ORES
Научно-практический электронный журнал
**Оригинальные исследования (ОРИС)**, *ISSN 2222-0402*
www.ores.su
original-research.ru

**УДК 004.021:004.056**

# СВОЙСТВА ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ И ИХ ПРИМЕНЕНИЕ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

**Басыров Ильдар Ильшатович,**
Студент магистратуры
2 курс, факультет «Сети и системы связи»
Кафедра «Сети связи и системы коммутации»
Московский технический университет связи и информатики
e-mail: basyrov.ildar@mail.ru

**Шишкин Сергей Русланович,**
Студент магистратуры
2 курс, факультет «Кибернетика и информационная безопасность»
Кафедра «Интеллектуальные системы управления и автоматизации»
Московский технический университет связи и информатики
e-mail: sergeyshishkin62@gmail.com

**Городилова Дарья Витальевна,**
Студент бакалавриата
4 курс, факультет «Кибернетика и информационная безопасность»
Кафедра «Информационная безопасность»
Московский технический университет связи и информатики
e-mail: d.v.gorodilova@edu.mtuci.ru

**Аннотация**

В работе рассмотрены свойства двоичных последовательностей, их статистические, корреляционные и спектральные характеристики, а также современные методы генерации. Особое внимание уделено применению рекуррентных нейронных сетей (Recurrent Neural Networks – RNN) и квантовых генераторов случайных чисел (Quantum Random Number Generators – QRNG), которые позволяют получать последовательности с улучшенными характеристиками. Предложен адаптивный подход к выбору последовательностей, учитывающий текущие параметры канала связи, такие как уровень шума и загруженность. Выявлено, что последовательности с высокой энтропией и минимальными корреляционными характеристиками обладают повышенной устойчивостью к криптоанализу, что делает их незаменимыми для задач криптографии и защиты информации.

**Ключевые слова:** двоичные последовательности, статистические характеристики, корреляционные свойства, спектральный анализ, нейронные сети, квантовые генераторы случайных чисел, криптоанализ, адаптивный выбор, информационная безопасность.

# PROPERTIES OF BINARY SEQUENCES AND THEIR APPLICATIONS IN MODERN INFORMATION SYSTEMS

**Basyrov Ildar Ilshatovich,**
Master's student
2nd year, Faculty of Networks and Communication Systems
Department of Communication Networks and Switching Systems
Moscow Technical University of Communications and Informatics

**Shishkin Sergey Ruslanovich,**
Master's student
2nd year, Faculty of Cybernetics and Information Security
Department of Intelligent Control Systems and Automation
Moscow Technical University of Communications and Informatics

**Gorodilova Darya Vitalievna,**
Bachelor's student
4th year, Faculty of Cybernetics and Information Security
Department of Information Security
Moscow Technical University of Communications and Informatics

ABSTRACT

The paper examines the properties of binary sequences, including their statistical, correlation, and spectral characteristics, as well as modern generation methods. Special attention is given to the use of Recurrent Neural Networks (RNN) and Quantum Random Number Generators (QRNG), which enable the creation of sequences with enhanced characteristics. An adaptive approach to sequence selection is proposed, taking into account current channel parameters such as noise level and load. It has been found that sequences with high entropy and minimal correlation characteristics demonstrate increased resistance to cryptanalysis, making them indispensable for cryptography and information security tasks.

**Keywords:** binary sequences, statistical characteristics, correlation properties, spectral analysis, neural networks, quantum random number generators, cryptanalysis, adaptive selection, information security.

Введение

Двоичные последовательности являются основой функционирования информационных систем, включая цифровую связь, обработку сигналов и криптографию. Их свойства, такие как равномерность распределения, низкая корреляция и высокая энтропия, напрямую влияют на надежность передачи данных, устойчивость к помехам и защиту информации от несанкционированного доступа [1].

С увеличением объемов данных и сложностью угроз традиционные методы генерации последовательностей, такие как линейные регистры сдвига, демонстрируют ограничения [2]. Современные подходы, включая методы машинного обучения и квантовые алгоритмы, позволяют генерировать последовательности с улучшенными

характеристиками, что особенно важно в условиях растущих требований к безопасности и эффективности передачи данных [3,4].

В данной работе проводится анализ свойств двоичных последовательностей, рассматриваются их современные методы генерации и оцениваются перспективы применения для оптимизации работы информационных систем в условиях современных вызовов.

Анализ основных свойств двоичных последовательностей

Двоичные последовательности являются основой современных цифровых технологий, таких как системы связи, криптография, цифровая обработка сигналов и машинное обучение. Их свойства определяют надежность, безопасность и эффективность передачи данных. Основные аспекты анализа включают их статистические, корреляционные и спектральные характеристики.

Статистические свойства двоичных последовательностей определяются равномерностью распределения нулей и единиц. Для обеспечения высокой энтропии, которая характеризует уровень случайности последовательности, важно, чтобы частота появления нулей и единиц была примерно одинаковой. Это особенно актуально для криптографических систем, где низкая энтропия последовательности может привести к предсказуемости, что увеличивает уязвимость к атакам.

Например, исследования показывают, что псевдослучайные последовательности, такие как последовательности, генерируемые с использованием линейных регистров сдвига с обратной связью (Linear Feedback Shift Register – LFSR), могут обладать предсказуемостью при недостаточно большом размере регистра [5]. Современные подходы предлагают использование нейросетевых моделей, таких как рекуррентные нейронные сети (Recurrent Neural Networks – RNN), для генерации двоичных последовательностей. Нейронные сети обучаются на больших массивах данных, что позволяет достичь равномерного распределения и гарантировать высокий уровень энтропии. [6,7]

Корреляционные свойства определяются способностью последовательности быть «саморазличимой». Основной инструмент анализа – это автокорреляционная функция, которая отражает степень схожести последовательности с ее сдвинутой копией. Важным условием является минимизация значений автокорреляционной функции вне центрального пика. Это свойство позволяет достичь синхронизации и точного обнаружения последовательности в системах связи и радиолокации.

Для анализа автокорреляционных свойств может быть использована таблица значений функции на основе алгоритмической оценки последовательностей (таблица 1). В данном статье предложен подход оптимизации автокорреляционных свойств на основе эволюционных алгоритмов, таких как генетические алгоритмы (Genetic Algorithms – GA). Эти алгоритмы позволяют находить последовательности с минимальной внепиковой корреляцией, что особенно полезно для задач синхронизации в условиях помех.

Таблица 1. Значения автокорреляционной функции для различных последовательностей

| Последовательность | Центральный пик | Внепиковые значения |
|---|---|---|
| Максимальная линейная (m-последовательность) | 1 | 0.1 |
| Псевдослучайная (RNN) | 1 | 0.05 |

Анализ спектральных характеристик двоичных последовательностей основан на изучении распределения энергии в частотной области. Для этого используется преобразование Фурье, которое позволяет оценить, как энергия распределяется по

частотам. Важным условием является равномерность распределения энергии, что предотвращает интерференцию и повышает надежность передачи данных.

Для улучшения спектральных характеристик в данном исследовании применяется вейвлет-преобразование, которое позволяет учитывать временные изменения спектра последовательности. Это особенно полезно для анализа непериодических последовательностей. Пример спектрального анализа представлен на рисунке 1, где показано распределение энергии для различных типов последовательностей.


Рисунок 1. Спектральное распределение энергии двоичных последовательностей

Современные методы генерации и анализа

Современные задачи информационных систем требуют генерации двоичных последовательностей с оптимальными характеристиками, такими как равномерное распределение, высокая энтропия и минимальные корреляционные свойства. Эти задачи требуют применения новых подходов, включающих машинное обучение и квантовые технологии. Такие методы позволяют адаптировать последовательности к конкретным условиям эксплуатации и требованиям.

Один из перспективных подходов к генерации двоичных последовательностей заключается в применении рекуррентных нейронных сетей. Эти модели машинного обучения учитывают последовательность данных, на которой они обучаются, что позволяет создавать двоичные последовательности с заранее заданными свойствами. Например, для криптографических задач важна высокая энтропия последовательности и её устойчивость к анализу. Для систем связи, напротив, необходимо учитывать минимизацию внепиковой корреляции для повышения точности синхронизации сигналов.

В рамках исследований RNN обучают на больших массивах данных, содержащих примеры двоичных последовательностей с оптимальными характеристиками. Например, используются m-последовательности, которые генерируются линейными регистрами сдвига с обратной связью, но дополнительно оптимизируются через обучение сети.

Квантовые генераторы случайных чисел (Quantum Random Number Generators – QRNG) предоставляют совершенно иной подход к генерации последовательностей. Их работа основана на квантовом механизме неопределенности, например, фиксации результатов измерений суперпозиционных квантовых состояний. Это позволяет получить абсолютно случайные последовательности с максимально возможной энтропией.

QRNG имеют существенное преимущество перед классическими алгоритмическими генераторами, которые, несмотря на псевдослучайность, могут быть предсказаны при наличии достаточного объема данных. QRNG исключают предсказуемость даже при полном знании алгоритма, что делает их особо эффективными для задач информационной безопасности, таких как генерация криптографических ключей.

Анализ применимости QRNG показывает, что такие устройства наиболее эффективны в высокозащищенных системах, например, для шифрования данных в виртуальных частных сетях (Virtual Private Networks – VPN) или в распределенных системах квантового ключевого распределения (Quantum Key Distribution – QKD). Пример сравнительного анализа QRNG и классических методов представлен в таблице 2.

Таблиц 2. Сравнительные характеристики QRNG и псевдослучайных генераторов

| Параметр | QRNG | LFSR |
|---|---|---|
| Уровень энтропии | Максимальный | Зависит от алгоритма |
| Сложность предсказания | Невозможно | Возможна при известных условиях |
| Применимость для криптографии | Высокая | Средняя |
| Производительность | Средняя | Высокая |

Инновационные подходы к применению

Современные информационные системы требуют адаптивных методов выбора и использования двоичных последовательностей. Эти методы учитывают изменяющиеся характеристики каналов связи, а также необходимость обеспечения высокого уровня информационной безопасности. В данном разделе рассматриваются два ключевых подхода: адаптивный выбор последовательностей в реальном времени и использование последовательностей в криптографических системах.

В условиях реального времени характеристики канала связи, такие как уровень шума, скорость передачи данных и наличие помех, могут меняться. Это требует адаптации используемых последовательностей. Предложена система, позволяющая анализировать текущие параметры канала и динамически выбирать наиболее подходящие двоичные последовательности.

Основой системы является алгоритм машинного обучения, который классифицирует состояние канала связи. Например, алгоритм на основе градиентного бустинга (Gradient Boosting Machine – GBM) оценивает уровень шума и загруженность канала, после чего выбирает оптимальную последовательность с минимальной внепиковой корреляцией. В таблице ниже представлены основные параметры выбора последовательностей в зависимости от состояния канала.

Таблица 3. Адаптивный выбор последовательностей в зависимости от состояния канала связи

| Состояние канала | Уровень шума | Рекомендуемая последовательность | Преимущества |
|---|---|---|---|
| Высокий уровень шума | Высокий | m-последовательность | Устойчивость к помехам |
| Средняя загруженность | Средний | Псевдослучайная последовательность | Баланс между скоростью и шумом |
| Низкая загруженность | Низкий | Случайная последовательность | Максимальная скорость передачи |

Адаптивный подход также позволяет учитывать изменения в скорости передачи данных. Например, при повышении скорости системы связи могут использовать более короткие последовательности, чтобы уменьшить задержки.

Информационная безопасность зависит от энтропии и корреляционных свойств последовательностей, используемых в криптографических системах. Для повышения

стойкости к криптоанализу предложена методика, основанная на оценке энтропии последовательностей.

Энтропия двоичных последовательностей измеряется с использованием формулы Шеннона:

$$H = -\sum_{i=1}^{n} P(x_i) \log_2 P(x_i) \quad (1)$$

где $P(xi)$ – вероятность появления i-го элемента последовательности. Высокая энтропия указывает на максимальную случайность последовательности, что минимизирует вероятность успешного анализа или предсказания её структуры.

Методика включает несколько этапов:

генерация набора последовательностей с различными статистическими свойствами;

оценка уровня их энтропии;

выбор последовательностей с максимально возможной энтропией.

Для подтверждения эффективности методики проведено сравнение стойкости последовательностей к криптоанализу методом частотного анализа. Результаты представлены на рисунке 5.

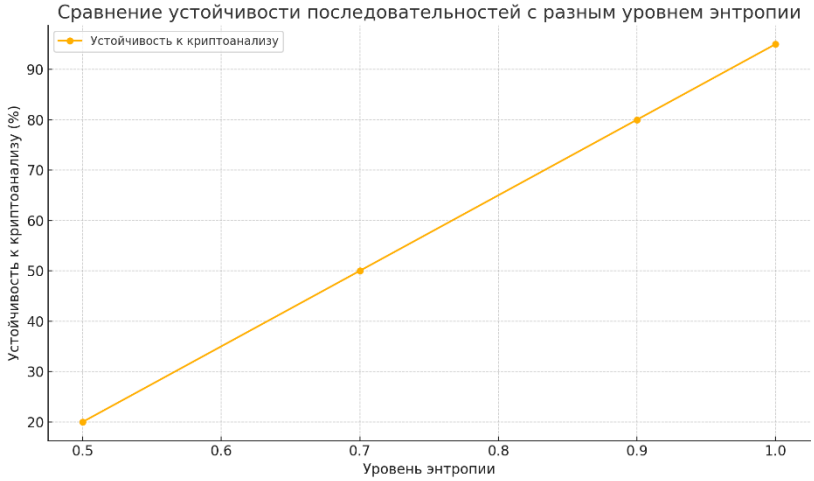


Рисунок 2. Сравнение устойчивости последовательностей с разным уровнем энтропии к криптоанализу

Кроме того, особое внимание уделено устойчивости последовательностей к атаке методом корреляционного анализа, когда атакующий пытается восстановить исходные данные, анализируя корреляционные зависимости. В криптографических системах такие последовательности находят применение при генерации ключей шифрования, в схемах потокового шифрования и системах распределения ключей.

Заключение

В данной работе проведен анализ свойств двоичных последовательностей, их статистических, корреляционных и спектральных характеристик, а также современных методов их генерации. Рассмотренные подходы, такие как рекуррентные нейронные сети и квантовые генераторы случайных чисел, продемонстрировали свою эффективность в решении задач повышения надежности передачи данных и информационной безопасности. Применение адаптивных методов выбора последовательностей, учитывающих текущие характеристики канала связи, позволяет динамически адаптировать параметры систем для достижения оптимальных результатов.

Особое внимание уделено обеспечению информационной безопасности. Показано, что последовательности с высокой энтропией и минимальной корреляцией обладают повышенной устойчивостью к криптоанализу. Предложенные методы могут быть успешно применены в задачах генерации криптографических ключей, потокового шифрования и защиты данных. Дальнейшие исследования могут быть направлены на интеграцию методов машинного обучения с квантовыми технологиями и разработку универсальных стандартов тестирования последовательностей.

**Список литературы:**


1. Proakis J.G., Salehi M. Digital Communications. 5th ed. – McGraw-Hill Higher Education, 2008.
2. Shannon C. E. A Mathematical Theory of Communication // The Bell System Technical Journal. – 1948. – Vol. 27. – P. 379–423, 623–656.
3. Гусаров, А. В. Программные и аппаратные генераторы двоичных последовательностей в информационных системах / А. В. Гусаров, Н. А. Хачикова. — Текст: непосредственный // Технические науки в России и за рубежом: материалы VIII Междунар. науч. конф. (г. Краснодар, июнь 2019 г.). — Краснодар : Новация, 2019.
4. Беляева, Т. А. Нейросетевое прогнозирование инцидентов информационной безопасности / Т. А. Беляева, А. А. Микрюков // Международный студенческий научный вестник. – 2023. – № 6. – С. 30. – EDN HLYWRW.
5. Golomb, S.W. "Shift Register Sequences." Aegean Park Press, 1982.
6. Proakis, J.G., Salehi, M. "Digital Communications." McGraw-Hill Higher Education, 2008.
7. Алесинский, Е. И. Исследование и разработка модели оценки информационной безопасности объекта / Е. И. Алесинский. — Текст: непосредственный // Молодой ученый. — 2021. — № 11 (353). — С. 8-12.


**References:**


1. Proakis J.G., Salehi M. Digital Communications. 5th ed. – McGraw-Hill Higher Education, 2008.
2. Shannon C. E. A Mathematical Theory of Communication // The Bell System Technical Journal. – 1948. – Vol. 27. – P. 379–423, 623–656.
3. Gusarov, A.V. Software and hardware generators of binary sequences in information systems / A.V. Gusarov, N.A. Khachikova. — Text: direct // Technical sciences in Russia and abroad: materials of the VIII Int. scientific conf. (Krasnodar, June 2019). — Krasnodar : Novation, 2019.
4. Belyaeva, TA Neural network forecasting of information security incidents / TA Belyaeva, AA Mikryukov // International student scientific bulletin. - 2023. - No. 6. - P. 30. - EDN HLYWRW.
5. Golomb, S.W. "Shift Register Sequences." Aegean Park Press, 1982.
6. Proakis, J.G., Salehi, M. "Digital Communications." McGraw-Hill Higher Education, 2008.
7. Alesinsky, EI Research and development of a model for assessing the information security of an object / EI Alesinsky. - Text: direct // Young scientist. - 2021. - No. 11 (353). - P. 8-12.