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

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.

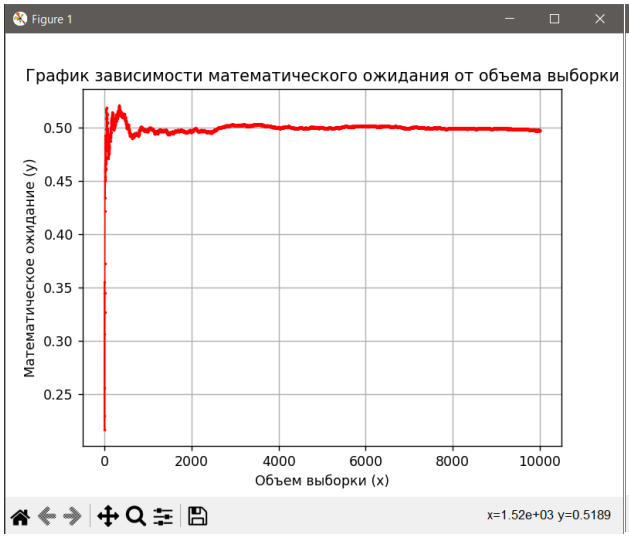
На выходе: точечные оценки параметров ППСЧ, ответ о соответствии ППСЧ указанному критерию.

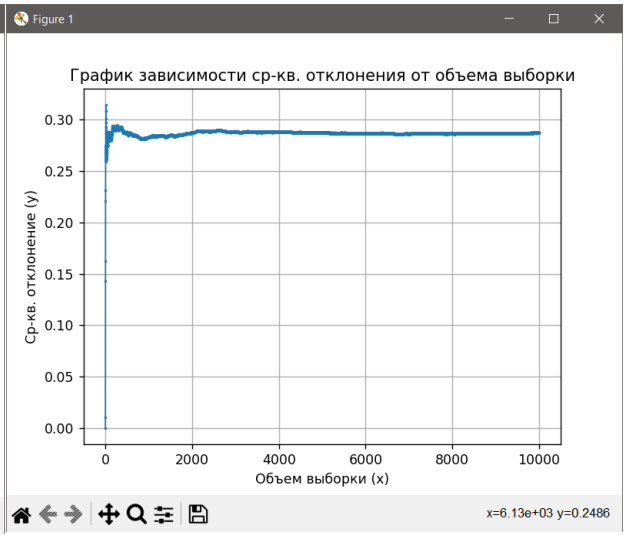
Итогом лабораторной работы будет отчет, составленный по результатам проделанных вычислений.

3 Точечные оценки параметров

3.1 Пятипараметрический метод

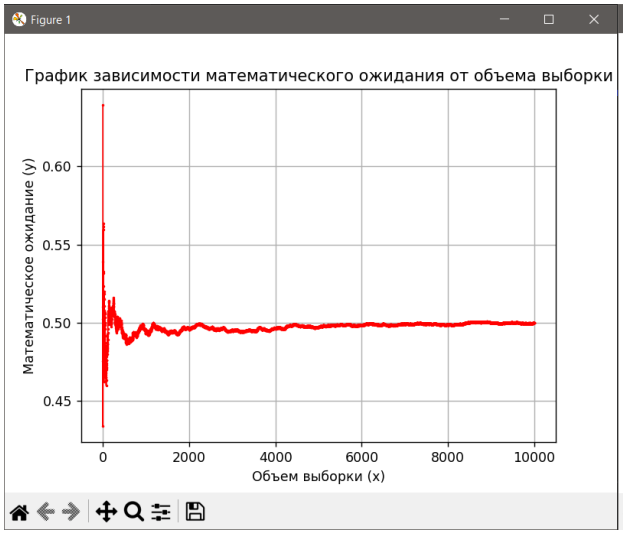
```
PS D:\tgpsch\lab> & C:/Users/kaydy/AppData/Local/Programs/P
Мат. ожидание:  0.49743675464320625
Ср-кв. отклонение:  0.2871879578110752
Отн. погрешность мат. ожидания:  0.0018632453567937746
Отн. погрешность ср-кв. отклонения:  0.0009120421889248 22
Критерий хи-квадрат:
->  True
Критерий серий:
->  False
Критерий интервалов:
->  True
Критерий разбиений:
->  True
Критерий перестановок:
->  True
Критерий монотонности:
->  True
Критерий конфликтов:
->  False
PS D:\tgpsch\lab>
```

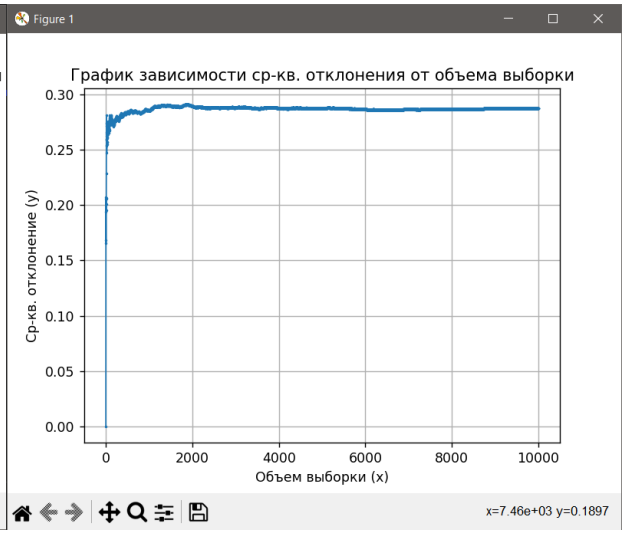




3.2 Аддитивный метод

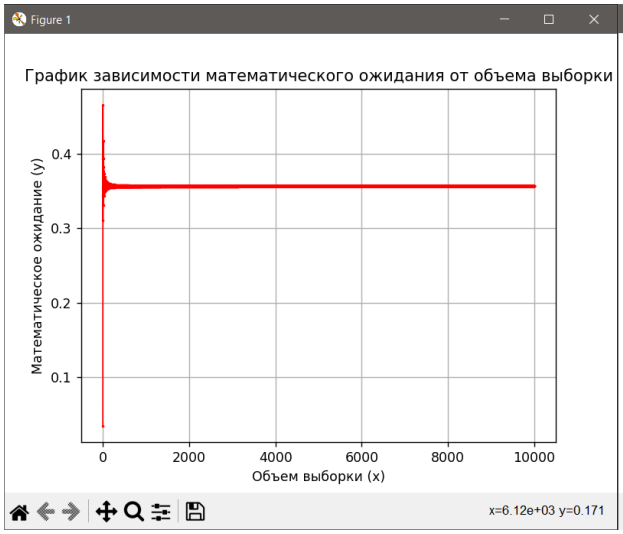
```
PS D:\tgpsch\lab> & C:/Users/kaydy/AppData/Local/Programs
/Python/Python312/python.exe d:/tgpsch/lab/lab.py -t all
-f "add.txt"
Мат. ожидание:  0.4998420332355816
Ср-кв. отклонение:  0.286981855632821
Отн. погрешность мат. ожидания:  0.0005420332355815516
Отн. погрешность ср-кв. отклонения:  0.001118144367178997
Критерий хи-квадрат:
->  True
Критерий серий:
->  False
Критерий интервалов:
->  True
Критерий разбиений:
->  True
Критерий перестановок:
->  True
Критерий монотонности:
->  True
Критерий конфликтов:
->  False
PS D:\tgpsch\lab>
```

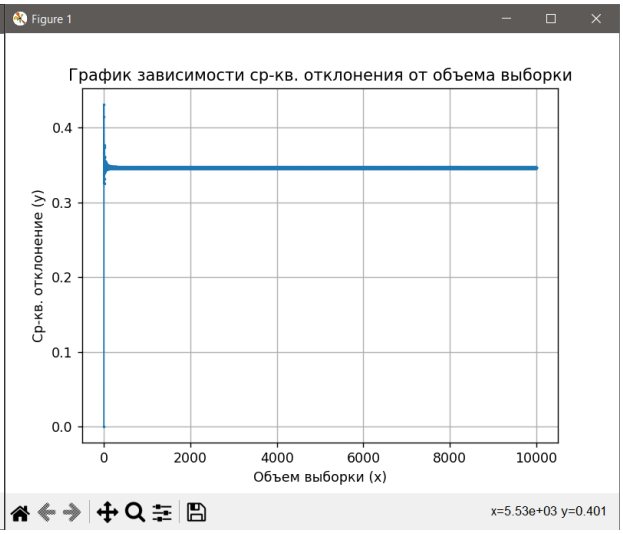




3.3 Блюма-Блюма-Шуба

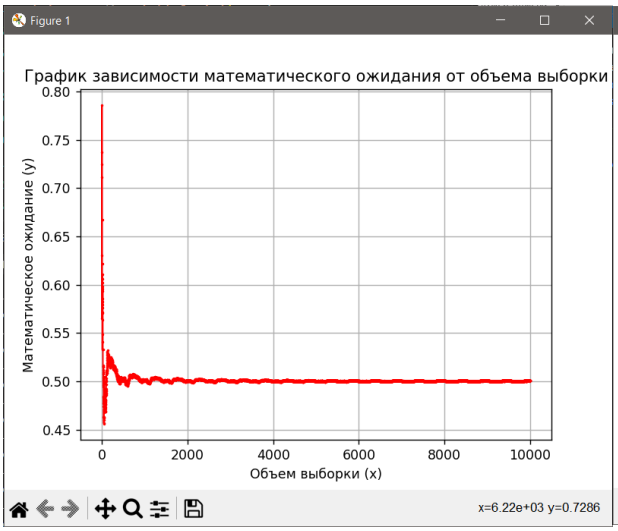
```
PS D:\tgpsch\lab> & C:/Users/kaydy/AppData/Local/Programs
/Python/Python312/python.exe d:/tgpsch/lab/lab.py -t all
-f "bbs.txt"
Мат. ожидание:  0.35632068965517244
Ср-кв. отклонение:  0.3463652116215497
Отн. погрешность мат. ожидания:  0.14297931034482758
Отн. погрешность ср-кв. отклонения:  0.058265211621549684
Критерий хи-квадрат:
->  False
Критерий серий:
->  False
Критерий интервалов:
->  False
Критерий разбиений:
->  True
Критерий перестановок:
->  False
Критерий монотонности:
->  False
Критерий конфликтов:
->  False
PS D:\tgpsch\lab>
```

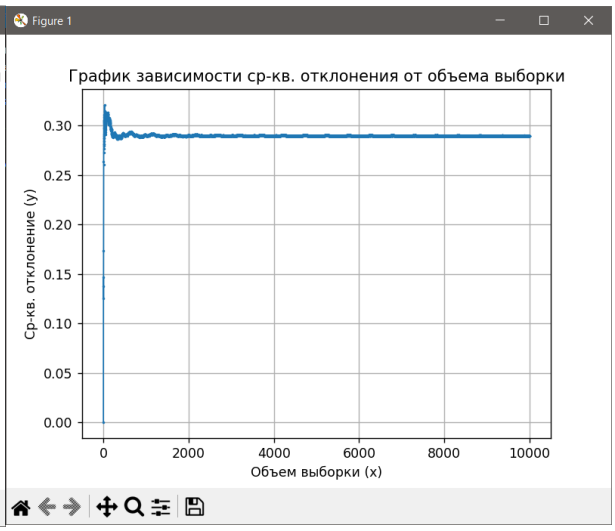




3.4 Линейно-конгруэнтный метод

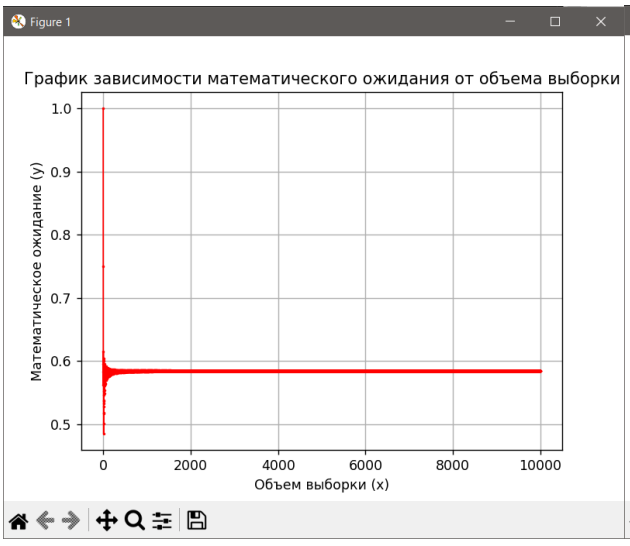
```
PS D:\tgpsch\lab> & C:/Users/kaydy/AppData/Local/Programs
/Python/Python312/python.exe d:/tgpsch/lab/lab.py -t all
-f "lc.txt"
Мат. ожидание:  0.5003791270410097
Ср-кв. отклонение:  0.28955577313965425
Отн. погрешность мат. ожидания:  0.0010791270410097087
Отн. погрешность ср-кв. отклонения:  0.0014557731396542262
Критерий хи-квадрат:
->  True
Критерий серий:
->  False
Критерий интервалов:
->  True
Критерий разбиений:
->  True
Критерий перестановок:
->  True
Критерий монотонности:
->  True
Критерий конфликтов:
->  False
PS D:\tgpsch\lab>
```

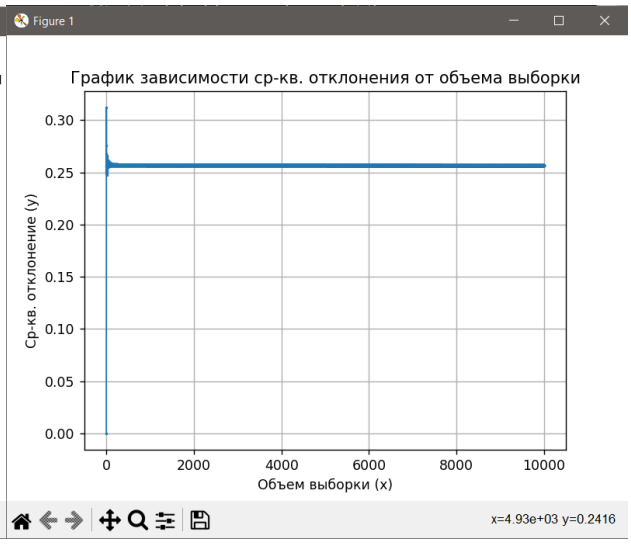




3.5 РСЛОС

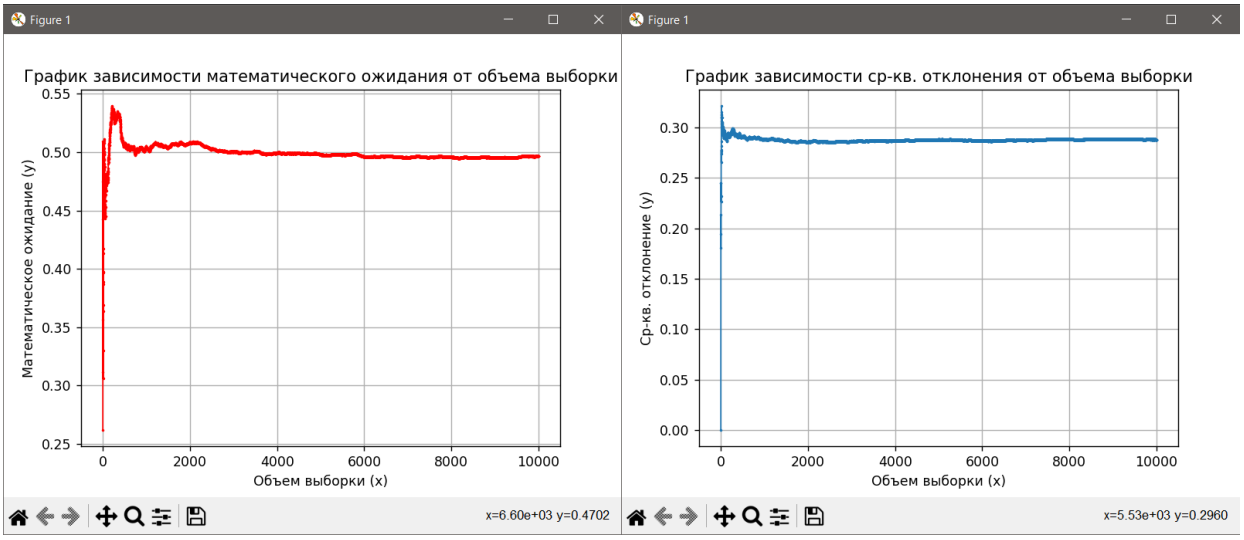
```
PS D:\tgpsch\lab> & C:/Users/kaydy/AppData/Local/Programs
/Python/Python312/python.exe d:/tgpsch/lab/lab.py -t all
-f "lfsr.txt"
Мат. ожидание:  0.5845714285714286
Ср-кв. отклонение:  0.2567775182479008
Отн. погрешность мат. ожидания:  0.08527142857142861
Отн. погрешность ср-кв. отклонения:  0.03132248175209923
Критерий хи-квадрат:
->  True
Критерий серий:
->  False
Критерий интервалов:
->  False
Критерий разбиений:
->  True
Критерий перестановок:
->  False
Критерий монотонности:
->  False
Критерий конфликтов:
->  False
PS D:\tgpsch\lab>
```





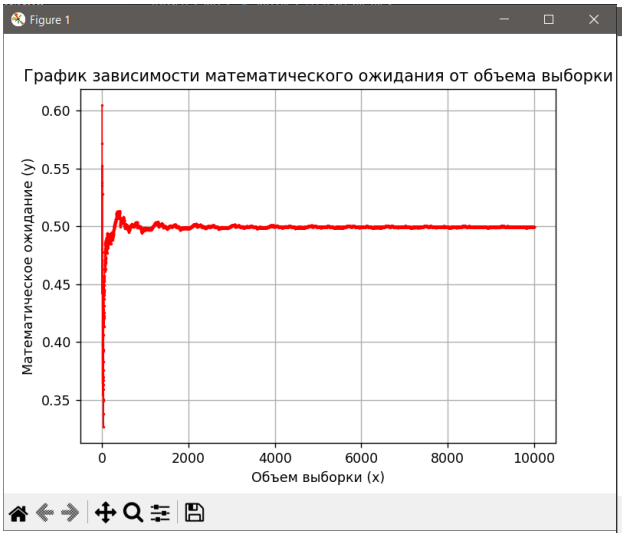
3.6 Вихрь Мерсенна

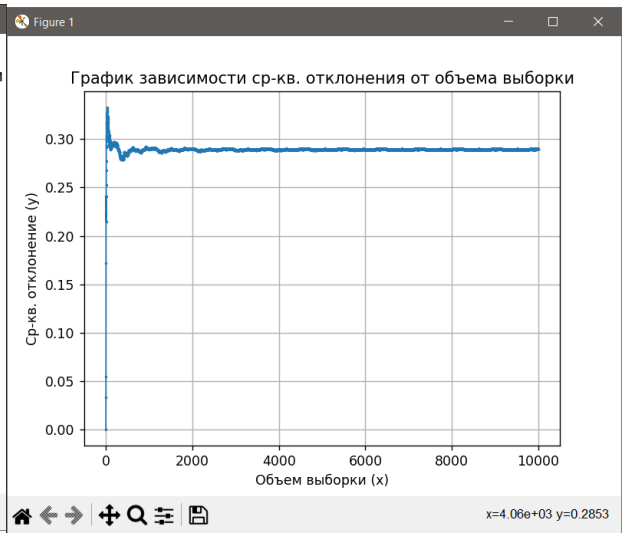
```
PS D:\tgpsch\lab> & C:/Users/kaydy/AppData/Local/Programs
/Python/Python312/python.exe d:/tgpsch/lab/lab.py -t all
-f "mt.txt"
Мат. ожидание:  0.4968078201368524
Ср-кв. отклонение:  0.2879432278493098
Отн. погрешность мат. ожидания:  0.0024921798631476477
Отн. погрешность ср-кв. отклонения:  0.0001567721506902097
8
Критерий хи-квадрат:
->  True
Критерий серий:
->  False
Критерий интервалов:
->  True
Критерий разбиений:
->  True
Критерий перестановок:
->  True
Критерий монотонности:
->  True
Критерий конфликтов:
->  False
PS D:\tgpsch\lab>
```



3.7 Нелинейная комбинация РСЛОС

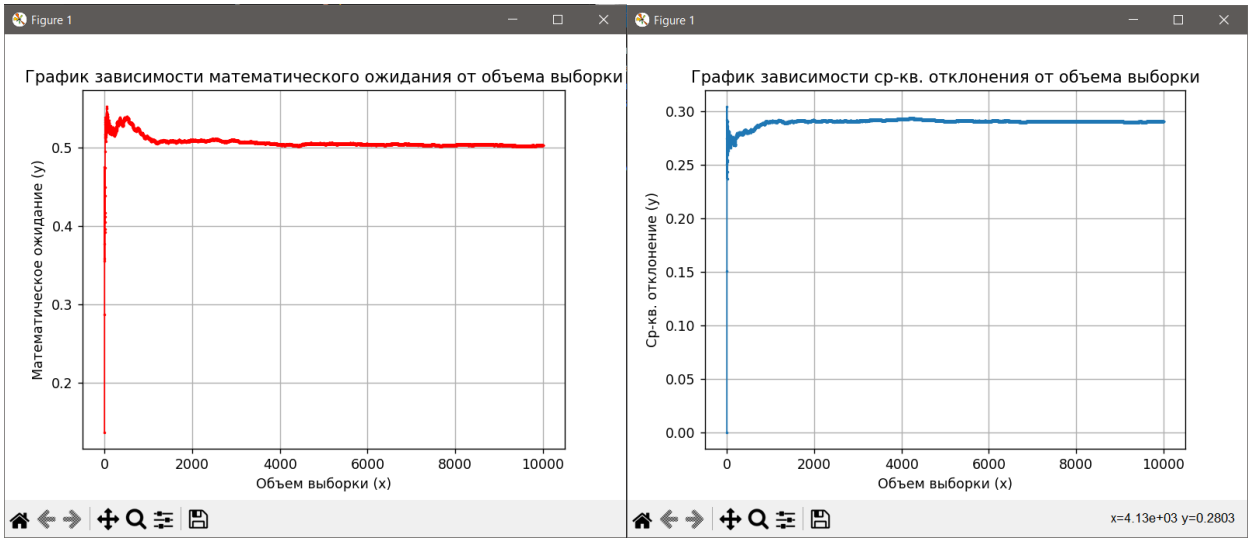
```
PS D:\tgpsch\lab> & C:/Users/kaydy/AppData/Local/Programs
/Python/Python312/python.exe d:/tgpsch/lab/lab.py -t all
-f "nfsr.txt"
Мат. ожидание:  0.499318590998043
Ср-кв. отклонение:  0.2896113931558169
Отн. погрешность мат. ожидания:  1.85909980429666e-05
Отн. погрешность ср-кв. отклонения:  0.0015113931558816887
Критерий хи-квадрат:
->  False
Критерий серий:
->  False
Критерий интервалов:
->  True
Критерий разбиений:
->  True
Критерий перестановок:
->  True
Критерий монотонности:
->  False
Критерий конфликтов:
->  False
PS D:\tgpsch\lab>
```





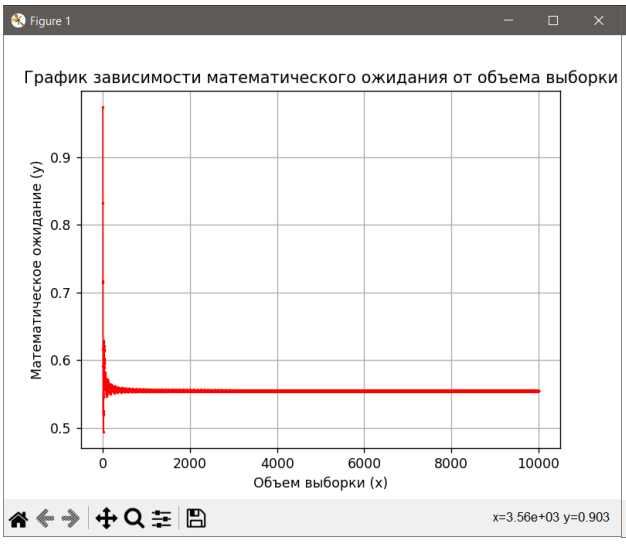
3.8 RC4

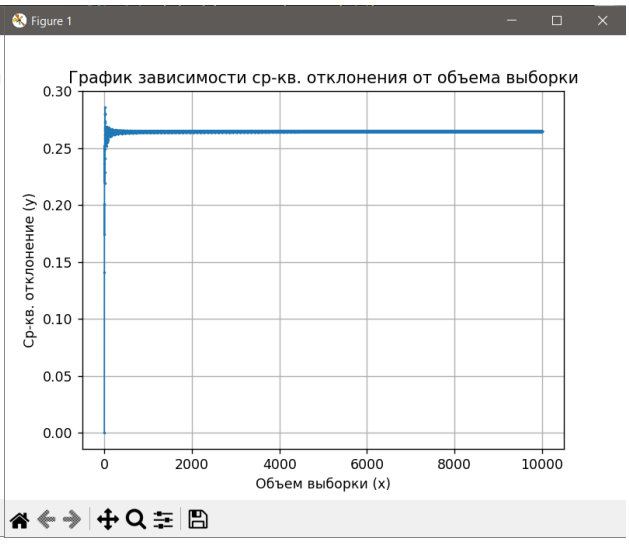
```
PS D:\tgpsch\lab> & C:/Users/kaydy/AppData/Local/Programs
/Python/Python312/python.exe d:/tgpsch/lab/lab.py -t all
-f "rc4.txt"
Мат. ожидание:  0.5029059584859585
Ср-кв. отклонение:  0.29050370937820047
Отн. погрешность мат. ожидания:  0.0036059584859516
Отн. погрешность ср-кв. отклонения:  0.0024037093782004 47
Критерий хи-квадрат:
->  True
Критерий серий:
->  False
Критерий интервалов:
->  True
Критерий разбиений:
->  True
Критерий перестановок:
->  True
Критерий монотонности:
->  True
Критерий конфликтов:
->  False
PS D:\tgpsch\lab>
```



3.9 RSA

```
PS D:\tgpsch\lab> & C:/Users/kaydy/AppData/Local/Programs
/Python/Python312/python.exe d:/tgpsch/lab/lab.py -t all
-f "rsa.txt"
Мат. ожидание:  0.5548032057911065
Ср-кв. отклонение:  0.2645837800142304
Отн. погрешность мат. ожидания:  0.055503205791106514
Отн. погрешность ср-кв. отклонения:  0.023516219985769637
Критерий хи-квадрат:
->  False
Критерий серий:
->  False
Критерий интервалов:
->  False
Критерий разбиений:
->  True
Критерий перестановок:
->  True
Критерий монотонности:
->  False
Критерий конфликтов:
->  False
PS D:\tgpsch\lab>
```





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	_	_	_	_	_	_	_	_	_