Научная статья
УДК 519.6
DOI: https://doi.org/10.25686/2306-2819.2024.4.68
EDN: TYWPLM

Тестирование на «случайность» генераторов псевдослучайных чисел для стендов полунатурного моделирования асинхронных радиоэлектронных систем

Р. Р. Раупов[1], С. С. Логинов[1,2], И. Н. Фролов[1], Ю. Р. Буткевич[1,2]✉
[1]АО «НПО «Радиоэлектроника» им. В.И. Шимко»,
Российская Федерация, 420088, Казань, ул. Журналистов, 50
[2]Казанский национальный исследовательский технический университет им. А.Н. Туполева - КАИ,
Российская Федерация, 420111, Казань, ул. Карла Маркса, 10
bytkevic@mail.ru✉

Аннотация. Разработаны программные средства моделирования двоичных последовательностей, формируемых генераторами псевдослучайных чисел по ГОСТ Р ИСО 28640 – 2012, для их дальнейшего использования в стендах полунатурного моделирования асинхронных радиоэлектронных систем. С помощью системы статистических тестов NIST проведено исследование статистических свойств сформированных разработанными генераторами псевдослучайных последовательностей и проведена их проверка на случайность посредством сравнения со статистикой идеально случайного ряда. По результатам исследования выбран пороговый уровень прохождения тестов NIST и выработаны инженерные рекомендации по выбору генератора псевдослучайных чисел с наибольшим количеством успешно пройденных тестов. Установлено, что для стендов полунатурного моделирования асинхронных радиоэлектронных систем рекомендуется применение генератора псевдослучайных чисел на основе метода Мерсенна Твистера. Также установлена необходимость совершенствования разработанных генераторов путём подбора входных параметров с целью повышения вероятности прохождения тестов.

Ключевые слова: генератор псевдослучайных чисел; псевдослучайная последовательность; статистические тесты NIST; тесты на случайность; стенд полунатурного моделирования

Финансирование: авторы заявляют об отсутствии внешнего финансирования при проведении исследования.

Для цитирования: Тестирование на «случайность» генераторов псевдослучайных чисел для стендов полунатурного моделирования асинхронных радиоэлектронных систем / Р. Р. Раупов, С. С. Логинов, И. Н. Фролов и др. // Вестник Поволжского государственного технологического университета. Сер.: Радиотехнические и инфокоммуникационные системы. 2024. № 4 (64). С. 68–77. DOI: https://doi.org/10.25686/2306-2819.2024.4.68; EDN: TYWPLM

Введение

Стенды полунатурного моделирования асинхронных радиоэлектронных систем позволяют производить экспериментальную оценку их вероятностных характеристик при воспроизведении заданной сигнально-помеховой обстановки, характеризующейся воздействием внутрисистемных помех, а также воздействием со стороны противника путём постановки преднамеренных помех и специализированных методов противодействия: имитации сигналов систем, провоцирования излучения средств систем. При проведении испытаний такие стенды создают близкое к реальному воздействие на испытываемый объект и используют различные методы моделирования: математическое, имитационное, полунатурное, натурное и др. Достоинствами полунатурного моделирования являются высокая достоверность результатов, возможность

доработки испытываемых изделий на более ранних стадиях, низкая стоимость по сравнению с натурными испытаниями [1].

Воспроизведение условий испытаний в стендах полунатурного моделирования предполагает формирование сигналов с различными типами вероятностных распределений по мощности и времени. Для формирования подобных распределений используются генераторы случайных и псевдослучайных чисел. Генераторы случайных чисел привлекательны с точки зрения многообразия их последовательностей. В то же время воспроизводимость статистических характеристик генераторов псевдослучайных чисел (ГПСЧ) делает их использование для стендов полунатурного моделирования более применимыми по сравнению с генераторами случайных чисел.

Формируемые на стенде потоки псевдослучайных чисел должны описываться различными законами распределения, среди которых наиболее востребованы равномерное, Гаусса, Релея, Райса и экспоненциальное [2]. Основой для формирования псевдослучайных чисел с различными законами распределения являются равновероятные случайные числа, которые могут формироваться и преобразовываться в числа с требуемыми для моделирования законами распределения в соответствии с ГОСТ[1]. Необходимость практического применения ГПСЧ для стендов полунатурного моделирования делает актуальным проведение анализа формируемых ими чисел на случайность [3]. В качестве тестов последовательностей чисел на случайность наиболее широко используется система тестов NIST, разработанная лабораторией информационных технологий Национального института стандартов и технологий [4]. Тесты NIST показывают схожесть статистических свойств сформированного псевдослучайного ряда чисел с эталонной статистикой идеально случайной последовательности.

Целью данной работы является анализ прохождения тестов двоичных последовательностей, формируемых генераторами псевдослучайных чисел, предлагаемых ГОСТ Р ИСО 28640 – 2012, на случайность с использованием тестов NIST на базе разработанных программных средств моделирования.

Для достижения поставленной цели необходимо решение следующих **задач**:

- проведение аналитического обзора по методам формирования псевдослучайных последовательностей, распределённых по равномерному закону;
- проведение аналитического обзора по системе статистических тестов NIST для оценки последовательностей чисел на случайность;
- создание средств моделирования генераторов псевдослучайных последовательностей с выбранными параметрами и их оценка на случайность;
- выработка инженерных рекомендаций по выбору генератора псевдослучайных чисел, характеризующегося наибольшим количеством успешно пройденных тестов.

Тематические разделы и подразделы

Для формирования псевдослучайных чисел с равномерным распределением на стендах полунатурного моделирования широко используются методы на основе М-последовательностей. Такие генераторы строятся с использованием сдвиговых регистров с выбираемыми из корзины начальными условиями и порождающими полиномами, определяющими коэффициенты обратной связи, а также схем суммирования по модулю два.

Метод М-последовательности формирует ряд двоичных чисел в соответствии с рекуррентной формулой:

$$\begin{aligned} x_{n+p} &= c_{p-1}\cdot x_{n+p-1} + c_{p-2}\cdot x_{n+p-2} + \dots \\ &\dots + c_1\cdot x_{n+1} + x_n \left(mod\, 2\right), n = 1,2,3\dots, \end{aligned} \quad (1)$$

где $c_1, c_2, \dots, c_{p-1}$ – коэффициенты обратной связи, определяемые посредством порождающего полинома.

[1] ГОСТ Р ИСО 28640 – 2012. Статистические методы. Генерация случайных чисел. Введ. с 29.11.2012. М.: Стандартинформ, 2014. 40 с.

М-последовательность характеризуется следующими свойствами:

- является периодической с периодом $N = 2^n - 1$, где n – длина регистра, с помощью которого формируется М-последовательность;
- распределение символов в периоде является равновероятным;
- М-последовательность содержит все n-значные комбинации двоичных символов кроме нулевой комбинации.

Схема построения типового генератора, построенного на основе М-последовательности, представлена на рис. 1.

Ввиду изученности и относительной простоты метода М-последовательности формируемый массив псевдослучайных чисел имеет легко выявляемые статистические закономерности и недостаточный уровень случайности.

В работе [5] предложен ГПСЧ, построенный на регистрах сдвига в условиях формирования циклов немаксимальной длины и позволяющий образовать наборы псевдослучайных чисел с разнообразными вероятностными и корреляционными свойствами. Также известен генератор гиперхаотических сигналов [6], построенный на основе хаотических систем и формирующий псевдослучайные сигналы, которые возможно использовать для обеспечения скрытности и надёжности передачи данных.

В данной статье разработаны программные средства моделирования генераторов, формирующих псевдослучайные последовательности, определяемые ГОСТ Р ИСО 28640 – 2012 и построенные на основе:

- пятипараметрического метода;
- метода Таусворта;
- комбинированного метода Таусворта;
- метода Мерсенна Твистера.

Пятипараметрический метод строится на основе сдвигового регистра с обратной связью и использует характеристический полином из пяти членов, позволяя генерировать последовательности w-битовых двоичных целых чисел в соответствии с рекуррентной формулой:

$$X_{n+p} = X_{n+q1} + X_{n+q2} + \\ + X_{n+q3} + X_n \left(mod\, 2\right), n = 1,2,3\ldots \quad (2)$$

При реализации генератора на основе пятипараметрического метода выбраны параметры: p =89; $q1$ = 20; $q2$ = 40; $q3$ = 69; w = 64.

Генератор псевдослучайных чисел на основе метода Таусворта использует рекуррентную формулу:

$$X_n = x_{nt} x_{nt+1} \ldots x_{nt+w-1}, n = 0,1,2\ldots, \quad (3)$$

где $x_{n+p} = x_{n+q} + x_n \left(mod\, 2\right), n = 0,1,2\ldots$.

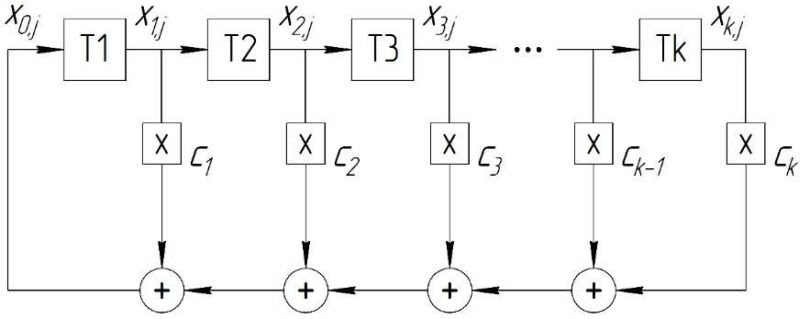

Рис. 1. Блок-схема генератора на основе метода М-последовательности: T1, T2, T3…Tk – сдвиговые регистры; c_1, c_2, c_3…c_k – коэффициенты, определяемые порождающим полиномом; $x_{0,j}$, $x_{1,j}$, x2,j, $x_{3,j}$… $x_{k,j}$ – символы на входе соответствующих сдвиговых регистров; k – количество сдвиговых регистров

Fig. 1. Block diagram of the generator based on the M-sequence T1, T2, T3…Tk – shift registers; c_1, c_2, c_3…c_k – coefficients determined by the generator polynomial; $x_{0,j}$, $x_{1,j}$, $x_{2,j}$, $x_{3,j}$… $x_{k,j}$ – symbols at the input of the corresponding shift registers; k – quantity of shift registers

Выбранные параметры генератора на основе метода Таусворта: $p = 16$; $q = 7$; $w = 16$; $t = 19$.

Комбинированный метод Таусворта представляет собой комбинацию нескольких простых последовательностей Таусворта с одной и той же длиной слова w и определяется формулой:

$$X_n = X_n^{(1)} + \\ + X_n^{(2)} + \ldots + X_n^{(J)} \left(mod\, 2\right),\ n = 0,1,2\ldots \quad (4)$$

Генератор на основе комбинированного метода Таусворта разрабатывался при помощи трёх простых последовательностей с параметрами: $p = 16$; $w = 16$; $t = 19$.

Метод Мерсенна Твистера позволяет генерировать последовательность двоичных псевдослучайных w-битовых чисел по рекуррентной формуле:

$$X_{n+p} = X_{n+q} + \\ + (X_n \mid X_{n+1})^{(r)} A \left(mod\, 2\right), n = 1,2,3\ldots, \quad (5)$$

где $(X_n^{(f)} \mid X_{n+1}^{(1)})^{(r)}$ – двоичное число, полученное конкатенацией чисел X_n и X_{n+1}, когда первые $\left(w - r\right)$ битов взяты из X_n, а последние r битов из X_{n+1}; A – матрица, состоящая из нулей и единиц и определённая посредством a.

Принцип построения генератора формирования псевдослучайных чисел на основе метода Мерсенна Твистера представлен на рис. 2.

Для улучшения рандомизации полученного ряда применяется метод закалки, определяемый по следующим формулам:

$$\begin{gathered} y1_n = X_{n+p}; \\ y2_n = (y1_n + (y1_n >> u)); \\ y3_n = (y2_n + (y2_n << s) \cdot b); \\ y4_n = (y3_n + (y3_n << t) \cdot c); \\ y5_n = (y4_n + (y4_n >> l)); \\ y_n = y5_n. \end{gathered} \quad (6)$$

Для реализации генератора на основе метода Мерсенна Твистера выбраны следующие параметры: $p = 624$; $q = 397$; $w = 32$; $r = 31$; $u = 11$; $s = 7$; $t = 15$; $l = 18$.

Для исследования разработанных генераторов на случайность оценивались результаты прохождения псевдослучайных последовательностей 16-ти тестов NIST [7], представленных в табл. 1.

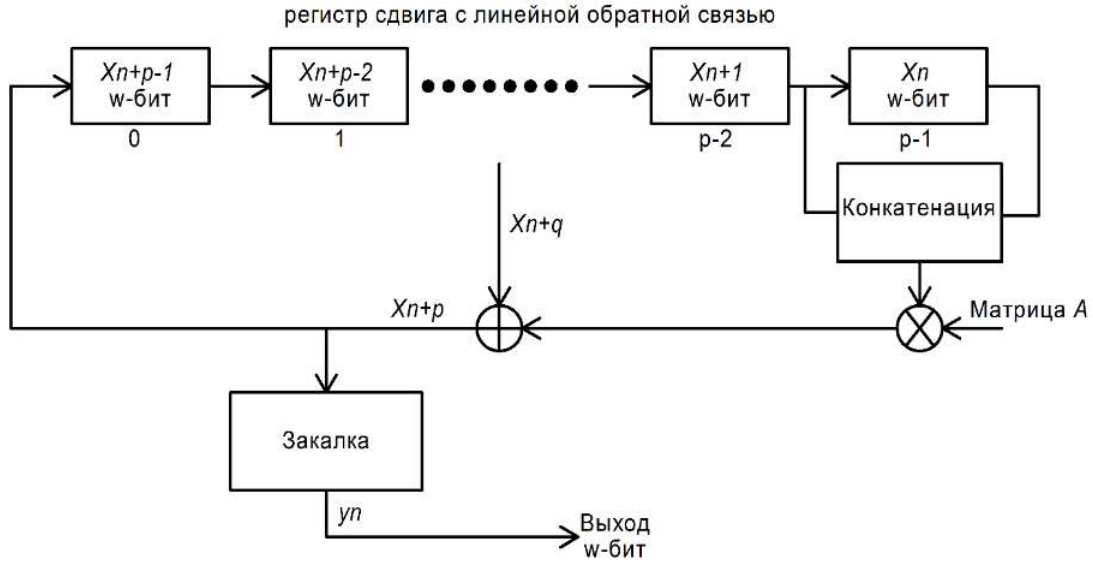

Рис. 2. Блок-схема генератора на основе метода Мерсенна Твистера
Fig. 2. Block diagram of the generator based on Mersenne Twister

Таблица 1. **Описание тестов NIST**
Table 1. Description of NIST tests

Тест № 1	Частотный побитовый тест	Определяет соотношения единиц и нулей в последовательности
Тест № 2	Частотный блочный тест	Определяет соотношения единиц и нулей в блоке определённой длины
Тест № 3	Тест на последовательность одинаковых битов	Определяет степень чередования единиц и нулей в последовательности
Тест № 4	Тест на самую длинную последовательность единиц в блоке	Определяет соотношение между самым длинным рядом единиц в блоке и ожидаемой длиной единиц в случайной последовательности
Тест № 5	Тест рангов бинарных матриц	Осуществляет расчёт рангов непересекающихся подматриц, образованных исходной двоичной последовательностью
Тест № 6	Спектральный тест	Оценивает высоты пиков при дискретном преобразовании Фурье исходной последовательности
Тест № 7	Тест приблизительной энтропии	Оценивает частоту всех возможных перекрываний блоков определённой длины
Тест № 8	Тест на совпадение непересекающихся шаблонов	Оценивает количество заранее определённых шаблонов в исходной последовательности
Тест № 9	Тест на совпадение пересекающихся шаблонов	Оценивает количество шаблонов, образованных исходной последовательностью со смещением на 1 бит
Тест № 10	Тест на подпоследовательности	Оценивает частоту нахождения всевозможных последовательностей определённой длины внутри исходной последовательности
Тест № 11	Тест на произвольные отклонения	Осуществляет расчёт кумулятивных сумм для 8-ми состояний циклов, образованных с помощью исходной последовательности
Тест № 12	Разновидность теста на произвольные отклонения	Осуществляет расчёт кумулятивных сумм для большего по сравнению с предыдущим тестом состояний циклов
Тест № 13	Тест на линейную сложность	Анализирует исходную последовательность по принципу работы линейного регистра сдвига с обратной связью
Тест № 14, Тест № 15	Тест кумулятивных сумм	Осуществляет расчёт кумулятивных сумм исходной последовательности с первого элемента до последнего и с последнего до первого соответственно
Тест № 16	Универсальный статистический тест Маурера	Оценивает степень сжимаемости исходной последовательности

Система тестов построена на основе проверки нулевой гипотезы. За нулевую гипотезу будет приниматься предположение, что проверяемая двоичная последовательность является истинно случайной. В этом случае последовательность будет обладать хорошими статистическими характеристиками. Альтернативной гипотезой будет считаться предположение о том, что тестируемая последовательность не случайна.

На вход каждого теста подавались сформированные генераторами псевдослучайных чисел конечные последовательности, для которых вычислялась статистика, характеризующая некое их свойство. Для оценки последовательностей на случайность полученная статистика сравнивалась с эталонной статистикой случайного ряда. По результатам сравнения высчитывалось значение P, характеризующее схожесть последовательности, сформированной разработанным генератором, с идеально случайной последовательностью. Полученное значение P сравнивалось с уровнем значимости α, $\alpha \in [0{,}001; 0{,}01]$.

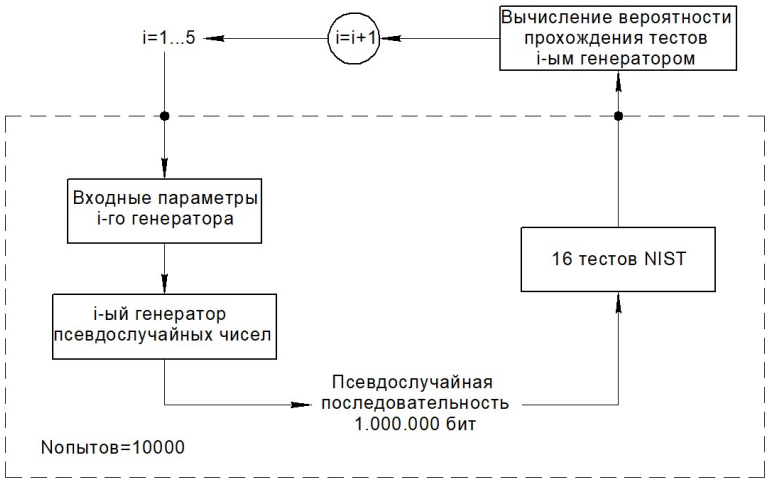

Рис. 3. Блок-схема разработанной модели
Fig. 3. Block diagram of developed model

При помощи программного средства MATLAB разработана модель формирования псевдослучайных последовательностей и проверки сформированной последовательности на случайность при помощи тестов NIST путём расчёта вероятности прохождения тестов при проведении 10 000 опытов. Блок-схема разработанной модели приведена на рис. 3.

При запуске модели переменная *i*, определяющая порядковый номер проверяемого генератора пседвослучайных чисел, выбирается равной 1. Для выбранного генератора определяются заранее заданные входные параметры и формируется двоичная псевдослучайная последовательность длиной 1 000 000 бит. Сформированная последовательность проходит параллельно 16 тестов NIST. По результатам 100 000 опытов набирается статистика, в ходе которой оценивается вероятность прохождения тестов для 1-го генератора. Аналогичный принцип расчёта вероятности применяется для остальных генераторов псевдослучайных чисел (при $i = 2…5$).

Результаты и их обсуждение

Разработаны программные средства моделирования для исследования двоичных последовательностей на «случайность» при помощи тестов NIST. Оценка производилась по вероятности прохождения тестов двоичных последовательностей длиной 1 000 000 бит, сформированных генераторами псевдослучайных чисел на основе метода М-последовательности (Ген. № 1), пятипараметрического метода (Ген. № 2), метода Таусворта (Ген. № 3), комбинированного метода Таусворта (Ген. № 4), метода Мерсенна Твистера (Ген. № 5). Полученные вероятности прохождения тестов NIST генераторами при проведении 10 000 опытов представлены в табл. 2.

Таблица 2. **Оценки вероятностей прохождения тестов NIST**
Table 2. Estimates of the probabilities of passing NIST tests

	Тест № 1	Тест № 2	Тест № 3	Тест № 4	Тест № 5	Тест № 6	Тест № 7	Тест № 8
Ген. № 1	0,9997	0,9997	0,9997	0,9691	0	0	0,9997	0,0306
Ген. № 2	0,3194	0	0,1575	0	0,9927	0	0,0012	0
Ген. № 3	0,9773	0,9734	0,9816	0	0	0	0,9999	0,9847
Ген. № 4	0,4798	0,8132	0,3530	0,3127	0,9429	0,0006	0,0770	0,8526
Ген. № 5	0,9898	0,9890	0,9889	0,5687	0,9921	1	0,9999	0,9894
	Тест № 9	Тест № 10	Тест № 11	Тест № 12	Тест № 13	Тест № 14	Тест № 15	Тест № 16
Ген. № 1	0,9997	0,9997	0,0014	0,5278	0	0,9997	0,9997	0,9997
Ген. № 2	1	0,0135	0,4048	0,9029	0,9895	0,0171	0,0182	1
Ген. № 3	0,9999	0,9951	0,0469	0,8553	0	0,9806	0,9816	0,9999
Ген. № 4	0,9715	0,1091	0,2843	0,8947	0,9537	0,4974	0,4984	0,9878
Ген. № 5	1	0,9821	0,0807	0,7022	0,9901	0,9903	0,9897	1

Для упрощения анализа полученных результатов успешность прохождения теста соответствующего генератора оценивалась по уровню пороговой вероятности равной 0,7. Количество успешно пройденных тестов NIST для разработанных генераторов псевдослучайных чисел представлено на рис. 4.

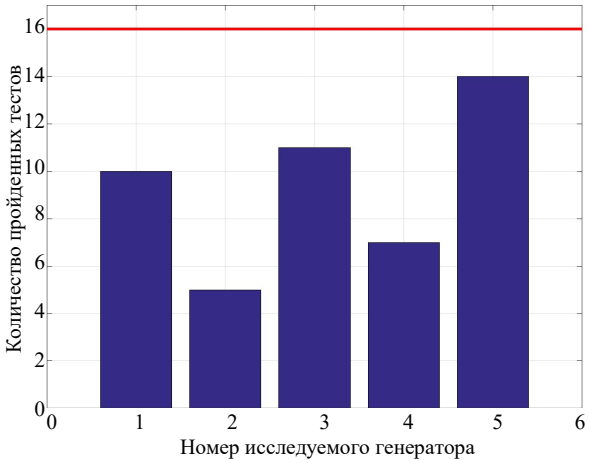

Рис. 4. Количество тестов, пройденных генераторами
Fig. 4. The number of tests passed by the generators

Наименьшее количество пройденных тестов характерно для генераторов № 2, № 4. Генераторы № 1, № 3 имеют сопоставимое количество пройденных тестов. Наиболее приближенной к эталонному случайному ряду является последовательность, сформированная генератором на основе метода Мерсенна Твистера (Ген. № 5), которая характеризуется наибольшим количеством успешно пройденных тестов NIST – 14.

Дальнейший анализ табл. 2 показывает, что существуют нулевые вероятности прохождения генератором № 1 тестов № 5, № 6, № 13; генератором № 2 тестов № 2, № 4, № 6, № 8; генератором № 3 тестов № 4, № 5, № 6, № 13 при выбранных параметрах моделирования. Установлено, что повышения вероятности прохождения некоторых тестов возможно добиться вариацией входных параметров метода генерации, формирующего последовательность с более высоким уровнем «случайности». Для выработки оптимальных с точки зрения «случайности» входных параметров разработанных генераторов требуются дополнительные исследования, выходящие за рамки данной работы.

Следует также отметить низкую вероятность прохождения тестов № 4, № 6, № 11 чисел, формируемых генераторами при выбранных параметрах. Низкая вероятность прохождения теста № 4 говорит о появлении длинных последовательностей единиц (нулей). Низкая вероятность прохождения теста № 6 показывает наличие большого количества спектральных пиков проверяемых последовательностей, что подтверждает рис. 5, на котором представлена спектральная характеристика генератора, построенного на основе М-последовательности. Для сравнения на рис. 5 приведён пороговый уровень, относительно которого очевидно наличие в спектре проверяемого сигнала высоких пиков. Результаты теста № 11 показывают наличие большой величины отклонений при расчёте кумулятивных сумм восьми состояний последовательностей, однако в данном тесте возможна неопределённость результатов прохождения, и в этом случае решение о схожести проверяемой последовательности с идеально случайной принимается на основе других тестов.

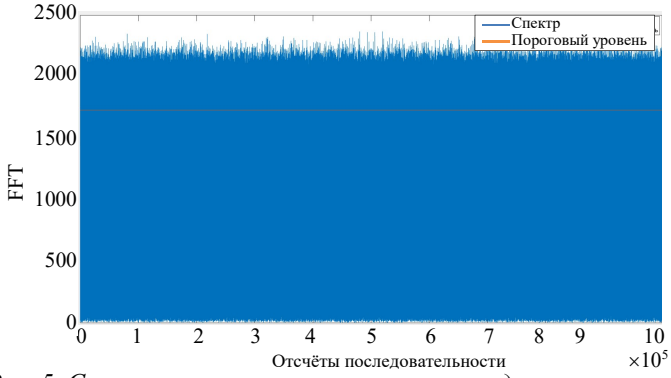

Рис. 5. Спектральная характеристика последовательности
Fig. 5. Spectral characteristic of a sequence

Заключение

В данной статье разработаны средства моделирования генераторов псевдослучайных чисел по ГОСТ Р ИСО 28640 – 2012 и проведена проверка формируемых ими последовательностей на случайность посредством прохождения тестов NIST. Проведённый анализ прохождения тестов NIST показал, что псевдослучайные последовательности, формируемые методами М-последовательности, соответствуют 10 тестам, пятипараметрическим методом – 5 тестам, методом Таусворта – 11 тестам, комбинированным методом Таусворта – 7 тестам, методом Мерсенна Твистера – 14 тестам с вероятностью не ниже 0,7. По результатам оценки установлено, что в качестве генераторов псевдослучайных чисел для стендов полунатурного моделирования асинхронных радиоэлектронных систем рекомендуется применение метода Мерсенна Твистера. Кроме того, оценки вероятностей прохождения тестов последовательностями, рассмотренными в данной работе, делают необходимым дальнейшее совершенствование генераторов псевдослучайных чисел с целью повышения вероятностей прохождения ими статистических тестов.

Список источников

1. Полунатурное моделирование радиотехнических систем / А. Б. Герасимов, А. Н. Кренёв, Е. А. Селянская. Ярославль: Яросл. гос. ун-т им. П. Г. Демидова, 2014. 128 с.

2. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер. с англ. М.: Издательский дом «Вильямс», 2003. 1104 с.

3. *Loginov S. S., Zuev M. Y.* Testing of generators of pseudo-random signals based on a Lorenz system, realized over a Galois finite field // 2018Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). 2018. Pp. 1-4. DOI: 10.1109/SYNCHROINFO.2018.8457039; EDN: JIIYRM

4. A statistical test suite for random and pseudorandom number generators for cryptographic application / A. Rukhin, J. Soto, J. Nechvatal et al. // NIST Special Publication. 800-22 Revision la. Gaithersburg. ational Institute of Standards and Technology, 2010. 131 p. DOI:10.6028/NIST.SP.800-22R1A

5. Генераторы псевдослучайных последовательностей немаксимальной длины на регистрах сдвига / В.А. Песошин, В.М. Кузнецов, А.С. Кузнецова и др. // Известия высших учебных заведений. Поволжский регион. Технические науки. 2019. № 1 (49). С. 3-17. DOI: 10.21685/2072-3059-2019-1-1; EDN: DNUPEW

6. *Гавришев А. А.* К вопросу об использовании гиперхаотических сигналов для передачи данных в системах радиосвязи // Научное приборостроение. 2023. Т. 33, № 2. С. 62-74. DOI: 10.18358/23122951_2023_33_2_62; EDN: RWJYDI

7. *Перов А.А.* Применение статистических тестов NIST для анализа выходных последовательностей блочных шифров // Научный вестник НГТУ. 2019. № 3 (76). С. 87-96. DOI: 10.17212/1814-1196-2019-3-87-96; EDN: UXVEEP

Статья поступила в редакцию 28.06.2024; одобрена после рецензирования 05.12.2024; принята к публикации 09.12.2024

Информация об авторах

РАУПОВ Руслан Рустемович – инженер (схемотехник) 3 категории, АО «НПО «Радиоэлектроника» им. В.И. Шимко». Область научных интересов – генераторы псевдослучайных чисел, цифровые системы передачи информации, динамический хаос. Автор 20 научных публикаций.

ЛОГИНОВ Сергей Сергеевич – доктор технических наук, доцент, профессор кафедры электронных и квантовых средств передачи информации, Казанский национальный исследовательский технический университет им. А.Н. Туполева - КАИ; ведущий инженер-конструктор (схемотехник) – ведущий научный сотрудник, АО «НПО «Радиоэлектроника» им. В.И. Шимко». Область научных интересов – цифровые системы передачи информации, системы опознавания, динамический хаос. Автор 100 научных публикаций. SPIN-код: 9460-6294

ФРОЛОВ Игорь Николаевич – кандидат технических наук, директор по научной работе (руководитель Департамента перспективных разработок), АО «НПО «Радиоэлектроника» им. В.И. Шимко». Область научных интересов – системы опознавания, БПЛА. Автор 50 научных публикаций.

БУТКЕВИЧ Юрий Рудольфович – аспирант кафедры электронных и квантовых средств передачи информации, Казанский национальный исследовательский технический университет им. А.Н. Туполева - КАИ; инженер (схемотехник) 3 категории, АО «НПО «Радиоэлектроника» им. В.И. Шимко». Область научных интересов – цифровые системы передачи информации, системы опознавания, динамический хаос. Автор 20 научных публикаций. SPIN-код: 5204-9499

Вклад авторов:

Раупов Р. Р. – разработка и программная реализация генераторов псевдослучайных чисел; анализ результатов.

Логинов С. С. – концепция работы; интерпретация данных; анализ результатов.

Фролов И. Н. – концепция работы.

Буткевич Ю. Р. – разработка и программная реализация статистических тестов NIST.

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Все авторы прочитали и одобрили окончательный вариант рукописи.

Scientific article
UDC 519.6
DOI: https://doi.org/10.25686/2306-2819.2024.4.68
EDN: TYWPLM

Randomness Testing of Pseudorandom Number Generators for Semi-Natural Simulation Stands in Asynchronous Electronic Systems

R. R. Raupov[1], S. S. Loginov[1,2], I. N. Frolov[1], Y. R. Butkevich[1,2]✉

[1]JSC «Scientific and Production Association «Radioelectronics», named after V.I. Shimko»,
50, Journalists St., Kazan, 420088, Russian Federation

[2]Kazan National Research Technical University named after A.N. Tupolev – KAI,
10, K.Marx St., Kazan, 420111, Russia

Email: bytkevic@mail.ru✉

Abstract. *Introduction.* To accurately reproduce test conditions in semi-natural simulation stands, it is essential to generate signals with various probability distributions over power and time. Pseudorandom number generators (PRNGs) are commonly used for this purpose. Given their practical application in semi-natural simulation stands, evaluating the randomness of their generated sequences is crucial. The NIST statistical test suite is widely used to assess the randomness of number sequences. It determines the statistical similarity between a generated pseudorandom sequence and a theoretically perfect random sequence. This study **aims** at analyzing the performance of binary sequences generated by PRNGs—defined by GOST R ISO 28640-2012—in NIST randomness tests using a developed simulation software. *Methods and Tools.* This research involves developing software tools to simulate PRNGs based on GOST R ISO 28640-2012 using the following methods: five-parameter method; Tausworthe method; combined Tausworthe method; Mersenne Twister method. To assess the randomness of these generators, their output sequences were subjected to 16 NIST statistical tests. Each test evaluated finite-length sequences, calculating statistics and comparing them with reference statistics of a perfectly random sequence. *Results.* The study found that the Mersenne Twister method generated the sequence most closely resembling a true random series, passing 14 out of 16 NIST tests. Furthermore, it was observed that modifying the input parameters of certain PRNG methods could enhance their ability to pass specific tests, thereby improving the overall "randomness" of the generated sequences. *Conclusion.* This research developed and implemented software tools for modeling PRNGs based on GOST R ISO 28640-2012 and evaluated their randomness using the NIST test suite. The results indicate that the Mersenne Twister method is the most suitable PRNG for semi-natural simulation stands in asynchronous electronic systems. Additionally, further improvements to PRNG algorithms are necessary to increase their statistical test pass rates.

Keywords: pseudorandom number generator; pseudorandom sequence; NIST statistical tests; randomness testing; semi-natural simulation stand

Funding: this study was not supported by any external sources of funding.

For citation: Raupov R. R., Loginov S. S., Frolov I. N. et al. Randomness Testing of Pseudorandom Number Generators for Semi-Natural Simulation Stands in Asynchronous Electronic Systems. *Vestnik of Volga State University of Technology. Ser.: Radio Engineering and Infocommunication Systems*. 2024;(4):68–77. https://doi.org/10.25686/2306-2819.2024.4.68; EDN: TYWPLM

REFERENCES

1. Gerasimov A.B., Krenyov A.N., Selyanskaya E.A. Semi-naturalistic modeling of radio engineering systems. Yaroslavl, P.G. Demidov Yaroslavl State University; 2014. 128 p. (In Russ.).

2. Skljar B. Digital communications: fundamentals and applications. Ed. 2nd, rev.: Trans. from English. Moscow, «Viljams» publishing house; 2003. 1104 p. (In Russ.).

3. Loginov S.S., Zuev M.Yu. Testing of generators of pseudo-random signals based on a Lorenz system, realized over a Galois finite field. *2018 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO),* 2018:1-4. DOI: 10.1109/SYNCHROINFO.2018.8457039; EDN: JIIYRM

4. Rukhin A., Soto J., Nechvatal J. et al. A statistical test suite for random and pseudorandom number generators for cryptographic application. Special Publication (NIST SP). Gaithersburg, MD, National Institute of Standards and Technology; 2010. 131 p. DOI:10.6028/NIST.SP.800-22R1A

5. Pesoshin V.A., Kuznetsov V.M., Kuznetsova A.S. et al. The generators of pseudorandom sequences of a namaximum length on shift registers. *University proceedings. Volga region. Technical sciences.* 2019;(1):3-17. DOI: 10.21685/2072-3059-2019-1-1; EDN: DNUPEW (In Russ.).

6. Gavrishev A.A. On the use of hyperchaotic signals for data transmission in radio communication systems. *Nauchnoe priborostroenie*. 2023;33(2):62-74. DOI: 10.18358/23122951_2023_33_2_62; EDN: RWJYDI (In Russ.).

7. Perov A.A. Using NIST statistical tests for the analysis of the output sequences of block ciphers. *Nauchnii Vestnik NGTU*. 2019;(3):87-96. DOI: 10.17212/1814-1196-2019-3-87-96; EDN: UXVEEP (In Russ.).

The article was submitted 28.06.2024; approved after reviewing 05.12.2024; accepted for publication 09.12.2024

Information about the authors

Ruslan R. Raupov – Engineer (circuit engineer, 3rd category), «Scientific and Production Association «Radioelectronics», named after V.I. Shimko». Research interests – pseudorandom number generators, digital information transmission systems, and dynamic chaos. The author of 20 scientific publications.

Sergei S. Loginov – Doctor of Engineering Sciences, Associate Professor, and Professor at the Department for Radio-Electronic and Quantum Devices of Kazan National Research Technical University named after A.N. Tupolev - KAI; Leading design-engineer (circuit engineer) and Leading researcher at «Scientific and Production Association «Radioelectronics», named after V.I. Shimko». Research interests – digital data transmission systems, identification systems, dynamic chaos. The author of 100 scientific publications. SPIN: 9460-6294

Igor N. Frolov – Candidate of Engineering Sciences and Director of Scientific Research (Head of the Advanced Development Department), «Scientific and Production Association «Radioelectronics», named after V.I. Shimko». Research interests – identification systems, UAVs. The author of 50 scientific publications.

Yuri R. Butkevich – PhD student at the Department for Radio-Electronic and Quantum Devices, Kazan National Research Technical University named after A.N. Tupolev - KAI. Engineer (circuit engineer, 3rd category) at «Scientific and Production Association «Radioelectronics», named after V.I. Shimko». Research interests are digital information transmission systems, identification systems, dynamic chaos. The author of 20 scientific publications. SPIN: 5204-9499

Contribution of authors:

Raupov R. R. – development and software implementation of pseudorandom number generator; gathering of experimental data.

Loginov S. S. – concept development; data interpretation; gathering of experimental data.

Frolov I. N. – concept development.

Butkevich Y. R. – development and software implementation of NIST statistical tests.

Conflict of interests: the authors declare no conflict of interest.

All authors reviewed and approved the final version of the manuscript.