Отчёт по лабораторной работе 2

Ду нашсименту Висенте Феликс

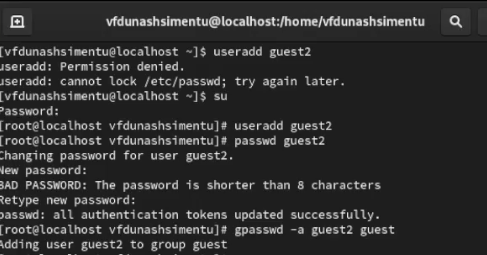
Содержание

## 2.1 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

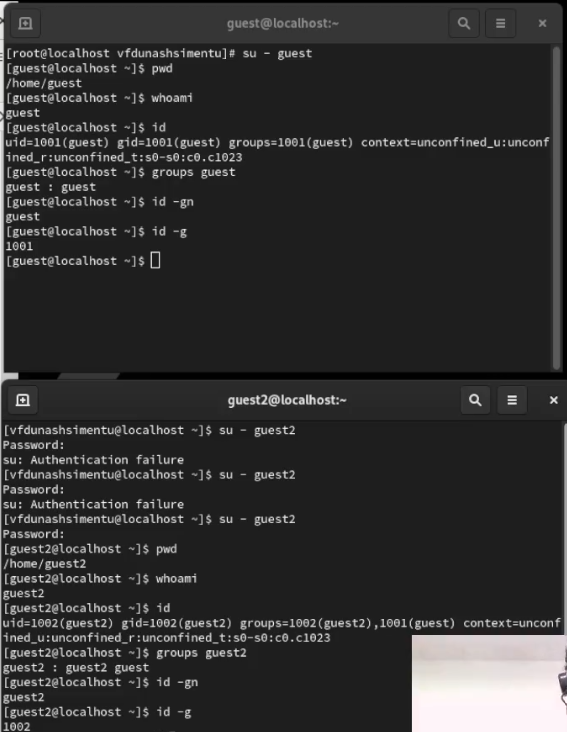
## 2. Указания к работе

Мы установливали при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (использую учётную запись администратора).



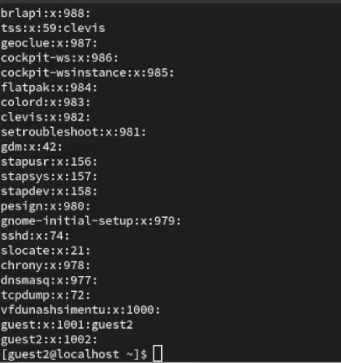
рисунка 1.1

Задавал пароль для пользователя guest (использую учётную запись администратора)



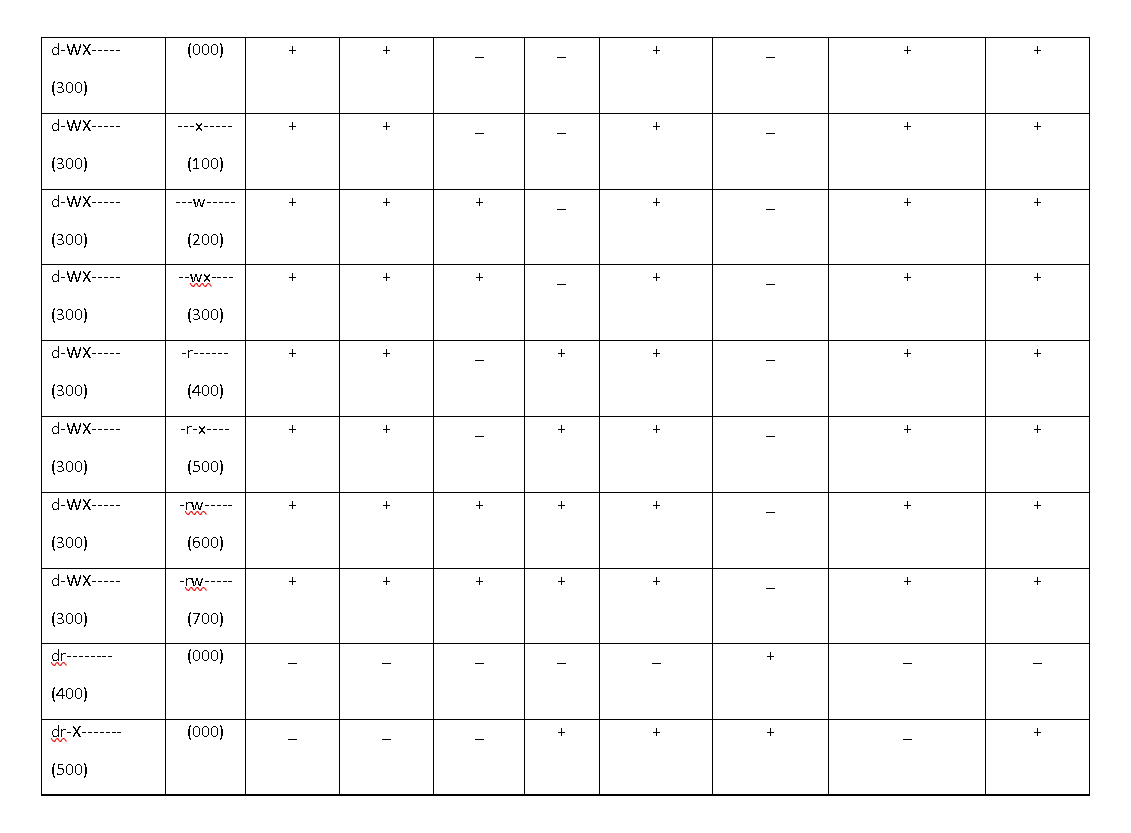
рисунка 1.2

Войду в систему от имени пользователя guest.



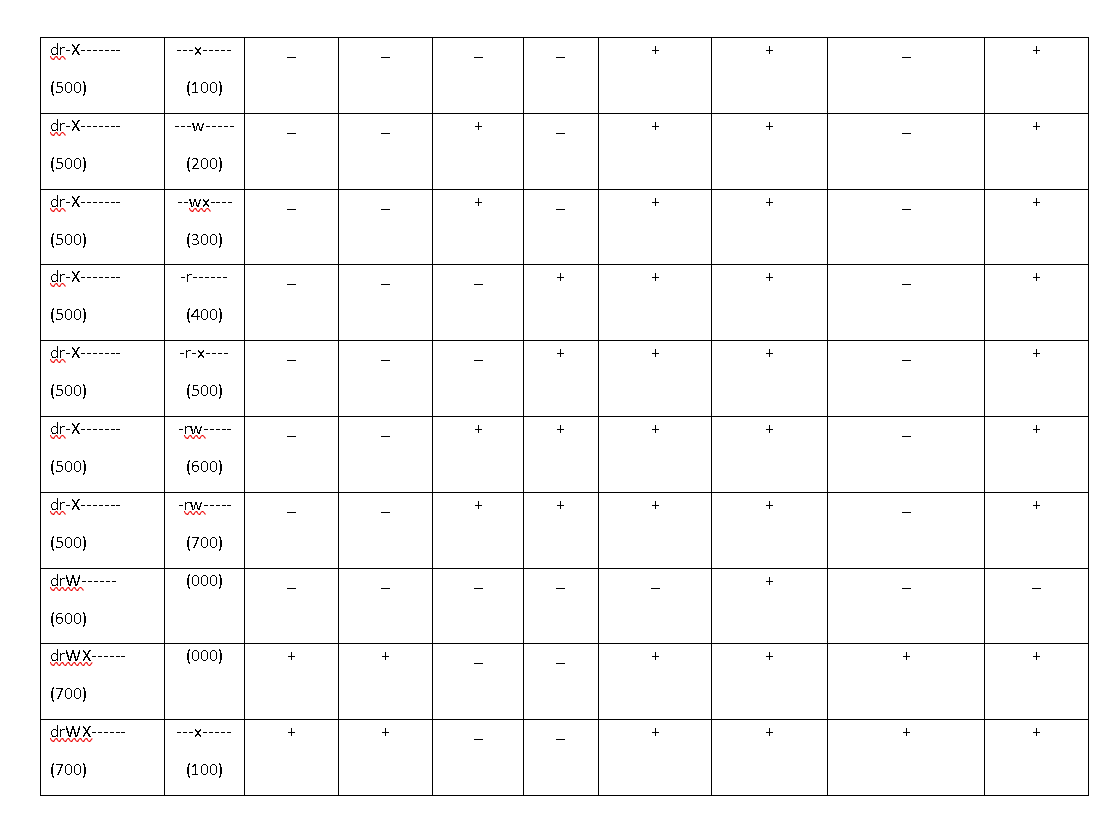
рисунка 1.3

Я определил каталог, в котором нахожусь, с помощью команды pwd. Я сравнил его с командной строкой. Я определил, что она мой домашний каталог.



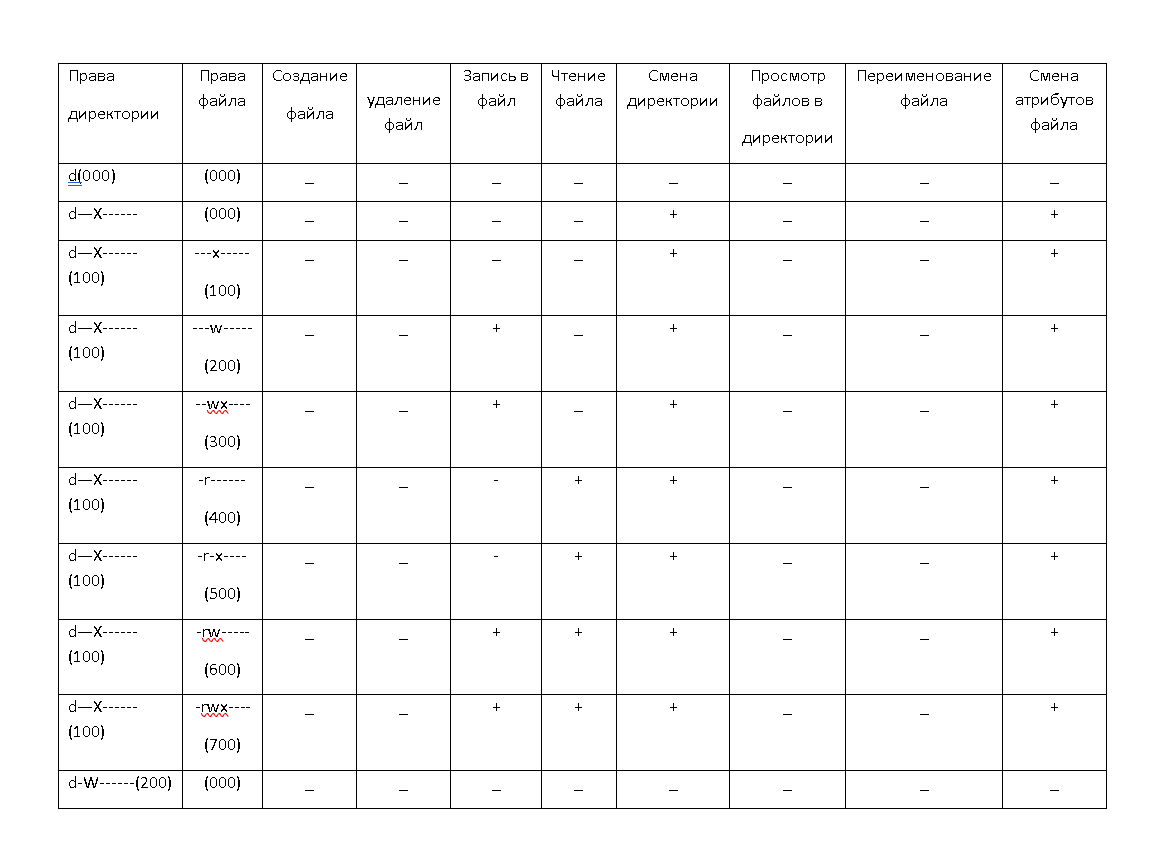
рисунка 1.4

Я Уточнил имя моего пользователя командой whoami.



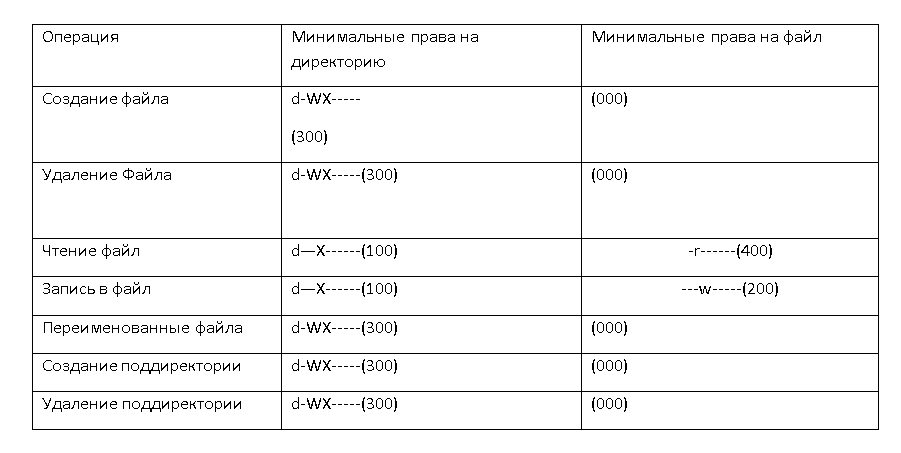
рисунка 1.5

Уточнил имя моего пользователя, его группу, а также группы, куда входит пользователь, командой id. Выведенные значения uid, gid и др. запомните. Сравните вывод id с выводом команды groups.



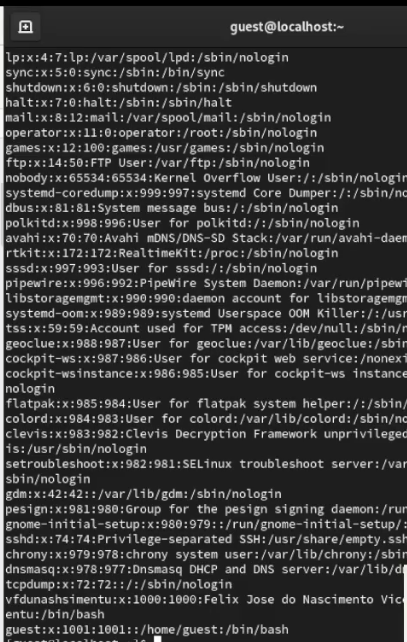
рисунка 1.6

Сравнивал полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. и я мог заметить, что имя было таким же.



рисунка 1.7

Я видел файл / etc / passwd с командой cat / etc / passwd Я нашел свой счет. Я определил uid пользователя. Я определил gid пользователя. Появился пользователь vfdunashsimentu



рисунка 1.8

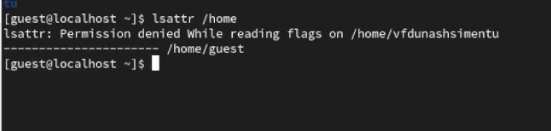
Я определил существующие каталоги в системе с помощью команды ls-l / home/ и мне удалось получить список подкаталогов каталога / home

Итак, drwx—— означает, что это каталог, и только владелец этого каталога имеет права на чтение, запись и доступ к его содержимому, а остальные пользователи не имеют никаких прав доступа к нему.



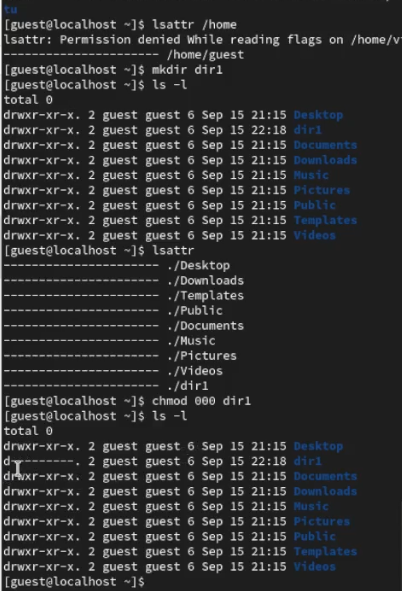
рисунка 1.9

Я проверил, какие расширенные атрибуты установлены в подкаталогах, расположенных в каталоге / home, с помощью команды: lsattr / home Но я не мог видеть ни расширенные атрибуты каталога, ни расширенные атрибуты каталог других пользователей.



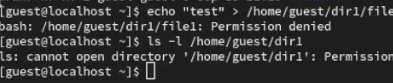
рисунка 1.10

Я создал подкаталог dir1 в домашнем каталоге с помощью команды mkdir dir1. Я определил с помощью команд ls-l и lsattr, какие разрешения и атрибуты расширения были установлены для каталога dir1, и я снял все атрибуты каталога dir1 с помощью команды chmod 000 dir1 и убедитесь, что команда выполнена правильно ls-l.

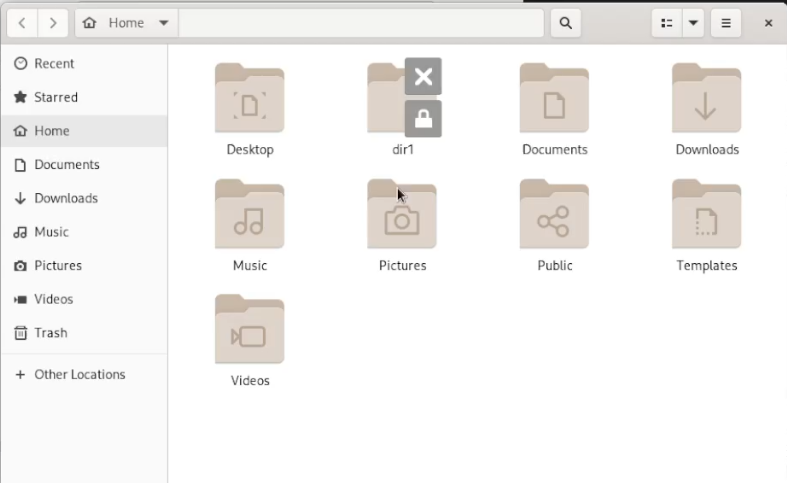


рисунка 1.11

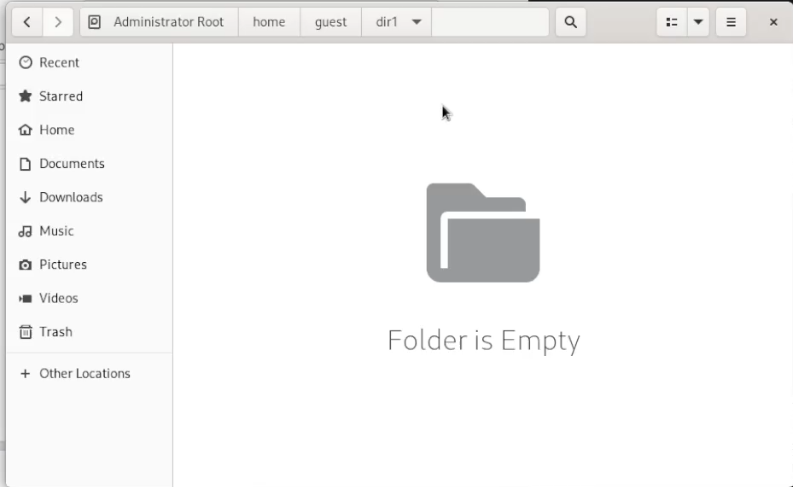
Я попытался создать файл file1 в каталоге dir1 с помощью команды echo “test” > / home / guest / dir1 / file1 Но операция создания файлов была отклонена, потому что у меня нет разрешения на открытие или создание файлов в папке . Я проверил с помощью команды ls-l / home / guest / dir1 файл file1 на самом деле не находится внутри каталога dir1.



рисунка 1.12



рисунка 1.13



рисунка 1.14

Заполнил таблицу «Установленные права и разрешённые действия» , выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесло в таблицу знак «+», если не разрешена, знак «-».

drwx—— - это строка, которая представляет собой права доступа к файлу или каталогу в системе Unix или Linux. Давайте разберем ее часть за частью:

Первый символ d указывает на то, что это каталог. Если бы это был файл, он бы начинался с символа -.

Затем идут три набора прав доступа, каждый из которых состоит из трех символов. Эти символы представляют права для владельца файла, группы и остальных пользователей соответственно.

**r** означает право на чтение. **w** означает право на запись. **x** означает право на выполнение (для каталогов - право на доступ к содержимому). В данном случае:

drw означает, что владелец имеет права на чтение, запись и доступ к содержимому каталога. — означает, что группа и остальные пользователи не имеют никаких прав доступа к этому каталогу. (700) означает, что владелец имеет полные права на чтение, запись и выполнение данного файла или каталога, а группа и остальные пользователи не имеют никаких прав доступа к нему.

**(drW\_\_\_\_\_\_)(600)** указывает, что владелец имеет право на чтение и запись данного файла или каталога, но не имеет права на выполнение. Группа и остальные пользователи не имеют никаких прав доступа к нему.

**(dr\_X\_\_\_\_\_)(500)** указывает, что только владелец имеет право на чтение данного файла или каталога, но не имеет прав на запись или выполнение. Группа и остальные пользователи не имеют никаких прав доступа к нему. **dr\_\_\_\_\_\_\_(400)** указывает, что только владелец имеет право на чтение данного файла или каталога, но не имеет прав на запись или выполнение. Группа и остальные пользователи не имеют никаких прав доступа к нему. Это наименьший уровень прав доступа, при котором файл может быть прочитан владельцем. **d\_WX\_\_\_\_\_(300)**:

Для владельца: 3 (право на чтение и запись, так как 2 - право на запись, и 1 - право на чтение, их сумма равна 3). Для группы: 0 (нет прав доступа). Для остальных пользователей: 0 (нет прав доступа).

(200):

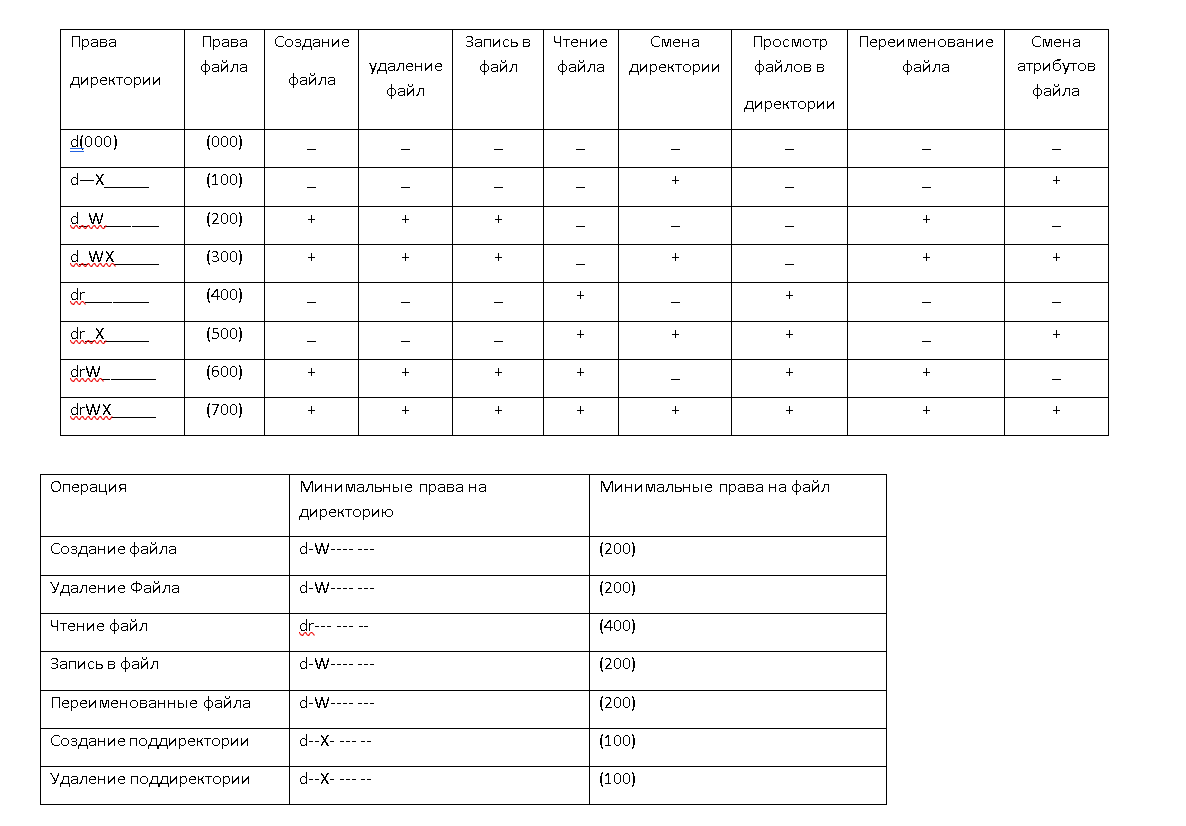
Для владельца: 2 (право на запись). Для группы: 0 (нет прав доступа). Для остальных пользователей: 0 (нет прав доступа).

(100):

Для владельца: 1 (право на чтение). Для группы: 0 (нет прав доступа). Для остальных пользователей: 0 (нет прав доступа).

(000): s Для владельца: 0 (нет прав доступа). Для группы: 0 (нет прав доступа). Для остальных пользователей: 0 (нет прав доступа).

Таким образом, (300) позволяет владельцу читать и записывать файл, а другим пользователям запрещает доступ. (200) позволяет только владельцу записывать файл, а (100) - только читать. (000) полностью запрещает доступ для всех пользователей



рисунка 1.15

## Выводы

Права доступа могут быть комбинированы, чтобы обеспечить необходимый уровень безопасности и функциональности для файлов и каталогов.

Права доступа влияют на то, кто может просматривать, изменять или выполнять файлы и каталоги, и они играют важную роль в обеспечении безопасности системы.

Регулярная проверка и настройка прав доступа являются важными аспектами управления файлами и каталогами в системе Unix/Linux, чтобы обеспечить безопасность данных и ресурсы