МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра «Информационная безопасность систем и технологий»

Отчет
по лабораторной работе №1
на тему «Реализация программного датчика случайных чисел на основе рекуррентной линии задержки с обратной связью»

Дисциплина: МиСКЗИ
Группа: 21ПИ1
Выполнил: Гусев Д. А.
Количество баллов:
Дата сдачи:
Принял: Липилин О. В.

2024

1 Цель работы: реализация программного датчика случайных чисел на основе генераторов линейных псевдослучайных последовательностей большого периода.

2 Задание на лабораторную работу.

2.1 В соответствии с вариантом задания построить структурную схему комбинирующего генератора ПСП, в качестве функции использовать операцию сложения по модулю 2. Определить период последовательности, вырабатываемой комбинирующим генератором. Вариант задания представлен на рисунке 1.

8	$x^{17}+x^{3}+1$	$x^{111}+x^{10}+1$	4, 9

Рисунок 1 — вариант задания

2.2 Программно реализовать комбинирующий генератор ПСП. В программе должна быть предусмотрена возможность задания количества бит вырабатываемой последовательности.

2.3 Реализовать с помощью разработанного генератора ПСП операцию маскирования данных. В качестве исходных данных для маскирования должен выступать файл произвольного формата. В программе должно быть предусмотрено два режима маскирования файла – полностью и без маскирования заголовка файла. В программе должна быть предусмотрена возможность определения статистических характеристик исходного и замаскированного файла.

3 Выполнение лабораторную работы:

3.1 Была построена структурная схема. Результат представлен на рисунке 2. Был найден период получившегося генератора. T <= НОК(2^{17}-1, 2^{111}-1). T <= 340279770772509196049560342183603470337.

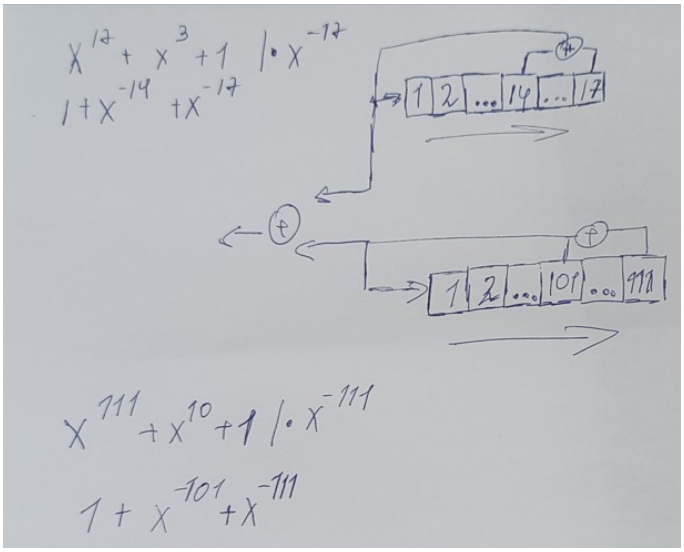

Рисунок 2 — Структурная схема

3.2 Был разработан код на языке C++, код представлен в репозитории на github: https://github.com/GooseG4G/PGU/blob/main/МиСКЗИ/gpsp.cpp. Рузультат работы генератора представлен на рисунке 2.

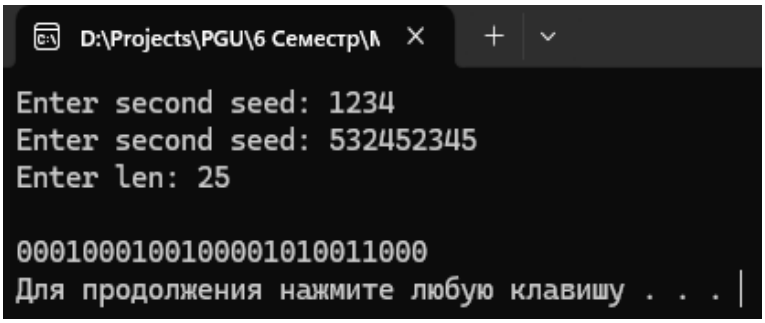

Рисунок 3 — Работа ГПСП

3.3 Был разработан код на языке C++ для маскирования файлов, код представлен в репозитории на github: https://github.com/GooseG4G/PGU/blob/main/МиСКЗИ/gpsp_mask.cpp. Рузультат маскирования представлен на рисунке 3.

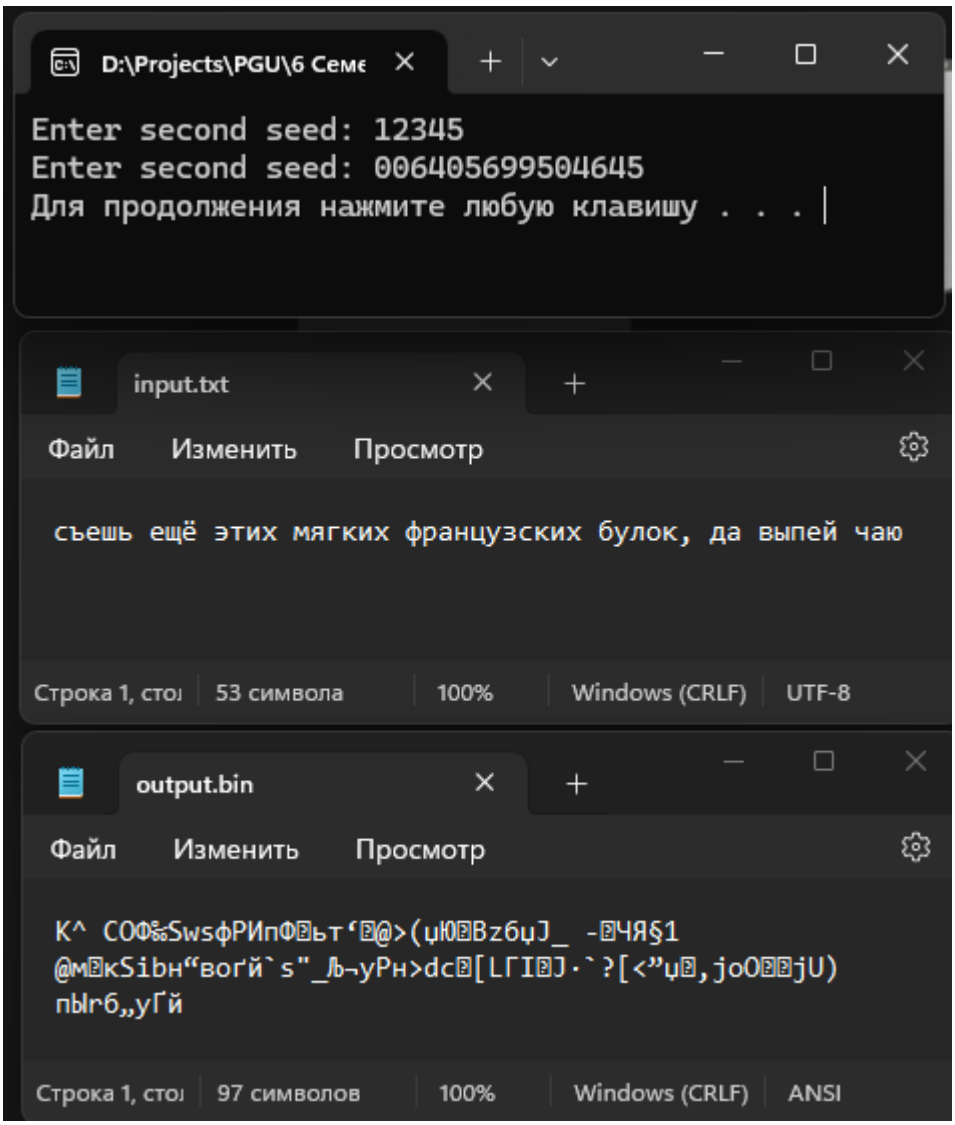

Рисунок 3 — маскирование файла

4 Вывод: был реализован программный датчика случайных чисел на основе генераторов линейных псевдослучайных последовательностей большого периода.