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

*Сергеева Сергея Евгеньевича*

фамилия, имя, отчество

Научный руководитель

Ст. преподаватель _____ И.И. Слеповичев

подпись, дата

Саратов 2024

1. Функция распределения и параметры генерации ППСЧ

В данной работе используются следующие параметры генерации ПСЧ:

ls prng.exe /g:lc 257 8 9 7

add prng.exe /g:add 257 3 7 1 2 3 4 5 6 7 8

5p prng.exe /g:5p 7 2 4 6 10 0b1001011

lfsr prng.exe /g:lfsr 0b1011011 0b1001011

nfsr prng.exe /g:nfsr 0b1001011 0b1011010 0b1001011 10 83 45 67

mt prng.exe /g:mt 1000 42

rc4 prng.exe /g:rc4 0 527 30 557 60 587 90 617 120 647 150 677 180 707 210 737 240 767 270 797 300 827 330 857 360 887 390 917 420 947 450 977 480 1007 510 13 540 43 570 73 600 103 630 133 660 163 690 193 720 223 750 253 780 283 810 313 840 343 870 373 900 403 930 433 960 463 990 493 1020 523 26 553 56 583 86 613 116 643 146 673 176 703 206 733 236 763 266 793 296 823 326 853 356 883 386 913 416 943 446 973 476 1003 506 9 53 6 39 566 69 596 99 626 129 656 159 686 189 716 219 746 249 776 279 806 309 836 339 866 369 896 399 926 429 956 459 986 4 89 1016 519 22 549 52 579 82 609 112 639 142 669 172 699 202 729 232 759 262 789 292 819 322 849 352 879 382 909 412 939 442 969 472 999 502 5 532 35 562 65 592 95 622 125 652 155 682 185 712 215 742 245 772 275 802 305 832 335 862 365 892 395 922 425 952 455 982 485 1012 515 18 545 48 575 78 605 108 635 138 665 168 695 198 725 228 755 258 785 288 815 318 845 348 875 378 905 408 935 438 965 468 995 498 1 528 31 558 61 588 91 618 121 648 151 678 181 708 211 738 241

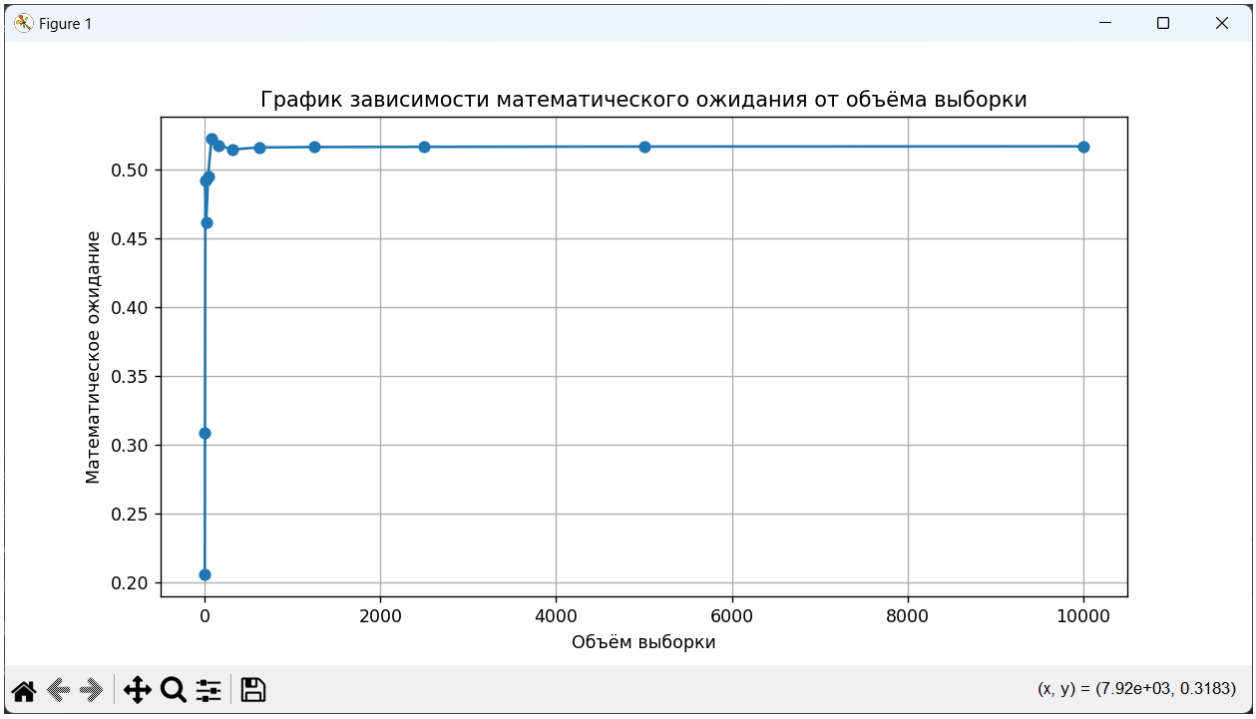
rsa prng.exe /g:rsa 308242199054357914579984950 79 17 10 11

bbs prng.exe /g:bbs 17

## 2. Точечные оценки параметров ППСЧ

### 2.1. Линейно-конгруэнтный метод

- Математическое ожидание: 0.517142857142869
- Среднеквадратичное отклонение: 0.3173517165977447
- Относительная погрешность математического ожидания: 0.017142857142869006
- Относительная погрешность среднеквадратичного отклонения: 0.037351716597744666



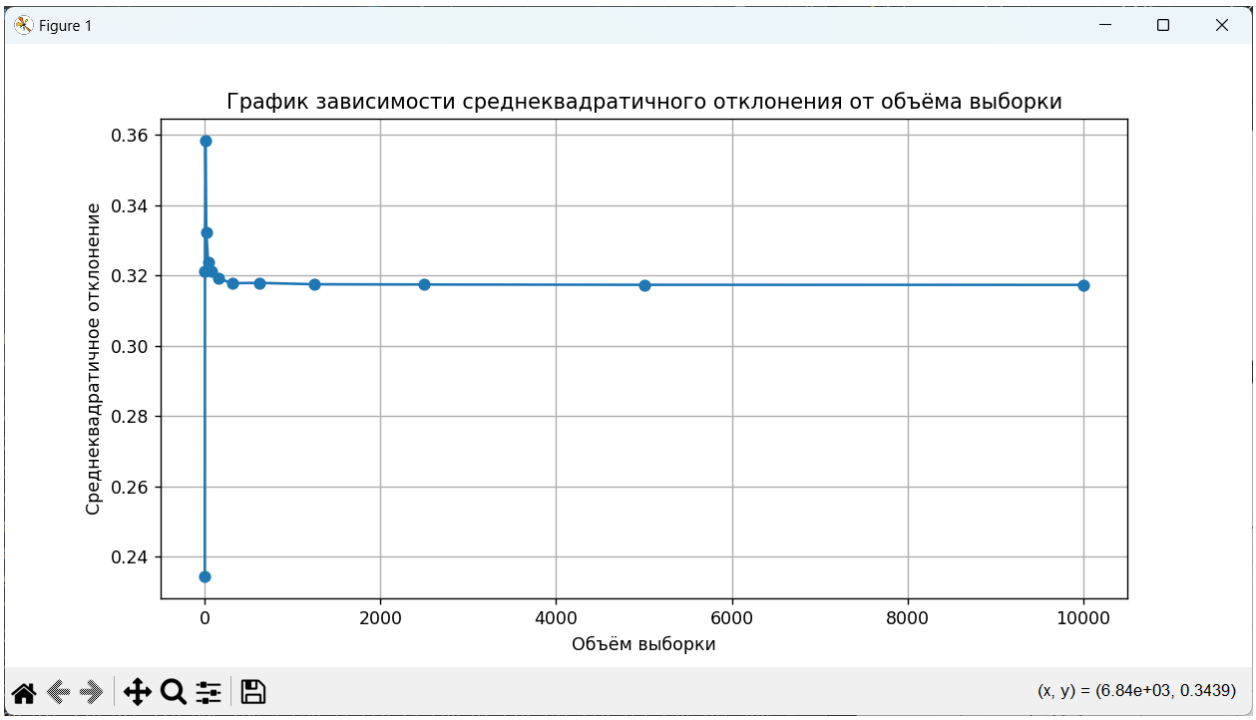
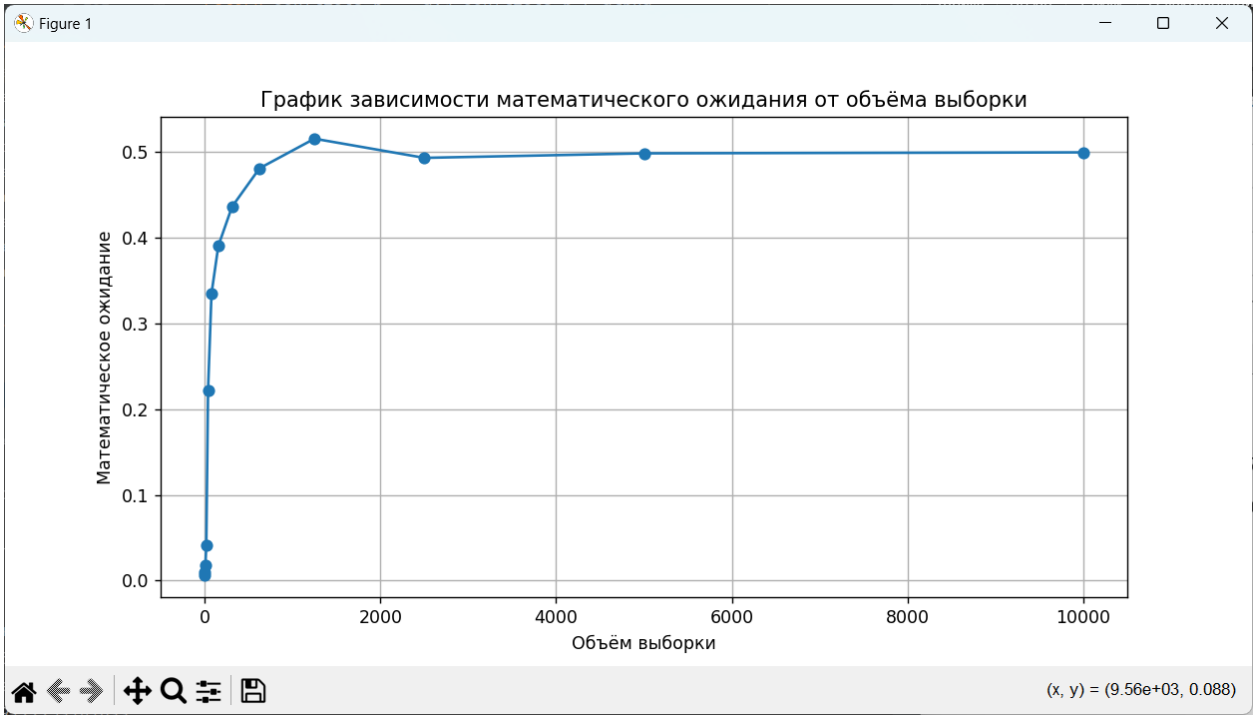
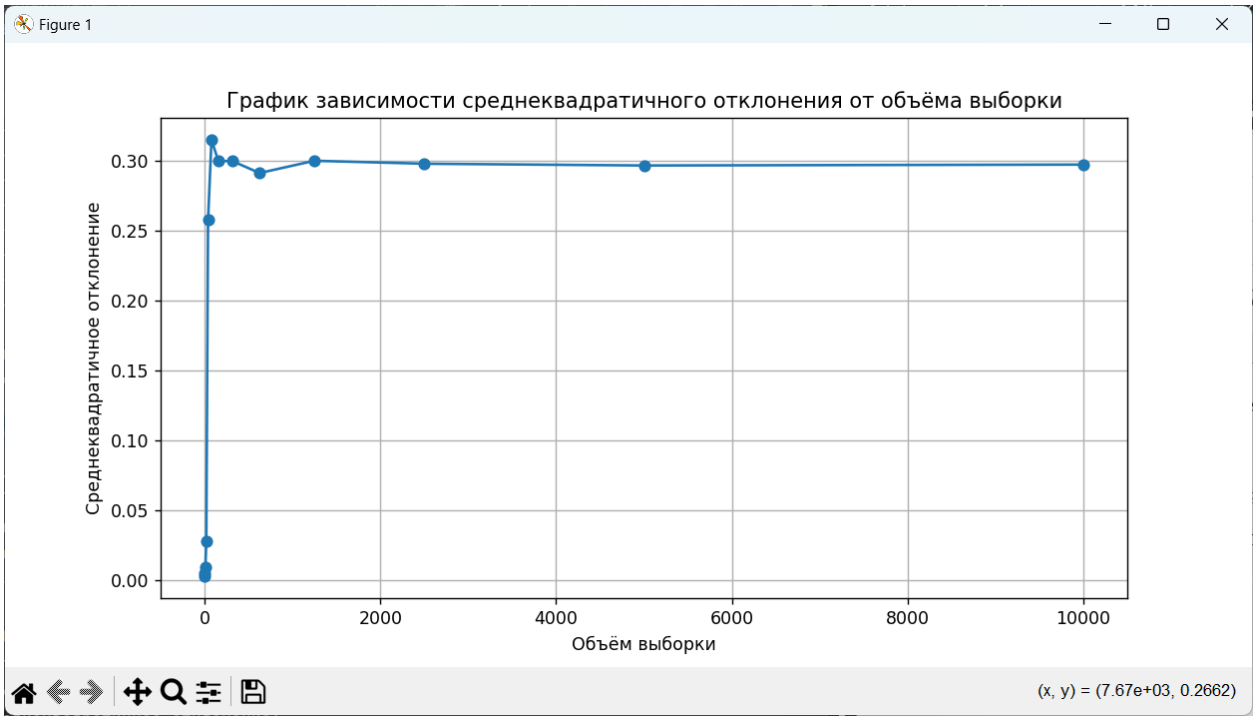


Figure 1
График зависимости среднеквадратичного отклонения от объёма выборки
Среднеквадратичное отклонение
0.36
0.34
0.32
0.30
0.28
0.26
0.24
0
2000
4000
6000
8000
10000
Объём выборки
(x, y) = (6.84e+03, 0.3439)

2.2. Аддитивный метод

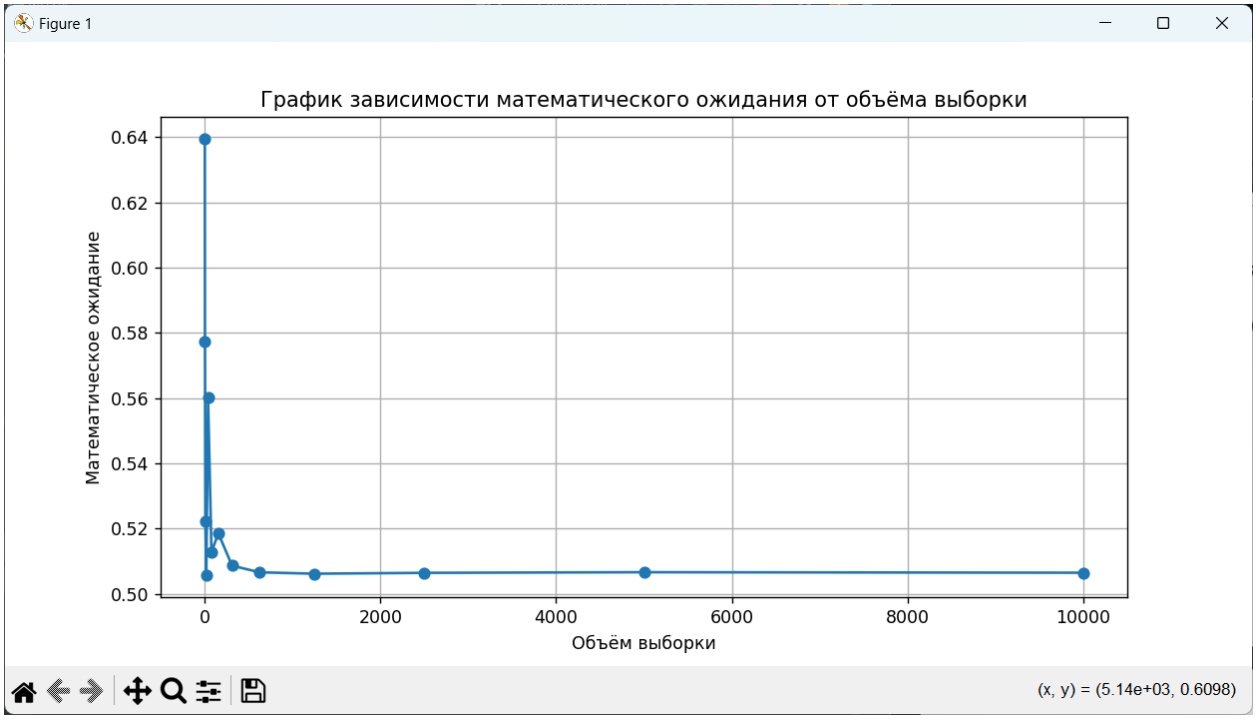
- Математическое ожидание: 0.49955719844358043
- Среднеквадратичное отклонение: 0.2969722239747699
- Относительная погрешность математического ожидания: 0.00044280155641956975
- Относительная погрешность среднеквадратичного отклонения: 0.016972223974769884

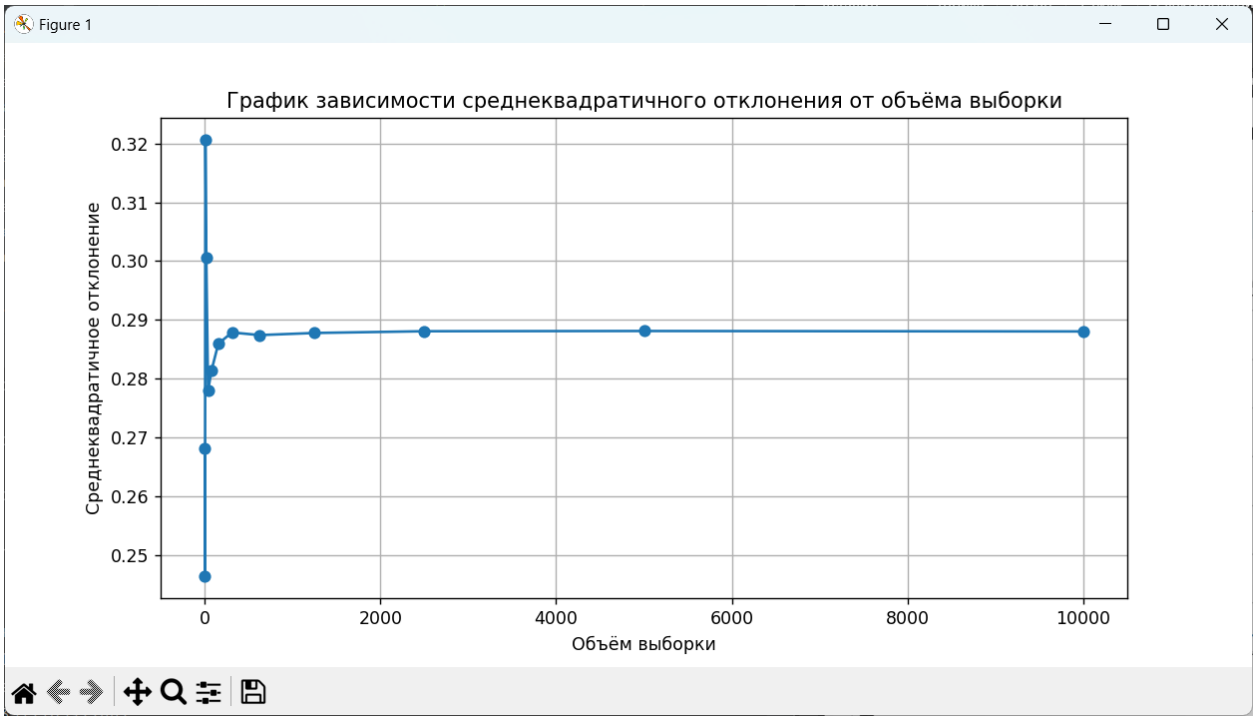


2.3. Пятипараметрический метод

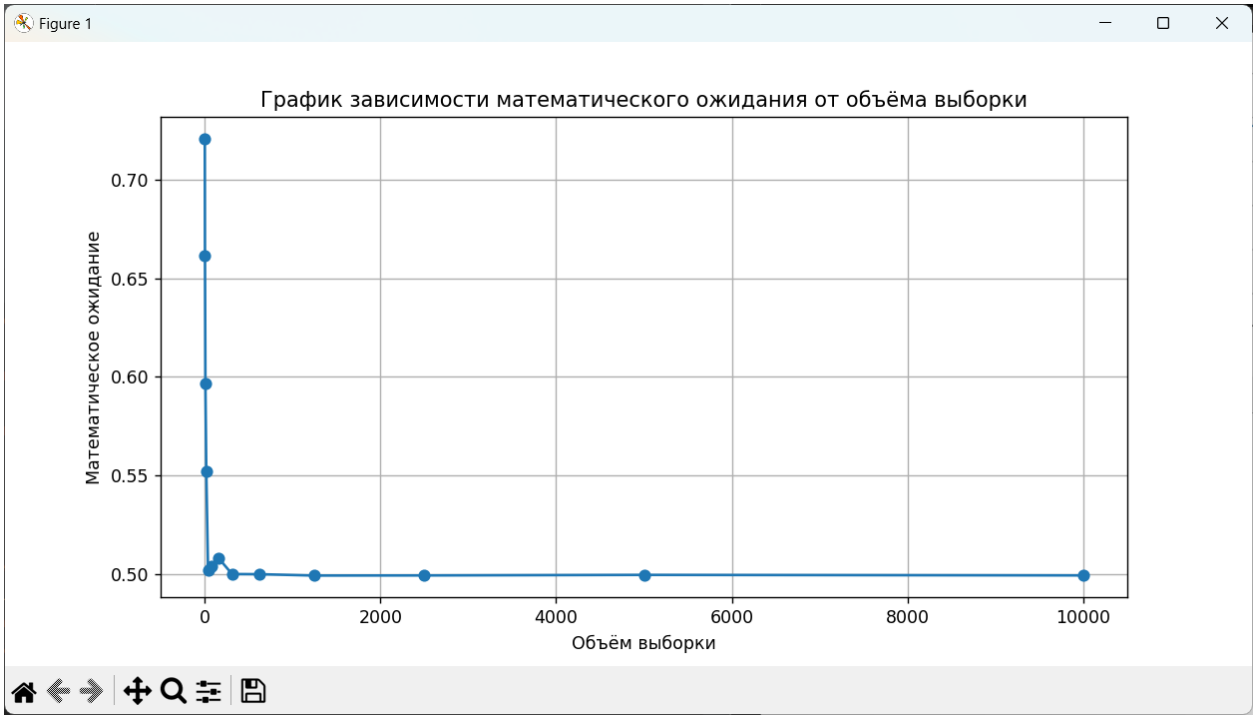
- Математическое ожидание: 0.5064516699410613
- Среднеквадратичное отклонение: 0.2880326519325355
- Относительная погрешность математического ожидания: 0.006451669941061278
- Относительная погрешность среднеквадратичного отклонения: 0.008032651932535495

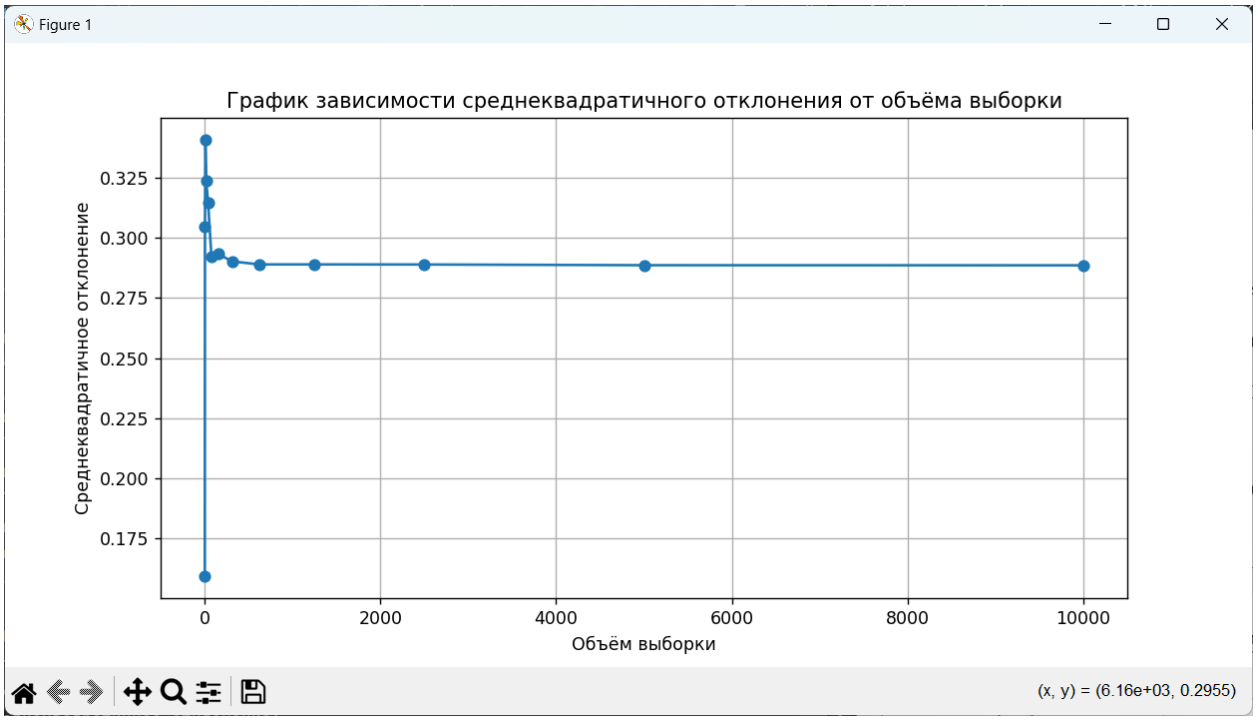


## 2.4. РСЛОС

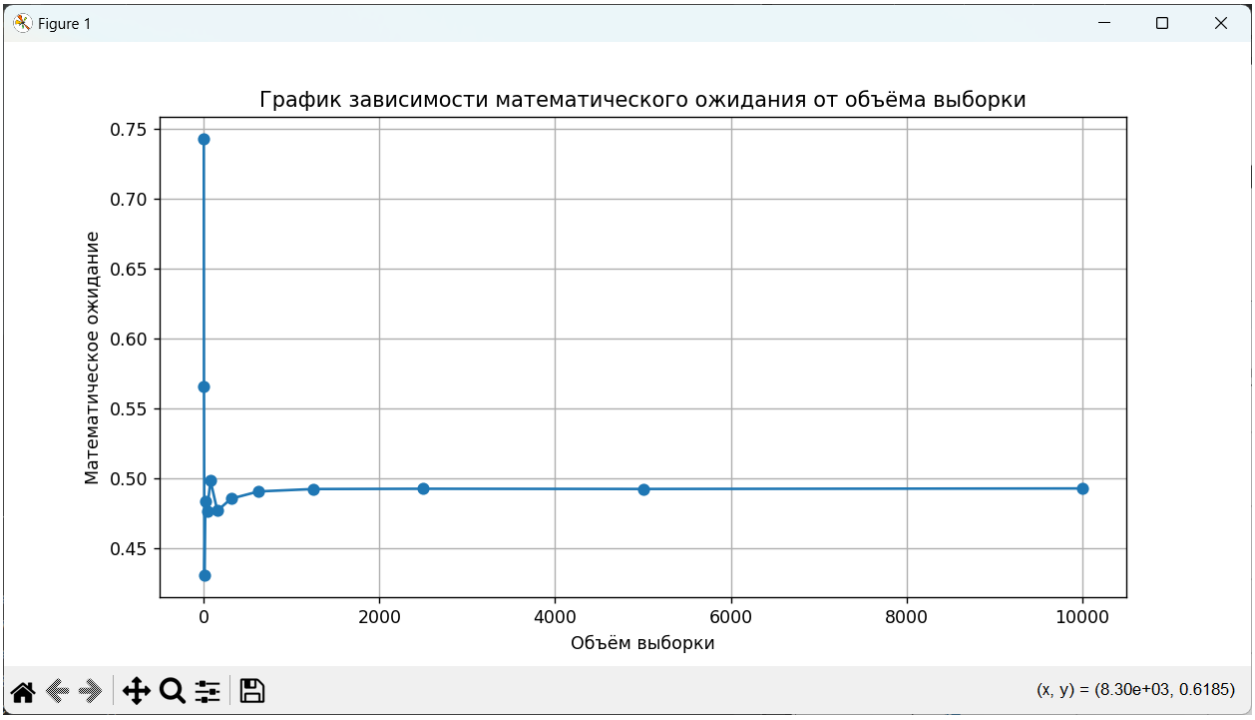
- Математическое ожидание: 0.4993764880952112
- Среднеквадратичное отклонение: 0.2885454697784817
- Относительная погрешность математического ожидания: 0.0006235119047888205
- Относительная погрешность среднеквадратичного отклонения: 0.008545469778481696

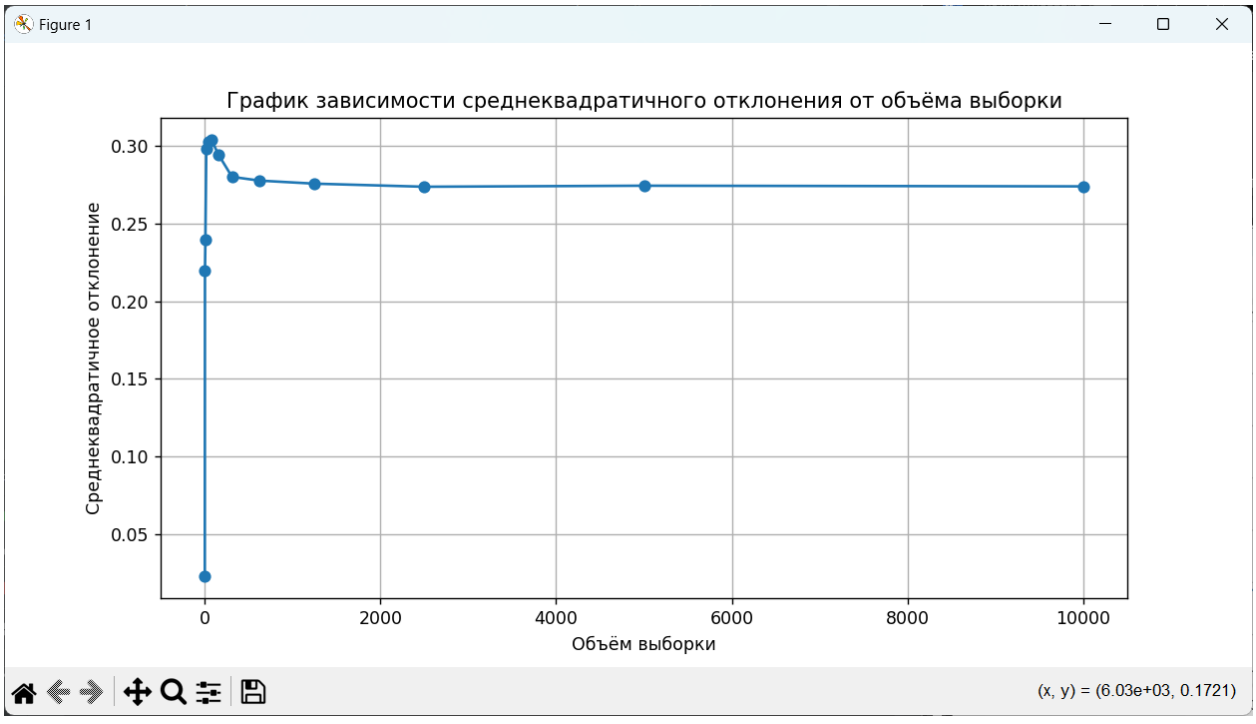


2.5. Нелинейная комбинация РСЛОС

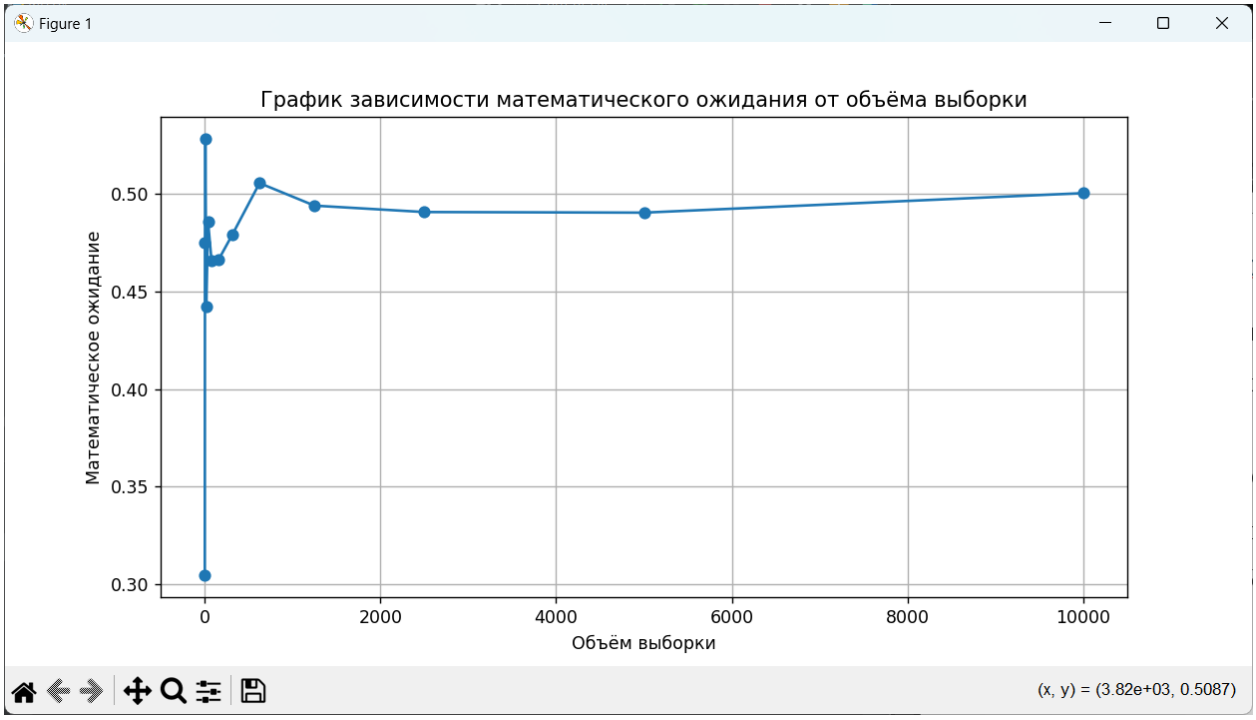
- Математическое ожидание: 0.49288779296875
- Среднеквадратичное отклонение: 0.2738668715008529
- Относительная погрешность математического ожидания: 0.007112207031249984
- Относительная погрешность среднеквадратичного отклонения: 0.0061331284991471

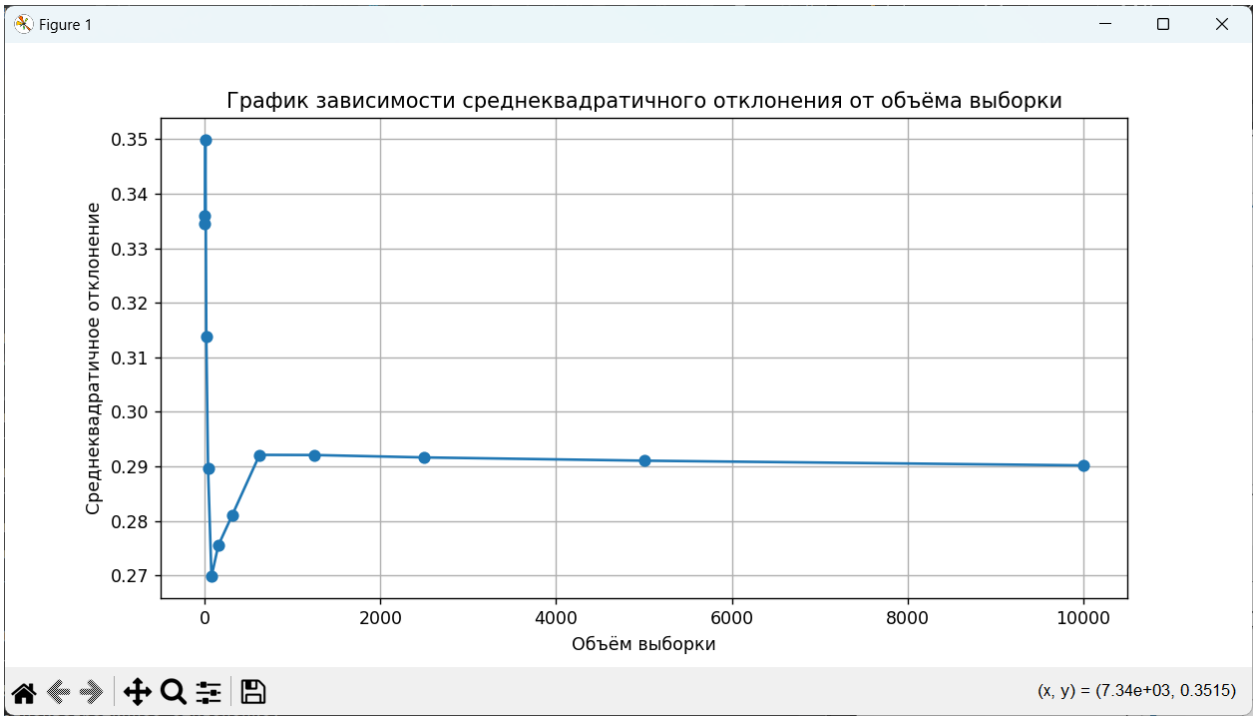


2.6. Вихрь Мерсенна

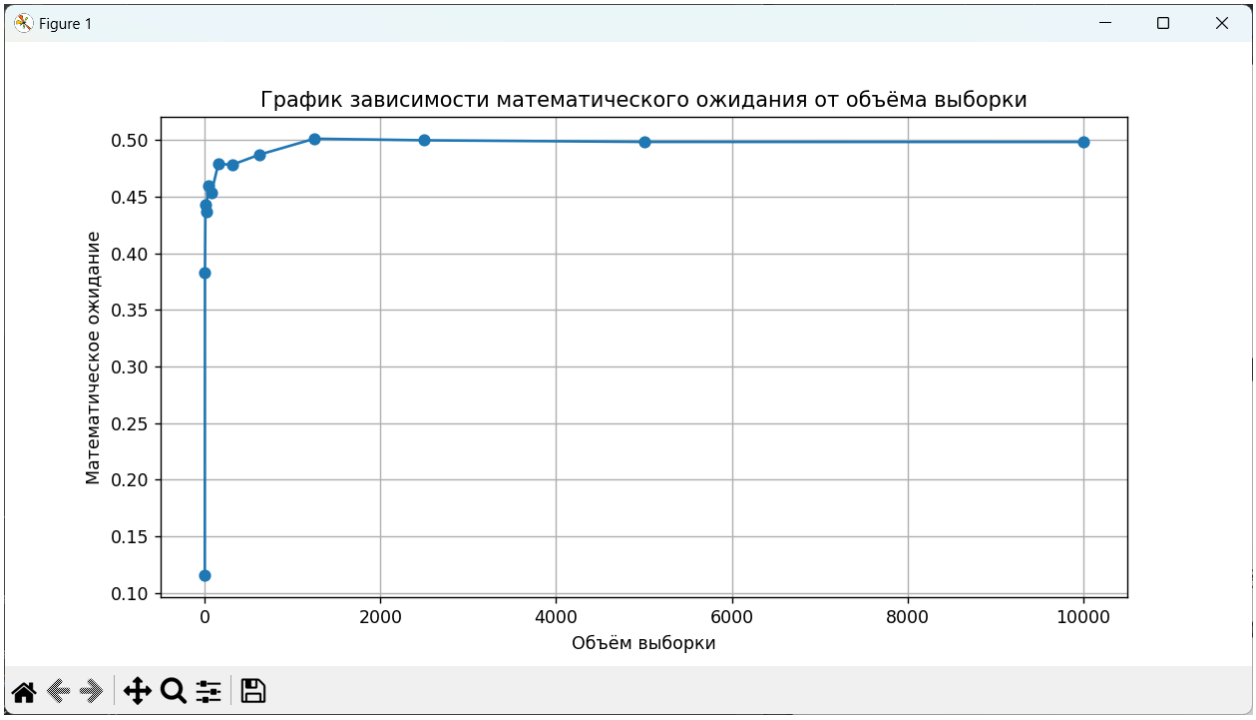
- Математическое ожидание: 0.5003483
- Среднеквадратичное отклонение: 0.2901646617701823
- Относительная погрешность математического ожидания: 0.0003482999999999681
- Относительная погрешность среднеквадратичного отклонения: 0.01016466177018227

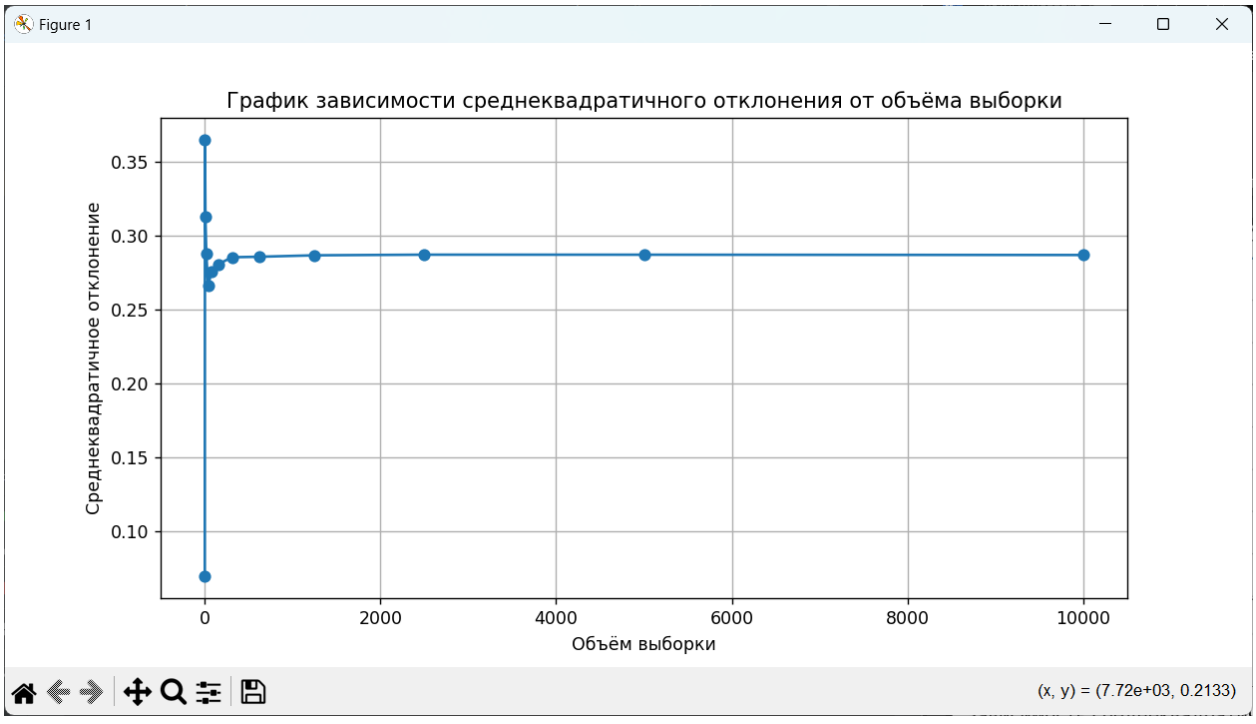


2.7. RC4

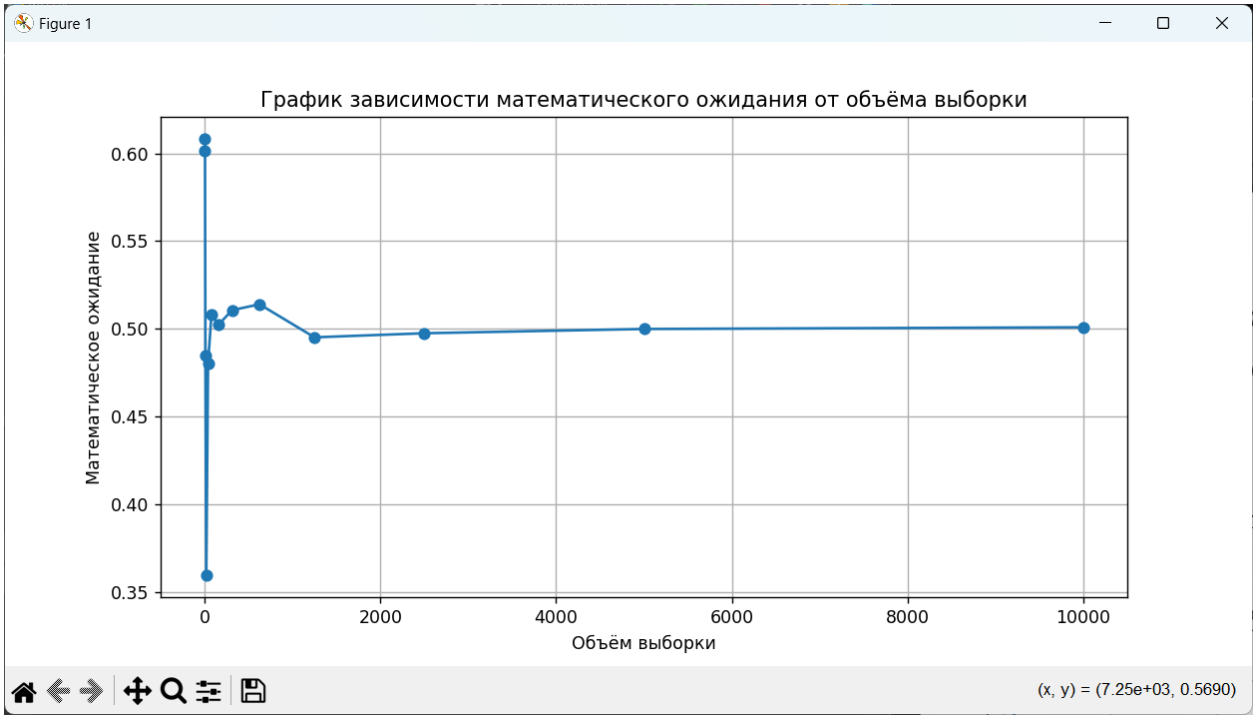
- Математическое ожидание: 0.49845
- Среднеквадратичное отклонение: 0.28672543766928854
- Относительная погрешность математического ожидания: 0.0015499999999999958
- Относительная погрешность среднеквадратичного отклонения: 0.006725437669288514

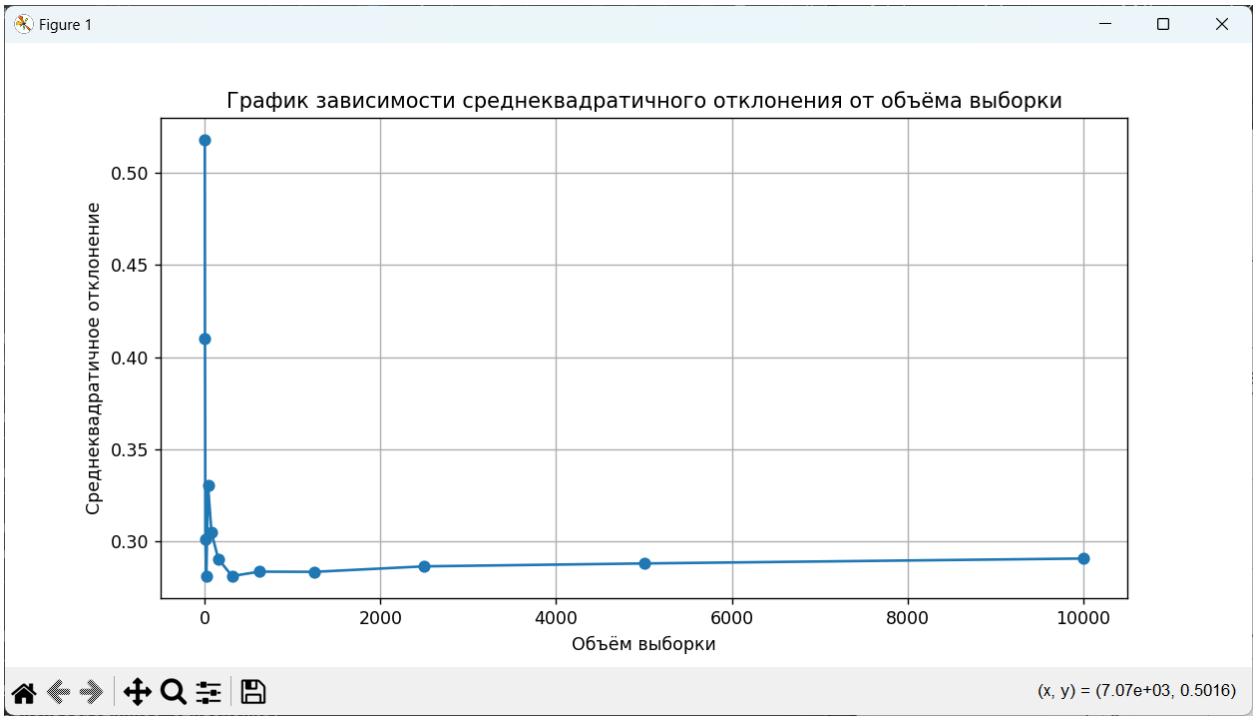


2.8. ГПСЧ на основе RSA

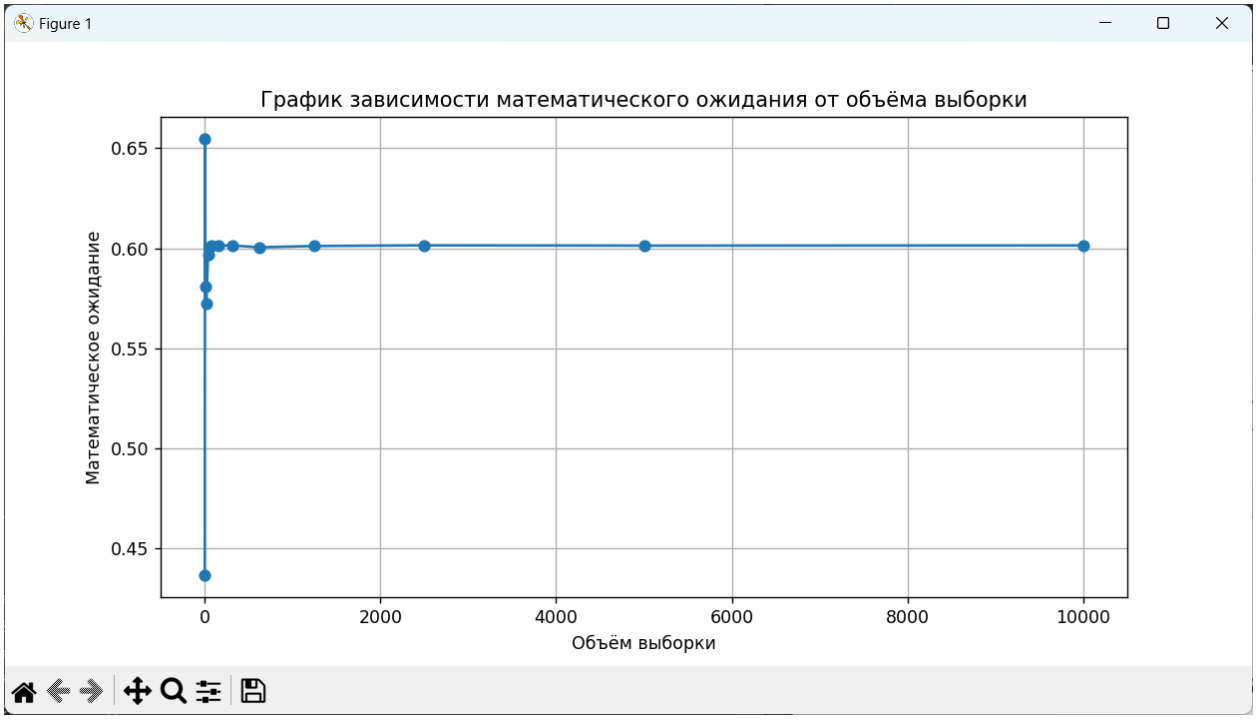
- Математическое ожидание: 0.50082900390625
- Среднеквадратичное отклонение: 0.29081600826446796
- Относительная погрешность математического ожидания: 0.0008290039062499588
- Относительная погрешность среднеквадратичного отклонения: 0.010816008264467936

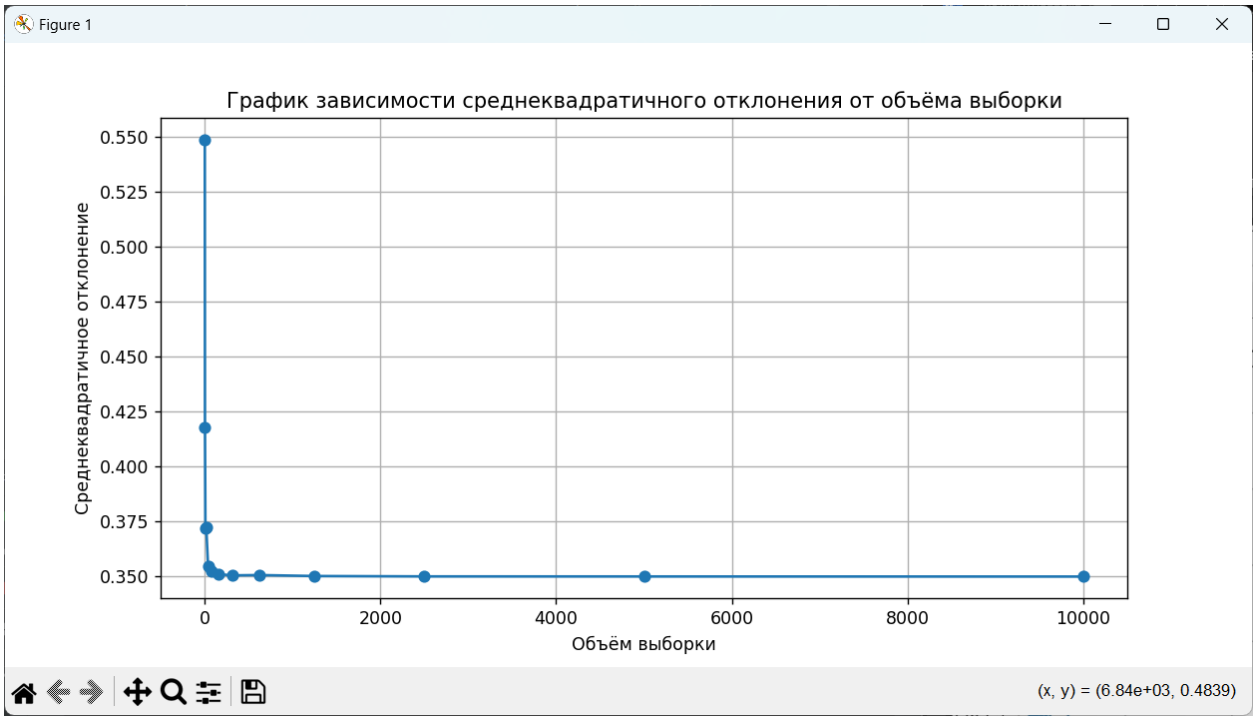


2.9. Блюма-Блюма-Шуба

- Математическое ожидание: 0.6014322751322828
- Среднеквадратичное отклонение: 0.34965371866047656
- Относительная погрешность математического ожидания: 0.10143227513228281
- Относительная погрешность среднеквадратичного отклонения: 0.06965371866047654



3. Результаты проверки точечных оценок и критериев ППСЧ

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