Отчет по лабораторной работе №2

по дисциплине: Информационная безопасность

Ким Михаил Алексеевич

Содержание

# 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

1. Создать, настроить пользователя guest и изучить информацию о пользователе.
2. Создать и изучить дериктории, провести эксперименты с правами доступа.
3. Заполнить таблицы “Установленные права и разрешённые действия” и “Минимальные права для совершения операций”.

# 3 Теоретическое введение

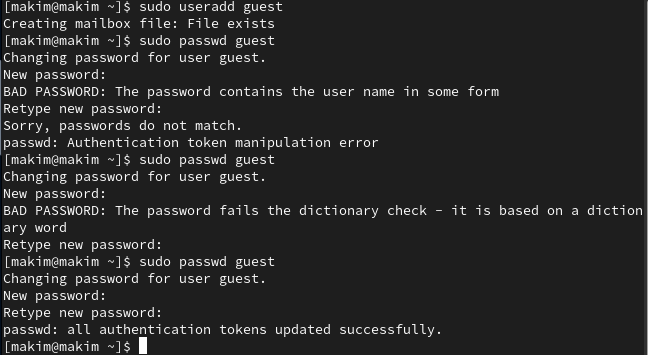
## 3.1 Термины

* Терминал (или «Bash», сокращение от «Bourne-Again shell») — это программа, которая используется для взаимодействия с командной оболочкой. Терминал применяется для выполнения административных задач, например: установку пакетов, действия с файлами и управление пользователями. [1]
* Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами. [2]

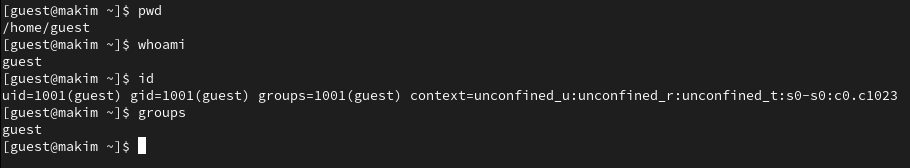
# 4 Выполнение лабораторной работы

## 4.1 Выполнение заданий

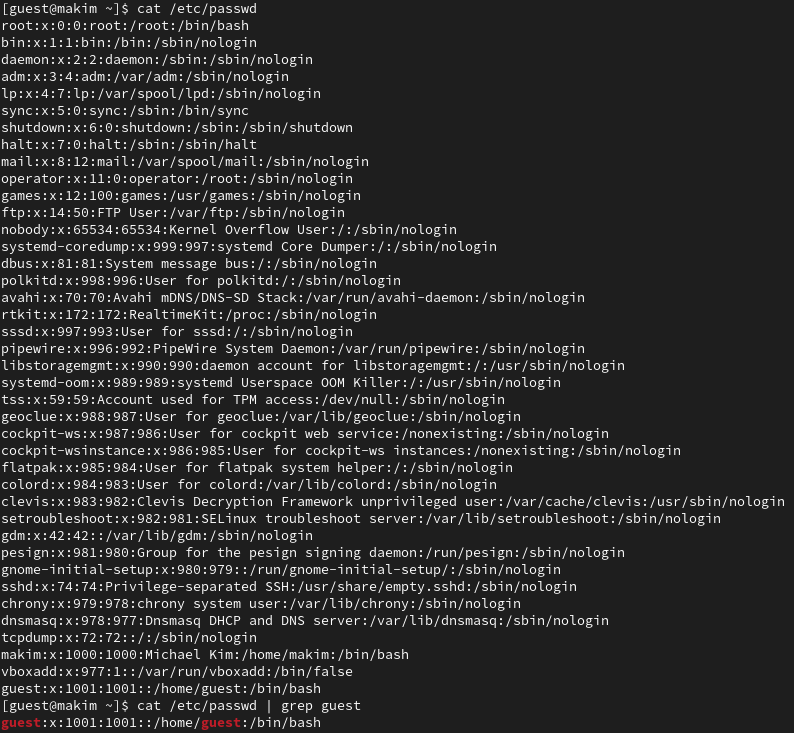
1. В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest (используя учётную запись администратора). Зададим пароль для пользователя guest (рис. [1](#fig:01)):

* 
* Figure 1: Создание новой учетной записи

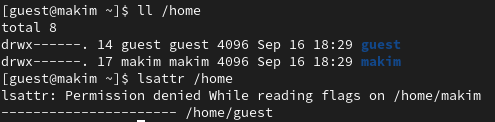
1. Войдем в систему от имени пользователя guest. Определим директорию, в которой находимся, командой pwd. Сравним её с приглашением командной строки: они совпадают. Определим, является ли он домашней директорией: да, является. Уточним имя вашего пользователя командой whoami. Уточним имя пользователя, его группу, а также группы, куда входит пользователь, командой id. Сравним вывод id с выводом команды groups: id выводит информации о пользователе, группе. groups выводит только имя группы. Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки: они совпадают (рис. [2](#fig:02)).

* 
* Figure 2: Использование команд pwd, whoami, id, groups

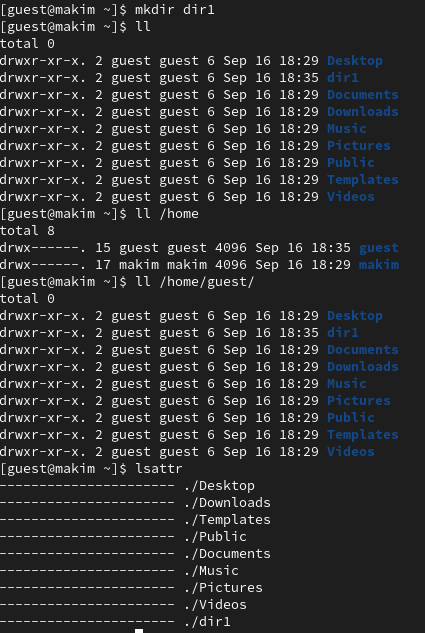
1. Просмотрим файл /etc/passwd командой cat /etc/passwd. Найдем в нём свою учётную запись. Определим uid пользователя (1001). Определите gid пользователя (1001). Сравним найденные значения с полученными в предыдущих пунктах: они совпадают (рис. [3](#fig:03)).

* 
* Figure 3: Просмотр файла /etc/passwd

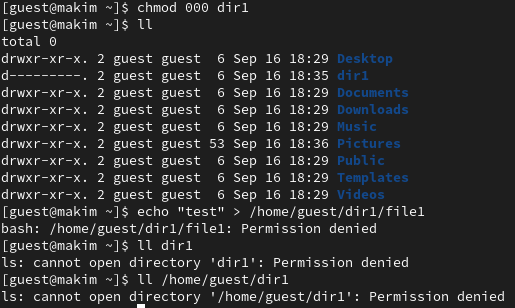
1. Определим существующие в системе директории командой ls -l /home/. Получаем все директории, находящиеся в /home. У них установлены права на чтение, запись и исполнение для пользователя. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: lsattr /home. Расширенные атрибуты удалось увидеть только у текущего пользователя терминала (рис. [4](#fig:04)).

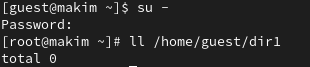
* 
* Figure 4: Директории в /home

1. Создадим в домашней директории поддиректорию dir1. Определим командами, какие права доступа и расширенные атрибуты были выставлены на директорию dir1 (рис. [5](#fig:05)).

* 
* Figure 5: Создание виртуальной машины. 4

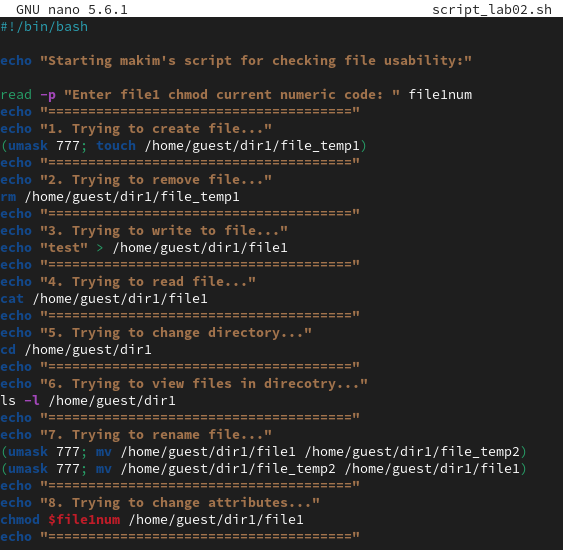
1. Снимем с директории dir1 все атрибуты и проверим с её помощью правильность выполнения команды ls -l. Попытайтемся создать в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1. Мы не можем это сделать, т.к. у пользователя не хватает прав на создание файла. Файл не создастся (рис. [6](#fig:06), [7](#fig:07)).

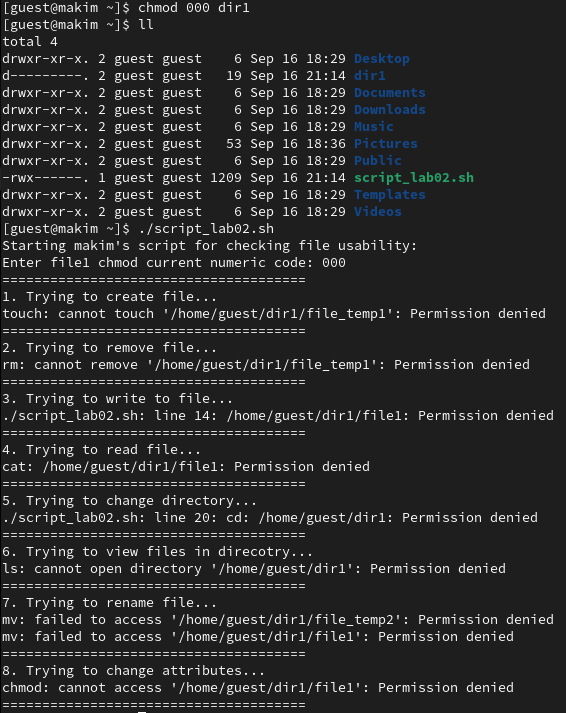
* 
* Figure 6: Изменение атрибутов

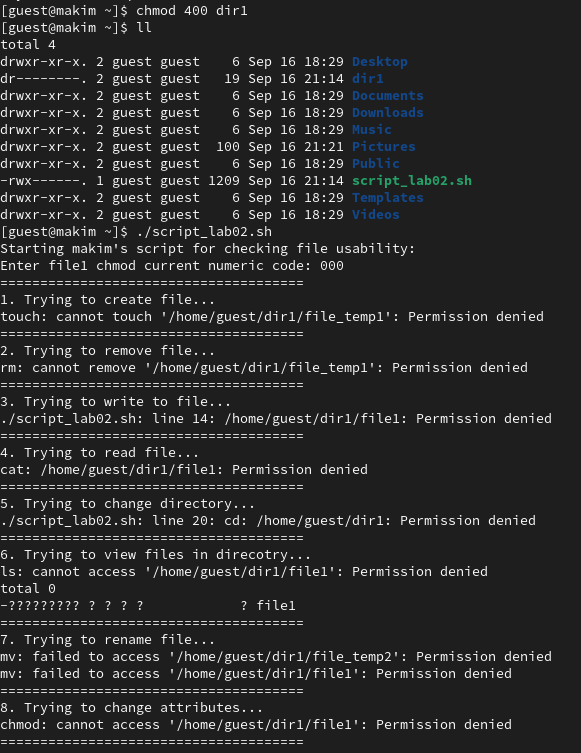
* 
* Figure 7: Использование root-пользователя для просмотра наличия файла

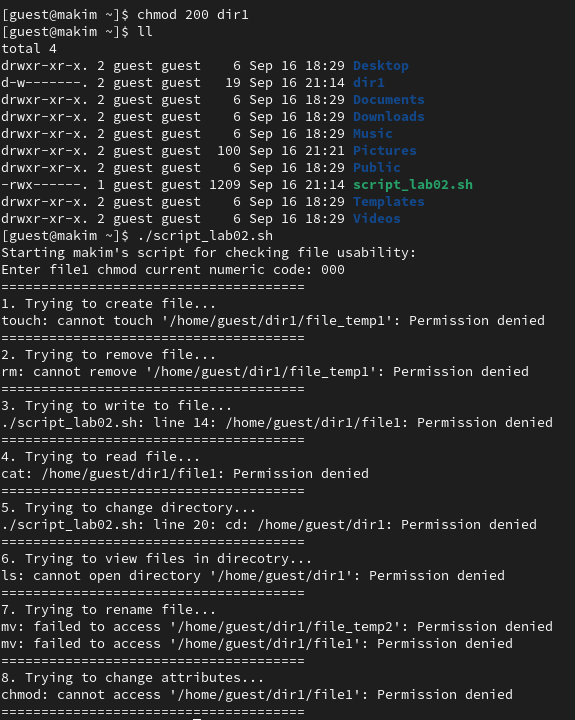
## 4.2 Заполнение таблиц

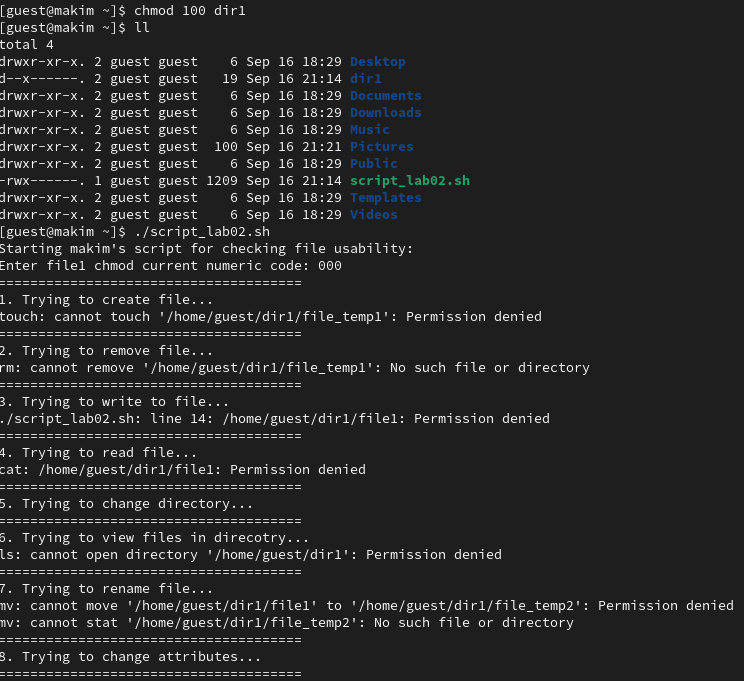
1. Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесем в таблицу знак «+», если не разрешена, знак «-». Для данных целей написал небольшой скрипт, чтобы не писать множество одинаковых команд вручную (рис. [8](#fig:09)). При помощи скрипта будем вносить значения в таблицу (рис. [9](#fig:10), [10](#fig:11), [11](#fig:12), [12](#fig:13), [13](#fig:14), [14](#fig:15), [15](#fig:16), [16](#fig:17)).

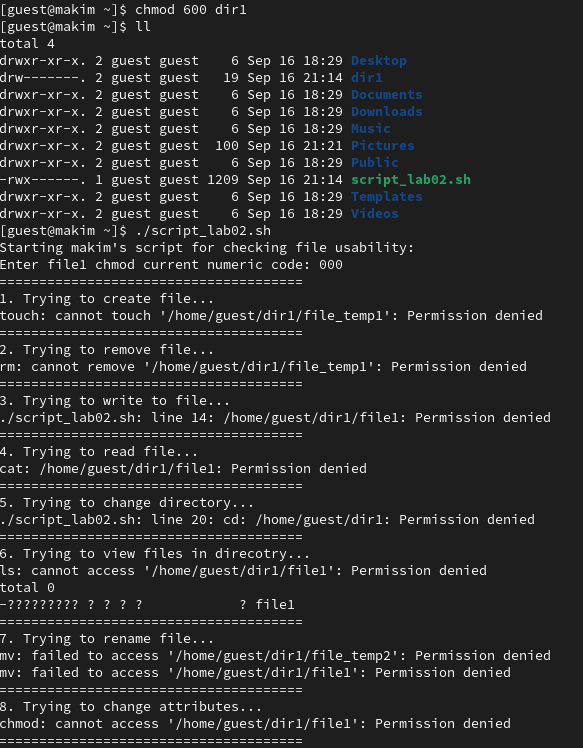
* 
* Figure 8: Bash-script

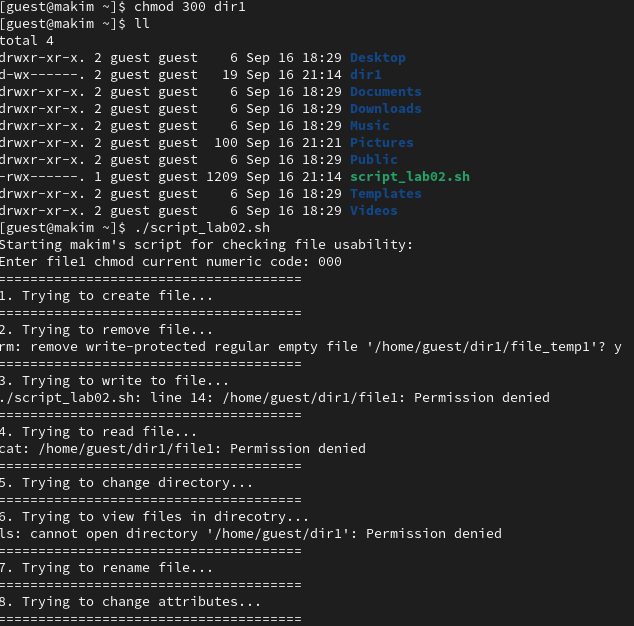
* 
* Figure 9: Использование bash-скрипта. 1

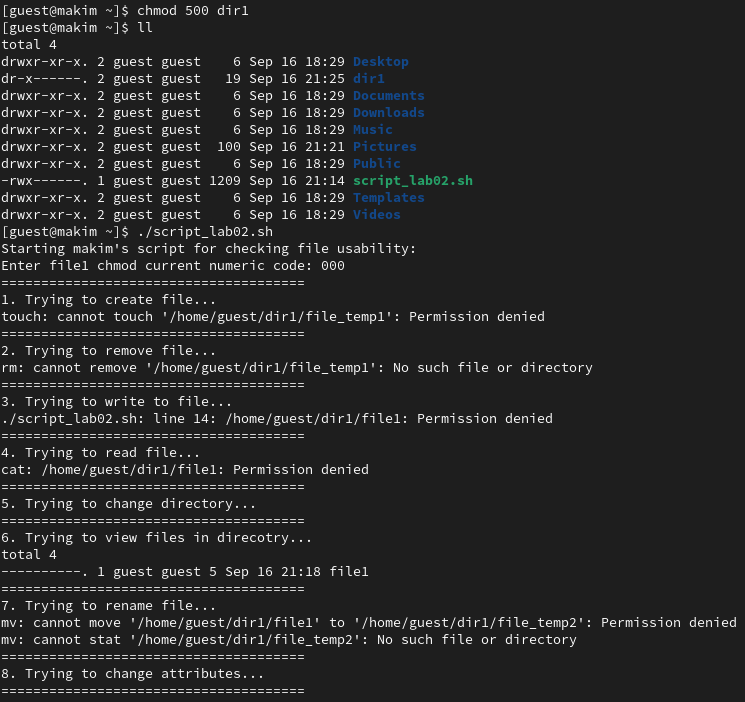
* 
* Figure 10: Использование bash-скрипта. 2

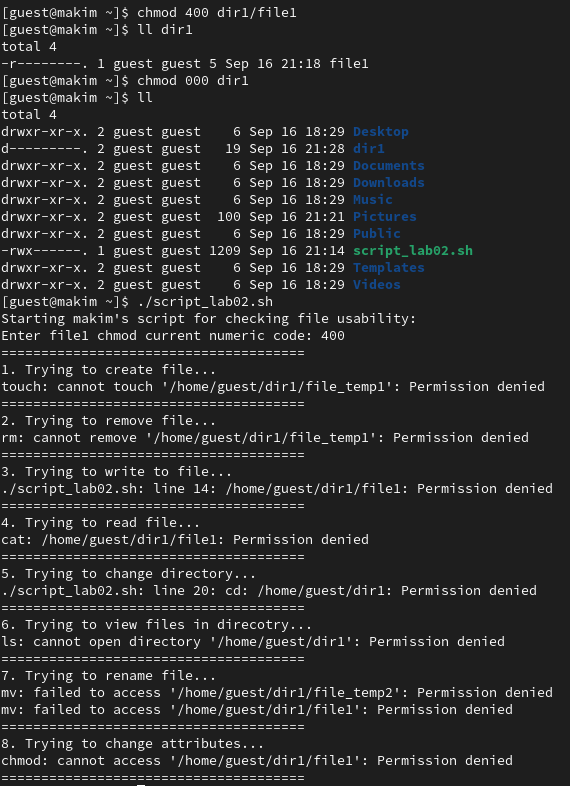
* 
* Figure 11: Использование bash-скрипта. 3

* 
* Figure 12: Использование bash-скрипта. 4

* 
* Figure 13: Использование bash-скрипта. 5

* 
* Figure 14: Использование bash-скрипта. 6

* 
* Figure 15: Использование bash-скрипта. 7

* 
* Figure 16: Использование bash-скрипта. 8

| Права 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——— (000) | –x—— (100) | - | - | - | - | - | - | - | - |
| d——— (000) | -w——- (200) | - | - | - | - | - | - | - | - |
| d——— (000) | -wx—— (300) | - | - | - | - | - | - | - | - |
| d——— (000) | r——– (400) | - | - | - | - | - | - | - | - |
| d——— (000) | r-x—— (500) | - | - | - | - | - | - | - | - |
| d——— (000) | rw——- (600) | - | - | - | - | - | - | - | - |
| d——— (000) | rwx—— (700) | - | - | - | - | - | - | - | - |
| d–x—— (100) | ——— (000) | - | - | - | - | + | - | - | + |
| d–x—— (100) | –x—— (100) | - | - | - | - | + | - | - | + |
| d–x—— (100) | -w——- (200) | - | - | + | - | + | - | - | + |
| d–x—— (100) | -wx—— (300) | - | - | + | - | + | - | - | + |
| d–x—— (100) | r——– (400) | - | - | - | + | + | - | - | + |
| d–x—— (100) | r-x—— (500) | - | - | - | + | + | - | - | + |
| d–x—— (100) | rw——- (600) | - | - | + | + | + | - | - | + |
| d–x—— (100) | rwx—— (700) | - | - | + | + | + | - | - | + |
| d-w——- (200) | ——— (000) | - | - | - | - | - | - | - | - |
| d-w——- (200) | –x—— (100) | - | - | - | - | - | - | - | - |
| d-w——- (200) | -w——- (200) | - | - | - | - | - | - | - | - |
| d-w——- (200) | -wx—— (300) | - | - | - | - | - | - | - | - |
| d-w——- (200) | r——– (400) | - | - | - | - | - | - | - | - |
| d-w——- (200) | r-x—— (500) | - | - | - | - | - | - | - | - |
| d-w——- (200) | rw——- (600) | - | - | - | - | - | - | - | - |
| d-w——- (200) | rwx—— (700) | - | - | - | - | - | - | - | - |
| d-wx—— (300) | ——— (000) | + | + | - | - | + | - | + | + |
| d-wx—— (300) | –x—— (100) | + | + | - | - | + | - | + | + |
| d-wx—— (300) | -w——- (200) | + | + | + | - | + | - | + | + |
| d-wx—— (300) | -wx—— (300) | + | + | + | - | + | - | + | + |
| d-wx—— (300) | r——– (400) | + | + | - | + | + | - | + | + |
| d-wx—— (300) | r-x—— (500) | + | + | - | + | + | - | + | + |
| d-wx—— (300) | rw——- (600) | + | + | + | + | + | - | + | + |
| d-wx—— (300) | rwx—— (700) | + | + | + | + | + | - | + | + |
| dr——– (400) | ——— (000) | - | - | - | - | - | + | - | - |
| dr——– (400) | –x—— (100) | - | - | - | - | - | + | - | - |
| dr——– (400) | -w——- (200) | - | - | - | - | - | + | - | - |
| dr——– (400) | -wx—— (300) | - | - | - | - | - | + | - | - |
| dr——– (400) | r——– (400) | - | - | - | - | - | + | - | - |
| dr——– (400) | r-x—— (500) | - | - | - | - | - | + | - | - |
| dr——– (400) | rw——- (600) | - | - | - | - | - | + | - | - |
| dr——– (400) | rwx—— (700) | - | - | - | - | - | + | - | - |
| dr-x—— (500) | ——— (000) | - | - | - | - | + | + | - | + |
| dr-x—— (500) | –x—— (100) | - | - | - | - | + | + | - | + |
| dr-x—— (500) | -w——- (200) | - | - | + | - | + | + | - | + |
| dr-x—— (500) | -wx—— (300) | - | - | + | - | + | + | - | + |
| dr-x—— (500) | r——– (400) | - | - | - | + | + | + | - | + |
| dr-x—— (500) | r-x—— (500) | - | - | - | + | + | + | - | + |
| dr-x—— (500) | rw——- (600) | - | - | + | + | + | + | - | + |
| dr-x—— (500) | rwx—— (700) | - | - | + | + | + | + | - | + |
| drw——- (600) | ——— (000) | - | - | - | - | - | + | - | - |
| drw——- (600) | –x—— (100) | - | - | - | - | - | + | - | - |
| drw——- (600) | -w——- (200) | - | - | - | - | - | + | - | - |
| drw——- (600) | -wx—— (300) | - | - | - | - | - | + | - | - |
| drw——- (600) | r——– (400) | - | - | - | - | - | + | - | - |
| drw——- (600) | r-x—— (500) | - | - | - | - | - | + | - | - |
| drw——- (600) | rw——- (600) | - | - | - | - | - | + | - | - |
| drw——- (600) | rwx—— (700) | - | - | - | - | - | + | - | - |
| drwx—— (700) | ——— (000) | + | + | - | - | + | + | + | + |
| drwx—— (700) | –x—— (100) | + | + | - | - | + | + | + | + |
| drwx—— (700) | -w——- (200) | + | + | + | - | + | + | + | + |
| drwx—— (700) | -wx—— (300) | + | + | + | - | + | + | + | + |
| drwx—— (700) | r——– (400) | + | + | - | + | + | + | + | + |
| drwx—— (700) | r-x—— (500) | + | + | - | + | + | + | + | + |
| drwx—— (700) | rw——- (600) | + | + | + | + | + | + | + | + |
| drwx—— (700) | rwx—— (700) | + | + | + | + | + | + | + | + |

1. На основании предыдущей таблицы заполним следующую таблицу.

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

# 5 Анализ результатов

Работа выполнена без каких-либо проблем. Работа с терминалом ОС Rocky Linux в данном случае нареканий не вызвала. Также порадовало наличие вкладок в терминале «из коробки».

# 6 Выводы

Получил практические навыки работы в консоли с атрибутами файлов, закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# Список литературы

1. Терминал Linux [Электронный ресурс]. URL: <{https://www.reg.ru/blog/linux-shpargalka-komandy-terminala-dlya-novichkov/#:~:text=%D0%A2%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%20(%D0%B8%D0%BB%D0%B8%20%C2%ABBash%C2%BB%2C,%D1%81%20%D1%84%D0%B0%D0%B9%D0%BB%D0%B0%D0%BC%D0%B8%20%D0%B8%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8F%D0%BC%D0%B8}>.

2. Права доступа [Электронный ресурс]. URL: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>.