Федеральное агентство связи

Северо-Кавказский филиал ордена Трудового Красного Знамени

федерального государственного бюджетного образовательного учреждения

высшего образования

«Московский технический университет связи и информатики»

Кафедра «Информатики и вычислительной техники»

Отчет

по лабораторной работе №5

« Пользователи Ubuntu ОС UBUNTU (Linux)»

по дисциплине «Операционные системы»

выполнил студент группы ДП-31

Гаврилов Владислав Вадимович

Ростов-на-Дону

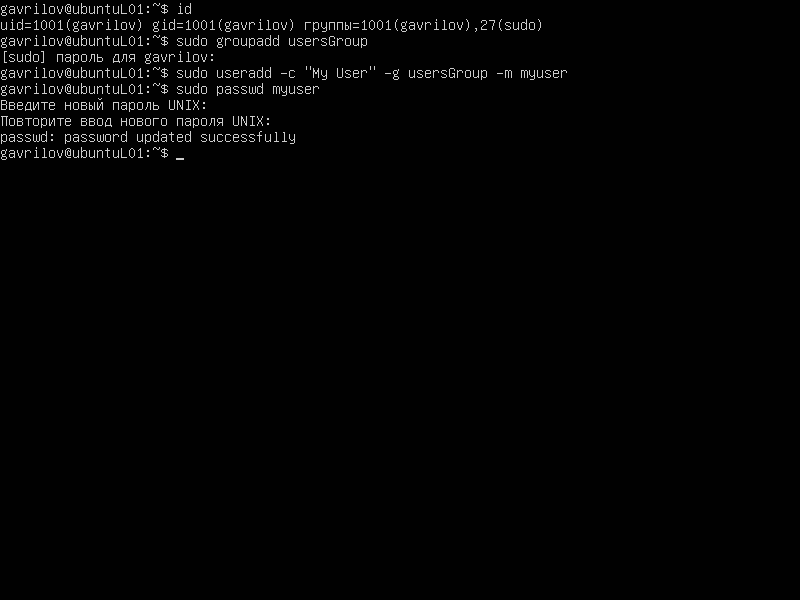
2019

**Цель работы:**

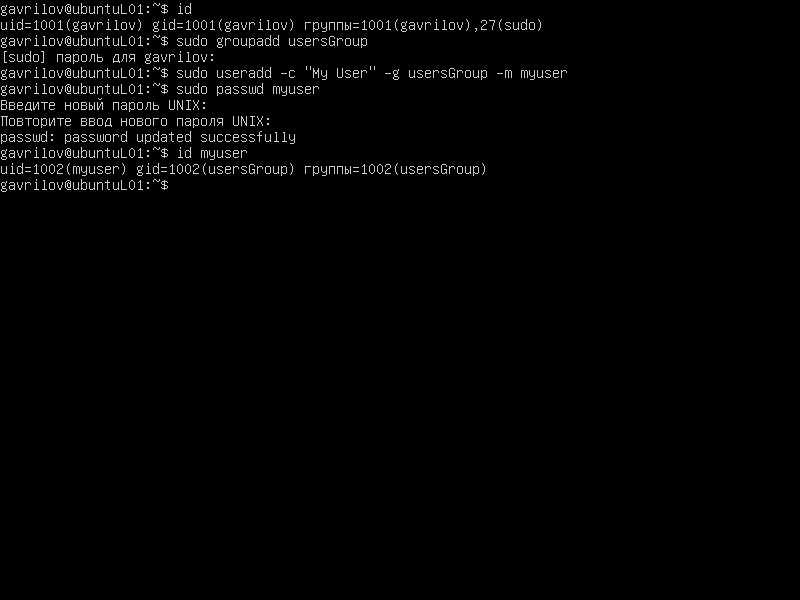
Изучить возможности Linux при работе с пользователями и управлении правами доступа, а также при работе с пакетами, установить и обновить программное обеспечение.

Узнал свой UID и GID, т.е. уникальный номер пользователя и номер группы введя команду id:

Создал группу пользователей с именем usersGroup, далее создал пользователя myuser в группе usersGroup, имеющего основную группу usersGroup:

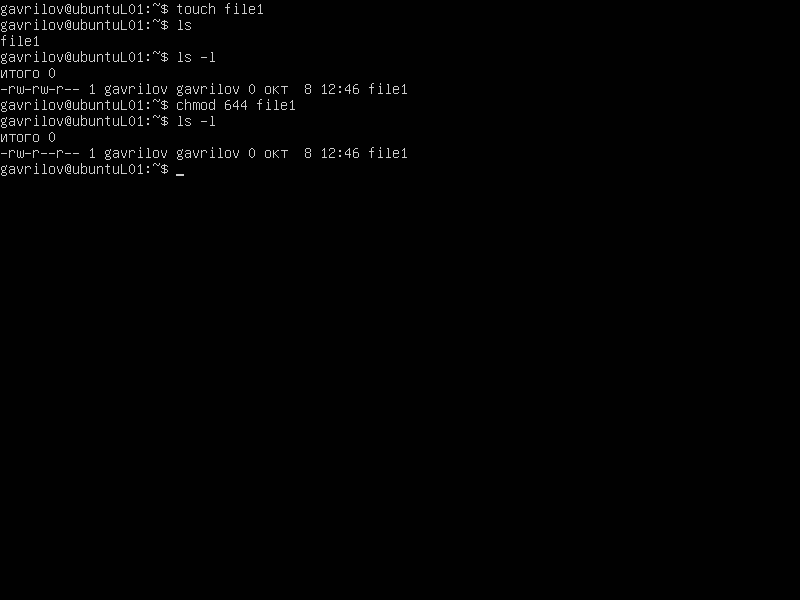


Вывел на экран UID и GID пользователя myUser:

UID = 1002

GID = 1002

Создал текстовый файл file1 и с помощью команды chmod 644 ограничил доступ на запись для :



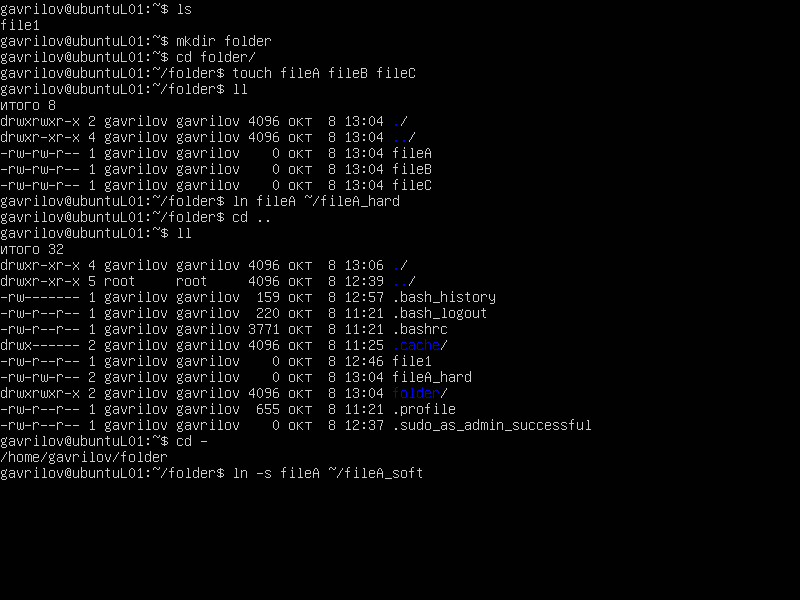
Зашел под пользователем myuser, попытался прочитать созданный файл:



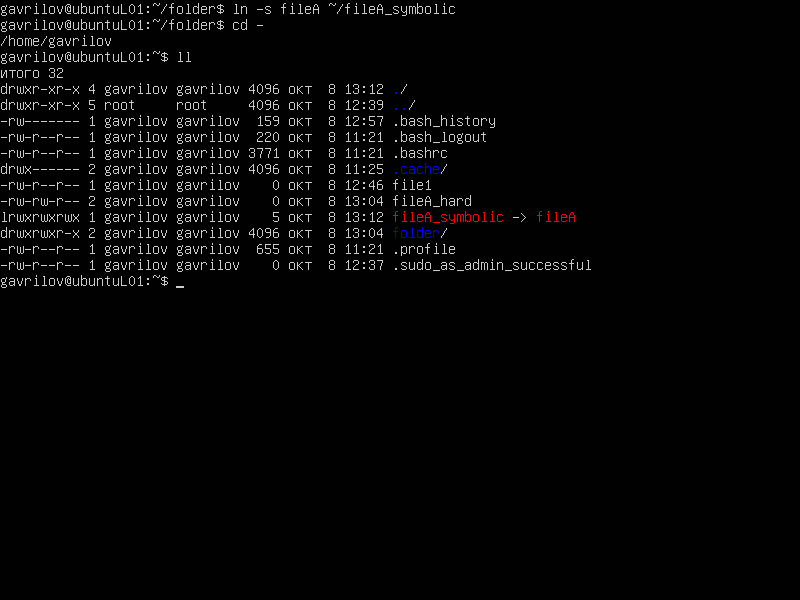
Получил предупреждение «No write permission»:



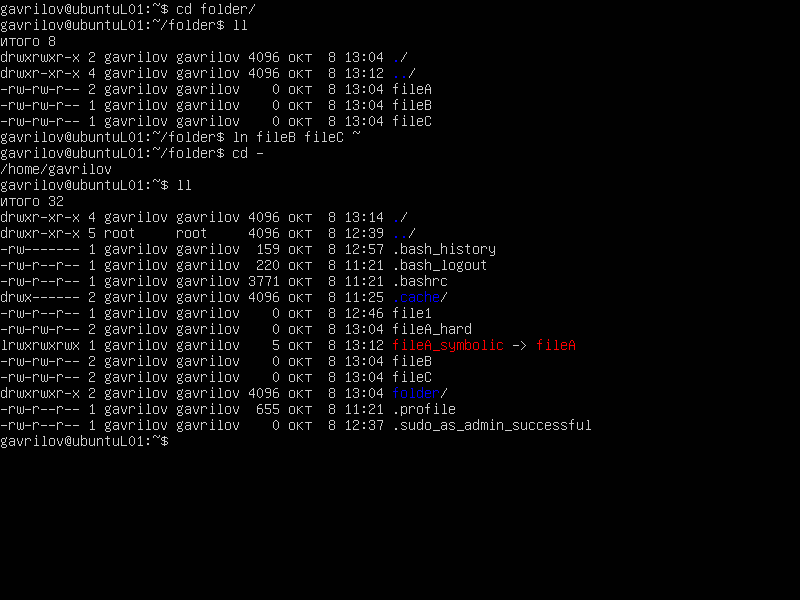
Создал директорию folder; в ней создал три файла — fileA, fileB, fileC; в домашней директории создал жесткую ссылку на fileA с названием fileA\_hard:



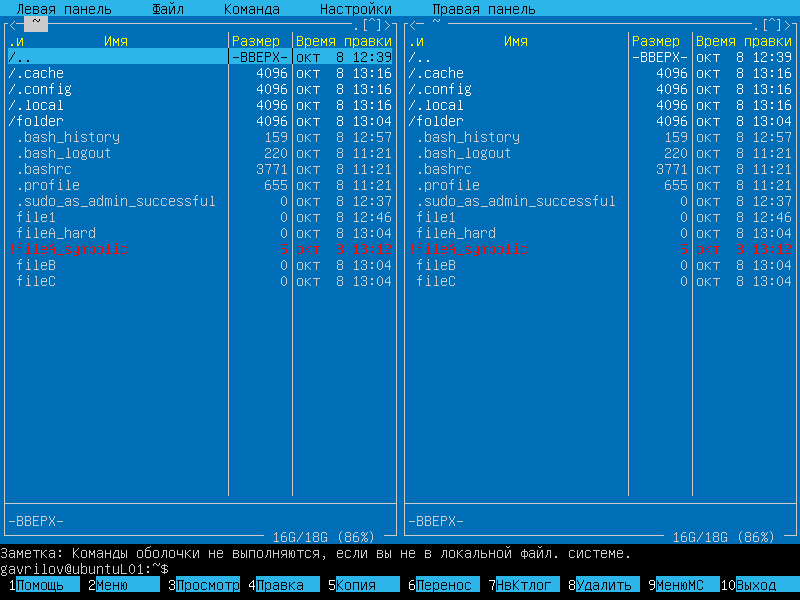
Затем создал символическую ссылку на fileA с именем fileA\_symbolic:



Создал несколько жестких ссылок на файлы из folder:



Файловый менеджер Midnight Commander работает:



**Контрольные вопросы:**

***Расскажите про идентификационные номера пользователей и групп в Linux.***

Каждому пользователю назначается идентификационный номер User ID. Сокращенно номер обозначается как UID, является уникальным идентификатором пользователя. Операционная система отслеживает пользователя именно по UID. Также, каждому пользователю назначается пароль для входа в систему.

Каждой группе назначается идентификационный номер Group ID, сокращенно GID, который является уникальным идентификатором группы. Принадлежность пользователя к группе устанавливается администратором.

***Расскажите о файлах Linux, содержащих информацию о пользователях и группах системы.***

Основные файлы, содержащие информацию о пользователях и группах, - это четыре файла в каталоге /etc.

1. /etc/passwd - файл паролей, содержащий основную информацию о пользователях;
2. /etc/shadow - файл теневых шифрованных паролей, содержащий зашифрованные пароли;
3. /etc/group - файл групп, содержащий основную информацию о группах и принадлежащих этим группам пользователях;
4. /etc/gshadow - файл теневых групп, содержащий шифрованные пароли групп.

***Как система Linux хранит пароли пользователей и групп?***

Пароль пользователя хранится в зашифрованном виде (encrypted).

Passwd – это текстовый файл, содержащий список учетных записей пользователей системы.

***Как организуется разграничение доступа к файлам в Linux?***

Операционная система Linux - это многопользовательская система, которая дает огромные возможности манипулирования доступом к данным для каждого пользователя отдельно. Это позволяет гибко регулировать отношения между пользователями, объединяя их в группы, что позволит защитить данные одного пользователя от нежелательного вмешательства других.

***Как изменить права доступа к файлу? Как сделать это с помощью битовой строки?***

Права пользователя могут быть изменены только владельцем файла или пользователем с правами администратора системы. Для изменения прав используется команда:

chmod[u|g|o|a] [+|-|=] [r|w|x] name1 [name2 ...]

В качестве аргументов команда принимает указание классов доступа («u» - владелец-пользователь, «g» - владелец-группа, «o» - остальные пользователи, «a» - все вышеперечисленные группы вместе), права доступа («r» - чтение, «w» - запись, «x» - выполнение) и операцию, которую необходимо произвести («+» - добавить, «-» -убрать, «=» - присвоить).

***Расскажите о Т-бит, SUID и SGID.***

Помимо стандартных «rwx» значений существуют еще и буквы «s» и «t». В действительности, битовая маска прав доступа к файлам содержит 4 группы по 3 бита в каждой. Таким образом, команда chmod 755 это всего лишь краткая запись полной формы команды: chmod 0755.

T-бит обычно используется с каталогами. Обычно, когда t-бит для каталога не установлен, файл в данном каталоге может удалить любой пользователь, имеющий доступ на запись к данному файлу. Устанавливая t-бит на каталог мы меняем это правило таким образом, что удалить файл из каталога может только владелец этого каталога или файла.

Установить t-бит можно при помощи команд:

chmod a+tw имя\_файла

chmod 1777 имя\_файла

Атрибуты SUID и SGID позволяют изменить права пользователя при запуске на выполнения файла, имеющего эти атрибуты.

Запускаемая программа получает права доступа к системным ресурсам на основе прав доступа пользователя, запустившего программу. Установка же флагов SUID и SGID изменяет это правило таким образом, что назначает права доступа к системным ресурсам исходя из прав доступа владельца файла. Т.е. запущенный исполняемый файл, которым владеет суперпользователь, получает права доступа к системным ресурсам на уровне суперпользователя (фактически неограниченные). При этом установка SUID приведет к наследованию прав владельца-пользователя файла, а установка SGID -владельца-группы.

Пользоваться такими мощными атрибутами как SUID и SGID нужно с крайней осторожностью, особенно подвергать пристальному вниманию программы и скрипты, владельцем которых является root (суперпользователь), т.к. это потенциальная угроза безопасности системы.

***Расскажите про файловые системы Linux.***

В ОС Linux следует различать физическую файловую систему, которая отвечает за управление дисковым пространством и размещение файлов в физических адресах диска и логическую файловую систему, которая обеспечивает логическую структуру хранения файлов - пространство имен файлов. ОС Unix и Linux могут работать с различными физическими файловыми системами (Ext2, ext3, ufs), логическое же представление файловой системы в Unix/Linux структурировано. Все файлы в логической файловой системе располагаются в виде дерева, промежуточные вершины которого соответствуют каталогам, и листья - файлам и пустым каталогам. Реально на каждом логическом диске (разделе физического дискового пакета) располагается отдельная иерархия каталогов и файлов. Для получения общего дерева в динамике используется «монтирование» отдельных иерархий к фиксированной корневой файловой системе в качестве ветвей общего дерева. Самым верхом иерархии является корень, который имеет предопределенное имя «/» (слэш). Этот же символ используется как разделитель имен в пути. Далее в корне находятся папки с определенными для каждого дистрибутива именами (etc, home, bin, mnt, proc и т.д.).

Полное имя файла, например, /bin/sh означает, что в корневом каталоге должно содержаться имя каталога bin, а в каталоге bin должно содержаться имя файла sh. Коротким или относительным именем файла называется имя, задающее путь к файлу от текущего рабочего каталога. В каждом каталоге содержатся два специальных имени, имя «.» - ссылка на текущий каталог, и имя «...» - ссылка «родительский» каталог данного текущего каталога, т.е. каталог, непосредственно предшествующий данному в иерархии каталогов. Так, например, для структуры, показанной на рис. 5.7 доступ к файлу file2 из текущего каталога (laba) возможен по полному имени: /home/myvar/file2 или по относительному имени: .../.../.../myvar/file5.

***Какие типы файлов существуют в Linux?***

ОС LINUX поддерживают несколько типов файлов:

• Обычные файлы (или регулярные) - представляют собой последовательность байтов. Это текстовые, исполняемые файлы и т.д. Данный тип файла отображается командой ls -l в виде «-» (черточки).

• Каталоги - представляют собой особый вид файлов, которые хранятся во внешней памяти подобно обычным файлам, но их структура поддерживается самой файловой системой. Данный тип файла отображается командой ls -l в виде символа «d».

• Специальные файлы устройств, бывают блочные и символьные. Данный тип файла отображается командой ls -l в виде символа «b» или «с» соответственно. Специальные файлы не хранят данные. Они обеспечивают механизм отображения физических внешних устройств в имена файлов файловой системы. Каждому устройству, поддерживаемому системой, соответствует, по меньшей мере, один специальный файл. При выполнении чтения или записи по отношению к специальному файлу, производится прямой вызов соответствующего драйвера устройства. При этом имена специальных файлов можно использовать практически всюду, где можно использовать имена обычных файлов.

• Ссылка (link). Данный тип файла отображается командой ls -l в виде символа «l». Файловая система UNIX/LINUX обеспечивает возможность связывания одного и того же файла с разными именами.

• Именованный программный канал (pipe) - одно из средств межпроцессных взаимодействий (IPC) в ОС UNIX/LINUX. Данный тип файла отображается командой ls -l в виде символа «p». Именованному программному каналу обязательно соответствует элемент некоторого каталога.

• Сокет (socket)- предоставляют весьма мощный и гибкий IPC. Данный тип файла отображается командой ls -l в виде символа «s». Они могут использоваться для организации взаимодействия программ на одном компьютере, по локальной сети или через Internet, что позволяет создавать распределённые приложения различной сложности. Кроме того, с их помощью можно организовать взаимодействие с программами, работающими под управлением других операционных систем.

***Расскажите о мягких и жестких ссылках.***

Существуют жесткие и мягкие ссылки.

Жесткая ссылка является просто еще одним именем для исходного файла и не является типом файла. Она прописывается в индексном дескрипторе исходного файла (в структуре, хранящей метаданные файла). После создания жесткой ссылки невозможно различить, где исходное имя файла, а где ссылка. Если вы удаляете один из этих файлов (точнее одно из этих имен), то файл еще сохраняется на диске (пока у него есть хоть одно имя - жесткая ссылка). Очень трудно различить первоначальное имя файла и позже созданные жесткие ссылки на него. Поэтому жесткие ссылки применяются там, где отслеживать различия и не требуется. Одно из применений жестких ссылок состоит в том, чтобы предотвратить возможность случайного удаления файла. Особенностью жестких ссылок является то, что они прямо указывают на номер индексного дескриптора, а, следовательно, такие имена могут указывать только на файлы внутри той же самой файловой системы (т. е., на том же самом носителе, на котором находится каталог, содержащий это имя).

Мягкие (символические) ссылки тоже могут рассматриваться как дополнительные имена файлов, но в то же время они представляются отдельными файлами - файлами типа мягких ссылок и являются самостоятельным типом файла. Однако блоки данных файла в системе представляются в одном экземпляре, у файла-ссылки адреса блоков данных те же, что и у исходного файла. В отличие от жестких ссылок мягкие ссылки могут указывать на файлы, расположенные в другой файловой системе, например, на монтируемом носителе, или даже на другом компьютере. Если исходный файл удален, мягкая ссылка не удаляется, но становится бесполезной. Используйте мягкие ссылки в тех случаях, когда хотите избежать путаницы, связанной с применением жестких ссылок.