МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
“БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ”
КАФЕДРА ИИТ

ОТЧЁТ

по лабораторной работе №2

«Ссылки. Права доступа»

Выполнил:

Студент 2 курса
группы ПО-9
Харитонович Захар Сергеевич
210672

Проверила:

Давидюк Ю. И.

Брест 2022

Цель работы: изучить понятия ссылок и прав доступа, получить практический навык создания ссылок, изменения прав доступа к файлам и каталогам.

Часть 1.

1. Изучить назначение и ключи команды ln.

- создать жесткую ссылку на файл.

```
$ ln file file-link
```

Просмотреть содержимое файла, используя ссылку.

```
$ cat file-link
Test file for lab2.
```

Удалить файл.

```
$ rm file
```

Просмотреть содержимое файла.

```
$ cat file-link
Test file for lab2.
```

Объяснить результат;

Жесткая ссылка создаёт связь между именем файла и inod. После удаления исходного файла остаётся файл-ссылка, который имеет тот же inod и, по сути, ссылается на ту же ячейку памяти.

- создать жесткую ссылку на каталог.

```
$ ln cat link-cat
ln: cat: не допускается создавать жёсткие ссылки на каталоги
```

Объяснить результат;

ОС Linux не позволяет создавать жёсткие ссылки на каталоги во избежание конфликтов.

2. Выполнить все задания пункта 1, создавая не жесткие, а символьные ссылки.

- создать символьную ссылку на файл.

```
$ ln --symbolic file file-symbolic-link
```

Просмотреть содержимое файла, используя ссылку.

```
$ cat file-symbolic-link
Test file for lab2.
```

Удалить файл.

```
$ rm file
```

Просмотреть содержимое файла.

```
$ cat file-symbolic-link
cat: file-symbolic-link: Нет такого файла или каталога
```

Объяснить результат;

Символьная ссылка в себе хранит путь к исходному файлу, поэтому при его удалении ссылка не может обратиться к несуществующему файлу.

- создать символьную ссылку на каталог.

```
$ ln --symbolic cat cat-symbolic-link
```

Объяснить результат;

ОС Linux позволяет создавать символьные ссылки на каталоги. Символьные ссылки, в отличие от жёстких, хранят только путь к исходному каталогу.

3. Создать жесткую и символьную ссылки на файл.

$ ln text text-link

$ ln --symbolic text text-symbolic-link

С помощью команды ls просмотреть inod файла и ссылок.

$ ls -l

итого 8

-rw-rw-r-- 2 kraken kraken 11 кас 1 17:12 text

-rw-rw-r-- 2 kraken kraken 11 кас 1 17:12 text-link

lrwxrwxrwx 1 kraken kraken 4 кас 1 17:13 text-symbolic-link -> text

Объяснить результат.
Исходный файл и его жёсткая ссылка имеют одинаковый inod (11), так как в этом и состоит суть жёсткой ссылки. Символьная ссылка имеет отличный inod (4).

Часть 2.
1. Изучите при помощи man опцию -l команды ls.

```
-l     use a long listing format
```

Просмотрите права каталогов /etc, /bin и домашнего каталога.

```
$ ls -l /
lrwxrwxrwx   1 root root          7 кра 30 19:11 bin -> usr/bin
drwxr-xr-x 139 root root      12288 вер 10 14:13 etc
$ ls -l /home/
drwxr-xr-x 34 kraken kraken 4096 вер 10 14:23 kraken
```

Просмотрите права файлов, содержащиеся в этих каталогов. Выявите тенденции (файлов с какими правами в каких каталогах больше).
В /bin rwxr-xr-x root root
В /etc rwxr-xr-x root root и rw-r--r-- root root
В домашнем каталоге rwxr-xr-x kraken kraken и rwxrwxr-x kraken kraken

В системных каталогах доступ к записи имеет только пользователь root, остальные пользователи, в том числе и пользователи группы root, имеют право только на чтение и исполнение (исполнение – не всегда).
В домашнем каталоге текущий пользователь kraken имеет полный набор прав доступа, пользователи группы зачастую так же имеют все права, остальные пользователи имеют право только на чтение и исполнение.

2. Изучите материал, посвящённый пользователям и группам пользователей. Изучите руководство по командам chown и chgrp.
Выясните, кто является владельцем и к какой группе владельцов принадлежат файлы вашего домашнего каталога, каталогов /etc, /root, /bin и /dev.
В домашнем каталоге владелец kraken группа kraken
В /etc владелец root группа root
В /root владелец root группа root
В /bin владелец root группа root
В /dev владелец root, группы root, i2c, tty, disk, dialout, video.

3. Определите атрибуты файлов /etc/shadow и /etc/passwd попробуйте вывести на экран содержимое этих файлов.

```
$ ls -l /etc
-rw-r-----  1 root shadow   1484 жні 16 10:06 shadow
-rw-r--r--  1 root root     2858 жні 16 10:06 passwd

$ cat /etc/shadow
cat: /etc/shadow: Отказано в доступе

$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

и т. д.

Объясните результат.
Текущий пользователь kraken принадлежит к группе kraken и не входит в группу shadow. Т. к. установлены права доступа rw-r----- для shadow, то мой пользователь (---) не имеет права на чтение файла.
В случае с passwd права доступа – rw-r--r--, значит мой пользователь (r--) как "прочий" имеет право на чтение файла.

4. Изучите команду chmod. Создайте в домашнем каталоге любые четыре файла, установите при помощи восмеричных масок на каждый из них в отдельности следующие права:
- для себя все права, для группы и остальных - никаких;
```
$ chmod 700 file1
```
- для себя чтение и запись, для группы чтение, для остальных - все;
```
$ chmod 647 file2
```
- для себя исполнение и запись, для группы никаких, для остальных чтение;
```
$ chmod 304 file3
```
- для себя запись, для группы все, для остальных - только запись.
```
$ chmod 272 file4
```
5. Выполните задание предыдущего пункта, используя в команде chmod только символы прав доступа.
- для себя все права, для группы и остальных - никаких;
```
$ chmod u+r+w+x,go-r-w-x file1
```
- для себя чтение и запись, для группы чтение, для остальных - все;
```
$ chmod u+r+w-x,g+r-w-x,o+r+w+x file2
```
- для себя исполнение и запись, для группы никаких, для остальных чтение;
```
$ chmod u-r+w+x,g-r-w-x,o+r-w-x file3
```
- для себя запись, для группы все, для остальных - только запись.
```
$ chmod u-r+w-x,g+r+w+x,o-r+w-x file4
```

6. Переведите номер своей зачетной книжки в восьмеричную систему счисления, разбейте полученное значение на группы по 2-3 цифры и создайте файлы с правами доступа, выраженными полученными масками.
210672_{10} -> 633360_8
```
$ chmod 633 file1
$ chmod 360 file2
```
Сопоставьте данные маски с символами прав доступа и объясните, какие операции с данными файлами доступны каким субъектам системы.
`-rw--wx-wx 1 kraken kraken 2 кас  1 17:57 file1` чтение и запись - пользователю, чтение и исполнение - группе и остальным.
`--wxrw---- 1 kraken kraken 2 кас  1 17:57 file2` чтение и исполнение - пользователю, чтение и запись - группе, ничего - остальным

7. В домашнем каталоге создайте файл и установите на него права так, чтобы его можно было только редактировать.
```
$ >file
$ chmod 222 file
```

8. Скопируйте в свой домашний каталог файл ls из каталога /bin. Запретите выполнение этого файла и попробуйте выполнить именно его, а не исходный(!).
```
$ cp /bin/ls ~
$ chmod a-x ls
$ ./ls
bash: ./ls: Отказано в доступе
```
Объясните результат.

Нельзя выполнить файл, не имея права на его выполнение.
9. Изучите на что влияют права доступа в случае каталогов. Попробуйте зайти в каталог /root, объясните результат и причину.
$ cd /root/
bash: cd: /root/: Отказано в доступе

drwx------ 10 root root   4096 вер 16 17:07 root
Право на чтение, запись и исполнение каталога root имеет только пользователь root, остальные же, в том числе и текущий пользователь, не имеет никаких прав.

Вывод: были изучены принципы работы с жёсткими и символьными ссылками, освоены и закреплены навыки определения и изменения прав доступа к файлам и каталогам.