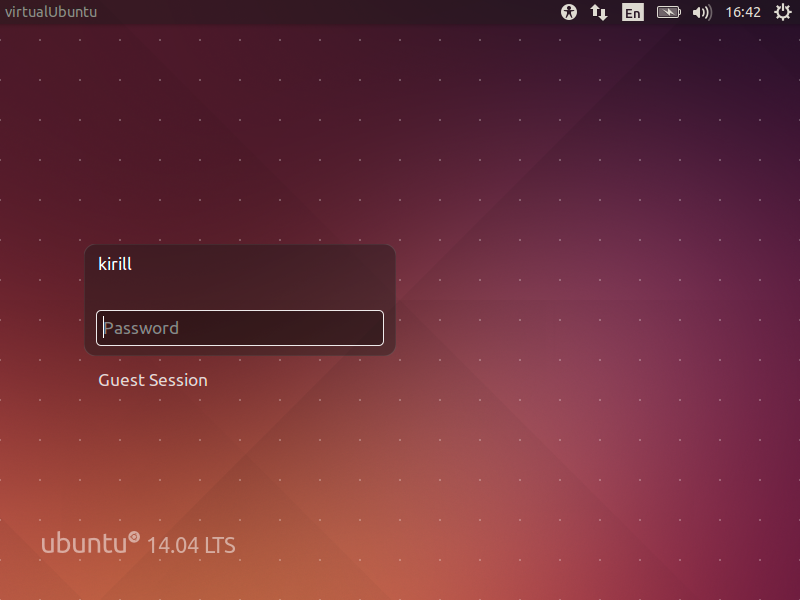
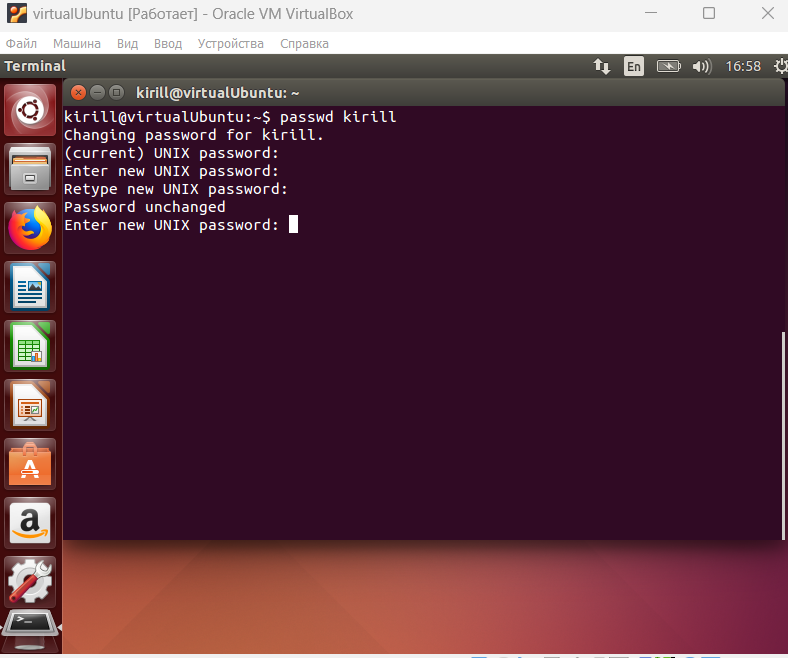
Лабораторная работа №6

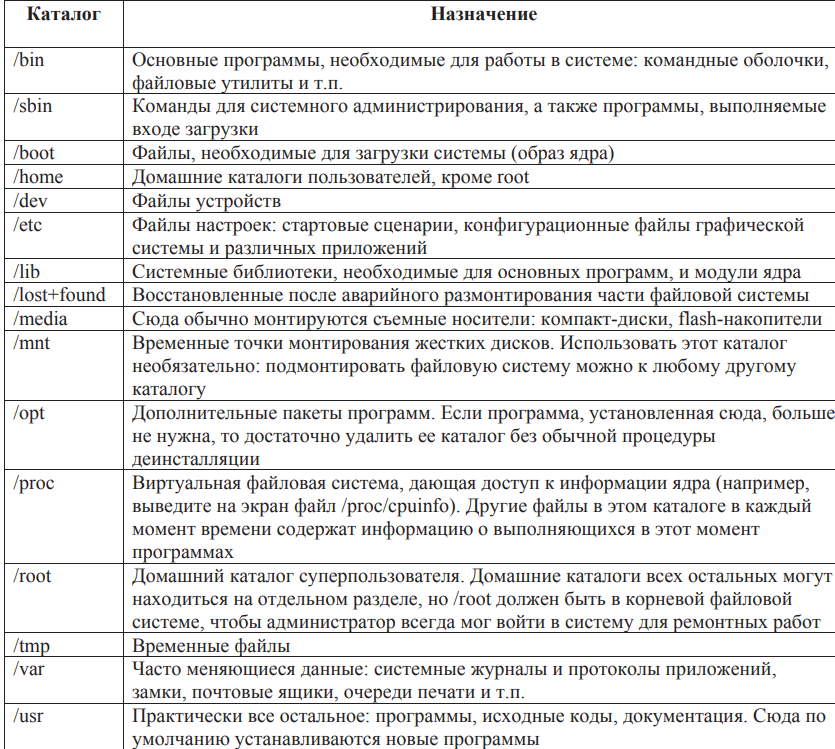
1. Зайдем под пользователем root с помощью графической оболочки



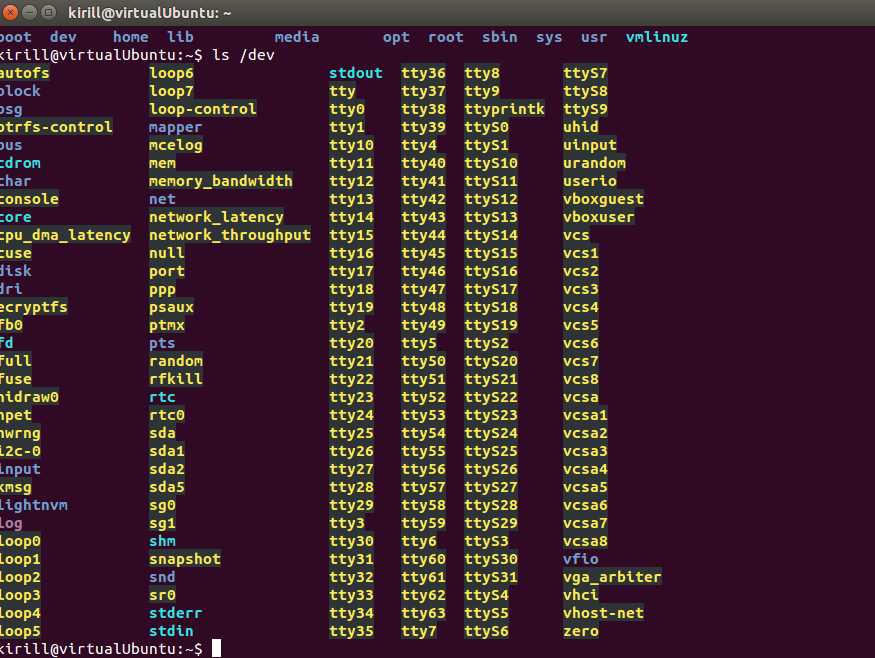
Далее, сменим пароль



1. Системные каталоги unix



3.Просмотрим содержимое каталога файла физических устройств.



Где /dev/console Системная консоль, т. е. монитор и клавиатура, физически подключенные к компьютеру

Жесткие диски с SCSI-интерфейсом /dev/fd Файлы дисководов для гибких дисков. Первому дисководу соответствует /dev/fd0, второму /dev/fd1

**/dev/tty обозначает терминал, к которому подключен процесс.**

/dev/null представляет собой что-то типа «мусорной корзины». Часто некоторые программы выводят множество ненужной информации. Shell-скрипты обычно используют /dev/null для того, чтобы пользователь не видел ненужных ему сообщений от вызываемых утилит.

/dev/zero близок к /dev/null. Как и /dev/null, устройство может быть использовано для блокирования вывода ненужной информации, но чтение /dev/zero возвращает \0 символы (чтение /dev/null возвращает символы end-of-file — конец файла). Поэтому /dev/zero обычно используется для создания пустых файлов.

/dev/full служит для имитации «полного» устройства. Запись в /dev/full сопровождается ошибкой. «Полное» устройство полезно для того, чтобы посмотреть, как тестируемое приложение будет себя вести при попытки доступа к заполненному устройству (т.е. например, к жесткому диску, на котором не осталось места).

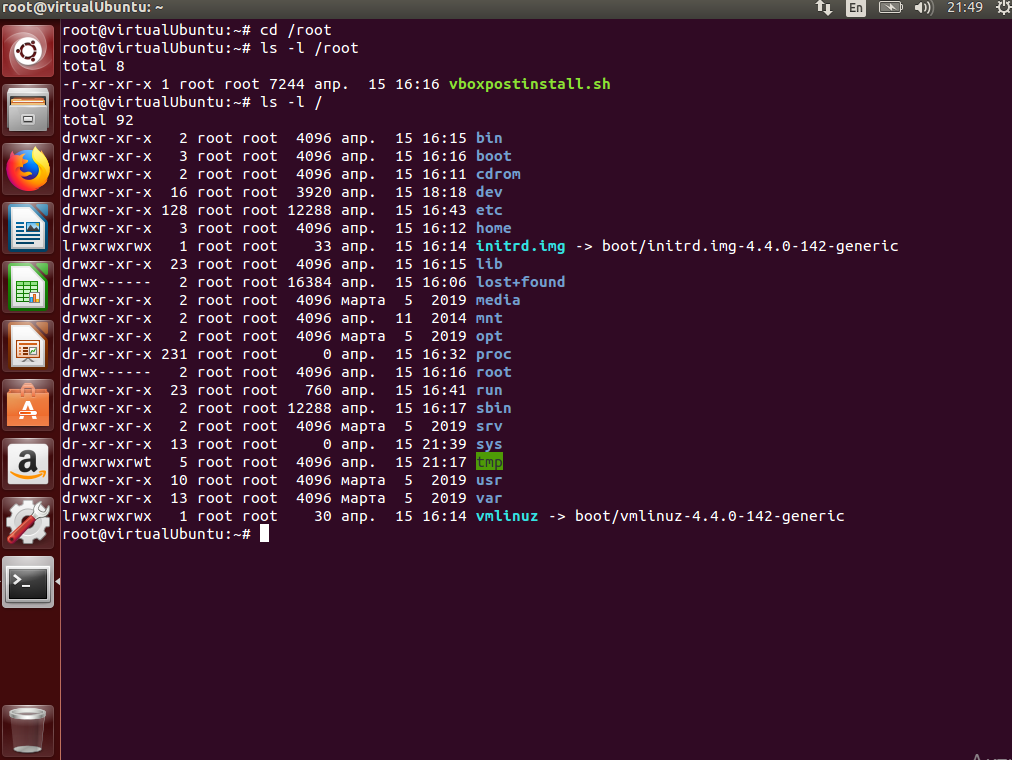
Например, каталог/dev/pts/0 существует в памяти. Содержимое каталога представляет собой псевдотерминалы, которые позволяют приложениям получать входные данные и отображать выходные данные:

В большинстве unices /dev/log это [сокет](http://en.wikipedia.org/wiki/Unix_domain_socket), который программы используют для отправки сообщений журнала

/dev/stdin обозначает стандартный ввод текущего процесса;

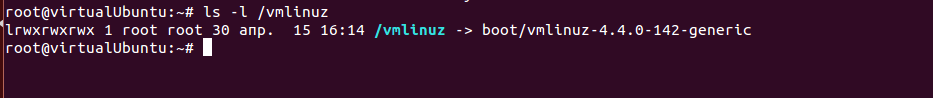
4.

Перейдем в директории пользователя root и посмотрим содержимое каталога



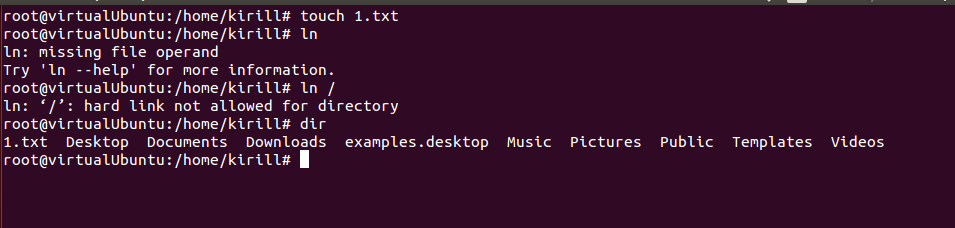
Файл vmlinuz из директории /boot является сжатым исполняемым файлом ядра ОС

Узнаем его права доступа

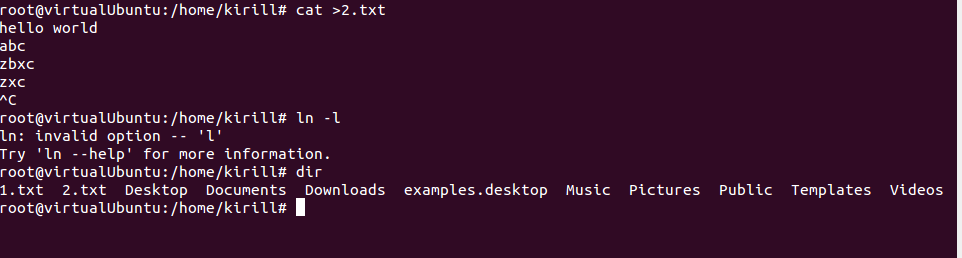


L в начале обозначает символическую ссылку данного файла, далее идут три группы по три символа с правами доступа – для владельца файла, для группы пользователей и для остальных пользователей системы. r – читать файл, w – производить запись, x – запускать файл на выполнение. В этом файле правда доступа выданы всем.

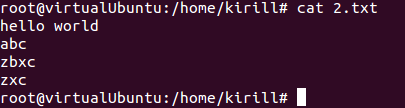
5. Создадим файл 1.txt в папке пользователя user с помощью touch – создает пустой файл



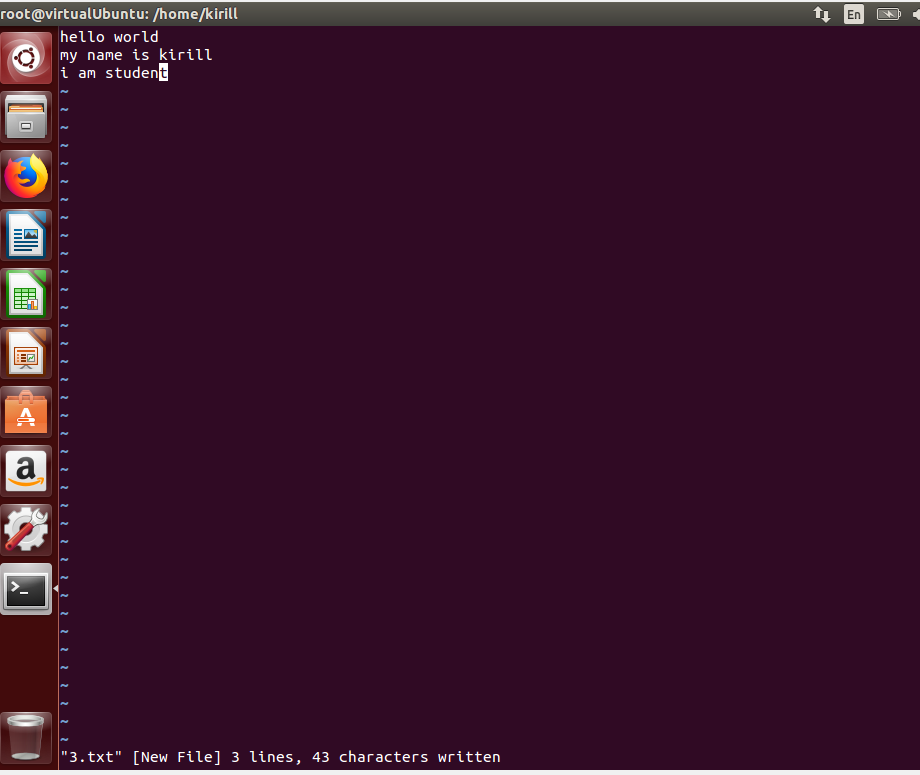
Создадим 2.txt с помощью cat и сразу запишем какие то данные

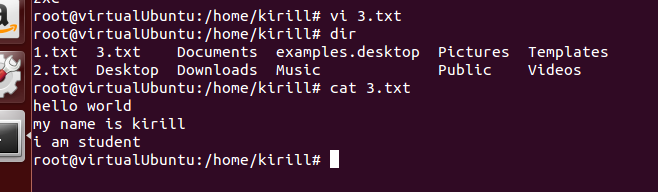


Содержимое

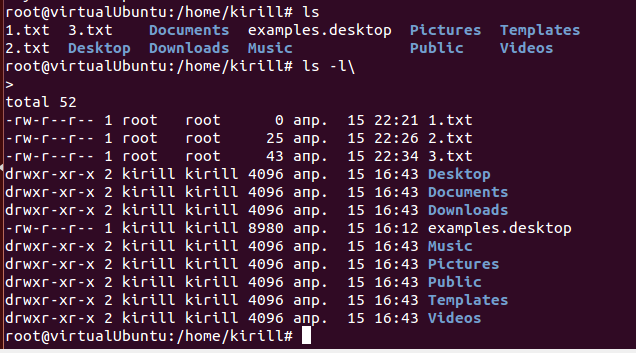


Создадим 3.txt с помощью vi редактора



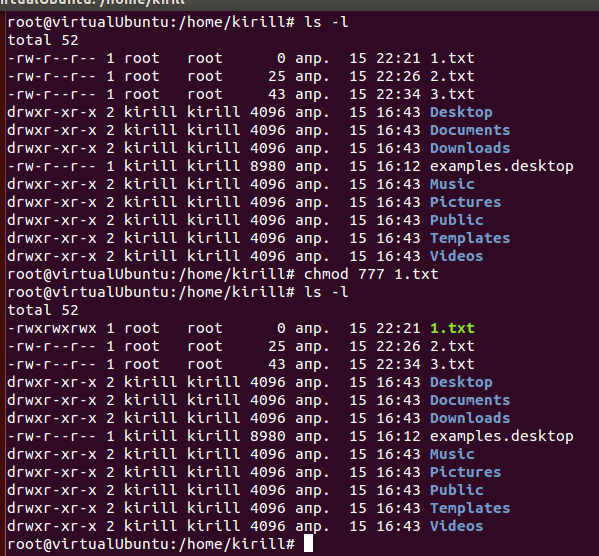


Проверим права доступа к файлу



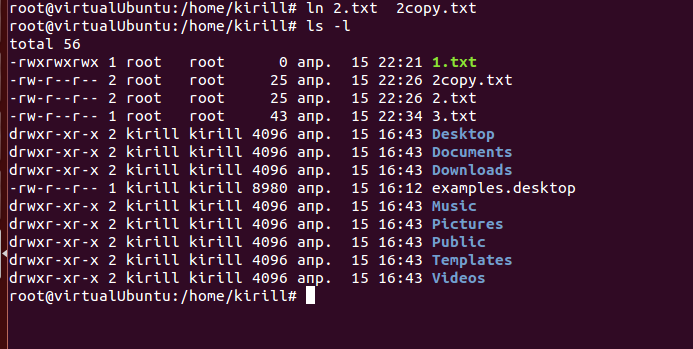
Три созданных файла может просматривать и записывать владелец – root, а все остальные – только читать.

6. Изменим права доступа к файлу 1.txt с помощью chmod , дадим права всем пользователям с помощью 777

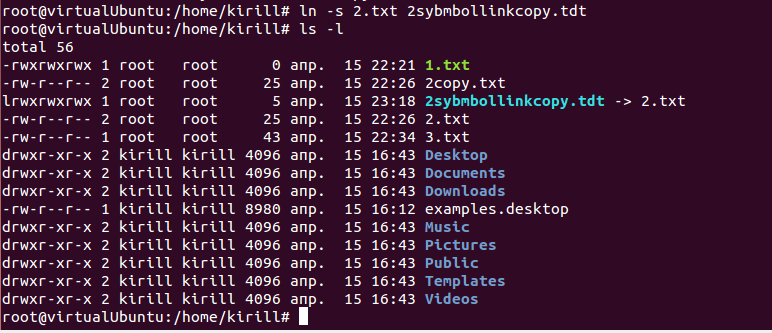


7. Создадим жесткую и символическую ссылки на файл 2.txt

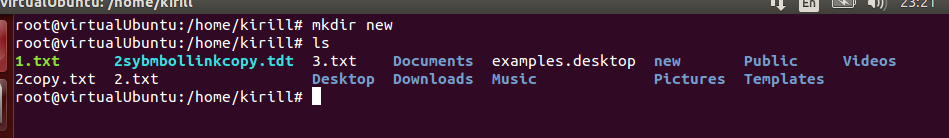
Жесткая ссылка



Символическая ссылка



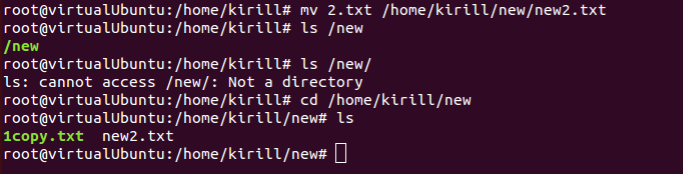
8. Создадим каталог new в каталоге пользователя



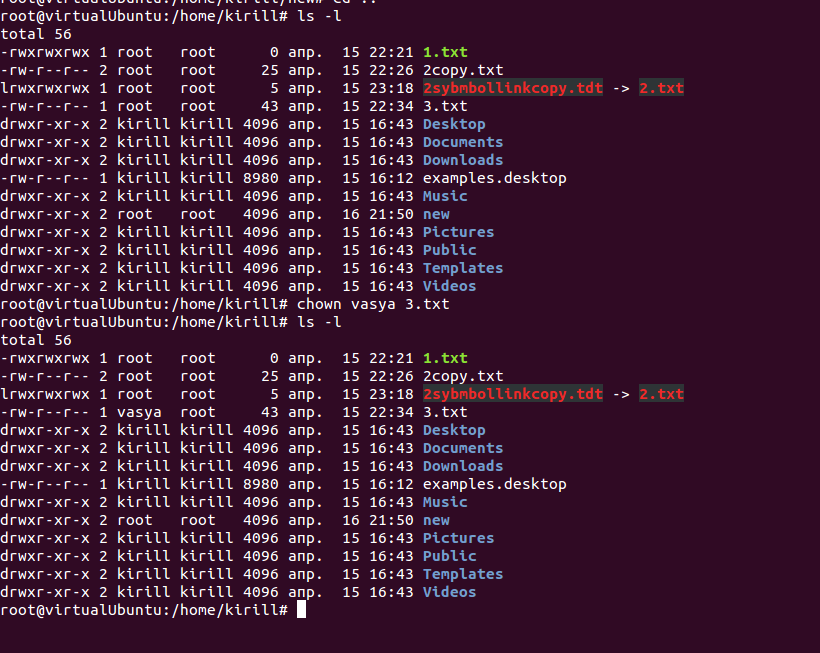
9. Скопируем 1.txt в каталог new



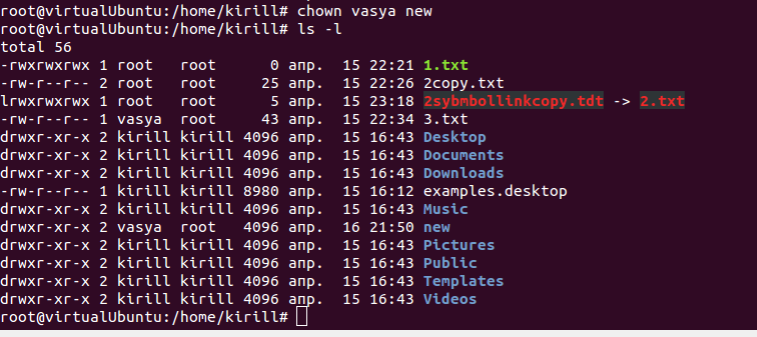
10. Переместим файл 2.txt в каталог new



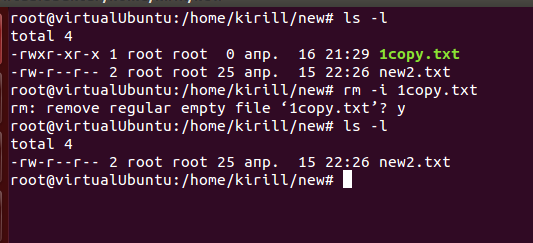
11. Сменим владельца файла 3.txt с root на vasya



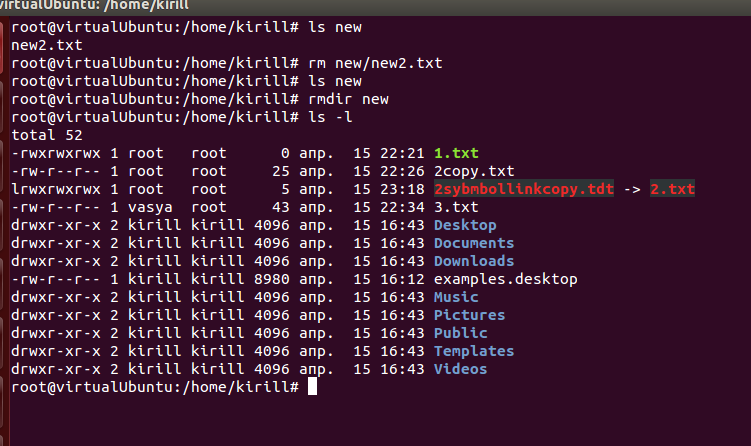
Теперь сменим владельца каталога new



12. Удалим копию 1.txt находящуюся в каталоге new



13. Далее удалим каталог new



14. найдем файл 1.txt с помощью find

