

Отчёт по лабораторной работе 2

Дискреционное разграничение прав в Linux. Основные атрибуты

Румянцева Александра Сергеевна

Содержание

1	Цель работы	5
2	Задание	6
3	Теория	7
4	Выполнение лабораторной работы	9
5	Библиография	21
6	Выводы	22

List of Figures

4.1	рис.1. Создание пользователя guest и задание для него пароля. . .	9
4.2	рис.2. Окно ввода пароля при входе в пользователя guest.	10
4.3	рис.3. Выполнение команды pwd, whoami, id и groups.	11
4.4	рис.4. Результат выполнения команды cat /etc/passwd. Учётная запись guest.	12
4.5	рис.5. Результат выполнения команды ls -l /home/ и lsattr /home .	12
4.6	рис.6. Выполнение команд mkdir dir1, ls -l и lsattr	13
4.7	рис.7. Результат команд chmod 000 dir1, ls -l и echo "test" > /home/guest/dir1/file1.	14
4.8	рис.8. Проверка создания пользователя в root пользователе. . . .	14
4.9	рис.9. Пример выполнения команд для заполнения таблицы установленных прав и разрешённых действий над файлами и директориями для случая 700 / 400.	15
4.10	рис.10. Выполнение заполнения таблицы 1.	16
4.11	рис.11. Выполнение заполнения таблицы 2.	20

List of Tables

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

Лабораторная работа подразумевает изучение установленных прав и разрешённых действий над файлами и директориями опытным путем, определение минимальных прав для операций.

3 Теория

Изучим, что представляют из себя права доступа в Linux.

Права доступа имеют всего 3 опции – чтение, запись и запуск на выполнение, устанавливаемые для владельца, группы и прочих пользователей (для папки запуск на выполнение означает просмотр содержимого – списка файлов и вложенных папок).

Права можно задавать либо буквами r (read), w (Write) и x (eXecute), либо в двоичной системе (точнее в восьмеричной с использованием цифр от 0 до 7, но на основе двоичной системы).

Праву на чтение (r) соответствует значение 4, записи (w) – 2 и выполнению/просмотру файлов (x) – 1. Комбинируя эти значения, можно получать разные права. Например:

- 6 = (4 + 2) – чтение и запись
- 5 = (4 + 1) – чтение и исполнение

Первыми задаются права доступа для владельца, затем для группы и в конце для всех прочих.

Обычно для документов и файлов данных устанавливаются права 644 или 664. Это означает, что владелец может читать и изменять файл (включая удаление), члены группы в первом случае только читать, а во втором изменять, а все прочие – только читать.

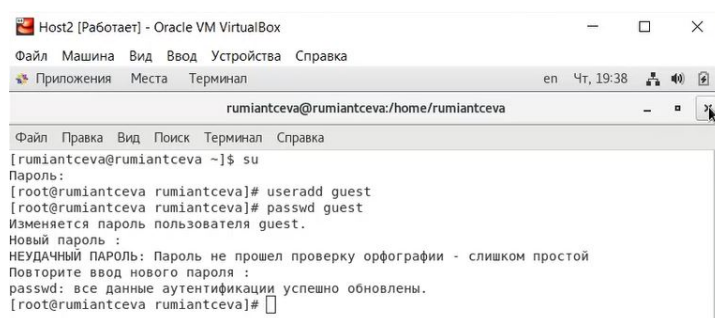
Для исполняемых файлов и папок обычно задаются права 755 или 775. Значения те же, что и в предыдущем абзаце плюс присутствует право на выполнение

или просмотр списка вложенных объектов.

Если задавать права доступа буквами, то указываются нужные права в виде `гwx`, а то, что нужно пропустить, заменяется дефисом. То есть, `644` соответствует `rw-r-r-`, а `755` – `rwxr-xr-x`.

4 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создала учётную запись пользователя guest с помощью команды `useradd guest` (рис. 1).
2. Задала пароль для пользователя guest командой `passwd guest` (рис. 1).



```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Места  Терминал
en  Чт, 19:38
rumiantceva@rumiantceva:/home/rumiantceva
Файл  Правка  Вид  Поиск  Терминал  Справка
[rumiantceva@rumiantceva ~]$ su
Пароль:
[root@rumiantceva rumiantceva]# useradd guest
[root@rumiantceva rumiantceva]# passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - слишком простой
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@rumiantceva rumiantceva]#
```

Figure 4.1: рис.1. Создание пользователя guest и задание для него пароля.

3. Вошла в систему от имени пользователя guest (рис. 2).

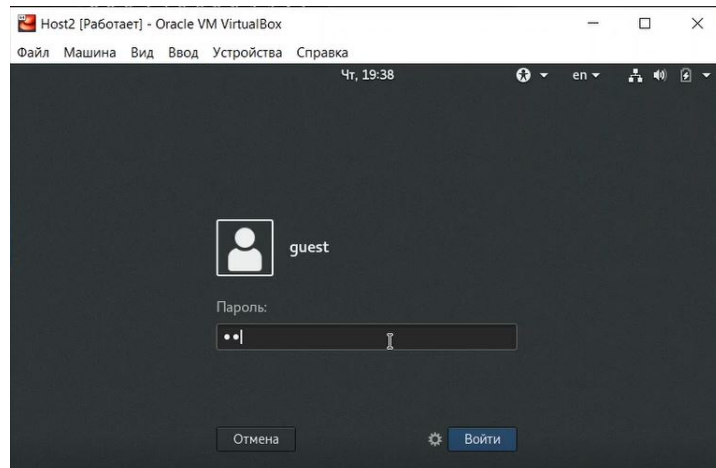


Figure 4.2: рис.2. Окно ввода пароля при входе в пользователя guest.

4. Определила директорию, в которой нахожусь, командой `pwd`.

Директория совпадает с приглашением командной строки, она является моей домашней директорией (видно по знаку тильды) (рис. 3).

5. Уточнила имя пользователя командой `whoami`(рис. 3). Видно, что имя пользователя `guest`.
6. Уточнила имя пользователя, его группу, а также группы, куда входит пользователь, командой `id` (рис. 3).

Видно, что имя пользователя `guest`, `uid = 1001`, его группа `guest`, `gid = 1001`, он входит только в группу `1001 (guest)`, то есть только в свою группу.

Сравнила вывод `id` с выводом команды `groups`. Команда `groups` так же вывела одну группу `guest`

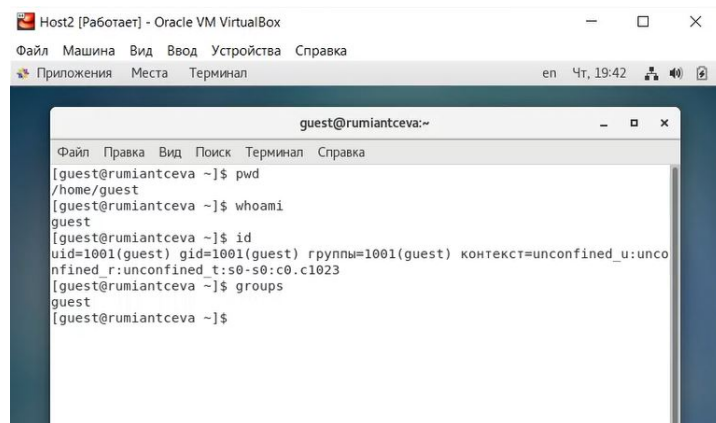


Figure 4.3: рис.3. Выполнение команды pwd, whoami, id и groups.

7. Сравнила полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. Имя пользователя во всех командах выводится как guest, что совпадает с именем в приглашении командной строки.
8. Просмотрела файл /etc/passwd командой cat /etc/passwd. Нашла в нём свою учётную запись (рис. 4).

Видим, что uid пользователя равен 1001, gid пользователя равен 1001, что совпадает с результатами выполнения команд, которые мы получили в предыдущих пунктах.

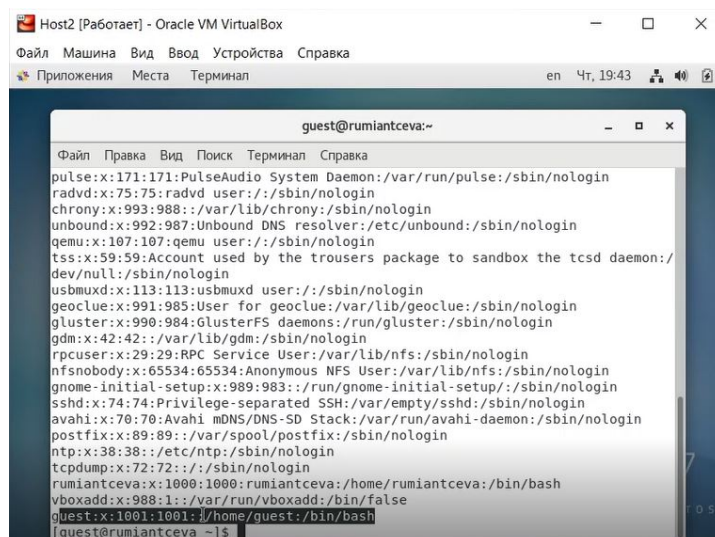


Figure 4.4: рис.4. Результат выполнения команды `cat /etc/passwd`. Учётная запись `guest`.

9. Определила существующие в системе директории командой `ls -l /home/` (рис. 5). Мне удалось получить список поддиректорий директории `/home`. На директориях `rumiantceva` и `guest` установлены права 700.
10. Проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой `lsattr /home` (рис. 5).

С помощью данной команды мне удалось увидеть расширенные атрибуты директории `guest`, то есть пользователя, в которм я нахожусь. Но не удалось увидеть расширенные атрибуты директории `rumiantceva`, отказано в доступе (что соответствует пункту выше).

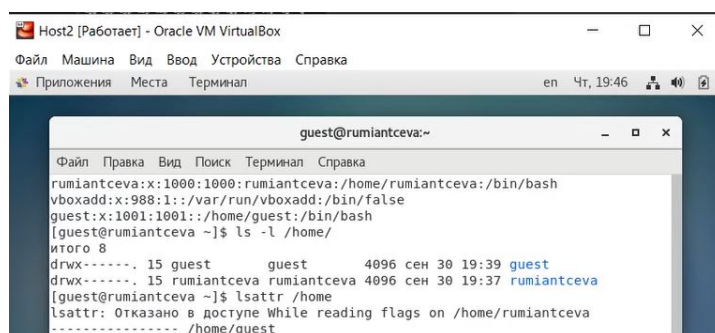
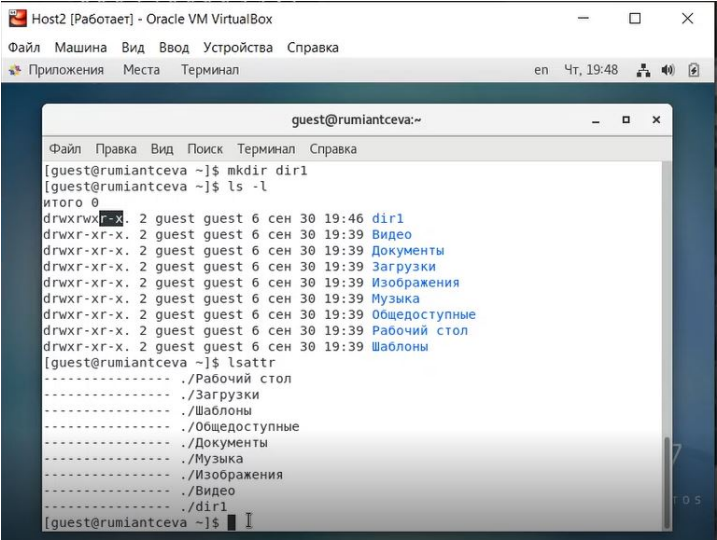


Figure 4.5: рис.5. Результат выполнения команды `ls -l /home/` и `lsattr /home`

11. Создала в домашней директории поддиректорию dir1 командой `mkdir dir1`. С помощью команд `ls -l` и `lsattr` посмотрела, какие права доступа и расширенные атрибуты были выставлены на директорию dir1 (рис.6).

Видим, что директория dir1 создана, кроме того, с помощью команды `ls -l` видим, что права у dir1 775, то есть для чтения, записи и исполнения для пользователя и групп, и только чтение и исполнение для остальных пользователей. С помощью команды `lsattr` видим, что расширенных атрибутов нет.



```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Места  Терминал
en  Чт, 19:48

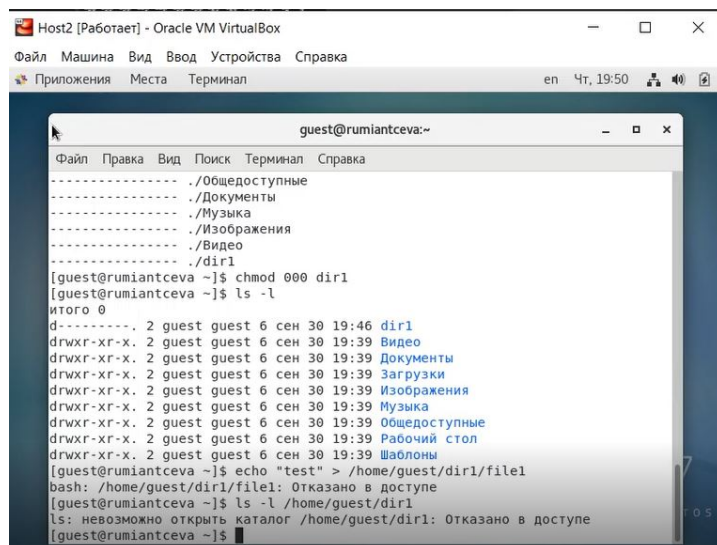
guest@rumiantceva:~
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@rumiantceva ~]$ mkdir dir1
[guest@rumiantceva ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 сен 30 19:46 dir1
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Видео
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Документы
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Изображения
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Музыка
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен 30 19:39 Шаблоны
[guest@rumiantceva ~]$ lsattr
-----
./Рабочий стол
./Загрузки
./Шаблоны
./Общедоступные
./Документы
./Музыка
./Изображения
./Видео
./dir1
[guest@rumiantceva ~]$
```

Figure 4.6: рис.6. Выполнение команд `mkdir dir1`, `ls -l` и `lsattr`

12. Сняла с директории dir1 все атрибуты командой `chmod 000 dir1` и проверила её правильность с помощью выполнения команды `ls -l`. Действительно, права стали 000 (рис.7).
13. Попыталась создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`. Данное действие выполнить не удалось из-за отсутствия доступа, так как мы сами сняли все права с директории dir1 в пункте выше (рис. 7).

Попробовала командой `ls -l /home/guest/dir1` проверить создание файла, так как у нас права dir1 установлены как 000, следовательно посмотреть что есть

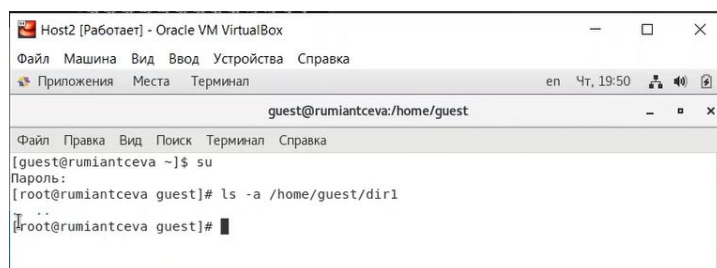
в dir1 не получилось (рис. 7). Поэтому я проверила создание файла file1 внутри директории dir1 под root (рис. 8). Видно, что всё же файл не был создан.



```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Места  Терминал
en  Чт, 19:50

guest@rumiantceva:~
Файл  Правка  Вид  Поиск  Терминал  Справка
-----
./Общедоступные
./Документы
./Музыка
./Изображения
./Видео
./dir1
[guest@rumiantceva ~]$ chmod 000 dir1
[guest@rumiantceva ~]$ ls -l
итого 0
d----- 2 guest guest 6 сен 30 19:46 dir1
drwxr-xr-x 2 guest guest 6 сен 30 19:39 Видео
drwxr-xr-x 2 guest guest 6 сен 30 19:39 Документы
drwxr-xr-x 2 guest guest 6 сен 30 19:39 Загрузки
drwxr-xr-x 2 guest guest 6 сен 30 19:39 Изображения
drwxr-xr-x 2 guest guest 6 сен 30 19:39 Музыка
drwxr-xr-x 2 guest guest 6 сен 30 19:39 Öffentlich
drwxr-xr-x 2 guest guest 6 сен 30 19:39 Рабочий стол
drwxr-xr-x 2 guest guest 6 сен 30 19:39 Шаблоны
[guest@rumiantceva ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@rumiantceva ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest@rumiantceva ~]$
```

Figure 4.7: рис.7. Результат команд `chmod 000 dir1`, `ls -l` и `echo "test" > /home/guest/dir1/file1`.



```
Host2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Места  Терминал
en  Чт, 19:50

guest@rumiantceva:/home/guest
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@rumiantceva ~]$ su
Пароль:
[root@rumiantceva guest]# ls -a /home/guest/dir1
.
..
[root@rumiantceva guest]#
```

Figure 4.8: рис.8. Проверка создания пользователя в root пользователе.

14. Заполнила таблицу 1 опытным путём.

Команды для проверки, которые я использовала:

- touch - проверка на создание файла
- rm - проверка на удаление файла
- echo - проверка на запись в файл

- cat - проверка на чтение файла
- cd - проверка на доступ в директорию
- ls - проверка на просмотр файлов в директории
- mv - проверка на переименование файла
- chattr - проверка добавление атрибутов

Для смены и задания прав на файл или директорию я использовала команду `chmod`. Пример выполнения одного из 64 случаев на рисунке 9 для случая 700 / 400 на риунке 9. Таким образом заполнялась вся таблица (рис. 10).

```

Host2 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Приложения Места Терминал en Пт, 01:36
guest@rumiantceva:/home/guest

guest@rumiantceva:~/dir1
-----d-----
[guest@rumiantceva ~]$ ls -l
итого 0
drwx----- 2 guest guest 19 окт 1 01:22 dir1
[guest@rumiantceva ~]$ touch dir1/file2
[guest@rumiantceva ~]$ rm dir1/file2
[guest@rumiantceva ~]$ echo "aa" > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest@rumiantceva ~]$ cat dir1/file1
[guest@rumiantceva ~]$ cd dir1
[guest@rumiantceva dir1]$ ls
file1
[guest@rumiantceva dir1]$ mv file1 file2
[guest@rumiantceva dir1]$ chattr +d file2

```

Figure 4.9: рис.9. Пример выполнения команд для заполнения таблицы установленных прав и разрешённых действий над файлами и директориями для случая 700 / 400.

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

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

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

15. На основании заполненной таблицы в пункте 14 определяйте или иные минимально необходимые права для выполнения операций внутри директории dir1 (рис. 11).

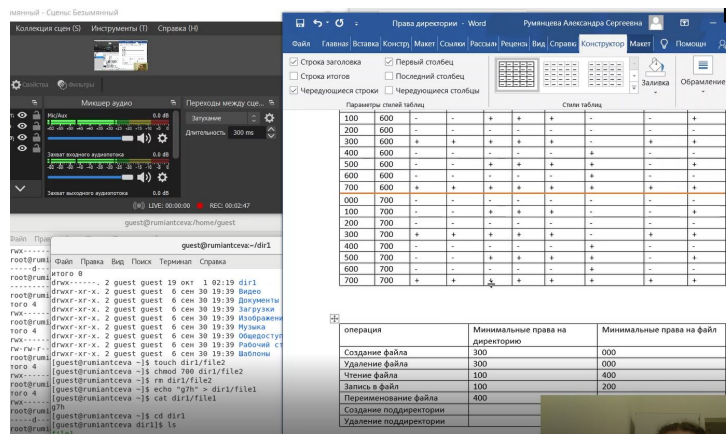


Figure 4.11: рис.11. Выполнение заполнения таблицы 2.

Таким образом у нас получилась следующая таблица:

Операция	Мин. права на директорию	Мин. права на файл
Создание файла	300	000
Удаление файла	300	000
Чтение файла	100	400
Запись в файл	300	200
Переименование файла	300	000
Создание поддиректории	300	-
Удаление поддиректории	300	-

В последнем столбце “-”, так как не зависит от файла

5 Библиография

1. ТУИС РУДН
2. Статья на сайте rizado.ru <https://rizado.ru/2019/03/23/prava-dostupa-k-fajlam-v-linux-ili-cto-takoe-666/#:~:text=Права%20можно%20задавать%20либо%20буквами,значения%2C%20можно%20получать%20разные%20права>

6 Выводы

Я получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.