Отчёт

по лабораторной работе № 4 по курсу «Информационная безопасность и защита информации»

(Шифрование произвольного файла методом гаммирования)

Выполнил: студент 2 курса института математики и информационных технологий группы 22205 И. О. Левицкий

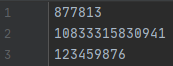
Руководитель: В. Е. Соколов

Петрозаводск

2022

**Описание структуры файла-ключа**

В файле ключе находятся три параметра для ГПСЧ (в порядке a-b-c0), которые отделены переносом строки

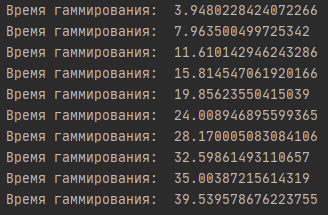


**Статистика**

Для статистики я использовал 10 текстовых файлов.

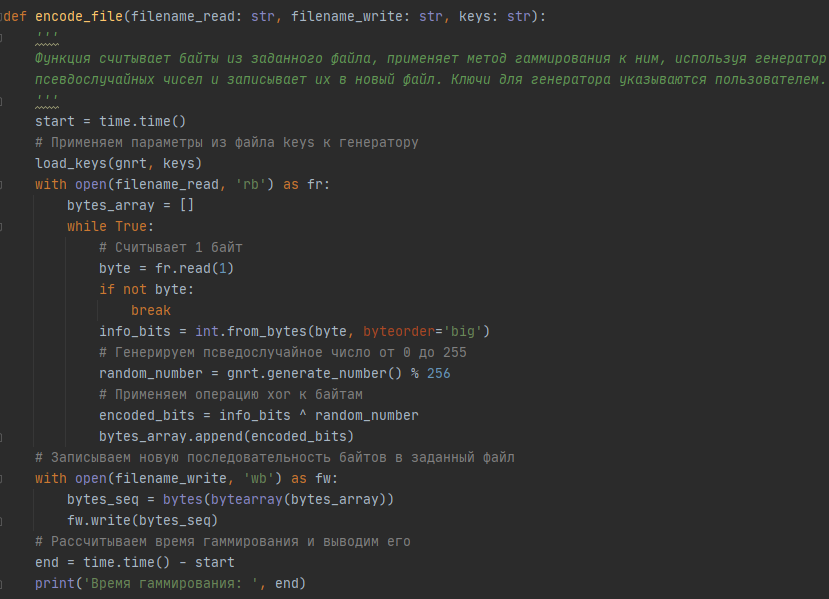
Размер каждого файла был больше предыдущего на 5 мегабайт

Время гаммирования всех файлов:



Видно, что каждый следующий файл шифровался дольше на примерно 4 секунды, значит зависимость времени гаммирования от размера файла линейная.

**Фрагмент программы выполняющий гаммирование**



В функции используется массив bytes\_array, в который помещаются зашифрованные байты