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 № 1a**

по дисциплине:” Системное программирование”

на тему: “ Основы администрирования ”

Выполнил**:** студент группы 10701321

Мацкевич М.Ю.

Принял**:** Давыденко Н.В.

Минск 2023

# Лабораторная работа № 1a Основы администрирования

# Цель работы Научиться создавать архивы, сжатие и распаковку файлов, создавать резервные копии данных, синхронизировать файлы и каталоги. Рассмотрим несколько программ, часто используемых для управления коллекциями файлов.

**Задание 1.**

**Создание пользователей**  Создайте стандартного пользователя с помощью GUI. Пользователю присвойте имя члена вашей команды, но в имени должен присутствовать суфффикс \*GUI.

# 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.

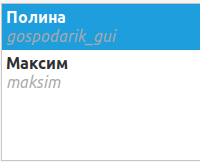


Рис.1. Пользователь, созданный через GUI

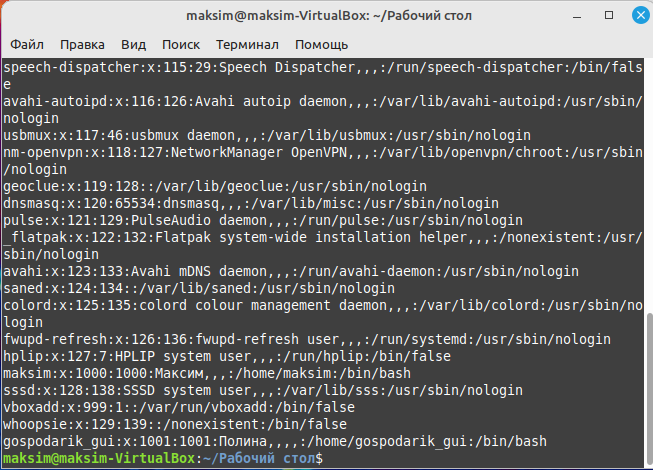


Рис.2. Файл passwd

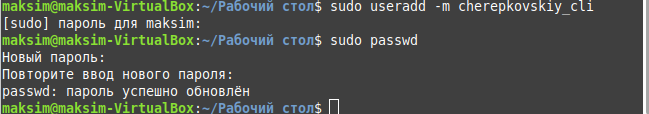


Рис.3.Создание первого пользователя через CLI

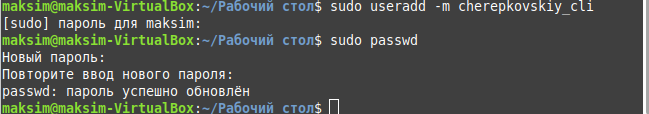


Рис.4.Создание второго пользователя через CLI

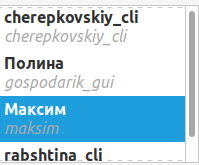


Рис.5.Список пользователей

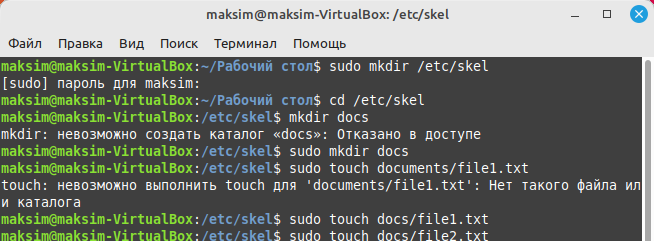


Рис.6.Создание скелета

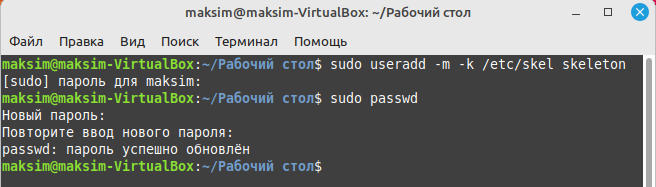


Рис.7.Создание пользователя на основе скелета

**Задание 2 – Изменение параметров паролей пользователей   
Просмотрите содержимое файла /etc/shadow, сравните атрибуты паролей пользователей, особое внимание обратите на шифр пароля у пользователей с одинаковым 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.**

Файл shadow

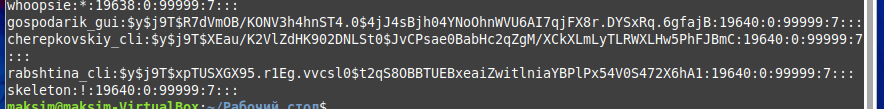


Рис.8. Файл shadow

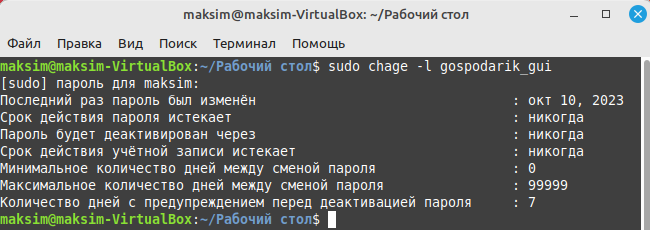


Рис.9. Параметры аккаунта до изменения

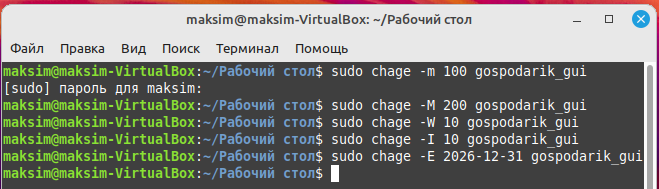


Рис.10. Изменение параметров аккаунта

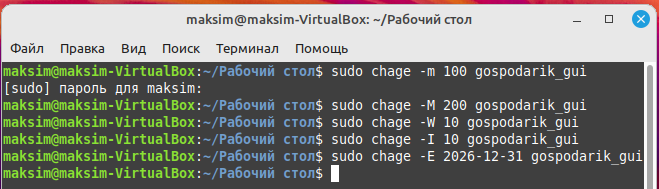


Рис.11. Параметры аккаунта после изменения

-m, --mindays MIN\_DAYS: Установка минимального возраста пароля в днях (пользователь не может изменить пароль в течение этого количества дней после его смены).

-M, --maxdays MAX\_DAYS: Установка максимального возраста пароля в днях (пользователь может использовать текущий пароль в течение этого количества дней).

-W, --warndays WARN\_DAYS: Установка периода предупреждения в днях (количество дней, за которое пользователь будет предупрежден о необходимости сменить пароль).

-I, --inactive INACTIVE: Установка периода бездействия в днях (количество дней, после которых пароль будет заблокирован в случае неактивности пользователя).

-E, --expiredate EXPIRE\_DATE используется для установки даты истечения срока действия аккаунта.

**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. Создайте общую группу пользователей. Выполните следующие требования:**

**1. Одного из пользователей перевести в группу shadow**

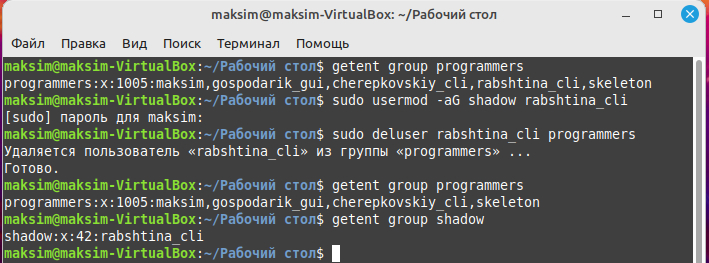


Рис.12. Перенос пользователя в группу shadow

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

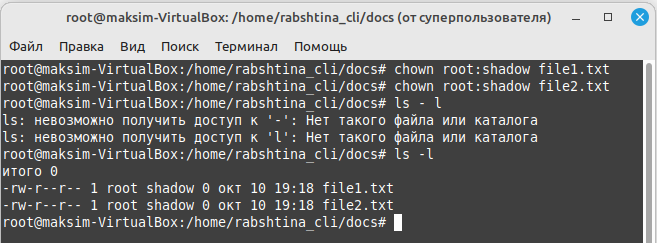


Рис.13. Изменение прав доступа к файлу

**5. Файлы второго пользователя(rabshtinagui) сделать доступными только владельцам**

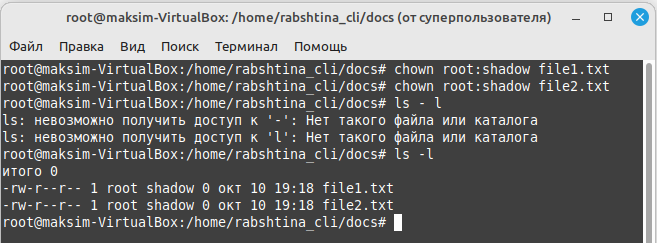


Рис.14. изменение прав доступа к файлу

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

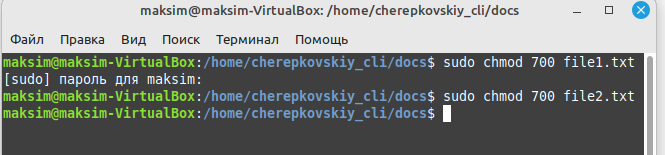


Рис.15. Изменение прав от имени админа

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

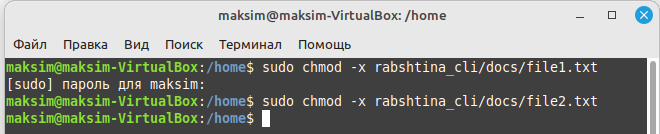


Рис.16. Изменение прав

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

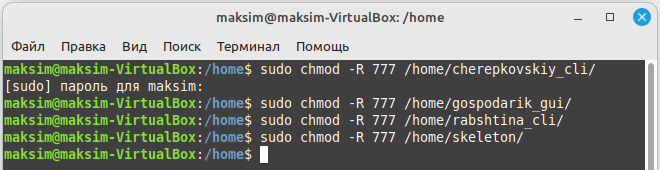


Рис.17. Изменение прав

**9. Удалить пользователя, находящегося в группе shadow Укажите является ли группа системной или создана пользователем.**

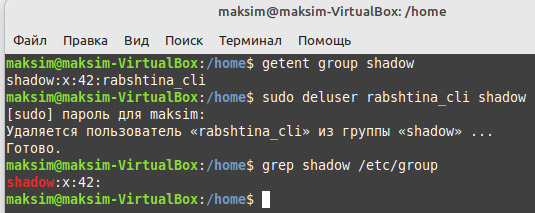


Рис.18. Удаление пользователя из группы

**Группа не системная**

**Получите идентификаторы пользователей и состояние активных пользователей системы.**

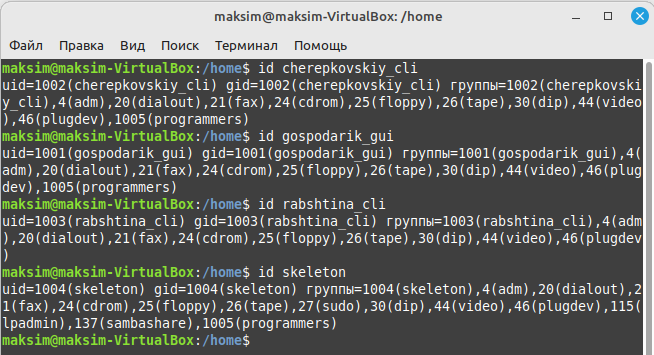
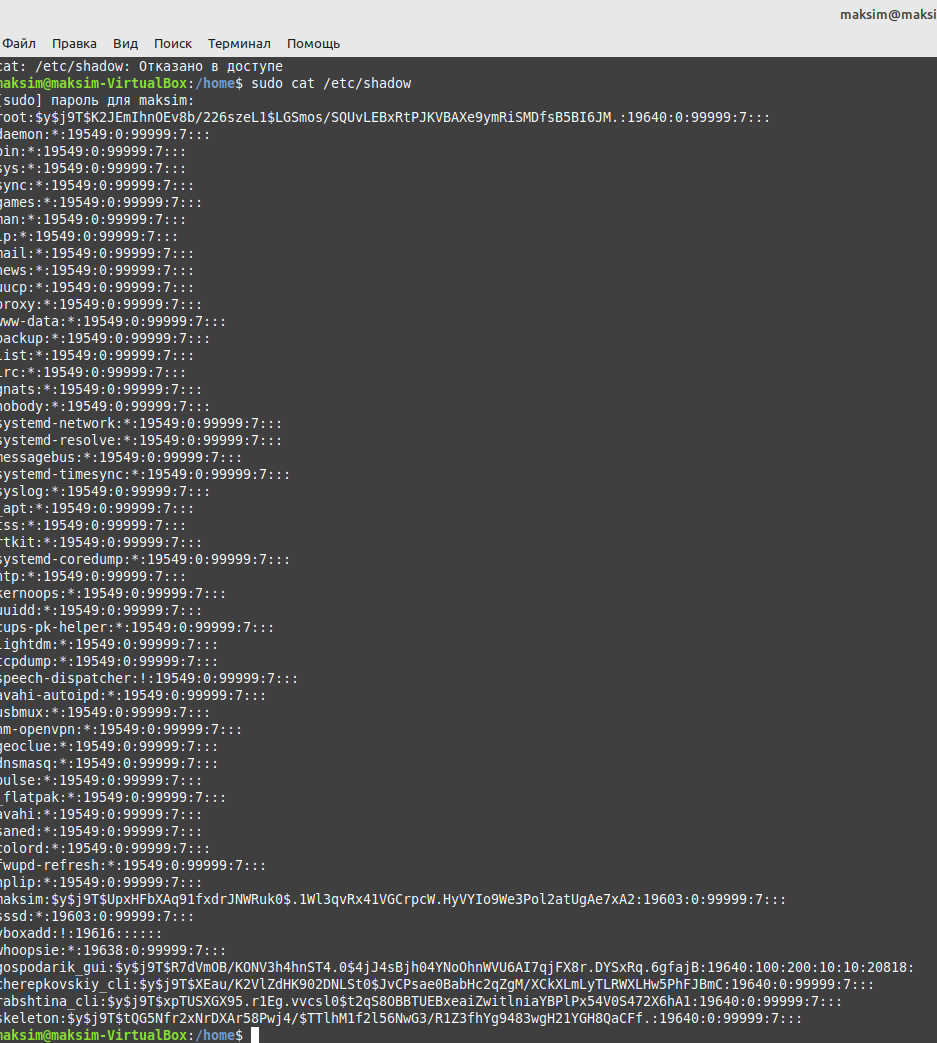
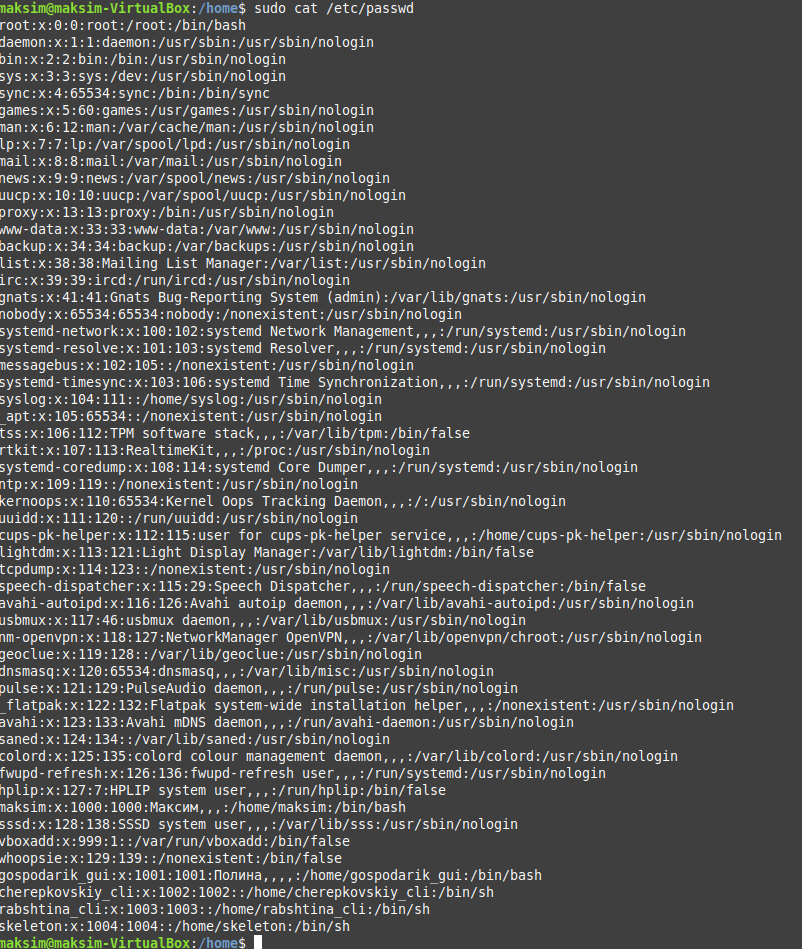


Рис.19. Идентификаторы пользователей

**Проверьте содержимое файлов /etc/shadow, /etc/passwd, /etc/group.**.

Рис.20. Файл /etc/shadow

  
Рис.21. Файл /etc/passwd

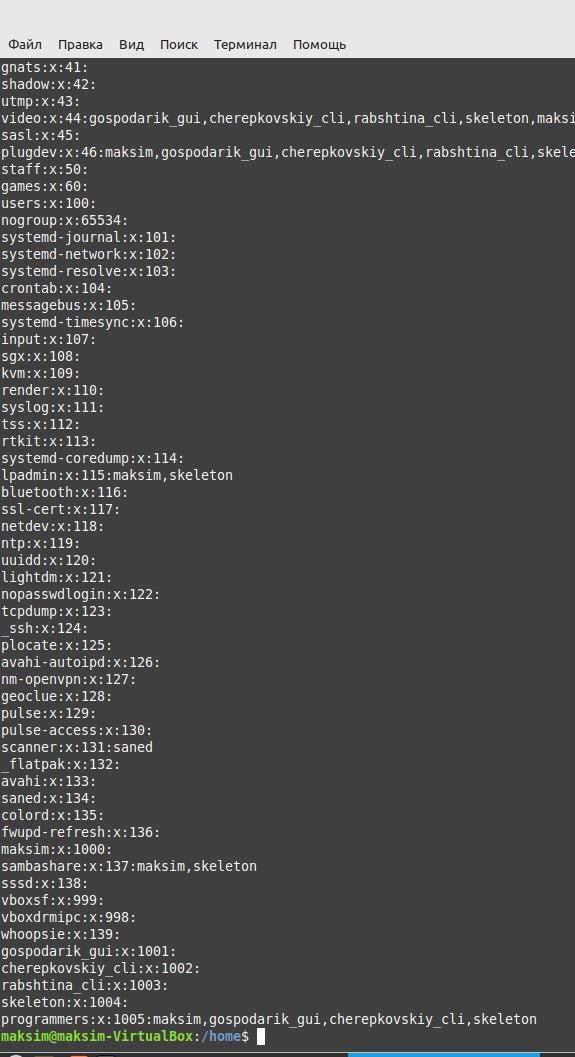


Рис.22. Файл /etc/group

**Создайте жесткую ссылку, перенесите эту ссылку в пространство другогопользователя и откройте ее в сеансе этого пользователя**

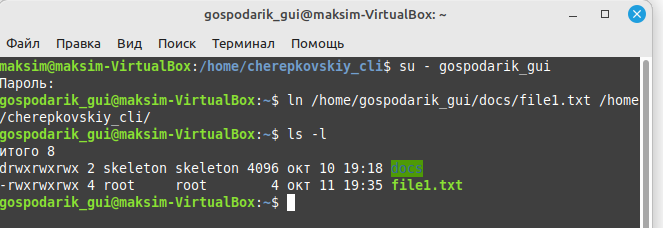
****

Рис.23. Создание жёсткой ссылки

**Измените владельца и группу жесткой ссылки и посмотрите, как изменились атрибуты основного файла.**

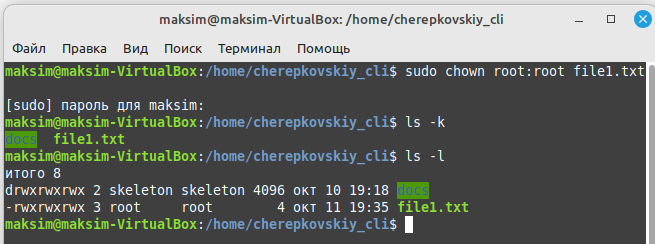


Рис.24. Изменённые атрибуты жёсткой ссылки

Вывод*:* В ходе выполнения лабораторной работы научились работать с сжатием и архивирование файлов на Ubuntu, научились синхронизировать директории, научились работе с пользователями и группами.  
  
Контрольные вопросы:  
**Опишите отличия команд su и sudo.**

1. su (Switch User):
   * su используется для переключения пользователя на другого пользователя или на суперпользователя (root).
   * При использовании su необходимо знать пароль целевого пользователя (или root), чтобы переключиться на его учетную запись.
   * Когда вы используете su, вы переключаетесь на новую учетную запись полностью и выполняете команды от ее имени.
   * su не записывает команды в журнал системы.
2. sudo (Superuser Do):
   * sudo позволяет текущему пользователю выполнять определенные команды с административными (суперпользовательскими) правами, без необходимости знать пароль суперпользователя (root).
   * Для того чтобы использовать sudo, пользователь должен быть включен в файл /etc/sudoers и иметь права на выполнение команд с sudo.
   * sudo записывает выполненные команды в журнал системы, что позволяет вести отслеживание и аудит действий пользователей с привилегиями.
   * sudo обычно требует ввод пароля текущего пользователя, чтобы подтвердить его личность перед выполнением команды с повышенными правами.