Results of Statistical Security Assessment of Generators Using M-Ary Codes Based on the NIST 802STS Package

Kh.N. Rzaev[1], E.Y. Bagirov[2], M.F. Mammadov[3]

[1] *Azerbaijan Technical University (H.Javid ave. 25, Baku, AZ 1073, Azerbaijan)*
[2] *Fogito Tech (Baku, Azerbaijan)*
[3] *Cybernet LLC (Khatai ave. 16, Baku, Azerbaijan)*

For correspondence:
Rzaev Xazail / e-mail: xazail49@mail.ru

Abstract

In the article, the research has been carried out on the stability of known algorithms for generating pseudo-random sequences and hashing functions. It is proposed to use the NIST 822STS package to evaluate the statistical security of pseudorandom number generators. The pre-sented results confirm the theoretical results of assessing the resistance of the proposed generators on m-ary codes. The results of a study of the performance of software implementations of generators based on re-dundant block codes and some well-known generators (generator based on FIPS 197, BBS) are pre-sented and showed that the developed algorithms for generating PRN have low computational com-plexity

Keywords: statistical stability, pseudorandom number generators using m-ary codes, NIST 822STS package.

DOI 10.52171/2076-0515_2023_15_04_96_107

Accepted *18.04.2023*
Received *14.12.2023*
Revised *20.12.2023*

For citation:
Kh.N. Rzaev, E.Y. Bagirov, M.F. Mammadov
[Results of Statistical Security Assessment of Generators Using M-Ary Codes Based on the NIST 802STS Package]
Herald of the Azerbaijan Engineering Academy, 2023, vol. 15, no. 4, pp. 96-107 *(in Russian)*

NIST 802STS paketi əsasında m-lik kodlar üzrə generatorların statistik təhlükəsizliyinin qiymətləndirilməsinin nəticələri

X.N. Rzayev[1], E.Y. Bağırov[2], M.F. Məmmədov[3]

[1] *Azərbaycan Texniki Universiteti (H.Cavid pr. 25, Bakı, AZ1073, Azərbaycan)*
[2] *Fogito Tech (Bakı, Azərbaycan)*
[3] *Cybernet MMC (Xətai pr. 16, Bakı, Azərbaycan)*

Yazışma üçün:
Rzayev Xəzail/ e-mail: xazail49@mail.ru

Xülasə

Məqalədə, yalançı təsadüfi ardıcıllıqların formalaşmasının məlum alqoritmlərinin, heşləmə funksiyalarının müqavimətinin tədqiqi aparılır. Yalançı təsadüfi ədəd generatorlarının statistik təhlükəsizliyini qiymətləndirmək üçün NIST 822STS paketindən istifadə etmək təklif olunur. Təqdim olunan nəticələr m-lik kodları üzrə təklif olunan generatorların təhlükəsizliyinin qiymətləndirilməsinin nəzəri nəticələrini təsdiq edir. Lazımsız blok kodları və bəzi tanınmış generatorlar (FIPS 197, BBS əsasında generator) əsasında generatorların proqram təminatının tətbiqi sürətinin tədqiqinin nəticələri göstərmişdir ki, hazırlanmış PTƏ generasiya alqoritmləri zəif hesablama mürəkkəbliyinə malikdir.

Açar sözlər: statistik dayanıqlıq, m-lik kodlar üzrə psevdo-təsadüfi ədəd generatorları, NIST 822STS paketi.

DOI 10.52171/2076-0515_2023_15_04_96_107

УДК 003.26

Результаты оценки статистической безопасности генераторов на m-ичных кодах на основе пакета NIST 802STS

Х.Н. Рзаев[1], Э.Я. Багиров[2], М.Ф. Маммадов[3]

[1] *Азербайджанский Технический Университет (пр. Г. Джавида 25, Баку, AZ 1073, Азербайджан)*
[2] *Фогито Тех (пр. Хатаи, 16, Баку, Азербайджан)*
[3] *Cybernet MMC (Баку, Азербайджан)*

Для переписки:
Рзаев Хазаил / e-mail: xazail49@mail.ru

Аннотация

В статье проведено исследования стойкости известных алгоритмов формирования псевдослучайных последовательностей, функций хеширования. Для оценки статистической безопаснотси генераторов псевдослучайных чисел (ПСЧ) предлагается использовать пакет НИСТ 822STS. Представленные результаты подтверждают теоретические результаты оценки стойкости предлагаемый генераторов на m-ичных кодах. Результаты исследования быстродействия программной реализации генераторов на избыточных блоковых кодах и некоторых известных генераторов (генератор на основе FIPS 197, BBS) показали, что разработанные алгоритмы формирования ПСЧ имеют низкую вычислительную сложность.

Ключевые слова: статистическая стойкость, генераторы псевдослучайных чисел на m-ичных кодах, пакет НИСТ 822STS.

Введение

Одной из основных составляющих оценки стойкости криптографических алгоритмов является оценка его статистической безопасности. Считается, что алгоритм является статистически безопасным, если последовательность, которую он генерирует, по своим свойствам не уступает случайной последовательности. Такие последовательности называются “псевдослучайными”.

Целью исследования является повышение алгоритма с использованием “псевдослучайных” чисел.

Постановка задачи и методика проведения экспериментов

Для экспериментальной оценки того, насколько близко крипто-алгоритмы аппроксимируют генераторы “случайных” последовательностей, используются статистические тесты. Предложенный NIST (Национальным Институтом Стандартов США) пакет тестов NIST STS для тестирования генераторов случайных или псевдослучайных чисел является одним из подходов реализации задачи оценки статистической безопасности криптографических примитивов. Использование данного пакета позволяет с высокой долей вероятности делать выводы относительно того, насколько последовательность, что генерируется исследуемым примитивом, является статистически безопасной. Набор тестов NIST STS был предложен в ходе проведения конкурса на новый национальный стандарт США блочной шифровки в 2000 году и разработан сотрудниками Национального института стандартных технологий. Этот набор использовался для исследований статистических свойств кандидатов на новый блочный шифр. Методика тестирования, что предложена NIST, является наиболее распространенной у разработчиков криптографических средств защиты информации [1–3]. Порядок тестирования отдельной двоичной последовательности S имеет следующий вид:

1. Выдвигается нулевая гипотеза H_0 – предположение о том, что данная двоичная последовательность S случайна.
2. По последовательности S рассчитывается статистика теста $c\ (S)$.
3. С использованием специальной функции и статистики теста рассчитывается значение вероятности:
$$P = f(c(S)),\ P \in [0,1].$$
4. Значение вероятности P сравнивается с уровнем значимости:

$\alpha \in [0.001, 0.01]$, Если $P \geq \alpha$, то гипотеза H_0 принимается. В противном случае принимается альтернативная гипотеза.

Пакет содержит в себе 16 статистических тестов. Но фактически, в зависимости от входных параметров вычисляется 189 значений вероятности P, которые можно рассматривать как результат работы отдельных тестов. В табл.1 приводятся собранные данные по всем тестам с указанием количества значений, которые вычисляются, вероятности P, физического содержания статистики теста и дефекта на выявление, которого направлен тест.

Таким образом, в результате тестирования двоичной последовательности формируется вектор значений вероятности. Анализ составляющих этого вектора позволяет указать на конкретные дефекты случайности тестируемой последовательности.

Таблица 1 – Набор статистических тестов NIST STS
Table 1 – NIST STS Statistical Test Suite

№ п/п	Статистический тест	Статистика теста	Выявляемый дефект
1	Частотный (монобитный тест)	Нормализованная абсолютная сумма значений элементов последовательности	Слишком много нулей или единиц в последовательности
2	Частотный тест (в середине блока)	Мера согласованности количества единиц, которые наблюдаются с теоретически ожидаемыми.	Локализованные отклонения частоты появления единиц в блоке от идеального значения S
3	Проверка накопленных сумм	Максимальное отклонение значений накопленной суммы элементов последовательности от исходной точки отсчета (точка 0)	Большое количество единиц или нулей в начале или в конце двоичной последовательности
4	Проверка серий	Общее количество серий на всей длине последовательности	Слишком быстрое или слишком медленное изменение знака в ходе генерации последовательности
5	Проверка максимальной длины серии в блоке.	Мера согласованности значений максимальной длины, которые наблюдаются с теоретически ожидаемыми.	Отклонение от теоретического закона распределения максимальных длин серий единиц.
6	Проверка ранга двоичной матрицы	Мера согласованности значения наблюдаемых рангов различного порядка с теоретически ожидаемыми.	Отклонение эмпирического закона распределения значений рангов матриц от теоретического, что указывает на зависимость символов в последовательности.
7	Спектральный анализ на основе дискретного преобразования Фурье	Нормализованная разность количества наблюдаемых частотных компонент с ожидаемыми, превышающими 95% уровень порога	Выявление периодических составляющих (трендов) в двоичной последовательности.
8	Проверка шаблонов, которые перекрываются	Мера согласованности количества наблюдаемых шаблонов, которые перекрываются, в последовательности с теоретическим значением.	Большое количество m-битных серий из единиц в последовательности.
9	Универсальный тест Маурера	Сумма логарифма расстояния между l –битными шаблонами.	Возможность сжатия последовательности.
10	Энтропийный тест	Мера согласованности наблюдаемого значения энтропии источника с тем, что теоретически ожидается для случайного источника.	Неравномерность распределения m-битных слов в последовательности (регулярность свойств источника)

№ п/п	Статистический тест	Статистика теста	Выявляемый дефект
11	Проверка случайных отклонений	Мера согласованности наблюдаемого количества визитов при случайном блуждании заданное состояние в середине цикла с тем, что ожидается теоретически	Отклонение от теоретического закона распределения визитов в конкретное состояние при случайном блуждании
12	Проверка случайных отклонений (вариант)	Общее количество визитов при случайном блуждании	Отклонение от теоретически ожидаемого общего количества визитов при случайном блуждании в заданное состояние
13	Последовательный тест	Мера согласованности количества наблюдаемых *m*-битных шаблонов, которые встретились с той, что ожидается теоретически.	Неравномерность распределения *m*-битных слов в последовательности.
14	Проверка сжатия согласно алгоритму Лемпеля-Зива	Количество в последовательности различных слов	Большая степень сжатия последовательности, что тестируется по уравниванию со степенью сжатия, что ожидается для случайной последовательности.
15	Проверка шаблонов, которые не перекрываются	Мера согласованности наблюдаемого количества непериодических шаблонов в последовательности с теоретическим значением.	Большое количество заданных непериодических шаблонов в последовательности.
16	Проверка линейной сложности	Мера согласованности наблюдаемого количества событий, которые заключаются в появлении фиксированной длины эквивалентного ЛРР для заданного блока с теоретическим.	Отклонение эмпирического распределения длин эквивалентных ЛРР для последовательностей фиксированной длины от теоретического закона распределения для случайной последовательности, что указывает на недостаточную сложность тестируемой последовательности.

В соответствие с методикой решение о прохождении статистического тестирования принимается в случае, если выполняются правила:

1. Правило. Прошло тестирование по всем q тестам, ($q=\overline{1,189}$), и если значение коэффициента r_j находится внутри доверительного интервала [0.96, 1.00];
2. Правило. Прошло тестирование по всем q тестам, ($q=\overline{1,189}$), и если для всех тестов по критерию χ^2-Пирсона выполняется условие $P(\chi^2) > 0{,}0001$.

Таким образом, предлагаемый пакет позволяет решить актуальную научно-

практическую задачу оценки статистической стойкости ГПСЧ на m-ичных кодах.

В статье дана оценка статистической безопасности генераторов на m-ичных кодах на основе пакета NIST 802STS.

Для проведения экспериментальных исследований свойств разработанных кодовых криптосистем разработана программная реализация предложенных средств защиты информации [1, 7, 8]. Описание программного пакета, реализующего кодовые криптосистемы, приведено в приложении.

При выполнении тестирования выбраны следующие параметры:

- длина тестируемой последовательности $n = 10^6$ бит;
- количество тестируемых последовательностей m=100. Таким образом, объем тестируемой выборки составил $N=10^6 \times 100=10^8$ бит;
- уровень значимости α =0.01;
- количество тестов q =189.

Разработка программной реализации ГПСЧ с использованием предложенных методов позволяет провести статистические исследования стойкости, а также сформировать библиотеки для их практического использования. На рис. 1 и 2 представлены скриншоты предлагаемых подходов построения генераторов на m-ичных кодах без обратной связи и с обратной связью. Начальные значения регистра сдвига и значения обратной связи представляют собой числа не более 2^{21}–1, так как используется регистр сдвига по модулю примитивного многочлена $g(x)=x^{21}+x^2+1$. Регистр сдвига не может быть равен 0, в связи с невозможностью его работы. С использованием разработанной программной реализации предложенных генераторов ПСЧ [4–6] проведём экспериментальные исследования статистической безопасности по методике NIST STS, а также выполним сравнительные исследования с известными генераторами.

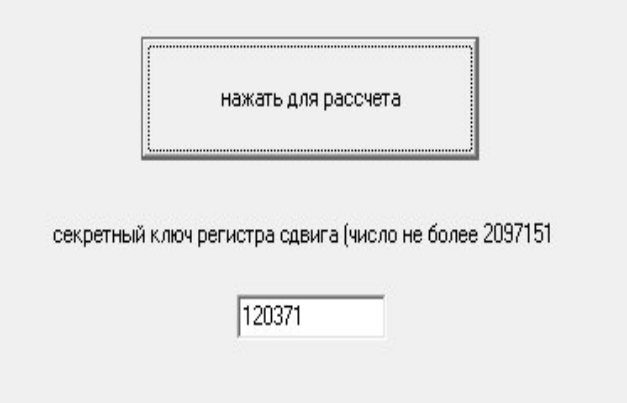

Рисунок 1 – Программная реализация генератора на m-ичных кодах без обратной связи
Figure 1 – Software implementation of the generator on m-ary codes without feedback

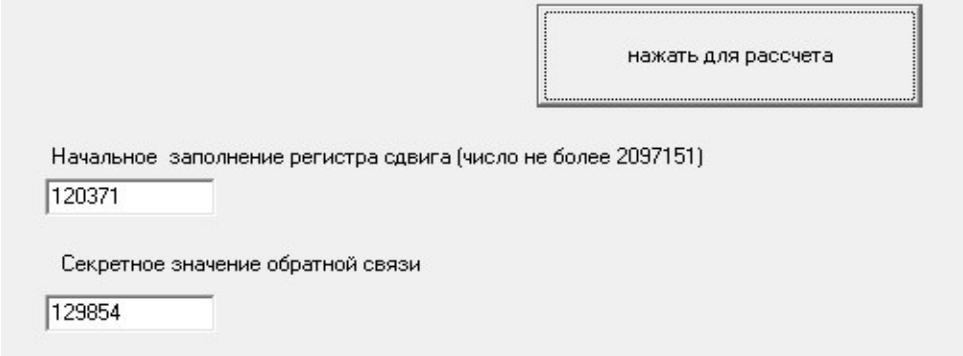

Рисунок 2 – Программная реализация генератора на m-ичных кодах с обратной связью
Figure 2 – Software implementation of the generator on m-ary codes with feedback

На рис. 3, 4 представлены статистические портреты исследуемых генераторов на m-ичных кодах.

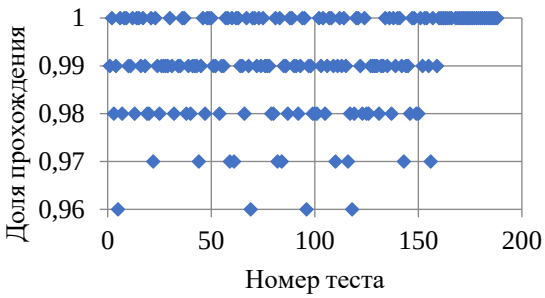

Рисунок 3 – Статистический портрет генератора на избыточных блоковых кодах без обратной связи
Figure 3 – Statistical portrait of the generator on redundant block codes without feedback

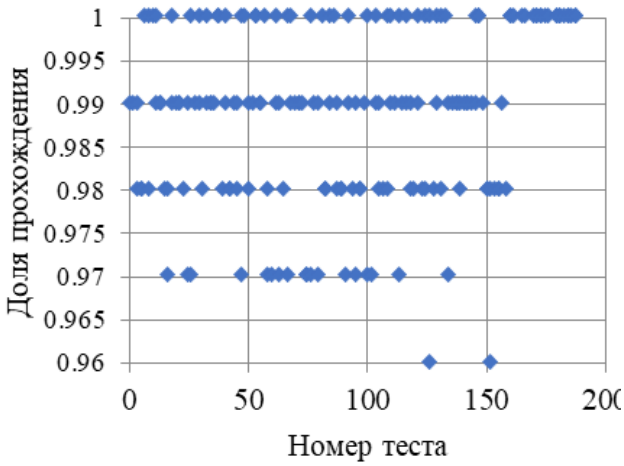

Рисунок 4 – Статистический портрет генератора на избыточных блоковых кодах с обратной связью
Figure 4 – Statistical portrait of the generator on redundant block codes with feedback

На рис. 5-13 представлены статистические портреты некоторых известных генераторов (на основе алгоритма SHA-1, линейный конгруэнтный генератор, генератор Микали-Шнора, квадратичный конгруэнтный генератор, генераторы на основе алгоритмов DES и 3-DES (тройного DES), генератор BBS, G using DES, доказуемо стойкий генератор GPSSD на избыточных кодах (использованный в диссертационной работе как метод-прототип)).

Таким образом, в результате тестирования двоичной последовательности формируется вектор значений вероятности.

Анализ составляющих этого вектора позволяет указать на конкретные дефекты случайности тестируемой последовательности.

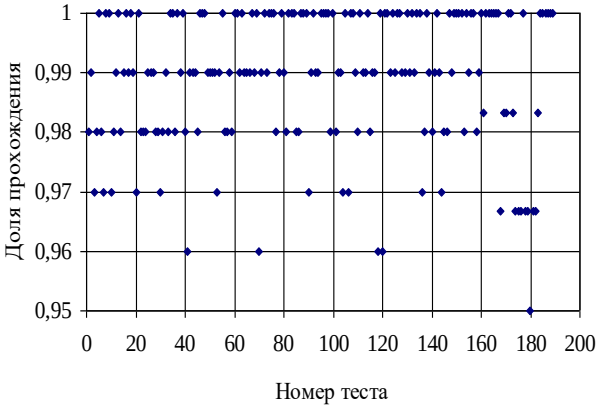

Рисунок 5 – Статистический портрет генератора на основе алгоритма SHA-1
Figure 5 – Statistical portrait of the generator based on the SHA-1 algorithm

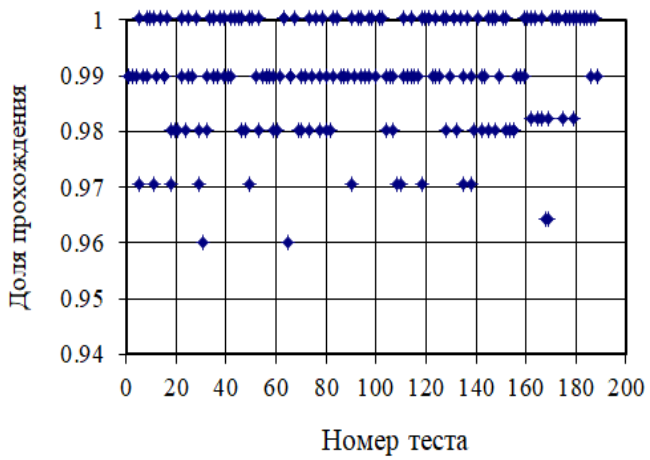

Рисунок 6 – Статистический портрет линейного конгруэнтного генератора
Figure 6 – Statistical portrait of a linear congruential generator

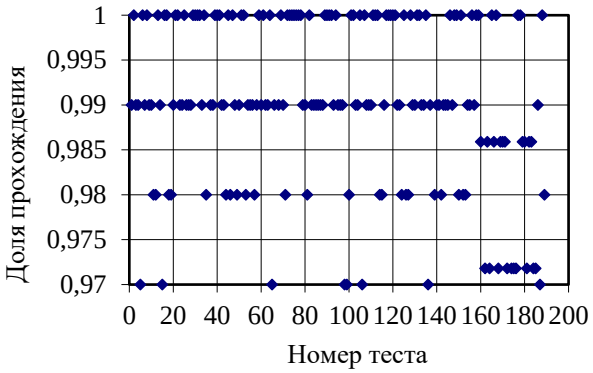

Рисунок 7 – Статистический портрет генератора Микали-Шнора
Figure 7 – Statistical portrait of the Mikali-Shnor generator

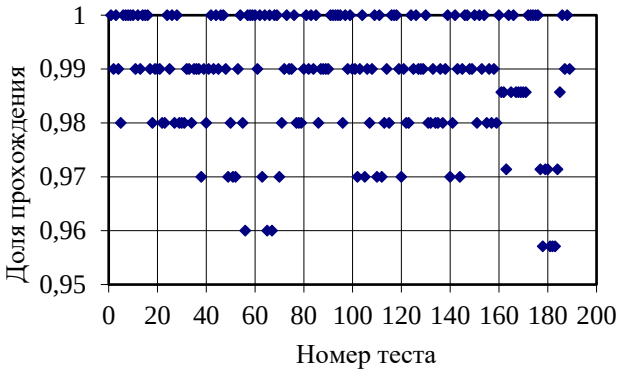

Рисунок 10 – Статистический портрет генератора на основе алгоритма 3-DES
Figure 10 – Statistical portrait of the generator based on the 3-DES algorithm

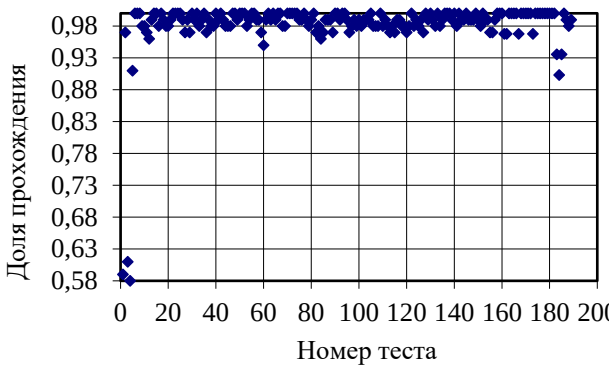

Рисунок 8 – Статистический портрет квадратичного конгруэнтного генератора
Figure 8 – Statistical portrait of a quadratic congruential generator

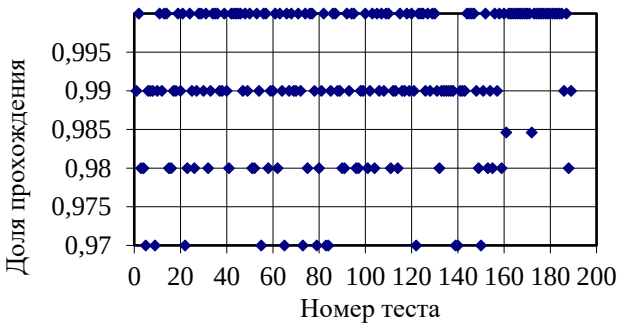

Рисунок 11 – Статистический портрет генератора BBS
Figure 11 – Statistical portrait of the BBS generator

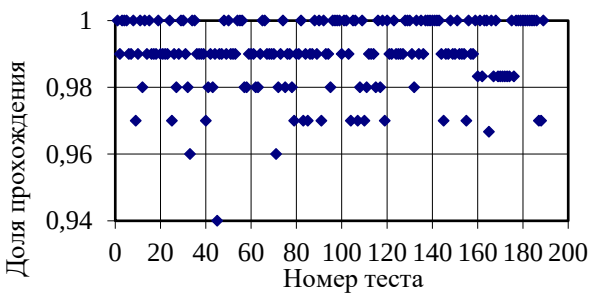

Рисунок 9 – Статистический портрет генератора на основе алгоритма DES
Figure 9 – Statistical portrait of the generator based on the DES algorithm

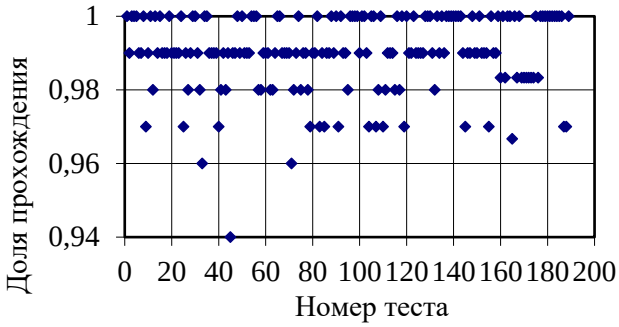

Рисунок 12 – Статистический портрет генератора G using DES
Figure 12 – Statistical portrait of the generator G using DES

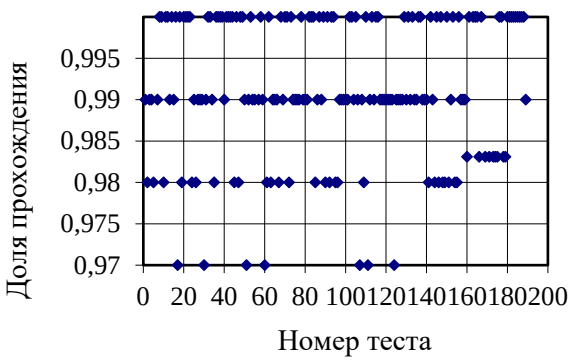

Рисунок 13 – Статистический портрет доказуемо стойкого генератора на избыточных кодах (метод-прототип)
Figure 13 – Statistical portrait of a provably stable generator on redundant codes (prototype method)

Анализ приведенных данных показывает, что статистические портреты предложенных генераторов на избыточных блоковых кодах не уступают по своим свойствам лучшим известным генераторам. Так, для сформированных ПСЧ нет статистических тестов, которые были бы пройдены с вероятностью ниже 0,96. Основная часть тестов пройдена с очень высоко вероятностью, близкой к 1. Окончательные результаты тестирования по методике NIST STS сведены в табл. 2, в которой приведены количества (доля) тестов, в которых тестирование прошло с вероятностью ≥0,99; ≥0,96 и < 0,96.

Таблица 2 – Результаты сравнительных исследований статистической безопасности предложенных и некоторых известных генераторов
Table 2 – Results of comparative studies of the statistical safety of the proposed and some known generators

№ п/п	Генератор псевдослучайных чисел	Количество тестов, в которых тестирование прошло М последовательностей (%)		
		M ≥ 99%	M ≥ 96%	M < 96%
1	G using SHA-1	122(65%)	188 (99,5%)	1 (0,5%)
2	Linear Congruential	139 (74%)	189 00%)	–
3	Micali-Schnorr	130 (69%)	189 00%)	–
4	Quadratic Congruential	124 (66%)	181 (96%)	8 (4%)
5	G using DES	142 (75%)	188 (99,5%)	1 (0,5%)
6	ANSI X9.17 (3-DES)	121 (64%)	187 (98%)	4 (2%)
7	BBS	134 (71%)	189 00%)	–
8	G using DES	142 (75%)	188 (99,5%)	1 (0,5%)
9	GPSSD (метод-прототип)	140 (74%)	189 00%)	–
10	Усовершенствованный генератор на избыточных блоковых кодах	140 (74%)	189 00%)	–
11	Предложенный генератор на избыточных блоковых кодах с повышенной длиной периода	142 (75%)	189 (100%)	–

Анализ результатов тестирования, сведенных в табл. 2., показывает, что предложенные генераторы на избыточных блоковых кодах обладают улучшенными показателями статистической безопасности. Они имеют одно из наибольших число (долю) тестов, прошедших по наиболее жесткому критерию с вероятностью ≥0,99 и не

уступают таким известным генераторам как генератор BBS и национальный алгоритм шифрования США в режиме счетчика.

В табл. 3 приведены результаты экспериментальной оценки быстродействия разработанной программной реализации ГПСЧ на m-ичных кодах и сравнительные исследования с программными реализациями известных генераторов. Экспериментальная оценка проводилась с фиксацией времени формирования ПСЧ – 1 сутки, замерялась длина сформированной последовательности, после чего рассчитывалось среднее время формирования ПСЧ.

Таблица 3 – Результаты сравнительных исследований быстродействия предложенных и некоторых известных генераторов
Table 3 – Results of comparative studies of the performance of the proposed and some well-known generators

Генератор псевдослучайных чисел	Быстродействие генератора	
	Абсолютное значение	Относительное значение
BBS	$3{,}6 \cdot 10^2$ бит/с	219444
FIPS 197	$7{,}9 \cdot 10^7$ бит/с	1
Micali-Schnorr	$1{,}1 \cdot 10^5$ бит/с	718
GPSSD (метод-прототип)	$3{,}29 \cdot 10^7$ бит/с	2,4
Усовершенствованный генератор на избыточных блоковых кодах	$2{,}96 \cdot 10^7$ бит/с	2,7
Предложенный генератор на избыточных блоковых кодах с повышенной длиной периода	$2{,}86 \cdot 10^7$ бит/с	2,8

Конкретная программная реализация ГПСЧ носит субъективный характер и не может служить объективной оценкой их быстродействия. В тоже время, сравнительные оценки быстродействия нескольких генераторов, реализованных одним программистом на одной вычислительной платформе с использованием одной среды разработки, могут претендовать на объективность. С целью адекватного сравнения быстродействия программной реализации исследуемых генераторов в последней графе таблицы приведены относительные оценки, полученные через отношение максимальной производительности и искомой производительности рассматриваемого генератора. Минимальное значение относительной оценки равно 1 и соответствует наиболее быстрому генератору. Увеличение относительной оценки соответствует снижению быстродействия по сравнению с самым быстрым генератором. Собственное значение относительной оценки соответствует коэффициенту пропорционального снижения быстродействия рассматриваемого генератора (по сравнению с наиболее быстрой реализацией).

Как следует из приведенных в табл. 3 значений наибольшую производительность показал генератор на основе алгоритма шифрования FIPS 197 (национальный алгоритм шифрования США). Вторым по показателям быстродействия является доказуемо стойкий генератор на основе избыточных блоковых кодов (генератор GPSSD), используемый в данной работе в качестве метода-прототипа. Снижение быстродействия по сравнению с FIPS 197 составило 2,4 раза, что объясняется увеличением числа выполняемых операций над формируе-

мой последовательностью в цепи обратной связи. Следующий (третий) по быстродействию оказался усовершенствованный генератор. Он медленнее FIPS 197 в 2,7 раза и практически сопоставим по быстродействию с генератором GPSSD. Несколько уступает по быстродействию предложенный генератор на избыточных блоковых кодах с повышенной длиной периода, он медленнее FIPS 197 в 2,8 раза. Значительно худший результат показал генератор BBS, который практически на 4 порядка медленнее рассмотренных выше генераторов. Подобная низкая вычислительная эффективность генератора BBS объясняется сложностью применяемого математического аппарата.

Достоверность полученных результатов и сделанных выводов подтверждается сходимостью теоретических расчетов с результатами эксперимента. Так, в разделе 3 показано, что при длине периода L = 100 – 200 разработанные алгоритмы формирования ПСЧ требуют выполнения от 1,5 до 2,5 операций на один формируемый бит ПСЧ. В тоже время известно, что для реализации алгоритма шифрования FIPS 197 (без учета времени разворачивания ключей) необходимо затратить около 4 операций на одно 32 битное слово (на одном раунде). При минимальном числе раундов 10 алгоритм FIPS 197 потребует около 1,25 операций на один формируемый бит. Таким образом, с учетом работы алгоритма разворачивания ключей генератор на основе FIPS 197 и предложенные генераторы обладают сравнимой вычислительной сложностью.

Таким образом, как показали проведенные исследования, предложенные методы формирования ПСЧ на основе избыточных блоковых кодов обладают высокой эффективностью: по своим криптографическим свойствам и быстродействию они не уступают лучшим мировым аналогам, описываются моделью доказуемой стойкости, легко реализуются в программном и аппаратном виде.

Заключение

Проведенные экспериментальные исследования стойкости рассматриваемых генераторов показали, что генераторы на избыточных блоковых кодах обладают улучшенными показателями статистической безопасности. Они имеют одно из наибольших число (долю) тестов, прошедших по наиболее жесткому критерию с вероятностью ≥0,99 и не уступают таким известным генераторам как генератор BBS и национальный алгоритм шифрования США в режиме счетчика. Исследования быстродействия программной реализации генераторов на избыточных блоковых кодах и некоторых известных генераторов (генератор на основе FIPS 197, BBS) показали, что разработанные алгоритмы формирования ПСЧ имеют низкую вычислительную сложность. Быстродействие формирования ПСЧ предложенными генераторами составляет $10^7 - 10^8$ бит/с, что сопоставимо с быстродействием наиболее быстрых блочных симметричных шифров (FIPS 197).

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов, связанных с публикацией данной статьи.

REFERENCES

1. **Rukhin, and J. Soto.** A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, 09.2000, 164 p. *(in English)*
2. **Serhii Yevseiev, Oleksandr Milov, Ivan Opirskyy, Olha Dunaievska, Oleksandr Huk, Volodymyr Pogorelov, Kyrylo Bondarenko, Nataliia Zviertseva, Yevgen Melenti, Bogdan Tomashevsky.** Development of concepts for the cyber security metrics classification. Eastern-European Journal of Enterprise Technologies. 4/4 (118). 2022. P. 6–18. *(in English)*
3. **Serhii Yevseiev, Khazail Rzaev, Oleksandr Laptiev, Ruslan Hasanov, Oleksandr Milov, Bakhar Askerova, Zhala Jamalova, Serhii Pohasii.** Development of a hardware cryptosystem based on a random number generator with two types of entropy sources. Eastern-European Journal of Enterprise Technologies. 2022. 5/9 (119). P. 6–16. *(in English)*
4. **Yevseiev S.P., Rzaev H.N, Korolov R.V., Mamedov M., Bagirov E.** Generator psevdovipadkovih chisel na m-ichnih kodah. HI mizhnarodna naukovo-praktichna konferenciya “Matematika. Informacijni tekhnologiï. Osvita”. Luc'k-Svityaz', 3–5 chervnya 2022. S. 70. *(in Ukrain)*
5. **R. Korolov, M. Mamedov, E. Bagirov.** Rozrobka vdoskonalenogo metodu formuvannya psevdovipadkovih chisel na osnovi nadlishkovih m-ichnih kodiv. V Mizhnarodna naukovo-praktichna konferenciya “Problemi kiberbezpeki informacijno-telekomunikacijnih si-stem” (PCSITS)”14–15 kvitnya 2022, Kiïv, Ukraïna. S. 11–13. *(in Ukrain)*
6. **R. Korolov, A. Tkachov, N. Voropay, M. Mammadov, E. Baghirov**. Development of an improved method for forming pseudorandom numbers based on redunte m-ary codes. Sistemi obrobki informaciï, 2022, v 1 (168), R.11–13. *(in English)*
7. **Korolov R.V.** Doslidzhennya periodichnih vlastivostej generatoriv psevdovipadkovih chisel, zasnovanih na vikoristanni nadmirnih kodiv / R.V.Korolov // Sistemi ozbroennya i vijskova tekhnika. – 2008. – №3(15). – S. 126 – 128. *(in Ukrain)*
8. **Rzaev H.N., Gasanov R.A.** Analiz protokolov bezopasnosti i dostovernosti v perspektivnyh sistemah predostavleniya uslug svyazi. *Azərbaycan Mühəndislik Akademiyasının Xəbərləri*, cild 8, № 4, Bakı, 2016, str.83-98. *(in Russian)*