ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 621.396

ТЕСТИРОВАНИЕ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ СИГНАЛОВ НА ОСНОВЕ СИСТЕМЫ ЛОРЕНЦА

Логинов С.С., Буткевич Ю.Р., Сивинцева О.А.
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ, Казань, РФ
E-mail: bytkevic@mail.ru

В данной работе представлены результаты тестирования модифицированных генераторов псевдослучайных сигналов. Рассмотрены два генератора, построенных на основе системы Лоренца с хаотической динамикой. Первый генератор описывается системой Лоренца, реализованной над полем Галуа, а второй описывается системой Лоренца, в которой формирование цифровой последовательности происходит методом периодической выборки из сигнатур сигналов. В качестве дополнительного подтверждения релевантности полученных результатов в работе оценивается генератор, построенный на основе стандартной функцией Matlab по формированию бинарной случайной последовательности. Тестирование генераторов осуществлялось с помощью набора тестов, разработанного Национальным институтом стандартов и технологий, который включает в себя 15 различных тестов. Полученные результаты сравниваются с результатами, полученные при тестировании эталонных генераторов. Результаты данного исследования могут быть применены при построении криптографических систем и систем передачи информации.

Ключевые слова: *генераторы псевдослучайных сигналов, система Лоренца, поля Галуа, тесты NIST*

Введение

Генераторы псевдослучайных чисел являются ключевым звеном любой криптографической системы. Надежность таких систем обусловлена статистическими свойствами последовательностей, формируемых генераторами. Поэтому со-здание генераторов псевдослучайных чисел с характеристиками, наиболее близкими к характеристикам случайных чисел, является важной и актуальной задачей.

Одним из источников формирования псевдослучайных последовательностей с требуемыми статистическими характеристиками в системах передачи информации может служить динамический хаос, который обеспечивает возможность существования сложного, непредсказуемого поведения. Динамический хаос, в отличии от шума, являющегося случайным процессом, описывается детерминированными системами уравнений. На сегодняшний день известны нелинейные динамические системы Лоренца, Ресслера, Дмитриева-Кислова, генераторы с инерционной нелинейностью Анищенко-Астахова, осциллятор Ван-дер-Поля и другие [1–3].

В данной работе проводятся исследования двух модифицированных генераторов с псевдослучайных сигналов на базе динамической системы Лоренца. В первом случае рассматривается система Лоренца, где операции выполняются над полем Галуа, а во втором случае используется система Лоренца в условиях квазирезонансных воздействий, где формирование цифровой последовательности происходит методом периодической выборки из сигнатур сигналов.

Одним из методов оценки качества генераторов псевдослучайных чисел является тестирование «на случайность» полученных последовательностей. Для тестирования последовательностей и определения их схожести со случайной существуют различные наборы тестов: Д. Кнута, Crypt-X, FIPS 140-2, NIST и др. [4].

В работе применяется набор статистических тестов NIST, разработанный Национальным институтом стандартов и технологий (National Institute of Standards and Technology).

Целью работы является сопоставительный анализ модифицированных генераторов псевдослучайных сигналов на основе системы Лоренца с помощью набора тестов NIST.

Динамические системы Лоренца

Высокие требования к безопасности систем передачи информации делает актуальным применение в таких системах криптографических и некриптографических методов защиты на основе хаотической динамики.

Однако, реализация генераторов хаоса на основе цифровой схемотехники оказывается до-вольно сложной за счет применения операций с плавающей/фиксированной запятой. В связи с этим предлагается использовать более удобные для реализации в цифровой форме модифициро-

ванные генераторы псевдослучайных сигналов. Например, генераторы с выполнением операций над полями Галуа [5–6].

В данной работе в качестве исходной системы была выбрана нелинейная динамическая система Лоренца. После ее модификации и реализации операций уравнения в полях Галуа система описывается следующим уравнением:

$$\begin{cases} X_{i+1} = X_i \oplus t \otimes (\sigma \otimes X_i \oplus \sigma \otimes Y_i); \\ Y_{i+1} = Y_i \oplus t \otimes (r \otimes X_i \oplus Y_i \oplus X_i \otimes Z_i); \\ Z_{i+1} = Z_i \oplus t \otimes (b \otimes Z_i \oplus X_i \otimes Y_i). \end{cases} \quad (1)$$

где t – шаг интегрирования; r, σ, b – параметры системы, все операции выполняются над полем Галуа.

С целью проведения более полного исследования в работе также рассматривается генератор псевдослучайных сигналов с управляемыми характеристиками, основанный на системе Лоренца в условиях квазирезонансных воздействий, где формирование последовательности происходит методом выборки полученной реализации через равные промежутки времени (1):

$$\begin{cases} X_{i+1} = X_i + t_i \cdot (-\sigma \cdot X_i + -\sigma \cdot Y_i); \\ Y_{i+1} = Y_i + t_i \cdot (r \cdot X_i - Y_i - X_i \cdot Z_i); \\ Z_{i+1} = Z_i + t_i \cdot (-b \cdot Z_i + X_i \cdot Y_i). \end{cases}$$

где $t_i = \Delta t(1 + mf_{i-1}), f_{i-1} = \mathrm{sgn}\left(\frac{|X_i|}{X^*} \pm a\right)$ – временная функция управляющего воздействия, Δt – величина шага, $a = X / X_{01}$, m – глубина модуляции.

Тесты NIST

В 1999 г. Национальным институтом стандартов и технологий был разработан набор статистических тестов NIST, на основе которых была предложена методика тестирования генераторов псевдослучайных чисел [7].

Статистические тесты являются мерой определения степени случайности последовательностей, создаваемых генераторами псевдослучайных сигналов. Тесты NIST представляют собой 15 тестов, в основе которых лежит принцип определения статистики, характеризующей некое свойство последовательности, с последующим ее сравнением с эталонной статистикой, полученной от случайной последовательности [8].

Рассмотрим подробно каждый из тестов:

1. Частотный (монобитный) тест определяет соотношение нулей и единиц в последовательности.

2. Частотный блочный тест определяет соотношение количества единиц и нулей в блоке длиной m (в данном исследовании $m = 3$).

3. Тест на последовательность одинаковых битов, в ходе которого определяется скорость чередования единиц и нулей.

4. Тест на нахождение наиболее длинной последовательности единиц в блоке определяет самый длинный ряд единиц внутри блока длиной m бит. Длина блока определяется динамически из длин 8, 128 и 10000 в зависимости от длины последовательности. Тест может проводиться несколько раз до окончания исходной последовательности.

5. Тест рангов бинарных матриц производит подсчет рангов непересекающихся подматриц, построенных из исходной бинарной последовательности (данный тест не проводился ввиду того, что длина исходной последовательности меньше 38912).

6. Спектральный тест, который оценивает пики после дискретного преобразования Фурье исходной бинарной последовательности.

7. Тест приблизительной энтропии, подсчитывающий частоты всех возможных перекрываний шаблонов длины m бит (в данном исследовании m = 3).

8. Тест на совпадение неперекрывающихся шаблонов, в котором подсчитывается количество заранее определенных шаблонов, найденных в исходной последовательности (длина шаблона принята равной 9).

9. В тесте на совпадение перекрывающихся шаблонов в отличие от теста № 8 поиск шаблона происходит со смещением на 1 бит (длина шаблона принята равной 3).

10. Тест на периодичность, ведущий подсчет частот всех возможных перекрываний шаблонов длины m бит на протяжении исходной последовательности битов.

11. Тест на произвольные отклонения – набор из восьми тестов, проводимых для каждого из восьми состояний цикла (-4 -3 -2 -1 1 2 3 4), представляющего серию случайных шагов единичной длины.

12. Разновидность теста на произвольные отклонения, отличающегося от предыдущего теста количеством анализируемых состояний (от -9 до 9 с шагом 1).

13. Тест на линейную сложность анализирует исходную последовательность по принципу работы линейного регистра сдвига с обратной связью.

14–15) Тест кумулятивных сумм находит отклонения от нуля при произвольном обходе, определяемом кумулятивной суммой биполярной исходной последовательности, тест № 14 и тест № 15 отличаются началом отсчета от начала или от конца исходной биполярной последовательности.

Таблица 1. Результаты прохождения тестов NIST разными генераторами псевдослучайных сигналов

№ ген.	№1	№2	№3	№4	№6	№7	№8	№9	№10	№11	№12	№13	№14	№15	№16
1	9909	9978	9887	0	9884	9995	0	14	7489	5019	8944	10000	4898	4887	10000
2	9455	5310	3183	0	9870	6371	0	0	644	5011	9051	10000	4922	4942	10000
3	9907	9990	9905	0	9878	9995	0	7	7442	4978	8984	10000	4846	4830	10000

Таблица 2. Результаты определения доверительных интервалов на основе проведенных тестов

№ ген.	1			2			3		
Ном. теста	P_H	P	P_B	P_H	P	P_B	P_H	P	P_B
1	0,9876	0,9909	0,9933	0,9383	0,9455	0,9519	0,9873	0,9907	0,9932
2	0,9959	09978	0,9988	0,5160	0,5310	0,5459	0,9975	0,9990	0,9996
3	0,9851	0,9887	0,9915	0,3045	0,3183	0,3324	0,9871	0,9905	0,9930
4	$1{,}08 \cdot 10^{-19}$	0	$8{,}99 \cdot 10^{-4}$	$1{,}08 \cdot 10^{-19}$	0	$8{,}99 \cdot 10^{-4}$	$1{,}08 \cdot 10^{-19}$	0	$8{,}99 \cdot 10^{-4}$
6	0,9847	0,9884	0,9912	0,9831	0,9870	0,9900	0,9840	0,9878	0,9907
7	0,9982	0,9995	0,9999	0,6226	0,6371	0,6514	0,9982	0,9995	0,9999
8	$1{,}08 \cdot 10^{-19}$	0	$8{,}99 \cdot 10^{-4}$	$1{,}08 \cdot 10^{-19}$	0	$8{,}99 \cdot 10^{-4}$	$1{,}08 \cdot 10^{-19}$	0	$8{,}99 \cdot 10^{-4}$
9	$6{,}41 \cdot 10^{-4}$	0,0014	0,0031	$1{,}08 \cdot 10^{-19}$	0	$8{,}99 \cdot 10^{-4}$	$2{,}38 \cdot 10^{-4}$	$7{,}00 \cdot 10^{-4}$	0,0021
10	0,7357	0,7489	0,7617	0,0574	0,0644	0,0722	0,7309	0,7442	0,7571
11	0,4869	0,5019	0,5169	0,4861	0,5011	0,5161	0,4828	0,4978	0,5128
12	0,8848	0,8944	0,9033	0,8959	0,9051	0,9135	0,8890	0,8984	0,9071
13	0,9991	1	1	0,0914	0,1000	0,1094	0,9991	1	1
14	0,4748	0,4898	0,5048	0,4772	0,4922	0,5072	0,4696	0,4846	0,4996
15	0,4737	0,4887	0.5037	0.4792	0.4942	0.5092	0.4680	0.4830	0.4980
16	0,0913	0,1000	0,1094	0,9991	1	1	0,9991	1	1

16) Универсальный статистический тест Маурера определяет число бит между одинаковыми шаблонами в исходной последовательности.

Результаты тестирования

В данной работе проводились тестирование и сравнительный анализ генераторов псевдослучайных последовательностей. Анализ проводился на основе оценки прохождения или непрохождения последовательностей вышеописанных тестов, формируемых генераторами.

В ходе эксперимента сравнивались три генератора. Генератор № 1 является генератором псевдослучайных сигналов на основе системы Лоренца, где операции уравнений реализованы в полях Галуа. Генератор № 2 построен на основе системы Лоренца, подверженной квазирезонансным воздействиям. В качестве дополнительного подтверждения релевантности был предложен Генератор № 3, являющийся стандартной функцией Matlab по формированию бинарной случайной последовательности. Алгоритм генерации в генераторе № 3 основан на линейном конгруэнтном методе.

Формирование последовательностей генераторами № 1 и № 2 осуществлялось при случайных начальных условиях, а генератор № 3 перезапускался при каждом опыте. Было проведено 10000 опытов, результаты прохождения тестов NIST приведены в таблице 1.

На основе проведенных опытов определена вероятность прохождения каждого теста , а также оценена точность и надежность полученных результатов. Точность и надежность оценивалась с помощью доверительного интервала. На основе проведения бесконечно большого количества испытаний может быть получено некоторое эталонное значение вероятности события. В реальности число проводимых испытаний всегда ограничено, из-за чего вместо эталонного значения вероятности вычисляется значение на основе этих испытаний. Такая замена параметра неизбежно приведет к появлению ошибки, выражающейся в колебании значении вероятности прохождения теста на некотором интервале $Рн < P < Рв$. Вероятность попадания в заданный интервал равна числу , за-

висящему от ширины указываемых границ. Доверительные интервалы (при) для каждого теста и каждого генератора приведены в таблице 2.

Генератор № 1 прошел тесты № 1–3, 6–7, 12–13, 16 с вероятностью более 89%, тесты № 10–11, 14–15 с вероятностью более 48%. Тесты № 4, № 8–9 не были пройдены.

В то же время, Генератор № 2 прошел тесты № 1, 6, 12–13, 16 с вероятностью более 90%, тесты № 2,7,11 с вероятностью более 50%, тесты № 3, 10, 12–15 с вероятностью менее 50%. Тесты № 4, № 8–9 не были пройдены.

Генератор № 3 прошел тесты № 1–3, 6–7, 12–13, 16 с вероятностью более 89%, тесты № 10–11, 14–15 с вероятностью более 48%. Тесты № 4, № 8–9 не пройдены. Генераторы № 1, № 3 показали схожие результаты.

Вероятность одновременного прохождения 86,6% тестов NIST Генератором № 1 составляет 7,77%, Генератором № 2 – 0,07%, генератором № 3 – 7,53%. Исходя из полученных результатов, ни один из генераторов не проходит тесты № 4, № 8, № 9, следовательно, и не проходит полный набор тестов NIST.

Отметим, что в методических рекомендациях к NIST [9] приведены результаты прохождения тестов эталонными генераторами. Например, генератор возведения в степень по модулю (Modular Exponentiation) и генератор, выполняющий операцию исключающую ИЛИ (XOR), также, как и вышеописанные нами генераторы, не проходят тесты № 8 и № 9. Кроме того, гене-ратор Modular Exponentiation не проходит тесты № 1, 3, 12, 7, 8, 14, 15. Расширенные результаты тестирования представлены в Приложении D работы [9].

В отличие от эталонных генераторов из [9], рассмотренные в данной работе генераторы не проходят тест № 4, тест на самую длинную последовательность единиц в блоке. Это связано с тем, что длина блока определяется динамически из длин 8, 128 и 10000.

Ранее в работе [10] проводилось тестирование генератора на основе системы Лоренца, реализованной в полях Галуа, с помощью другого набора тестов FIPS-140-2, и полученные последовательности успешно прошли проверку «на случайность» по результатам тестирования. Таким образом, можно сделать вывод, что тесты NIST предъявляют более расширенные требования по сравнению с тестами FIPS-140-2.

Заключение

В данной работе представлены результаты тестирования модифицированных генераторов псевдослучайных сигналов. Рассмотрены два генератора на основе динамической системы Лоренца. Генератор № 1 построен на основе системы Лоренца, в которой операции уравнений реализованы в полях Галуа, Генератор № 2 основан на системе Лоренца, в которой формирование цифровой последовательности происходит методом периодической выборки из сигнатур сигналов.

В качестве дополнительного подтверждения релевантности был предложен Генератор № 3, являющийся стандартной функцией Matlab по формированию двоичной случайной последовательности.

Тестирование вышеописанных генераторов осуществлялось с помощью набора тестов NIST, разработанного Национальным институтом стандартов и технологий.

Генератор № 1 с вероятностью более 89% прошел тесты № 1–3, 6–7, 12–13, 16. Генератор № 2 с вероятностью более 90% прошел тесты № 1, 6, 12–13, 16. Генератор № 1 прошел больше тестов, чем Генератор № 2.

Генератор № 3, реализованный на алгоритме работы Matlab, с вероятностью более 89% прошел тесты № 1–3, 6–7, 12–13, 16.

Проведенные тесты NIST показали, что генератор № 1 на основе системы Лоренца, в которой операции уравнений реализованы в полях Галуа, обеспечивает характеристики, сопоставимые с встроенным генератором псевдослучайных сигналов Matalab.

Кроме того, представление в данной работе генераторы показали результаты релевантные результатом для эталонных генераторов: Modular Exponentiation, XOR и др.

Литература

1. Логинов С.С., Зуев М.Ю. Статистические характеристики генераторов псевдослучайных сигналов на основе систем Лоренца, Чуа и Дмитриева-Кислова, реализованных над конечным полем Галуа // Инженерный вестник Дона. 2018. № 4 (51). С. 1–13.
2. Зуев М. Ю., Кафаров К.М., Логинов С.С. О взаимосвязи показателей хаотической динамики и статистических характеристик псевдослучайных сигналов на основе нелинейных систем Лоренца и Чуа // Вестник Поволжского государственного технологического университета. Серия: Радиотехнические и инфокоммуникационные системы. 2021. № 2 (50). С. 21–29.
3. Логинов С.С., Зуев М.Ю., Агачева Я.Г. Генератор псевдослучайных сигналов на основе системы Лоренца, подверженной квазирезонанс-

ным воздействиям // Волновая электроника и инфокоммуникационные системы: материалы XXIII международной научной конференции. СПб: Изд-во ГУАП, 2020. Т. 1. С. 284–290.
4. Григорьев А.Ю. Методы тестирования генераторов случайных и псевдослучайных последовательностей // Ученые записки УдГУ. Серия: Математика и информационные технологии. 2017. № 1. С. 22–28.
5. Зуев М.Ю. Комплексное повышение эффективности радиоэлектронных устройств и систем передачи информации с OFDM на основе нелинейных систем с динамическим хаосом // Физика волновых процессов и радиотехнические системы. 2022. Т. 25, № 1. С. 55–64.
6. Логинов С.С. Формирователи псевдослучайных сигналов на основе модифицированной системы Лоренца, реализованной над конечным полем Галуа // Нелинейный мир. 2017. Т. 15, № 5. С. 26–29.
7. Вильданов Р.Р., Мещеряков Р.В., Бондарчук С.С. Тесты псевдослучайных последовательностей и реализующее их программное средство // Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. № 1-2 (25). С. 108–111.
8. Перов А.А. Применение статистических тестов NIST для анализа выходных последовательностей блочных шифров // Научный вестник Новосибирского государственного технического университета. 2019. № 3 (76). С. 87–96.
9. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications /A.L. Rukhin [et al.]. USA: National Institute of Standards and Technology, 2010. 131 p.
10. Логинов С.С., Зуев М.Ю. Тестирование генераторов псевдослучайных сигналов на основе системы Лоренца, реализованной над конечным полем Галуа // Системы синхронизации, формирования и обработки сигналов. 2018. № 1 (9). С. 111–114.

Получено 23.10.2023

Логинов Сергей Сергеевич, д.т.н., доцент кафедры электронных и квантовых средств передачи информации (ЭКСПИ) Казанского национального исследовательского технического университета им. А.Н. Туполева-КАИ (КНИТУ-КАИ). 420111, Российская Федерация, Республика Татарстан, г. Казань, ул. Карла Маркса, д. 10. Тел. +7 905 023-67-99. E-mail: sslogin@mail.ru

Буткевич Юрий Рудольфович, аспирант кафедры ЭКСПИ КНИТУ-КАИ. 420111, Российская Федерация, Республика Татарстан, г. Казань, ул. Карла Маркса, д. 10. Тел. +7 986 929-15-91. E-mail: bytkevic@mail.ru

Сивинцева Ольга Андреевна, аспирант кафедры ЭКСПИ КНИТУ-КАИ. 420111, Российская Федерация, Республика Татарстан, г. Казань, ул. Карла Маркса, д. 10. Тел. +7 960 033-66-55. E-mail: sivinceva96@mail.ru

TESTING OF PSEUDORANDOM SIGNAL GENERATORS BASED ON THE LORENTZ SYSTEM

Loginov S.S., Butkevich Y.R., Sivintseva O.A.
Kazan National Research Technical University named after A.N. Tupolev-KAI, Kazan, Russian Federation
E-mail: bytkevic@mail.ru

This work presents results of the testing of modified pseudorandom signal generators. Two generators developed on the basis of the Lorentz system with chaotic dynamics are considered. The first generator is described by the Lorentz system implemented over a Galois field, and the second is described by the Lorentz system in which digital sequence formation occurs by periodic sampling from signal signatures. As an additional confirmation of the relevance of the results obtained, the article valuates a generator developed on the basis of the standard Matlab function for binary random sequence generating. Generator testing was carried out using a test battery developed by the National Institute of Standards and Technology, which includes 15 different tests. The results obtained are compared with the results obtained by testing reference generators. The results of this research can be applied in the development of cryptographic and data transmission systems.

Keywords: *pseudorandom signal generators, Lorentz system, Galois fields, NIST tests*

DOI: 10.18469/ikt.2023.21.2.01

Loginov Sergey Sergeevich, Kazan National Research Technical University named after A.N. Tupolev-KAI, 10, Karl Marx Street, Kazan, Republic of Tatarstan, 420111, Russian Federation; Associate Professor of Electronic and Quantum Means of Information Transmission Department, Doctor of Technical Sciences. Tel. +7 905 023-67-99. E-mail: sslogin@mail.ru

Butkevich Yuri Rudolfovich, Kazan National Research Technical University named after A.N. Tupolev-KAI, 10, Karl Marx Street, Kazan, Republic of Tatarstan, 420111, Russian Federation; PhD Student of Electronic and Quantum Means of Information Transmission Department. Tel. +7 986 929-15-91. E-mail: bytkevic@mail.ru

Sivintseva Olga Andreevna, Kazan National Research Technical University named after A.N. Tupolev-KAI, 10, Karl Marx Street, Kazan, Republic of Tatarstan, 420111, Russian Federation; PhD Student of Electronic and Quantum Means of Information Transmission Department. Tel. +7 960 033-66-55. E-mail: sivinceva96@mail.ru

References

1. Loginov S.S., Zuev M.Yu. Statistical characteristics of pseudorandom signal generators based on Lorentz, Chua and Dmitriev-Kislov systems, implemented over a finite Galois field. *Inzhenernyj vestnik Dona*, 2018, no. 4 (51). pp. 1–13. (In Russ.)
2. Zuev M. Yu., Kafarov K. M., Loginov S. S. On the relationship between indicators of chaotic dynamics and statistical characteristics of pseudo-random signals based on nonlinear Lorentz and Chua systems. *Vestnik Povolzhskogo gosudarstvennogo tekhnologicheskogo universiteta. Seriya: Radiotekhnicheskie i infokommunikacionnye sistemy,* 2021. no. 2 (50). pp. 21–29. (In Russ.)
3. Loginov S.S., Zuev M.Yu., Agacheva Ya.G. Pseudorandom signal generator based on the Lorentz system subject to quasi-resonant influences. *Volnovaya elektronika i infokommunikacionnye sistemy: materialy XXIII mezhdunarodnoj nauchnoj konferencii.* Saint Petersburg: Izd-vo GUAP, 2020, vol. 1, pp. 284–290. (In Russ.)
4. Grigoriev A.Yu. Methods of testing generators of random and pseudorandom sequences. *Uchenye zapisi UdGU. Seriya: Matematika i informacionnye tekhnologii,* 2017, no. 1, pp. 22–28. (In Russ.)
5. Zuev M.Yu. Complex improvement of the efficiency of radio-electronic devices and information transmission systems with OFDM based on nonlinear systems with dynamic chaos. *Physics of wave processes and radio engineering systems,* 2022, vol. 25, no. 1, pp. 55–64. (In Russ.)
6. Loginov S.S. Modified Lorenz system based pseudorandom numbers generator. *Nelinejnyj mir,* 2017, vol. 15, no. 5. pp. 26–29. (In Russ.)
7. Vildanov R.R., Meshcheryakov R.V., Bondarchuk S.S. Tests of pseudo-random sequences and implementing their software. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki*, 2012, no. 1-2 (25), pp. 108–111. (In Russ.)
8. Perov A.A. Using NIST statistical tests for the analysis of the output sequences of block ciphers. *Nauchnyj vestnik Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta,* 2019, no. 3 (76), pp. 87–96. (In Russ.)
9. Rukhin A.L. et al. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. USA: National Institute of Standards and Technology, 2010, 131 p.
10. Loginov S.S., Zuev M.Yu. Testing pseudorandom signal generators based on the Lorentz system implemented over a finite Galois field. *Sistemy sinhronizacii, formirovaniya i obrabotki signalov*, 2018, no. 1 (9), pp. 111–114. (In Russ.)

Received 23.10.2023