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 № 1а**

по дисциплине: «Системное программирование»

на тему: «Администрирование системы Linux»

Выполнила: ст. гр. 10702221

Баяманова А.К.

Проверил: Давыденко Н.В.

Минск 2023

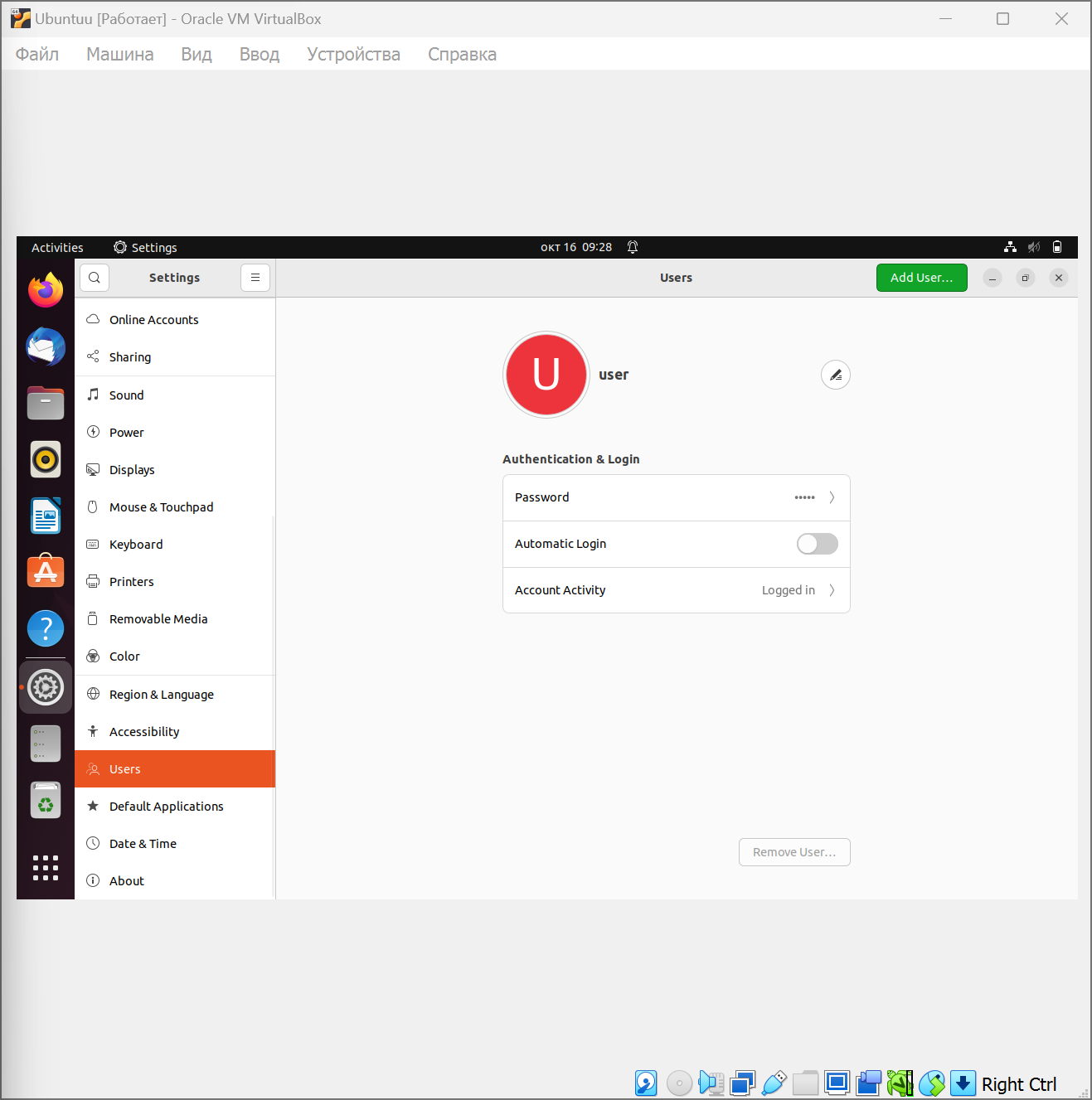
**ЛАБОРАТОРНАЯ РАБОТА #1а**

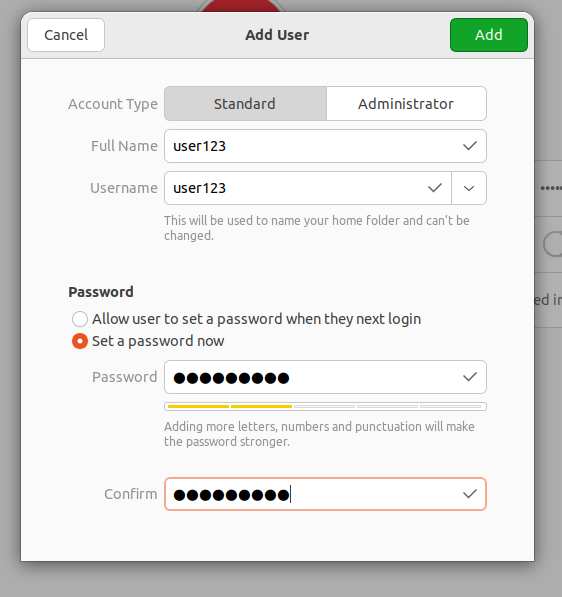
**Администрирование системы Linux**

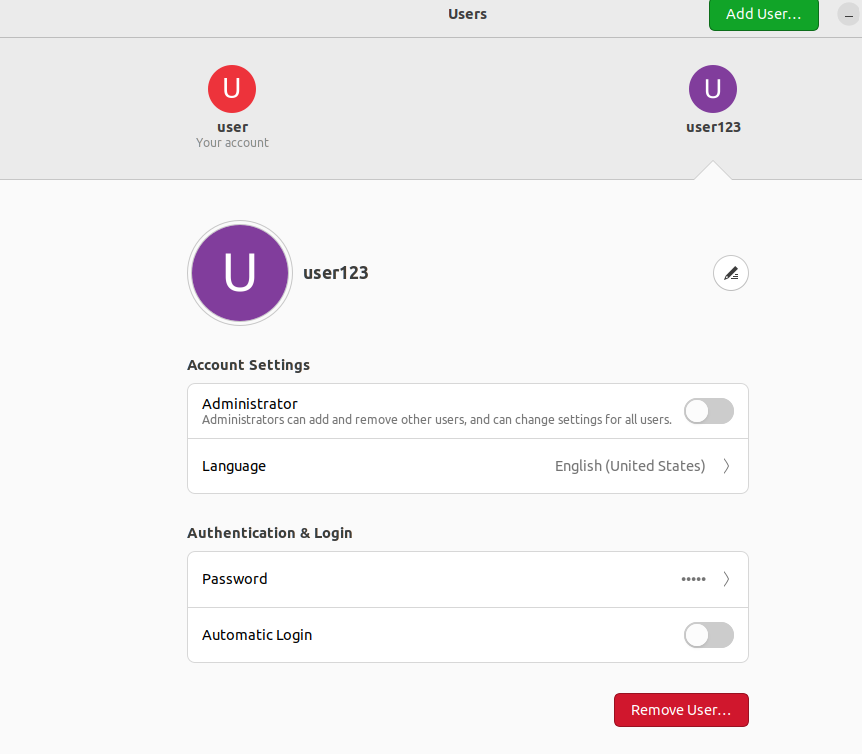
**Цель работы:** Закрепить на практике основы администрирования системы Linux, изучить атрибуты файлов и права доступа к ним, освоить работус файлами и каталогами.

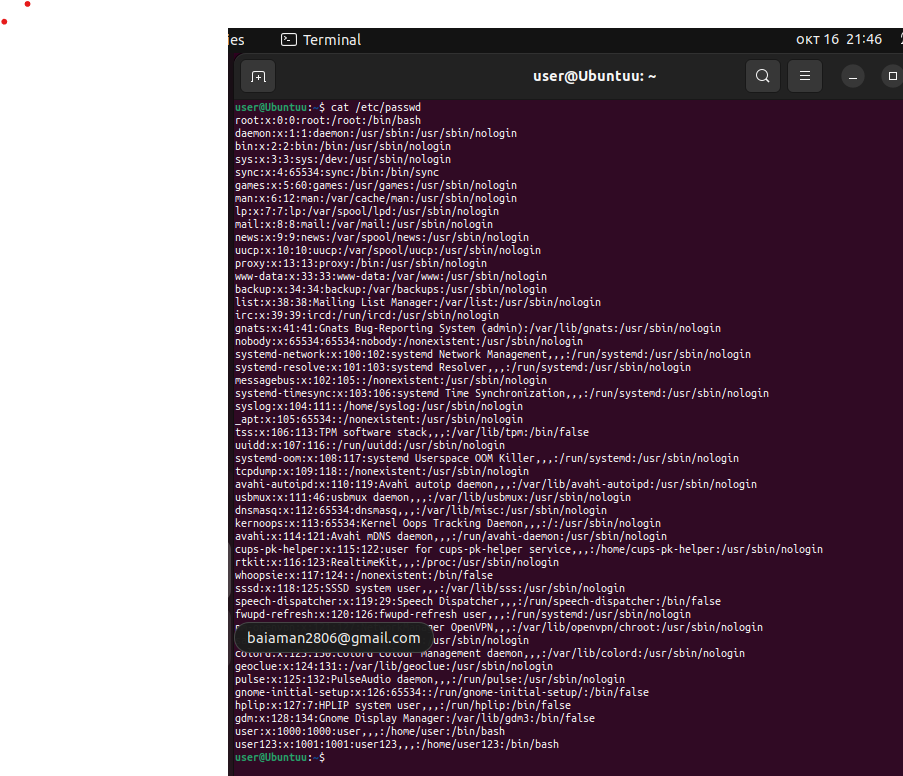
**Задание 1 – Создание пользователей**

Создайте стандартного пользователя с помощью GUI. Пользователю присвойте имя члена вашей команды, но в имени должен присутствовать суфффикс \*GUI. Это нужно для проведения экспериментов. При присвоении имен действуйте по принципу: «Относитесь к именам переменных, как к именам детей своих». Пароль пользователя должен быть простым, например «123».

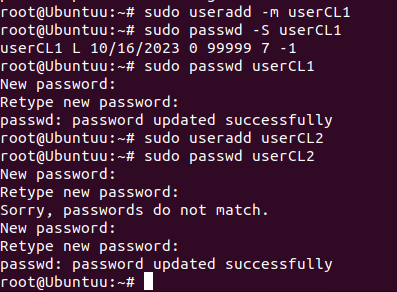




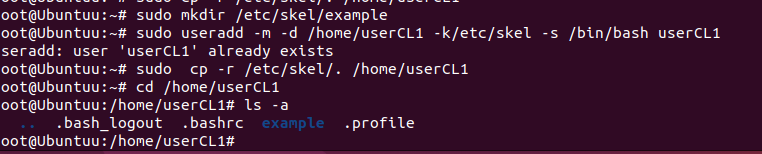


Просмотрите содержимое файла /etc/passwd, сравните атрибуты реальных пользователей и пользователя root. Результат поддтвердите скриншотом. Дайте пояснения. 

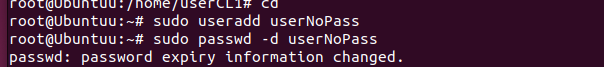
Создайте несколько стандартных пользователей (аккаунтов) посредсвам командной строки. При этом пользователям присвойте имена членов вашей команды, но в имени должен присутствовать суфффикс \*CL или \*CLI. Это нужно для того, чтобы отличить пользователей созданных при помощи графического и консольного интерфейсов. Создайте двуъ пользователей с одинаковыми простыми паролями.



Создайте скелет и пользователя с шаблоном скилета в директории /home.

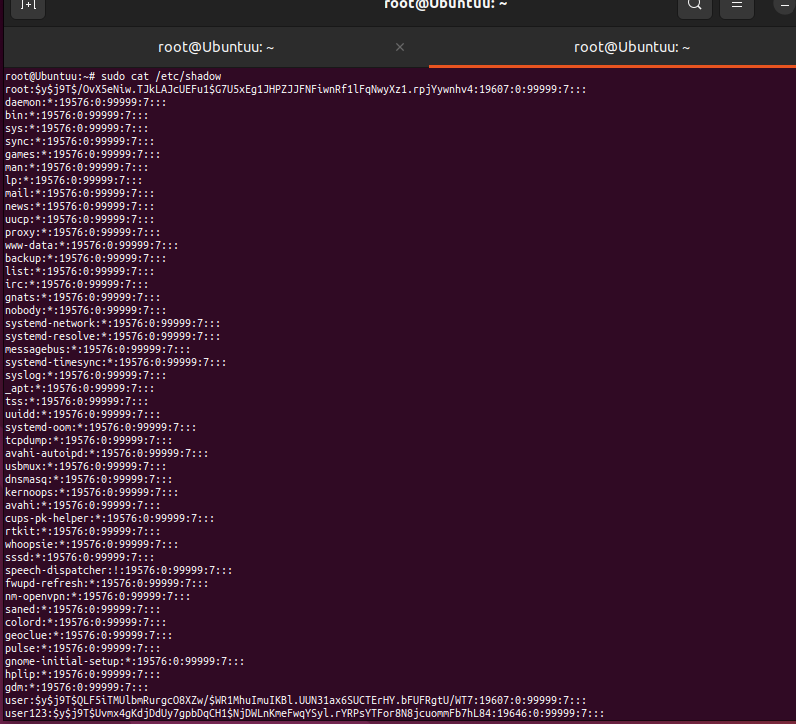


Также попробуйте создать аккаунт реального пользователя без пороля.

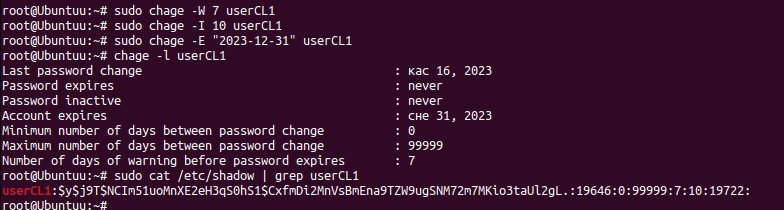


**Задание 2 – Изменение параметров паролей пользователей :**

Пароли должны быть простые и одинаковые. Это нужно для проведения экспериментов. Просмотрите содержимое файла /etc/passwd, сравните атрибуты реальных пользователей. Просмотрите содержимое файла /etc/shadow, сравните атрибуты паролей пользователей, особое внимание обратите на шифр пароля у пользователей с однаковым паролем.



Измените периоды изменения паролей для пользователей. Внесите ограничения в следующие атрибуты: минимальный возраст пароля (сутки);максимальный возраст пароля (сутки); период предупреждения пароля; период бездействия пароля; дата истечения срока действия аккаунта. Результат подтвердите скриншотом. Дайте пояснения.



Установить минимальный и максимальный возраст пароля (в днях):

sudo chage -m 1 -M 30 username

Установить период предупреждения пароля (в днях):

sudo chage -W 7 username

Установить период бездействия пароля (в днях):

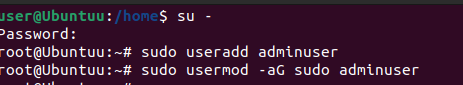
sudo chage -I 10 username

Установить дату истечения срока действия аккаунта (в формате ГГГГ-ММ-ДД):

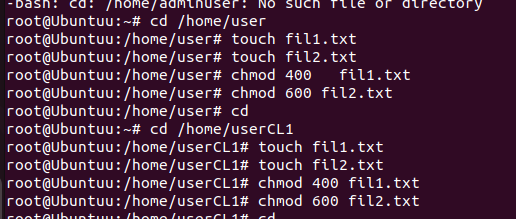
sudo chage -E "2023-12-31" username

**Задание 3 – Создание групп и работа с правами доступа к файлам:**

Создайте пользователя (аккаунт) с правами администратора.



В каталогах /home/ администраторов и других пользователей создайте по несколько файлов с разными правами доступа.

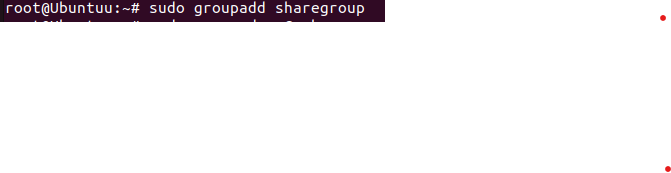


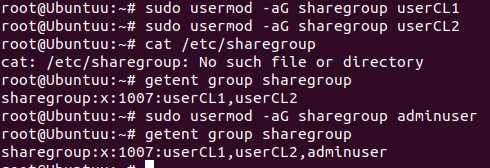
4 представляет право "только для чтения".

6 представляет права "чтение и запись".



Создайте общую группу пользователей.





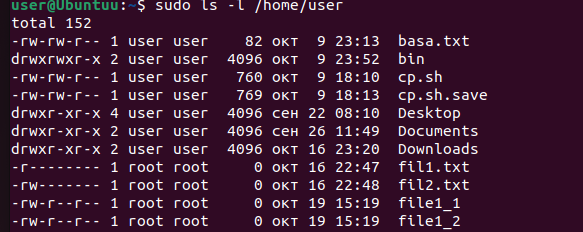
Выполните следующие требования:

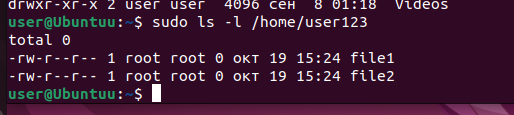
1. Одного из пользователей перевести в группу shadow 
2. Создать у каждого пользователей директорию с 2 файлам





1. Просмотреть текущие права доступа к файлам для всех пользователей





1. Каталог пользователя в группе shadow сделать доступным только в своей группе



1. Файлы второго пользователя сделать доступными только владельцам



1. **Под админом назначить всем созданным файлам права только для чтения для всех пользователей**



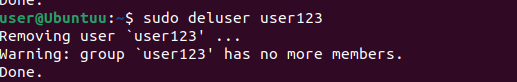
1. **Пользователем в группе shadow лишить всех остальных пользователей права исполнять его файлы**



1. **Под админом назначить всем пользователям все права**



1. **Удалить пользователя, находящегося в группе shadow**



**Укажите является ли группа системной или создана пользвателем.**

**Получите индентификаторы пользователей и состояние активных пользователей системы. Проверьте содержимое файлов /etc/shadow, /etc/passwd,/etc/group**

Системные группы:

• root (GID 0) - суперпользователь.

• bin (GID 1) - системная группа для бинарных файлов и команд.

• adm (GID 4) - системная группа для журналов и отчетов.

Группы, созданные пользователями:

• users (GID 100) - группа, в которой могут состоять обычные пользователи.

• developers (GID 101) - группа, созданная для разработчиков программного обеспечения.

• friends (GID 102) - группа, созданная для друзей пользователя.

Вы можете использовать команду getent group или просмотреть файл /etc/group, чтобы просмотреть список всех групп в системе и определить, к какому из двух типов они относятся. Системные группы будут перечислены в начале файла /etc/group, а группы, созданные пользователями, будут перечислены позже.

**Некоторые файлы защитите липким битом. Попробуйте удалить созданные**

**файлы из других аккаунтов администраторов и простых пользователей.**

**Опишите какой получили результат.**

Установка "липкого бита" (sticky bit) на директории в Linux означает, что только владелец файла может удалять его из этой директории, даже если другие пользователи имеют права записи в эту директорию. Это обычно используется на директории /tmp, чтобы предотвратить случайное удаление файлов другими пользователями.

Чтобы установить "липкий бит" на директорию, вы можете использовать команду chmod с параметром "+t".

После установки "липкого бита" на директорию, даже если у других пользователей есть права на запись в эту директорию, они не смогут удалить файлы, которые они сами создали в ней. Только владелец файла сможет удалить свои файлы.

Просто пользователи, даже с правами администратора, не смогут удалить файлы других пользователей из этой директории, если они не являются владельцами этих файлов. Администратор может изменить права на файлы или директории, но это делается отдельно и не зависит от "липкого бита".



**Контрольные вопросы:**

В Linux (и Unix-подобных операционных системах) существует несколько типов пользователей, каждый из которых имеет определенные права и привилегии. Вот основные типы пользователей:

**1. \*\*Суперпользователь (root)\*\*:**

- Также известен как администратор.

- Имеет максимальные привилегии в системе.

- Может выполнять любую операцию и изменять системные настройки.

- Доступ к системе root следует использовать осторожно, так как неправильные действия могут повредить систему.

**2. \*\*Системные пользователи\*\*:**

- Эти пользователи создаются системой для выполнения служб и процессов.

- Они обычно не предназначены для интерактивного входа и работы пользователей.

- Примеры системных пользователей включают `root`, `daemon`, `nobody`, и другие.

**3. \*\*Обычные пользователи\*\*:**

- Это обычные учетные записи для обычных пользователей системы.

- Они имеют ограниченные привилегии и доступ к системным ресурсам.

- Эти пользователи используются для выполнения обычных задач и приложений.

**4. \*\*Группы пользователей\*\*:**

- В Linux существуют группы пользователей, которые объединяют пользователей с общими задачами или привилегиями.

- Группы могут быть использованы для управления доступом к файлам и ресурсам.

- Например, группа `sudo` содержит пользователей, которым разрешено выполнение команд с правами суперпользователя.

**5. \*\*Псевдопользователи\*\*:**

- Эти учетные записи используются для выполнения определенных служб и задач, но они не имеют интерактивного доступа к системе.

- Примеры псевдопользователей включают `nobody`, `mail`, `ftp`, и другие.

**6. \*\*Сетевые и удаленные пользователи\*\*:**

- Это пользователи, которые могут получить доступ к системе удаленно через сеть, например, по SSH или FTP.

- Система обычно имеет пользователей, специально предназначенных для удаленного доступа.