Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

**ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ**

студента 4 курса 431 группы

факультета компьютерных наук и информационных технологий

*Кайдышевой Дарьи Сергеевны*

Научный руководитель

Ст. преподаватель \_\_\_\_\_\_\_\_\_\_\_\_\_ И.И. Слеповичев

подпись, дата

Саратов 2024

**СОДЕРЖАНИЕ**

[1 Генерация псевдослучайных чисел в фалйы с использованием prng.exe 3](#_Toc166975261)

[2 Постановка задачи 4](#_Toc166975262)

[3 Точечные оценки параметров 6](#_Toc166975263)

[3.1 Пятипараметрический метод 6](#_Toc166975264)

[3.2 Аддитивный метод 7](#_Toc166975265)

[3.3 Блюма-Блюма-Шуба 8](#_Toc166975266)

[3.4 Линейно-конгруэнтный метод 9](#_Toc166975267)

[3.5 РСЛОС 10](#_Toc166975268)

[3.6 Вихрь Мерсенна 11](#_Toc166975269)

[3.7 Нелинейная комбинация РСЛОС 12](#_Toc166975270)

[3.8 RC4 13](#_Toc166975271)

[3.9 RSA 14](#_Toc166975272)

[4 Таблица 15](#_Toc166975273)

# **1 Генерация псевдослучайных чисел в фалйы с использованием prng.exe**

1. /g:lc /i:1024,171,513,577 /f:lc.txt
2. /g:lc /i:1024,7,11, 654,234,654,234,546,345,875,334,345,765,546,998,34,756,987,544 /f:add.txt
3. /g:5p /i:107,31,57,82,10,11101010101101011010 /f:5p.txt
4. /g:lfsr /i:1000010001,1011010110 /f:lfsr.txt
5. /g:nfsr /i:1001110110,1011010110,1100101001,9,491,424,532 /f:nfsr.txt
6. /g:mt /i:4563 /f:mt.txt
7. /g:rc4 /i:2309,1203,3836,4107,1944,1438,7472,4532,9239,1077,5584,4680,5754,5801,199,5117,2565,1804,7971,6885,8378,1106,8790,5904,4452,9068,6075,2725,9864,8279,1988,4034,1876,5932,1248,2420,8835,6797,2803,5213,4804,3972,6051,7912,6017,4107,3940,3122,9365,5713,6289,5731,364,8800,7892,3089,3138,5523,3726,5040,1898,7809,1386,2869,7844,8246,5254,2503,1253,1130,3368,4382,5316,5249,6276,4071,7893,1765,4508,9952,2734,3559,2313,3554,4483,889,7323,1518,3766,672,2132,4096,6167,8673,1219,4086,3241,7996,4274,7696,5617,8175,3383,4388,519,9199,9937,8095,489,5095,7591,2498,476,1727,4817,3592,9017,9533,7800,247,8154,2620,9273,8977,8271,5786,301,8425,3318,9171,8835,3691,2379,6213,5385,8338,7764,5322,3286,2193,2187,6189,3051,9366,1614,8210,9968,4723,2478,435,3064,9248,8619,2021,3841,5971,2077,382,7749,9034,8472,8598,5136,8417,5803,9549,4291,4550,4321,1675,2637,6206,4375,7893,9847,7974,5142,6210,7902,6811,5930,5351,7533,4732,944,2317,4393,3491,9393,8178,2293,6346,172,508,9567,6172,673,6877,2249,9612,9801,6299,7482,2324,6037,2548,910,5037,5532,5077,2594,9638,4022,719,5356,1184,4081,2277,7486,9883,8842,7460,266,246,8079,6422,8838,2102,1858,9034,9417,9342,351,4897,1161,2116,3740,4348,4506,4074,8019,7703,2228,279,2787,1763,2594,4193,9236,3038,3772,9463,9862,1853,7645,721 /f:rc4.txt
8. /g:rsa /i:10967,571,77,10 /f:rsa.txt
9. /g:bbs /i:791,5 /f:bbs.txt

# **2 Постановка задачи**

**Цель**

1. Сгенерировать псевдослучайную последовательность заданным методом.

2. Исследовать полученную псевдослучайную последовательность на случайность.

**Исходные данные**

Исходными данными для лабораторных занятий являются метод генерации псевдослучайных чисел, диапазон генерации случайных чисел, функция распределения, которой должны подчиняться случайные числа, количество генерируемых чисел.

**3 Задачи**

1) Сгенерировать последовательность из 10000 случайных чисел из диапазона [0,1]. Исходной программой для генерации ПСЧ может быть программа, созданная в рамках практической работы по данному курсу. (Изначально они генерировались не в указанном диапазоне, но была написана функция, которая нормировала их).

2) Протестировать статистические свойства последовательности псевдослучайных чисел:

a) Вычислить математическое ожидание последовательности;

b) Вычислить среднеквадратичное отклонение последовательности;

c) Сравните полученные оценки с заданными в пп. 1 параметрами. Постройте графики зависимостей оценок от объема выборки. Оцените относительные погрешности для какой-либо одной выборки.

d) Вычислить значение и дать ответ на вопрос удовлетворяет ли ППСЧ

i) Критерию хи-квадрат;

ii) Критерию серий;

iii) Критерию интервалов;

iv) Критерию разбиений;

v) Критерию перестановок;

vi) Критерию монотонности;

vii) Критерию конфликтов.

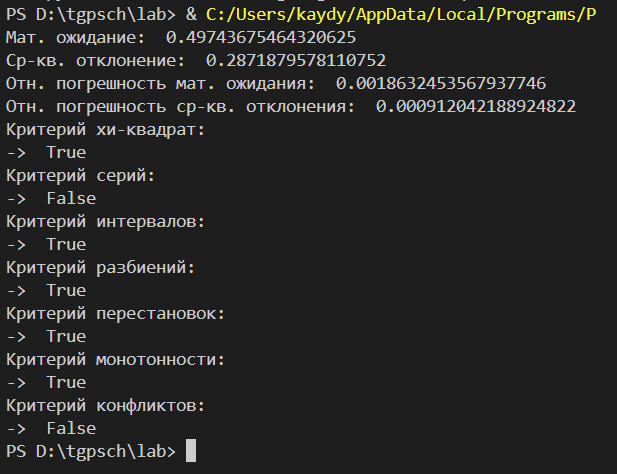
На входе: текстовый файл с ПСЧ, обозначения критерия.

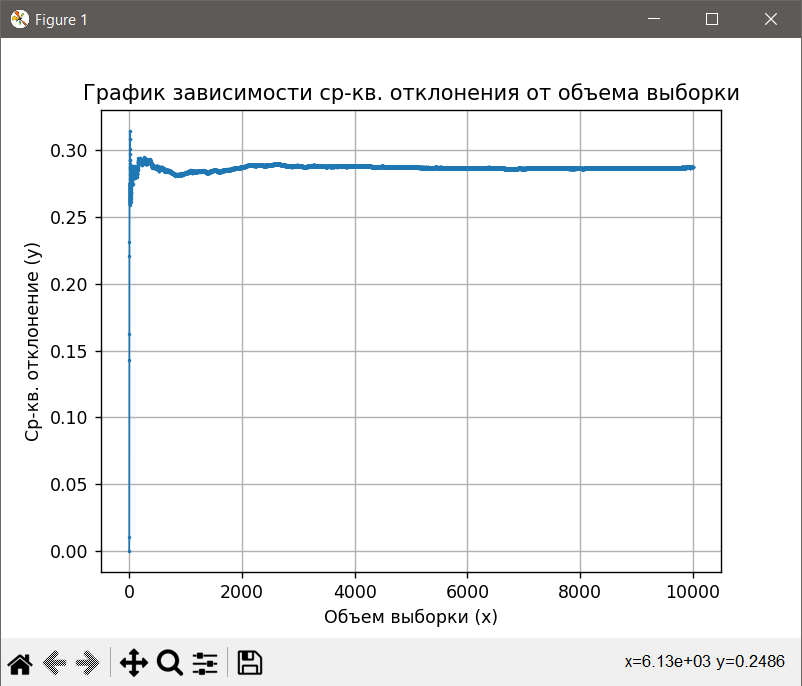
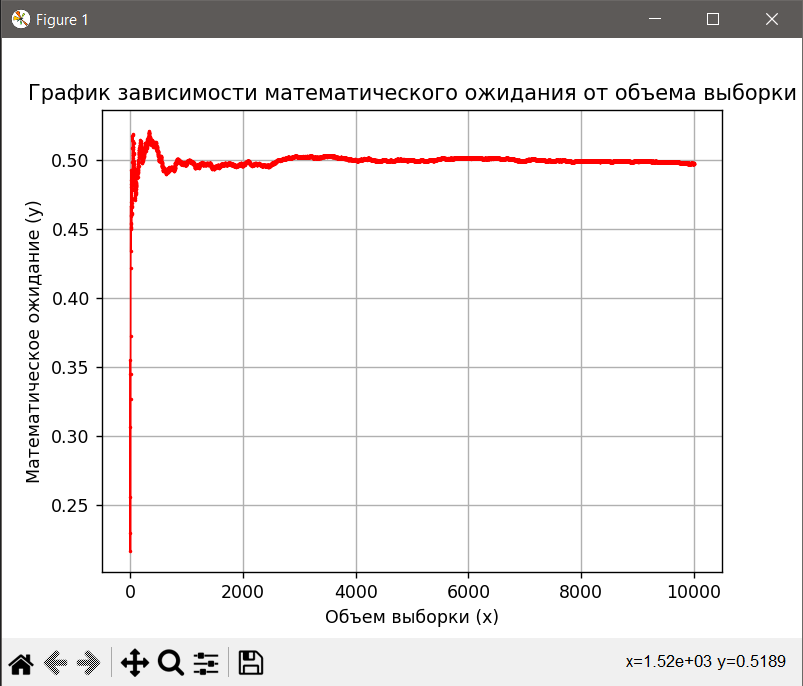
На выходе: точечные оценки параметров ППСЧ, ответ о соответствии ППСЧ указанному критерию.

Итогом лабораторной работы будет отчет, составленный по результатам проделанных вычислений.

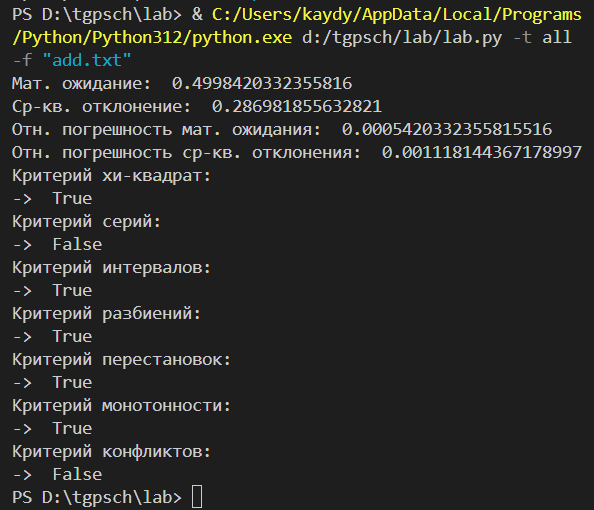
# **3 Точечные оценки параметров**

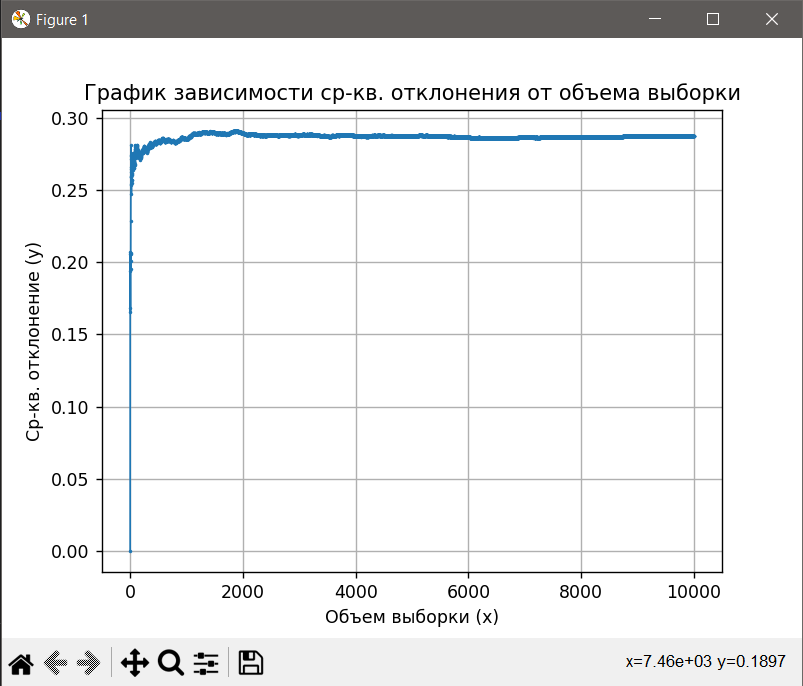
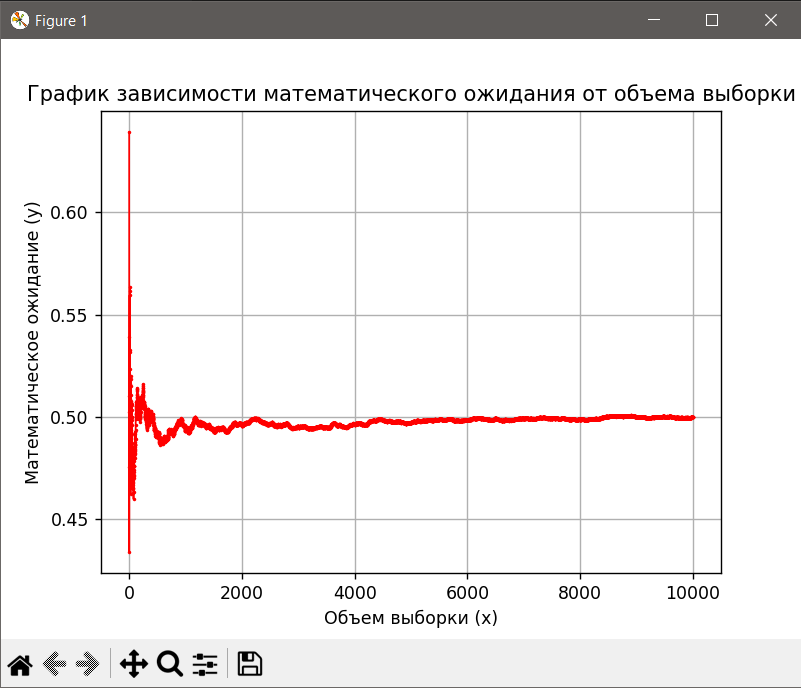
## **3.1 Пятипараметрический метод**

****

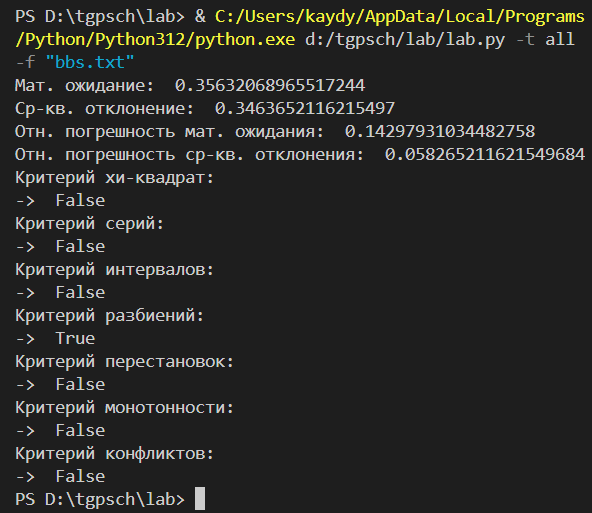


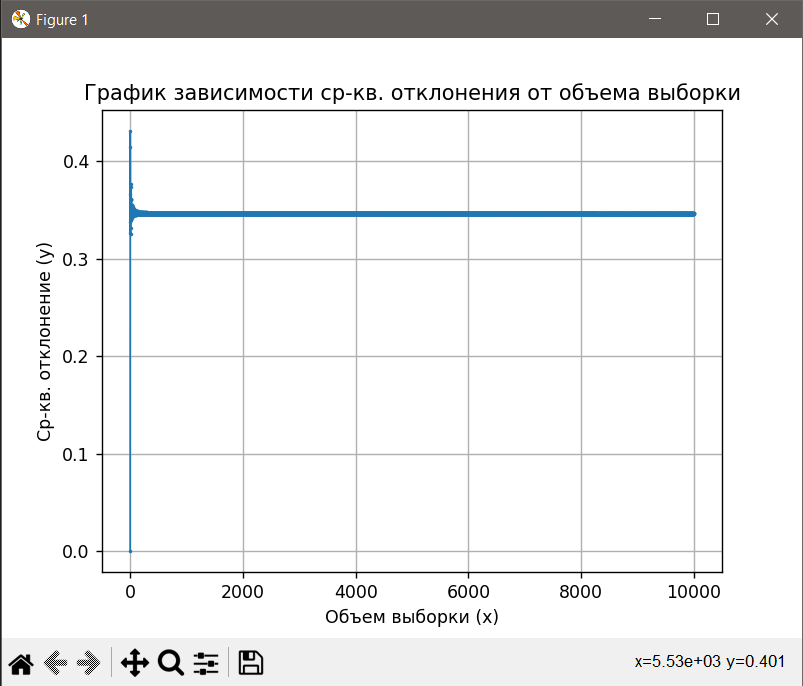
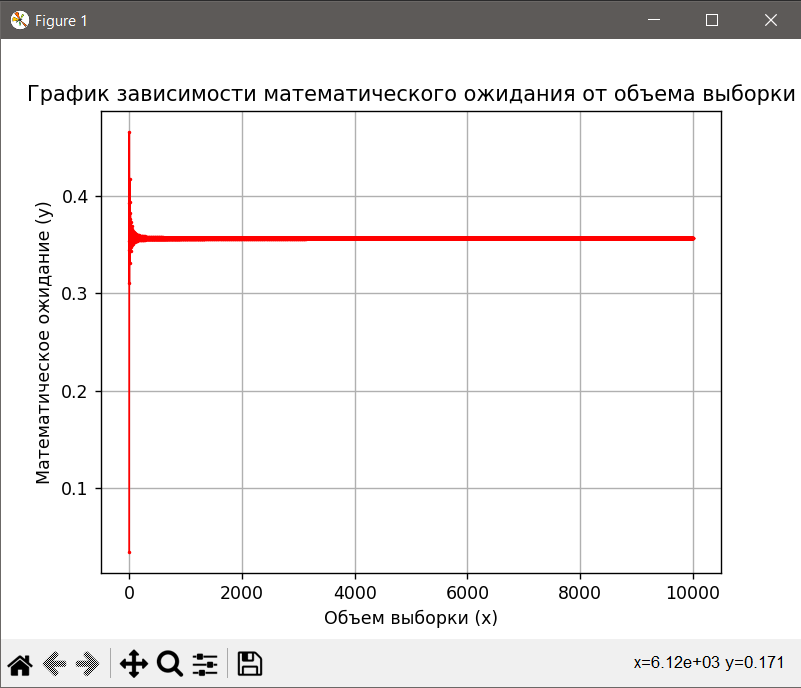
## **3.2 Аддитивный метод**

****

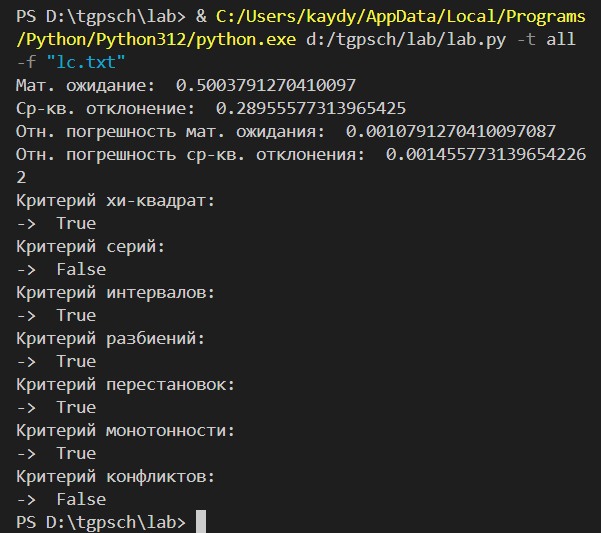


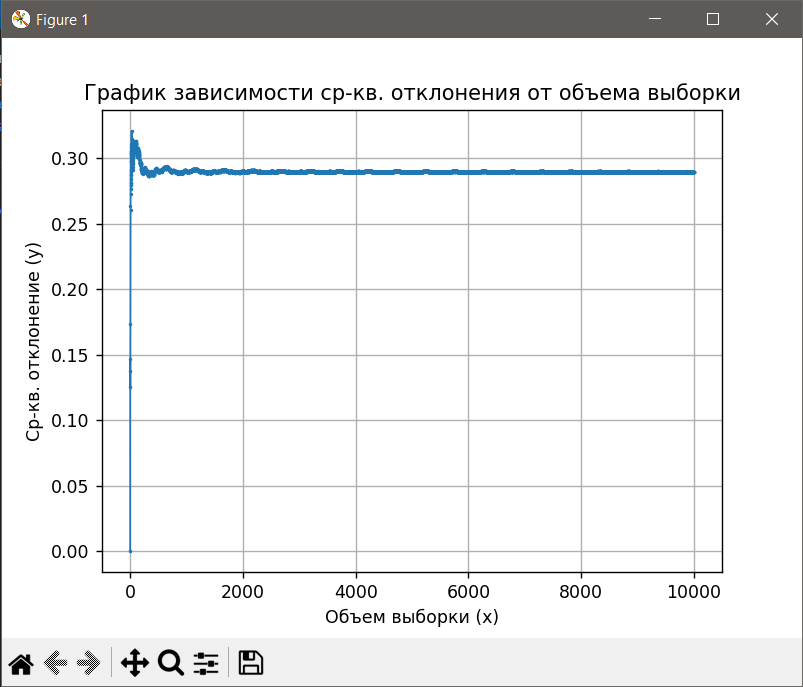
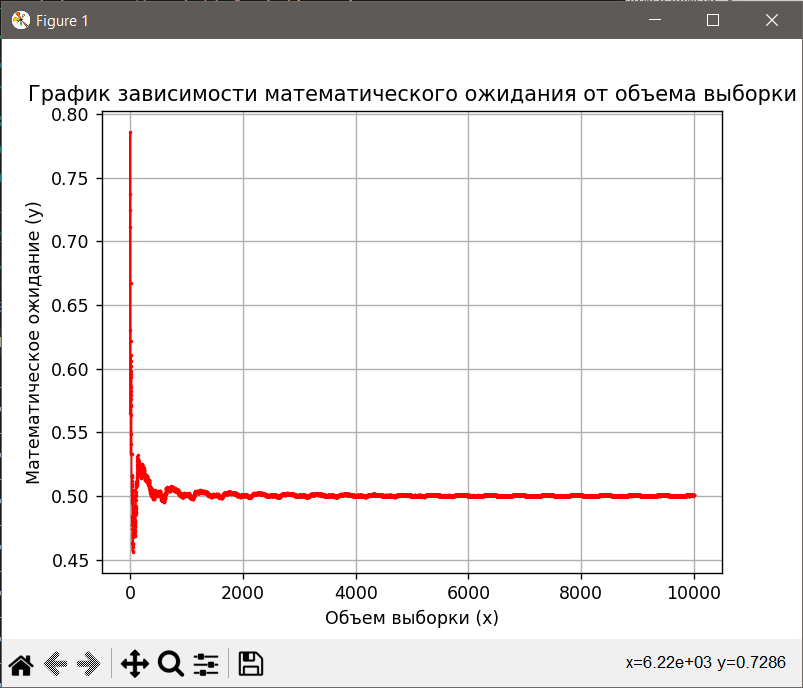
## **3.3 Блюма-Блюма-Шуба**

****

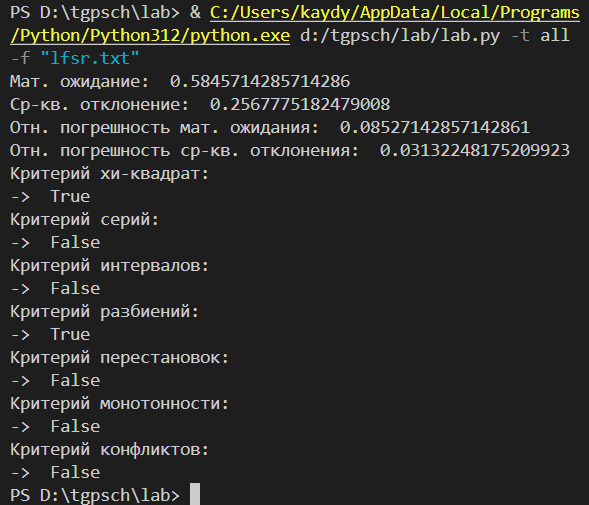


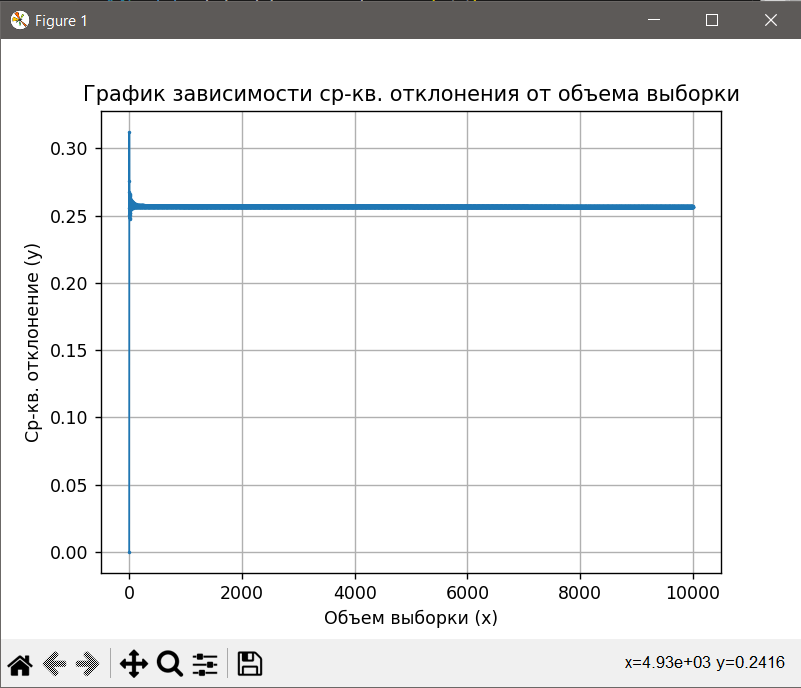
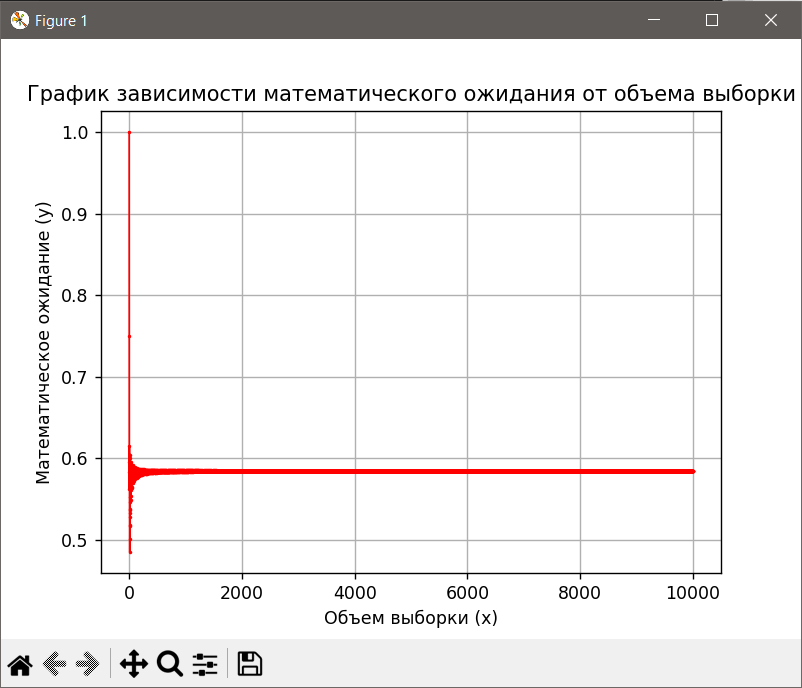
## **3.4 Линейно-конгруэнтный метод**

****

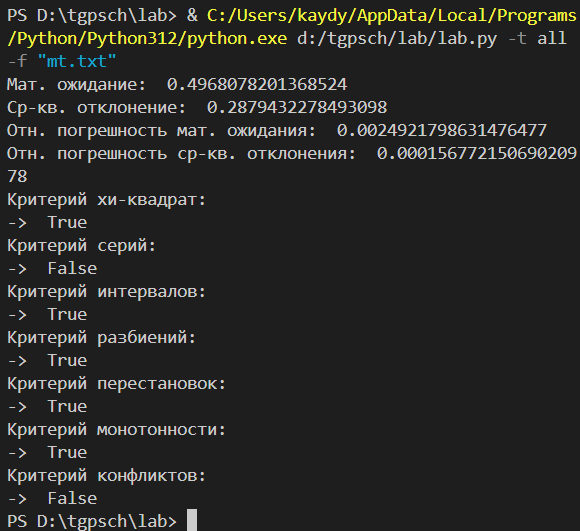


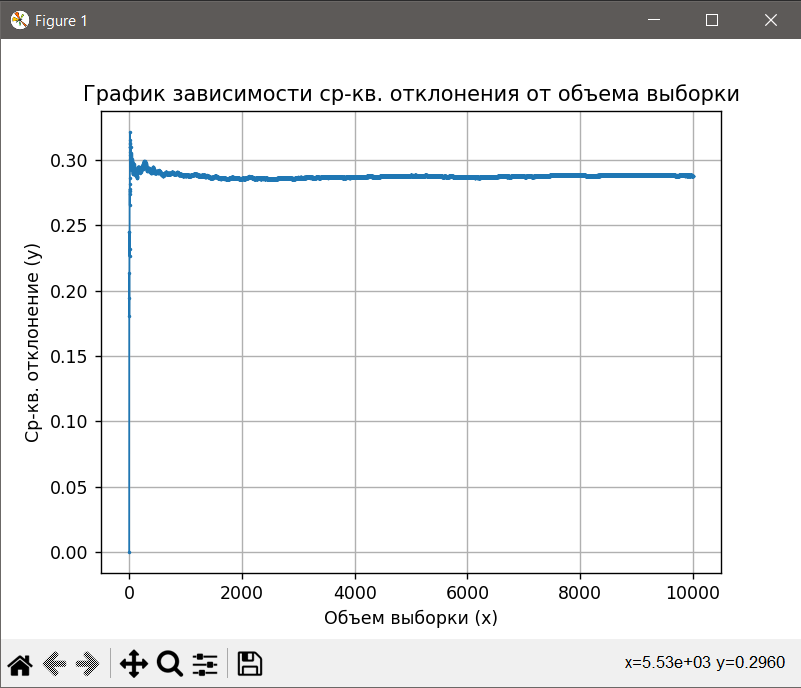
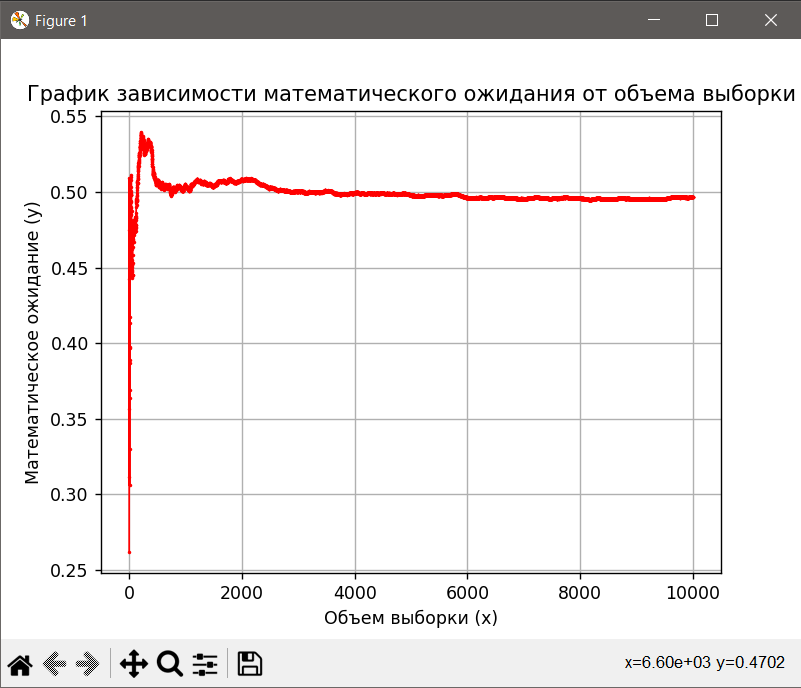
## **3.5 РСЛОС**

****

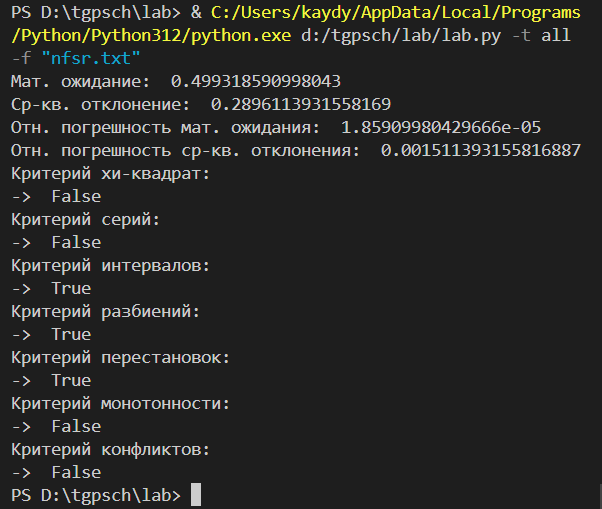


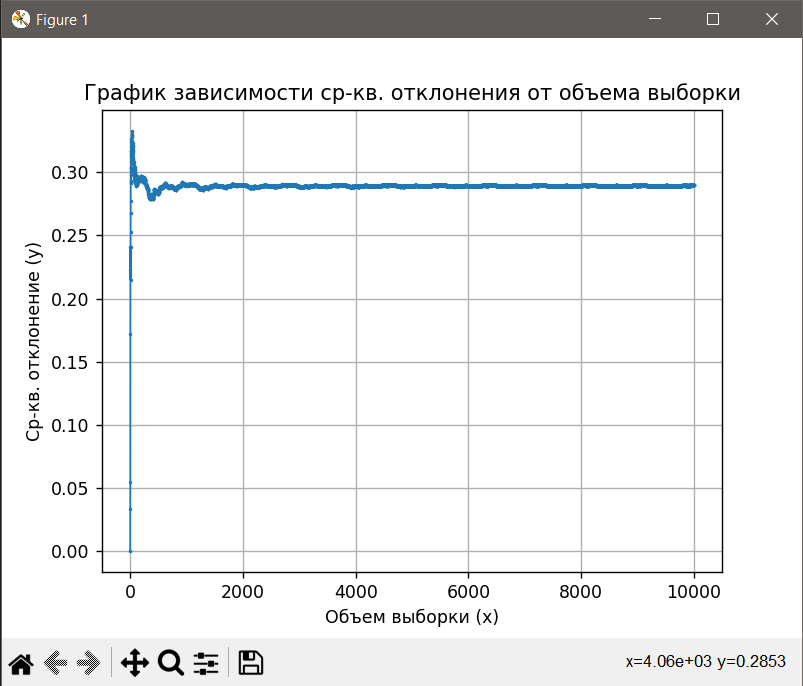
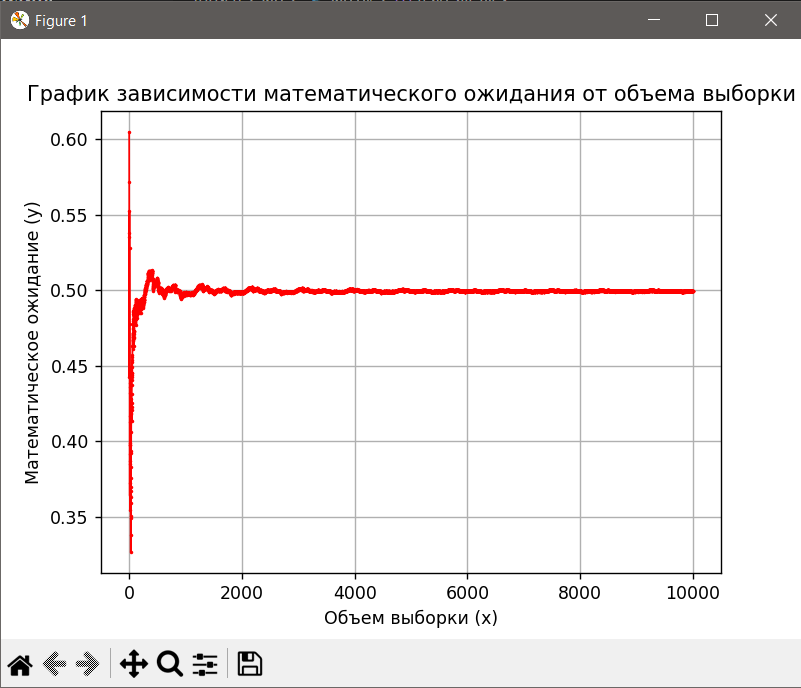
## **3.6 Вихрь Мерсенна**

****

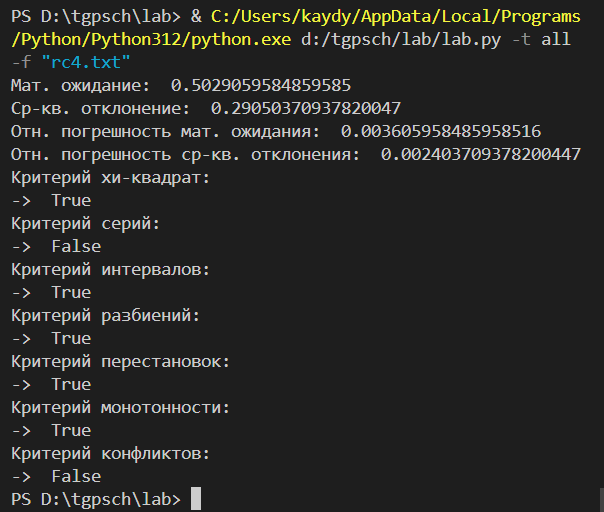


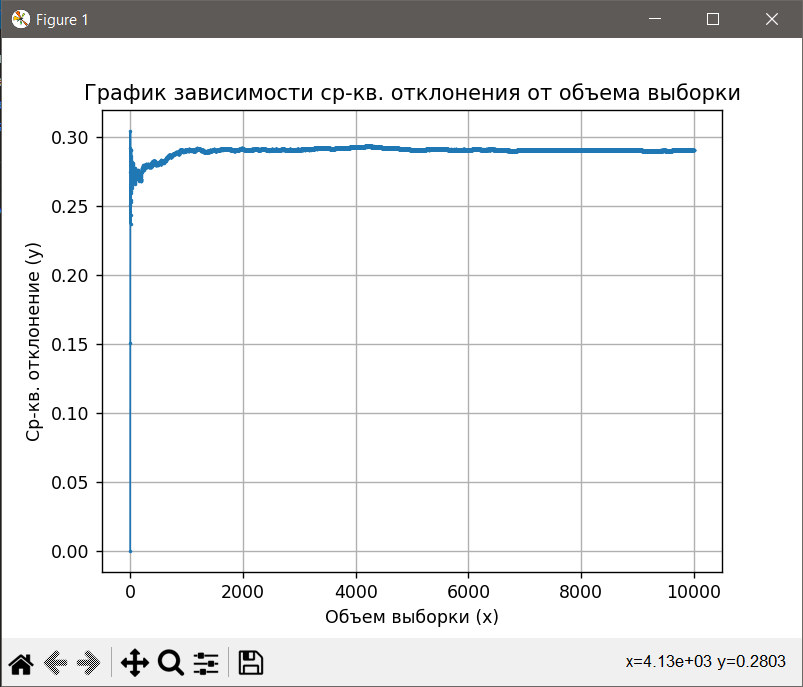
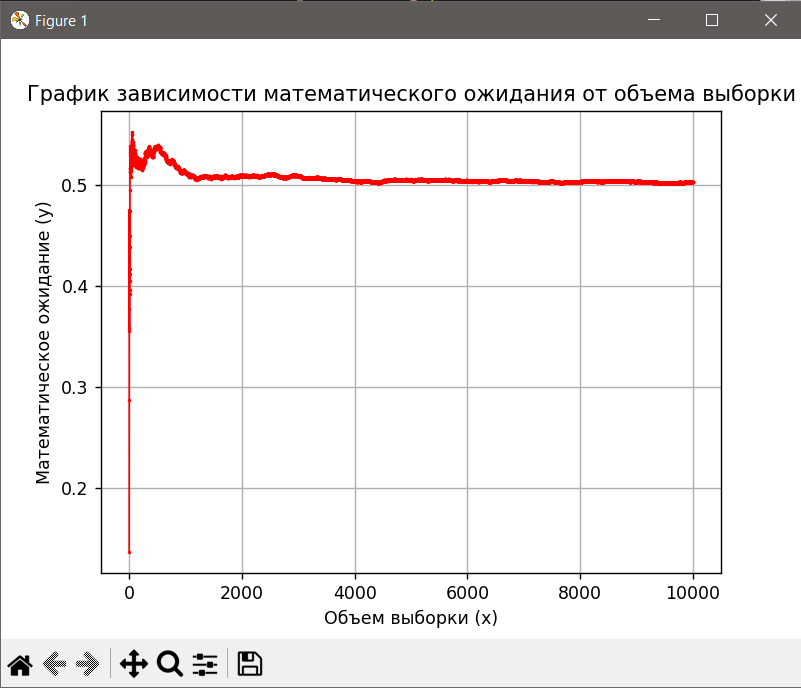
## **3.7 Нелинейная комбинация РСЛОС**

****

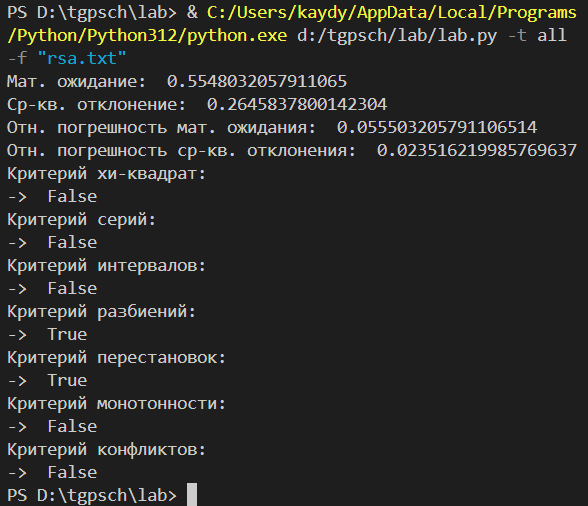


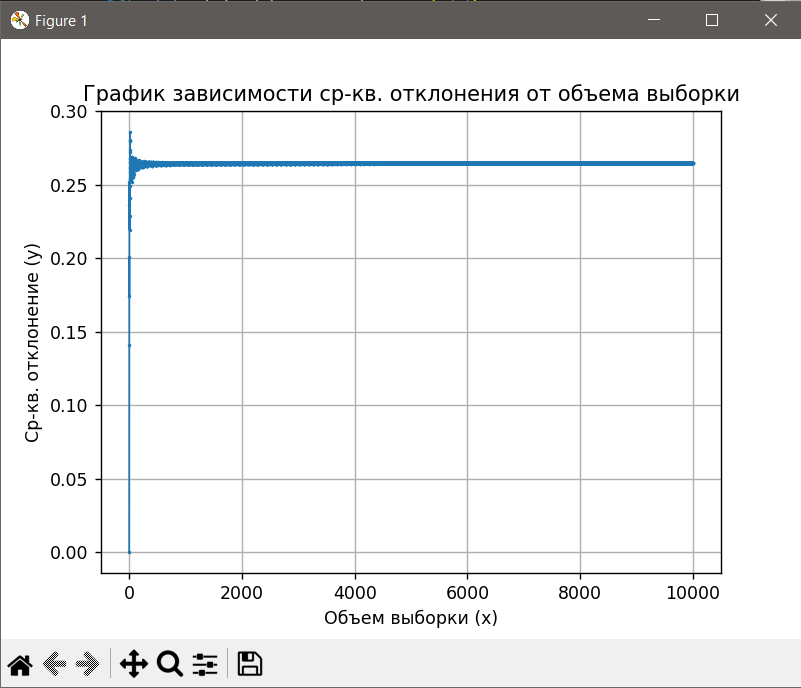
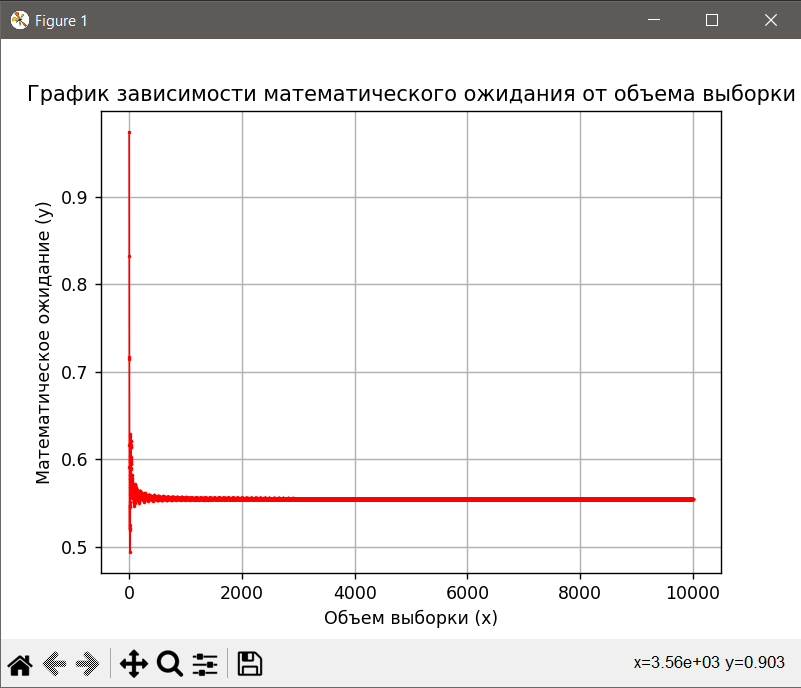
## **3.8 RC4**

****



## **3.9 RSA**

****



**4 Таблица**

Таблица 1. Результаты проверки ПСП различными критериями

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **5p** | **add** | **bbs** | **lc** | **lfsr** | **mt** | **nfsr** | **rc4** | **rsa** |
| **Хи-квадрат** | + | + | \_ | + | + | + | \_ | + | \_ |
| **серий** | \_ | \_ | \_ | \_ | \_ | \_ | \_ | \_ | \_ |
| **интервалов** | + | + | \_ | + | \_ | + | + | + | \_ |
| **разбиений** | + | + | + | + | + | + | + | + | + |
| **перестановок** | + | + | \_ | + | \_ | + | + | + | + |
| **монотонности** | + | + | \_ | + | \_ | + | \_ | + | \_ |
| **конфликтов** | \_ | \_ | \_ | \_ | \_ | \_ | \_ | \_ | \_ |