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”***

Вариант 1

Выполнил**:** студент группы 10701321 Беть Е.А.

Приняла**:** пр. Давыденко Н.В.

Минск 2023

# Лабораторная работа №1a.

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.

## 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»

***Небольшой совет***. Имена пользователей пишите с маленьких букв, это поможет ускорить вашу дальнейшую работу. Разделителем в имени используйте нижнее подчеркивание «\_», тире «-» или заглавную букву. Например, serhey\_stankevich, sergei-stankewich, sergStankevich.

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

***При создании пользователей***, которые нужны для экспериментов, назначайте им одинаковые пароли (это тоже эксперимент), такие чтобы не забыть. Например, «123»

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 двух пользователей с одинаковыми простыми паролями. Создайте скелет и пользователя с шаблоном скелета 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:

* Одного из пользователей перевести в группу Shadow
* Создать у каждого пользователя директорию с 2 файлами
* Посмотреть текущие права доступа к файлам для всех пользователей
* Каталог пользователя в группе Shadow сделать доступным только в своей группе
* Файлы второго пользователя сделать доступными только владельцам
* Под админом назначить всем созданным файлам права только для чтения для всех пользователей
* Пользователем в группе Shadow лишить всех остальных пользователей права исполнять его файлы
* Под админом назначить всем пользователям все права
* 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.

### Скриншоты результатов

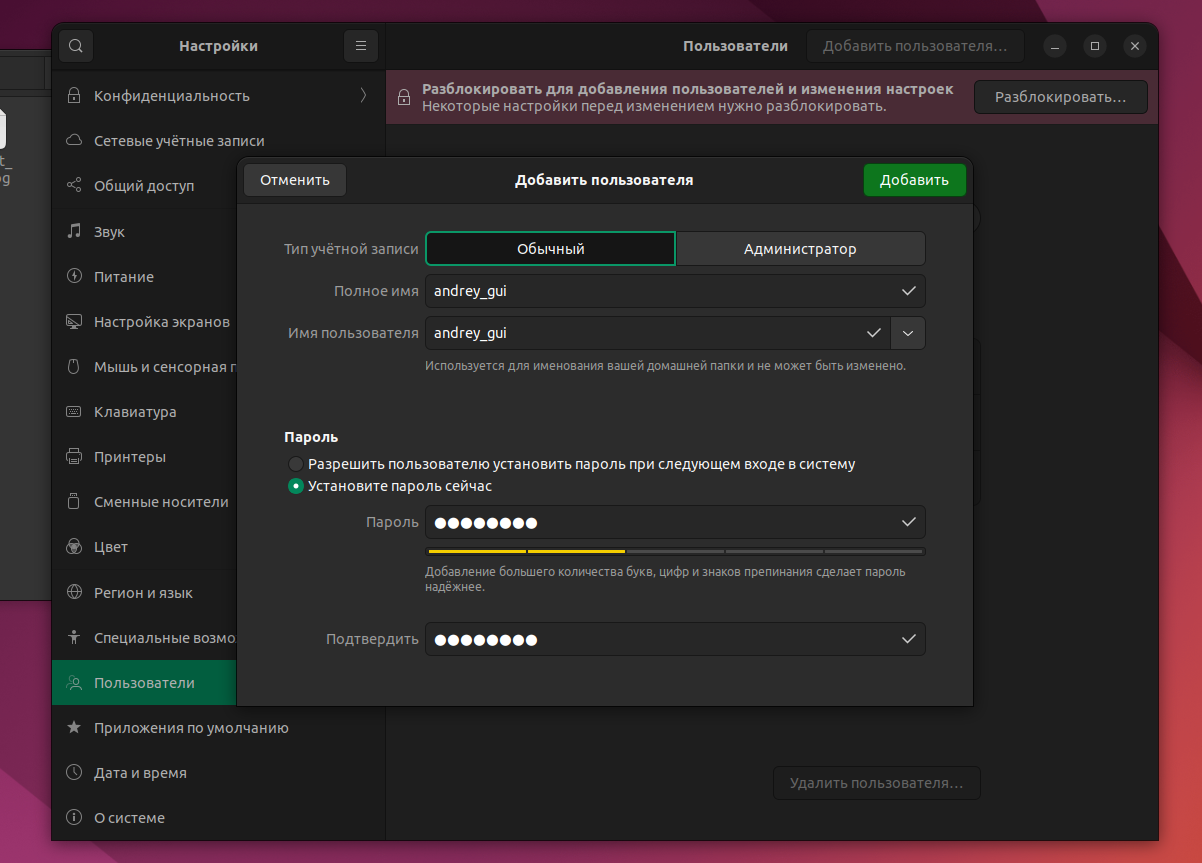


Рисунок 1 – задание 1 (создание пользователя с помощью GUI)

Каждая строка файла passwd является записью конкретного пользователя и имеет формат – семь полей (атрибутов), разделенных двоеточиями.

***NAME:PASSWD-ENCOD:UID:GID:COMMENTS:HOME-DIR:SHELl***

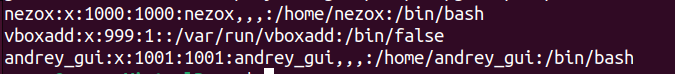


Рисунок 2 – задание 1



Рисунок 3 – задание 1

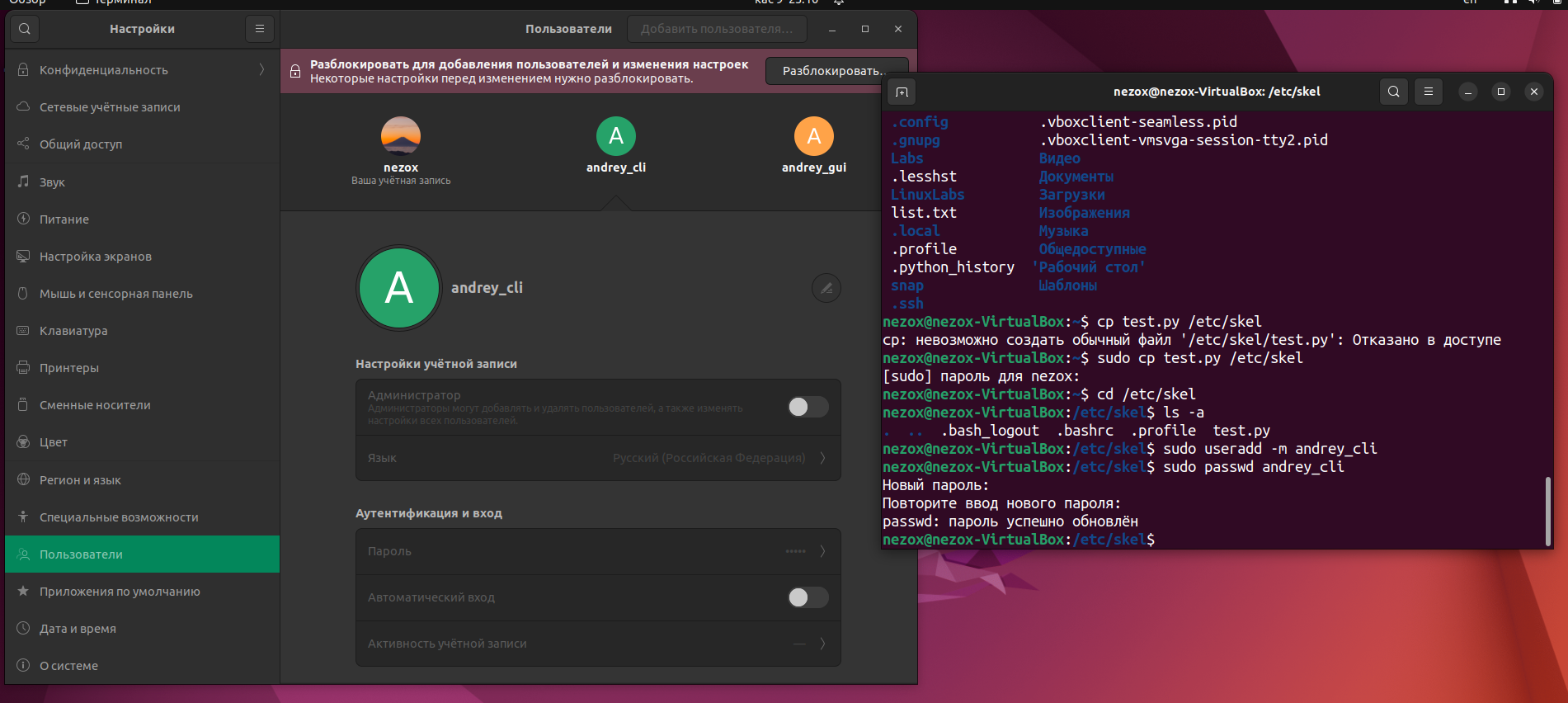
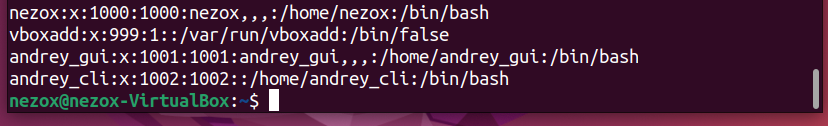


Рисунок 4 – задание 1

****

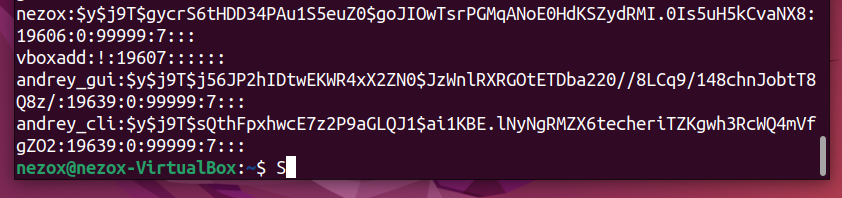
****

Рисунок 5 – задание 2 (содержимое файлов /etc/passwd, /etc/shadow)

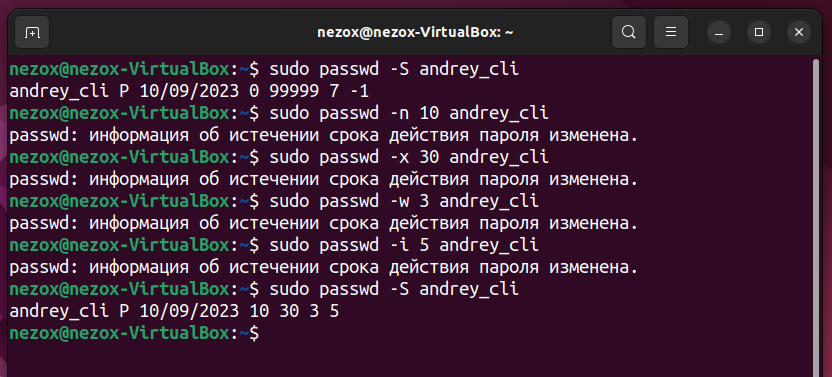


Рисунок 6 – задание 2 (Изменение периодов изменения паролей для пользователя andrey\_cli)

1. Имя пользователя
2. Это поле показывает одно из значений: Р – пароль установлен, L – пользователь заблокирован, NP – нет пароля
3. Дата последнего изменения пароля
4. Минимальное время до смены пароля (10 дней)
5. Максимальное время действия пароля (30 дней)
6. За сколько дней надо предупреждать об истечении срока действия пароля (3 дня)
7. Через сколько дней пароль надо деактивировать (5 дней)

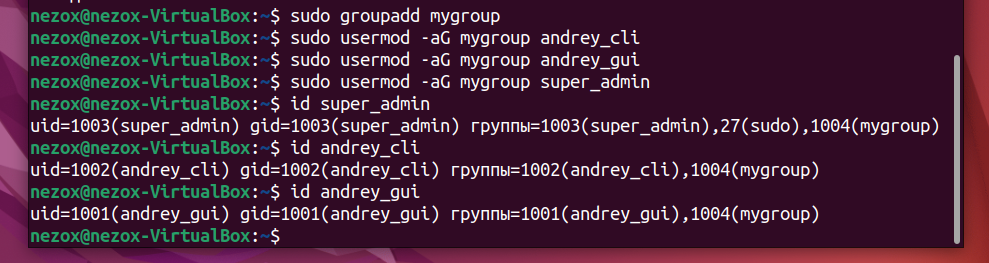


Рисунок 7 – задание 3 (Создание группы и добавление туда пользователей)

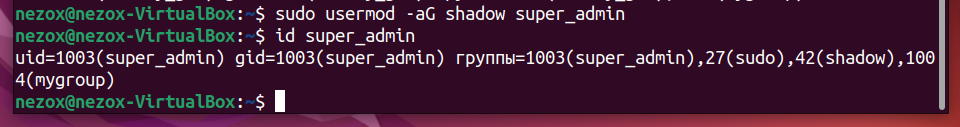


Рисунок 8 – задание 3 (перевод пользователя в группу shadow)

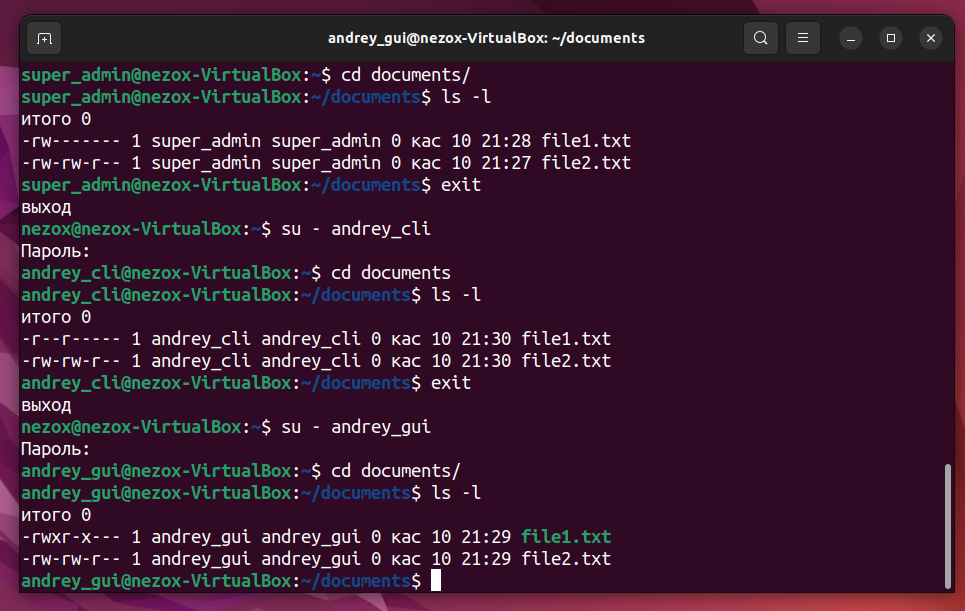


Рисунок 9 – задание 3 (создание директории с 2 файлами и просмотр текущих прав доступа к файлам для всех пользователей)

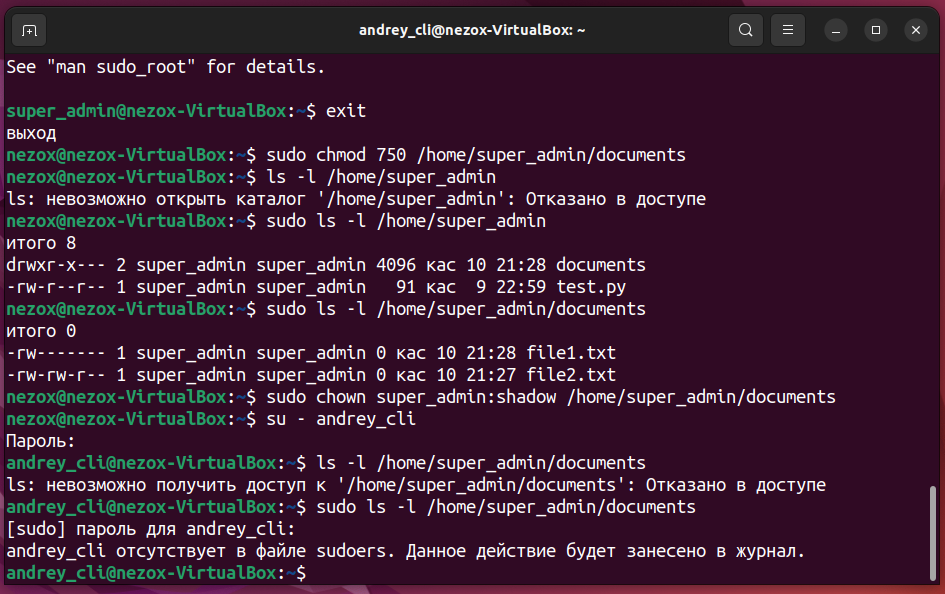


Рисунок 10 – задание 3 (каталог пользователя в группе Shadow сделан доступным только в своей группе)

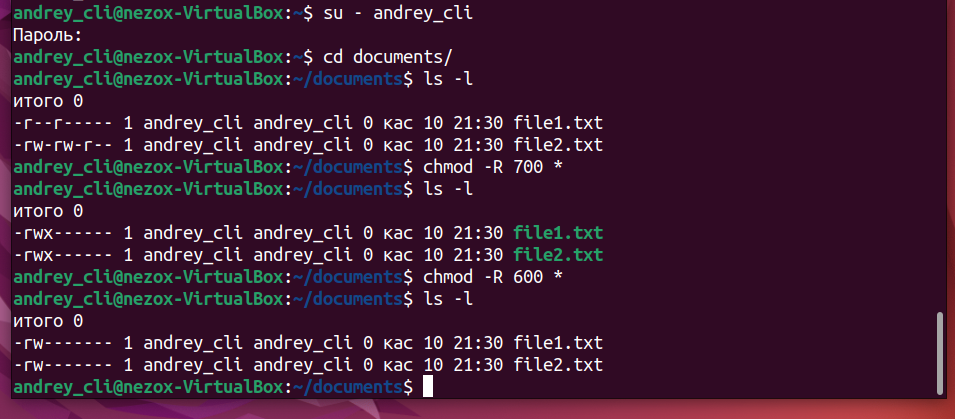


Рисунок 11 – задание 3 (доступ к файлам другого пользователя разрешен только владельцам)

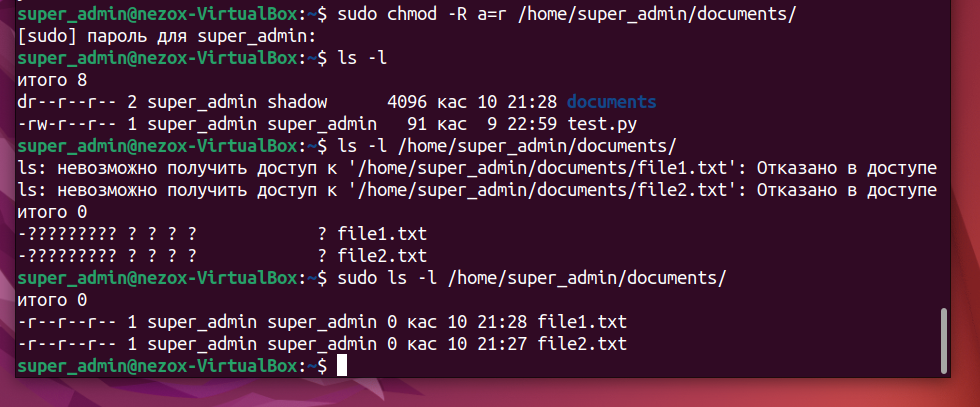


Рисунок 12 – задание 3 (назначение всем созданным файлам права только для чтения для всех пользователей)

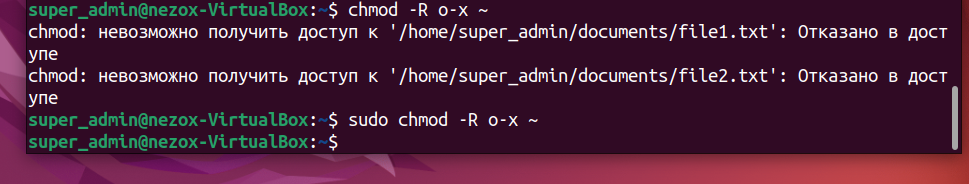


Рисунок 13 – задание 3 (лишение всех остальных пользователей права исполнять файлы пользователя из группы shadow)

Здесь:

* -R указывает на рекурсивное применение команды ко всем файлам и подкаталогам внутри вашего домашнего каталога (~).
* o-x устанавливает права "без выполнения" для остальных пользователей (не владельца файла и не из группы владельца).

Эта команда уберет права на выполнение у всех файлов в вашем домашнем каталоге для остальных пользователей, не нарушая права доступа для вас и членов группы.

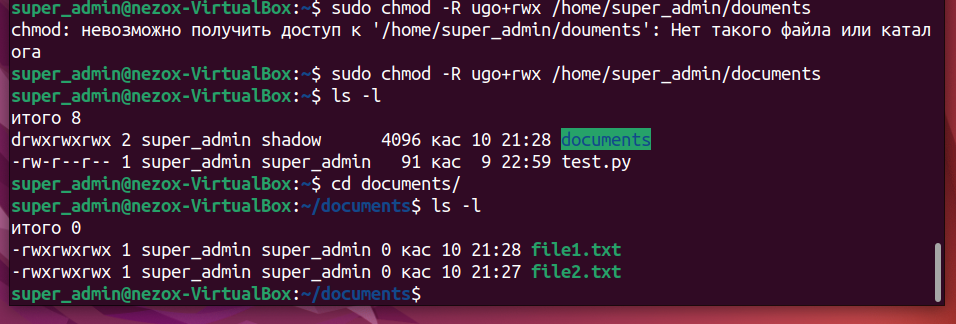


Рисунок 14 – задание 3 (назначение всем пользователям всех прав)

Здесь:

* -R указывает на рекурсивное применение команды ко всем файлам и подкаталогам внутри указанной директории.
* ugo+rwx устанавливает права для пользователя (u), группы (g) и остальных (o) на чтение (r), запись (w) и выполнение (x).

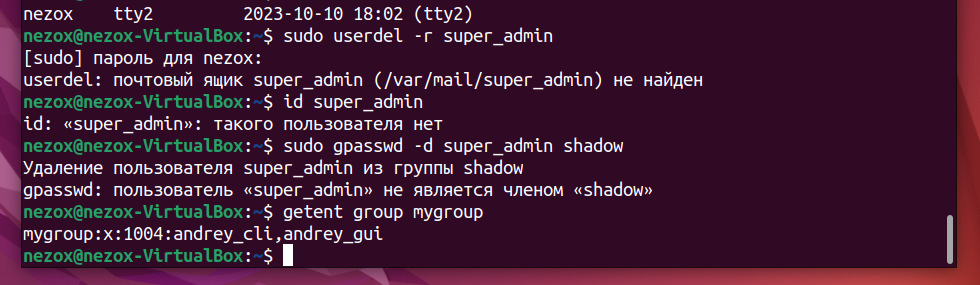


Рисунок 15 – задание 3 (удаление пользователя, находящегося в группе shadow)

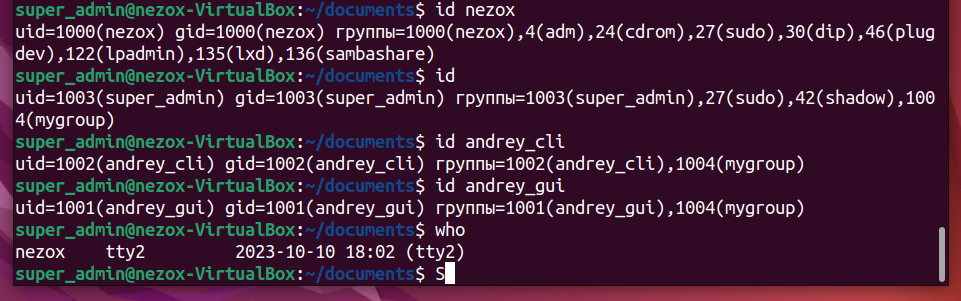


Рисунок 16 – задание 3 (идентификаторы пользователей и состояние активных пользователей системы)

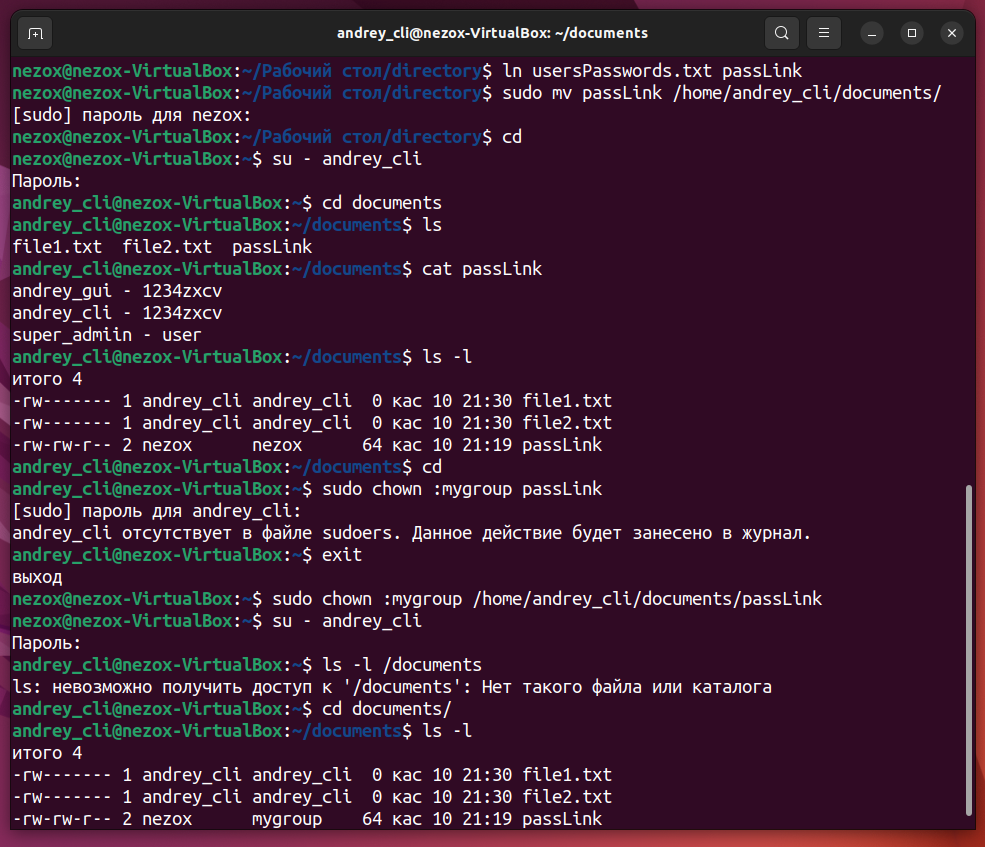


Рисунок 17 – задание 3 (создание и манипуляции с жесткой ссылкой)

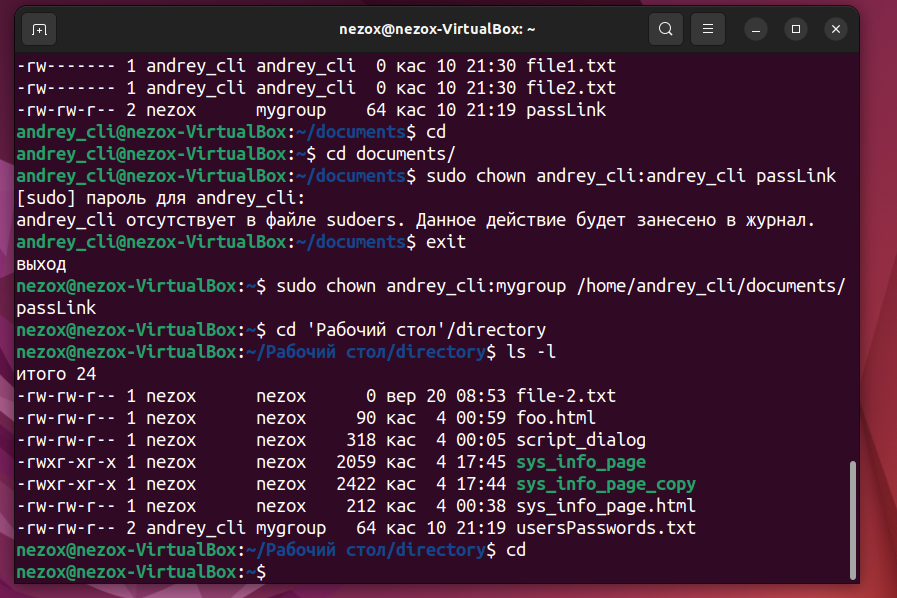


Рисунок 18 – задание 3 (изменение владельца и группы жесткой ссылки)

## Контрольные вопросы

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

Ответ: Для каждой из перечисленных категорий (владелец, группа, другие) устанавливаются индивидуальные права доступа исходя из трех критериев:

1. Право на чтение (r – read)

2. Право на запись (w – write)

3. Право на выполнение (x – execute)

## Вывод: закрепили на практике основы администрирования системы Linux, изучили атрибуты файлов и права доступа к ним, освоили работу с файлами и каталогами.