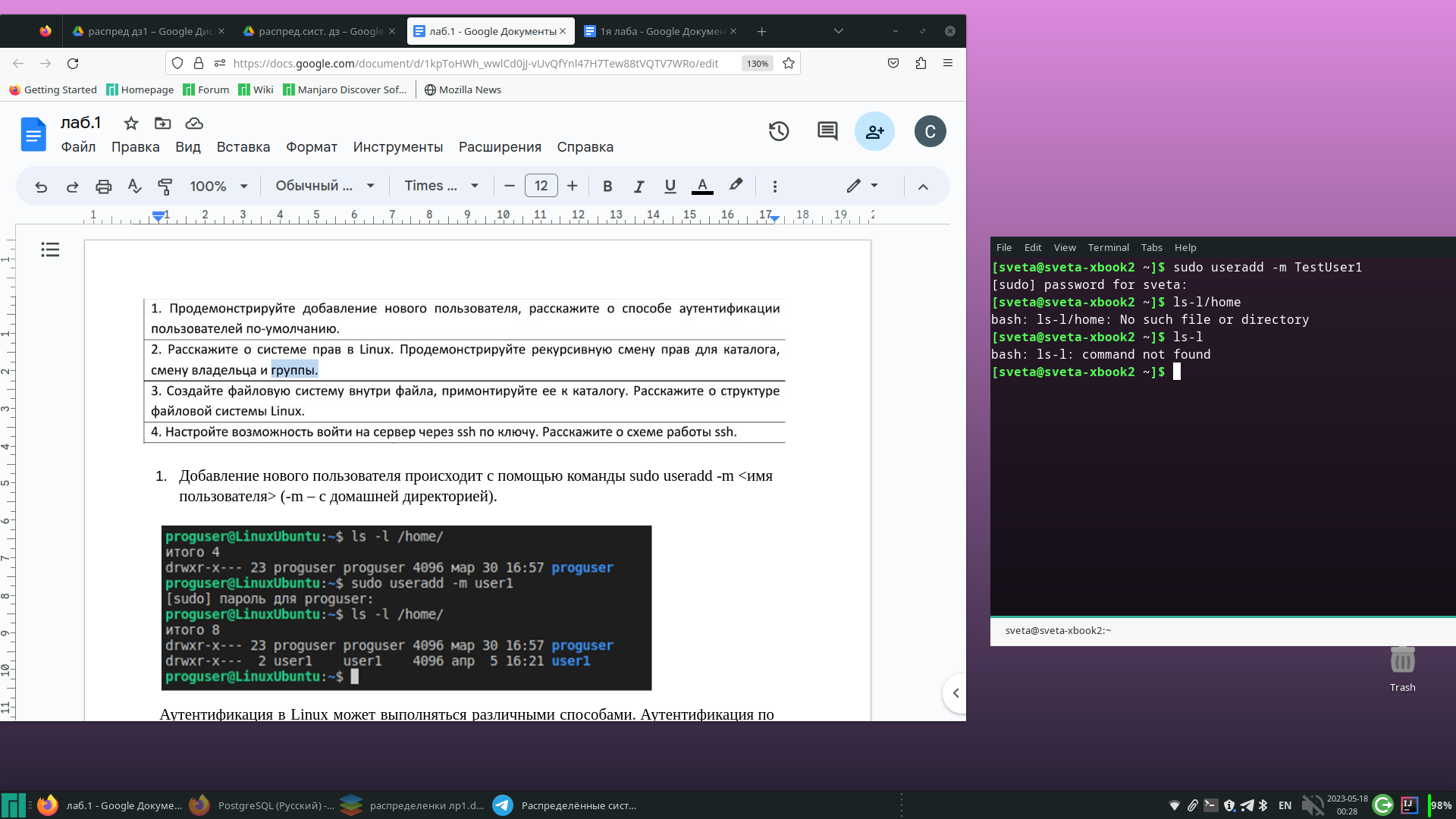


1. Добавление нового пользователя происходит с помощью команды sudo useradd -m <имя пользователя>. Добавление пользователя TestUser1.



В Linux наиболее распространенным методом аутентификации пользователей является метод, основанный на использовании многоразового пароля. Пользователи вводят свой логин и пароль для входа в систему.

Однако, помимо этого, существуют и другие методы аутентификации, такие как аутентификация на основе ключа. При использовании аутентификации на основе ключа для аутентификации пользователей потребуется использовать фразу-пропуск и файл личного ключа. Для реализации процедур аутентификации в Linux используется система PAM (Pluggable Authentication Modules). Система PAM берет на себя работу по реализации процедур аутентификации.

Для того, чтобы задать новому пользователю пароль, используется команда sudo passwd <имя пользователя>.

1. Права доступа к файлам в Linux определяются для трех категорий пользователей: владельца файла, группы владельца и всех остальных пользователей. Каждая категория имеет свои права на чтение, запись и выполнение файлов. Права доступа к файлам в Linux можно изменять с помощью команды chmod. В системе Linux обычно только два человека могут изменять права доступа к файлу или каталогу: владелец файла или каталога и пользователь root - суперпользователь.

Права доступа подразделяются на три типа:

- чтение (read);

- запись (write);

- выполнение (execute).

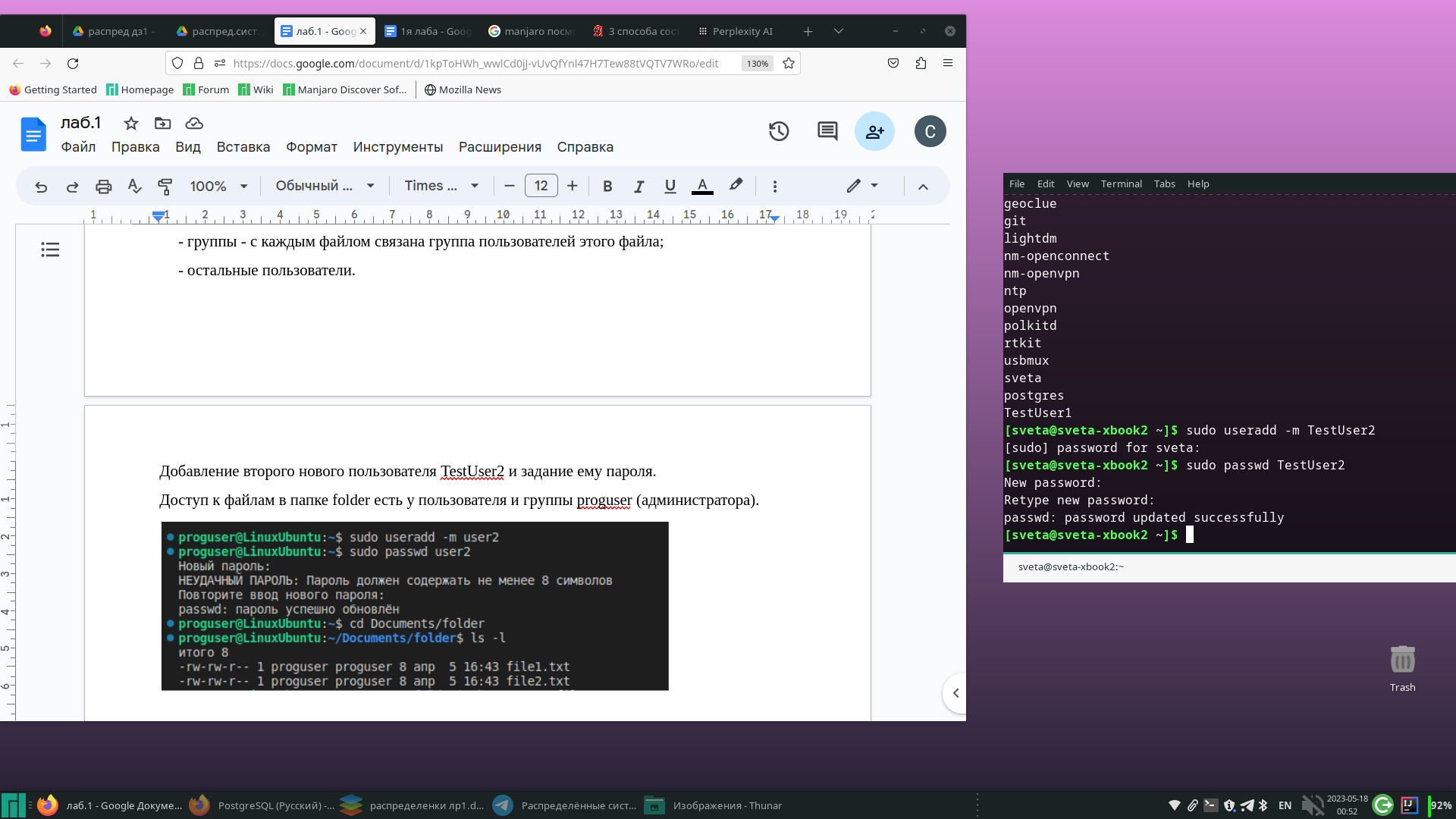
Эти типы прав доступа могут быть предоставлены для трех классов пользователей:

- владельцы - у каждого файла есть один владелец;

- группы - с каждым файлом связана группа пользователей этого файла;

- остальные пользователи.

Добавление второго нового пользователя TestUser2 и задание ему пароля.

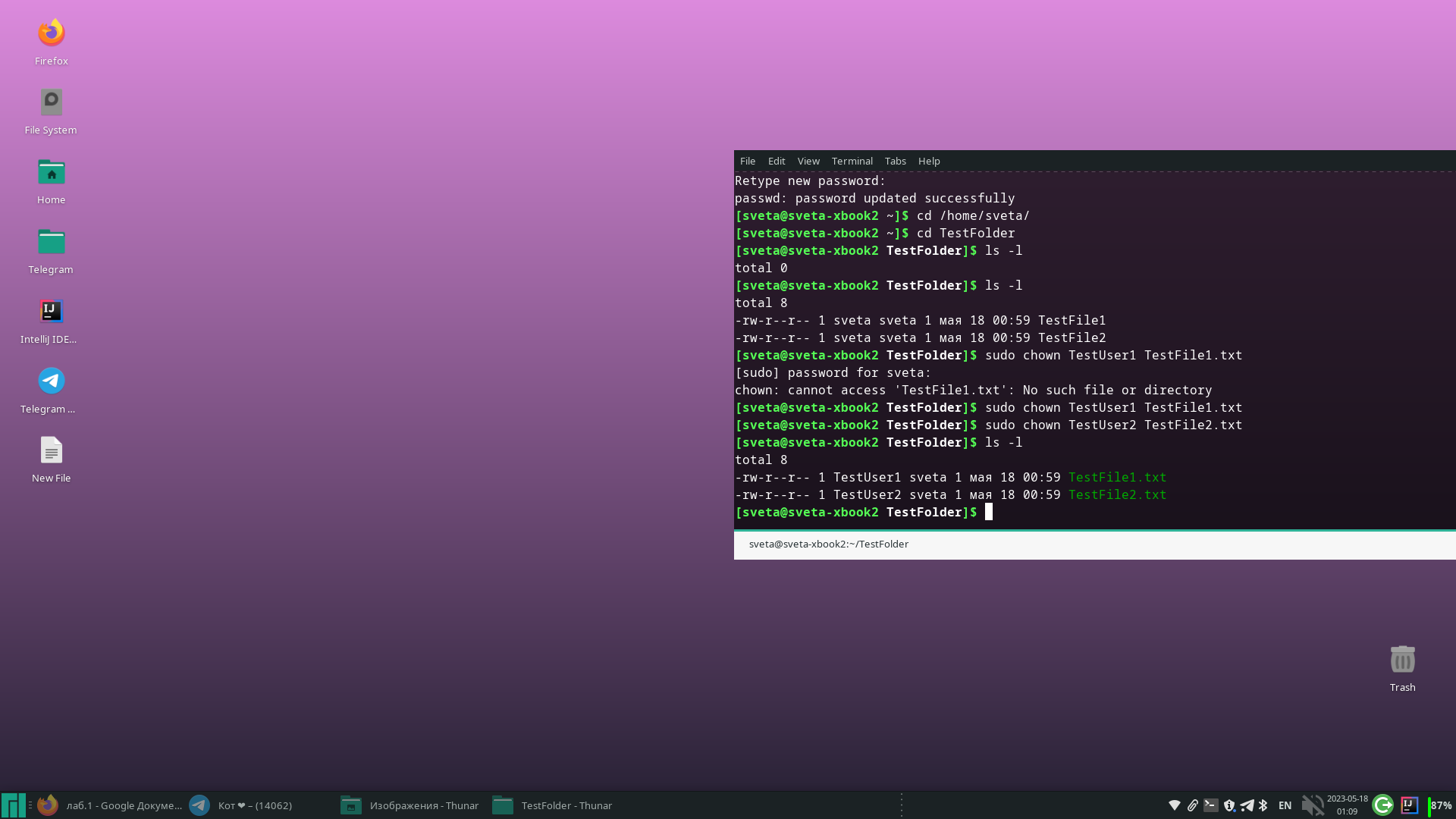


Доступ к файлам в папке TestFolder есть у пользователя и группы sveta (администратора).



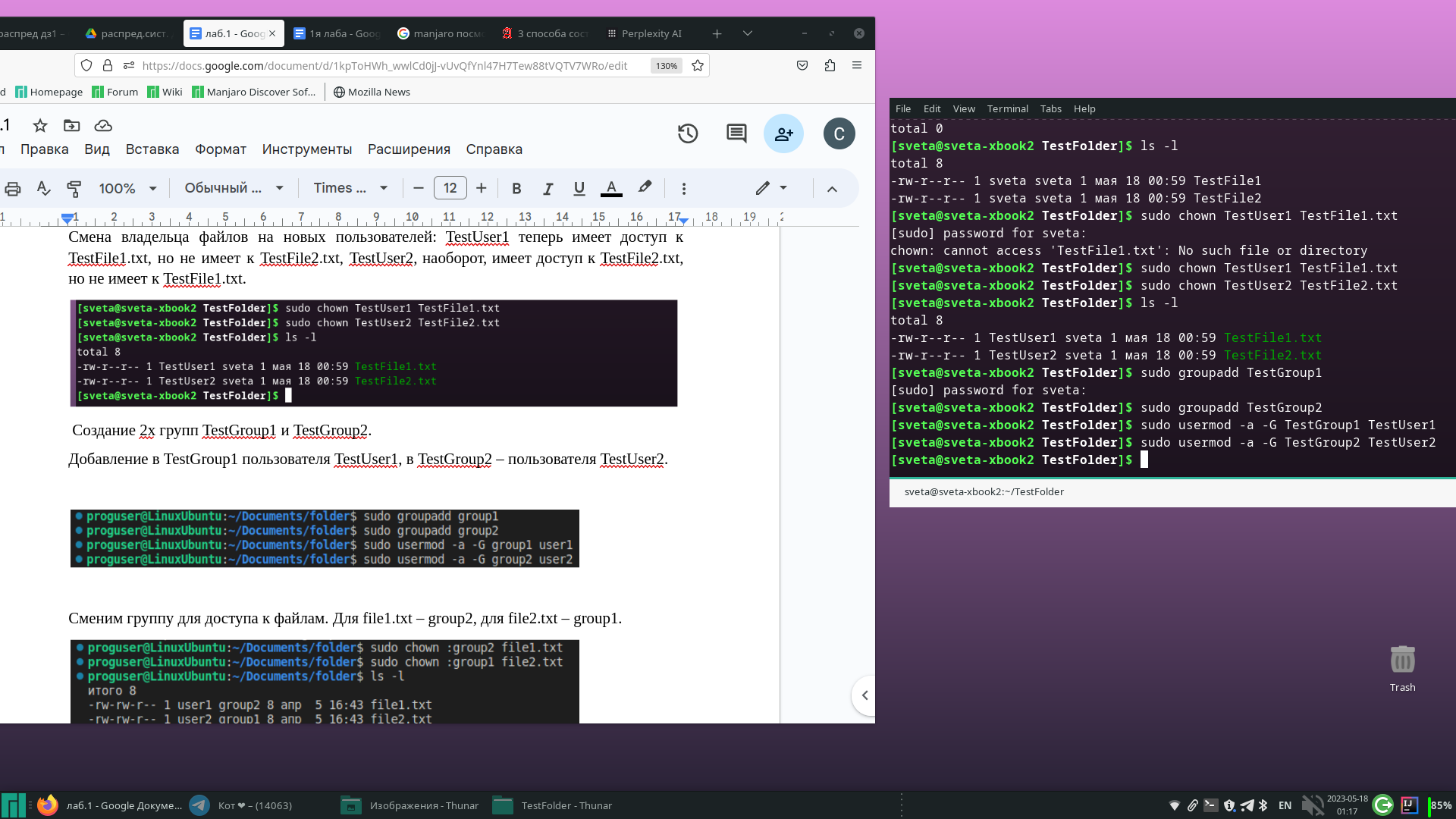
Смена прав доступа производится с помощью команды chown <имя пользователя>:<имя группы> <имя файла>.

Смена владельца файлов на новых пользователей: TestUser1 теперь имеет доступ к TestFile1.txt, но не имеет к TestFile2.txt, TestUser2, наоборот, имеет доступ к TestFile2.txt, но не имеет к TestFile1.txt.

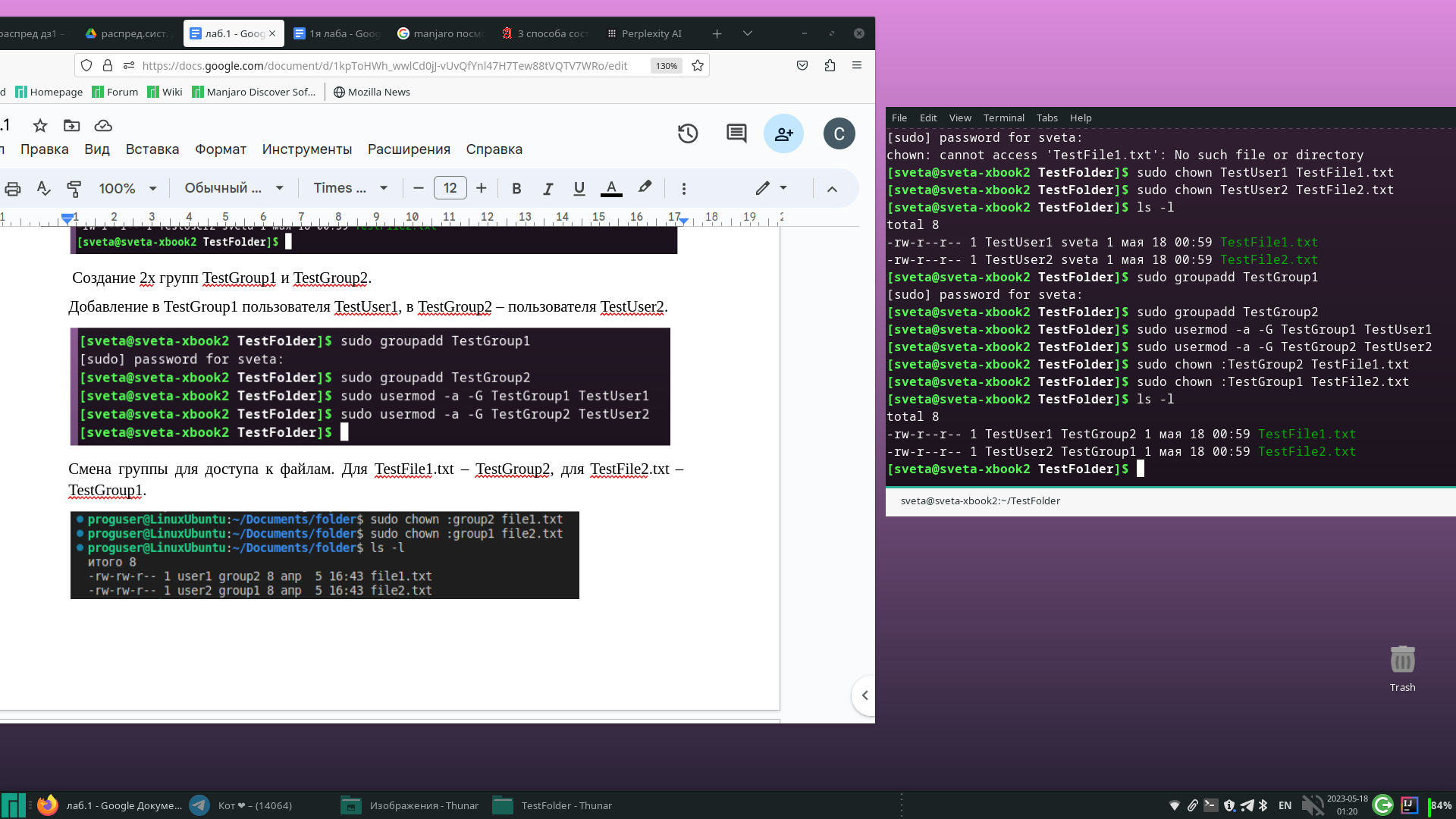


Создание 2х групп TestGroup1 и TestGroup2.

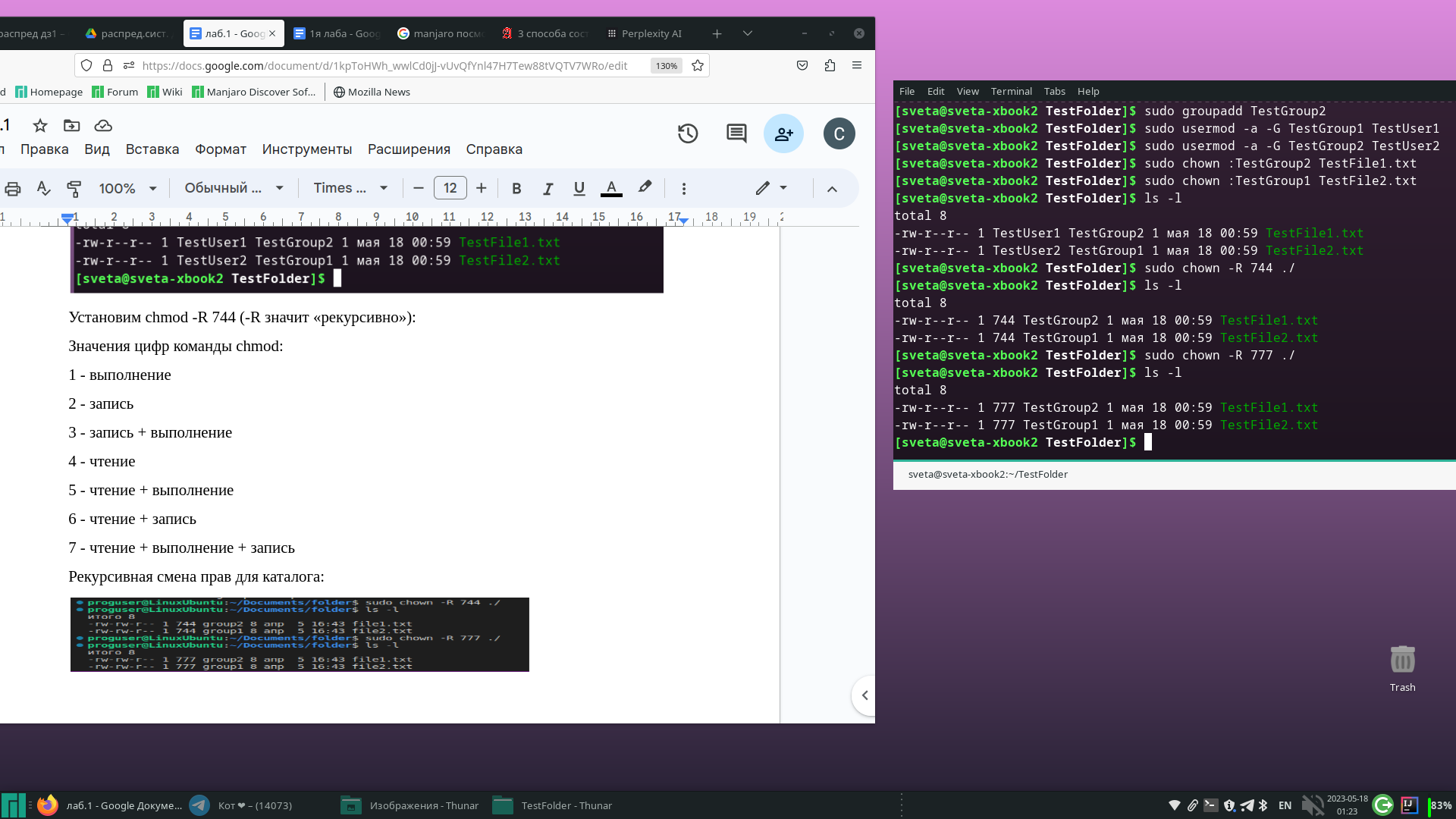
Добавление в TestGroup1 пользователя TestUser1, в TestGroup2 – пользователя TestUser2.



Смена группы для доступа к файлам. Для TestFile1.txt – TestGroup2, для TestFile2.txt – TestGroup1.



Рекурсивная смена прав для каталога:



Значения цифр команды chmod:

1 - выполнение

2 - запись

3 - запись + выполнение

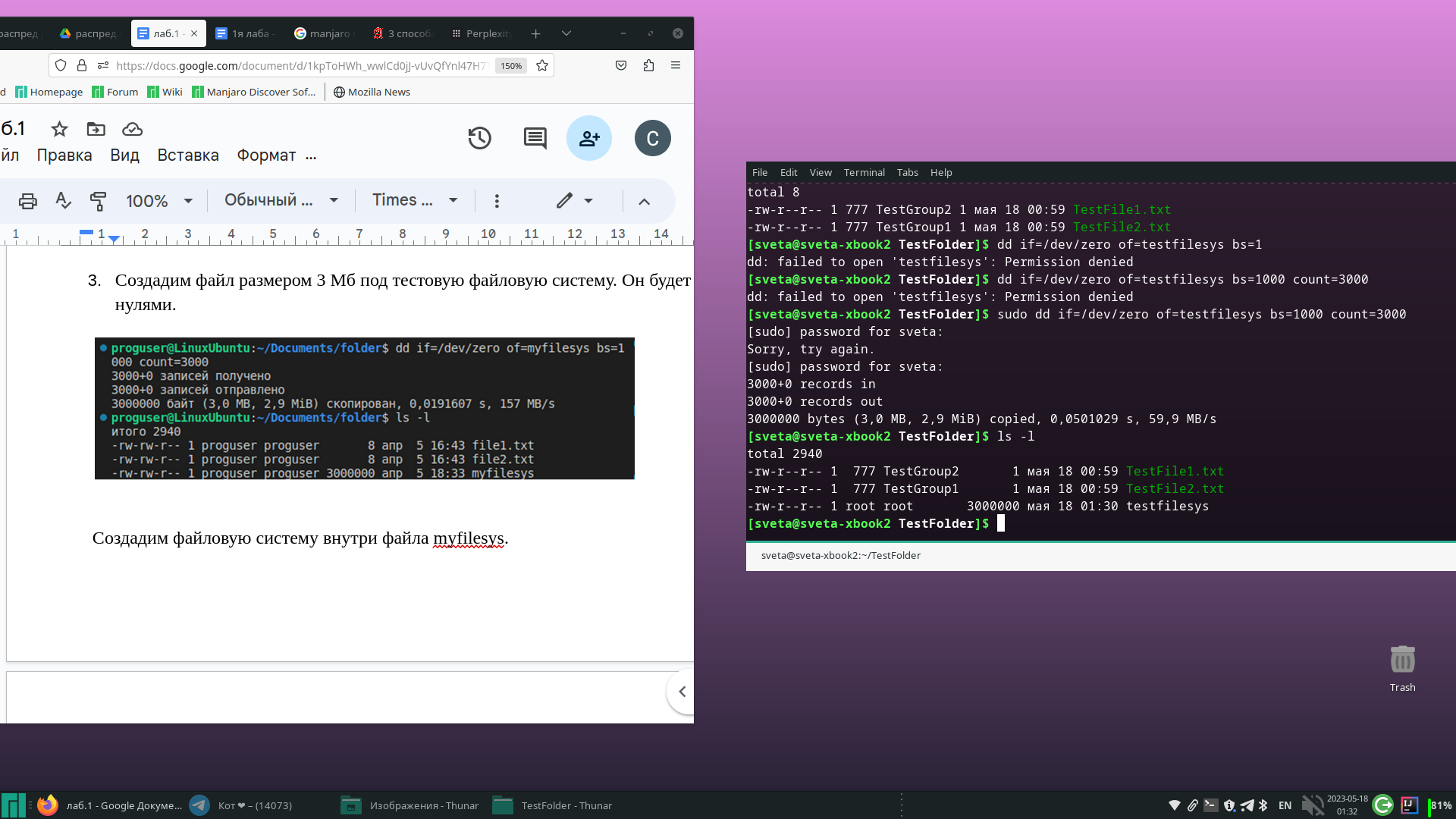
4 - чтение

5 - чтение + выполнение

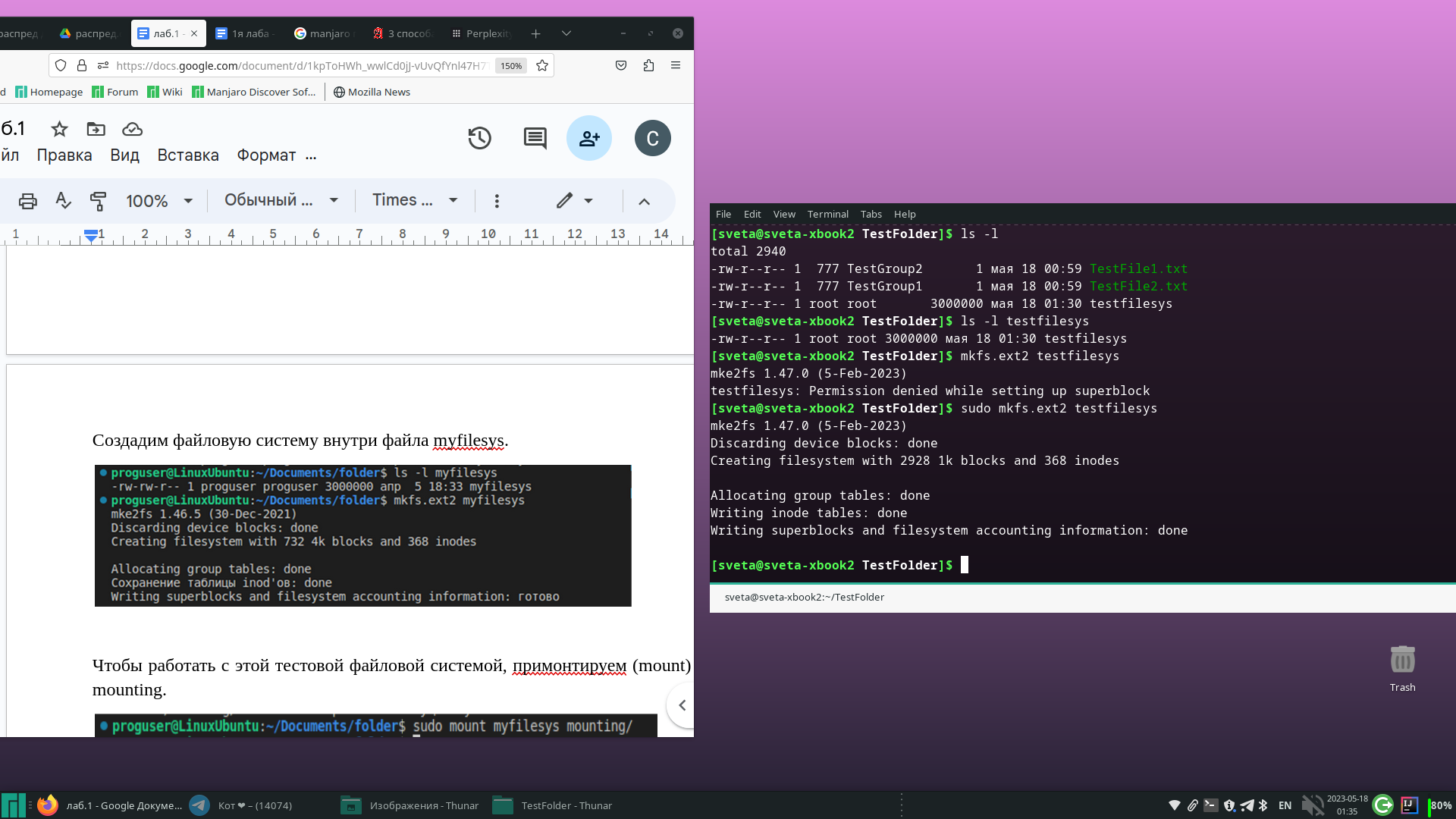
6 - чтение + запись

7 - чтение + выполнение + запись

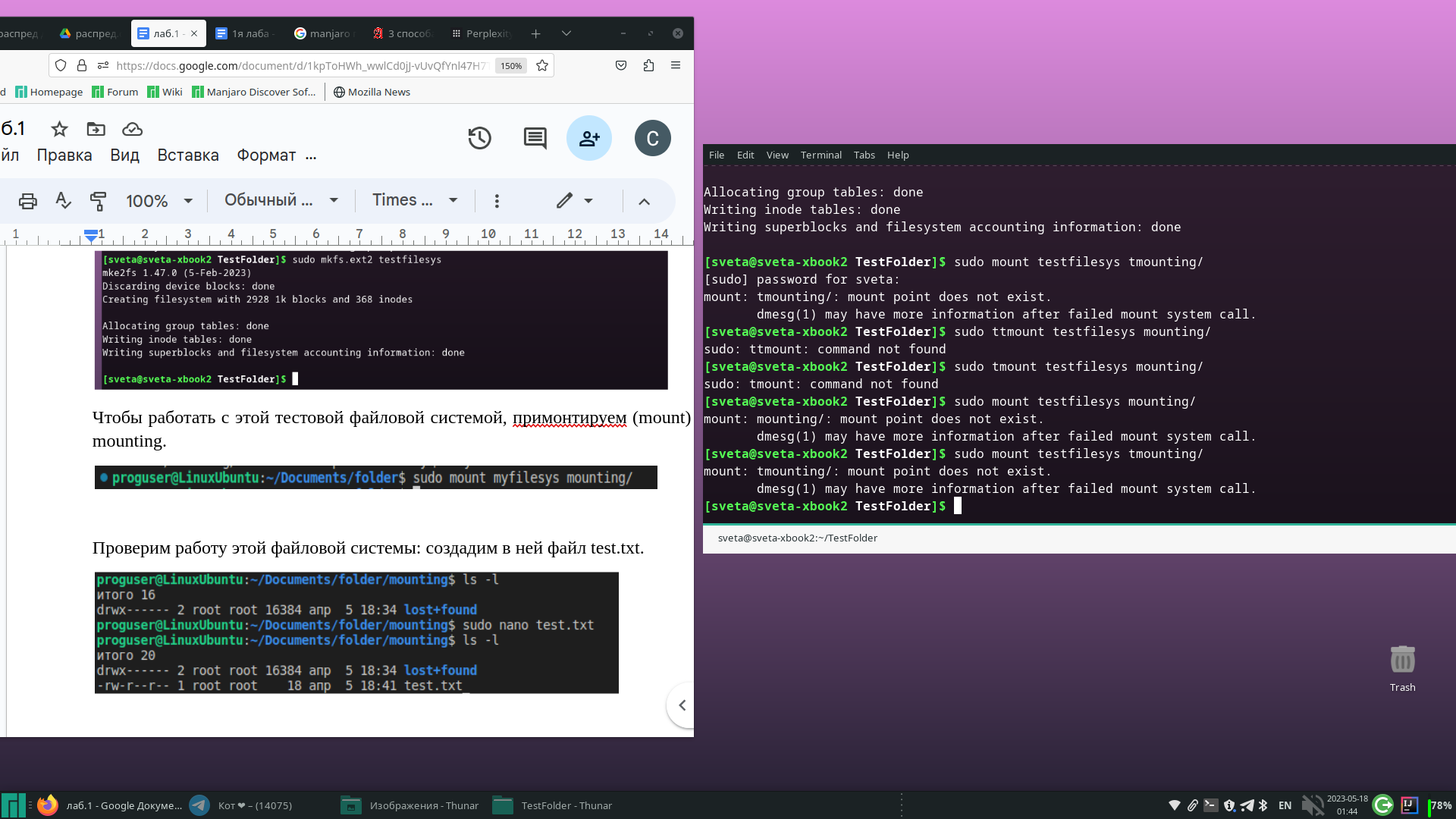
1. Создание файла размером 3 Мб под тестовую файловую систему. Он будет заполнен нулями.



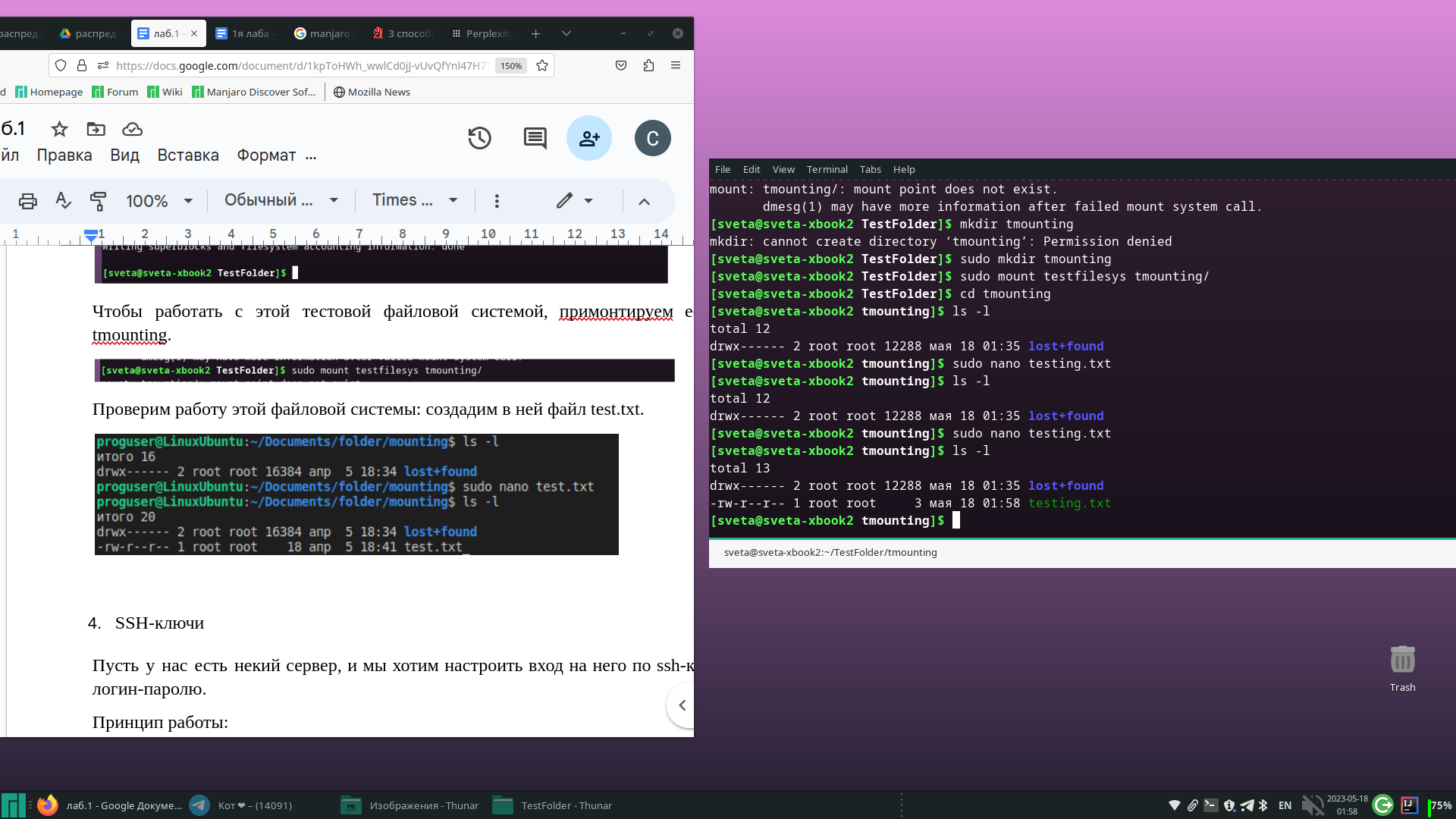
Создадим файловую систему внутри файла testfilesys.



Чтобы работать с этой тестовой файловой системой, примонтируем ее к каталогу tmounting.



Проверим работу этой файловой системы: создадим в ней файл testing.txt.



Структура файловой системы в Linux является иерархической и начинается с корневого каталога /. В Linux существует несколько типов файловых систем, таких как Ext, Ext2, Ext3, Ext4, JFS, XFS, Btrfs.

Файловая система Linux является древовидной (tree-shared) сложной структурой, состоящей из каталогов (директорий). Каталоги в Linux могут содержать другие каталоги и файлы.Корневой каталог содержит всю файловую иерархию.

Основные каталоги в Linux включают /bin, /boot, /dev, /etc, /home, /lib, /mnt, /opt, /proc, /root, /sbin, /tmp, /usr и /var. Каждый каталог имеет свою функциональность и содержит соответствующие файлы и подкаталоги.

1. SSH-ключи

SSH (Secure Shell) - это защищенный протокол удаленного соединения между компьютером-клиентом и сервером.

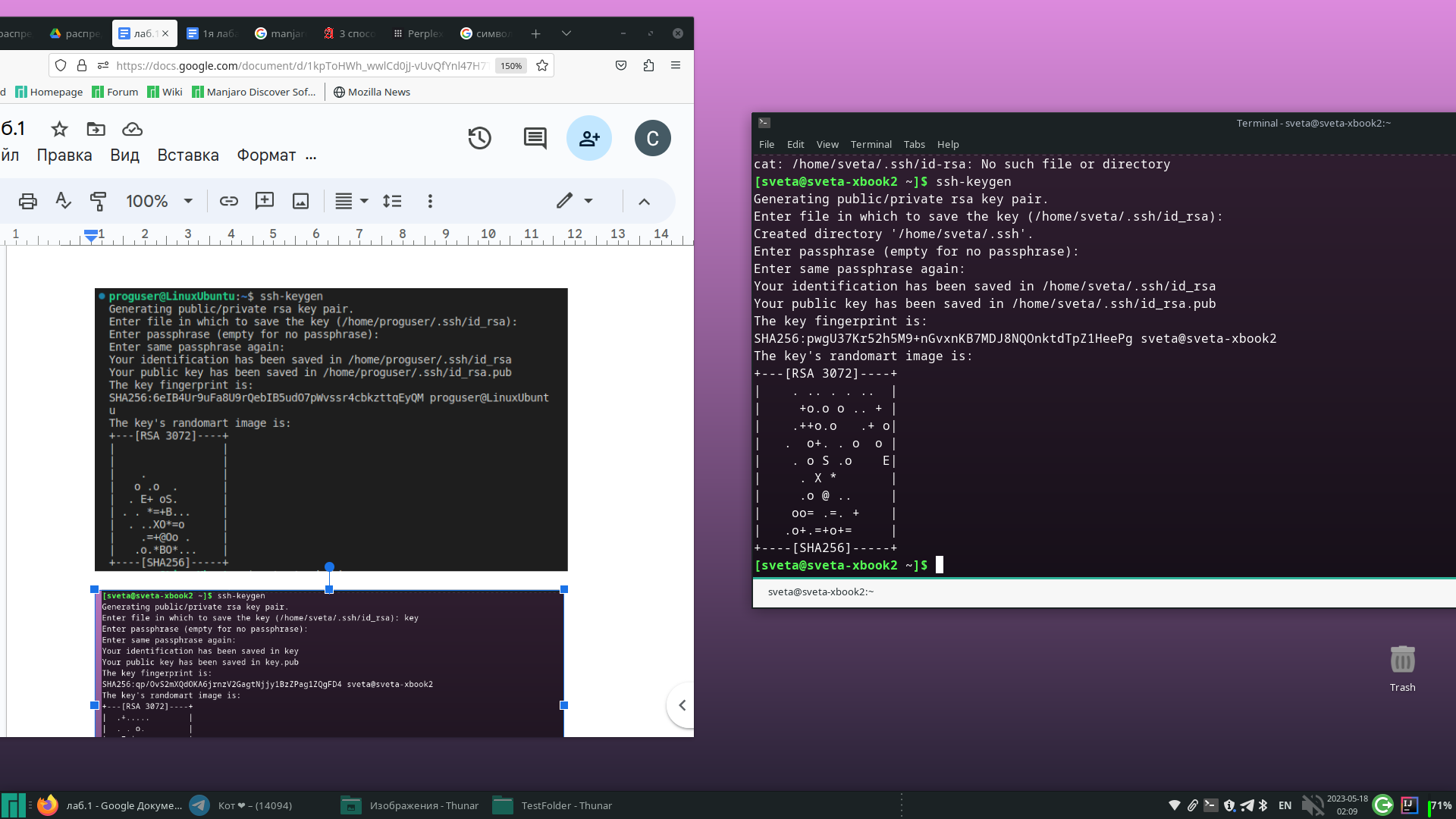
Принцип работы SSH заключается в использовании модели клиент-сервер для аутентификации двух удаленных систем и шифрования данных, передаваемых между ними.

Когда клиент подключается к серверу, он отправляет запрос на подключение и передает свой открытый ключ. Сервер проверяет ключ клиента и отправляет свой открытый ключ. Клиент использует открытый ключ сервера для шифрования сессионного ключа, который используется для шифрования данных, передаваемых между клиентом и сервером.

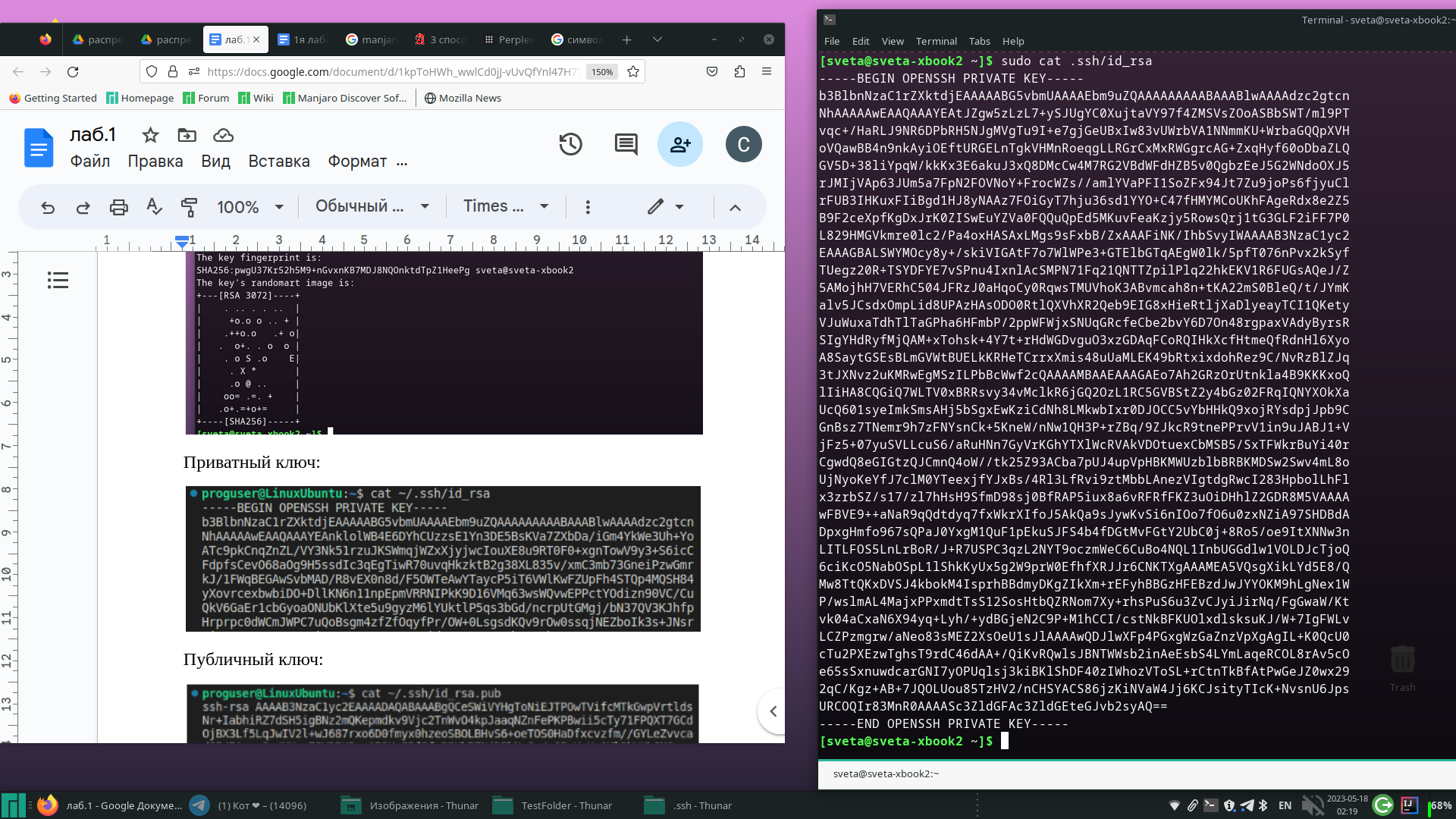
SSH использует криптографические методы для обеспечения безопасности передачи данных, включая шифрование, аутентификацию и цифровые подписи.

SSH также может использоваться для туннелирования других протоколов, таких как FTP и HTTP.

Генерация ключей:



Приватный ключ:



Публичный ключ:

