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: ”Администрирование системы Linux***”***

Выполнил**:** студент группы 10701321 Кругликовский М.А.

Принял**:** ст.пр. Станкевич C.П.

Минск 2023

# **Лабораторная работа № 5**

**Цель работы**

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

**Задание**

**Задание 1**

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**

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 поддтвердите скриншотом. Дайте пояснения.

**Задание 3**

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 2. Создать у каждого пользователей директорию с 2 файлами 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 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.

Некоторые файлы защитите липким битом. Попробуйте удалить созданные файлы из других аккаунтов администраторов и простых пользователей. Опишите какой получили результат. Создайте жесткую ссылку, перенесите эту ссылку в пространство другого пользователя и откройте ее в сеансе этого пользователя, затем присвойте жесткой ссылке одну группу и откройте ссылку из пользователя этой группы. Измените владельца и группу жесткой ссылки и посмотрите, как изменились атрибуты основного файла. Примените разные варианты изменения атрибутов доступа файла и каталогов. Попробуйте совершить разные операции с этими файлами от имени других пользователей. Активно используйте команду su.

**Результаты выполнения**

**Задание 1**

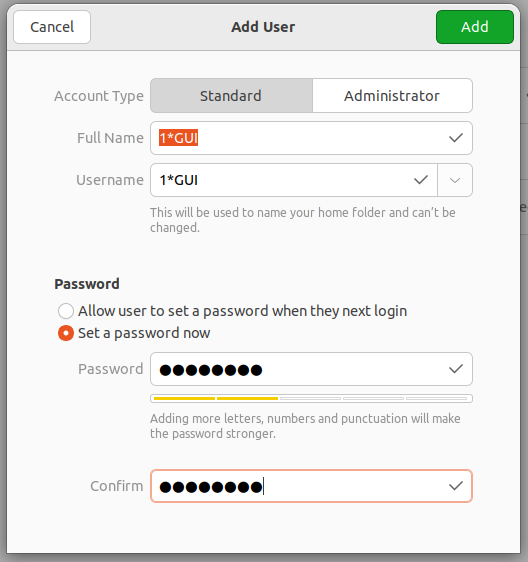
****

Рисунок 1. Создание пользователя через GUI

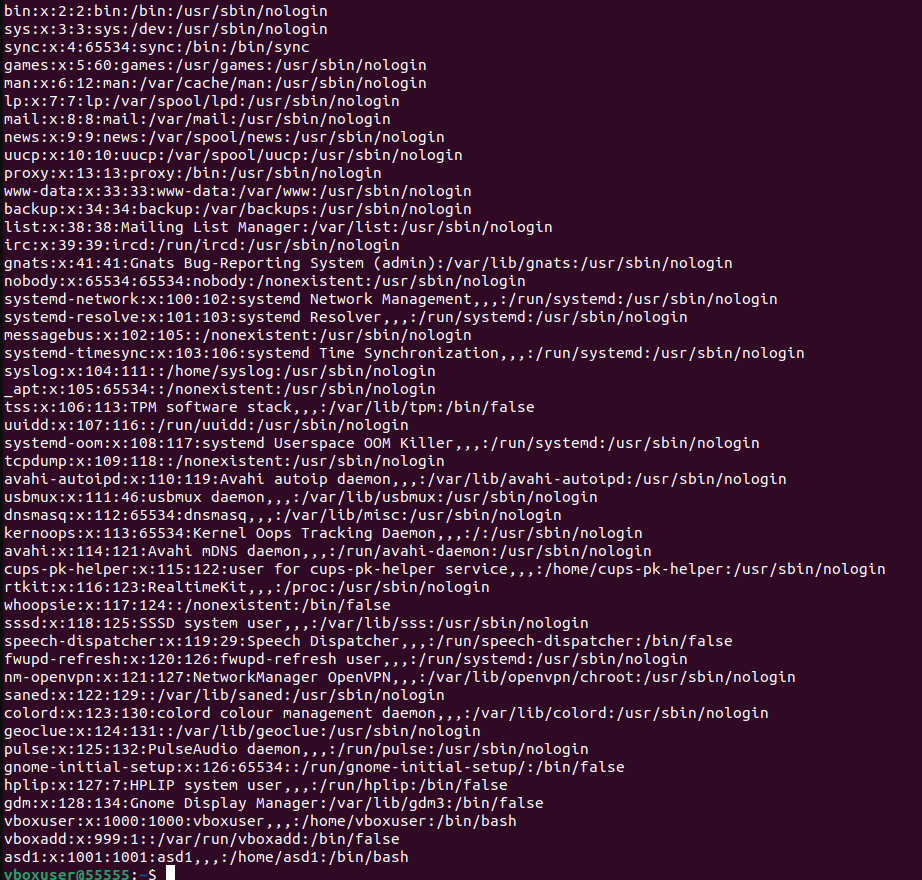


Рисунок 2. Просмотр содержимого файла /etc/passwd

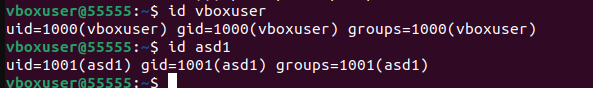


Рисунок 3. Сравнение атрибутов пользователей root и созданного мной пользователя

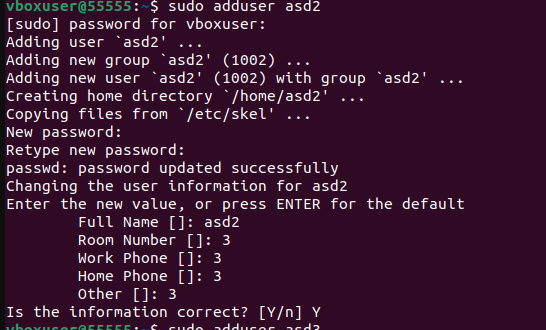


Рисунок 4. Создания пользователей через командную строку

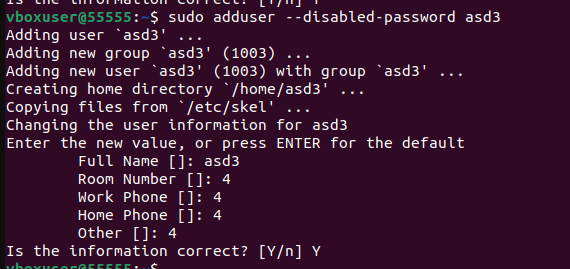


Рисунок 5. Создание пользователя без пароля

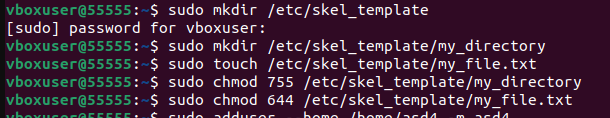


Рисунок 6. Создание шаблона скелета

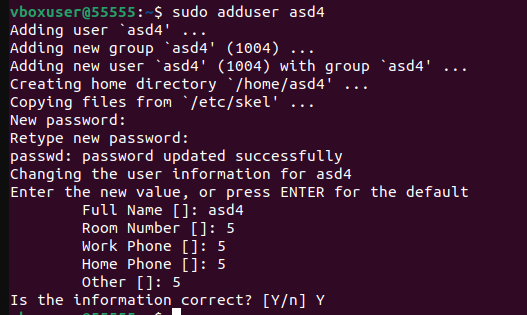


Рисунок 7. Создание пользователя с шаблоном скилета

**Задание 2**

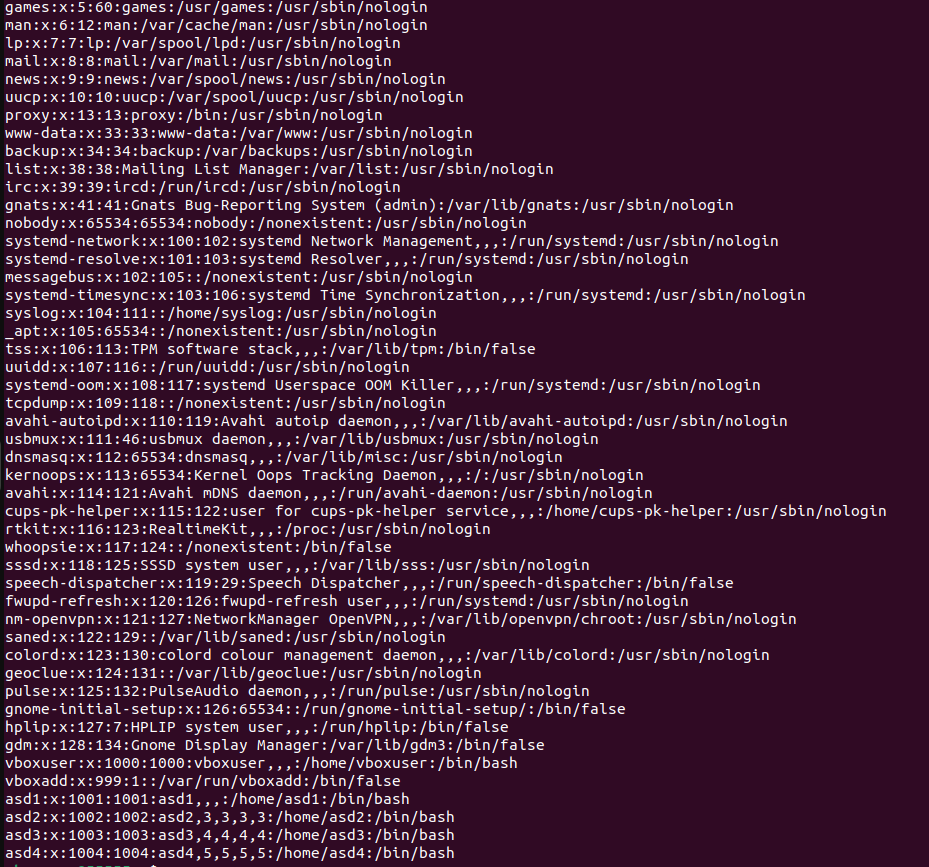


Рисунок 8. Просмотр содержимого файла /etc/passwd и атрибутов пользователей

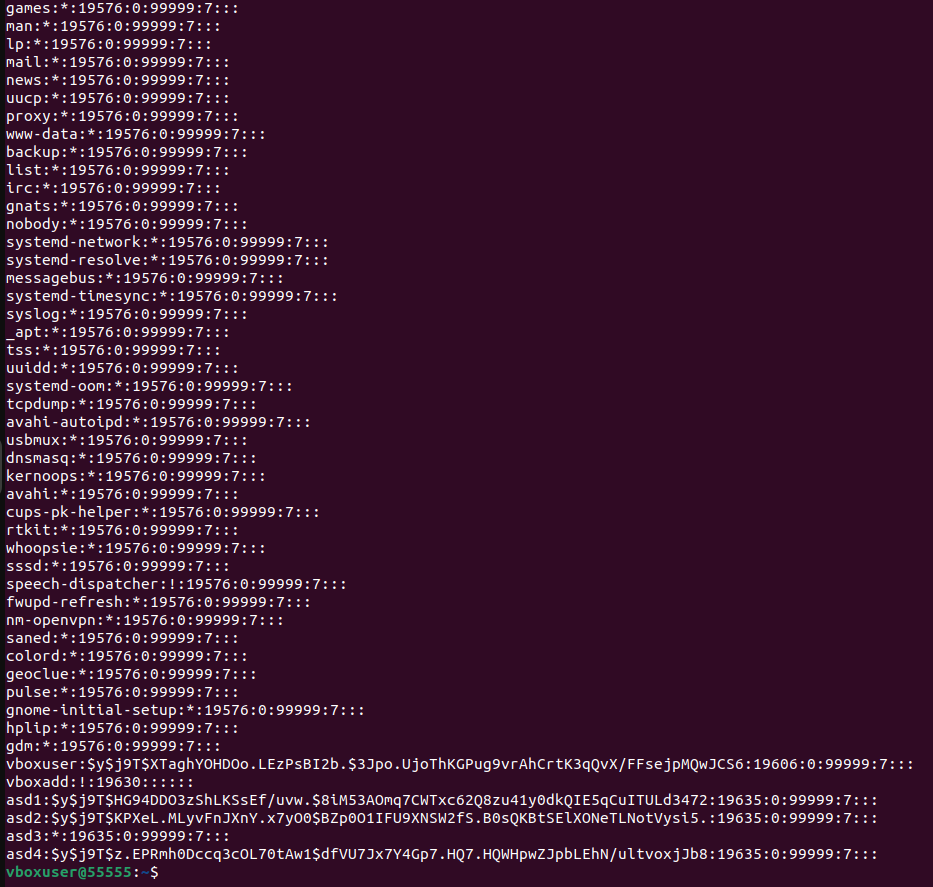


Рисунок 9. Просмотр содержимого файла /etc/shadow и атрибутов паролей



Рисунок 10. Установка минимальный возраста пароля в 1 сутки



Рисунок 11. Установка максимальный возраста пароля в 90 суток



Рисунок 12. Установка периода предупреждения пароля (количество дней, до истечения срока действия пароля, когда пользователь будет уведомлен)



Рисунок 13. Установка периода бездействия пароля (количество дней, когда пароль может быть неактивен)



Рисунок 14. Установка даты истечения срока действия аккаунта (пользователь не сможет войти после этой даты)

**Задание 3**



Рисунок 15. Создание пользователя с правами администратора

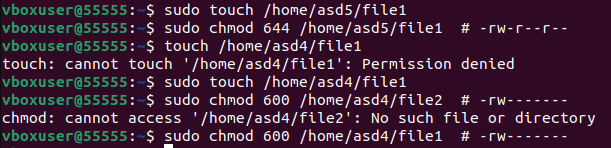


Рисунок 16. Создание файлов с разными правами доступа с помощью команды touch и измените их права с помощью chmod



Рисунок 17. Создание общей группы пользователей



Рисунок 18. Перевод пользователя в группу shadow



Рисунок 19. Создание директорий с файлами

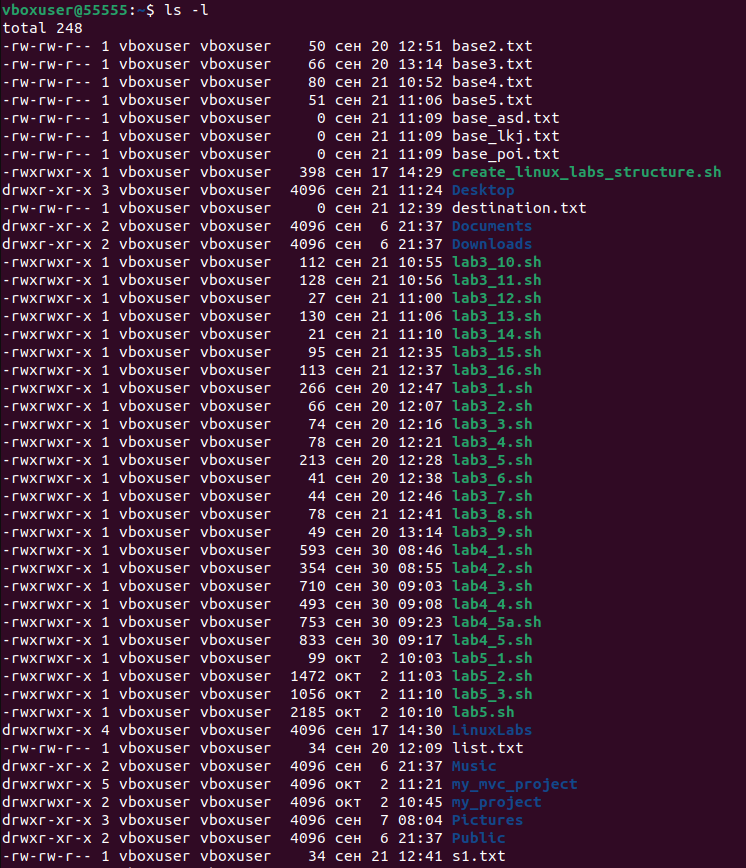


Рисунок 20. Просмотр текущих прав доступа к файлам и каталогам



Рисунок 21. Ограничение доступа к каталогу только для его группы



Рисунок 22. Ограничение доступа к файлам только владельцам



Рисунок 23. Установка прав только для чтения всем пользователям



Рисунок 24. Лишение пользователей в группе shadow права исполнения

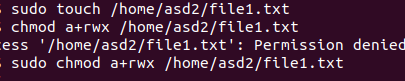


Рисунок 25. Назначения прав на чтение, запись и исполнение всем пользователям



Рисунок 26. Удаление пользователя из группы shadow

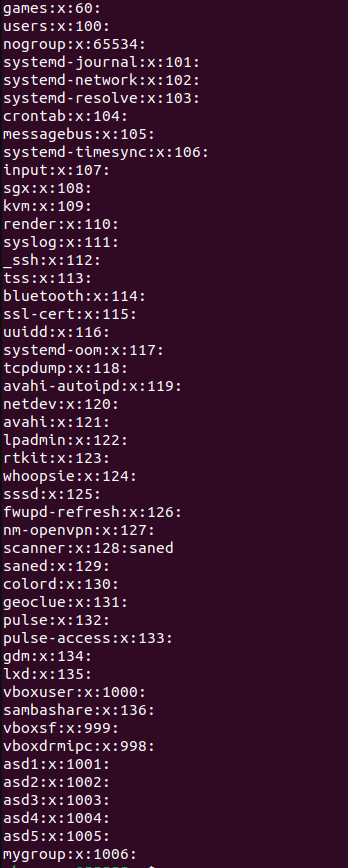


Рисунок 27. Просмотр списка групп используя команду cat /etc/group

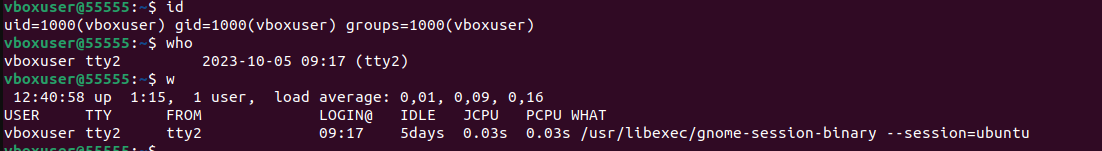


Рисунок 28. Получение идентификаторов пользователей и состояния активных пользователей: получения идентификаторов пользователей использую команду id. для просмотра состояния активных пользователей, использую команду who или w



Рисунок 29. Установить липкий бит на файле



Рисунок 30. Удаление файлов из другого аккаунта

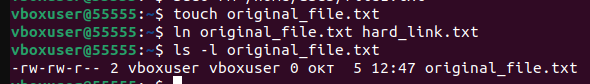


Рисунок 31. Создается жесткая ссылка с именем hard\_link.txt на оригинальный файл original\_file.txt. Чтобы узнать, сколько жестких ссылок существует на файл, вы можете использовать команду ls -l. Первое число в выводе команды ls -l представляет собой количество жестких ссылок на файл



Рисунок 32. Изменения владельца и группы жесткой ссылки

asd2 - это новый владелец, которому присваиваем жесткую ссылку.

1010 - это новая группа, которой надо присвоить жесткую ссылку.

hardlink.txt - это имя жесткой ссылки, которую хотим изменить.

Изменение атрибутов доступа файлов и каталогов в Linux выполняется с помощью команды chmod. Эта команда позволяет устанавливать различные права на чтение, запись и выполнение для владельца, группы и остальных пользователей.

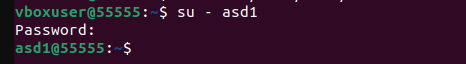


Рисунок 33. Переключение пользователя

**Контрольные вопросы**

**Опишите отличия команд su и sudo.**

Команды su и sudo в Linux предоставляют разные способы выполнения команд от имени других пользователей, но существуют существенные отличия между ними:

su (Switch User):

su позволяет вам переключиться на другую учетную запись (обычно суперпользователя, root) и работать от ее имени.

Вы должны знать пароль учетной записи, на которую вы переключаетесь.

После входа в учетную запись с помощью su, вы находитесь в ее среде, и все команды выполняются от ее имени.

Команда su часто используется для выполнения команд с правами суперпользователя.

sudo (Superuser Do):

sudo позволяет выполнять одиночные команды с правами суперпользователя (root) или другого пользователя с правами администратора, без необходимости переключения на его учетную запись.

Пользователь, запускающий sudo, должен быть включен в специальную группу (обычно "sudoers") и иметь право на выполнение операций суперпользователя.

Пользователь вводит свой собственный пароль, а не пароль суперпользователя.

Все команды, выполненные с помощью sudo, записываются и аудитятся системой, что обеспечивает большую безопасность.