Отчёт по лабораторной работе 3

Дискреционное разграничение прав в Linux. Два пользователя

Румянцева Александра Сергеевна

Содержание

# Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользовалетей.

# Задание

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

# 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.

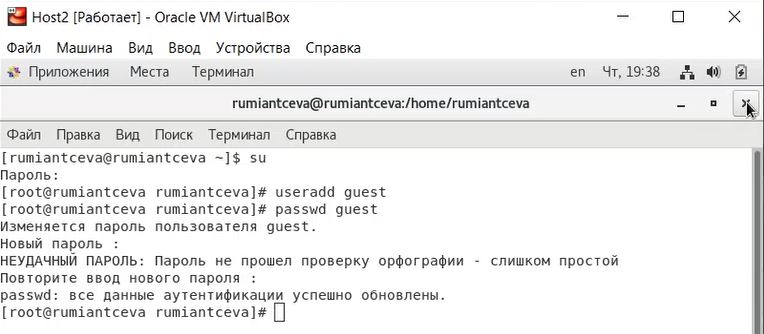
Обычно для документов и файлов данных устанавливаются права 644 или 664. Это означает, что владелец может читать и изменять файл (включая удаление), члены группы в первом случае только читать, а во втором изменять, а все прочие − только читать.

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.

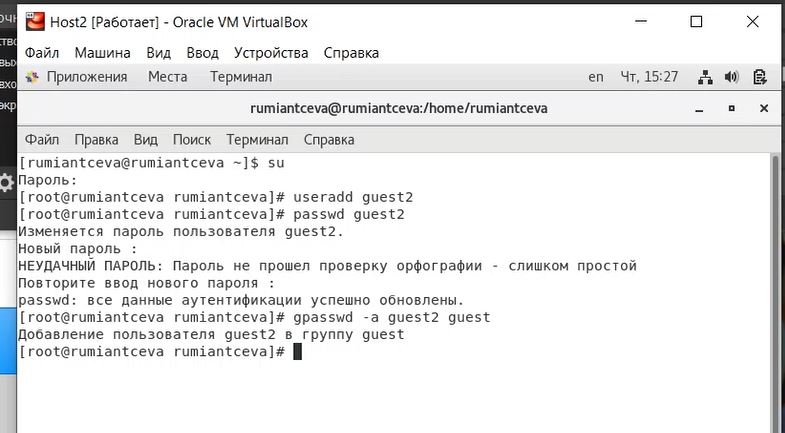
Если задавать права доступа буквами, то указываются нужные права в виде rwx, а то, что нужно пропустить, заменяется дефисом. То есть, 644 соответствует rw-r–r–, а 755 − rwxr-xr-x.

# Выполнение лабораторной работы

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

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

1. Аналогично создала второго пользователя guest и задала для него пароль (рис. 2).
2. Добавила пользователя guest2 в группу guest командой gpasswd -a guest2 guest (рис. 2).

* 
* Figure 2: рис.2. Создание и добавление в группу пользователя guest2.

1. Осуществила вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли (рис. 3)
2. Для обоих пользователей командой pwd определила директорию, в котрой вы находитесь (рис. 3).

Сравнила полученную информацию об именах пользователей с данными, выводимыми в приглашениях командных строк. Имя пользователя во всех командах выводится как guest / guest2, что совпадает с именем в приглашениях командных строк.(рис. 3).

1. Уточните имя пользователей, их группы, кто входит в них и к каким группам принадлежат они сами с помощью команды id для обоих пользователей (рис. 3).

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

Для пользователя guest2: имя пользователя guest2, uid = 1002, его группа guest2, gid = 1002, он входит в группы 1001 (guest) и 1002 (guest2), то есть в свою группу и группу guest.

Определила командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2 (рис. 3). Вижу аналогичные результаты: guest входит только в группу guest, а guest2 в группы guest, guest2.

Сравнила вывод команды groups с выводом команд id -Gn и id -G: релультаты аналогичны: guest входит только в группу guest (1001), а guest2 в группы guest (1001), guest2 (1002). Видим, что id -Gn выводин названия групп, куда входит пользователь, а id -G индексы этих групп.

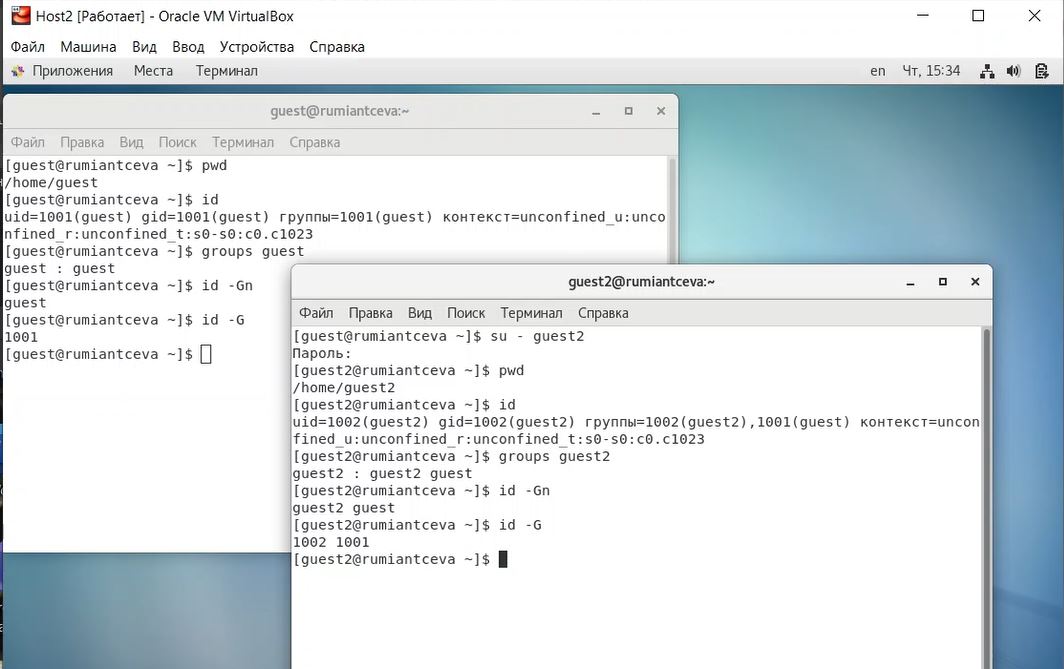


Figure 3: рис.3. Выполнение команд pwd, id и groups, id -Gn, id -G для пользователей guest и guest2.

1. Сравнила полученную информацию с содержимым файла /etc/group, просмотрела файл командой cat /etc/group (рис. 4)

Видим, что в группе guest есть пользователи guest и guest2, а в группе gues2 есть только пользователь guest2.

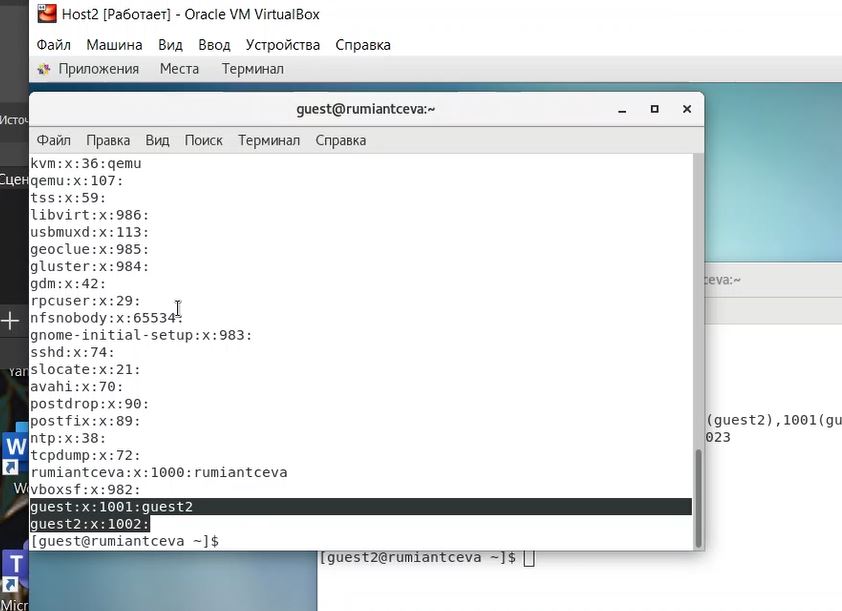
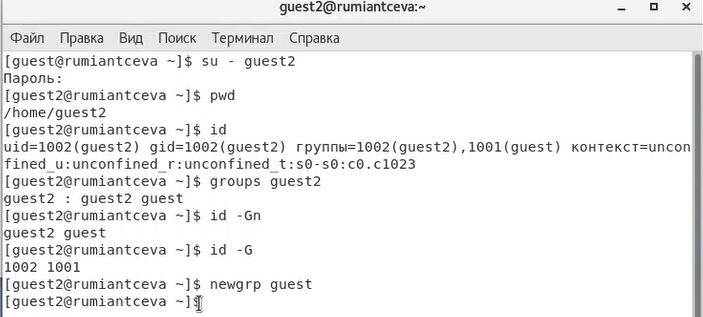


Figure 4: рис.4. Результат выполнения команды cat /etc/group.

1. От имени пользователя guest2 выполнила регистрацию пользователя guest2 в группе guest командой newgrp guest (рис. 5)

* 
* Figure 5: рис.5. Выполнение команды newgrp guest.

1. От имени пользователя guest изменила права директории /home/guest, разрешив все действия для пользователей группы командой chmod g+rwx /home/guest (рис. 6).



Figure 6: рис.6. Выполнение команды chmod g+rwx /home/guest.

1. От имени пользователя guest сняла с директории /home/guest/dir1 все атрибуты командой chmod 000 dirl и проверила правильность снятия атрибутов (рис. 7).

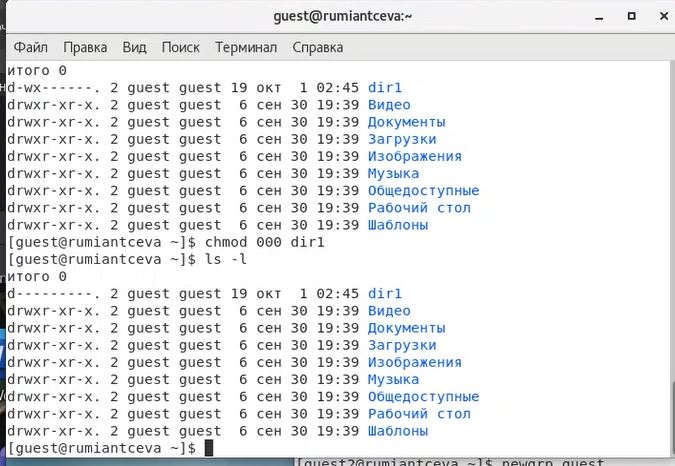


Figure 7: рис.7. Выполнение команды chmod 000 dirl и её проверка.

1. Заполнила таблицу 1 опытным путём, меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2.

Команды для проверки, котрые 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 8 для случая 010 / 000. Таким образом заполнялась вся таблица (рис. 9).

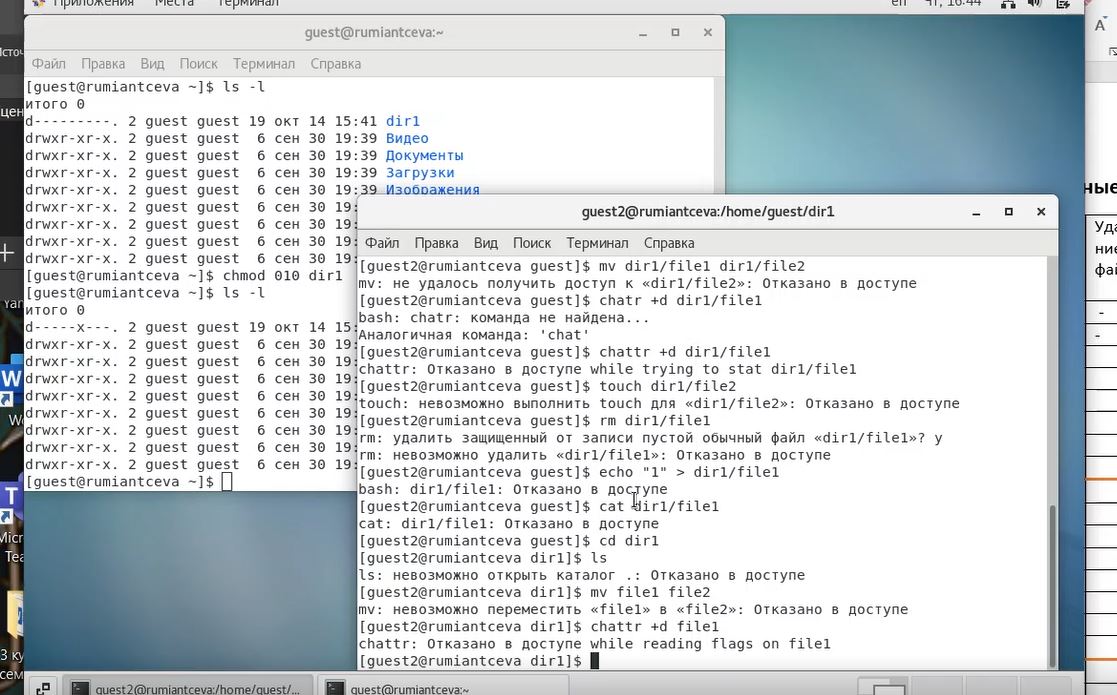


Figure 8: рис.8. Пример выполения команд для заполнения таблицы установленных прав и разрешённых действий над файлами и директориями для случая 010 / 000.

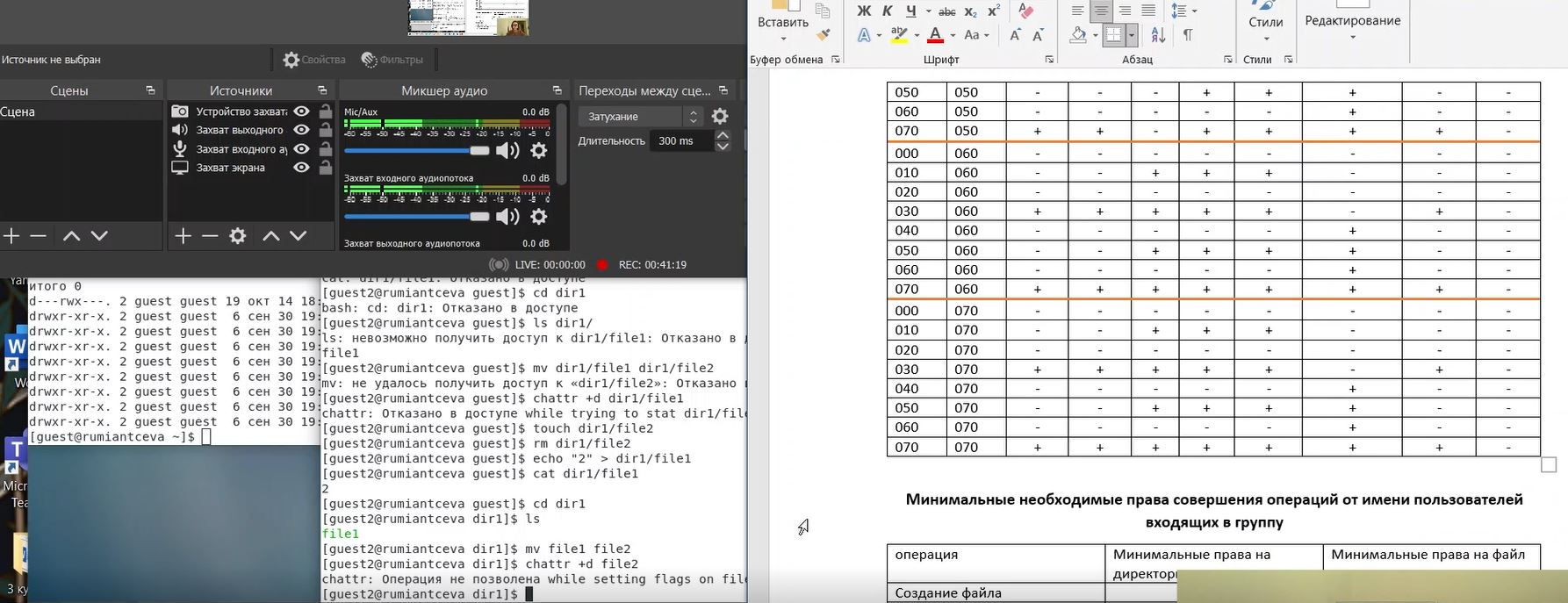


Figure 9: рис.9. Выполнение заполнения таблицы 1.

Таким образом у нас получилась следующая таблица:

| Правка директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение файла | Смена директории | Просмотр файлов в директории | Переименование файла | Смена атрибутов файла |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| d(000) | (000) | - | - | - | - | - | - | - | - |
| d(010) | (000) | - | - | - | - | + | - | - | - |
| d(020) | (000) | - | - | - | - | - | - | - | - |
| d(030) | (000) | + | + | - | - | + | - | + | - |
| d(040) | (000) | - | - | - | - | - | + | - | - |
| d(050) | (000) | - | - | - | - | + | + | - | - |
| d(060) | (000) | - | - | - | - | - | + | - | - |
| d(070) | (000) | + | + | - | - | + | + | + | - |
|  |  |  |  |  |  |  |  |  |  |
| d(000) | (010) | - | - | - | - | - | - | - | - |
| d(010) | (010) | - | - | - | - | + | - | - | - |
| d(020) | (010) | - | - | - | - | - | - | - | - |
| d(030) | (010) | + | + | - | - | + | - | + | - |
| d(040) | (010) | - | - | - | - | - | + | - | - |
| d(050) | (010) | - | - | - | - | + | + | - | - |
| d(060) | (010) | - | - | - | - | - | + | - | - |
| d(070) | (010) | + | + | - | - | + | + | + | - |
|  |  |  |  |  |  |  |  |  |  |
| d(000) | (020) | - | - | - | - | - | - | - | - |
| d(010) | (020) | - | - | + | - | + | - | - | - |
| d(020) | (020) | - | - | - | - | - | - | - | - |
| d(030) | (020) | + | + | + | - | + | - | + | - |
| d(040) | (020) | - | - | - | - | - | + | - | - |
| d(050) | (020) | - | - | + | - | + | + | - | - |
| d(060) | (020) | - | - | - | - | - | + | - | - |
| d(070) | (020) | + | + | + | - | + | + | + | - |
|  |  |  |  |  |  |  |  |  |  |
| d(000) | (030) | - | - | - | - | - | - | - | - |
| d(010) | (030) | - | - | + | - | + | - | - | - |
| d(020) | (030) | - | - | - | - | - | - | - | - |
| d(030) | (030) | + | + | + | - | + | - | + | - |
| d(040) | (030) | - | - | - | - | - | + | - | - |
| d(050) | (030) | - | - | + | - | + | + | - | - |
| d(060) | (030) | - | - | - | - | - | + | - | - |
| d(070) | (030) | + | + | + | - | + | + | + | - |
|  |  |  |  |  |  |  |  |  |  |
| d(000) | (040) | - | - | - | - | - | - | - | - |
| d(010) | (040) | - | - | - | + | + | - | - | - |
| d(020) | (040) | - | - | - | - | - | - | - | - |
| d(030) | (040) | + | + | - | + | + | - | + | - |
| d(040) | (040) | - | - | - | - | - | + | - | - |
| d(050) | (040) | - | - | - | + | + | + | - | - |
| d(060) | (040) | - | - | - | - | - | + | - | - |
| d(070) | (040) | + | + | - | + | + | + | + | - |
|  |  |  |  |  |  |  |  |  |  |
| d(000) | (050) | - | - | - | - | - | - | - | - |
| d(010) | (050) | - | - | - | + | + | - | - | - |
| d(020) | (050) | - | - | - | - | - | - | - | - |
| d(030) | (050) | + | + | - | + | + | - | + | - |
| d(040) | (050) | - | - | - | - | - | + | - | - |
| d(050) | (050) | - | - | - | + | + | + | - | - |
| d(060) | (050) | - | - | - | - | - | + | - | - |
| d(070) | (050) | + | + | - | + | + | + | + | - |
|  |  |  |  |  |  |  |  |  |  |
| d(000) | (060) | - | - | - | - | - | - | - | - |
| d(010) | (060) | - | - | + | + | + | - | - | - |
| d(020) | (060) | - | - | - | - | - | - | - | - |
| d(030) | (060) | + | + | + | + | + | - | + | - |
| d(040) | (060) | - | - | - | - | - | + | - | - |
| d(050) | (060) | - | - | + | + | + | + | - | - |
| d(060) | (060) | - | - | - | - | - | + | - | - |
| d(070) | (060) | + | + | + | + | + | + | + | - |
|  |  |  |  |  |  |  |  |  |  |
| d(000) | (070) | - | - | - | - | - | - | - | - |
| d(010) | (070) | - | - | + | + | + | - | - | - |
| d(020) | (070) | - | - | - | - | - | - | - | - |
| d(030) | (070) | + | + | + | + | + | - | + | - |
| d(040) | (070) | - | - | - | - | - | + | - | - |
| d(050) | (070) | - | - | + | + | + | + | - | - |
| d(060) | (070) | - | - | - | - | - | + | - | - |
| d(070) | (070) | + | + | + | + | + | + | + | - |

Можно заметить, что таблица очень похожа на 1 таблицу из лабораторной 2, единственное различие - нигде нет доступа для смены атрибутов файла, значит это может делать только пользователь-владелец.

1. На основании заполненной таблицы в пункте 12 опредяю те или иные минимально необходимые права для выполнения операций внутри директории dir1 от имени пользователей входящих в группу (рис. 10).

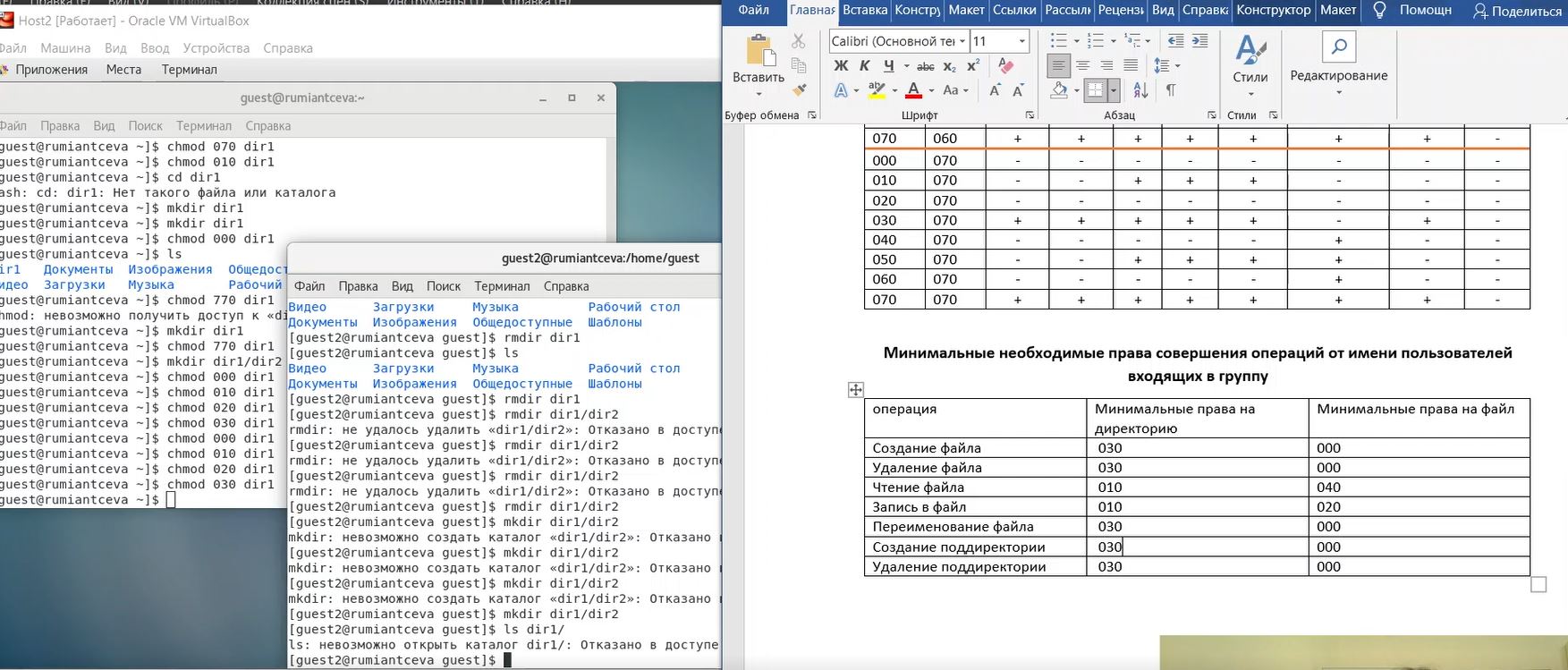


Figure 10: рис.10. Выполнение заполнения таблицы 2.

Таким образом у нас получилась следующая таблица:

| Операция | Мин. права на директорию | Мин. права на файл |
| --- | --- | --- |
| Создание файла | 030 | 000 |
| Удаление файла | 030 | 000 |
| Чтение файла | 010 | 040 |
| Запись в файл | 010 | 020 |
| Переименование файла | 030 | 000 |
| Создание поддиректории | 030 | - |
| Удаление поддиректории | 030 | - |

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

# Библиография

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

# Выводы

Я получила практические навыки работы в консоли с атрибутами файлов для групп пользовалетей.