Лабораторная работа №2

Дисциплина: Основы информационной безопасности

Феоктистов Владислав Сергеевич

Содержание

# 1 Цель работы

Целью данной работы является: приобретение практических навыков работы в консоли с правами и атрибутами файлов и каталогов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux, проверка необходимых наборов прав для выполнения различных действий над файлами и каталогами, получение навыков чтения выделенных прав через консоль.

# 2 Задание

Создать нового пользователя под именем guest с паролем; войти в систему от имени нового пользователя и получить о нем всю необходимую информацию через консоль; проверить и изменить права на существующие и созданные файлы и каталоги; проверить как снятие всех атрибутов с директории повлияло на возможности работы с ним.

# 3 Теоретическое введение

В ОС Linux права доступа к файлам, атрибуты и владение управляют уровнем доступа, который система обрабатывает, а пользователи имеют к файлам. Это гарантирует, что только авторизованные пользователи и процессы могут получить доступ к опеределенным файлам и каталогам. Атрибуты сосотят из девяти битов, которые и определяют права для разных групп пользователей. Первая тройка битов определяет права доступа для владельца, вторая тройка - для членов группы, последняя тройка - для всех остальных пользователей в системе. Каждая тройка битов (класс пользователей) определяет права на чтение, запись и исполнение. Эта концепция позволяет контролировать, какие пользователи могут читать, записывать (изменять) или выполнять файлы/каталоги.

Чтобы просмотреть права доступа к файлу, использовуется команда ls с опцией -l. Первый символ указывает тип файла. Это может быть обычный файл (-), каталог (d), символическая ссылка (l) или другие спицефические типы файлов. Следующие девять символов предоставляют доступ к файлу, три тройки по три символа каждая (три пользователя, три типа прав: r - чтение, w - запись, x - исполнение).

Права доступа к файлу/каталогу можно изменить с помощью команды chmod. Только root, владелец файла или пользователь с привилегией sudo могут изменять права доступа к файлу или каталогу. Разрешения можно указывать с помощью символьного, числового или справочного режимов.

Таблица 1: Описание некоторых каталогов файловой системы GNU Linux

| Имя каталога | Описание каталога |
| --- | --- |
| / | Корневая директория, содержащая всю файловую |
| /bin | Основные системные утилиты, необходимые как в однопользовательском режиме, так и при обычной работе всем пользователям |
| /etc | Общесистемные конфигурационные файлы и файлы конфигурации установленных программ |
| /home | Содержит домашние директории пользователей, которые, в свою очередь, содержат персональные настройки и данные пользователя |
| /media | Точки монтирования для сменных носителей |
| /root | Домашняя директория пользователя root |
| /tmp | Временные файлы |
| /usr | Вторичная иерархия для данных пользователя |

Таблица 2: Описание некоторых используемых в работе команд

| Команда | Описание команды |
| --- | --- |
| useradd | Создание пользователя в Linux. Необходимо будет указать имя нового пользователя. |
| passwd | Создание и изменение пользовательских паролей. Необходимо будет указать имя пользователя, для которого нужно создать/изменить пароль. |
| pwd | Выводит полный путь от корневого каталога к текущему рабочему каталогу: в контексте которого (по умолчанию) будут исполняться выводимые команды. |
| whoami | Отображает имя вошедшего в систему пользователя. |
| id | Выводи UID (идентификатор пользователя), GID (идентификатор группы пользователя), groups (основные группы пользователя) |
| groups | Выводит список групп, в которых состоит текущий пользователь или пользователь с указанным именем. |
| cat | Вывод содержимого указанного файла. |
| ls | Выводит содержимое каталога. Опция -l выводит дополнительную информацию, -a отображает скрытые файлы, в названии которых в самом начале стоит символ ‘.’ |
| lsattr | Просмотр аттрибутов файлов/каталогов в файловой системе Linux. |
| mkdir | Создание каталога по указанному пути и с указанным именем внутри пути. |
| chmod | Изменение прав доступа к файлам и каталогам, используемых в Unix-подобных операционных системах. |
| echo | Вывод переданных аргументов, строки, текста. |
| chattr | Изменяет атрибуты файлов/каталогов в файловой системе Linux. |
| touch | Создает текстовый файл по указанному пути и с указанным именем внутри пути. |
| rm | Удаляет файл(ы) (каталог(и) при указании опции -r) по указанному(ым) пути(ям). |
| rename | Переименование файла/каталога. Формат rename [старое имя] [новое имя] [путь до файла]. |
| cd | Перемещение по файловой системе. |
| grep | Дает возможность вести поиск строкт. Также можно передать вывод любой команды в grep, что сильно упрощает работу во время поиска |

Более подробно об Unix см. в [1–6].

# 4 Выполнение лабораторной работы

## 4.1 Иполнение команд в консоли

Создаю нового пользователя под именем *guest* через команду useradd [**cmd:** *sudo useradd guest*] и создаю для него пароль с помощью команды passwd [**cmd:** *sudo passwd guest*]. После терминал попросит указать и подтвердить новый пароль (рис. 1).

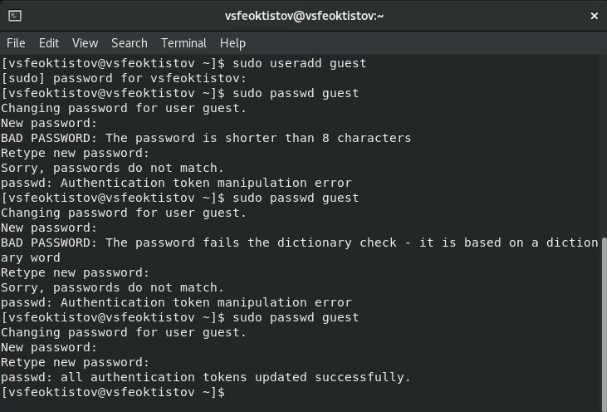


Рис. 1: Создание нового пользователя и пароля

Далее захожу в систему под только что созданным пользователем, вводя установленный ранее пароль. Сменить пользователя можно нажав на кнопку с иконкой замка в меню с выключением системы. В случае, если Вам предлагается ввести пароль для предыдущего пользователя, то нажмите на кнопку “Log in as another user” (рис. 2).

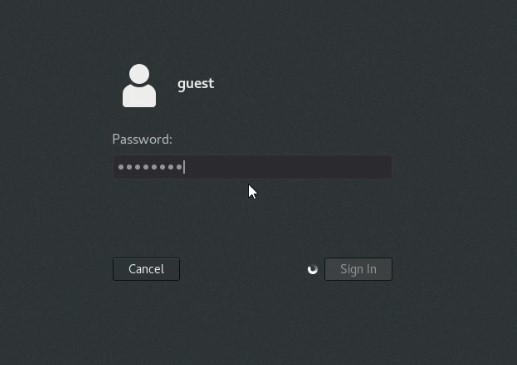


Рис. 2: Смена пользователя

После входа в систему под именем пользователя guest, я запустил терминал и выполнил команду *pwd*, тем самым получим путь до текущего каталога (домашняя директория пользователя *guest*). Далее можно уточнить имя пользователя, через которого я вошел в систему, для этого ввожу команду whoami. Очевидно, что выведится имя пользователя *guest*. С помощью команды *id* можно узнать UID пользователя (идентификатор пользователя = 1001), GID (индентификатор группы пользователя = 1001), а также к какой группе пользователей он принадлежит (на данный момент только к группе пользователей *guest*). Информацию о принадлежности текущего пользователя к группам пользователей можно также получить через команду *groups* (рис. 3).

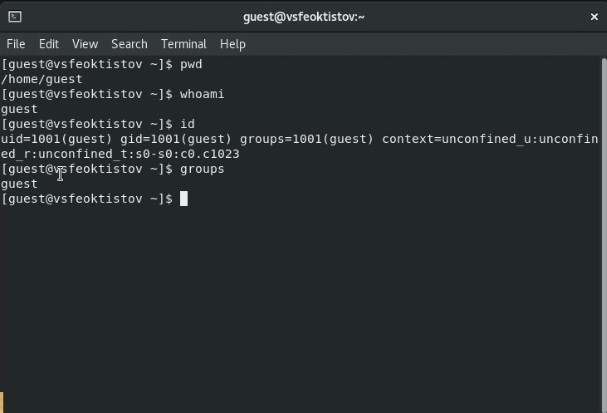


Рис. 3: Инфомация о текущем пользователе

Схожую информацию можно найти в содержании файла /etc/passwd (рис. 4).

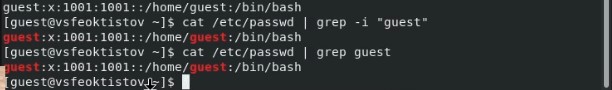


Рис. 4: Инфомация о всех пользователях в файле /etc/passwd

Далее я определил содержимое каталога /home с помощью команды *ls* [**cmd:** *ls -l /home*]. Получил информацию о двух каталогах: *vsfeoktistov* и *guest* - , которые находятся в указанной директории. Также через команду lsattr посмотрел расширенные атрибуты каталогов в директории /home [**cmd:** *lsattr /home*]. По выводу команды можно определить, что расширенные атрибуты можно увидеть только у файлов, владельцем которых является текущий пользователь (рис. 5).

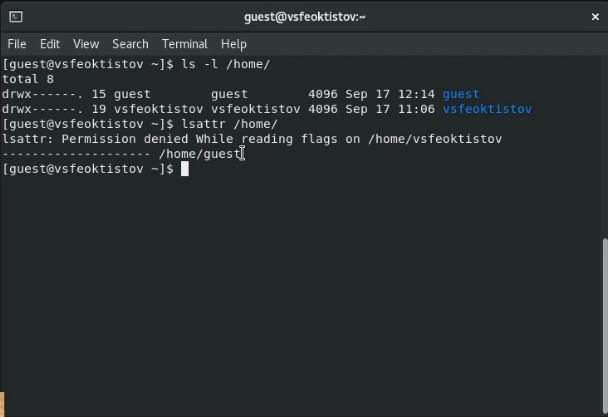


Рис. 5: Права и расшренные атрибуты каталогов в директории /home

После я создал каталог dir1 в домашней директории [**cmd:** *mkdir dir1*] и посмотрел чем он отличается по правам и расшренным атрибутам от других файлов в домашней директории [**cmds:** *ls -l* и *lsattr*]. Как видно, каталог dir1 имеет чуть больше прав, чем другие каталоги: членны группы имеют право редактирования/изменения (вторая тройка символов прав). В плане расширенных атрибутов каталог dir1 ни чем не отличается от других: не имеет никаких расширенных атрибутов (рис. 6).

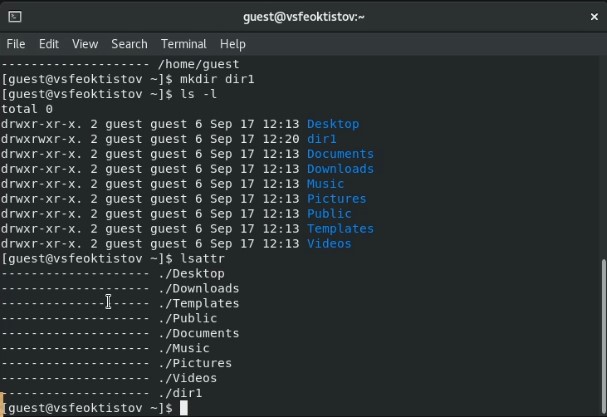


Рис. 6: Права и расшренные атрибуты нового каталога ~/dir1

Далее я снял все атрибуты прав с директории dir1 [**cmd:** *chmod 000 dir1*] и проверил изменения, к которым эта команда привела: посмотрел какие права доступа теперь имеет этот каталог [**cmd:** *ls -l*], попробовал создать и внести данные в файл внутри этого каталога (файл не создался, поскольку все изменения в каталоге запрещены) [**cmd:** *echo “test” > /home/guest/dir1/file1*], попробовал просмотреть содержимое каталога (просмотр не удался, поскольку у каталога забрал права на чтение, т.е. просмотр) [**cmd:** ls -l */home/guest/dir1*]. Проверить факт того, что файл file1 не было создан можно только после переназначения прав для каталога dir1 [**cmd:** *chmod 700 dir1*], либо командой [**cmd:** *chmod 400 dir1*] (дает права только на просмотр содержимого каталога) (рис. 7).

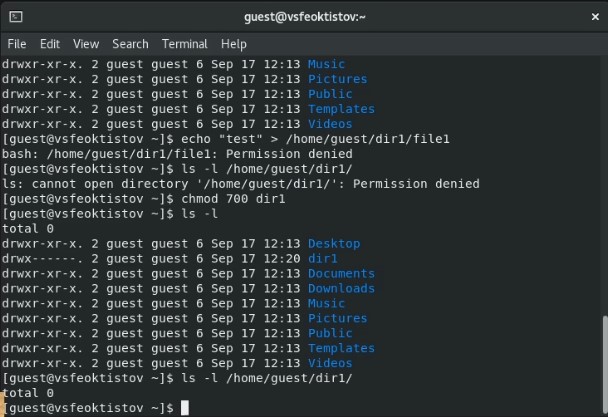


Рис. 7: Изменение прав для каталога dir1

## 4.2 Создание и использование скрипта

Далее я изучил какие действия можно будет совершать над файлами/каталогами при различных комбинациях атрибутов прав доступа. Для этого можно последовательно выполнить ряд команд: *touch* - попытка создать файл, *rm* - попытка удопить файл, *echo “” > /path* - попытка записать данные в файл, *cat* - попытка прочитать информацию из файла, *cd* - попытка перейти в директорию, *ls* - попытка просмотреть содержимое директории, *rename* - попытка переименовать файл, *chattr* - попытка изменить расширенные атрибуты файла. Но поскольку всего таких комбинаций атрибутов 8*8=64, то учитывая то, что нужно еще заполнить 8 колонок, то понадобится исполнить не менее 8*8\*8=512 команд, что достаточно много. Поэтому я написал bash скрипт, который упрощает проверку (рис. 8).

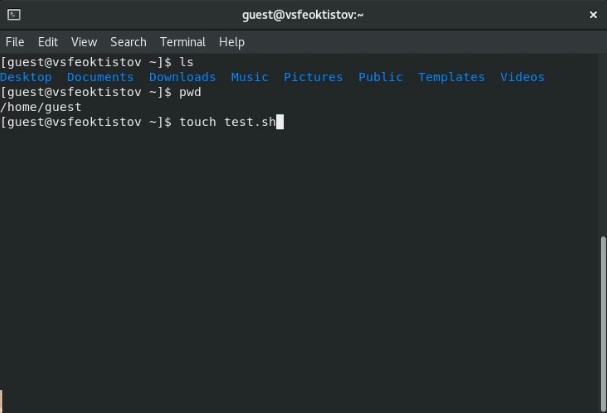


Рис. 8: Создание bash-скрипта для автоматизации проверки

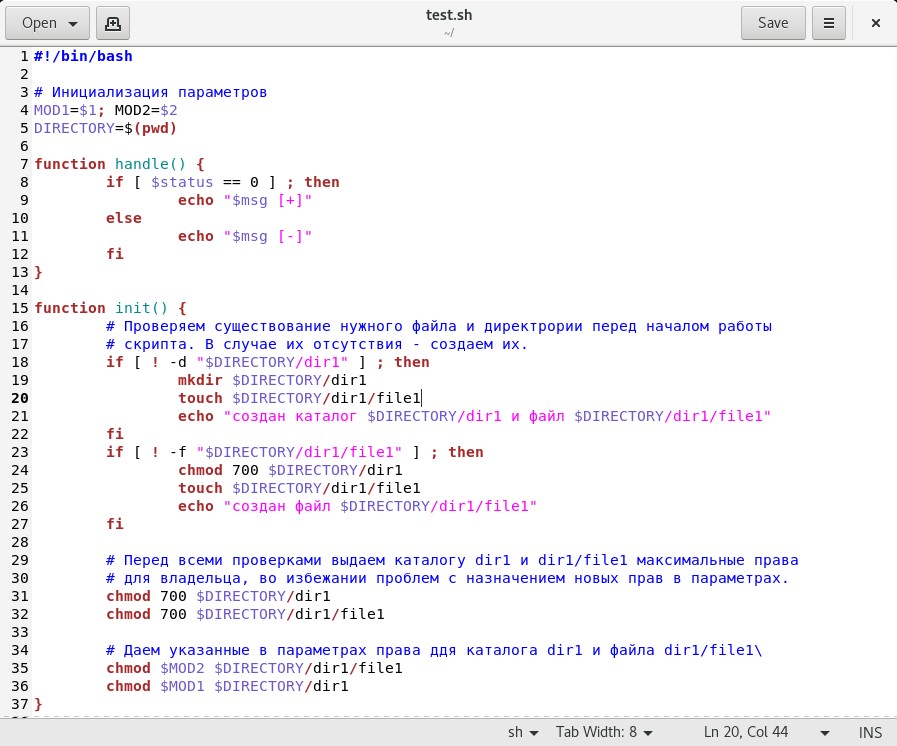


Рис. 9: Создание bash-скрипта для автоматизации проверки

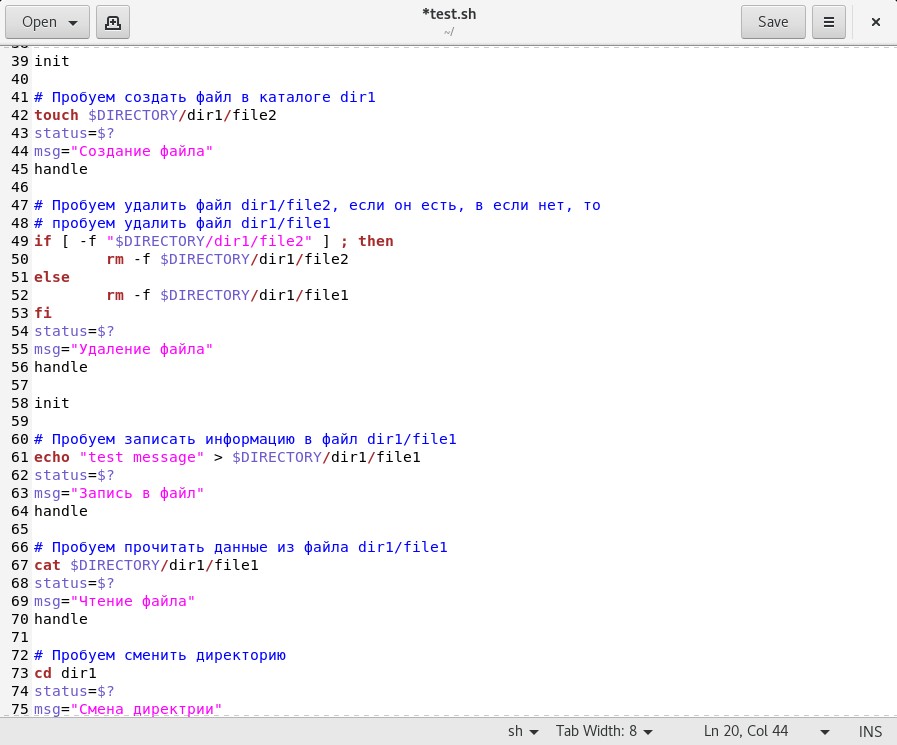


Рис. 10: Создание bash-скрипта для автоматизации проверки

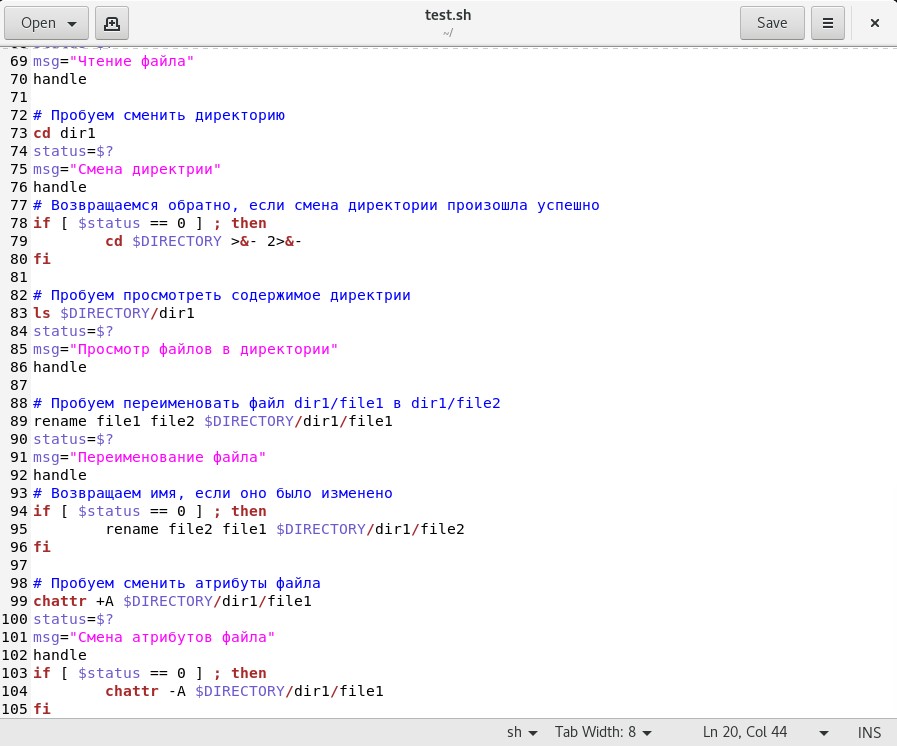


Рис. 11: Создание bash-скрипта для автоматизации проверки

Запустить этот скрипт можно с помощью команды [**cmd:** *sh test.sh 000 000*]. Таким образом, он снимет все права для файла file1 и каталога dir1 и покажет какие действия можно будет над ними выполнить (рис. 12).

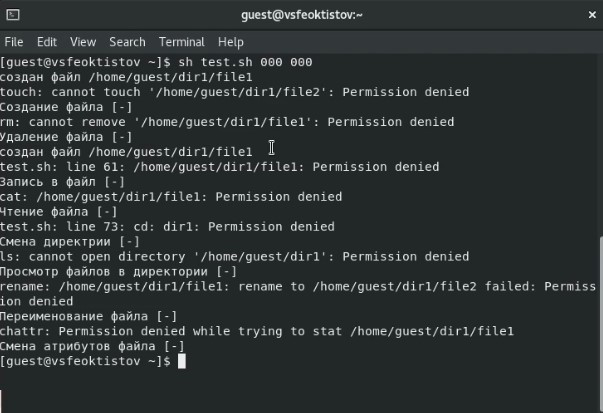


Рис. 12: Запуск bash-скрипта

## 4.3 Таблицы прав и разрешенных действий

Таблица 3: Установленные права и разрешенные действия

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

Таблица 4: Минимальные права для совершения операций

| 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 Выводы

В процессе выполнения лабораторной работы я приобрел практические навыки работы в консоли с правами и атрибутами файлов и каталогов, закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux, проверил необходимый наборов прав для выполнения различных действий над файлами и каталогами, получил навыки чтения выделенных прав через консоль.

# Список литературы

1. GNU Bash Manual [Электронный ресурс]. Free Software Foundation, 2016. URL: <https://www.gnu.org/software/bash/manual/>.

2. Newham C. [Learning the bash Shell: Unix Shell Programming](http://www.amazon.com/Learning-bash-Shell-Programming-Nutshell/dp/0596009658). O’Reilly Media, 2005. 354 с.

3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.

4. Robbins A. [Bash Pocket Reference](https://www.ncbi.nlm.nih.gov/pubmed/25246403). O’Reilly Media, 2016. 156 с.

5. Таненбаум Э. Архитектура компьютера. 6-е изд. СПб.: Питер, 2013. 874 с.

6. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.