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

Дусалиева Тахира Ахатовича

фамилия, имя, отчество

Научный руководитель

Ст. преподаватель _____ И.И. Слеповичев

подпись, дата

Саратов 2023

1. Параметры генерации

В данной лабораторной работе используются следующие параметры генерации последовательностей ПСЧ.

- /g:lc /i:2147483647,48271,0,350 /n:10000 /m:1024 /f:rnd_lc.dat
- /g:add /i:100,24,55,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55 /n:10000 /m:1024 /f:rnd_add.dat
- /g:5p /i:89,20,40,69,1024,61593000964469013744936311 1 /n:10000 /m:1024 /f:rnd_5p.dat
- /g:lfsr /i:1000001010011,1110101001001 /n:10000 /m:1024 /f:rnd_lfsr.dat
- /g:nfsr /i:1000001010011,1000000000000011,100011101,1024,7497,49311,345 /n:10000 /m:1024 /f:rnd_nfsr.dat
- /g:mt /i:4096,25 /n:10000 /m:1024 /f:rnd_mt.dat
- /g:rc4 /i:3179,3298,3097,2987,2258,2437,195,583,1623,2324,1886,3533,1935,254,1697,2568,2181,2266,3523,3830,535,3541,1025,2103,290,3932,3481,909,4047,2991,2586,129,2338,1775,706,1232,2149,3662,2979,175,3241,2746,431,1137,2249,806,3589,22,2536,3305,3375,844,4047,3642,3293,3153,2464,437,488,3122,2235,771,828,3208,2879,3482,2070,1233,11,1985,2594,1762,3934,642,2227,3319,1403,2038,4071,3533,1740,3480,2488,2788,2784,890,264,163,4012,662,762,1410,2948,1937,2593,369,2871,1094,1347,4041,1516,3187,2897,3381,342,1125,1350,512,3698,1854,692,2027,1682,3734,4003,753,1349,20,2203,3273,3287,3889,458,691,2666,2126,617,2832,142,2853,3938,843,2352,2377,435,1051,1383,4070,3333,1726,1382,3098,2874,2303,2592,2034,874,3591,2833,1628,3144,3702,2086,3820,783,966,4039,1654,3876,3345,3243,3645,49,1549,22,1945,3010,2182,3350,3038,3687,1545,3194,1693,3793,3947,3254,3438,1337,2986,1500,1970,1130,2007,2477,3272,2090,746,2576,78,1204,3821,2162,1001,3963,2814,273,2751,419,735,175,1385,1844,63,264,1379,2546,3196,863,1

185,3727,3353,662,1172,2545,2122,1470,2940,1036,3108,3717,1266,2252,2540,2065,993,2492,1469,187,2773,4091,2432,2003,509,1930,2326,2440,2882,2673,562,1563,2950,367,2366,2763,3293,2654,2122,1836,4089,1000,3463,3052,9,1078,2453 /n:10000 /m:1024 /f:rnd_rc4.dat

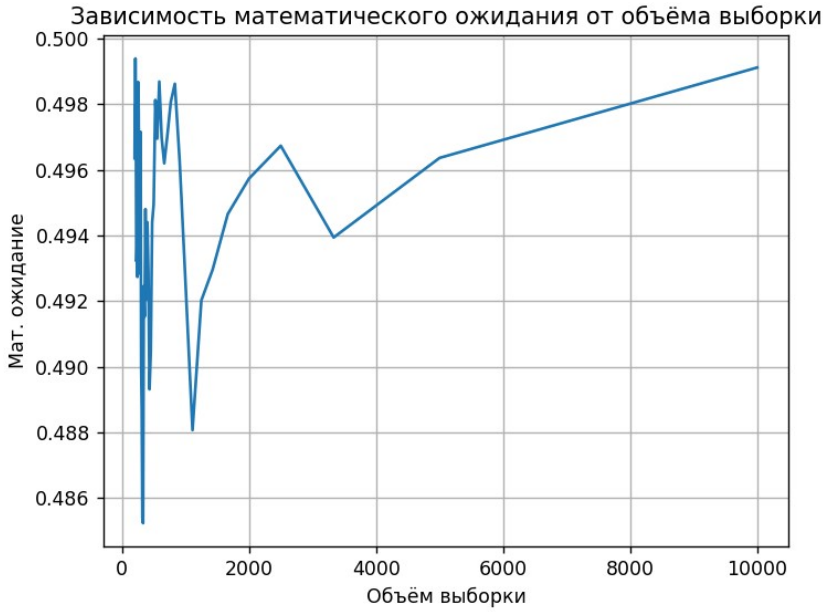
- /g:rsa /i:12709189,53,300,25 /n:10000 /m:1024 /f:rnd_rsa.dat
- /g:bbs /i:25 /n:10000 /m:1024 /f:rnd_bbs.dat

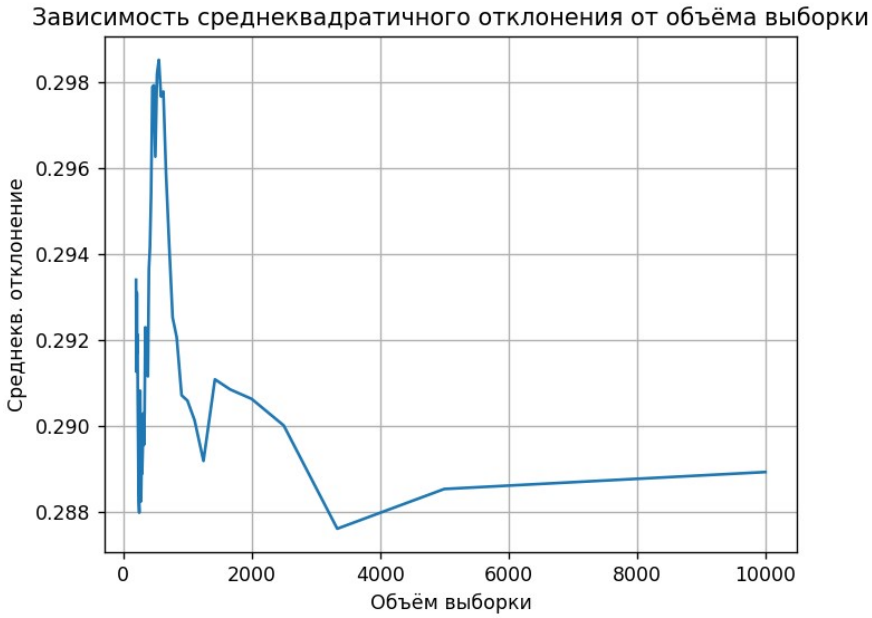
Они описаны в файле prng.sh. Если файла prng.sh не существует программа создаст свой с этими параметрами.

2. Точечные оценки параметров ППСЧ

2.1. Линейно-конгруэнтный метод

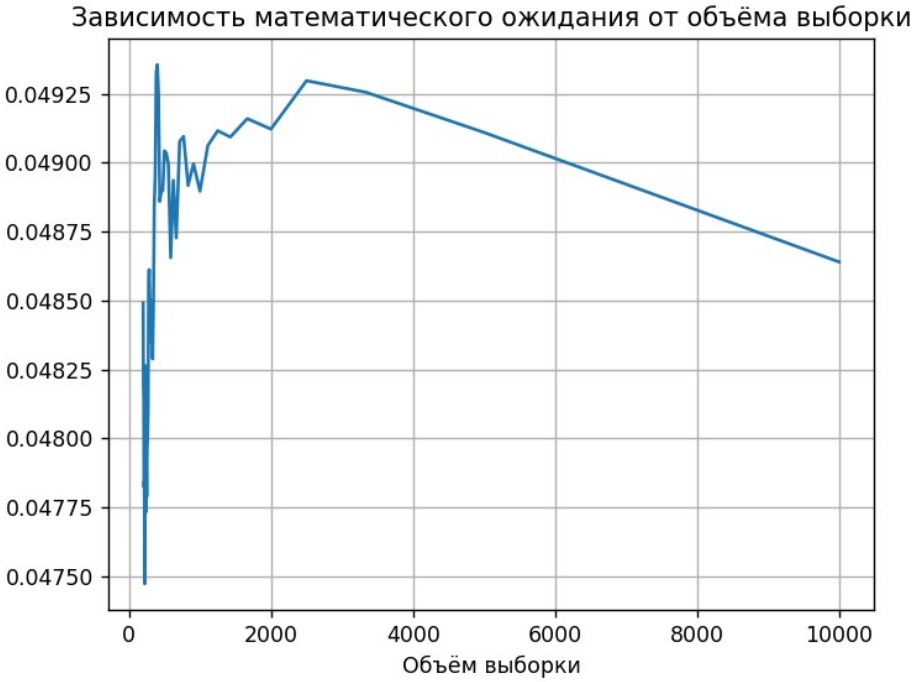
- Математическое ожидание = 0.49912109374999875
- Среднеквадратичное отклонение = 0.2889403319487144
- Относительная погрешность математического ожидания = 0.0008789062500012546
- Относительная погрешность среднеквадратичного отклонения = 0.0012403319487143682

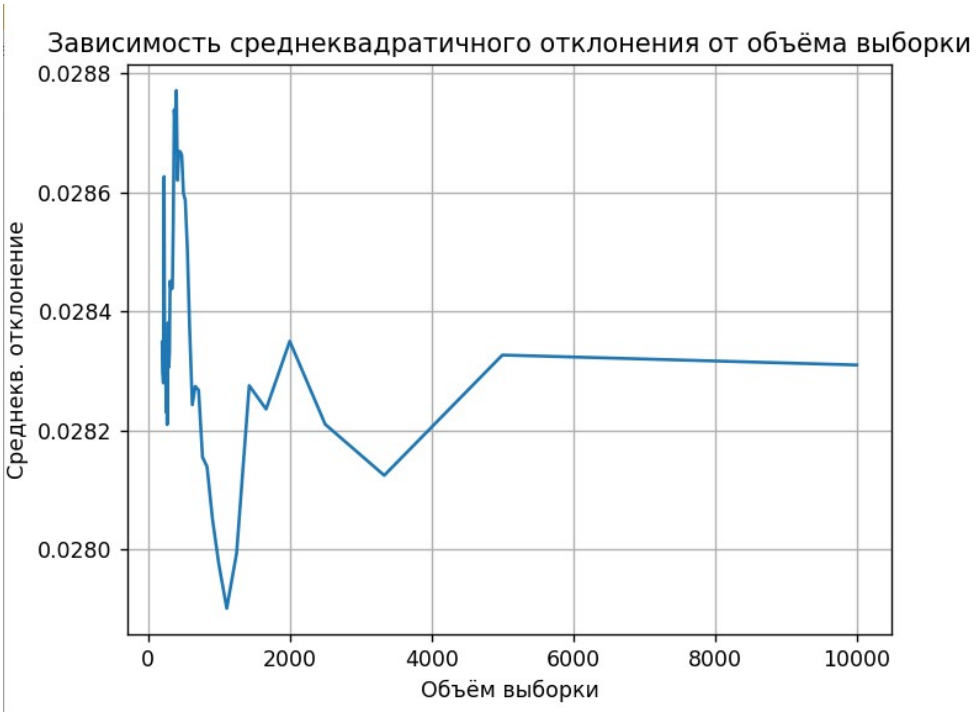




2.2. Аддитивный метод

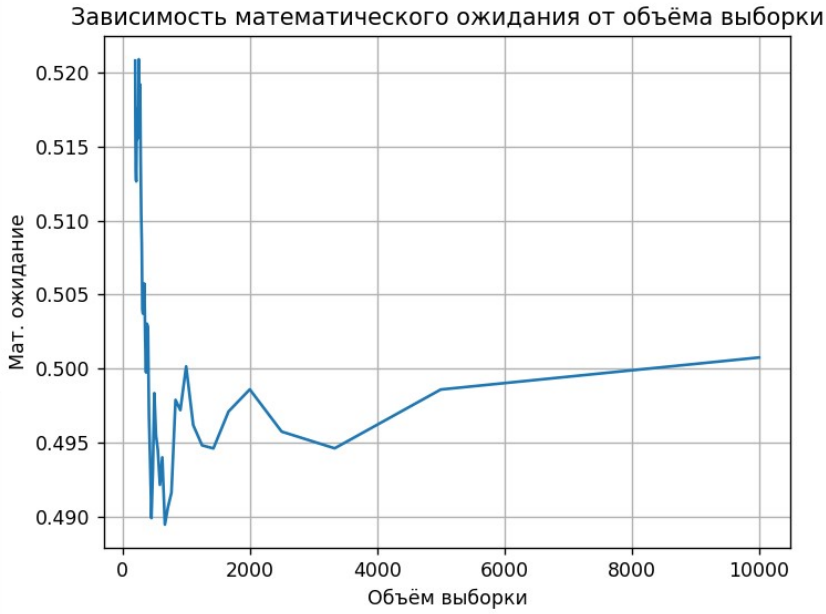
- Математическое ожидание = 0.04864003906249996
- Среднеквадратичное отклонение = 0.028309917024593793
- Относительная погрешность математического ожидания = 0.4513599609375
- Относительная погрешность среднеквадратичного отклонения = 0.2593900829754062





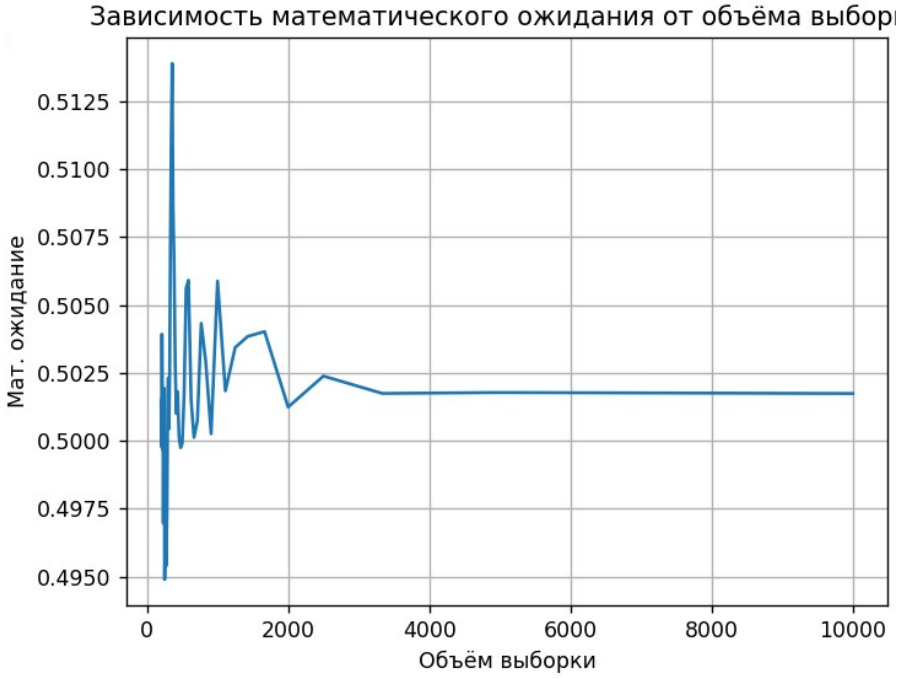
2.3. Пятипараметрический метод

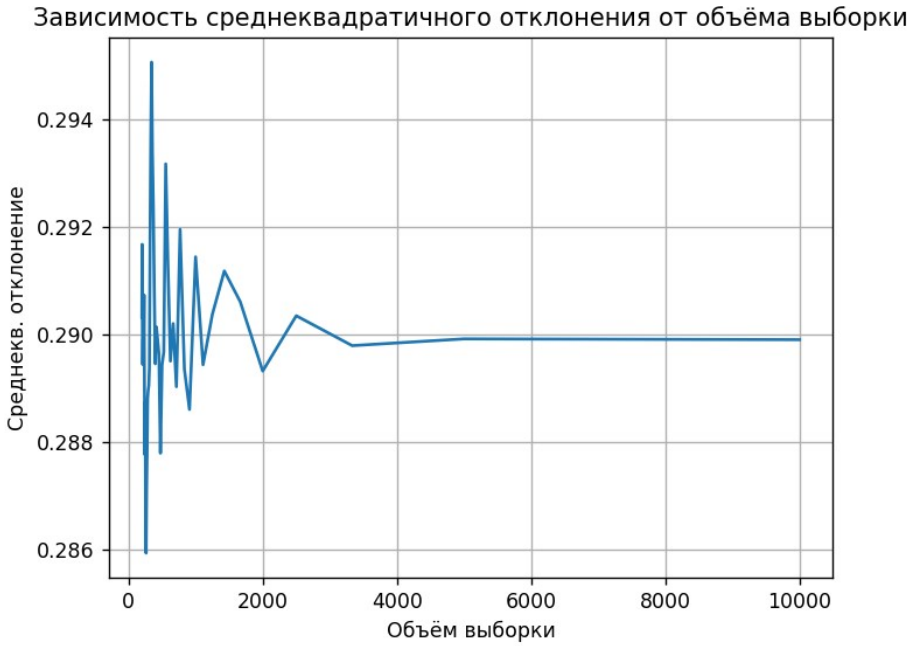
- Математическое ожидание = 0.500749609374999
- Среднеквадратичное отклонение = 0.2908220777022537
- Относительная погрешность математического ожидания = 0.0007496093749990163
- Относительная погрешность среднеквадратичного отклонения = 0.0031220777022537005



2.4. РСЛОС

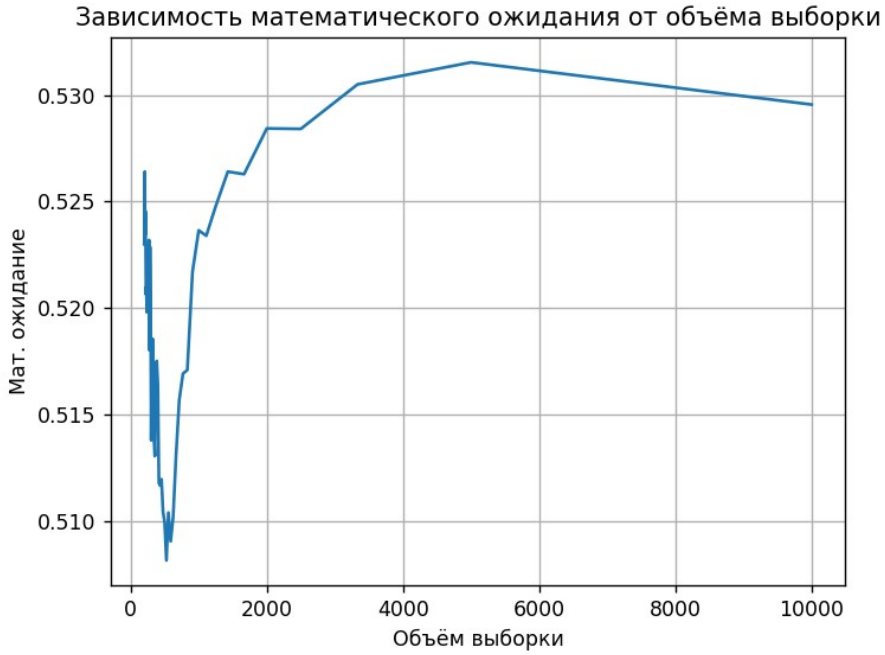
- Математическое ожидание = 0.5017422851562475
- Среднеквадратичное отклонение = 0.28990858920748286
- Относительная погрешность математического ожидания = 0.001742285156247525
- Относительная погрешность среднеквадратичного отклонения = 0.0022085892074828473

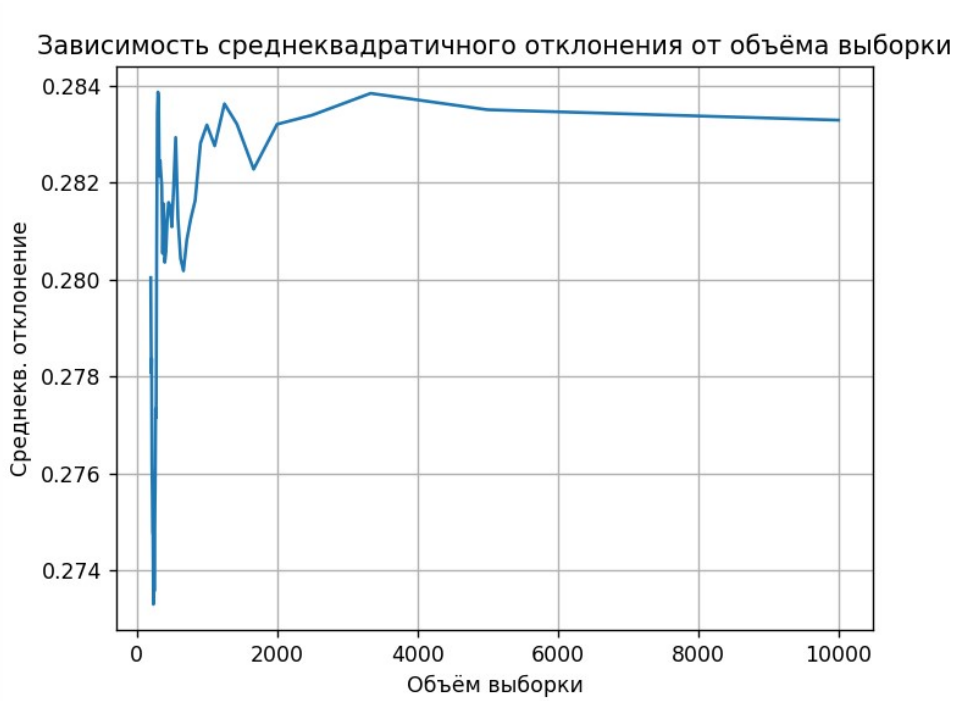




2.5. Нелинейная комбинация РСЛОС

- Математическое ожидание = 0.5295584960937546
- Среднеквадратичное отклонение = 0.28329466282224963
- Относительная погрешность математического ожидания = 0.029558496093754605
- Относительная погрешность среднеквадратичного отклонения = 0.004405337177750379





2.6. Вихрь Мерсенна

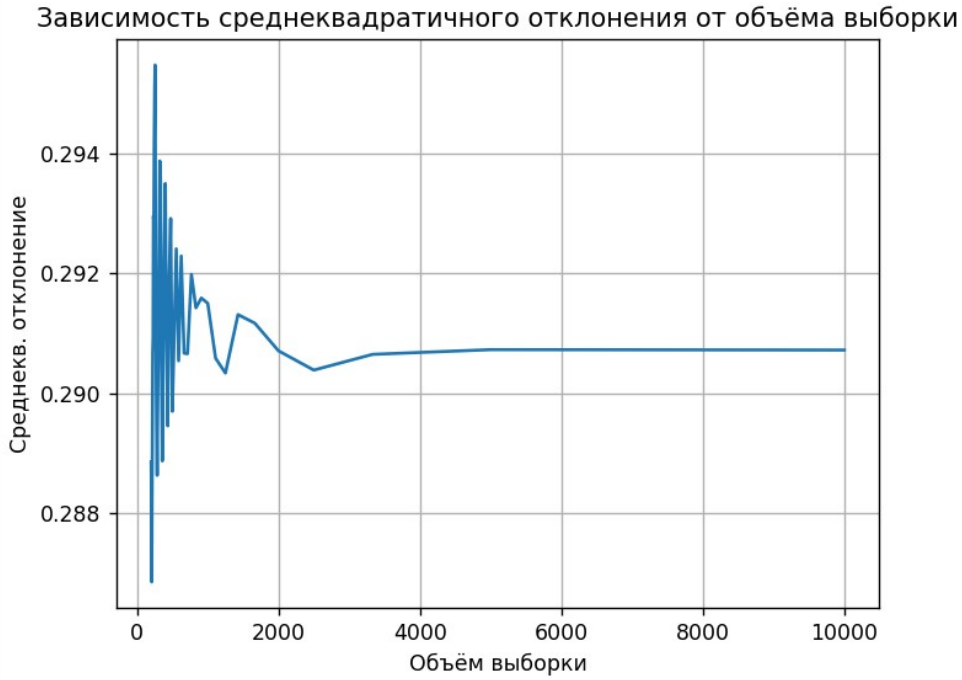
- Математическое ожидание = 0.5005868164062496
- Среднеквадратичное отклонение = 0.2880121625265761
- Относительная погрешность математического ожидания = 0.0005868164062495795
- Относительная погрешность среднеквадратичного отклонения = 0.00031216252657606525

2.7. RC4

- Математическое ожидание = 0.4994845703125004
- Среднеквадратичное отклонение = 0.288954875028642
- Относительная погрешность математического ожидания = 0.0005154296874996245
- Относительная погрешность среднеквадратичного отклонения = 0.0012548750286419663

2.8. ГПСЧ на основе RSA

- Математическое ожидание = 0.5009959960937505
- Среднеквадратичное отклонение = 0.2907224700961812
- Относительная погрешность математического ожидания = 0.0009959960937504508
- Относительная погрешность среднеквадратичного отклонения = 0.0030224700961811735



2.9. Блюма-Блюма-Шуба

- Математическое ожидание = 0.749267578125
- Среднеквадратичное отклонение = 0.22804603255019268
- Относительная погрешность математического ожидания = 0.249267578125
- Относительная погрешность среднеквадратичного отклонения = 0.05965396744980733

3. Проверка критериев

	Хи-квадрат	Серий	Интервалов	Разбиений	Перестановок	Монотонности	Конфликтов
Линейно-конгруэнтный	+	+	-	+	+	-	+
Аддитивный	+	-	-	-	+	-	+
Пятипара-метрический	-	+	-	+	+	-	+
РСЛОС	+	-	-	-	+	-	+
Нелинейная комбинация РСЛОС	-	-	-	+	+	-	+
Вихрь Мерсенна	+	+	-	-	+	-	+
RC4	+	+	-	+	+	-	+
RSA	-	-	-	-	-	-	+
Блюма-Блюма-Шуба	+	-	-	-	-	-	+