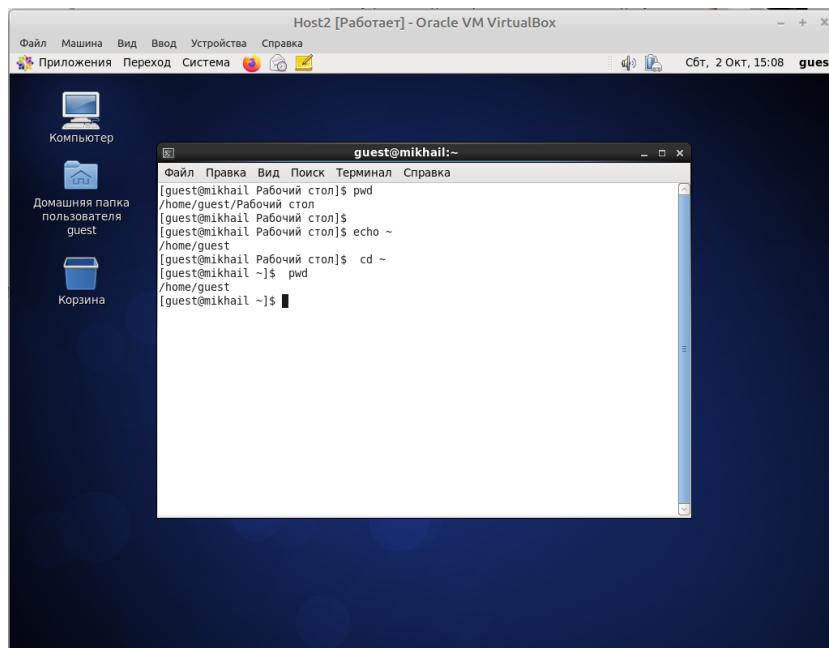


Рис. 3.3: Определение текущей директории. Переход в домашнюю директорию

Уточнил имя своего пользователя командой `whoami` (рис @fig:005).

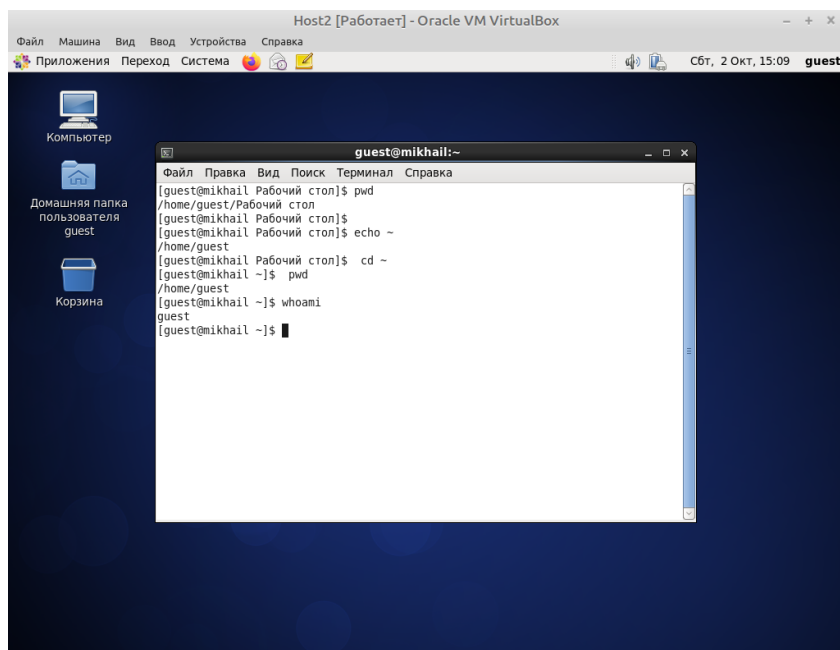
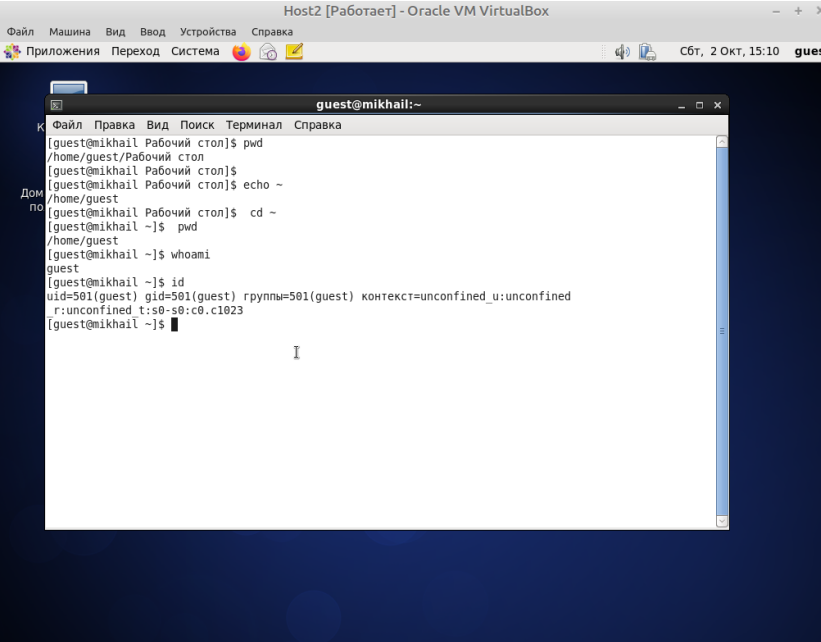


Рис. 3.4: Уточнение имени пользователя

Уточнил имя своего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомнил. Группы совпадают, однако вывод команды `id` объемнее (рис @fig:006).



```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Переход  Система
guest@mikhaill:~$ pwd
/home/guest/Рабочий стол
guest@mikhaill:~$ echo ~
/home/guest
guest@mikhaill:~$ cd ~
/home/guest
guest@mikhaill:~$ pwd
/home/guest
guest@mikhaill:~$ whoami
guest
guest@mikhaill:~$ id
uid=501(guest) gid=501(guest) rpyrny=501(guest) контекст=unconfined_u:unconfined
r:unconfined t:s0-s0:c0.c1023
guest@mikhaill:~$
```

Рис. 3.5: Уточнение имени, его группы

Сравнил полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. Как видно из рисунка, информация об имени пользователя, полученная командой `id` (`gid=501(guest)`), совпадает с приглашением командной строки (`guest@mikhaill home`)

Просмотрел файл `/etc/passwd` командой `cat /etc/passwd` (рис @fig:008)

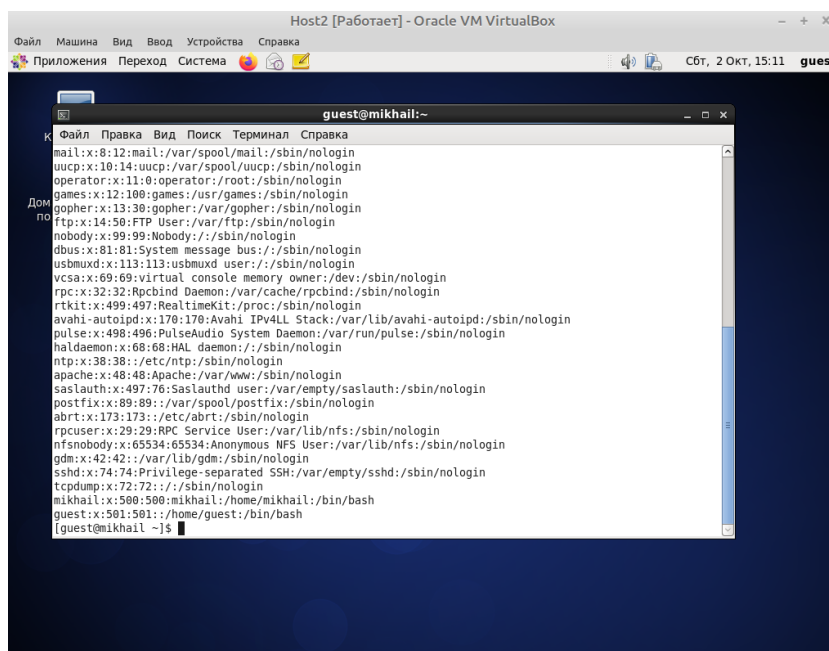


Рис. 3.6: Просмотр файла с помощью команды cat

Нашел свою учетную запись (последняя строчка). Определил uid и gid пользователя (501 и 501 соответственно). Они совпадают со значениями uid и gid, полученными на предыдущих пунктах.

Для того, чтобы вывести только строки, содержащие определенные буквенные сочетания, необходимо воспользоваться программой ggrep в терминале (рис @fig:010)

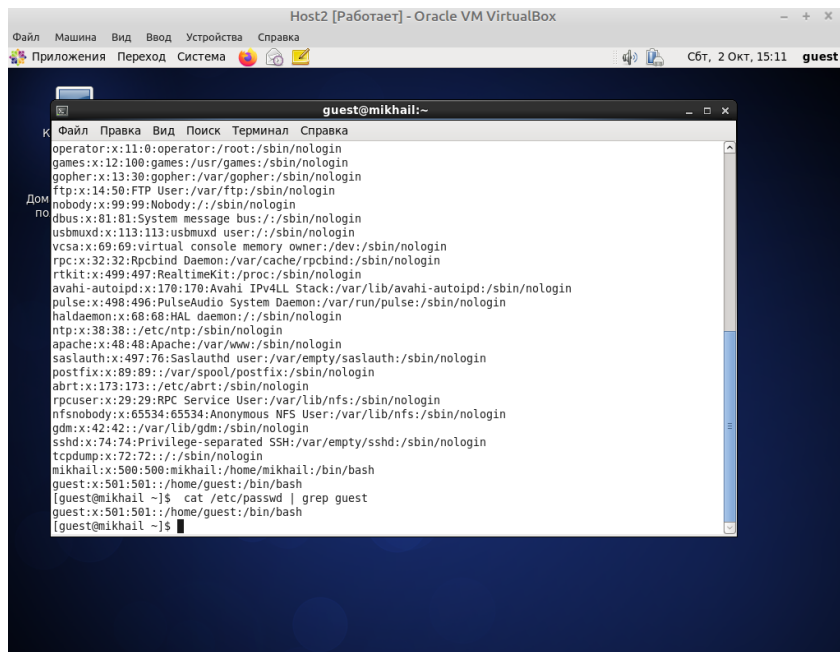


Рис. 3.7: Фильтрованный вывод строк

Определил существующие в системе директории командой `ls -l /home/` (рис @fig:011)

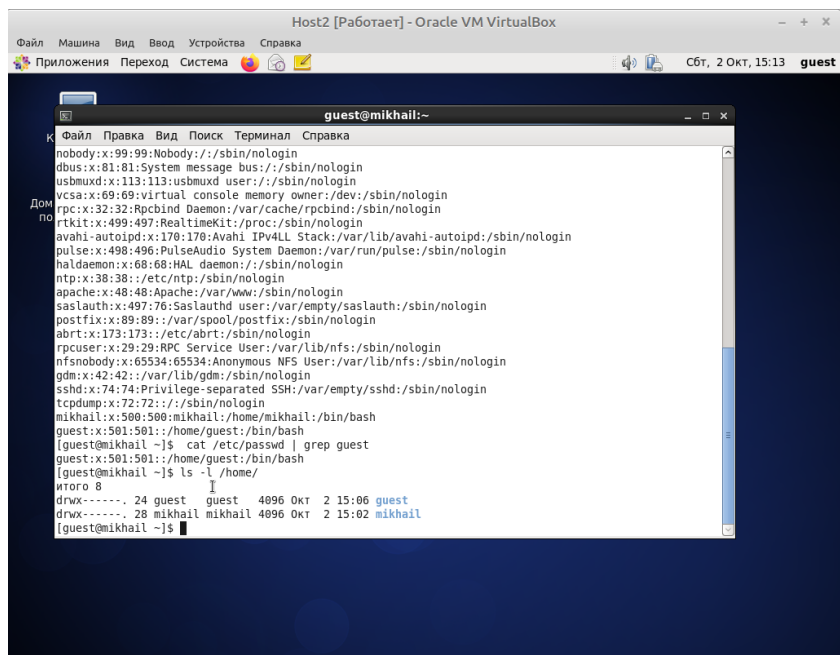
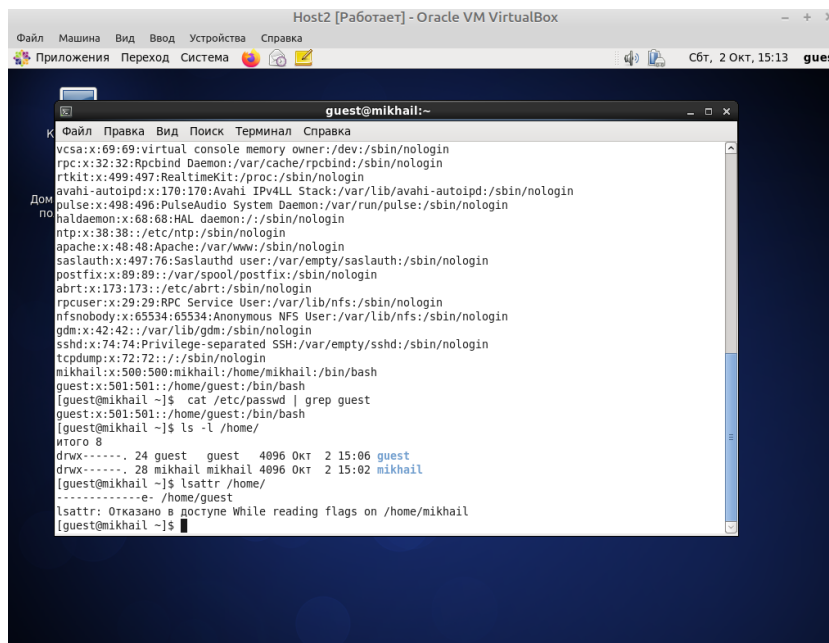


Рис. 3.8: Определение существующих в системе директорий

Мне удалось получить список поддиректорий директории /home. На поддиректориях установлены права на чтение (r), запись (w) и исполнение (x).

Проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home с помощью команды `lsattr /home` (рис @fig:012)



```
Host2 [Работае] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Переход  Система

guest@mikhail:~$ cat /etc/passwd | grep guest
guest:x:501:501::/home/guest:/bin/bash
[guest@mikhail ~]$ lsattr /home/
-----e- /home/guest
lsattr: Отказано в постыне While reading flags on /home/mikhail
[guest@mikhail ~]$
```

Рис. 3.9: Проверка установленных расширенных атрибутов

Удалось увидеть расширенные атрибуты директории guest. Однако не удалось увидеть расширенные атрибуты других директорий (mikhail).

Создал в домашней директории поддиректорию dir1 командой `mkdir dir1` (рис. @fig:013)

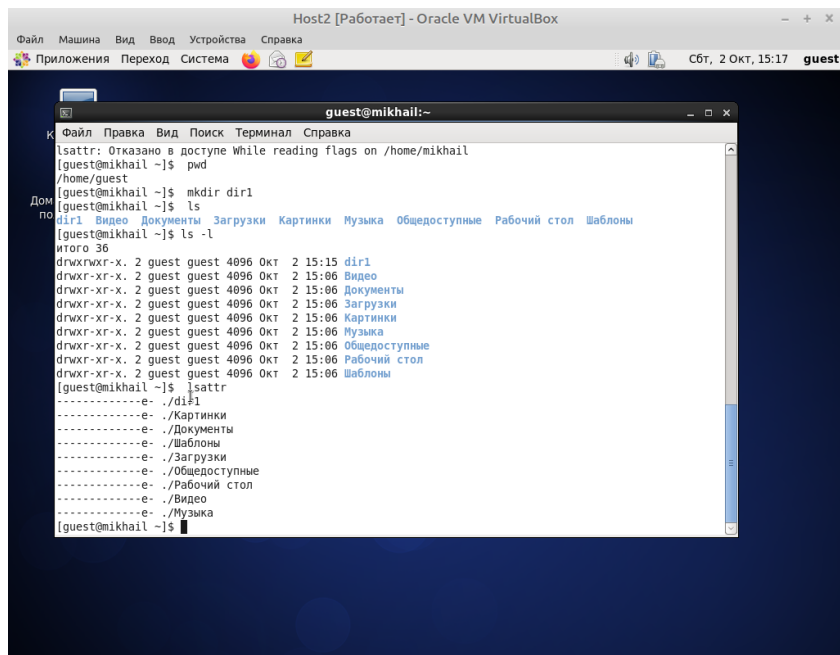


Рис. 3.10: Создание директории dir1

Также с помощью команд `ls -l` и `lsattr` просмотрел, какие атрибуты выставлены на директорию `dir1` (`drwxrwxr-x` и `-----e-` соответственно).

Снял с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверил правильность выполнения команды с помощью `ls -l` (рис. @fig:014)

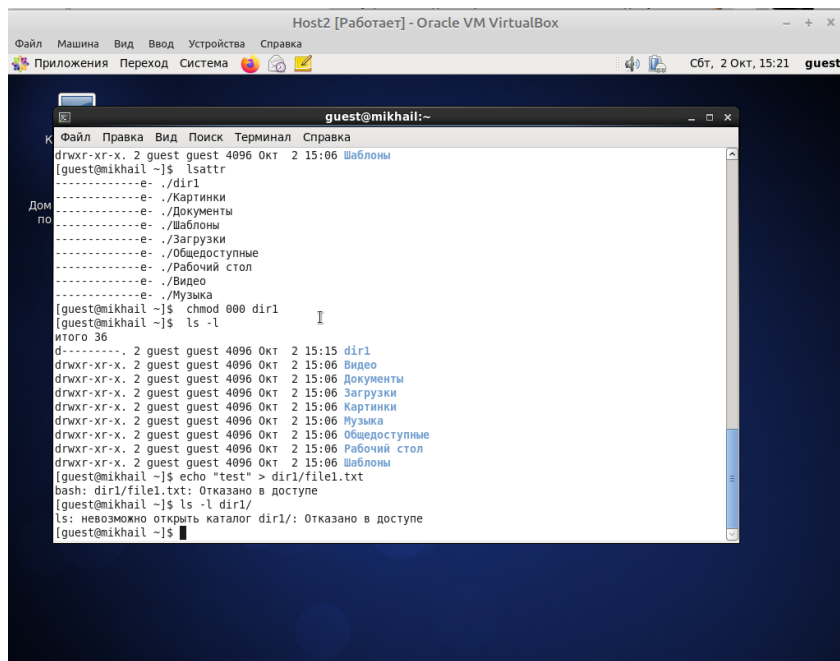


Рис. 3.11: Снятие всех атрибутов с директории dir1

Попытался создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1` (рис. @fig:015). Я получил отказ, т.к. на предыдущим шаге для директории dir были сняты все атрибуты.

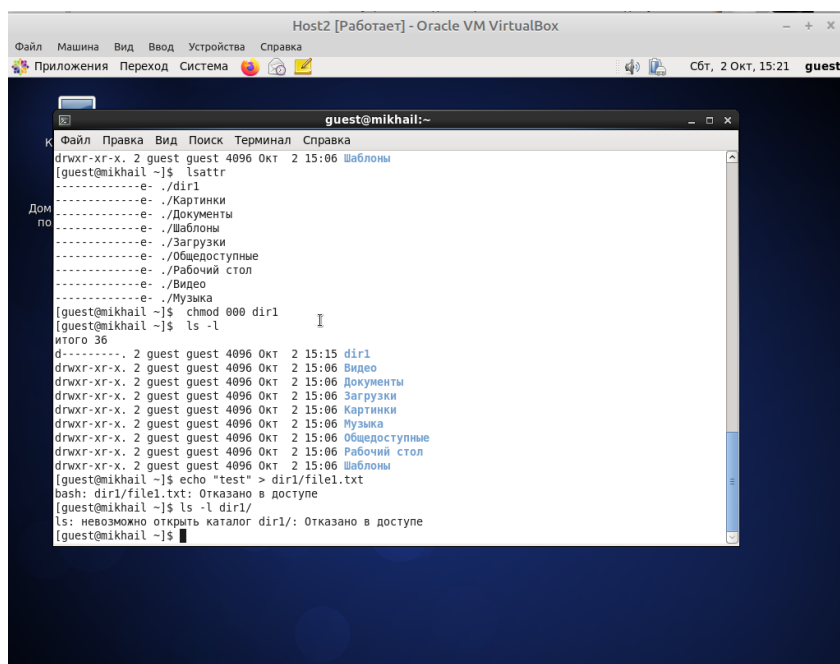


Рис. 3.12: Попытка создания файла file1

С помощью команды `ls -l /home/guest/dir1` выяснил, что невозможно получить доступ к директории `dir1`. Файл `file1` действительно не находится в директории

3. Заполнил таблицу “Установленные права и разрешенные действия”, выполняя действия от имени владельца директории (файлов), определив опытным путем, какие операции разрешены, а какие нет. “+” - операция разрешена, “-” - операция не разрешена (таб. 3.1)

Таблица 3.1: Установленные права и разрешённые действия

Пра- ва	Со- зда- ние	Уда- ле- ние	За- пись в файл	Чте- ние фай- ла	Сме- на рек- то- рии	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d(000)	(000)	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	-	-	+
d(100)	(100)	-	-	-	-	-	-	+
d(100)	(200)	-	+	-	-	-	-	+
d(100)	(300)	-	+	-	-	-	-	+
d(100)	(400)	-	-	+	-	-	-	+
d(100)	(500)	-	-	+	-	-	-	+
d(100)	(600)	-	+	+	-	-	-	+
d(100)	(700)	-	+	+	-	-	-	+
d(200)	(000)	-	-	-	-	-	-	-
d(200)	(100)	-	-	-	-	-	-	-
d(200)	(200)	-	-	-	-	-	-	-
d(200)	(300)	-	-	-	-	-	-	-
d(200)	(400)	-	-	-	-	-	-	-

Пра- ва	Со- зда- ние	Уда- ле- ние	За- пись	Чте- ние	Сме- на	ди- рек- то- рии	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d(200)	(500)	-	-	-	-	-	-	-	-
d(200)	(600)	-	-	-	-	-	-	-	-
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(300)	(100)	+	+	-	-	+	-	+	+
d(300)	(200)	+	+	+	-	+	-	+	+
d(300)	(300)	+	+	+	-	+	-	+	+
d(300)	(400)	+	+	-	+	+	-	+	+
d(300)	(500)	+	+	-	+	+	-	+	+
d(300)	(600)	+	+	+	+	+	-	+	-
d(300)	(700)	+	+	+	+	+	-	+	-
d(400)	(000)	-	-	-	-	-	+	-	-
d(400)	(100)	-	-	-	-	-	+	-	-
d(400)	(200)	-	-	-	-	-	+	-	-
d(400)	(300)	-	-	-	-	-	+	-	-
d(400)	(400)	-	-	-	-	-	+	-	-
d(400)	(500)	-	-	-	-	-	+	-	-
d(400)	(600)	-	-	-	-	-	+	-	-
d(400)	(700)	-	-	-	-	-	+	-	-
d(500)	(000)	+	-	-	-	-	+	-	+
d(500)	(100)	+	-	-	-	-	+	-	+
d(500)	(200)	+	-	+	-	-	+	-	+
d(500)	(300)	+	-	+	-	-	+	-	+

Пра-					Сме-				
ва		Со-	Уда-			на			
ди-	Пра-	зда-	ле-	За-	Чте-	ди-	Просмотр	Пере-	Смена
рек-	ва	ние	ние	пись	ние	рек-	файлов в	имено-	атрибу-
то-	фай-	фай-	фай-	в	фай-	то-	директо-	вание	тов
рии	ла	ла	ла	файл	ла	рии	рии	файла	файла
d(500)	(400)	+	-	-	+	-	+	-	+
d(500)	(500)	+	-	-	+	-	+	-	+
d(500)	(600)	+	-	+	+	-	+	-	+
d(500)	(700)	+	-	+	+	-	+	-	+
d(600)	(000)	-	-	-	-	-	+	-	-
d(600)	(100)	-	-	-	-	-	+	-	-
d(600)	(200)	-	-	-	-	-	+	-	-
d(600)	(300)	-	-	-	-	-	+	-	-
d(600)	(400)	-	-	-	-	-	+	-	-
d(600)	(500)	-	-	-	-	-	+	-	-
d(600)	(600)	-	-	-	-	-	+	-	-
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	+	+
d(700)	(100)	+	+	-	-	+	+	+	+
d(700)	(200)	+	+	+	-	+	+	+	+
d(700)	(300)	+	+	+	-	+	+	+	+
d(700)	(400)	+	+	-	+	+	+	+	+
d(700)	(500)	+	+	-	+	+	+	+	+
d(700)	(600)	+	+	+	+	+	+	+	+
d(700)	(700)	+	+	+	+	+	+	+	+

4. На основании заполненной выше таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории

dir1, заполняя таблицу “Установленные права и разрешенные действия” (таб. 3.2).

Таблица 3.2: Минимальные права для совершения операций

Операция	min права на директорию	min права на файл
Создание файла	(-wx)(3)	(- - -)(0)
Удаление файла	(-wx)(3)	(- - -)(0)
Чтение файла	(- - x)(1)	(r - -)(4)
Запись в файл	(- - x)(1)	(-w-)(2)
Переименование файла	(-wx)(3)	(- - -)(0)
Создание поддиректории	(-wx)(3)	(- - -)(0)
Удаление поддиректории	(-wx)(3)	(- - -)(0)

4 Выводы

Получил практически навыки работы в консоли с атрибутами файлов, закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

5 Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 2. Дискреционное разграничение прав в Linux. Основные атрибуты