Надежность, том 25, №3, 2025 / Dependability 3, 2025
Системный анализ в задачах надежности и безопасности

УДК 004.421 + 004.056
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-3-21-28

Интеллектуальная система анализа и классификации генераторов псевдослучайных чисел

Intelligent system for analysing and classifying pseudorandom number generators

Автоношкин А.М.[1], Куминов В.П.[1]*, Сидоренко В.Г.[1], Смецкая А.С.[1]
Avtonoshkin A.M.[1], Kuminov V.P.[1]*, Sidorenko V.G.[1], Smetskaya A.S.[1]

[1] РУТ(МИИТ), Российская Федерация, Москва
[1] RUT(MIIT), Russian Federation, Moscow
**1036301@edu.rut-miit.ru*

Автоношкин А.М.

Куминов В.П.

Сидоренко В.Г.

Смецкая А.С.

Резюме. Цель. *Настоящая работа посвящена рассмотрению вопросов построения интеллектуальной системы анализа и классификации генераторов псевдослучайных чисел (ГПСЧ), объединяющей возможности машинного обучения и направленного перебора для решения задачи определения типа источника случайной последовательности чисел. Основное внимание уделяется выявлению слабостей некриптографических ГПСЧ, которые могут быть предсказуемыми, что несет риски для их использования в области информационной безопасности.* **Методы.** *В ходе исследования использовались методы машинного обучения, в частности нейронные сети, корреляционный анализ и статистические тесты NIST. Разработанные модели обучались на больших выборках выходных последовательностей ГПСЧ, что позволило оценить предсказуемость ГПСЧ и возможность восстановления внутренних состояний. Структура нейронных сетей выбиралась с учетом результатов работы процедур оптимизации значений гиперпараметров нейронных сетей. Показано влияние размера выборки на получаемые результаты.* **Результаты.** *Анализ и классификация ГПСЧ включает несколько этапов: вычисление автокорреляционной функции выходных последовательностей и их спектр, выполнение статистических тестов, разработанных лабораторией NIST; классификация ГПСЧ на основе анализа выходных последовательностей; выявление особенностей внутренней структуры ГПСЧ или его внутренних состояний; прогнозирование значений на выходе. Для алгоритма Xorshift128 нейронная сеть показала высокую точность восстановления выходных значений, подтверждая его уязвимость. Анализ алгоритма Mersenne Twister выявил определенные закономерности, но потребовал более сложных архитектур для полной реконструкции последовательностей. Для алгоритма «стоп-пошел» удалось выявить закономерности построения структуры с использованием алгоритмов машинного обучения, но решить задачу прогнозирования значения на выходе ГПСЧ только по предыдущим значениям выходной последовательности без знания внутренних состояний с высокой точностью не удалось. Линейный конгруэнтный генератор и генератор Геффе удается классифицировать и прогнозировать с использованием алгоритмов направленного перебора. Объединенные в систему модели классифицируют ГПСЧ по их характеристикам и прогнозируют их дальнейшие выходные значения. Анализ полученных результатов подтверждает значимость выбора не только структуры ГПСЧ, но и числовых параметров и задействованных в вычислениях битов внутри чисел.* **Заключение.** *Проведенное исследование подтверждает эффективность сочетания методов машинного обучения и направленного перебора при анализе и классификации ГПСЧ. Полученные результаты позволяют рекомендовать разработанную систему для использования в практических задачах оценки безопасности ГПСЧ. Перспективы дальнейших исследований связаны с расширением множества анализируемых ГПСЧ и рассмотрением других типов нейронных сетей для повышения качества и производительности моделей.*

Abstract. Aim. *This paper examines the construction of an intelligent system for analysing and classifying pseudorandom number generators (PRNGs) that combines the capabilities of machine learning and directed search for determining the type of the source of a random sequence of numbers. The focus is on identifying weaknesses in non-cryptographic PRNGs that may be predictable, which entails risks for their use in information security.* **Methods.** *The research used machine learning methods, including neural networks, correlation analysis, and NIST statistical tests. The developed models were trained on large samples of PRNG output strings, which allowed estimating the predictability of the PRNG and internal state restorability. Neural network structures were chosen taking into account the results of optimisation of the neural network hyperparameter values. The paper shows the effect of the sample size on the obtained results.* **Results.** *The analysis and classification of a PRNG involves a number*

of steps: calculating the autocorrelation function of the output strings and their spectrum; execution of statistical tests developed by the NIST laboratory; classification of PRNGs based on the output strings analysis; identifying the specificity of the PRNG's internal structure or its internal states; prediction of the output values. For the Xorshift128 algorithm, the neural network showed a high accuracy of output value restoration, which confirms its vulnerability. An analysis of the Mersenne Twister algorithm revealed certain patterns, but required more complex architectures to completely reconstruct the strings. Using machine learning algorithms, the authors managed to identify the structure building patterns for the "stop-and-go" algorithm, but failed to highly accurately predict the PRNG output value based only on the prior output string values with no knowledge of the internal states. Directed search algorithms allow classifying and predicting a linear congruentional generator and a Geffe generator. The models combined into a system classify PRNGs according to their characteristics and predict their eventual output values. An analysis of the obtained results confirms the significance of not only the selected PRNG structure, but also the numerical parameters and the bits within numbers involved in the computation. **Conclusion.** *The conducted study confirms the efficiency of the combination of machine learning and directed search as part of the analysis and classification of PRNGs. The findings allow recommending the developed system for use in practical PRNG safety assessment. Further research will focus on expanding the set of analysed PRNGs and examining other types of neural networks for improving the quality and performance of models.*

Ключевые слова: *генератор псевдослучайных чисел, классификация, прогнозирование последовательностей, машинное обучение, информационная безопасность.*
Keywords: *pseudorandom number generator, classification, string prediction, machine learning, information security.*

Для цитирования: *Автоношкин А.М., Куминов В.П, Сидоренко В.Г., Смецкая А.С. Интеллектуальная система анализа и классификации генераторов псевдослучайных чисел // Надежность. 2025. №3. С. 21-28. https://doi.org/10.21683/1729-2646-2025-25-3-21-28*
For citation: *Avtonoshkin A.M., Kuminov V.P., Sidorenko V.G., Smetskaya A.S. Intelligent system for analysing and classifying pseudorandom number generators. Dependability 2025;3: 21-28. https://doi.org/10.21683/1729-2646-2025-25-3-21-28*

Поступила: *08.03.2025* / **После доработки:** *14.05.2025* / **К печати:** *25.07.2025*
Received on: *08.03.2025* / **Revised on:** *14.05.2025* / **For printing:** *25.07.2025*

Введение

Генераторы псевдослучайных чисел (ГПСЧ) используются в различных областях, от лотерей до криптографии. Предсказуемость таких генераторов может привести к серьезным последствиям, таким как снижение точности вычислений и утечка данных, например, при компрометации ключей шифрования или параметров стеганографических алгоритмов [1]. Проблема усугубляется тем, что по незнанию или ошибке вместо генераторов истинно случайных чисел, порождаемых природными процессами, могут использоваться ГПСЧ. Актуальность данной работы обуславливается необходимостью освещения проблем использования ГПСЧ и сложностью их классификации [2].

Анализу безопасности ГПСЧ посвящено большое число публикаций.

В продолжение цикла исследований и публикаций на тему анализа ГПСЧ и их классификации авторами была выдвинута идея создания интеллектуальной системы, предназначенной для классификации, а в некоторых случаях и для прогнозирования поведения таких генераторов [3-4].

Цель данной статьи – создание интеллектуальной системы анализа и классификации генераторов псевдослучайных чисел (ГПСЧ), объединяющей возможности машинного обучения и направленного перебора для решения задачи определения типа источника случайной последовательности чисел. Для достижения поставленной цели решались следующие задачи анализа и классификации ГПСЧ: анализ уязвимостей ГПСЧ, анализ автокорреляционных функций выходных последовательностей ГПСЧ и их спектров, анализ результатов выполнения статистических тестов, разработанных лабораторией *NIST*; классификация ГПСЧ на основе анализа выходных последовательностей; выявление особенностей внутренней структуры ГПСЧ или его внутренних состояний; прогнозирование значений на выходе.

1. Слабости ГПСЧ

ГПСЧ имеют ряд существенных слабостей. Примеры таких слабостей, отражены в *Common Weakness Enumeration* (*CWE*) [5]. Системы машинного обучения (МО) с высокой точностью могут прогнозировать значения на выходе ГПСЧ, если они зависят от предыдущих выходных значений. Эта проблема зафиксирована, например, в следующих элементах CWE:

– *CWE*-340: проблемы прогнозируемости;

– *CWE*-341: прогнозируемость по наблюдаемому состоянию;

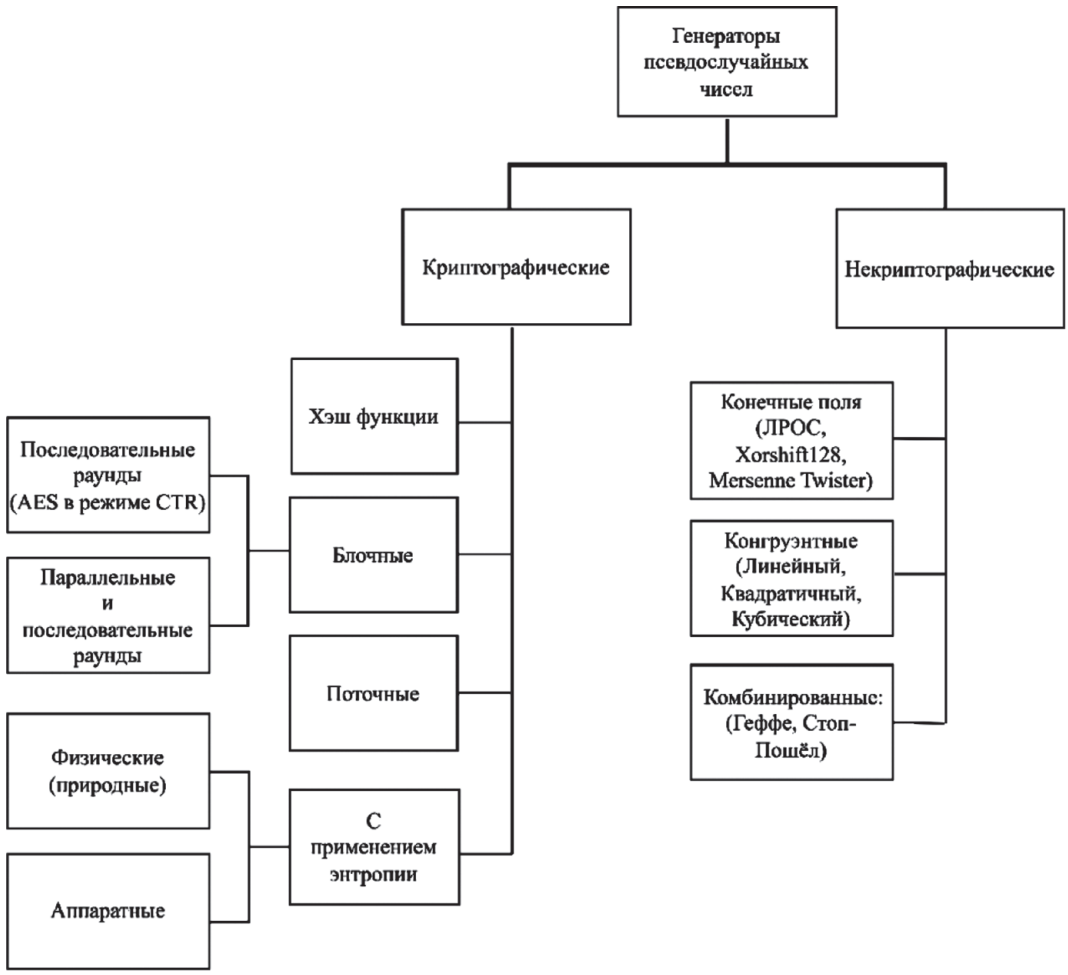
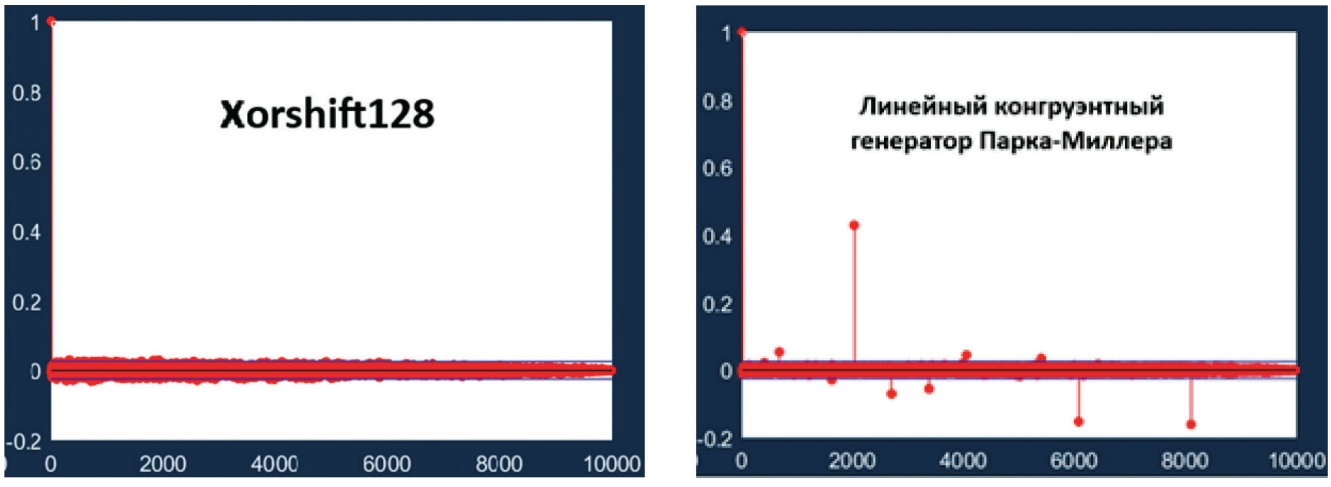


Рис. 1. Классификация ГПСЧ

– *CWE*-342: прогнозирование точного значения по предыдущим значениям;

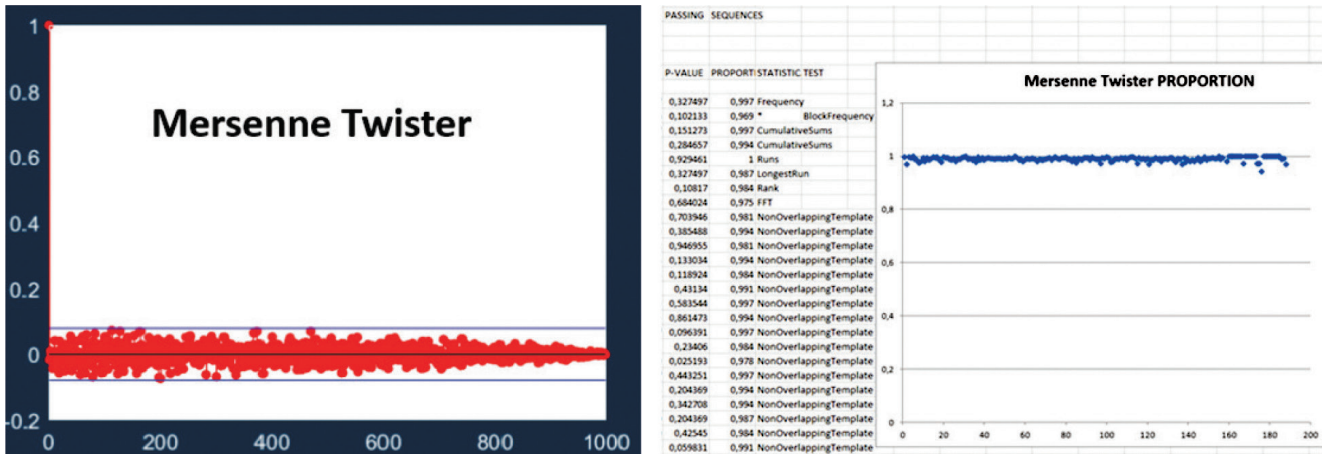
– *CWE*-343: прогнозирование диапазона значений по предыдущим значениям.

ГПСЧ можно разделить на криптографические и некриптографические (рис. 1). Поскольку криптографические ГПСЧ защищены от прогнозирования [4], в данном исследовании акцент сделан на некриптографических ГПСЧ. Непредсказуемость криптографических ГПСЧ может быть пересмотрена в будущем в условиях наращивания вычислительных ресурсов и развития новых технологий.



а) б)

Рис. 2. Автокорреляционные функции выходных последовательностей ГПСЧ Xorshift128 (а) и ЛКГ Парка-Миллера (б)



а) б)

Рис. 3. Автокорреляционная функция выходной последовательности (а) и результаты тестов *NIST* для ГПСЧ Mersenne Twister (б)

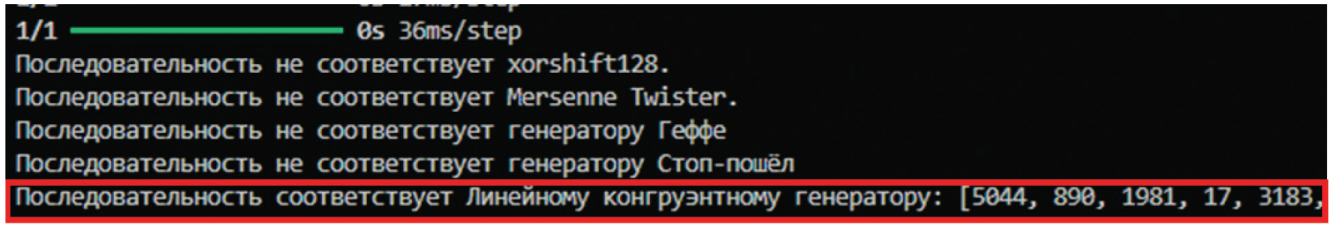


Рис. 4. Результаты работы систем по классификации ГПСЧ

2. Анализ выходных последовательностей ГПСЧ

Анализ выходных последовательностей ГПСЧ поводится разными способами:

- вычисление автокорреляционной функции выходных последовательностей и их спектра. Например, быстро убывающая, без всплесков автокорреляционная функция указывает на высокое качество рассмотренных алгоритмов Xorshift128 (рис. 2а) и Mersenne Twister (рис. 3а). Имеющая всплески автокорреляционная функция линейного конгруэнтного генератора (ЛКГ) Парка-Миллера, напротив, указывает на его непригодность для применения в задачах с высокими требованиями к случайности (рис. 2б);

- выполнение статистических тестов, разработанных лабораторией *NIST*. Как правило, результаты тестов *NIST* для классических алгоритмов ГПСЧ с правильно подобранными параметрами подтверждают хорошее качество алгоритмов с небольшими погрешностями, однако, как показали дальнейшие исследования, результаты работы этих алгоритмов могут быть спрогнозированы нейронными сетями (НС) или раскрыты путем направленного перебора и уже не могут считаться достаточно безопасными для использования. Например, проведенные для генератора Mersenne Twister тесты показали его хорошее качество, выявив небольшие слабости при генерации отдельных шаблонов и указывая на возможные скрытые закономерности, например, тест неперекрывающихся шаблонов показал слабости в генерации отдельных паттернов (рис. 3б).

3. Определение типа ГПСЧ – источника случайной последовательности чисел

В ходе выполненных исследований были разработаны НС и алгоритмы направленного перебора, объединенные в систему и отвечающие на вопрос: является ли последовательность, поданная на вход системы, выходной последовательностью ГПСЧ, соответствующего данной НС или алгоритму. Для каждого из рассмотренных ГПСЧ был разработан собственный алгоритм. В ходе проведенных экспериментов не было зафиксировано ошибок в классификации (рис. 4).

Анализ работы алгоритма Xorshift128 показал, что только два предыдущих значения выходной последовательности участвуют в генерации текущего (первого с конца последовательности): 2-е и 5-е с конца последовательности (рис. 5). Во входном слое построенной НС, которая прогнозирует следующее значение выходной последовательности, 64 узла, соответствующих двум значениям выходной последовательности, у каждого из которых длина 32 бита. В скрытом слое 1024 узла. Такое число узлов является компромиссным: достаточным для распознавания шаблонов нелинейной операции XOR, но не приводящим к переобучению. В выходном слое 32 узла, описывающих 32 разряда выходного числа. Если прогнозируемое значение на выходе НС совпадает с известным заключительным числом последовательности, то считаем, что поданная последовательность является выходной для ГПСЧ Xorshift128.

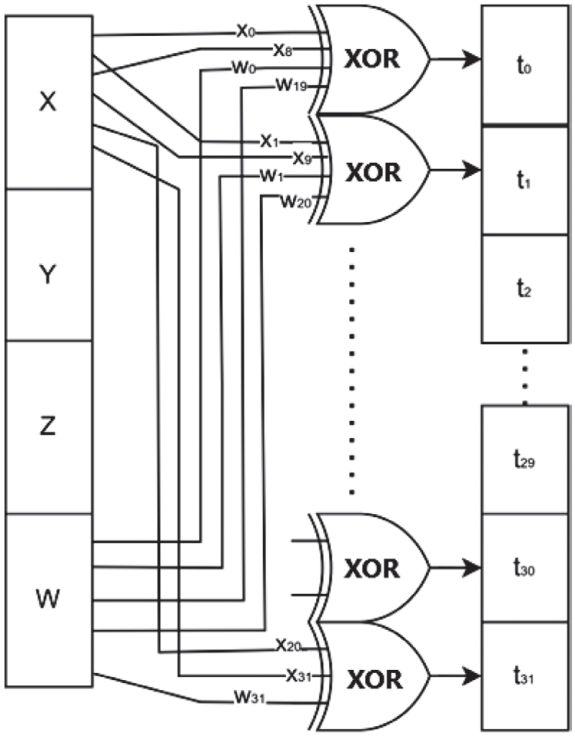


Рис. 5. Структурная схема ГПСЧ Xorshift128 [4]

В разработанной системе рассмотрен ГПСЧ *Mersenne Twister*, более сложный, чем Xorshift128, и используемый в текущих реалиях. Он также основан на операциях сдвигах и исключающего ИЛИ (XOR), но уже имеет блок внутреннего состояния из 624-х внутренних значений и блок преобразования, усложняющий восстановление скрытых процессов работы генератора (рис. 6) [6]. В связи с этим задача классификации решалась за три шага (см. рис. 6):

• восстановление внутреннего состояния. Несмотря на необратимость с точки зрения традиционных методов, связанную с использованием операции XOR, НС с одним скрытым слоем из 800 узлов, реализующая это восстановление, не допустила ошибок в процессе тестирования. На вход подавалось число в бинарном 32-битном виде после преобразования, на выходе ожидалось число до преобразования;

• моделирование основного блока. Поскольку известно, что каждое новое состояние зависит от трех предыдущих, а именно 1-го, 2-го и 398-го, то для решения этой задачи была построена НС, на вход которой подается три 32-битных числа, а на выходе получается одно 32-битное число;

• повторная модификация, преобразующая результат моделирования внутреннего блока в результат выполнения операции Xorshifter.

В случае ГПСЧ «стоп-пошел», как и в случае ГПСЧ Mersenne Twister, зная его внутренние состояния, удалось с использованием НС спрогнозировать значение на выходе ГПСЧ, но зная только предыдущие значения на выходе, не удается прогнозировать внутренние состояния и значения на выходе. Это подтверждает то, что алгоритм «стоп-пошел» обладает большей непредсказуемостью. НС, позволяющие выявить особенности внутренней структуры ГПСЧ, о чем будет рассказано ниже, помогли задать направление перебора. Удалось выяснить, что для классификации необходимо только 3 бита от каждого из линейных регистров с обратной связью (ЛРОС), которые участвуют в организации обратных связей соответствующего ЛРОС (рис. 7).

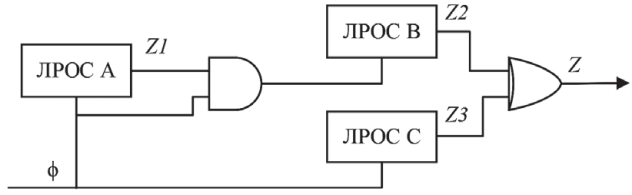


Рис. 7. Генератор «стоп-пошел»

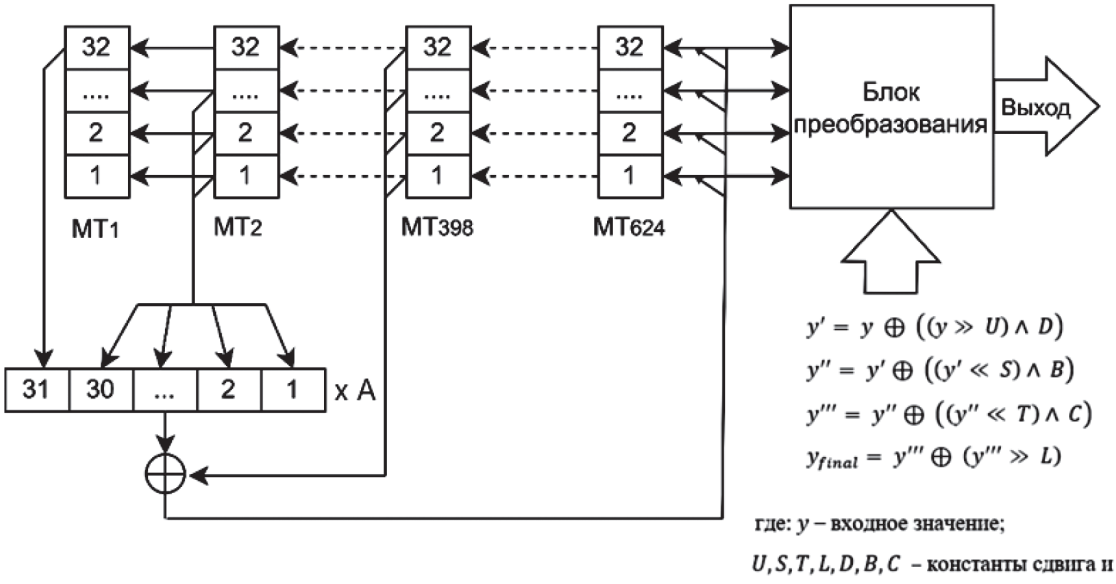


Рис. 6. Структурная схема ГПСЧ Mersenne Twister 1997 [6]

Для ЛКГ и нелинейных конгруэнтных генераторов в связи с использованием в них операций определения остатка от деления не удалось построить НС, точность прогнозирования в которых превышала бы 70%. Поэтому для их классификации в системе используются алгоритмы направленного перебора.

4. Выявление особенностей внутренней структуры ГПСЧ или его внутренних состояний

Особенность алгоритма Xorshift128, заключающаяся в зависимости текущего выходного значения (первого с конца последовательности) от 2-го и 5-го чисел с конца последовательности была выявлена заранее и учтена при построении НС, используемой для классификации ГПСЧ и прогнозирования выходного значения.

Представленный на рис. 8 график соединения узлов скрытого слоя НС, построенной для восстановления внутреннего состояния ГПСЧ Mersenne Twister, с узлами входного слоя наглядно демонстрирует работу алгоритма согласно рис. 6. Узлы с первого по тридцать второй оказались «мертвыми», то есть неиспользуемыми. Это говорит о том, что модель МО успешно нашла зависимости, не зная о них: в генерации нового значения принимают участие только старший бит первого числа, все, кроме старшего, биты второго числа и 398 число.

Определить внутренние зависимости для ГПСЧ, не всегда удается. Для примера рассмотрим упрощенную версию ГПСЧ «стоп-пошел». Пусть значение на выходе генератора Z определяется по формуле:

$$Z = \left((Z1 \wedge Z2)\, XOR \left(\overline{Z1} \wedge Z3 \right) \right),$$

где $Z1$ – значение на выходе ЛРОС A, $Z2$ – значение на выходе ЛРОС B, $Z3$ – значение на выходе ЛРОС C.

Если длины регистров B, C и A равны 8, 10 и 22 разряда, соответственно, то, как показано на рис. 9а, наличие обратных связей определилось только для регистров C (для 6-го, 7-го и 10-го разрядов) и A (для 11-го, 16-го и 22-го разрядов).

Если длины регистров B, C и A равны 16, 8 и 16 разрядов, соответственно, то, как показано на рис. 9б, наличие обратных связей определилось для всех трех регистров: C (для 4-го, 5-го и 8-го разрядов), A (для 5-го, 10-го и 16-го разрядов) и B (для 9-го, 15-го и 16-го разрядов). Как и в случае анализа автокорреляционных функций это подтверждает значимость не только выбранного типа структуры ГПСЧ, но и используемых числовых параметров и задействованных в вычислениях битов внутри чисел.

Параметры ЛКГ удается определить с использованием направленного перебора, имея два последовательных значения на выходе генератора. Для нелинейных конгруэнтных генераторов существуют теоретические предпосылки для создания систем определения параметров.

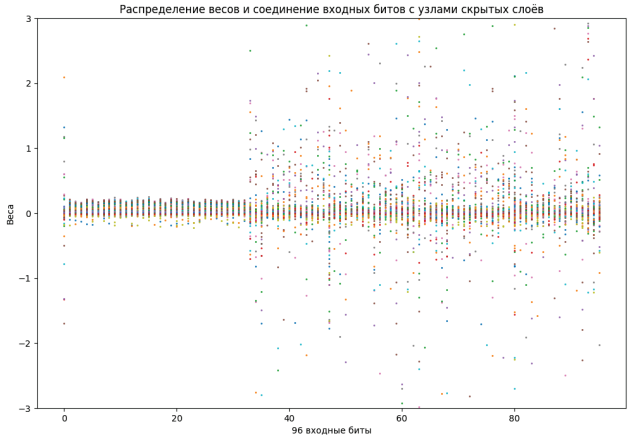
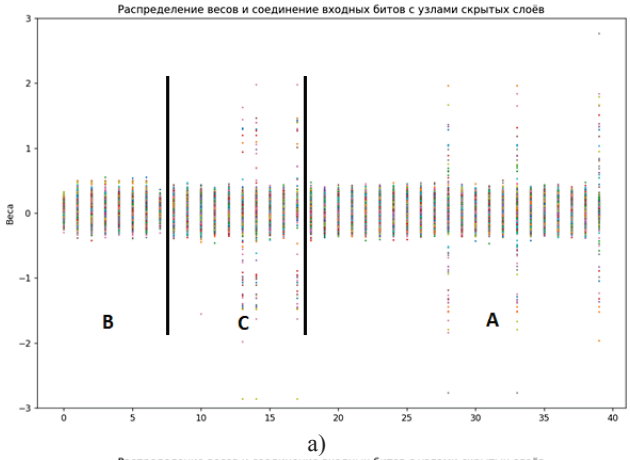
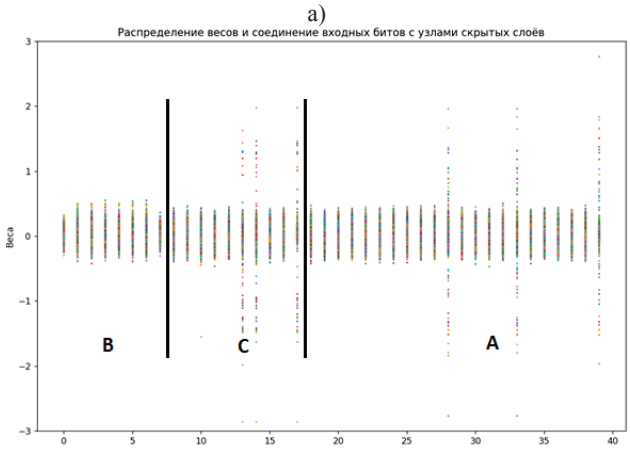


Рис. 8. Веса входных битов на входах узлов скрытого слоя НС моделирования основного блока ГПСЧ Mersenne Twister



а)



б)

Рис. 9. Веса входных битов на входах узлов скрытого слоя НС определения внутренней структуры ГПСЧ «стоп-пошел» при длинах регистров B, C и A 8, 10 и 22 разрядов, (а) и 16, 8 и 16 разрядов (б), соответственно

Решение задачи определения типа ГПСЧ не всегда означает возможность прогнозирования следующего значения на его выходе. Прогнозирование значений на выходе ГПСЧ Xorshift128 и Mersenne Twister осуществляется на выходе НС, которая участвует в классификации. После определения параметров ЛКГ также возможно прогнозирование выходного значения.

5. Анализ результатов синтеза моделей МО

В процессе разработки интеллектуальной системы анализа и классификации ГПСЧ при построении моделей МО использовались процедуры оптимизации, позволяющие выбрать структуры моделей, обеспечивающие высокое быстродействие без ущерба качеству прогнозирования.

В большинстве случаев обучение моделей занимало не более10 эпох.

При исследовании ГПСЧ «стоп-пошел» были проведены эксперименты по определению размера обучающей выборки, достаточной для получения высокого качества, что позволило сократить ее с миллионов значений до десятков тысяч. При этом время обучения сокращалось пропорционально уменьшению размера обучающей выборки.

Методы МО способны эффективно анализировать и прогнозировать работу ГПСЧ, значительно превосходя традиционные подходы. Например, восстановление чисел после операции xorshifter в ГПСЧ *Mersenne Twister* с использованием модели МО занимает всего 3 секунды против 35 минут методом полного перебора. Это дает возможность работы с алгоритмами более высокой сложности. Одновременно, при исследовании более сложных ГПСЧ методы МО не давали желаемого результата, а методы перебора оказывались действенными и давали положительный результат.

Таким образом, можно сделать вывод о необходимости интеграции различных методов для достижения поставленной цели [4]. В дальнейшем можно провести эксперименты с другими типами архитектур МО, которые могут оказаться эффективнее простой полносвязной сети, например рекуррентные сети.

Заключение

Разработанные модели МО и алгоритмы направленного перебора анализа и классификации ГПСЧ объединены в систему, способную идентифицировать последовательности. Программа, принимающая на вход псевдослучайные последовательности, классифицирует их или возвращает отрицательный ответ при отсутствии совпадений. Тесты подтвердили ее эффективность при идентификации ГПСЧ-источников последовательностей, а также корректное отклонение случайных данных, что делает систему готовой к расширению и интеграции новых моделей.

Разработанный прототип системы внедрен в учебный процесс на специальности «Компьютерная безопасность» РУТ (МИИТ). Студенты изучают применение ГПСЧ в разных сферах, проводят анализ различных типов ГПСЧ, выявляя их особенности и слабости, определяя влияние числовых параметров ГПСЧ на их качество, возможность классификации и прогнозирования [7]. Данная работа позволила углубить понимание работы ГПСЧ, развить аналитическое мышление и практические навыки при работе с методами МО. Студенты приняли участие в создании системы, интегрировав в нее алгоритмы классификации нескольких генераторов, что подчеркивает ее образовательную и практическую ценность. Наиболее заметные результаты получены при анализе линейного конгруэнтного генератора, генераторов Геффе и «стоп-пошел».

Основные проблемы при построении системы заключались в отсутствии выявленных зависимостей между вновь сгенерированным числом и последующим, а значит, непредсказуемости ГПСЧ и использовании необратимых операций.

В будущем планируется интеграция новых генераторов в систему и усовершенствование существующих методов классификации.

Список литературы

1. Schneier B., Ferguson N. Fortuna. URL: https://www.schneier.com/academic/fortuna/ (дата обращения: 15.12.2024).

2. Куминов В.П., Сидоренко В.Г. Решение задач анализа криптографической стойкости генераторов псевдослучайных чисел с использованием машинного обучения // Материалы XXXII Международной конференции «Проблемы управления безопасностью сложных систем» (посвящена памяти В.В. Кульбы). М.: ИПУ РАН, 2024. URL: https://iccss2024.ipu.ru/proceedings/%D0%9A%D1%83%D0%BC%D0%B8%D0%BD%D0%BE%D0%B2.pdf (дата обращения: 20.01.2025).

3. Куминов В.П., Сидоренко В.Г. Методы оценки качества генераторов псевдослучайных чисел // Интеллектуальные транспортные системы: Материалы III Международной научно-практической конференции, Москва, 30 мая 2024 года. М.: Российский университет транспорта (МИИТ), 2024. С. 631–636. DOI: 10.30932/9785002446094-2024-631-636

4. Hassan M. Cracking Random Number Generators using Machine Learning – Part 1: xorshift128. URL: https://www.nccgroup.com/us/research-blog/cracking-random-number-generators-using-machine-learning-part-1-xorshift128/ (дата обращения: 26.06.2025).

5. Common Weakness Enumeration. URL: https://cwe.mitre.org/data/definitions/330.html (дата обращения: 20.01.2025).

6. Вихрь Мерсенна (Справочник). URL: https://dic.academic.ru/dic.nsf/ruwiki/88739 (дата обращения: 20.01.2025).

7. Hassan, M. Cracking Random Number Generators using Machine Learning – Part 1: Xorshift128 [Сайт]. – URL: https://research.nccgroup.com/2021/10/15/cracking-random-number-generators-using-machine-learning-part-1-Xorshift128/ (дата обращения: 20.01.2025).

8. Воронина Е.Г., Сидоренко В.Г. Генераторы случайных чисел: Учебное пособие / Российский университет

транспорта (МИИТ). М.: ФГАОУ ВО «Российский университет транспорта», 2018. 80 с.

References

1. Schneier B., Ferguson N. Fortuna. (accessed 15.12.2024). Available at: https://www.schneier.com/academic/fortuna.

2. Kuminov V.P., Sidorenko V.G. [Analysing cryptographic strength of pseudorandom number generators using machine learning]. In: Proceedings of the XXXII International Conference Complex System Security Management (in memory of V.V. Kulba). Moscow: IPU RAS; 2024. (accessed 20.01.2025). (in Russ.) Available at: https://iccss2024.ipu.ru/proceedings/%D0%9A%D1%83%D0%BC%D0%B8%D0%BD%D0%BE%D0%B2.pdf.

3. Kuminov V.P., Sidorenko V.G. [Methods for evaluating the quality of pseudorandom number generators]. In: Intelligent Transportation Systems: Proceedings of the III International Research and Practice Conference. Moscow; May 30, 2024. Moscow: Russian University of Transport (MIIT); 2024. Pp. 631-636. (in Russ.) DOI: 10.30932/9785002446094-2024-631-636.

4. Hassan M. Cracking Random Number Generators using Machine Learning – Part 1: xorshift128. (accessed 26.06.2025). Available at: https://www.nccgroup.com/us/research-blog/cracking-random-number-generators-using-machine-learning-part-1-xorshift128.

5. Common Weakness Enumeration. (accessed 20.01.2025). Available at: https://cwe.mitre.org/data/definitions/330.html.

6. Mersenne twister (reference). (accessed 20.01.2025). Available at: https://dic.academic.ru/dic.nsf/ruwiki/88739.

7. Hassan M. Cracking Random Number Generators using Machine Learning – Part 1: Xorshift128. (accessed 20.01.2025). Available at: https://research.nccgroup.com/2021/10/15/cracking-random-number-generators-using-machine-learning-part-1-Xorshift128.

8. Voronina E.G., Sidorenko V.G. [Random number generators: A textbook]. Moscow: Russian University of Transport; 2018. (in Russ.)

Сведения об авторах

Автоношкин Александр Михайлович – студент, Российский университет транспорта (*Russian University of Transport (MIIT)*), Российская Федерация, Москва, e-mail: 1146248@edu.rut-miit.ru.

Куминов Валерий Павлович – студент, Российский университет транспорта (*Russian University of Transport (MIIT)*), Российская Федерация, Москва, e-mail: 1036301@edu.rut-miit.ru.

Сидоренко Валентина Геннадьевна – доктор технических наук, профессор, профессор кафедры «Управление и защита информации», Российский университет транспорта (*Russian University of Transport (MIIT)*), Российская Федерация, Москва, e-mail: valenfalk@mail.ru.

Смецкая Анастасия Сергеевна – студент, Российский университет транспорта (*Russian University of Transport (MIIT)*), Российская Федерация, Москва, e-mail: 1137782@edu.rut-miit.ru.

About the authors

Alexander M. Avtonoshkin, student, *Russian University of Transport (MIIT)*, Russian Federation, Moscow, e-mail: 1146248@edu.rut-miit.ru.

Valery P. Kuminov, student, *Russian University of Transport (MIIT)*, Russian Federation, Moscow, e-mail: 1036301@edu.rut-miit.ru.

Valentina G. Sidorenko, Doctor of Engineering, Professor, Chair Professor, Department of Management and Protection of Information, *Russian University of Transport (MIIT)*, Russian Federation, Moscow, e-mail: valenfalk@mail.ru.

Anastasia S. Smetskaya, student, *Russian University of Transport (MIIT)*, Russian Federation, Moscow, e-mail: 1137782@edu.rut-miit.ru.

Вклад авторов в статью

Автоношкин А.М. – анализ работы генератора псевдослучайных чисел «стоп-пошел».

Куминов В.П. – анализ работы генераторов псевдослучайных чисел Xorshift128 и Mersenne Twister, планирование работы по исследованию других генераторов псевдослучайных чисел.

Сидоренко В.Г. – руководство работой и обобщение полученных результатов.

Смецкая А.С. – разработка программного обеспечения для анализа работы генератора псевдослучайных чисел «стоп-пошел».

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.