Отчет по лабораторной работе №2

Дискреционные разграничения прав в Linux. Основные атрибуты

Евсеева Дарья Олеговна

17 сентября, 2022

Содержание

# Цель работы

Целью данной работы является 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.

# Задание

1. Создать гостевого пользователя.
2. Провести работу с директориями от имени гостевого пользователя.
3. Заполнить таблицы прав доступа.

# Теоретическое введение

Дискреционное разграничение доступа — подход к разграничению доступа, предполагающий назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют.

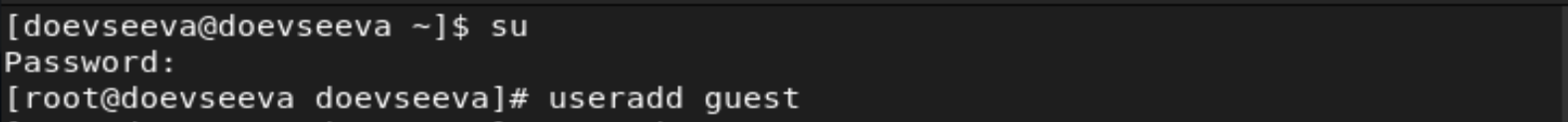
Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей.

# Выполнение лабораторной работы

Выполнять работу будем в операционной системе, установленной при выполнении предыдущей лабораторной работы.

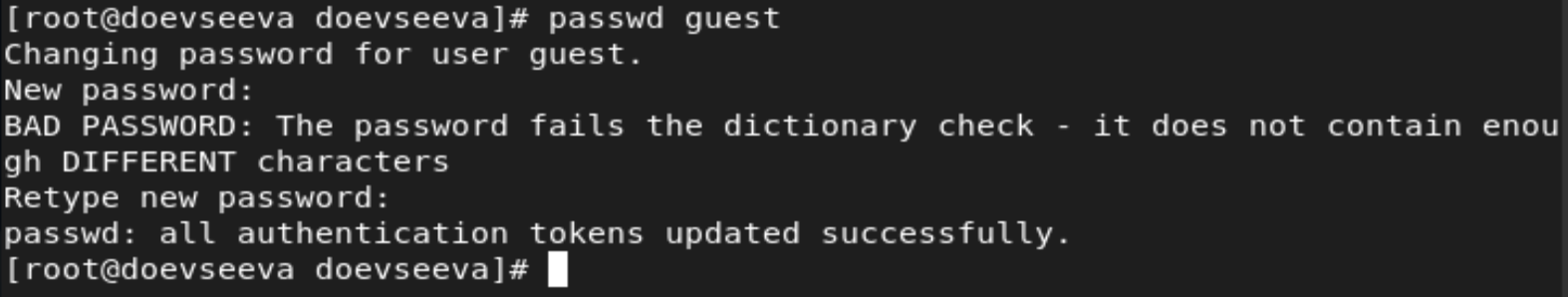
## 1. Создание пользователя

Для начала, используя учетную запись администратора, создадим пользователя guest с помощью команды useradd.



Создание пользователя guest

Дале установим пароль для созданного пользователя.



Установка пароля для пользователя guest

Войдем в систему от имени созданного пользователя guest.



Вход в систему через пользователя guest

Выполним команду pwd, чтобы определить текущую директорию.



Определение текущей директории

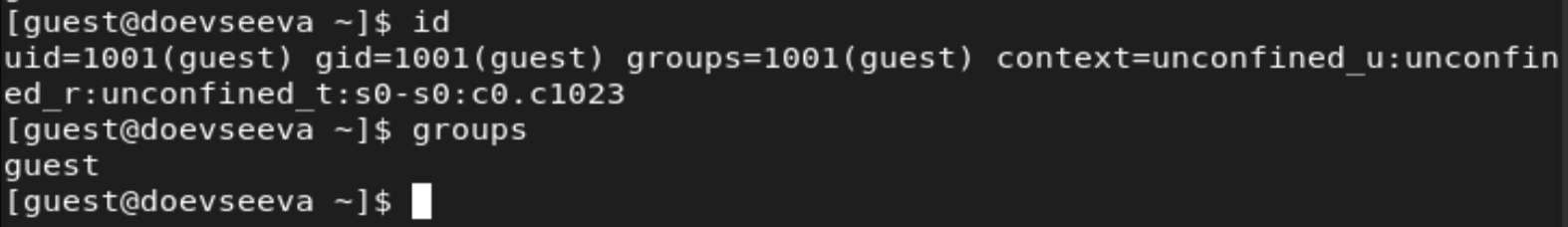
Мы видим, что директория является домашней директорией для пользователя guest и совпадает с приглашением командной строки.

Выполним команду whoami для уточнения имени пользователя.



Уточнение имени пользователя

Далее выполним команду id для просмотра информации о пользователе. Также проверим вывод команды groups.

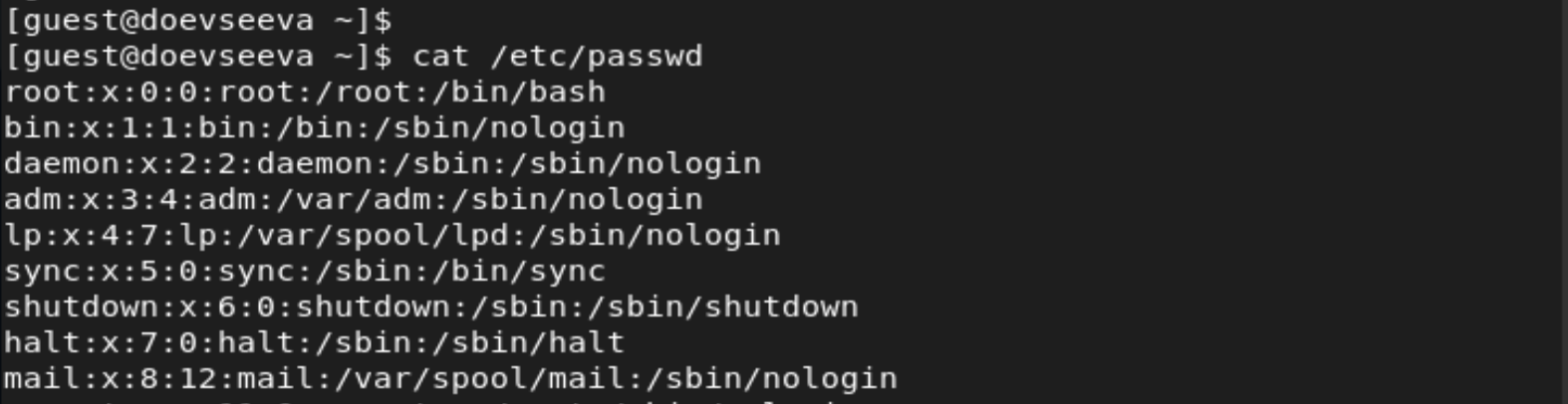


Просмотр информации о пользователе

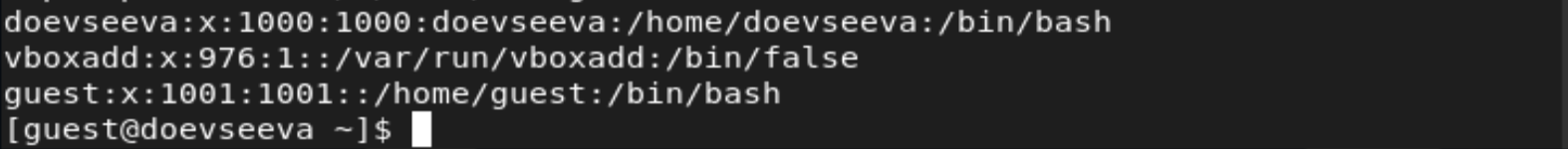
Здесь мы видим, что имя пользователя — guest, значение uid равняется 1001(guest), значение gid равняется 1001(guest), также пользователь входит в единственную группу — 1001(guest). Выводы обеих команд соотносятся друг с другом.

Полученные данные также соответствуют данным в приглашении командной строки.

Посмотрим содержимое файла /etc/passwd.



Просмотр файла /etc/passwd (1)

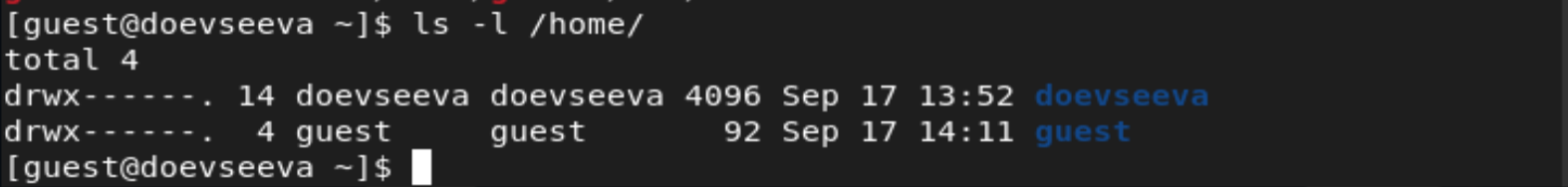


Просмотр файла /etc/passwd (2)

Мы видим, что в последней строке вывода содержится информация о текущем пользователе guest. Значение uid равняется 1001 и значение gid равняется 1001, что совпадает с данными , полученными ранее.

## 2. Работа с директориями

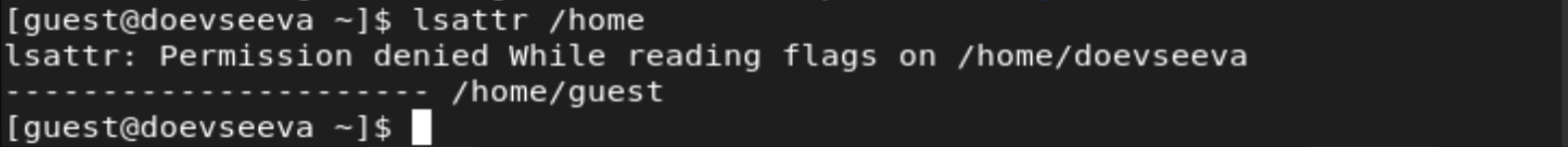
Определим существующие в системе директории.



Просмотр директорий в системе

Нам удалось получить список поддиректорий директории /home, и мы видим, что в системе есть домашние директории пользователей doevseeva и guest. У обеих директорий установлены права на чтение, запись и исполнение для пользователя.

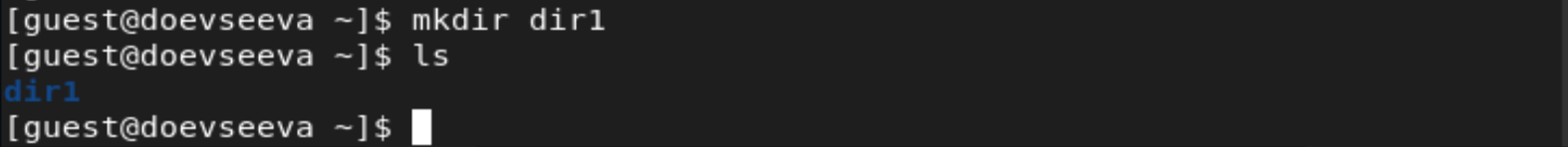
Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home.



Просмотр расширенных атрибутов

Нам удалось получить только данные о домашней директории текущего пользователя guest, и можно видеть, что установленных расширенных атрибутов нет. Данные о домашней директории пользователя doevseeva не были получены.

Создадим в домашней директории поддиректорию dir1.



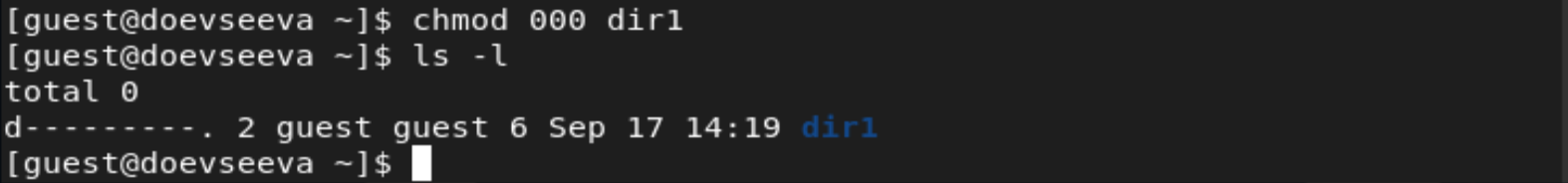
Создание поддиректории dir1

Далее определим, какие права доступа и расширенные атрибуты были выставлены на созданную директорию.



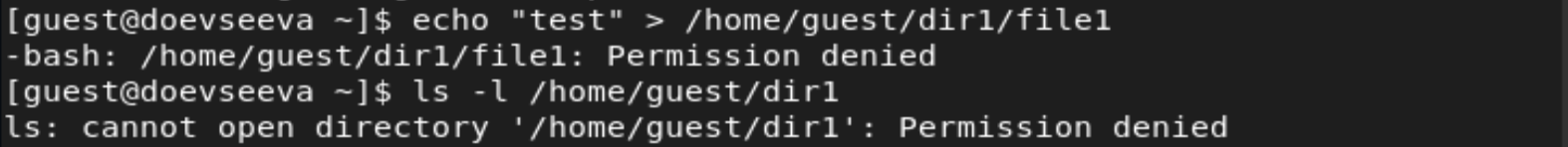
Проверка прав доступа и расширенных атрибутов dir1

Снимем с созданной директории все атрибуты.



Снятие атрибутов с директории

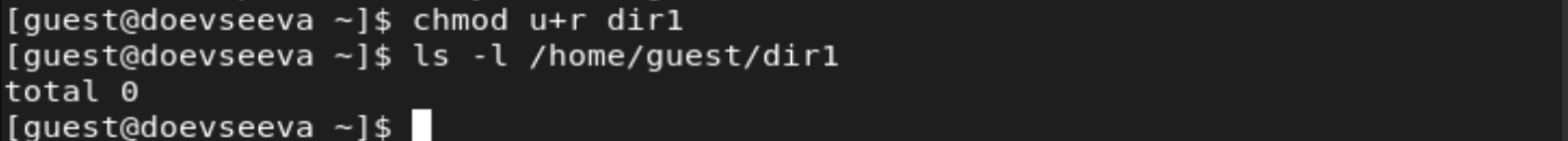
Далее попытаемся создать внутри директории файл.



Проверка возможности создания файла

Как мы видим, в доступе было отказано, так как мы сняли все атрибуты с директории, также из-за этого мы не можем увидеть, действительно ли не создался файл.

Добавим к директории право на чтение и проверим список файлов в ней.



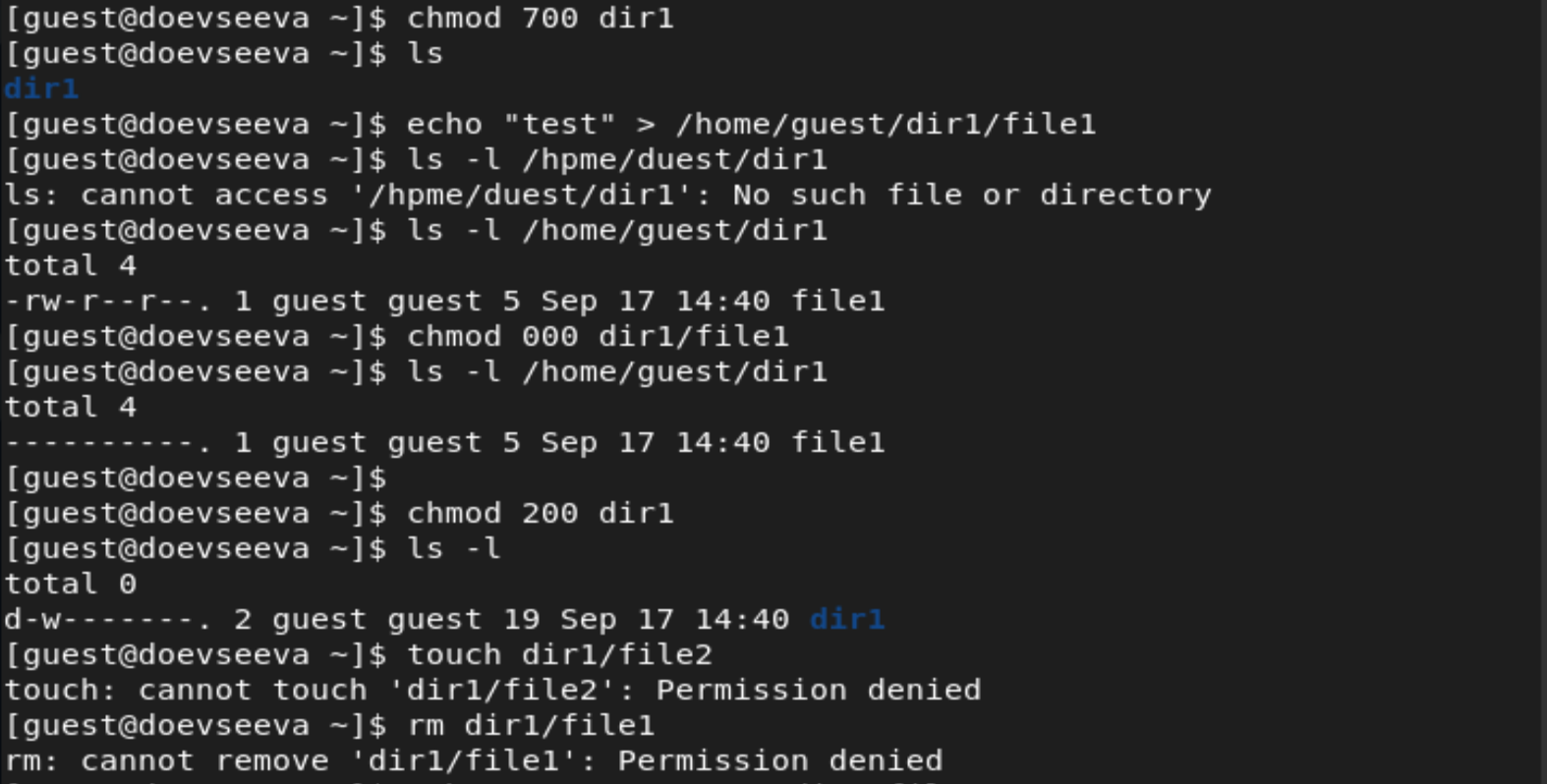
Проверка наличия файла в директории

Мы видим, что директория действительно пуста.

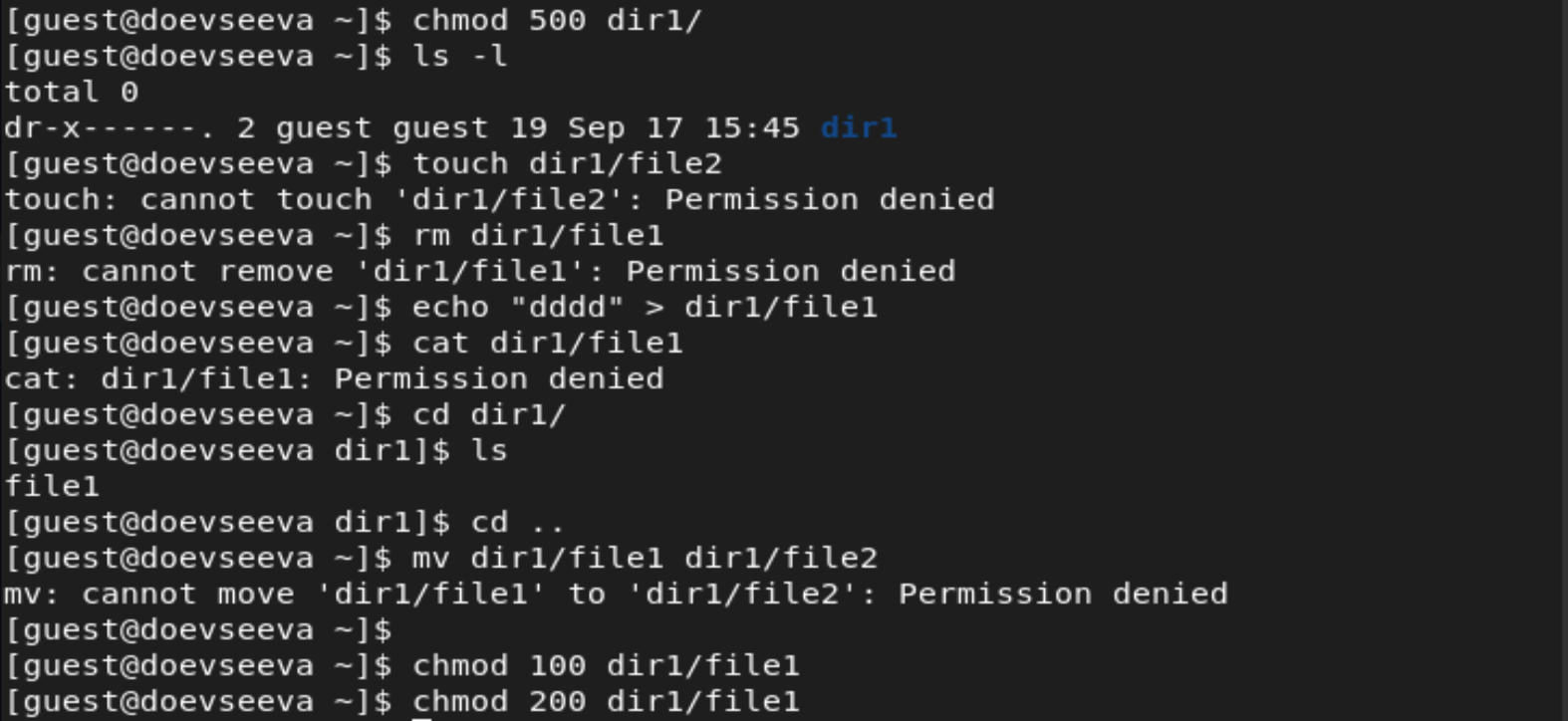
## 3. Заполнение таблиц прав доступа.

Заполним таблицу “Установленные права и разрешенные действия”, выполняя действия от имени владельца директории (файлов), определив опытным путем, какие операции разрешены, а какие нет.

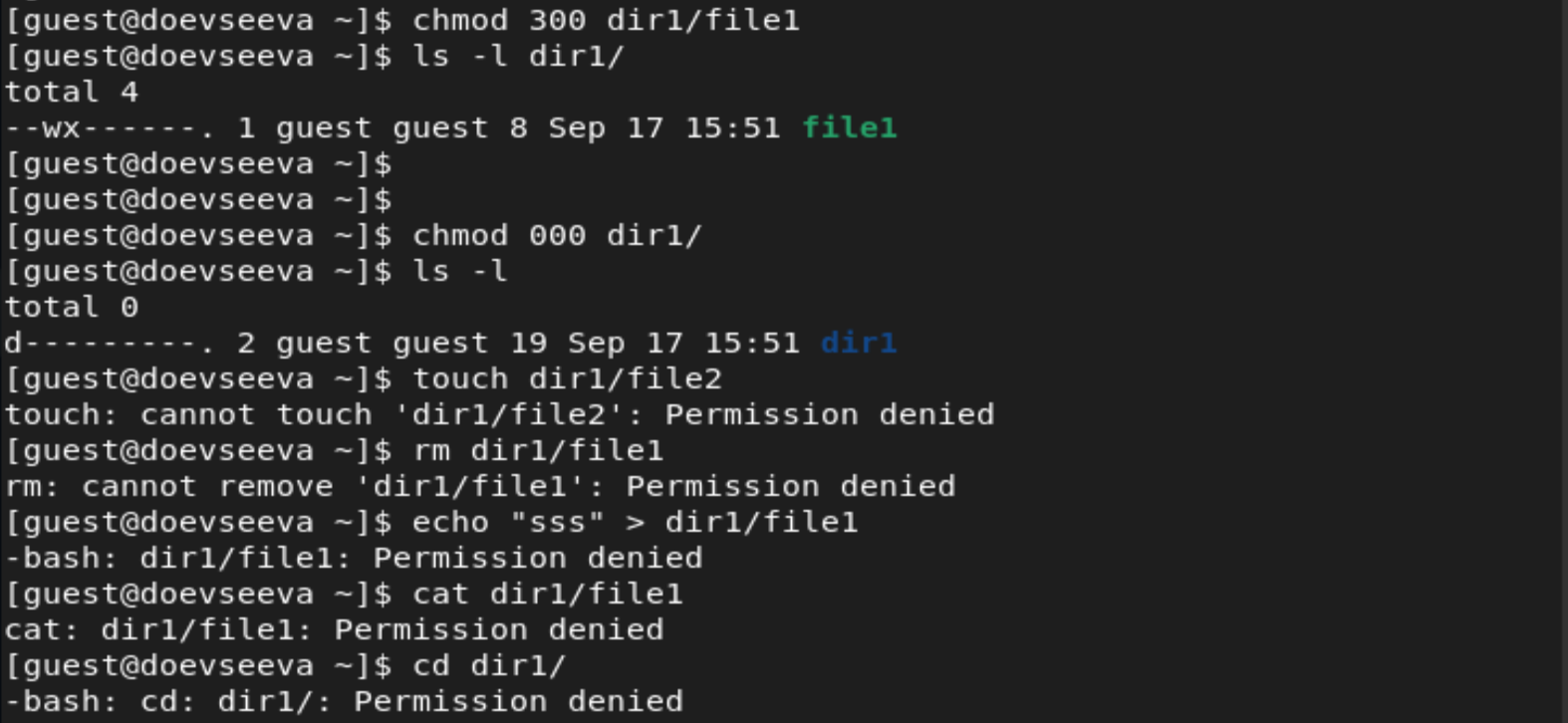
Для начала вернем директории все права доступа для пользователя и создадим в ней файл для дальнейшей проверки действий. Затем приступим к заполнению таблицы.



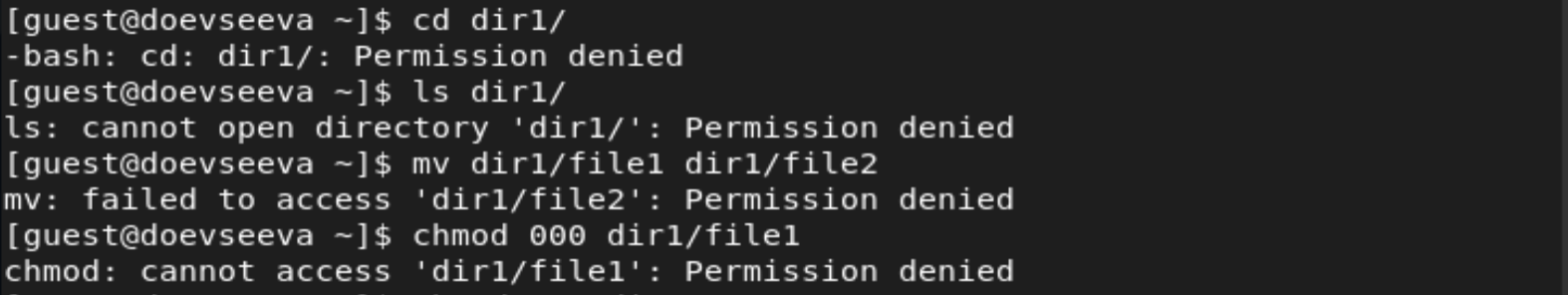
Создание файла и проверка прав и действий



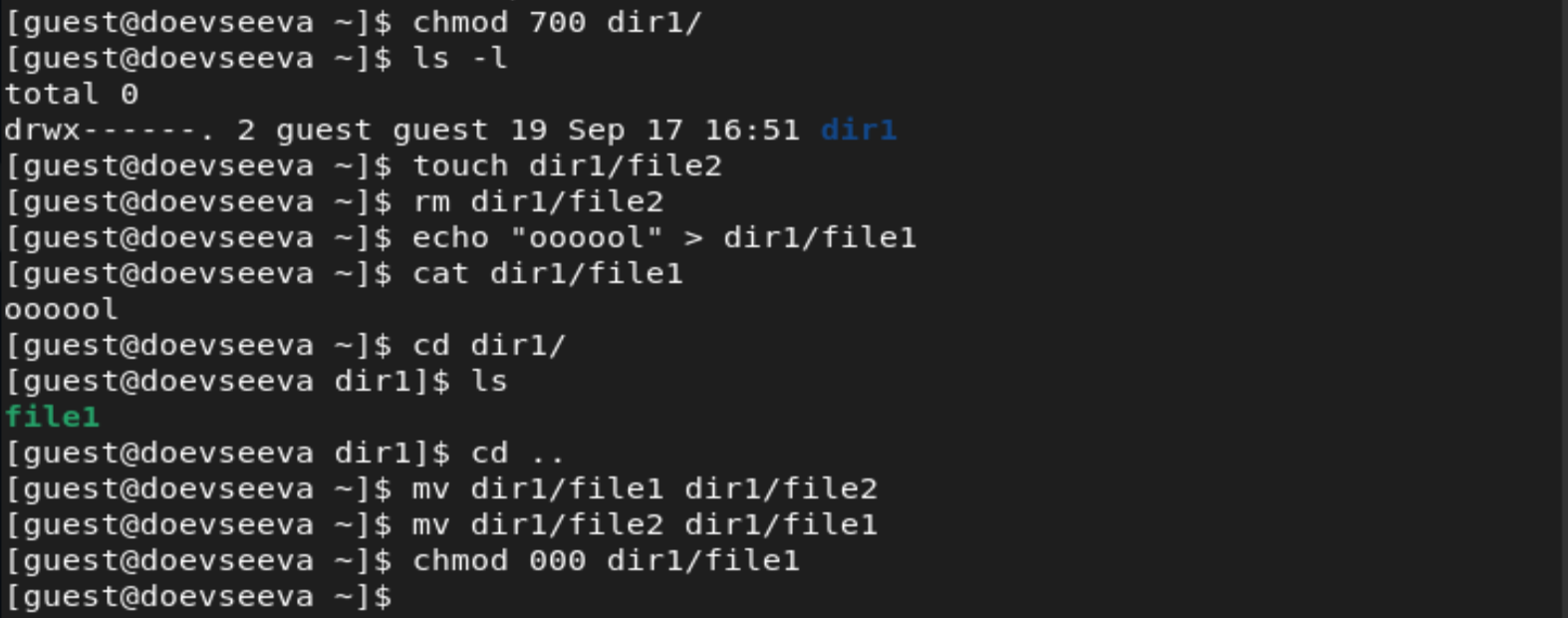
Проверка прав и действий (1)



Проверка прав и действий (2)

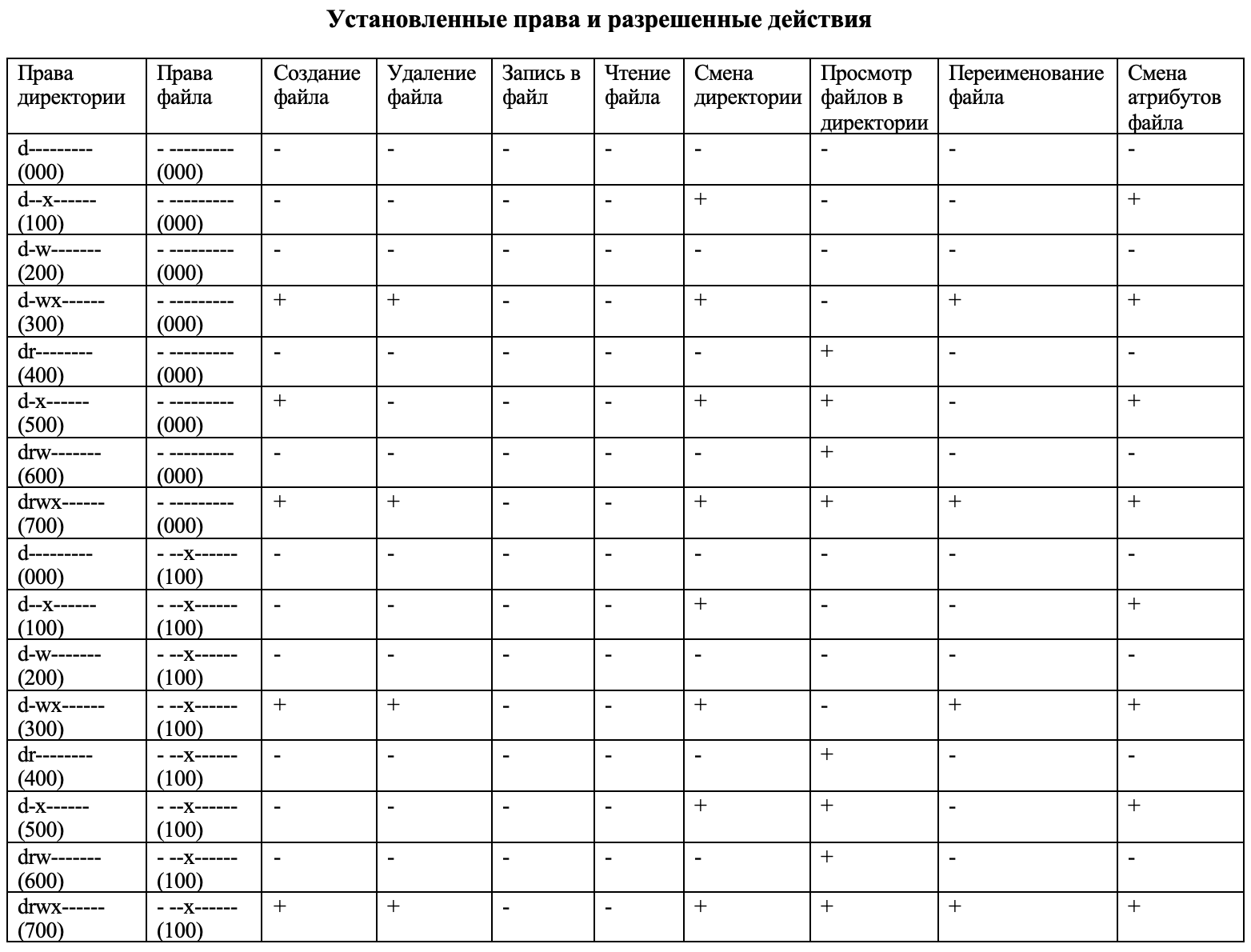


Проверка прав и действий (3)

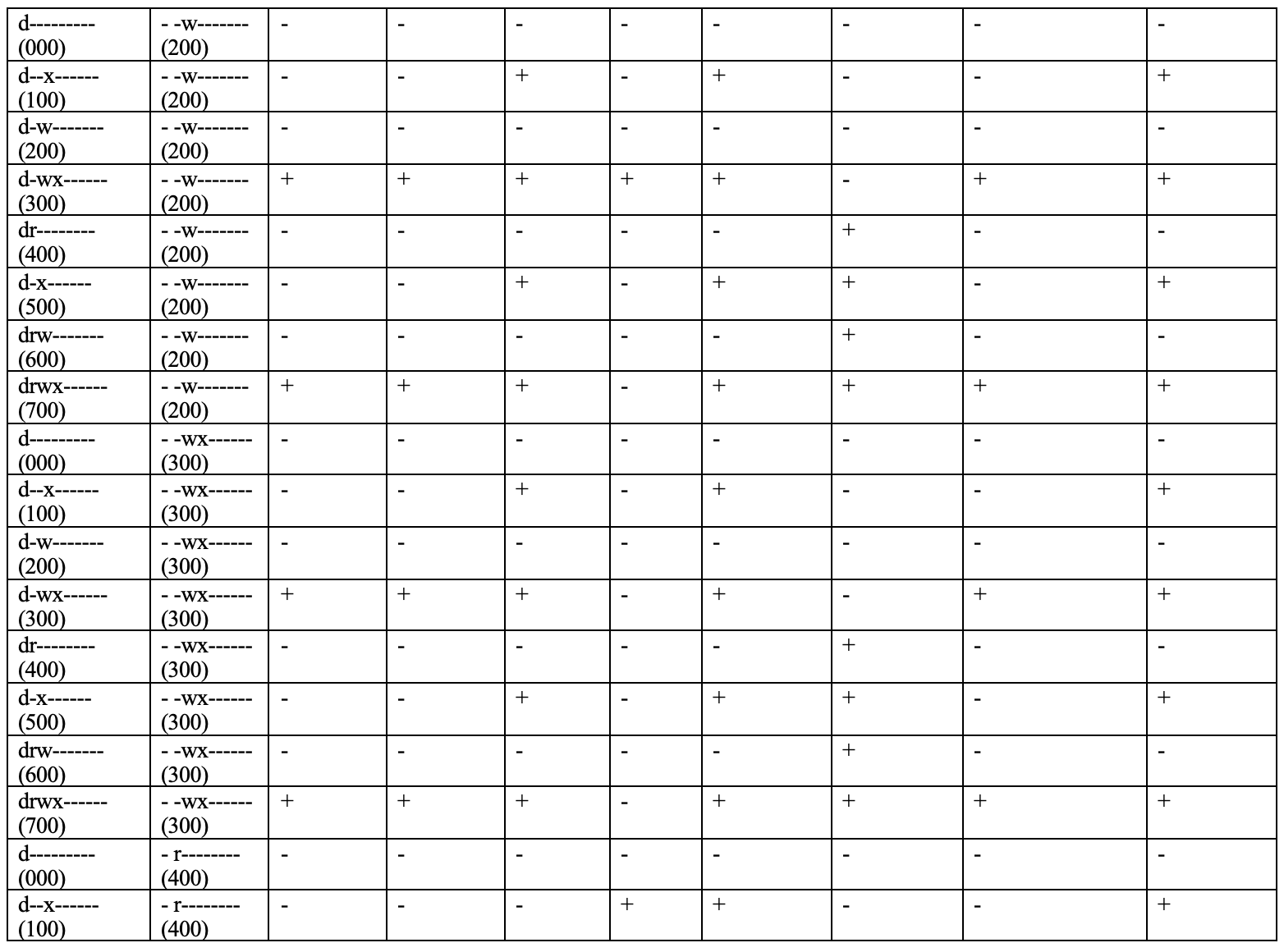


Проверка прав и действий (4)

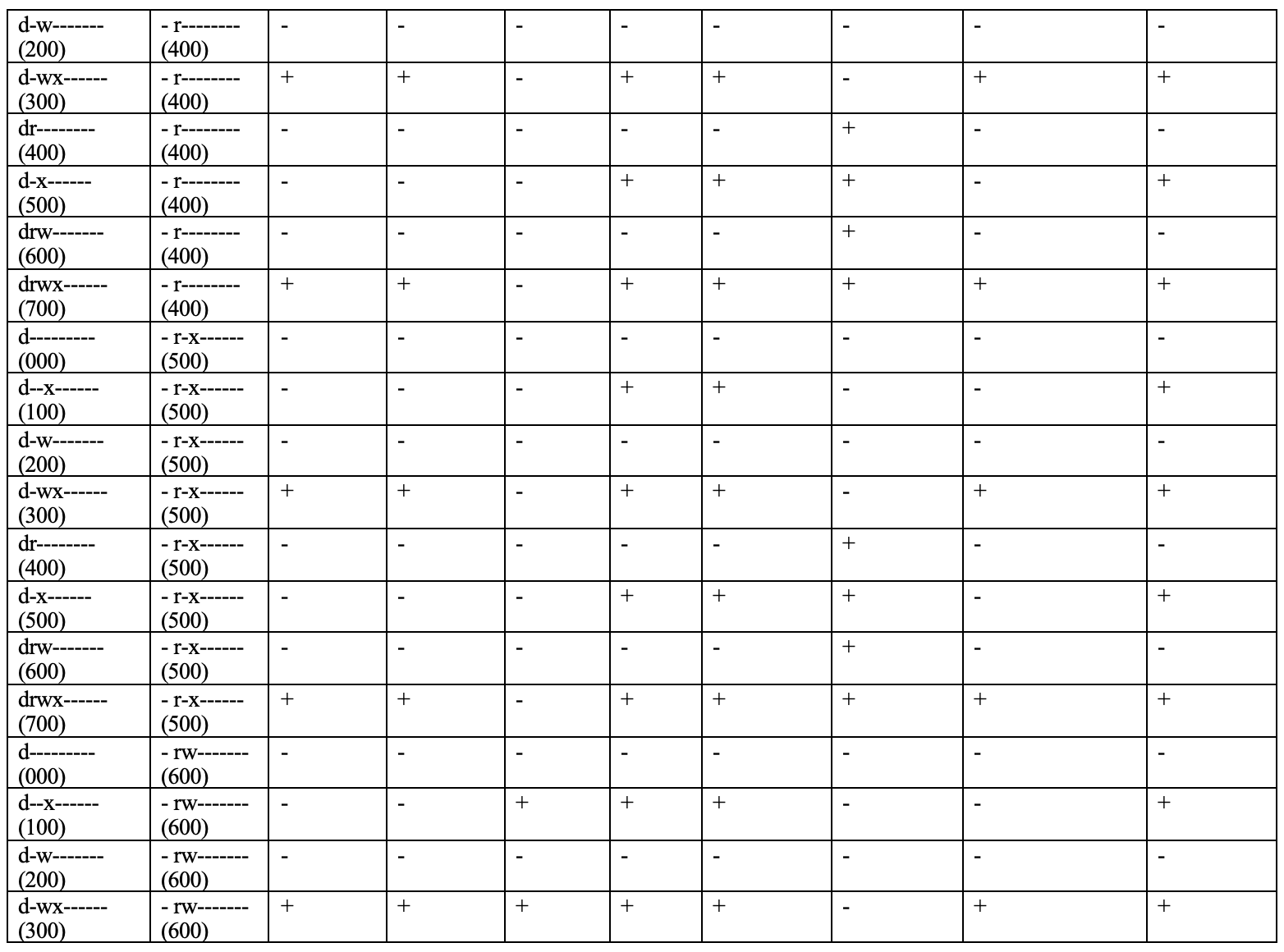
Итак, закончим заполнение таблицы “Установленные права и действия”.



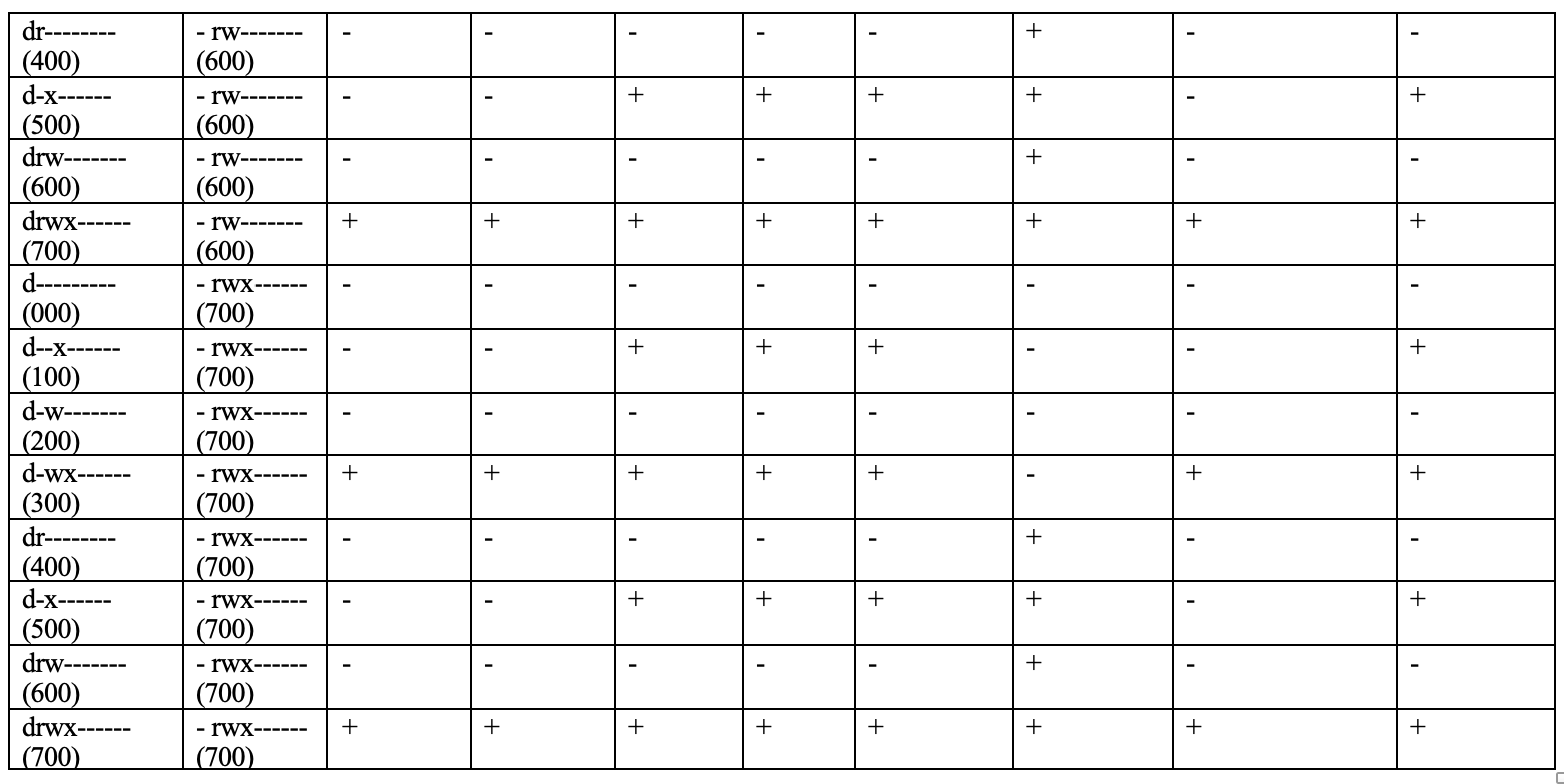
Установленные права и действия (1)



Установленные права и действия (2)

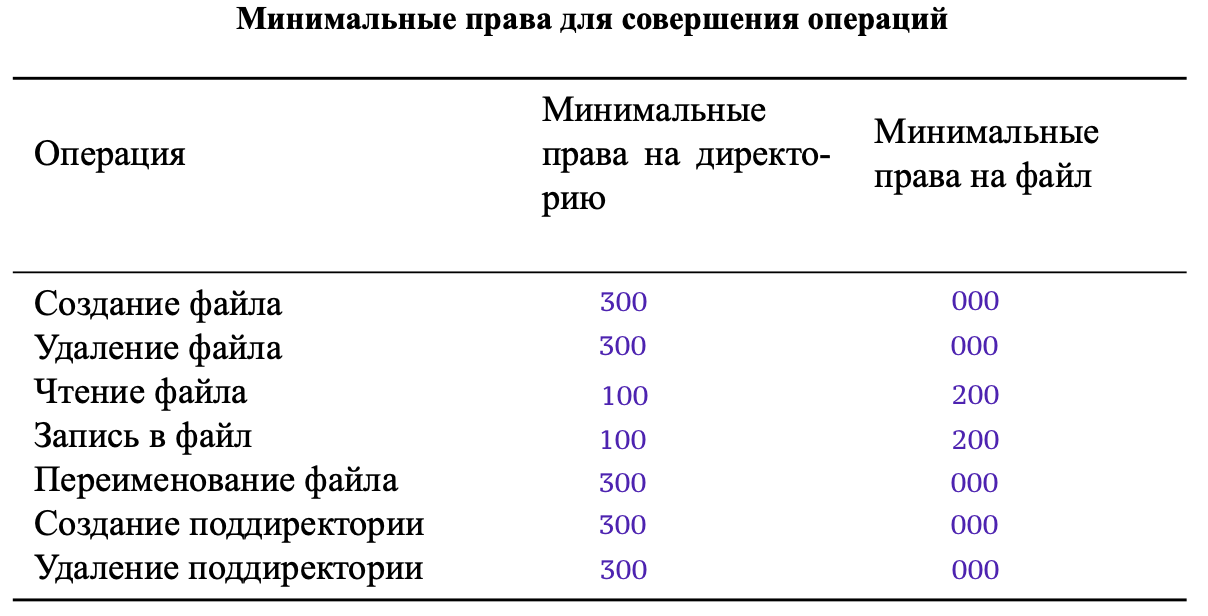


Установленные права и действия (3)



Установленные права и действия (4)

Теперь, на основании заполненной таблицы определим те или иные минимально необходимые права для выполнения операций внутри директории и заполним таблицу “Минимальные права для совершения операций”.



Минимальные права для совершения операций

# Выводы

В результате проделанной работы мы приобрели практические навыки работы в консоли с атрибутами файлов и закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# Список литературы

* Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН” https://esystem.rudn.ru/