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 № 5**

по дисциплине:” Системное программирование”

на тему: “Командный язык и скрипты Shell”

Выполнил**:** студент группы 10701321

Черепковский М.В.

Принял**:** Давыденко Н.В.

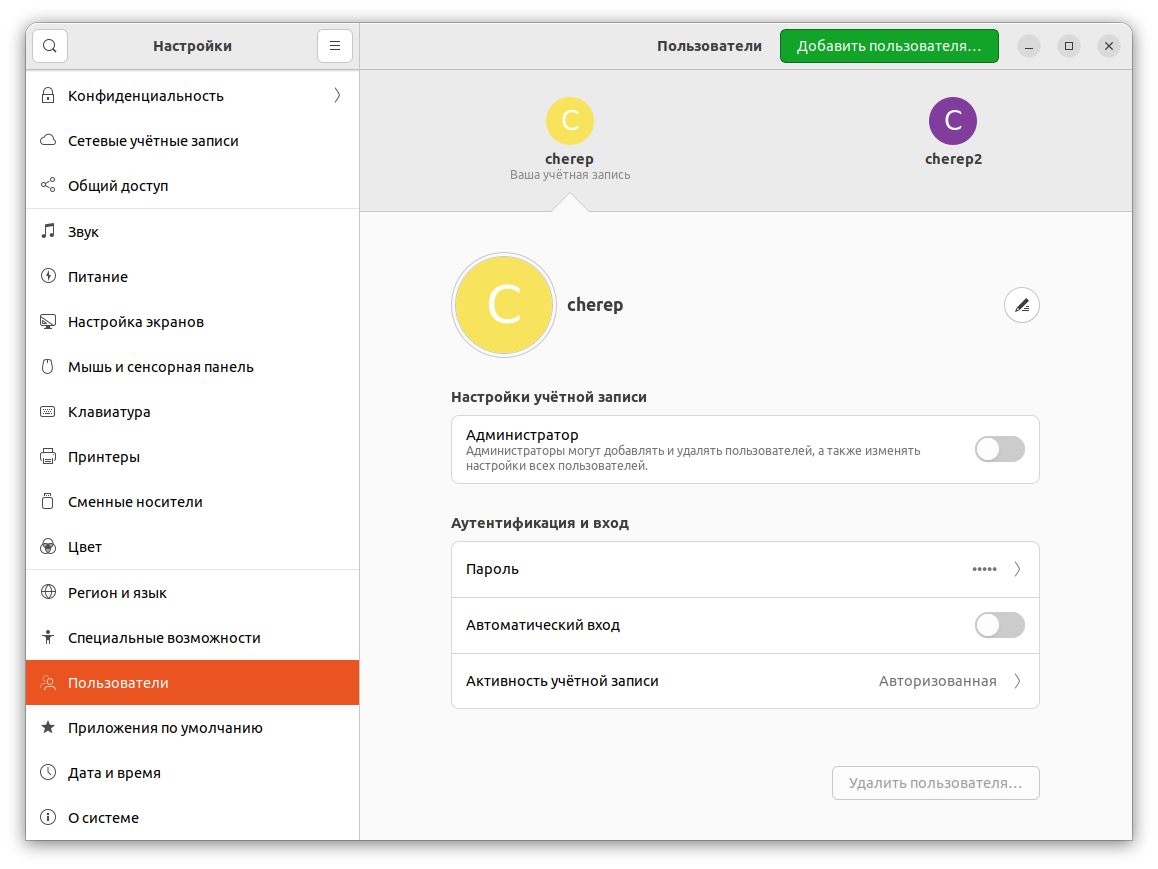
Минск 2023

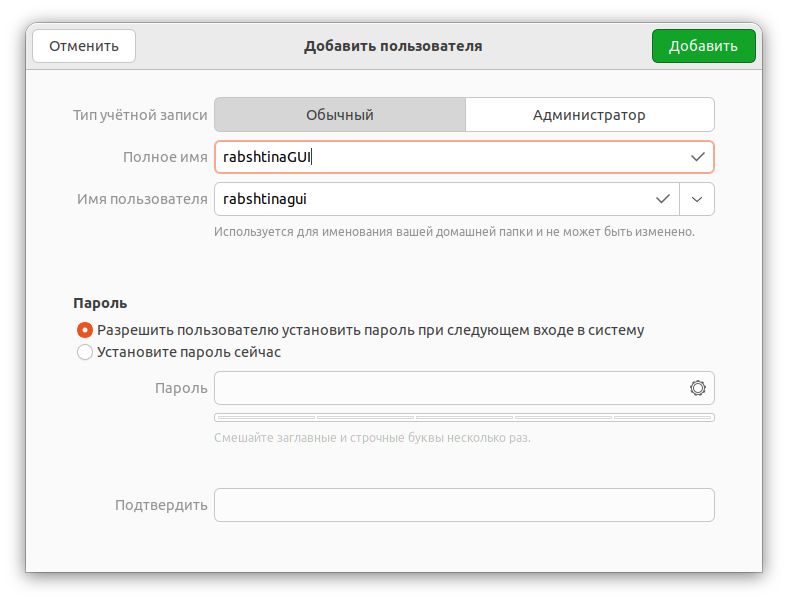
# Лабораторная работа № 5 Администрирование системы Linux

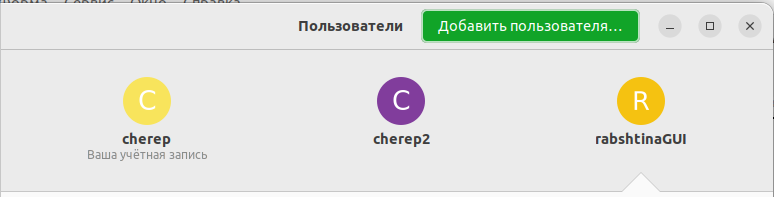
# Цель работы: Закрепить на практике основы администрирования системы Linux, изучить атрибуты файлов и права доступа к ним, освоить работу с файлами и каталогами.

Задание 1 - Создание пользователей

1. Создайте стандартного пользователя с помощью GUI.

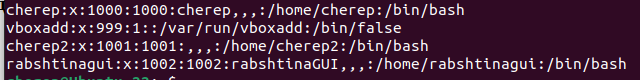






2. Просмотрите содержимое файла /etc/passwd, сравните атрибуты реальных

пользователей и пользователя root.

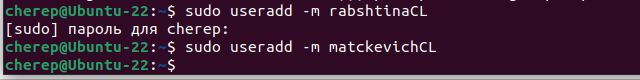


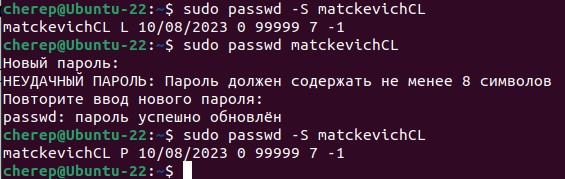
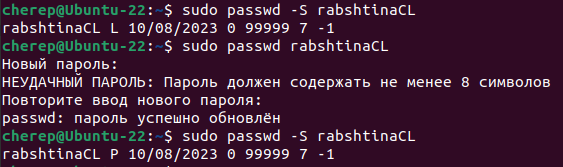
Пользователь "root" обычно имеет UID 0 и имеет полные привилегии в системе. Он также обычно имеет домашний каталог "/root" и использует оболочку "/bin/bash" или "/bin/sh".

Атрибуты реальных пользователей могут различаться в зависимости от их роли и настроек в системе. Обычно, UID реальных пользователей отличается от 0, и у них есть свои собственные домашние каталоги и оболочки.

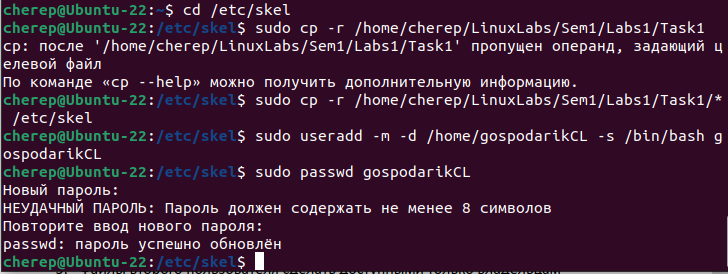
3. Создайте несколько стандартных пользователей (аккаунтов) посредсвам

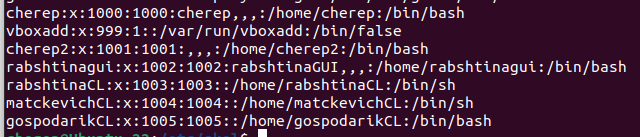
командной строки.



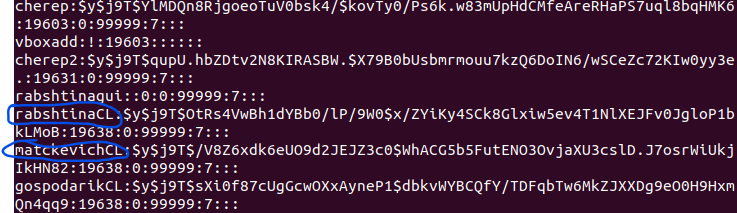
4. Создайте двух пользователей с одинаковыми простыми паролями.

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



Задание 2 - Изменение параметров паролей пользователей  
Сравниваем атрибуты реальных ползователей

Сравниваем шифры пользователей с одинаковыми паролями



Измените периоды изменения паролей для пользователей.

Минимальный возраст пароля (минимальное количество дней, которые должны пройти, прежде чем пользователь сможет изменить пароль):

sudo chage -m <минимальный\_возраст> имя\_пользователя





Максимальный возраст пароля (максимальное количество дней, после которого пользователь должен изменить пароль):

sudo chage -M <максимальный\_возраст> имя\_пользователя





Период предупреждения пароля (количество дней, за которое пользователь будет предупрежден о необходимости изменения пароля):

sudo chage -W <период\_предупреждения> имя\_пользователя





Период бездействия пароля (количество дней, в течение которых пароль может оставаться неизменным после истечения максимального возраста пароля):

sudo chage -I <период\_бездействия> имя\_пользователя





Дата истечения срока действия аккаунта (количество дней с момента создания аккаунта, после которых он станет недействительным):

sudo chage -E <дата\_истечения> имя\_пользователя





Задание 3 - Создание групп и работа с правами доступа к файлам

1. \*\*Создание пользователя с правами администратора\*\*:

```bash

sudo useradd -m -G sudo admin

```



2. \*\*Создание каталогов и файлов с разными правами доступа\*\*:

```bash

# Создание каталогов

sudo mkdir /home/administrator /home/otheruser

# Создание файлов в каталоге пользователя "admin"

sudo touch /home/administrator/file1

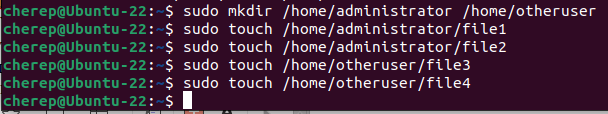
sudo touch /home/administrator/file2

# Создание файлов в каталоге пользователя "otheruser"

sudo touch /home/otheruser/file3

sudo touch /home/otheruser/file4

```



3. \*\*Создание общей группы пользователей\*\*:

```bash

sudo groupadd sharedgroup

```



4. \*\*Назначение прав доступа\*\*:

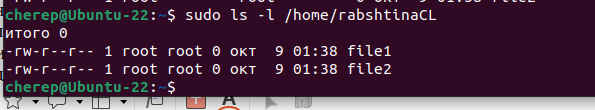
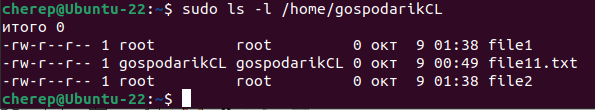
```bash

sudo chmod ug+rwx /home/administrator/file1

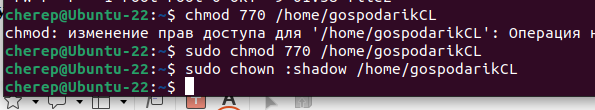
sudo chown admin:sharedgroup /home/administrator/file1

```

Это назначит права на чтение, запись и выполнение (rwx) файлу "file1" пользователю "admin" и группе "sharedgroup".  
  
  
  
  
1. Одного из пользователей перевести в группу shadow  
  
  
2. Создать у каждого пользователей директорию с 2 файлам  

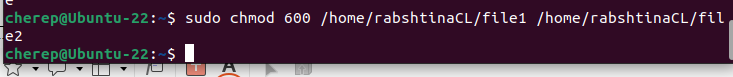

3. Просмотреть текущие права доступа к файлам для всех пользователей

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

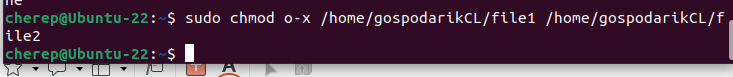


5. Файлы второго пользователя сделать доступными только владельцам

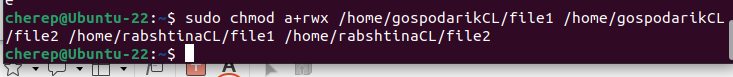
6. Под админом назначить всем созданным файлам права только для чтения для всех пользователей



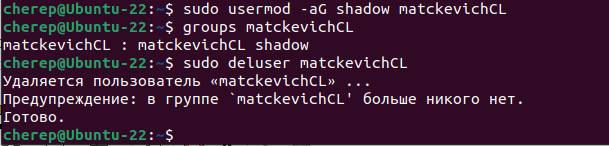
7. Пользователем в группе shadow лишить всех остальных пользователей права исполнять его файлы



8. Под админом назначить всем пользователям все права



9. Удалить пользователя, находящегося в группе shadow



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.

Вывод*:* В ходе выполнения лабораторной работы изучили основные команды для администрирования.  
  
Контрольные вопросы:  
**В чем отличие символов строки приглашения $ и # ?**

$ (Доллар) - Обычный пользователь (Пользовательский режим)

# (Решетка) - Суперпользователь (Режим суперпользователя)

1)                       Какая концепция прав доступа к файлу реализована в ядре?

2)                       Какие типы пользователей существуютс в Linux (UNIX)?

1)                       В чем отличие символов строки приглашения **$** и **#** ?