

# **Лабораторная работа № 2**

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

Абдуллаев Сайидазизхон Шухратович

# Содержание

Цель работы	5
Задание	6
Теоретическое введение	7
Ход работы	9
Выводы	22

# Список иллюстраций

1	Создание новой учетной записи . . . . .	9
2	Пароль для новой учетной записи . . . . .	10
3	Вход в систему . . . . .	11
4	Определение текущей директории . . . . .	12
5	Группы, в которые входит пользователь . . . . .	13
6	Вывод команды groups . . . . .	13
7	Просмотр файла /etc/passwd и определение uid и gid пользователя	14
8	Поддиректории директории /home . . . . .	14
9	Проверка расширенных атрибутов . . . . .	15
10	Создание поддиректории . . . . .	15
11	Проверка прав доступа и расширенных атрибутов . . . . .	16
12	Создание файла в директории dir1 . . . . .	16
13	Проверка создания файла . . . . .	17
14	Процесс проверки разрешенных операций . . . . .	17
15	Процесс проверки разрешенных операций . . . . .	18
16	Процесс проверки разрешенных операций . . . . .	18
17	Процесс проверки разрешенных операций . . . . .	19
18	Заполненная таблица . . . . .	20
19	Проверка минимально необходимых прав для выполнения операций внутри директории . . . . .	21

## Список таблиц

# 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.

# Задание

Закрепить дискреционное разграничение прав в Linux.

# Теоретическое введение

В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов. Один из подходов к разграничению доступа — так называемый дискреционный — предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют. Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ в (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей. Чтобы получить доступ к файлам в Linux, используются разрешения. Эти разрешения назначаются трем объектам: файлу, группе и другому объекту. Для управления правами используется команда `chmod`. При использовании `chmod` в относительном режиме вы работаете с тремя индикаторами, чтобы указать, что вы хотите сделать. Сначала вы указываете, для кого вы хотите изменить разрешения. Для этого вы можете выбрать между пользователем (u), группой (g) и другими (o). Затем вы используете оператор для добавления или удаления разрешений из текущего режима или устанавливаете их абсолютно. В конце вы используете r(read), w(write) и x(execute), чтобы указать, какие разрешения вы хотите установить. При использовании `chmod` вы можете устанавливать разрешения для пользователя (user), группы (group) и других (other). Помимо основных разрешений, о которых вы только что прочитали, в Linux также есть набор расширенных раз-

решений. Это не те разрешения, которые вы устанавливаете по умолчанию, но иногда они предоставляют полезное дополнение.



# Ход работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создаем учётную запись пользователя guest. (Рис. [-@fig:001]).

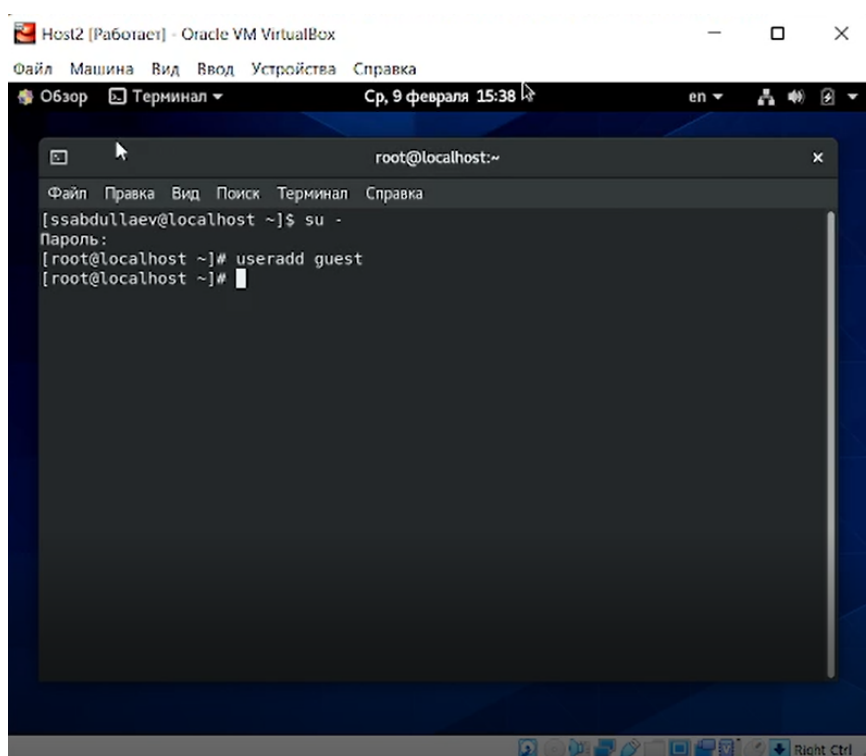


Рис. 1: Создание новой учетной записи

2. Задаем пароль для пользователя guest (используя учётную запись администратора). (Рис. [-@fig:002]).

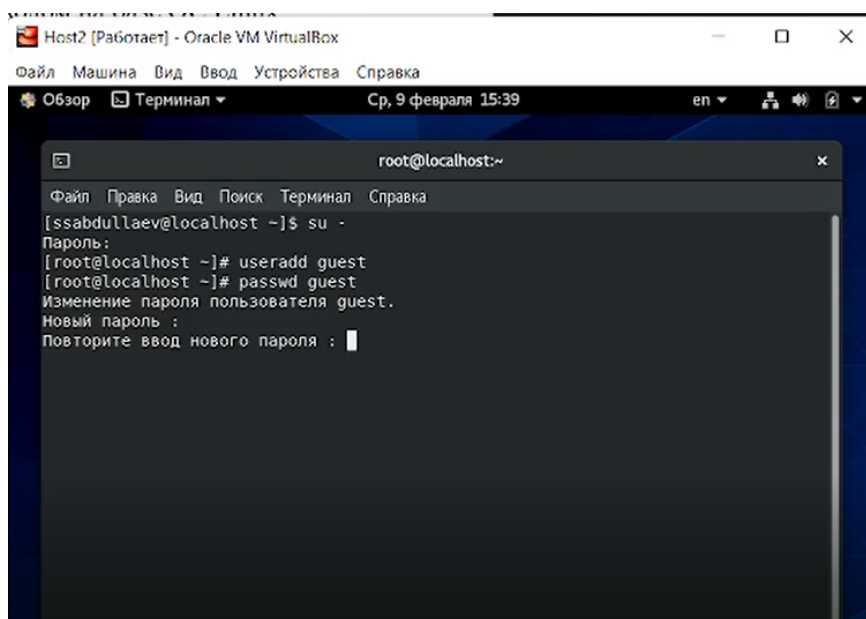


Рис. 2: Пароль для новой учетной записи

3. Входим в систему от имени пользователя guest и определяем директорию, в которой мы находимся. Как можно заметить, мы находимся в домашней директории, о чем свидетельствует значок тильды, а также результат введения команды pwd. (Рис. [-@fig:003], [-@fig:004]).

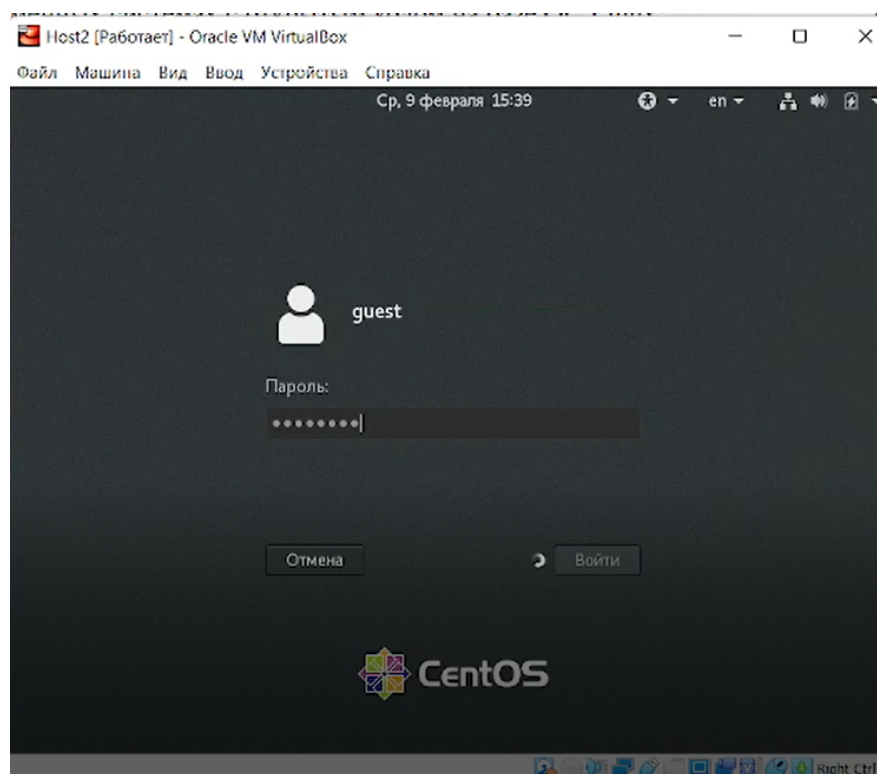


Рис. 3: Вход в систему

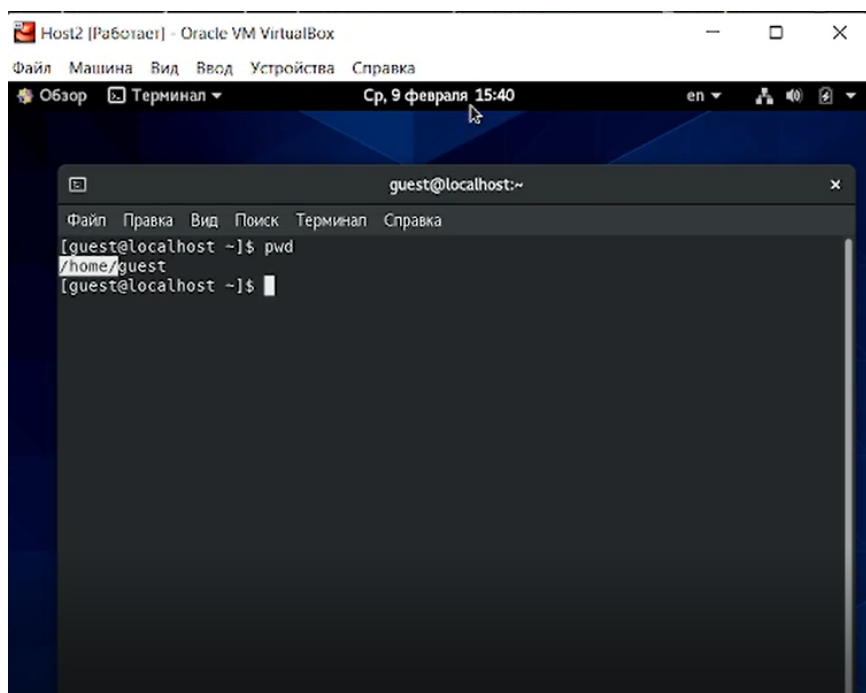


Рис. 4: Определение текущей директории

4. Уточняем имя пользователя командой `whoami`. Уточняем его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` сравниваем с выводом команды `groups`. Нетрудно заметить, что они совпадают. Кроме того, полученная информация совпадает с данными, выводимыми в приглашении командной строки. (`[-@fig:006]`, `[-@fig:007]`).

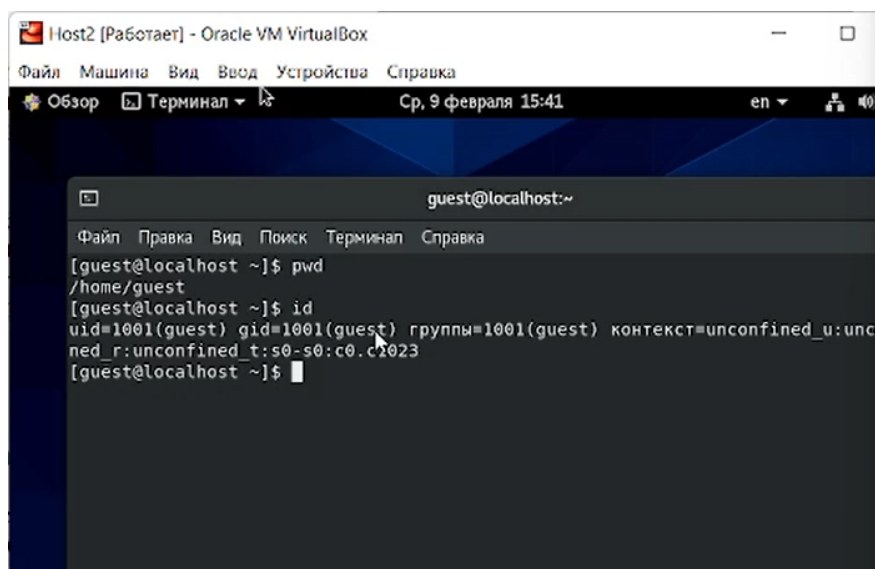


Рис. 5: Группы, в которые входит пользователь

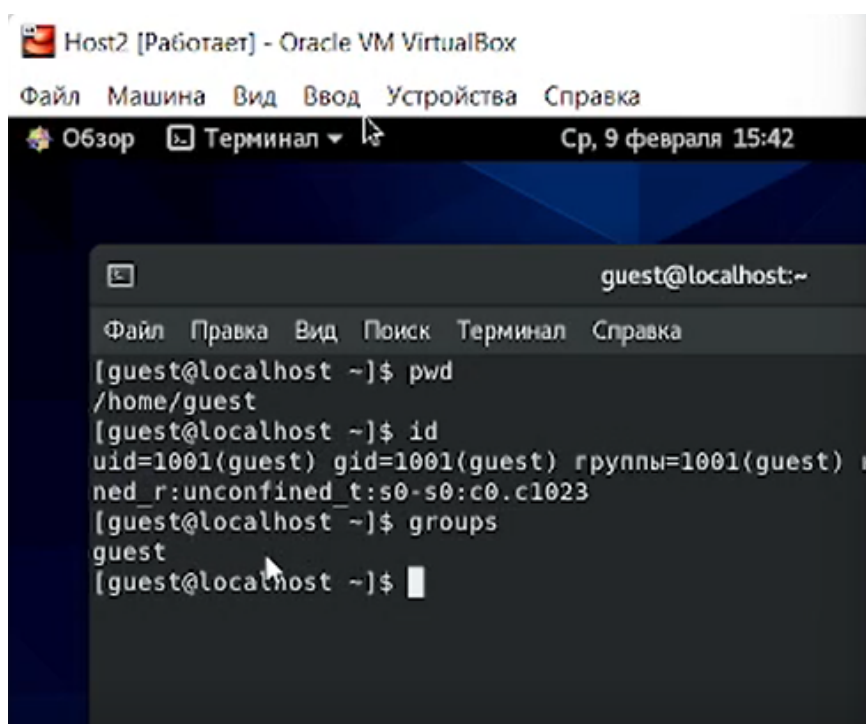


Рис. 6: Вывод команды groups

5. Просматриваем файл `/etc/passwd` командой `cat /etc/passwd`. Найдя в нём

свою учётную запись, определяем uid и gid пользователя. Значения совпадают с полученными в предыдущих пунктах. (Рис. [-@fig:009]).

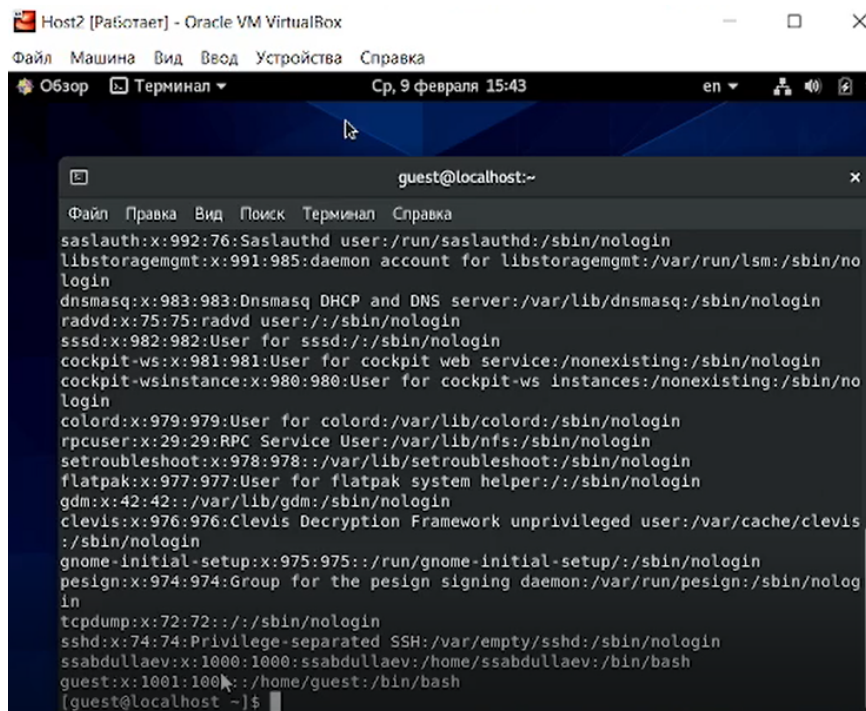


Рис. 7: Просмотр файла /etc/passwd и определение uid и gid пользователя

6. Определяем существующие в системе директории командой `ls -l /home/`. В результате удалось получить список поддиректорий директории /home. На имеющихся директориях (avaksenova и guest) был установлен полный набор прав. (Рис. [-@fig:010]).

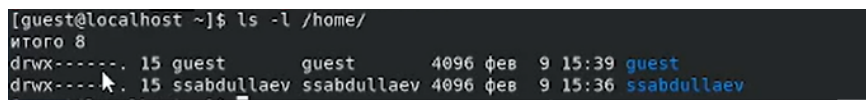


Рис. 8: Поддиректории директории /home

7. Командой `lsattr /home` проверяем, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home. Расширенные

атрибуты директории avaksenova увидеть не удалось из-за нехватки прав доступа, а расширенные атрибуты директории guest отсутствуют. (Рис. [-@fig:011]).

```
[guest@localhost ~]$ lsattr /home
lsattr: Отказано в доступе while reading flags on /home/ssabdullaev
----- /home/guest
[guest@localhost ~]$
```

Рис. 9: Проверка расширенных атрибутов

8. Создаем в домашней директории поддиректорию dir1 командой `mkdir dir1`. Определяем командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию dir1, а затем снимаем с директории dir1 все атрибуты командой `chmod 000 dir1` и проверяем правильность выполнения с помощью `ls -l`. (Рис. [-@fig:012], [-@fig:013]).

```
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls -l
итого 0
drwxrwxr-x. 2 guest guest 6 фев 9 15:47 dir1
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Видео
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Документы
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Загрузки
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Изображения
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Музыка
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Общедоступные
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Шаблоны
```

Рис. 10: Создание поддиректории



```
[guest@localhost ~]$ lsattr
..... ./Рабочий стол
..... ./Загрузки
..... ./Шаблоны
..... ./Общедоступные
..... ./Документы
..... ./Музыка
..... ./Изображения
..... ./Видео
..... ./dir1

[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
итого 0
d----- . 2 guest guest 6 фев 9 15:47 dir1
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Видео
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Документы
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Загрузки
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Изображения
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Музыка
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Общедоступные
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Шаблоны
[guest@localhost ~]$
```

Рис. 11: Проверка прав доступа и расширенных атрибутов

9. Пытаемся создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`. В результате получаем отказ в выполнении операции по созданию файла, поскольку в предыдущих пунктах с директории dir1 были сняты все атрибуты. Таким образом, файл не создался, в чем убеждаемся, применив команду `ls -l /home/guest/dir1`. (Рис. [-@fig:014], [-@fig:015]).

```
[guest@localhost ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@localhost ~]$
```

Рис. 12: Создание файла в директории dir1



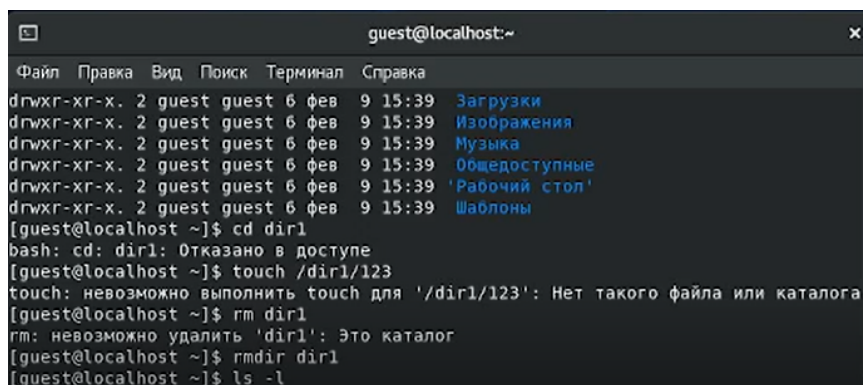
```

[guest@localhost ~]$ su -
Пароль:
[root@localhost ~]# ls
anaconda-ks.cfg  initial-setup-ks.cfg
[root@localhost ~]# cd /home/guest/dir1
[root@localhost dir1]# ls
[root@localhost dir1]# ls /home/guest/dir1
[root@localhost dir1]# ls -l
итого 0
[root@localhost dir1]#

```

Рис. 13: Проверка создания файла

10. Заполняем таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определяем опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносим в таблицу знак «+», если не разрешена, знак «-». При заполнении таблицы рассматриваем не все атрибуты файлов и директорий, а лишь «первые три»: г, w, x, для «владельца». В итоге рассматриваем 64 варианта. (Рис. [-@fig:016], [-@fig:017]).



```

guest@localhost:~
Файл  Правка  Вид  Поиск  Терминал  Справка
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Загрузки
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Изображения
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Музыка
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Общедоступные
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 фев 9 15:39 Шаблоны
[guest@localhost ~]$ cd dir1
bash: cd: dir1: Отказано в доступе
[guest@localhost ~]$ touch /dir1/123
touch: невозможно выполнить touch для '/dir1/123': Нет такого файла или каталога
[guest@localhost ~]$ rm dir1
rm: невозможно удалить 'dir1': Это каталог
[guest@localhost ~]$ rmdir dir1
[guest@localhost ~]$ ls -l

```

Рис. 14: Процесс проверки разрешенных операций

```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Общедоступные  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 'Рабочий стол'  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Шаблоны  
[guest@localhost ~]$ chmod 000 dir1  
[guest@localhost ~]$ touch file /dir1  
touch: невозможно выполнить touch для '/dir1': Отказано в доступе  
[guest@localhost ~]$ chmod 100 dir1  
[guest@localhost ~]$ ls -l  
итого 0  
d--x-----. 2 guest guest 6 фев 9 16:06 dir1  
-rw-rw-r--. 1 guest guest 0 фев 9 16:06 file  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Видео  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Документы  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Загрузки  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Изображения  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Музыка  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Общедоступные  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 'Рабочий стол'
```

Рис. 15: Процесс проверки разрешенных операций

```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Загрузки  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Изображения  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Музыка  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Общедоступные  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 'Рабочий стол'  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Шаблоны  
[guest@localhost ~]$ cd dir1  
[guest@localhost dir1]$ touch file  
touch: невозможно выполнить touch для 'file': Отказано в доступе  
[guest@localhost dir1]$ cd ..  
[guest@localhost ~]$ chmod 111 dir1  
[guest@localhost ~]$ ls -l  
итого 0  
d--x--x--x. 2 guest guest 6 фев 9 16:06 dir1  
-rw-rw-r--. 1 guest guest 0 фев 9 16:06 file  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Видео  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Документы  
d-rwxr-xr-x. 2 guest guest 6 фев 9 15:39 Загрузки
```

Рис. 16: Процесс проверки разрешенных операций

```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@localhost ~]$ chmod 300 dir1  
[guest@localhost ~]$ ls -l  
итого 0  
d-wx----- 2 guest guest 6 фев 9 16:06 dir1  
-rw-rw-r-- 1 guest guest 0 фев 9 16:06 file  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 Видео  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 Документы  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 Загрузки  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 Изображения  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 Музыка  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 Общедоступные  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 'Рабочий стол'  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 Шаблоны  
[guest@localhost ~]$ cd dir1  
[guest@localhost dir1]$ touch file  
[guest@localhost dir1]$ ls -l  
ls: невозможно открыть каталог '.': Отказано в доступе  
[guest@localhost dir1]$ rm file
```

Рис. 17: Процесс проверки разрешенных операций

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
000	000	—	—	—	—	—	—	—	—
100	000	—	—	—	—	+	—	—	—
200	000	—	—	—	—	—	—	—	—
300	000	+	+	—	—	+	—	+	—
400	000	—	—	—	—	—	+	—	—
500	000	—	—	—	—	+	+	—	—
600	000	—	—	—	—	—	+	—	—
700	000	+	+	—	—	+	+	+	—
000	100	—	—	—	—	—	—	—	—
100	100	—	—	—	—	+	—	—	—
200	100	—	—	—	—	—	—	—	—
300	100	+	+	—	—	+	—	+	—
400	100	—	—	—	—	—	+	—	—
500	100	—	—	—	—	+	+	—	—
600	100	—	—	—	—	—	+	—	—
700	100	+	+	—	—	+	+	+	—
000	200	—	—	—	—	—	—	—	—
100	200	—	—	+	—	+	—	—	—
200	200	—	—	—	—	—	—	—	—
300	200	+	+	+	—	+	—	+	—
400	200	—	—	—	—	—	+	—	—
500	200	—	—	+	—	+	+	—	—
600	200	—	—	—	—	—	+	—	—
700	200	+	+	+	—	+	+	+	—
000	300	—	—	—	—	—	—	—	—
100	300	—	—	+	—	+	—	—	—
200	300	—	—	—	—	—	—	—	—
300	300	+	+	+	—	+	—	+	—
400	300	—	—	—	—	—	+	—	—
500	300	—	—	+	—	+	+	—	—
600	300	—	—	—	—	—	+	—	—
700	300	+	+	+	—	+	+	+	—
000	400	—	—	—	—	—	—	—	—
100	400	—	—	—	+	+	—	—	+
200	400	—	—	—	—	—	—	—	—
300	400	+	+	—	+	+	—	+	+
400	400	—	—	—	—	—	+	—	—
500	400	—	—	—	+	+	+	—	+
600	400	—	—	—	—	—	+	—	—
700	400	+	+	—	+	+	+	+	+
000	500	—	—	—	—	—	—	—	—
100	500	—	—	—	+	+	—	—	+
200	500	—	—	—	—	—	—	—	—
300	500	+	+	—	+	+	—	+	+
400	500	—	—	—	—	—	+	—	—
500	500	—	—	—	+	+	+	—	+
600	500	—	—	—	—	—	+	—	—
700	500	+	+	—	+	+	+	+	+
000	600	—	—	—	—	—	—	—	—
100	600	—	—	+	+	+	—	—	+
200	600	—	—	—	—	—	—	—	—
300	600	+	+	+	+	+	—	+	+
400	600	—	—	—	—	—	+	—	—
500	600	—	—	+	+	+	+	—	+
600	600	—	—	—	—	—	+	—	—
700	600	+	+	+	+	+	+	+	+
000	700	—	—	—	—	—	—	—	—
100	700	—	—	+	+	+	—	—	+
200	700	—	—	—	—	—	—	—	—
300	700	+	+	+	+	+	—	+	+
400	700	—	—	—	—	—	+	—	—
500	700	—	—	+	+	+	+	—	+
600	700	—	—	—	—	—	+	—	—
700	700	+	+	+	+	+	+	+	+

Рис. 18: Заполненная таблица

11. На основании заполненной таблицы определяем те или иные минимально необходимые права для выполнения операций внутри директории `dir1`, внося данные во вторую таблицу. (Рис. [-@fig:018]).

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

Рис. 19: Проверка минимально необходимых прав для выполнения операций внутри директории

## **Выводы**

В результате выполнения данной 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 CentOS.