МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение   
высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

**ОТЧЕТ ПО ПРАКТИЧЕСКОМУ ЗАДАНИЮ №16**

**«Системы виртуализации в среде ОС GNU/ Linux. Наблюдение и аудит в ОС GNU/ Linux.»**

Практическая работа

по дисциплине «Системное программное обеспечение»

студента 3 курса группы ИВТ-б-о-222(1)

Гоголева Виктора Григорьевича

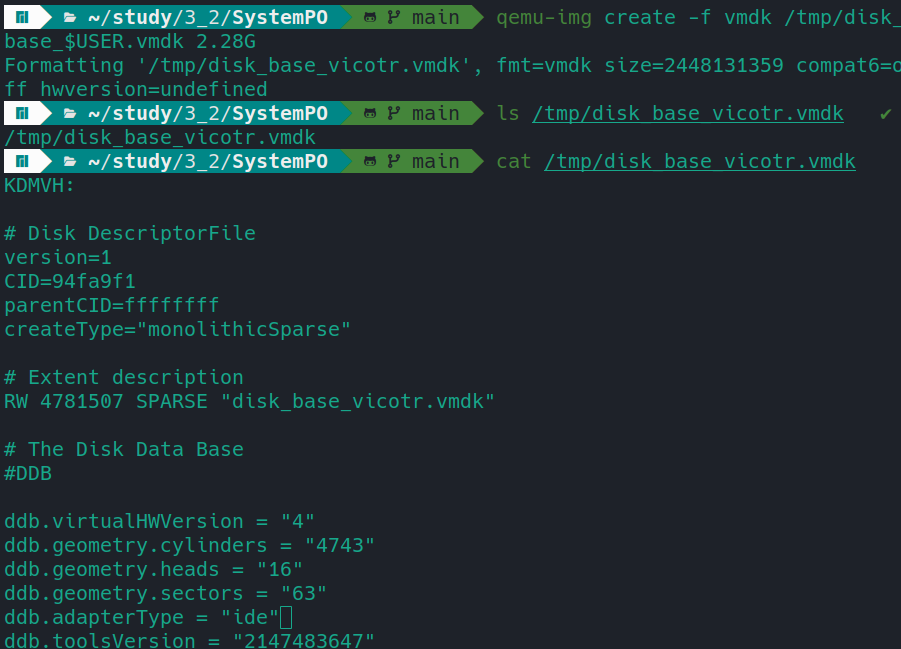
09.03.01 «Направление подготовки»

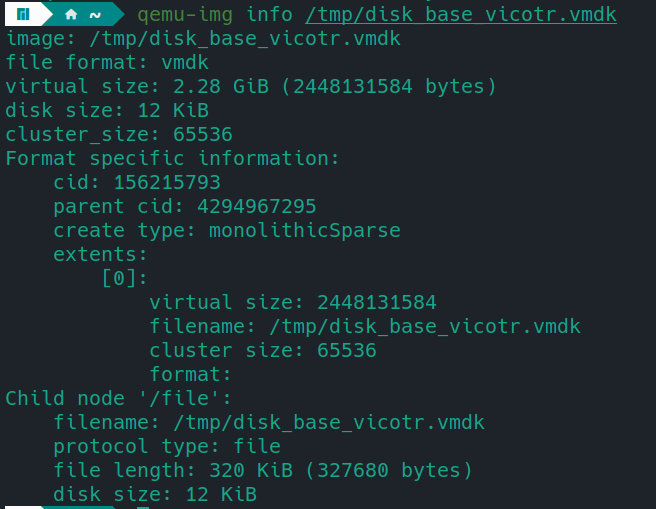
Симферополь, 2025

1) Изучите возможности команды qemu-img:

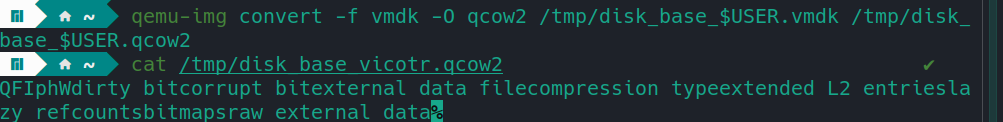
(a) Создайте образ виртуального жёсткого диска в папке /tmp/ размером 1.5GB в формате vmdk с именем disk\_base\_$USER.vmdk

(b) $USER переменная среды окружения в которой хранится логин текущего пользователя

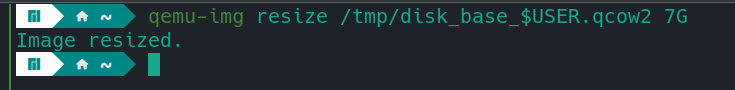
Рисунок 1 — создание образа виртуального жесткого диска объемом 2.28 Гибибайт через утлиту qemu-img

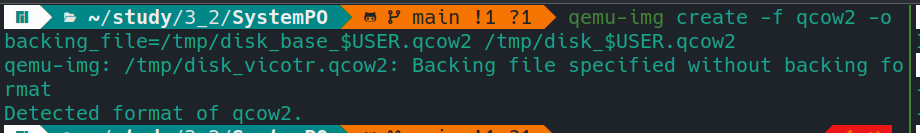
Рисунок — проверка что образ диска успешно создан объемом хранилища 2.28 Гибибайта

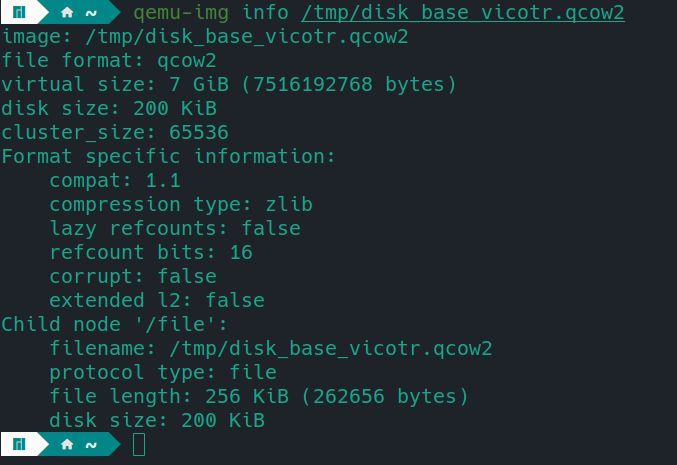
(c) Измените формат образа на qcow2, изменив также расширение файла

Рисунок 2 — конвертирование vmdk формата образа в qcow2

(d) Увеличьте размер образа диска до 7Gb

Рисунок 3 — изменение размера образа до 7 Гибибайт

Рисунок 4 — создание дочернего образа disk\_vicotr.qcow2 на основе образа disk\_base\_vicotr.qcow2

Рисунок 5 — проверка что размер образа диска изменился с 2.28 Гибибайт на 7 Гибибайта

(e) С помощью qemu-img создайте целевой (дочерний) образ диска,базирующийся на образе диска, созданном на предыдущем этапе. Образ в формате qcow2 должен называться disk\_$USER.qcow2 и располагаться в директории /tmp/

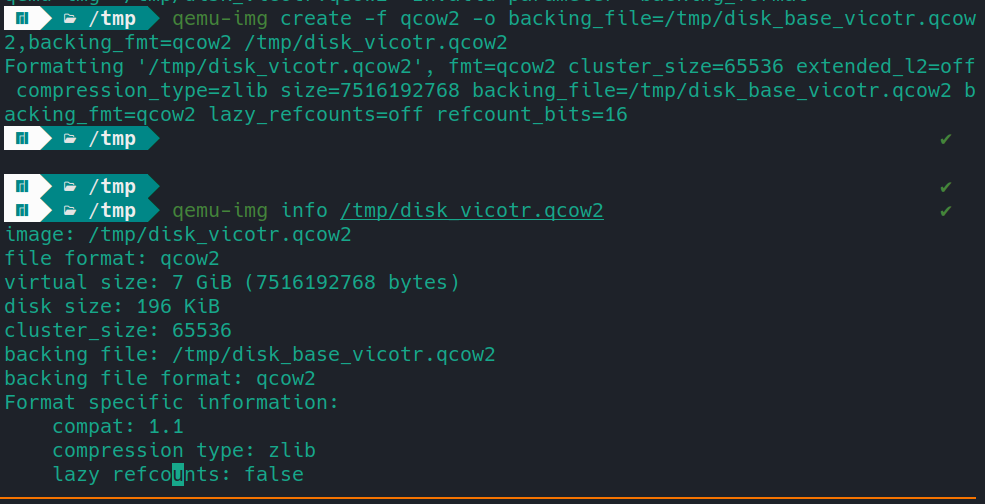


Рисунок 6 — создание образа виртуального диска на основе базового и проверка через утилиту qemu-img info что он связан с базовым

2) Определите поддерживается ли гипервизор KVM на вашем оборудовании как описано в предыдущей главе (для тестов можно использовать файл CD-ROM /var/qemu/OS/ubuntu14.iso). Если KVM поддерживается, в дальнейшем используйте его при работе с ВМ.

3) Запустите виртуальную машину qemu с необходимыми параметрами: Количество процессоров 1

• Оперативная память 512Mb

• Тип эмулируемой видеокарты std

• Образ жёсткого диска образ, созданный вами на предыдущем этапе лабораторной работы (целевой) • Файл CD-ROM /var/qemu/OS/xubuntu14.iso

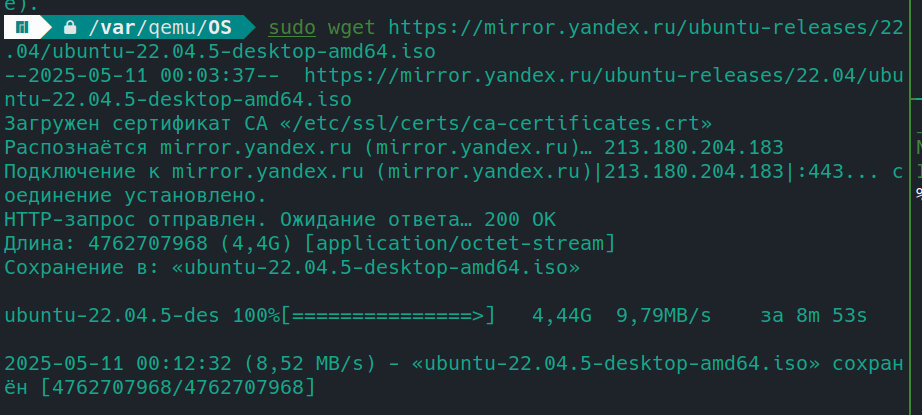
• Сеть пользовательская сеть

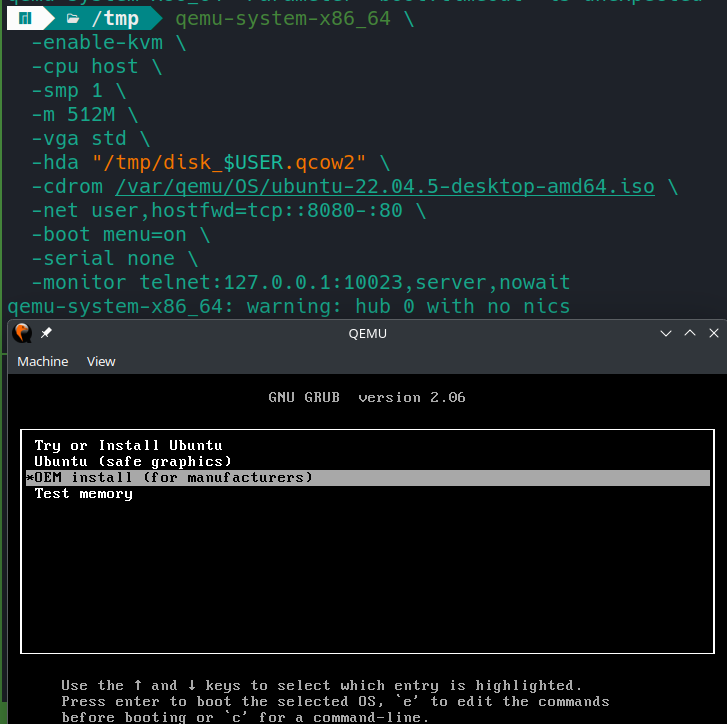
• Проброс портов: порт хост-компьютера = 8080) порт виртуальной машины = 80

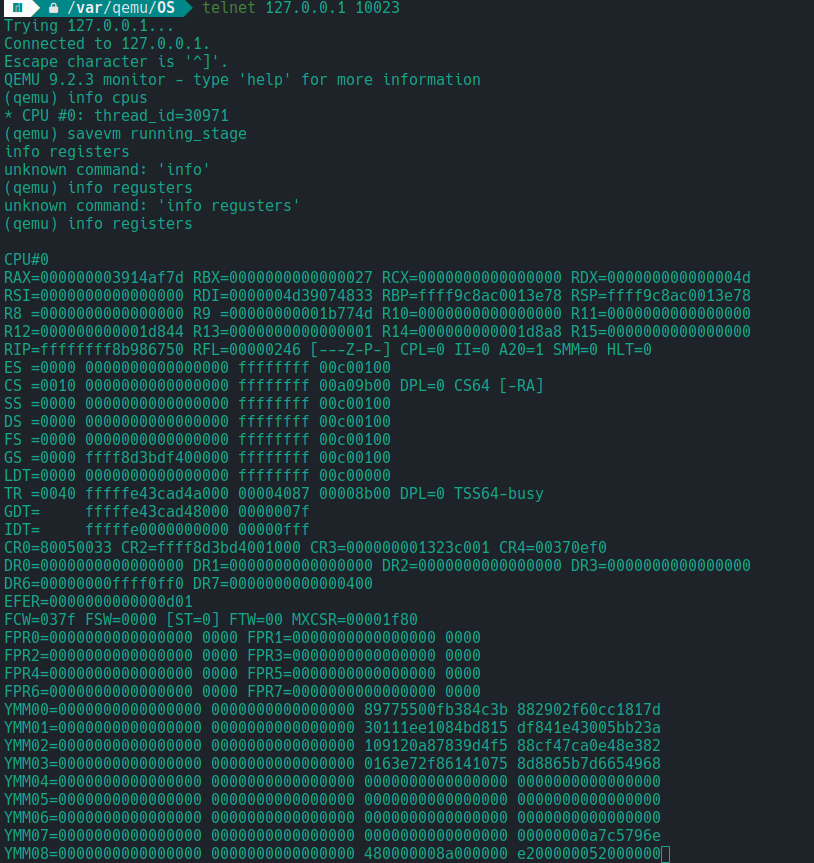
• Включите отображение меню выбора устройства для загрузки

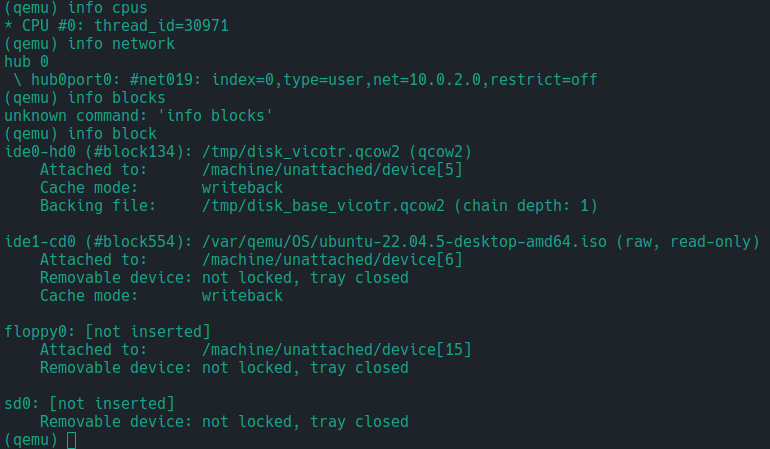
• Таймаут отображения меню 10 секунд

• Дополнительные опции:

Рисунок 7 — скачал образ ubuntu 22.04 с зеркала yandex

Рисунок 8 — запуск эмулятора qemu с парамтерами из ТЗ

Рисунок 9 — подключение к монитору виртуальной машины по протоколу telnet и вывод информации о процессоре и его регистрам

Рисунок 10- вывод информации о блочных устройствах и сети виртуальной машины

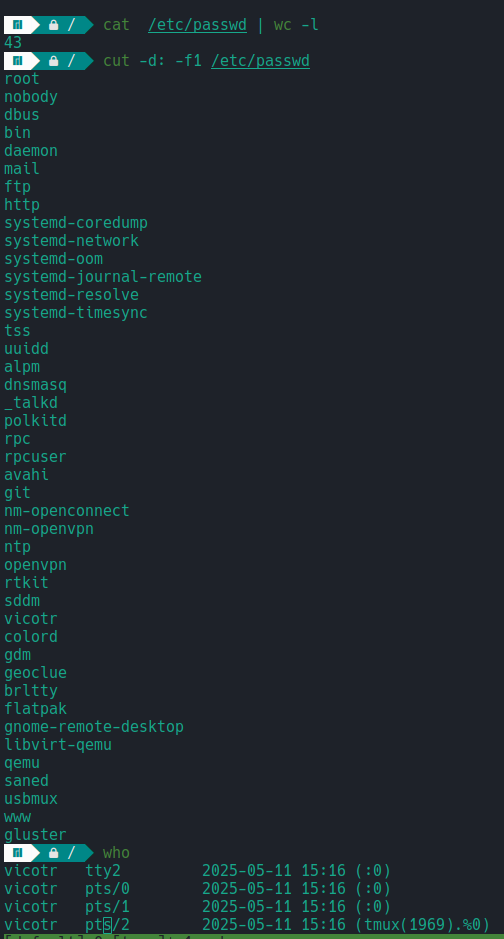
ВТОРАЯ ЧАСТЬ ЗАДАНИЯ:

Б) Auditd

1. Узнайте список всех пользователей Linux

2. Получите вывод только имён пользователей в системе

3. Узнайте список всех подключенных пользователей к системе в данный момент времени

Рисунок 11 — выполнение задания 1,2,3

4. С помощью команды find найдите в корневом каталоге файлы:

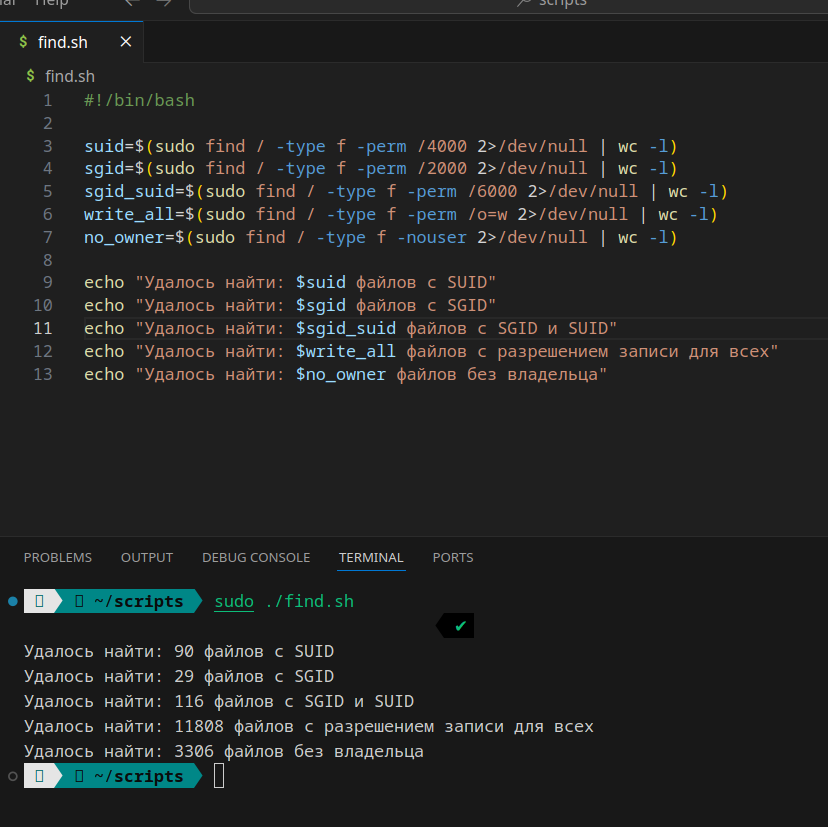
a) имеющие атрибуты SUID;

b) имеющие атрибуты SGID;

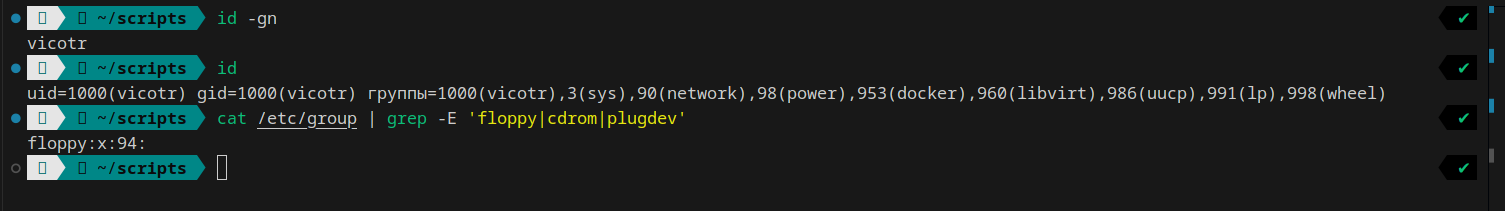
c) имеющие атрибуты SGID и SUID;

d) файлы, которые разрешено модифицировать всем;

e) файлы, не имеющие владельца

Рисунок 12 – скрипт для поиска файлов с различными правами в системе

5. С помощью команды id user\_name посмотрите список основной и дополнительных групп пользователей. Найдите дополнительные группы floppy, cdrom и plugdev, дающие право использовать сменные машинные носители /etc/cdrom, /etc/fd0 и т.д. для бесконтрольного блочного копирования данных.

Рисунок 13 - выполнение задания на работу с группами

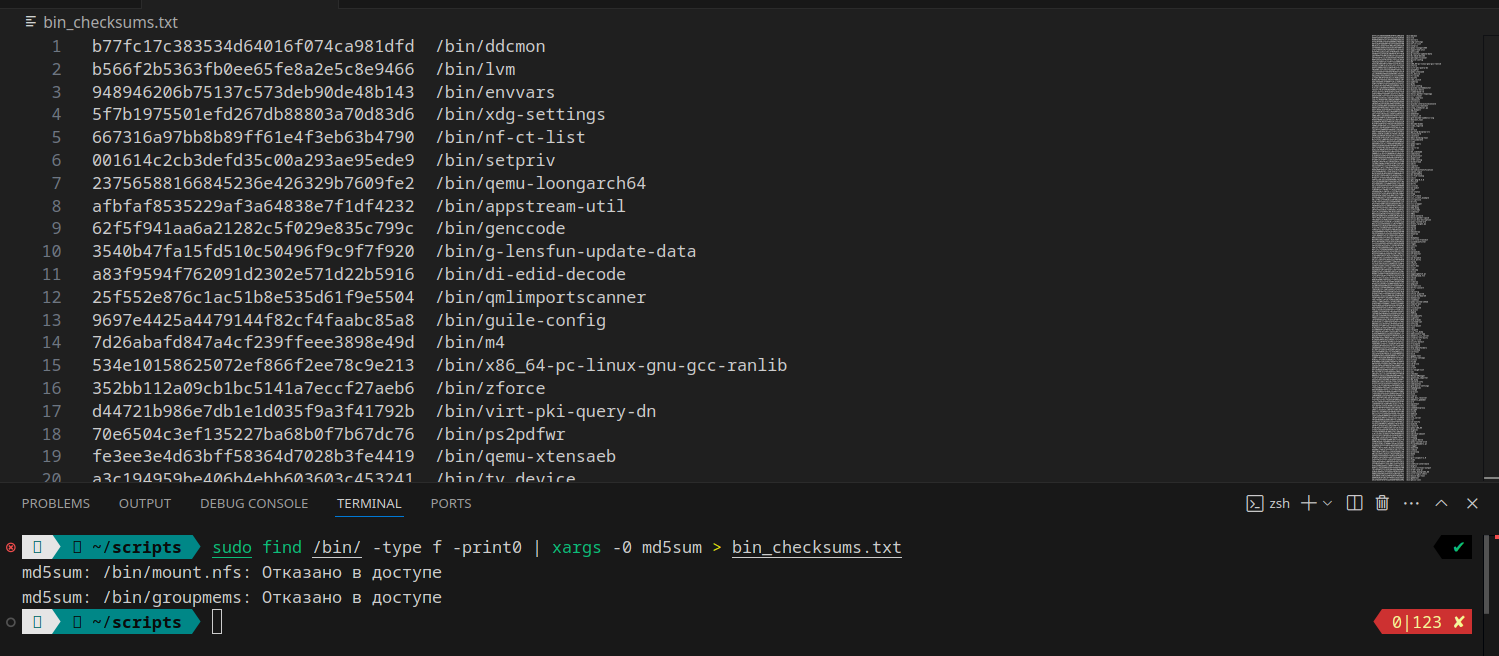
Зарегистрируйте нового пользователя и добавьте его в разные группы, выведите список существующих пользователей и группы, проверьте наличие нового пользователя

Рисунок 14 – выполнение заданий на работу с пользователем/группой

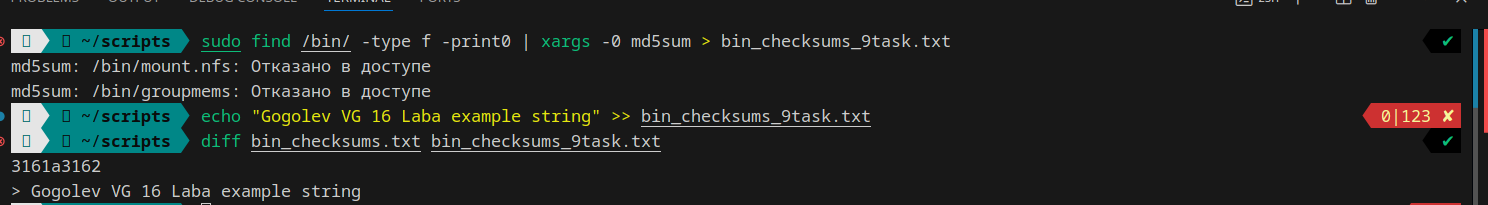
7. С помощью команды md5sum вычислите и запишите контрольную сумму для одного из файлов в каталоге /home/

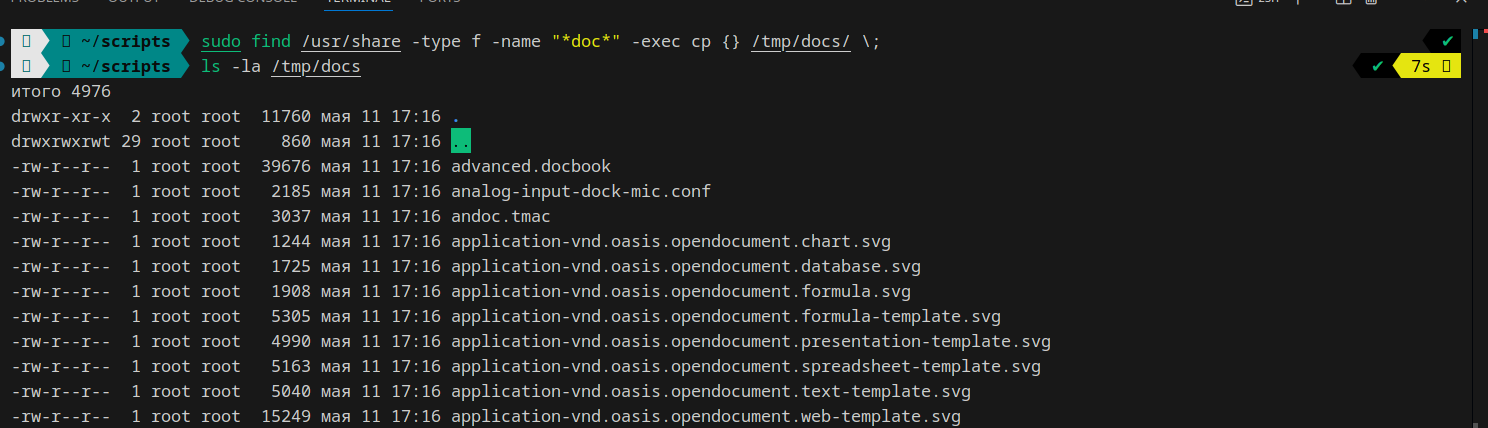
Рисунок 15 – выполнение задания 7

8. С помощью команды md5sum вычислите и запишите в файл контрольную сумму всех файлов в каталоге /bin.

Рисунок 16 – выполнение задания 8

9. Снова с помощью команды md5sum вычислите и запишите в файл контрольную сумму всех файлов в каталоге /bin и добавьте какие-нибудь символы в конце файла, после сравните обе суммы

Рисунок 17 – выполнение задания 9

Рисунок 18 – выполнение задания на поиск файлов содержащих в названии “doc” и копирование в /tmp/docs

10. Найдите в папке /usr/share, включая подкаталоги, простые файлы “doc” и скопируйте найденное в папку /tmp/docs/

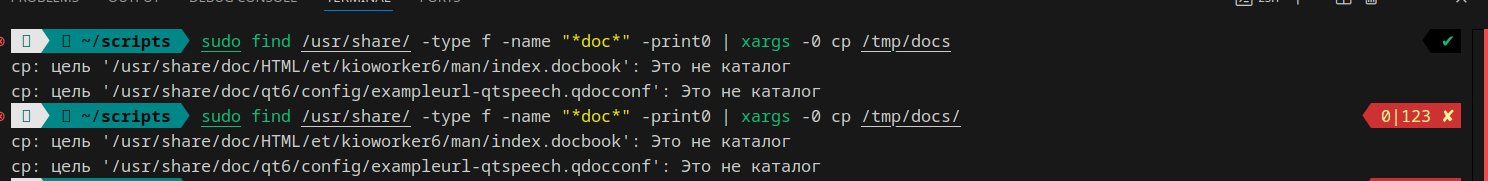


Рисунок 19 – почему-то решение через -print0 -xargs -0 не работает((  
  
11. Установите пакет auditd для мониторинга событий операционной системы и записи их в журналы событий

12. Просмотрите статус службы auditd

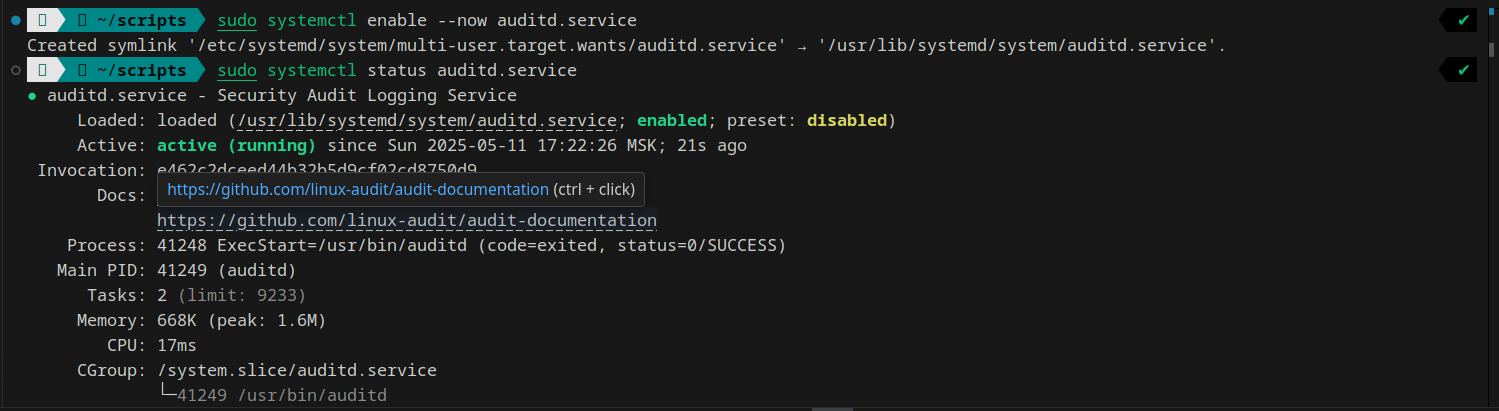
13. Запустите службу auditd

14. Выведите абсолютно все события аудита за день

15. Выведите результаты аудита по времени

16. Установите пакет figlet

17. Запустите figlet таким образом, чтобы на экране отобразилась ваша фамилия и группа

Рисунок 20 – запуск и проверка службы auditd.service

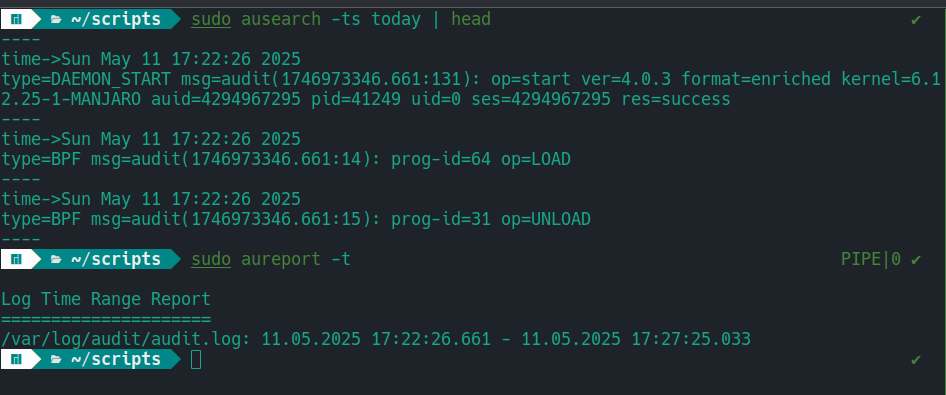


Рисунок 21 – вывод всех событий аудита за день и за время 5 минут

ausearch

Назначение: Поиск событий в логах аудита.

Основные ключи:

-m (или --message) — фильтр по типу события (например, LOGIN, USER\_AUTH, SYSCALL).

-k (или --key) — поиск по ключу аудита (например, ausearch -k my\_script).

-ui — поиск по UID пользователя.

-sc — поиск по системному вызову (например, open, execve).

-ts — фильтр по времени (-ts today, -ts "05/11/2025 17:22:26").

aureport

Назначение: Генерация отчетов на основе логов аудита.

Основные ключи:

-t (или --log-time) — показывает временной диапазон логов.

-u — отчет по действиям пользователей.

-l — отчет по событиям входа/выхода.

Рисунок 22 – запустил figlet так чтобы вывело мою фамилию и группу