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 ПРАКТИЧЕСКОМУ КУРСУ

студента 4 курса 431 группы

факультета компьютерных наук и информационных технологий

Мухи Семена Андреевича

фамилия, имя, отчество

Научный руководитель

Ст. преподаватель _____ И.И. Слеповичев

подпись, дата

Саратов 2024

1 Генерация ППСЧ и запуск программы

ППСЧ была сгенерирована с помощью функции random.uniform(0.0, 1.0), выдающей числа из отрезка [0; 1]. Во входной файл было записано 10000 таких чисел с точностью до 3 знака после десятичной точки. Также для критерия конфликтов были сгенерированы и записаны во второй входной файл 10000 целых чисел из отрезка [0; 99999] с помощью функции random.randint(0, 100000).

2 Математическое ожидание и среднеквадратичное отклонение

Математическое ожидание было вычислено как среднее арифметическое, а среднеквадратичное отклонение как корень из дисперсии. Результаты вычисления представлены на рисунке ниже.

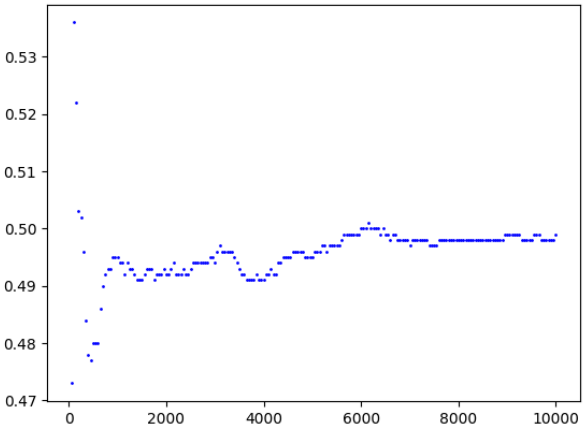
```
Мат.ожидание = 0.5
Среднеквадратичное отклонение = 0.288
```

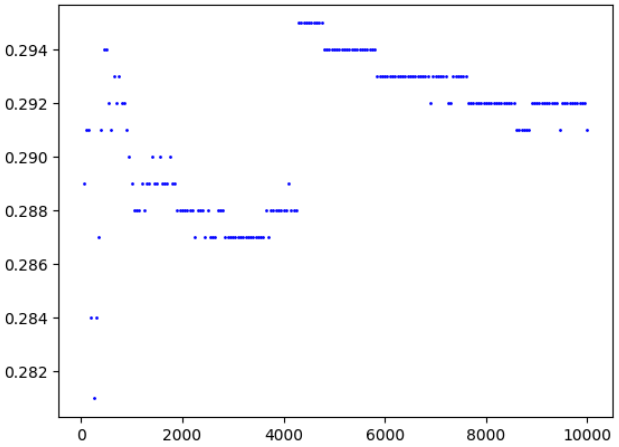
Так как распределение является непрерывным равномерным, то математическое ожидание для него равняется 0.5, а среднеквадратичное отклонение — 0.2886. Разница между практическими и теоретическими значениями минимальна.

Таким образом, легко подсчитать относительную погрешность.

```
Погрешность для мат.ожидания в % = 0.0
Погрешность для среднеквадратичного отклонения в % = 0.2
```

Затем на языке Python была написана программа, подсчитывающая зависимость математического ожидания и среднеквадратичного отклонения от размера выборки. Код программы приведен в приложении А. Ниже приведены графики зависимостей.





3 Проверка критериев

Ниже приведены критерии, степени свободы, для которых считалось хи-квадрат. Если вычисленное хи - квадрат попало в интервал, то критерий выполняется. Для этого была взята таблица квантилей.

- Критерий хи-квадрат, 1 степень, интервал [0.0158, 3.8415].
- Критерий серий, 3 степень, интервал [0.5844, 7.8147].
- Критерий интервалов, 3 степень, интервал [0.5844, 7.8147].
- Критерий разбиений, 2 степень, интервал [0.2107, 5.9915].
- Критерий перестановок, 1 степень, интервал [0.0158, 3.8415].
- Критерий монотонности, 2 степень, интервал [0.2107, 5.9915].
- Критерий конфликтов, 1 степень, интервал [0.0158, 3.8415].

Код программы в приложенном файле.

Результат работы программы приведен ниже.

```
Мат.ожидание = 0.5
Среднеквадратичное отклонение = 0.3
Погрешность для мат.ожидания в % = 0.0
Погрешность для среднеквадратичного отклонения в % = 3.8
Критерий Хи-квадрат подтвержден и он равен 0.212
Критерий Серий подтвержден и оно равен 1.316
Критерий Интервалов подтвержден и он равен 0.894
Критерий Разбиений подтвержден и он равен 5.945
Критерий Перестановок подтвержден и он равен 0.542
Критерий Монотонности подтвержден и он равен 0.458
Критерий Кофликтов подтвержден и он равен 0.11218947368421052
```

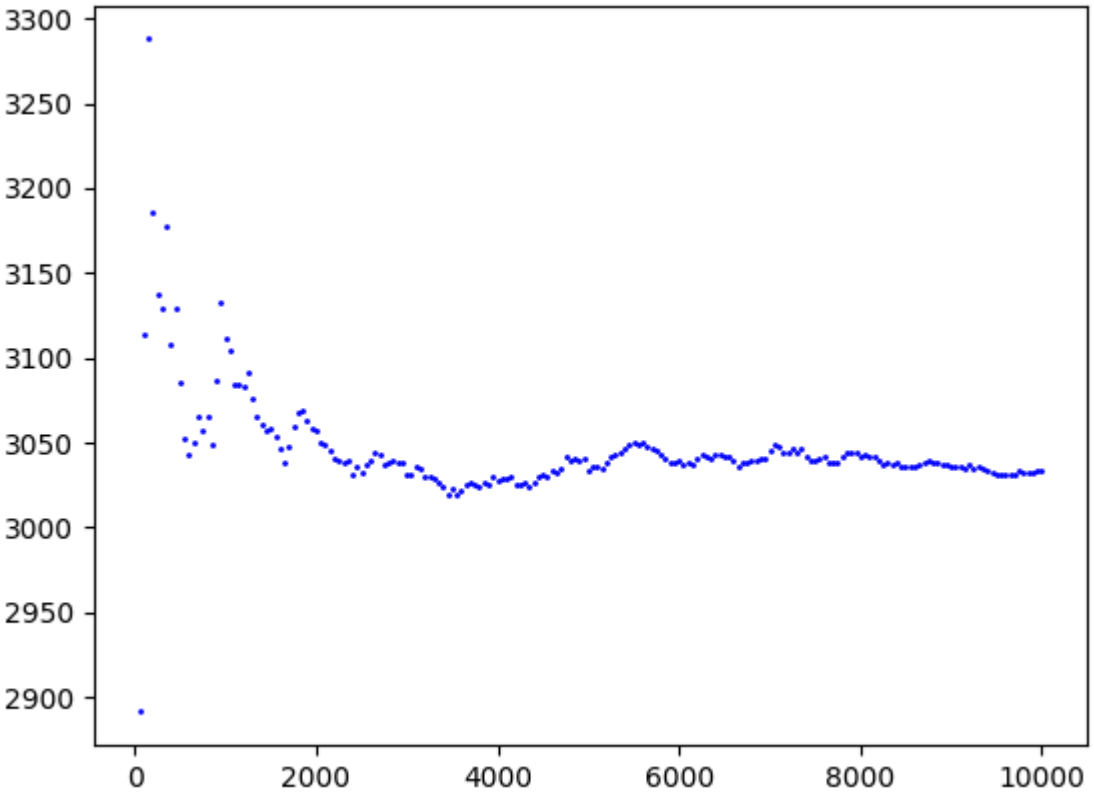
4 Проверка критериев для ГПСЧ

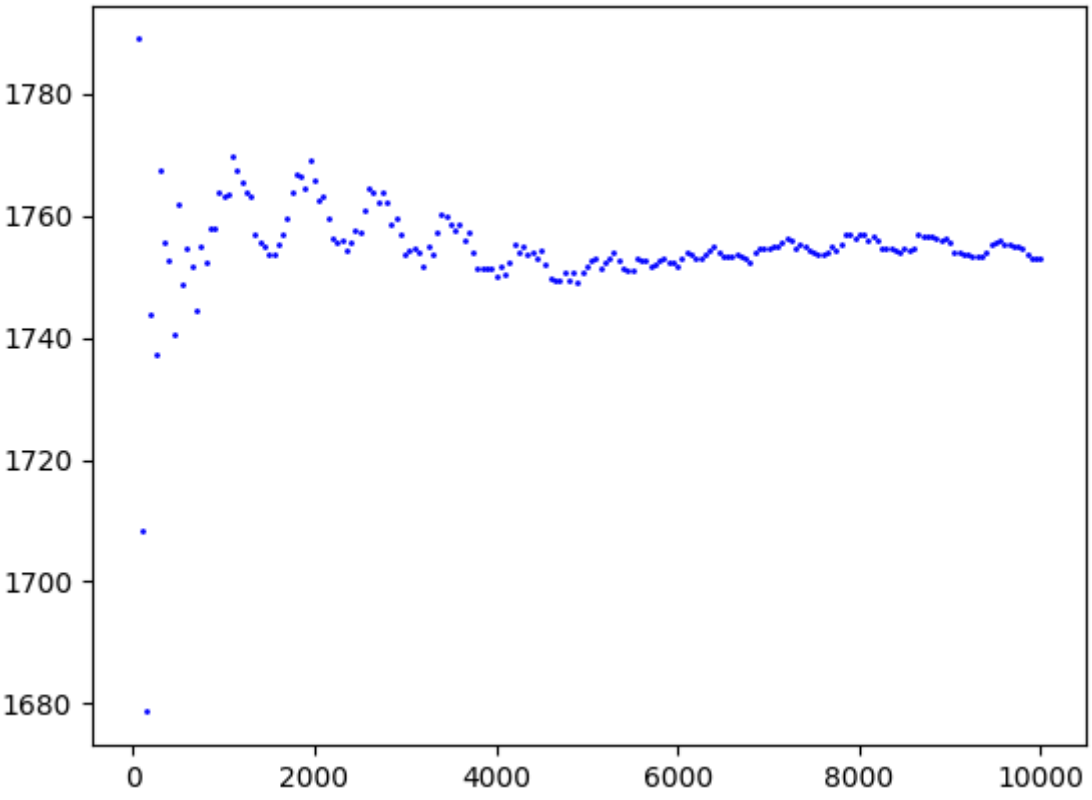
Сгенерируем каждым генератором 10000 случайных чисел и приведем их к стандартному равномерному распределению. После этого с каждым из них проделаем те же самые действия, что и со встроенным.

Ниже приведены результаты для следующих генераторов:

1) линейный конгруэнтный;

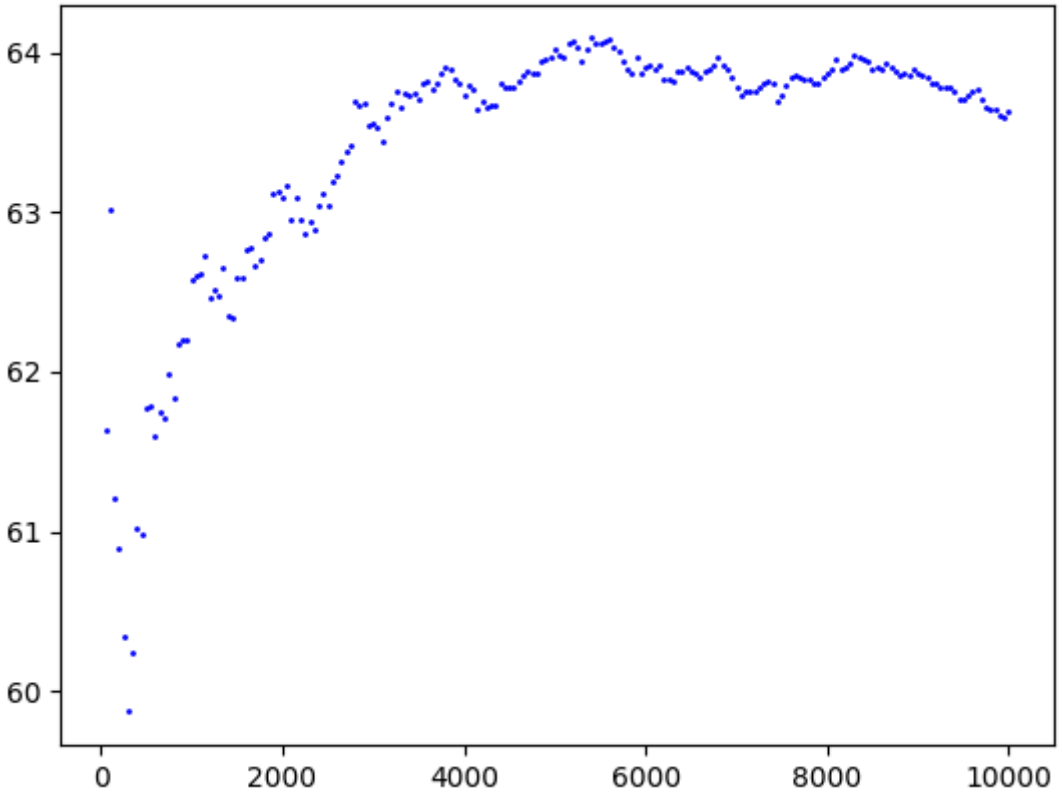
```
Мат.ожидание = 0.501
Среднеквадратичное отклонение = 0.292
Погрешность для мат.ожидания в % = 0.2
Погрешность для среднеквадратичного отклонения в % = 1.0999999999999999
Критерий Хи-квадрат подтвержден и он равен 0.09
Критерий Серий подтвержден и оно равен 1.644
Критерий Интервалов подтвержден и он равен 2.239
Критерий Разбиений подтвержден и он равен 4.81536
Критерий Перестановок не подтвержден и он равен 3.94
Критерий Монотонности подтвержден и он равен 1.111
Критерий Конфликтов не подтвержден и он равен 0.0041263157894736845
```

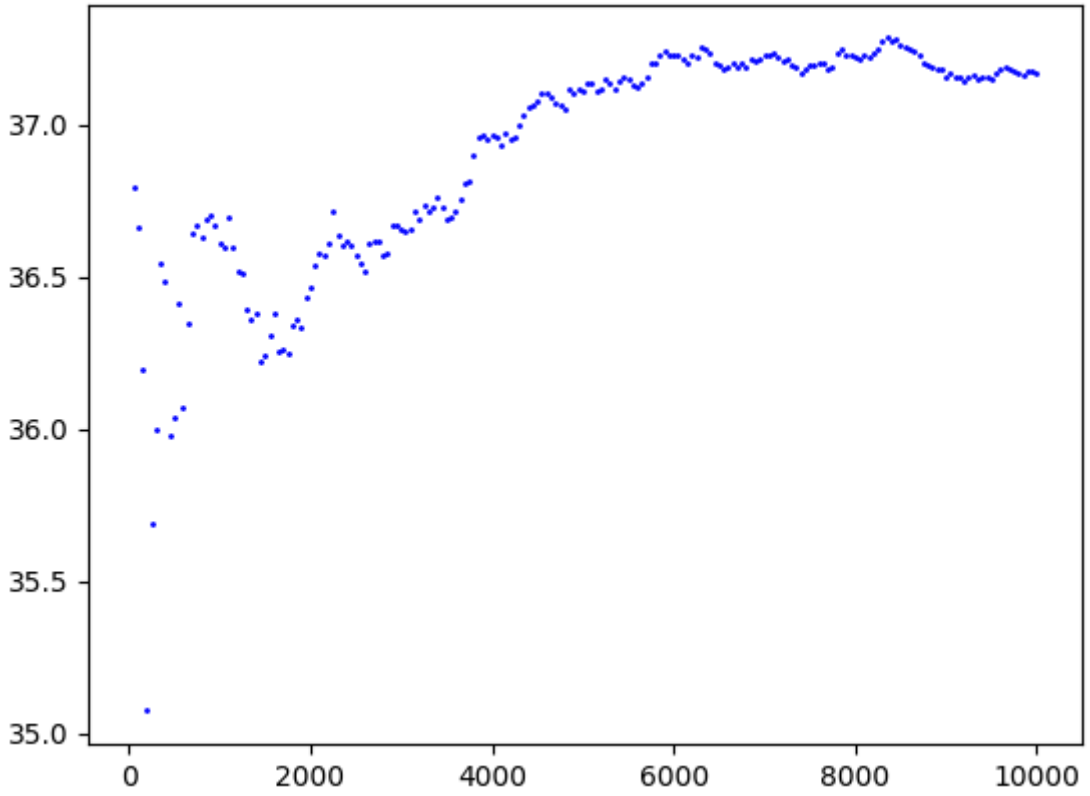




2) аддитивный;

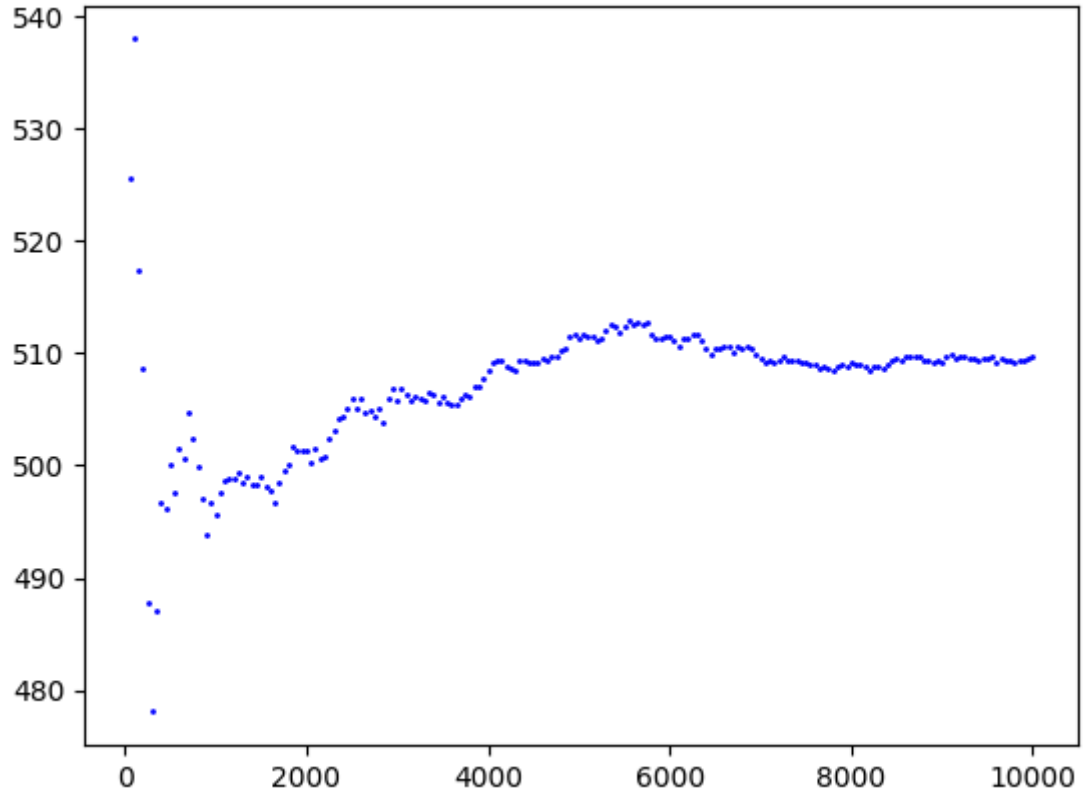
```
Мат.ожидание = 0.5
Среднеквадратичное отклонение = 0.288
Погрешность для мат.ожидания в % = 0.0
Погрешность для среднеквадратичного отклонения в % = 0.2
Критерий Хи-квадрат подтвержден и он равен 0.16
Критерий Серий подтвержден и оно равен 3.154
Критерий Интервалов подтвержден и он равен 2.273
Критерий Разбиений не подтвержден и он равен 23.839
Критерий Перестановок подтвержден и он равен 0.785
Критерий Монотонности подтвержден и он равен 0.451
Критерий Конфликтов не подтвержден и он равен 0.002105263157894737
```

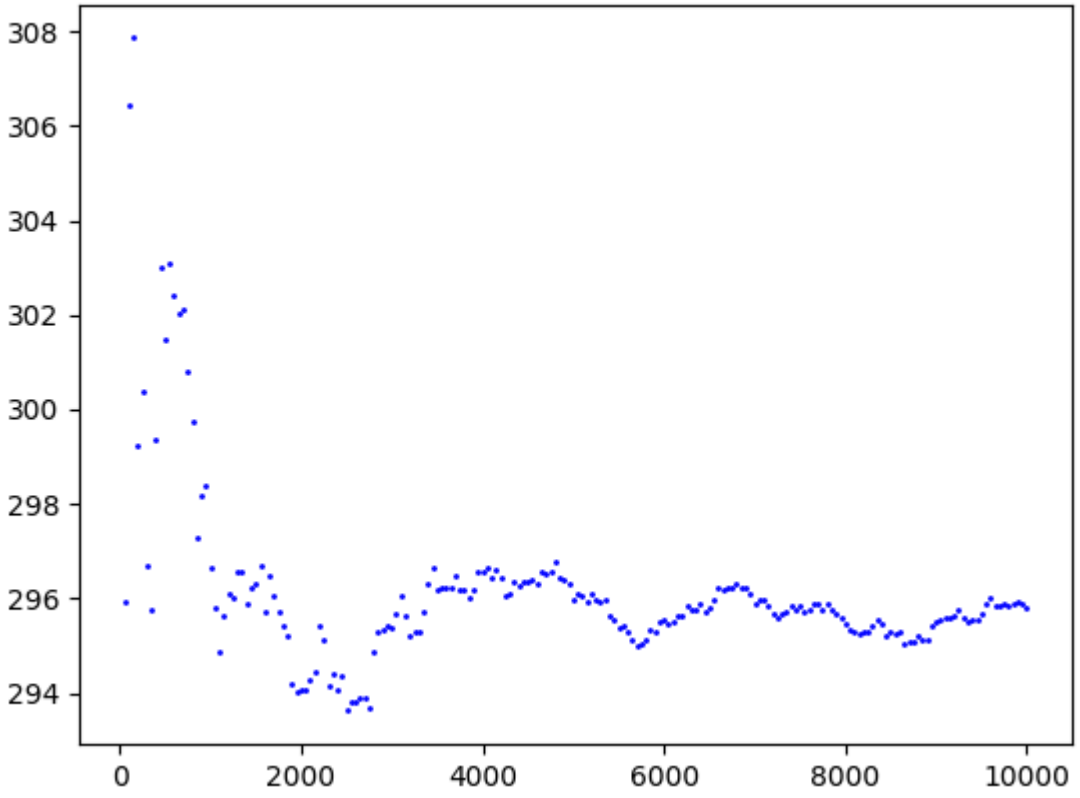




3) регистр сдвига с обратной связью (РСЛОС);

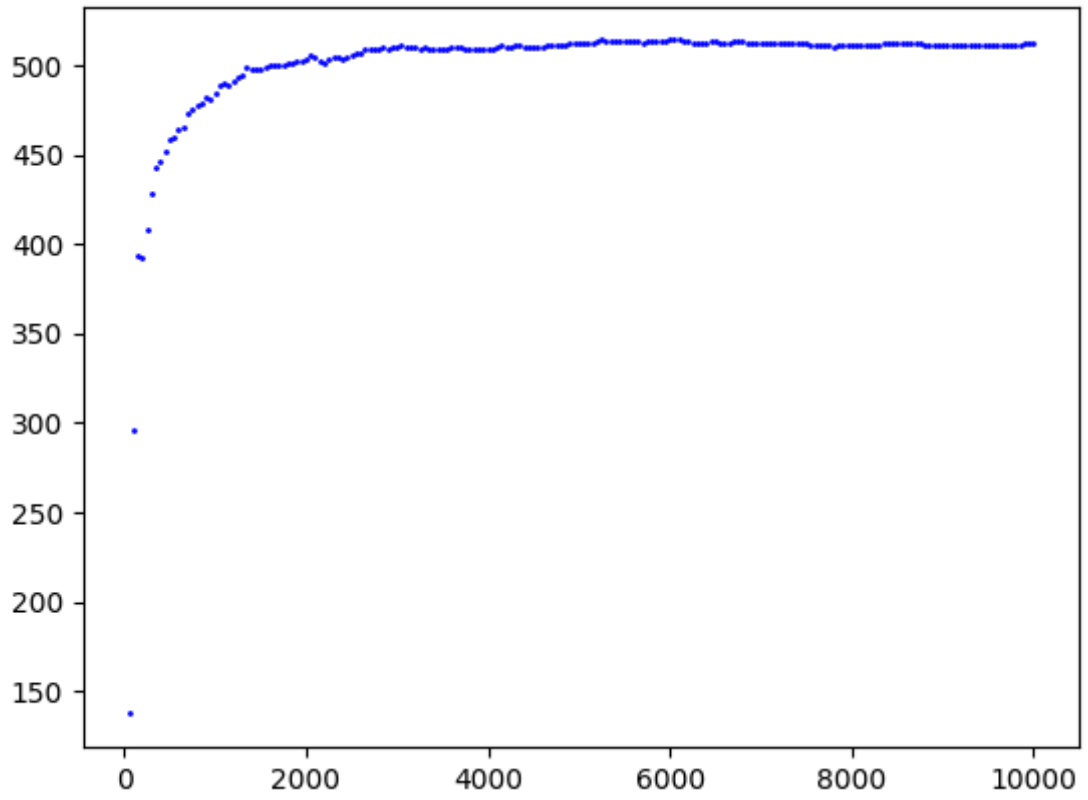
```
Мат.ожидание = 0.52
Среднеквадратичное отклонение = 0.289
Погрешность для мат.ожидания в % = 3.8
Погрешность для среднеквадратичного отклонения в % = 0.1
Критерий Хи-квадрат не подтвержден и он равен 12.39
Критерий Серий не подтвержден и оно равен 15.744
Критерий Интервалов подтвержден и он равен 2.355
Критерий Разбиений подтвержден и он равен 2.641
Критерий Перестановок не подтвержден и он равен 24.804
Критерий Монотонности подтвержден и он равен 0.782
Критерий Конфликтов не подтвержден и он равен 0.0030315789473684207
```

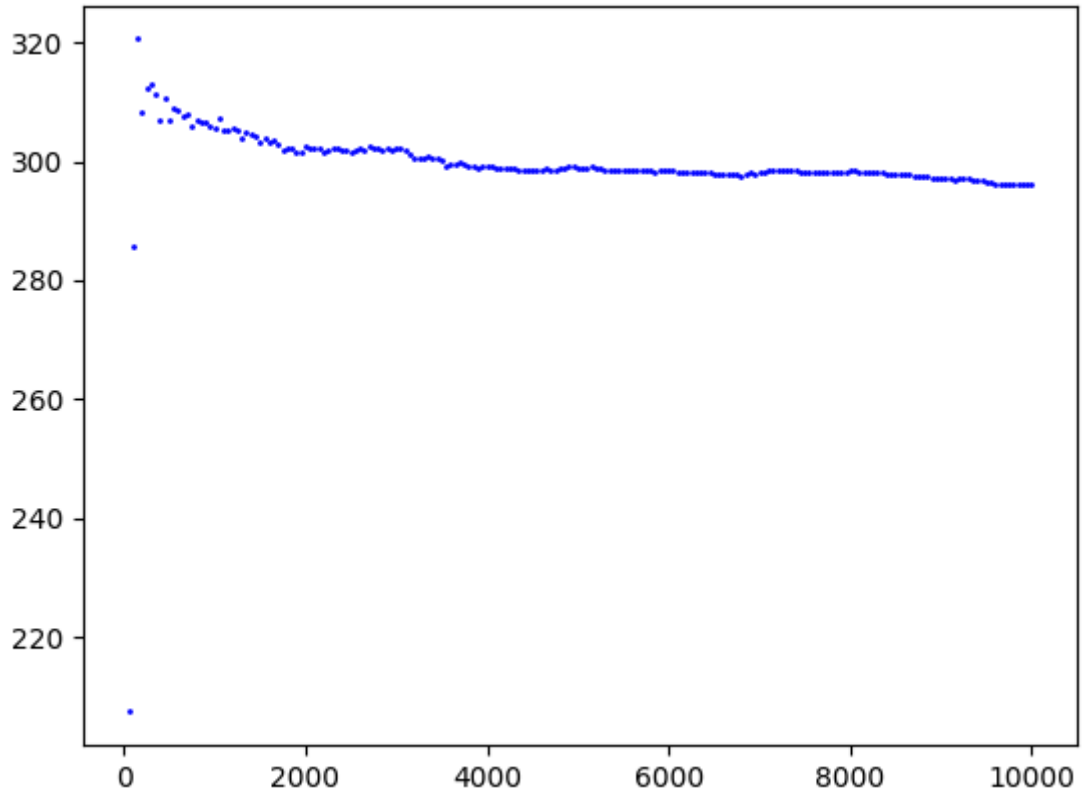




4) пятипараметрический;

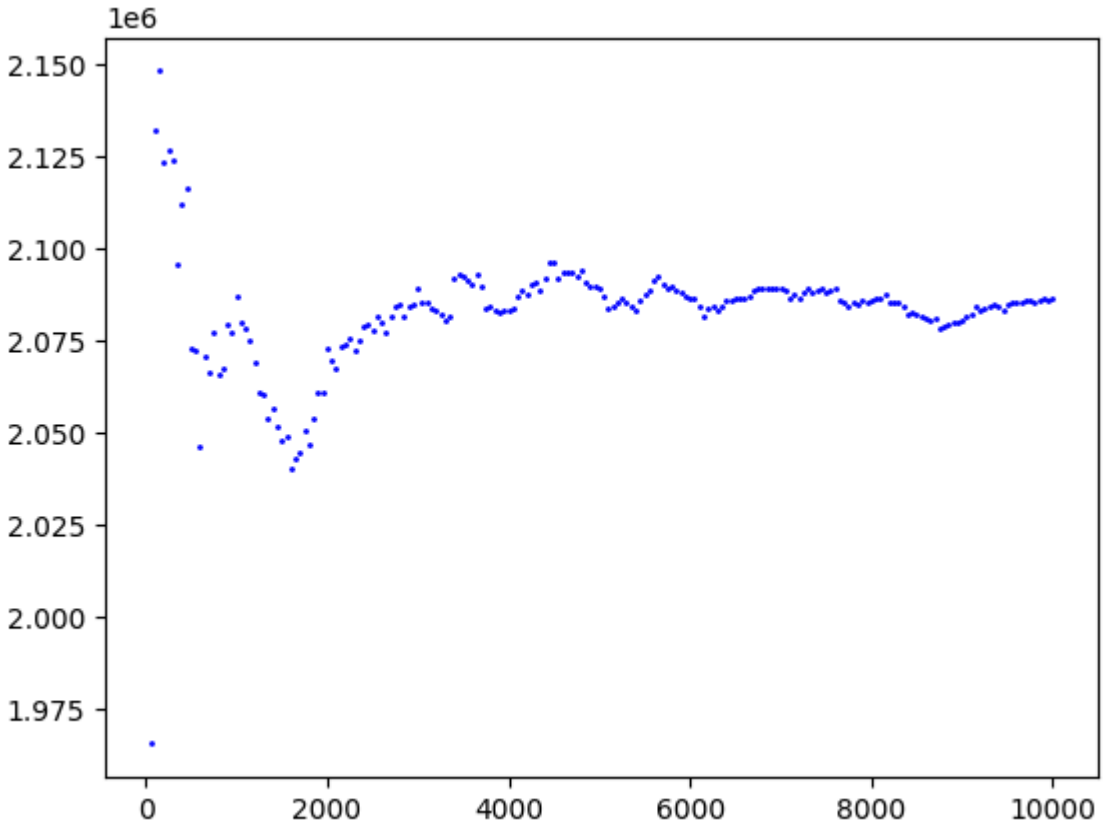
```
Мат.ожидание = 0.482
Среднеквадратичное отклонение = 0.294
Погрешность для мат.ожидания в % = 3.6999999999999997
Погрешность для среднеквадратичного отклонения в % = 1.7999999999999998
Критерий Хи-квадрат не подтвержден и он равен 9.86
Критерий Серий не подтвержден и оно равен 11.465
Критерий Интервалов подтвержден и он равен 5.189
Критерий Разбиений не подтвержден и он равен 30.367
Критерий Перестановок не подтвержден и он равен 20.852
Критерий Монотонности подтвержден и он равен 1.007
Критерий Кофликтов подтвержден и он равен 0.0304
```

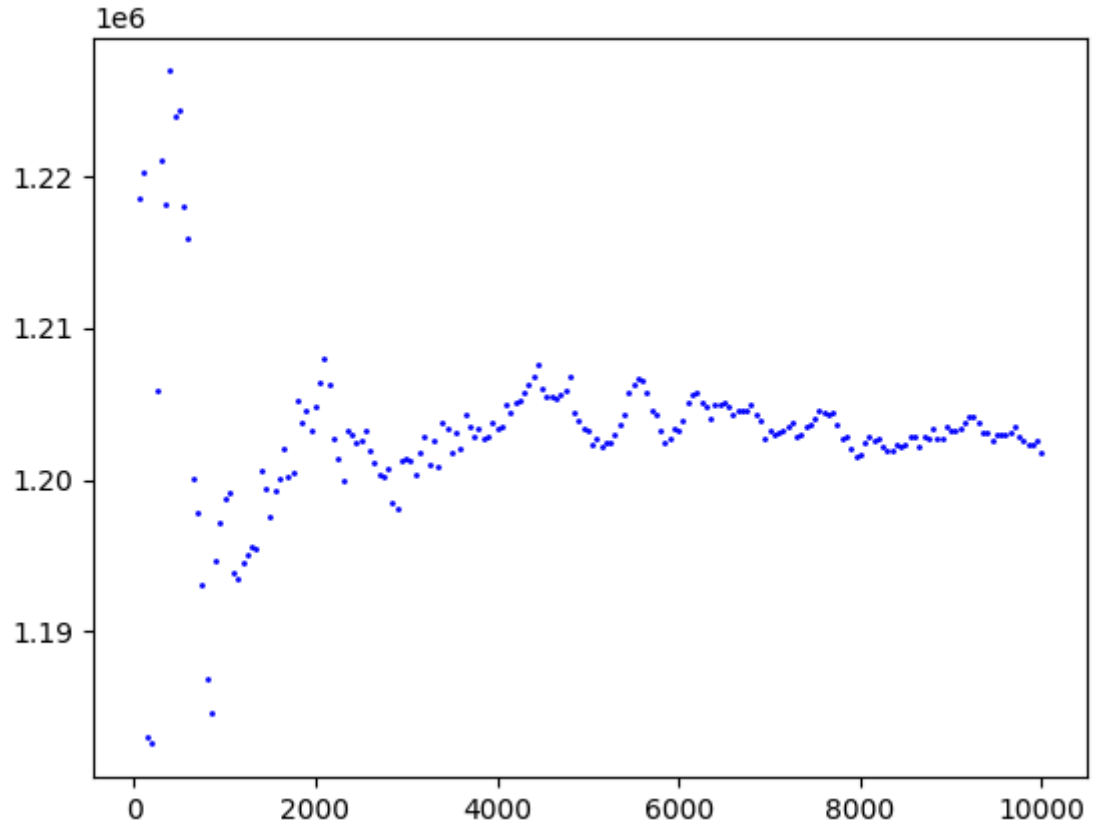




5) RSA;

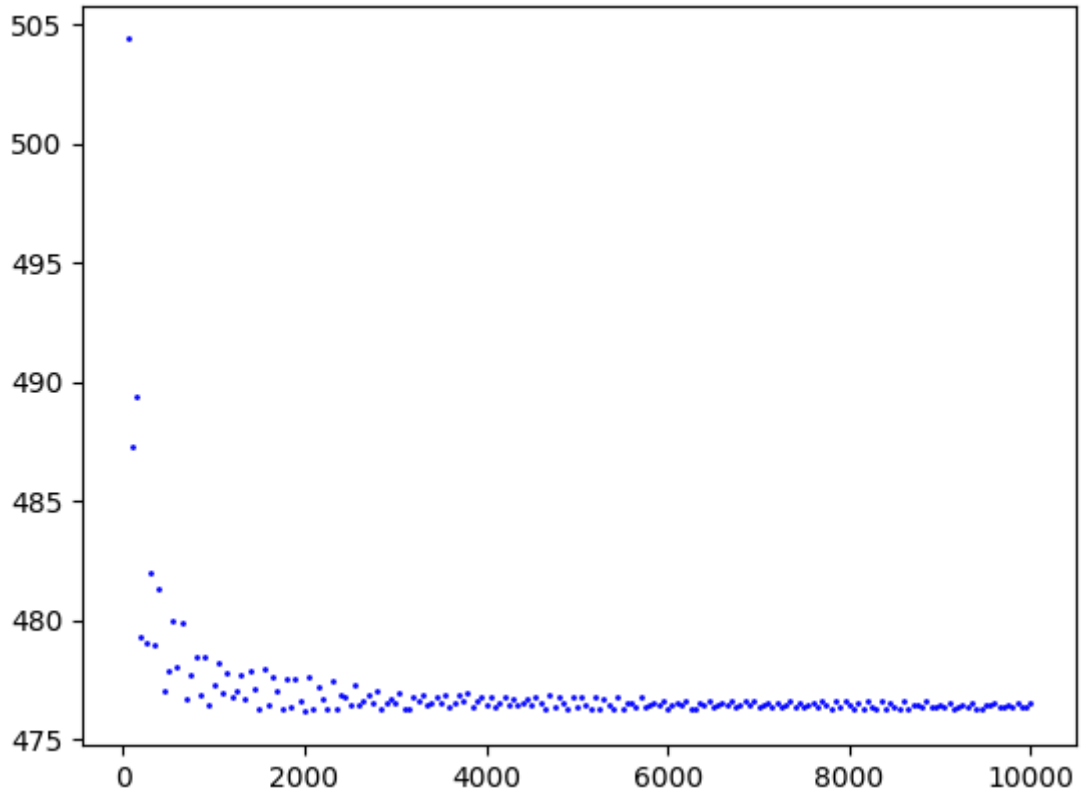
```
Мат.ожидание = 0.509
Среднеквадратичное отклонение = 0.287
Погрешность для мат.ожидания в % = 1.7999999999999998
Погрешность для среднеквадратичного отклонения в % = 0.6
Критерий Хи-квадрат подтвержден и он равен 2.132
Критерий Серий не подтвержден и оно равен 8.689
Критерий Интервалов не подтвержден и он равен 8.138
Критерий Разбиений не подтвержден и он равен 8.739
Критерий Перестановок подтвержден и он равен 3.751
Критерий Монотонности подтвержден и он равен 0.312
Критерий Кофликтов подтвержден и он равен 0.02023157894736842
```

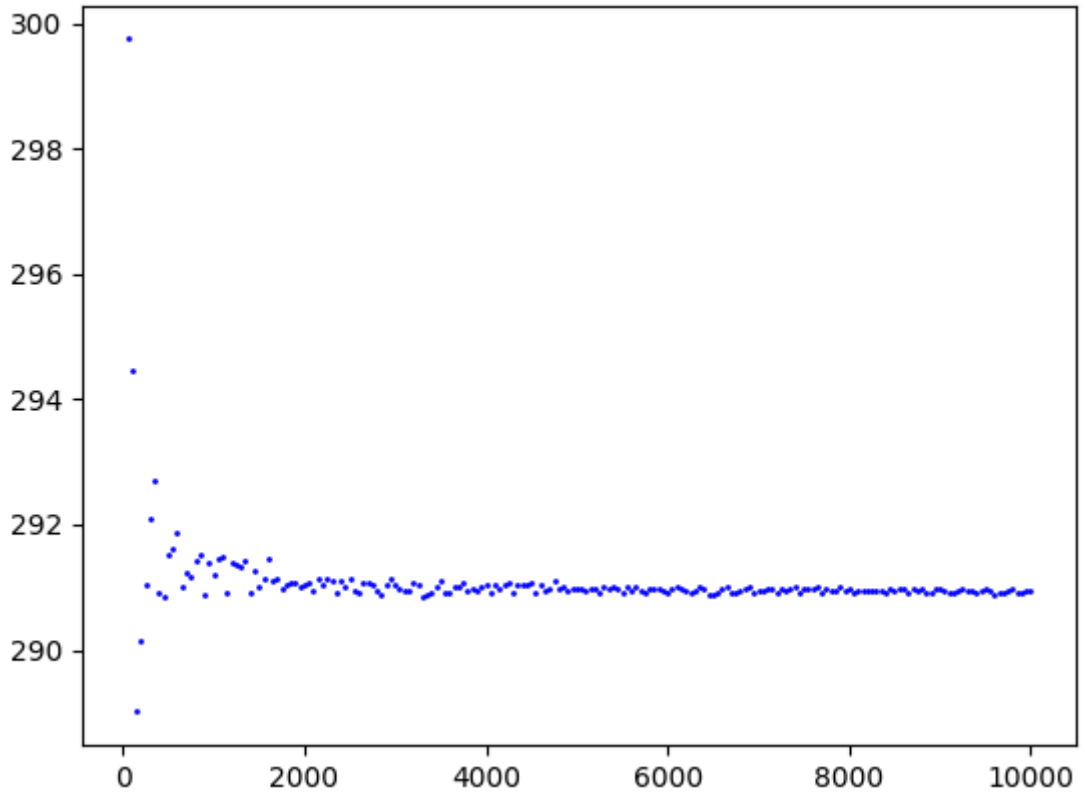

1e6
2.150
2.125
2.100
2.075
2.050
2.025
2.000
1.975
0
2000
4000
6000
8000
10000


1e6
1.22
1.21
1.20
1.19
0
2000
4000
6000
8000
10000

6) BBS (Блюма-Блюма-Шуба);

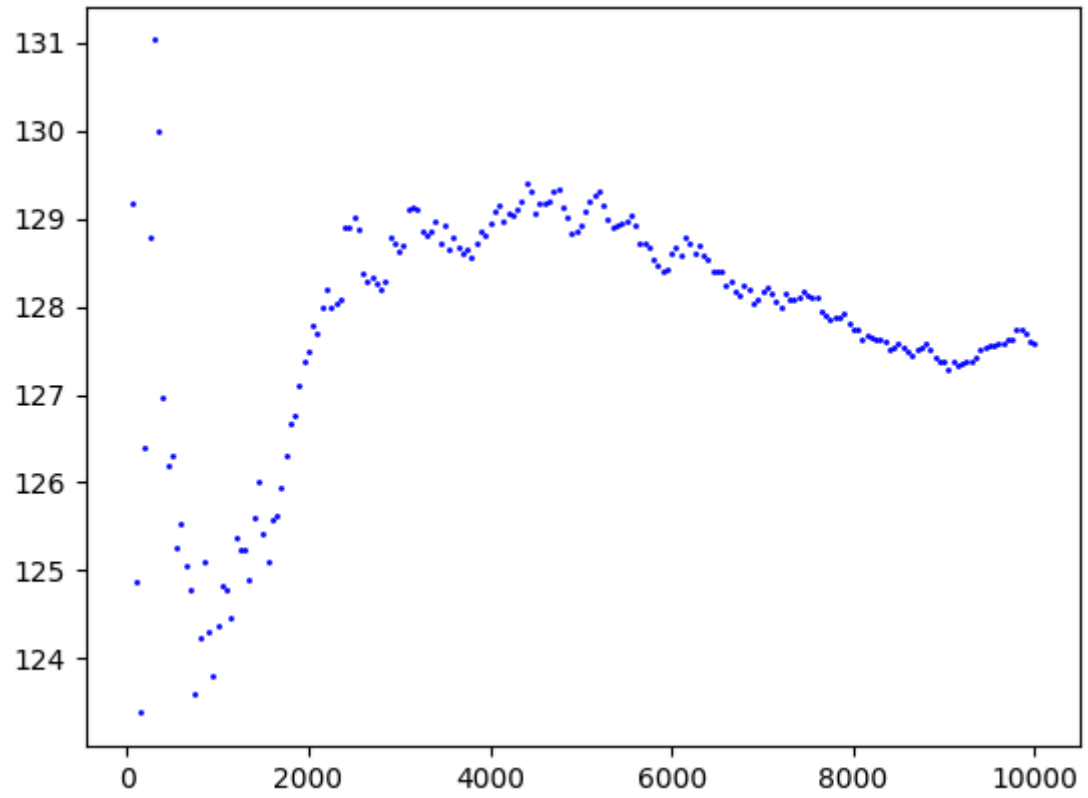
```
Мат.ожидание = 0.553
Среднеквадратичное отклонение = 0.29
Погрешность для мат.ожидания в % = 9.6
Погрешность для среднеквадратичного отклонения в % = 0.5
Критерий Хи-квадрат не подтвержден и он равен 124.992
Критерий Серий не подтвержден и оно равен 99.618
Критерий Интервалов подтвержден и он равен 2.917
Критерий Разбиений не подтвержден и он равен 8.53
Критерий Перестановок не подтвержден и он равен 245.764
Критерий Монотонности подтвержден и он равен 0.408
Критерий Конфликтов не подтвержден и он равен 0.0053894736842105264
```

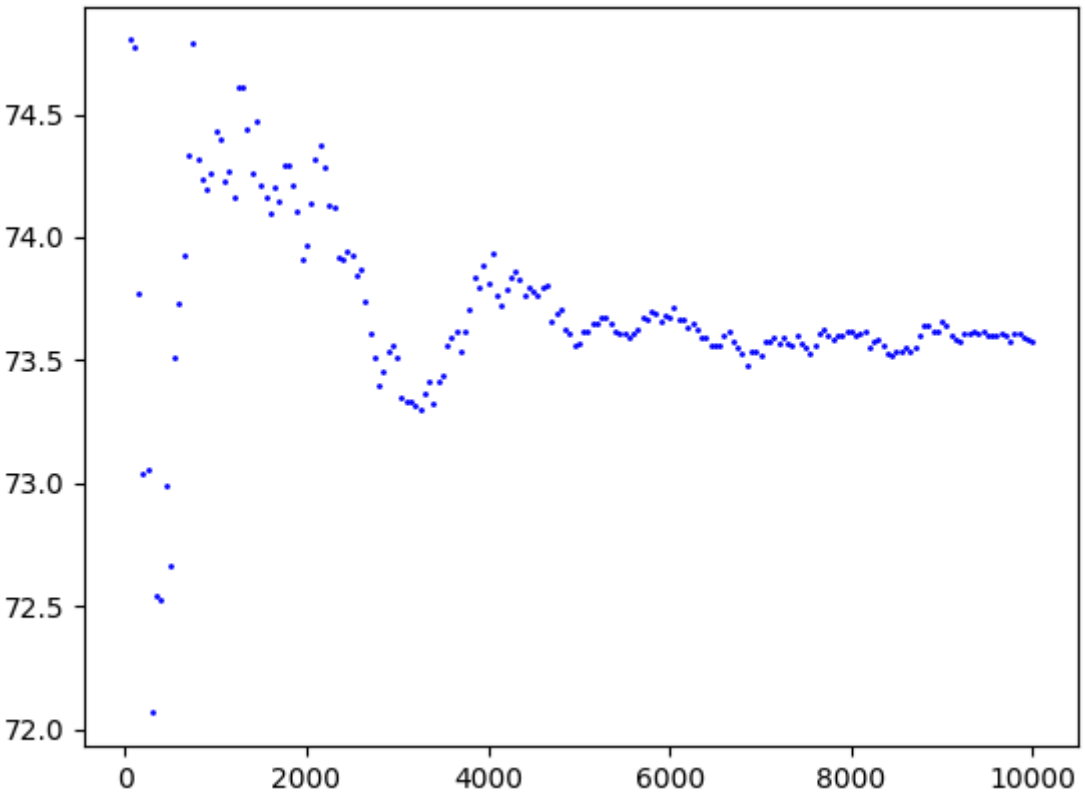




7) RC4;

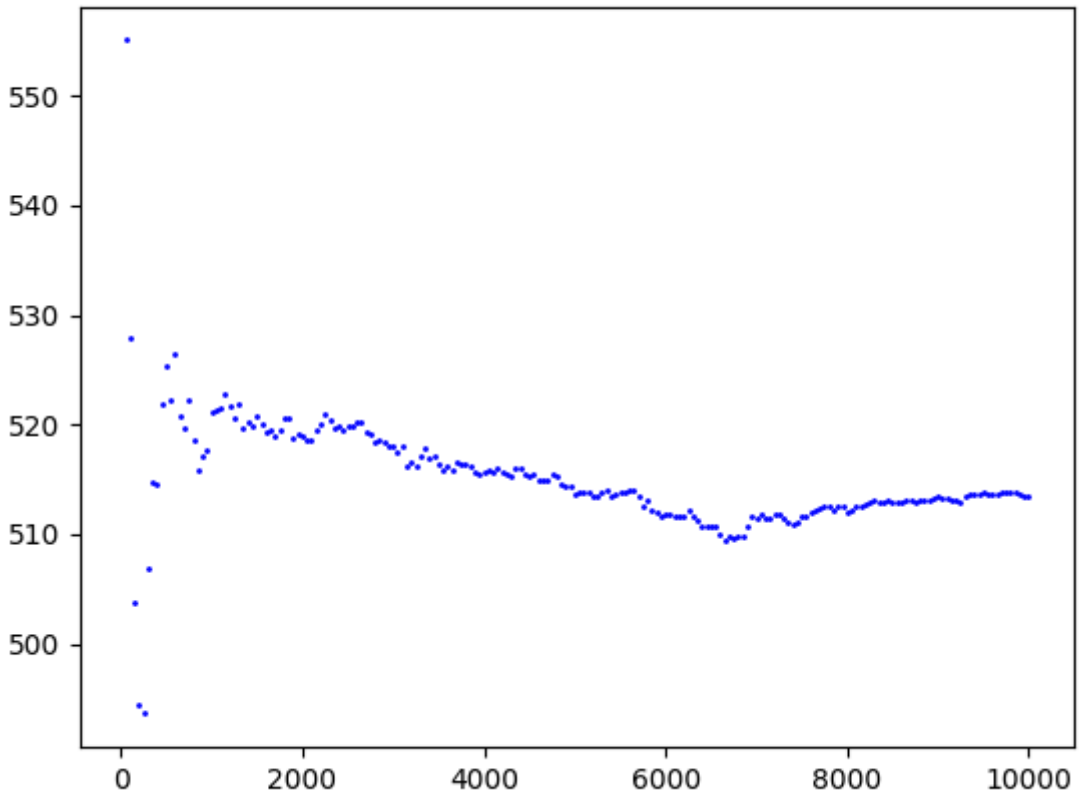
```
Мат.ожидание = 0.508
Среднеквадратичное отклонение = 0.29
Погрешность для мат.ожидания в % = 1.6
Погрешность для среднеквадратичного отклонения в % = 0.5
Критерий Хи-квадрат подтвержден и он равен 1.346
Критерий Серий подтвержден и оно равен 5.117
Критерий Интервалов подтвержден и он равен 0.929
Критерий Разбиений не подтвержден и он равен 7.142
Критерий Перестановок не подтвержден и он равен 7.669
Критерий Монотонности подтвержден и он равен 0.215
Критерий Кофликтов подтвержден и он равен 0.017705263157894738
```

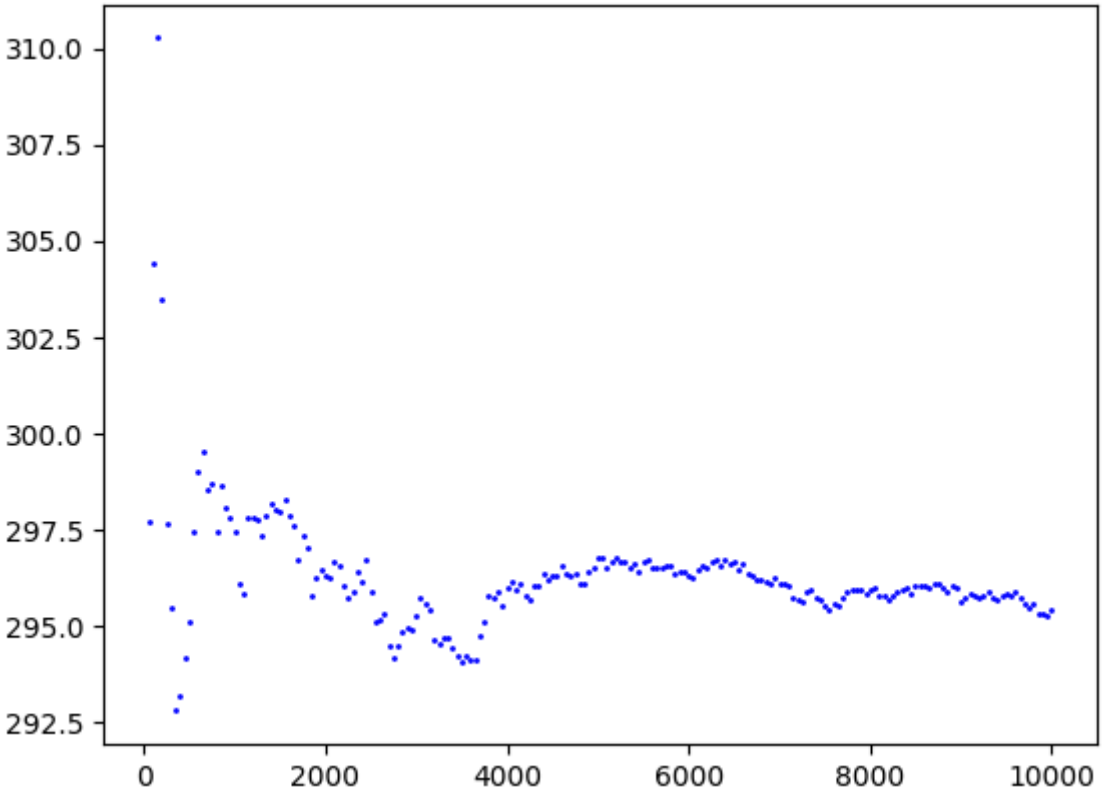




8) нелинейная комбинация РСЛОС;

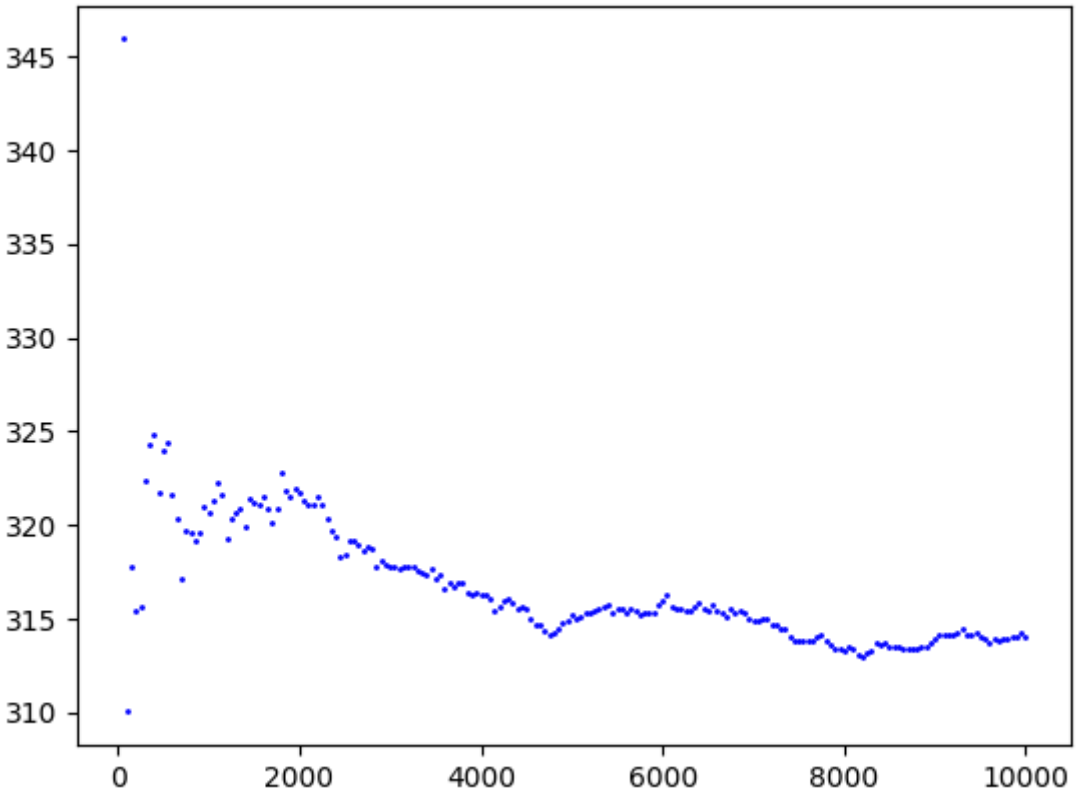
```
Мат.ожидание = 0.504
Среднеквадратичное отклонение = 0.29
Погрешность для мат.ожидания в % = 0.8
Погрешность для среднеквадратичного отклонения в % = 0.5
Критерий Хи-квадрат подтвержден и он равен 2.19
Критерий Серий подтвержден и оно равен 3.38
Критерий Интервалов подтвержден и он равен 1.299
Критерий Разбиений не подтвержден и он равен 7.377
Критерий Перестановок не подтвержден и он равен 3.923
Критерий Монотонности не подтвержден и он равен 0.069
Критерий Конфликтов не подтвержден и он равен 0.0025473684210526315
```

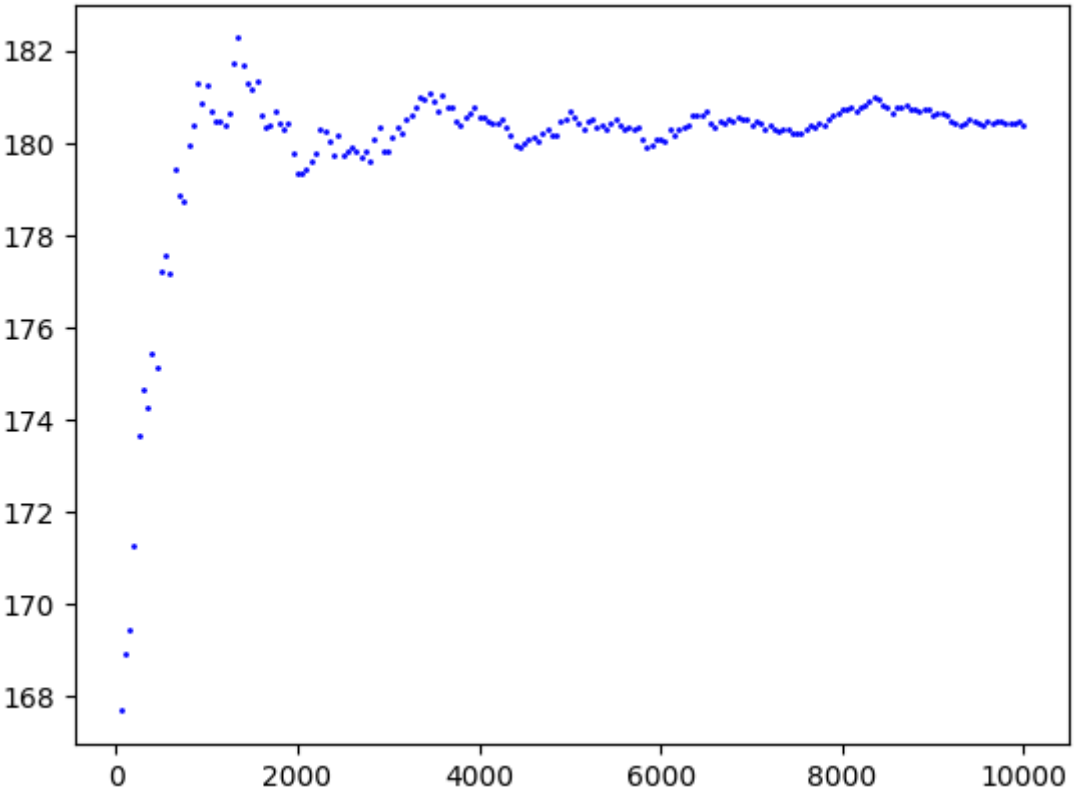




9) вихрь Мерсена.

```
Мат.ожидание = 0.448
Среднеквадратичное отклонение = 0.332
Погрешность для мат.ожидания в % = 11.600000000000001
Погрешность для среднеквадратичного отклонения в % = 13.0
Критерий Хи-квадрат не подтвержден и он равен 97.614
Критерий Серий не подтвержден и оно равен 115.748
Критерий Интервалов не подтвержден и он равен 10.485
Критерий Разбиений не подтвержден и он равен 59.957
Критерий Перестановок не подтвержден и он равен 197.514
Критерий Монотонности подтвержден и он равен 1.635
Критерий Конфликтов не подтвержден и он равен 0.0010315789473684211
```





Таким образом, исходя из результатов, можно составить следующую таблицу.

Критерии	Хи-квадрат	Серий	Интервалов	Разбиений	Перестановок	Монотонности	Конфликтов
lc	+	+	+	+	-	+	-
add	+	+	+	-	+	+	-
lfsr	-	-	+	+	-	+	-
5p	-	-	+	-	-	+	+
rsa	+	-	-	+	+	+	+
bbs	-	-	+	-	-	+	-
rc4	+	+	+	-	-	+	+
nfsr	+	+	+	-	-	-	-
mt	-	-	-	-	-	+	-