МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

## Факультет информационных технологий и робототехники

Кафедра программного обеспечения информационных систем

и технологий

**Отчет**

**по лабораторной работе № 2**

по дисциплине: ”Системное программирование”

на тему: ***”*****Администрирование системы Linux*”***

Выполнил**:** студент группы *10702121* Мялик А.С.

Писарик А. Г.

Филанович Д. Л.

Принял**:** пр. Давыденко Н. В.

Минск 2023

# Лабораторная работа №2.

**Цель работы:** Приобретение практических навыков администрирования и архивирования.

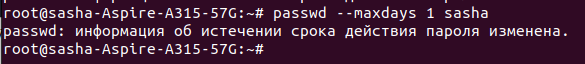
**Сравнение атрибутов реального пользователя и пользователя root в /etc/passwd:**





**Установка минимального и максимального возраста пароля:**





**Установка** **даты истечения срока действия учетной записи:**



**Установка дней предупреждения об истечении срока действия пароля:**



**Установка периода бездействия пароля:**



**Установка пользователю прав admina:**



**Создание пустого файла в директории home у пользователя maks:**







**Установка права доступа к файлу:**

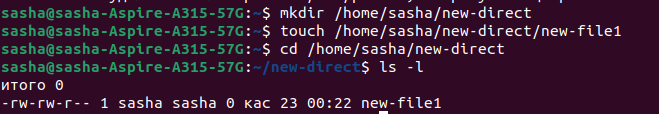


**Перевод пользователя в группу shadow:**



**Создание новой папки и создание в ней файлов:**

**Проверка прав доступа к файлам в папке:**



**Доступ к каталогу пользователя maks только самому пользователю и группе shadow:**



**Файлы второго пользователя доступны только владельцам. Назначение разрешения файлам только чтение:**



**Удаление пользователя из группы shadow:**



**Защита липким битом:**



8. Под админом назначить всем пользователям все права



С помощью команды usermod -aG groupname username добавляем пользователей в группу shadow.

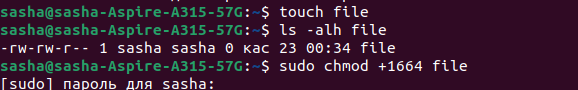
С помощью команды sudo chmod g+rwx /directory присваиваем права на чтение, запись и выполнение.

9. Удалить пользователя, находящегося в группе shadow



С помощью команды sudo deluser username groupname, удаляем пользователя из группы.

Создаем файл file и с помощью команды sudo chmod +1664 filename добавляем «липкий байт»



Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

При попытке удалить файл администратором admin выдает ошибку Permission denied.

**Ответы на контрольные вопросы:**

1. **Какая концепция прав доступа к файлу реализована в ядре?**

В ядре Linux реализована концепция прав доступа к файлам, основанная на системе управления правами доступа (DAC - Discretionary Access Control). В этой концепции каждый файл и каталог имеет владельца и группу, а также набор разрешений для трех категорий пользователей: владельца, членов группы и всех остальных пользователей.

Разрешения включают в себя:

Чтение (Read): Позволяет просматривать содержимое файла или каталога.

Запись (Write): Позволяет вносить изменения в файл или каталог (включая создание или удаление файлов в каталоге).

Выполнение (Execute): Позволяет запускать исполняемые файлы или входить в каталоги (для каталогов это право также называется "поиском").

Каждый файл или каталог имеет набор разрешений для каждой из трех категорий пользователей, и эти разрешения задаются с помощью команды chmod или через атрибуты файла.

**6. Опишите отличия команд su и sudo.**

Команда su (от switch user) используется для переключения пользователя в системе. При использовании команды su без указания имени пользователя, пользователь получает полные привилегии суперпользователя (root) и может выполнять любые команды. Если указать имя пользователя с помощью команды su, то пользователь переключится на учетную запись этого пользователя с сохранением текущего рабочего каталога и среды. При этом будут доступны только права и ресурсы, которые были назначены этой учетной записи.

Команда sudo (от superuser do) позволяет пользователю выполнять команды от имени суперпользователя без необходимости полного переключения на его учетную запись. При использовании команды sudo перед командой, пользователь должен указать свой пароль и после этого выполнение команды будет разрешено, если у пользователя есть соответствующие права. Таким образом, команда sudo предоставляет временные привилегии суперпользователя только в рамках конкретной команды, после выполнения которой вернется режим обычного пользователя.

Главное отличие между командами su и sudo заключается в том, что команда su позволяет получить полные привилегии суперпользователя на весь сеанс, в то время как команда sudo предоставляет временные права суперпользователя только для конкретной команды. Кроме того, команда sudo позволяет более гибко управлять доступом пользователей к определенным командам, поскольку права на выполнение каждой команды можно настроить отдельно.

**8. Для чего предназначена системная директория etc, какие файлы в ней храняться?**

Директория /etc в системах Unix/Linux предназначена для хранения конфигурационных файлов и скриптов, относящихся к системе и установленным программам. В этой директории содержатся текстовые файлы, определяющие параметры работы различных компонентов системы.

Некоторые типичные файлы и поддиректории в /etc:

/etc/passwd - файл, содержащий информацию о пользователях системы.

/etc/group - файл, описывающий группы пользователей.

/etc/hostname - файл с именем хоста (имя компьютера) системы.

/etc/network/ - поддиректория, содержащая файлы конфигурации сетевых настроек.

/etc/hosts - файл, используемый для разрешения IP-адресов именами хостов.

/etc/resolv.conf - файл с настройками DNS-резольвера.

/etc/apt/ - директория для конфигурационных файлов системы управления пакетами APT (Advanced Package Tool) в Debian и его производных.

/etc/fstab - файл, определяющий монтирование файловых систем при загрузке.

/etc/ssh/ - поддиректория с настройками для SSH (Secure Shell).

/etc/sysconfig/ - в некоторых дистрибутивах Linux, таких как Red Hat, здесь хранятся файлы конфигурации системы.

Эти файлы и директории предоставляют средства для настройки различных аспектов системы и приложений, позволяя администраторам адаптировать поведение системы под свои потребности.

**10. В чем различие понятий «пользователь» и «аккаунт пользователя»? Объясните это на примере строки файла /etc/passwd**.

Понятия "пользователь" и "аккаунт пользователя" связаны с учетными записями пользователей в операционной системе Unix/Linux. Они имеют следующие различия:

Пользователь - это абстрактное понятие, представляющее собой человека или системный процесс, который использует операционную систему. Пользователь может быть физическим лицом, работающим на компьютере, или системным компонентом (например, службой или процессом), который имеет собственный идентификатор пользователя (UID).

Аккаунт пользователя - это конкретная учетная запись, которая связана с пользователем и предоставляет ему доступ к системе. Аккаунт пользователя содержит информацию, такую как имя пользователя (login name), пароль (хешированный или ссылка на файл с хешем), идентификатор пользователя (UID), идентификатор группы (GID), домашний каталог пользователя и дополнительные параметры.

Пример строки файла /etc/passwd:

john:x:1000:1000:John Doe:/home/john:/bin/bash

В этой строке:

john - это имя пользователя (login name).

x - это поле для хранения хеша пароля (фактический хеш пароля хранится в /etc/shadow).

1000 - это UID (идентификатор пользователя).

1000 - это GID (идентификатор группы).

John Doe - это поле с полным именем пользователя.

/home/john - это домашний каталог пользователя.

/bin/bash - это командный интерпретатор (shell), который используется при входе пользователя в систему.

Таким образом, в данном примере "пользователь" - это John Doe, а "аккаунт пользователя" - это информация, предоставляющая John Doe доступ к системе, включая его имя пользователя и другие параметры. Каждая строка в файле /etc/passwd представляет собой аккаунт одного пользователя.