МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра «Информационная безопасность систем и технологий»

Отчет

по лабораторной работе №2

на тему «Исследование статистических свойств программного датчика ПСП»

Дисциплина: МиСКЗИ

Группа: 21ПИ1

Выполнил: Гусев Д. А.

Количество баллов:

Дата сдачи:

Принял: Липилин О. В.

2024

1 Цель работы: исследование статистических характеристик ПСП и их влияния на результат криптографического преобразования.

2 Задание на лабораторную работу.

2.1 Дополнить программу, реализующую комбинирующий генератор ПСП, функционалом, позволяющим определять статистические характеристики вырабатываемой последовательности, маскируемых данных и замаскированных данных. В программе должна быть предусмотрена возможность указания длины комбинаций, для которых определяются вероятности появления, и возможность указания значения сдвига при вычислении АКФ.

2.2 Провести статистические исследования ПСП. Определить:

- объем выборки для проведения статистических исследований ПСП;

- вероятности появления комбинаций длиной от 1 до 4 бит;

- вероятности появления комбинаций длиной от 2 до 4 бит, содержащих одинаковое количество единиц;

- автокорреляционную функцию ПСП для от 0 до 32 бит;

Результаты исследования представить в графическом виде. Сделать выводы по результатам исследования.

2.3 Провести маскирование текстового файла (размер файла не менее 20 Кб, текст должен иметь семантическое содержание). Определить статистические характеристики файла до и после маскирования (распределение вероятностей появления символов кодовой таблицы). Результаты исследования представить в графическом виде. Сделать выводы по результатам исследования. Привести содержимое файла до и после маскирования.

2.4 Внести преобладания в маскирующую гамму (путем инверсии каждой n-й единицы в последовательности). Провести маскирование текстового файла. Определить статистические характеристики файла после маскирования. Сделать выводы по результатам исследования о влиянии качества ПСП на качество маскирования.

3 Выполнение лабораторную работы:

3.1 Программа из лабораторной работы 1 была модифицирована, были добавлены функции для сбора статистических данных. Генератор ПСП был помещен в отдельный класс. Код программы находится в каталоге в репозитории на github в файлах LB2.cpp и common.cpp: https://github.com/Goose-Student/6s-MiSKZI-Lipilin/tree/main/2LB/source.

3.2 Был проведен сбор статистических данных. Таблицы calc находятся в репощитории на github: https://github.com/Goose-Student/6s-MiSKZI-Lipilin/blob/main/2LB/calculate.ods.

Был определен обьем выборки. Для сбора данных было использовано 10^6 бит. Результаты представлены на рисунке 1.

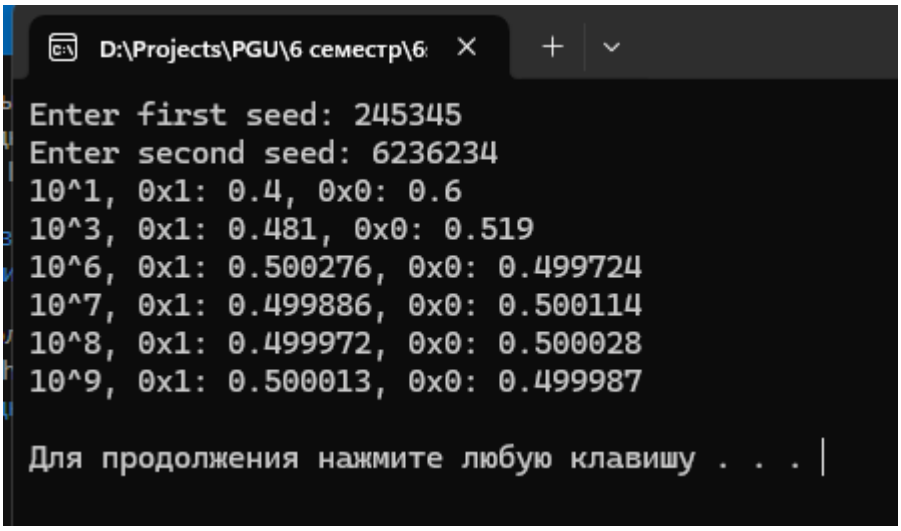

Рисунок 1 — Определение объема выборки

Были определены вероятности появления комбинаций длиной от 1 до 4 бит. Результат представлен в таблице 1.

Таблица 1 — Вероятности появления комбинаций доиной от 1 до 4 бит.

Биты	Вероятность
0	0,50012
1	0,49988
00	0,250317
01	0,249753
10	0,249753
11	0,250176

000	0,125421
001	0,124895
010	0,124834
011	0,124919
100	0,124896
101	0,124857
110	0,124919
111	0,125257
0000	0,062931
0001	0,062489
0010	0,062468
0011	0,062427
0100	0,062262
0101	0,062572
0110	0,062513
0111	0,062406
1000	0,06249
1001	0,062406
1010	0,062365
1011	0,062492
1100	0,062634
1101	0,062285
1110	0,062406
1111	0,062851

Были определнены вероятности появления комбинаций длиной от 2 до 4 бит, содержащих одинаковое количество единиц. Результат представлен в таблице 2 и на рисунке 2.

Таблица 2 — вероятности появления комбинаций длиной от 2 до 4 бит, содержащих одинаковое количество единиц;

	0 ед	1 ед	2 ед	3 ед	4 ед
2 бита	0,250317	0,499506	0,250176	-	-
3 бита	0,125421	0,374625	0,374695	0,125257	-
4 бита	0,062931	0,249709	0,374917	0,249589	0,062851

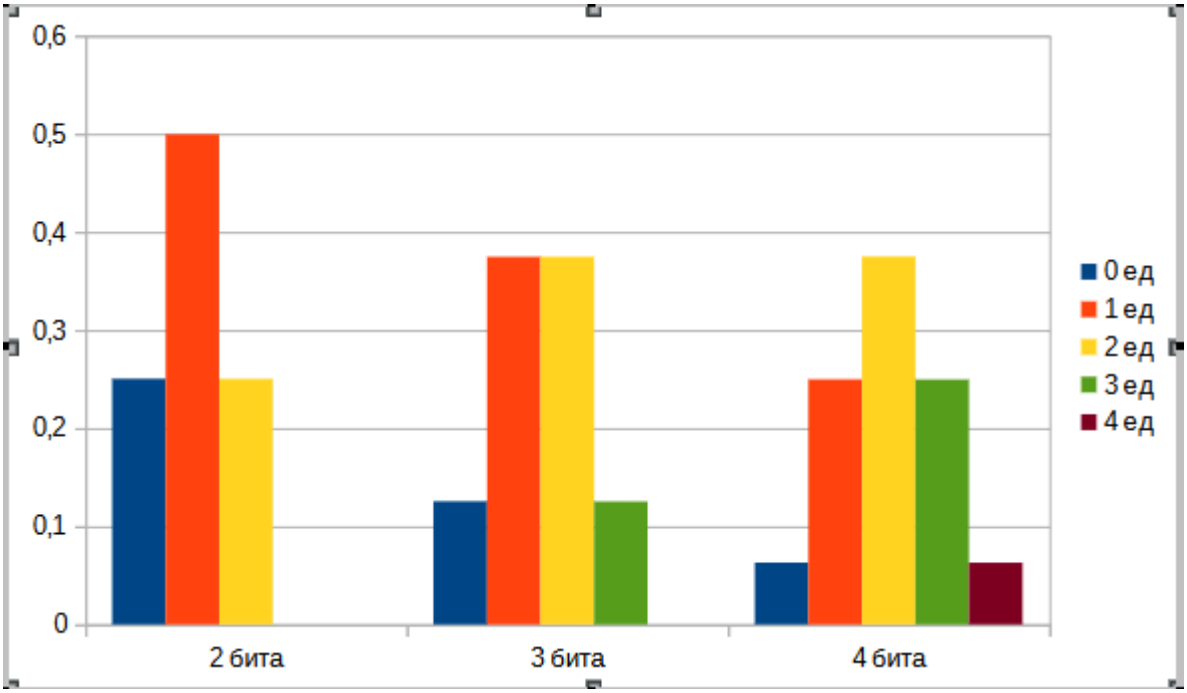

Рисунок 2 — вероятности появления комбинаций длиной от 2 до 4 бит, содержащих одинаковое количество единиц;

Была определена автокорреляционная функция ПСП для от 0 до 32 бит. Результат представлен в таблице 3.

Таблица 3 - автокорреляционная функция ПСП для от 0 до 32 бит;

t	P
0	1,00
1	0,00730073
2	-0,00270027
3	-0,00710071
4	-0,00330033
5	0,00810081
6	-0,00790079
7	-0,0161016
8	-0,00350035
9	-0,00770077

10	0,00650065
11	-0,00790079
12	-0,00870087
13	0,00510051
14	-0,00730073
15	-0,00290029
16	-0,0147015
17	-0,00790079
18	-0,00210021
19	0,00490049
20	-0,00890089
21	-0,00610061
22	-0,00250025
23	-0,010301
24	-0,010301
25	-0,0105011
26	-0,00650065
27	0,0141014
28	-0,00910091
29	-0,00110011
30	-0,00010001
31	-0,00990099
32	-0,00290029

3.3 Были определены вероятности появления каждого символа ASCII в файле размером >20кб без маскирования (рисунок 3), при маскировании (рисунок 4), и с внесением преобладания (рисунок 5).

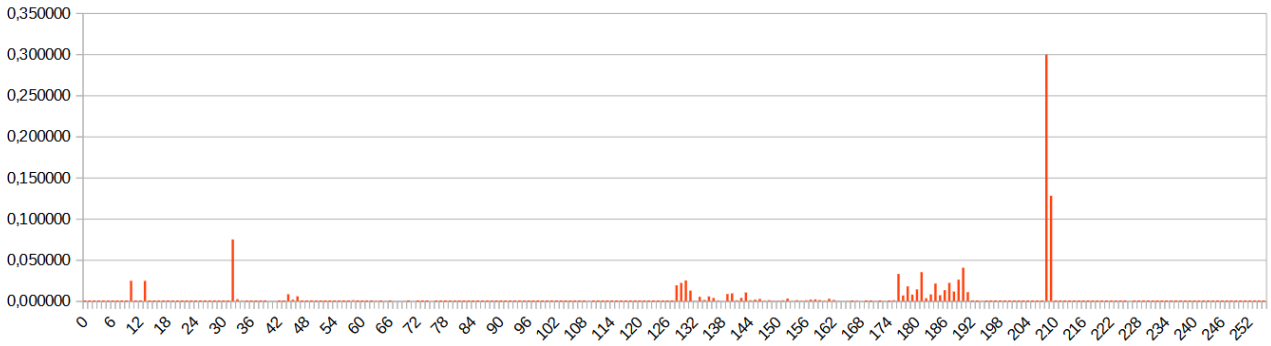

Рисунок 3 — Вероятности символов без маскирования

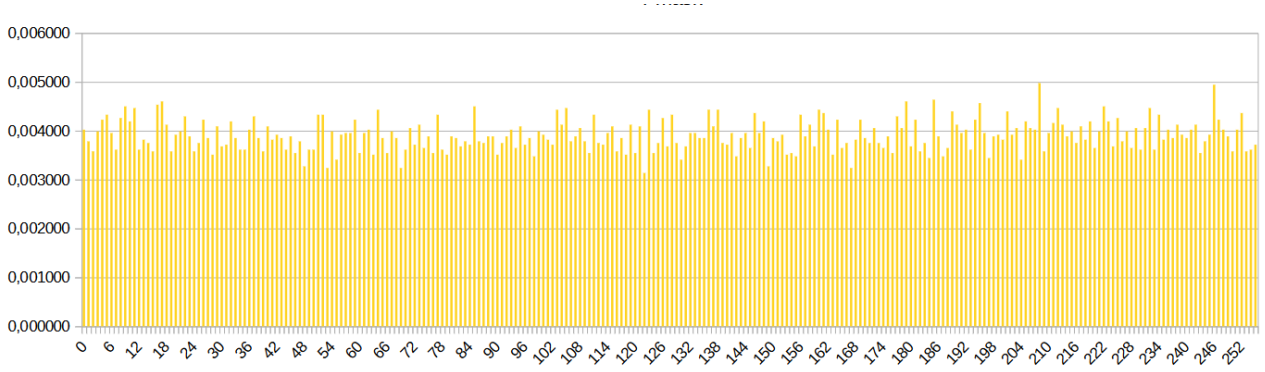

Рисунок 4 — Вероятности символов с маскированием

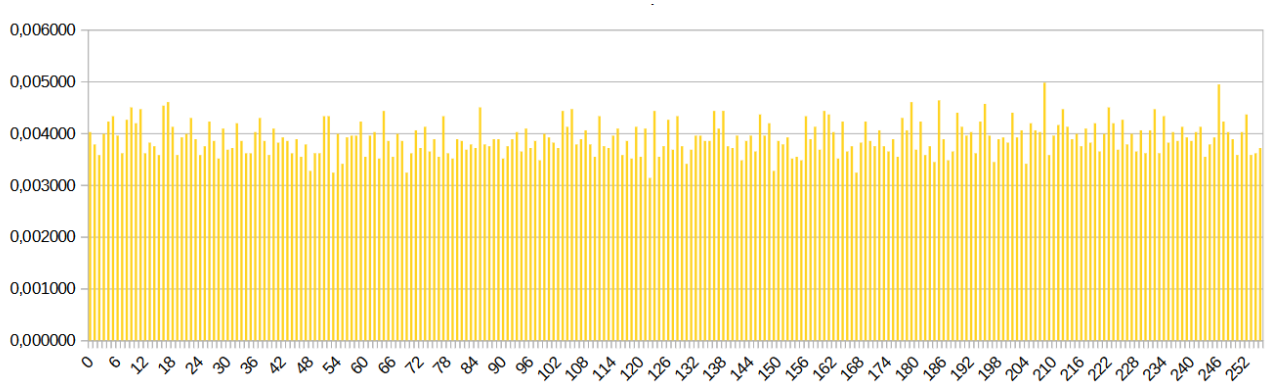

Рисунок 5 — Вероятности символов с маскированием и преобладанием (n = 5)

4 Вывод: были исследованы статистические характеристики ПСП и их влияние на результат криптографического преобразования.