DOI: 10.17725/rensit.2022.14.047

Информационные технологии на основе шумоподобных сигналов: I. Дискретные хаотические алгоритмы

Агейкин Н.А., Грачев В.И., Рябенков В.И., Колесов В.В.
Институт радиотехники и электроники им. В.А. Котельникова РАН, http://www.cplire.ru/
Москва 125009, Российская Федерация
E-mail: ageykin_niki@mail.ru, grachev@cplire.ru, ryabenkov.vi@list.ru, kvv@cplire.ru

Поступила 20.03.2022, рецензирована 24.03.2022, принята 27.03.2022

Аннотация: **Рассмотрены перспективные направления использования информационных технологий на основе динамического хаоса для передачи, обработки, хранения и защиты информации. На основе нелинейных систем с хаотической динамикой разработаны конечномерные порождающие математические алгоритмы для синтеза хаотических кодирующих сигналов с повышенной структурной сложностью. Проведен анализ структурной и фрактальной сложности псевдослучайных целочисленных и бинарных последовательностей. Показано, что сложные кодирующие сигналы такого типа обладают высокой информационной емкостью и по статистическим, корреляционным и фрактальным свойствам практически совпадают с параметрами случайных последовательностей и могут эффективно использоваться в различных многопользовательских радиотехнических системах, где требуется высокая помехоустойчивость, защита от несанкционированного доступа и криптостойкость.**

Ключевые слова: **информационные технологии, хаотическая динамика, псевдослучайные последовательности, кодирование информации**

УДК 621.391

Благодарности: Работа выполнена в рамках государственного задания ИРЭ им.В.А. Котельникова РАН от Минобрнауки РФ.

Для цитирования: Агейкин Н.А., Грачев В.И., Рябенков В.И., Колесов В.В. Информационные технологии на основе шумоподобных сигналов: I. Дискретные хаотические алгоритмы. *РЭНСИТ: Радиоэлектроника. Наносистемы. Информационные технологии,* 2022, 14(1)47-64. DOI: 10.17725/rensit.2022.14.047.

Information Technologies Based on Noise-like Signals: I. Discrete Chaotic Algorithms

Nikita A. Ageykin, Vladimir I. Grachev, Viktor I. Ryabenkov, Vladimir V. Kolesov
Kotelnikov Institute of Radioengineering and Electronics of RAS, http://www.cplire.ru/
Moscow 125009, Russian Federation
E-mail: ageykin_niki@mail.ru, grachev@cplire.ru, ryabenkov.vi@list.ru, kvv@cplire.ru

Received March 20, 2022, peer-reviewed March 24, 2022, accepted March 27, 2022

Abstract: **Perspective directions of using information technologies based on dynamic chaos for the transmission, processing, storage and protection of information are considered. On the basis of nonlinear systems with chaotic dynamics, finite-dimensional generating mathematical algorithms have been developed for the synthesis of chaotic encoding signals with increased structural complexity. The analysis of structural and fractal complexity of pseudo-random integer and binary sequences has been carried out. It is shown that complex coding signals of this type have a high information capacity and, in terms of statistical, correlation, and fractal properties, practically coincide with the parameters of random sequences and can be effectively used in various multi-user radio engineering systems where high noise immunity, protection against unauthorized access, and cryptographic strength are required.**

Keywords: **information technologies, chaotic dynamics, pseudo-random sequences, information coding**

UDC 621.391

Acknowledgments: Work is carried out in frame of State assignments from the Ministry of Science and Higher Education of the Russian Federation for Kotelnikov Institute of Radio Engineering and Electronics of RAS.

For citation: Nikita A. Ageykin, Vladimir I. Grachev, Viktor I. Ryabenkov, Vladimir V. Kolesov. Information Technologies Based on Noise-like Signals: I. Discrete Chaotic Algorithms. *RENSIT: Radioelectronics. Nanosystems. Information Technologies*, 2022, 14(1):47-64. DOI: 10.17725/rensit.2022.14.047.

Содержание

1. ВВЕДЕНИЕ

Поиск информационных носителей (процессов и сигналов), обладающих повышенной информационной емкостью, а также математических алгоритмов, порождающих такие процессы, является наиболее актуальной задачей при разработке новых информационных технологий. Такими носителями информации могут быть графика, тексты, нотные записи, числа, а также электромагнитные сигналы, которые используются в современных телекоммуникационных системах. Информация в этих системах записывается, обрабатывается и передается либо в виде непрерывного электрического сигнала – аналоговая форма кодирования информации, либо в виде последовательности электрических импульсов – цифровая форма кодирования. При аналоговом кодировании необходимая информация передается при соответствующей модуляции амплитуды, частоты или фазы колебаний непрерывного электрического сигнала. В цифровой форме информация представляется в виде двоичного кода 0, 1. Цифровые коды благодаря хорошей защищенности от ошибок и помех, высоким скоростям обработки в вычислительных системах и высокой плотности передачи по каналам связи преимущественно распространены в современных радиорелейных системах.

Наблюдающаяся в последние годы тенденция глобального распространения разнообразных открытых телекоммуникационных систем и резкий рост числа абонентов, приводят к необходимости защиты информации не только на уровне государственных органов, специальных служб или деловых кругов, но и на уровне практически каждого индивидуального пользователя. В информационных сетях данная проблема связана не столько с конфиденциальностью информации, сколько с потерями информации из-за низкой помехоустойчивости различных каналов связи [1].

Насыщенность частотного диапазона традиционными многоканальными средствами связи, основанными на принципе частотного разделения каналов, привела к разработке новых методов кодирования для так называемого кодового разделения каналов, в которых в качестве кодов применяются кодирующие потоки случайных (псевдослучайных) чисел (CDMA-technology – Code Division Multiple Access). При потоковом кодировании информации с помощью непрерывных случайных кодирующих потоков с равномерной функцией распределения обеспечивается максимальная помехоустойчивость, а значит и максимальная криптостойкость информационного канала. Необходимо отметить, что в телекоммуникационных системах с кодовым разделением абонентов все абонентские каналы

связи работают в общей широкой полосе частот [2].

В настоящее время в радиорелейных системах связи и особенно в радиолокации активно развивается перспективное направление, представляющее широкополосные и сверхширокополосные технологии. В рамках этого направления представляется возможным перейти к качественно новому уровню решения задач по помехоустойчивости и защите информации в каналах связи, а также дистанционному радиолокационному обнаружению объектов. Например, в дополнение к стандартному радиолокационному энергетическому критерию (на уровне "да"/"нет") обнаружения объекта на фоне шумов и подстилающей поверхности можно перейти к формированию радиолокационного портрета объекта и разработке систем автоматического распознавания объекта по его портрету, что качественно увеличивает информационные возможности радиолокационных систем. Радиолокация сигналами с широким спектром частот позволяет осуществлять высокоточные, информативные измерения параметров отражающих объектов в сложных условиях электромагнитной обстановки при воздействии активных и пассивных помех.

Повышение точности и разрешающей способности радиолокационных измерений связано с усложнением структуры и расширением полосы частот зондирующего сигнала. Такое расширение может быть достигнуто либо за счет укорочения импульса, либо при использовании частотной или фазовой модуляции непрерывной или квазинепрерывной несущей. Предельным случаем непрерывного широкополосного зондирующего сигнала является так называемый белый шум с равномерным спектром, т.е. сигнал, имеющий функцию неопределенности типа δ-функции. Такой сигнал обеспечивает высокоточные однозначные измерения как дальности до цели, так и радиальной составляющей скорости цели. Дополнительным преимуществом непрерывного широкополосного шума является возможность обеспечения хорошего соотношения сигнал/шум на входе приемного устройства в сравнении с импульсными сигналами. В случае применения сверхкоротких импульсов для получения удовлетворительного отношения сигнал/шум требуется огромная мощность сигнала в импульсе, тогда как при непрерывном режиме работы необходимая величина отношения сигнал/шум легко достигается при мощности, намного порядков меньших мощности в импульсе.

Широкополосные шумоподобные сигналы (ШПС) благодаря своим специфическим особенностям, таким как низкая спектральная плотность, высокая помехозащищенность по отношению к стационарным и организованным помехам большой мощности, возможность разделения по кодовому признаку, высокая стойкость в условиях многолучевого распространения, высокая разрешающая способность при измерении расстояний, все более широко применяются в различных радиотехнических системах. ШПС используются при построении спутниковых систем связи и навигации, сотовых систем подвижной радиосвязи, локальных радиосетей, систем связи внутри зданий и в ряде других систем [3].

В последнее время в связи с развитием многопользовательских коммуникационных систем большое внимание привлекает такой класс широкополосных сигналов, как сигналы с кодовым расширением спектра [4]. Полоса частот передаваемого сигнала с кодовым расширением спектра может быть значительно шире полосы частот информационного сообщения. Для многих коммуникационных систем важно иметь возможность передавать информацию одновременно нескольким пользователям по одной и той же линии связи за счет кодового разделения абонентских каналов (CDMA technology).

Широкополосные сигналы образуются за счет расширения полосы частот информационного сигнала и (или) за счет расширения несущей. Расширение полосы частот сигнала достигается за счет модуляции несущего колебания по закону передаваемых сообщений, например, частотной

модуляции с большим индексом, фазовой манипуляции с помощью псевдослучайной последовательности из коротких двоичных символов. Расширение полосы свойственно также цифровым сигналам с дополнительным, помехоустойчивым кодированием, так как введение избыточных символов при сохранении неизменной скорости передачи сообщения приводит к необходимости уменьшить длительность каждого символа. При этом расширяется полоса частот передаваемого кодированного сигнала [5].

Эффективная расширяющая функция должна удовлетворять определенным требованиям в отношении ширины полосы частот, структуры приемника и метода передачи сообщения. Расширяющая функция должна быть детерминированной на относительно большом интервале времени и иметь шумоподобный равномерный спектр в широкой полосе частот (большую базу), следовательно, узкую автокорреляционную функцию с малыми боковыми выбросами [6].

Ансамбль расширяющих функций, используемых различными системами или одной многоканальной системой, должен обладать хорошими взаимокорреляционными и групповыми свойствами. Расширяющая функция может быть непрерывной аналоговой или дискретной цифровой. Формирование широкополосных псевдослучайных сигналов наиболее перспективно осуществлять методами цифровой обработки сигналов. В этом случае расширяющие функции формируются на основе цифровых кодовых последовательностей. В некоторых случаях возможно одновременное расширение спектра сигнала за счет различных методов модуляции, когда, например, наряду с расширяющей функцией используется цифровое, помехоустойчивое кодирование сообщений восстанавливающими кодами.

К виду и качеству сигналов в радиотехнических системах с ШПС предъявляется ряд достаточно жестких требований:

1) сигнал должен быть достаточно широкополосным: база сигнала B, т.е. произведение длительности сигнала T на ширину его полосы F, должно быть много больше единицы;

2) спектральная плотность шума в полосе канала передачи должна быть равномерной;

3) автокорреляционная функция (АКФ) сигнала должна иметь один узкий пик и малые боковые выбросы на интервале T;

4) сигнал должен быть воспроизводим в приемном устройстве в случае корреляционного способа приема.

Такие сигналы обычно формируются на основе псевдослучайных кодовых последовательностей.

Бинарные псевдослучайные последовательности (ПСП) должны удовлетворять трем критериям случайности:

- сбалансированность бинарного кода;
- для бинарного кода вероятность появления блока из k одинаковых символов должна быть близка к $1/2^k$;
- результат суммирования кода по модулю 2 с его циклическим сдвигом должен давать также сбалансированный код.

1.1. Псевдослучайные кодирующие последовательности

Из теории информации известно, что наибольшей информационной емкостью обладают стохастические сигналы, порождаемые случайными процессами [7]. Основная проблема при разработке информационных носителей в цифровых телекоммуникационных каналах заключается в трудности генерирования случайных двоичных последовательностей с применением короткого задающего ключа. Математические алгоритмы, которые на основе ключа формируют псевдослучайные последовательности (ПСП) числовых значений, должны обладать рядом необходимых свойств:

1) сколь угодно большой длиной периода непериодического сегмента получаемой ПСП,

2) статистическим подобием получаемой последовательности чисел свойствам чисто случайной выборки,

3) возможностью программно-аппаратной реализации генератора случайных чисел для применения в канале связи с соответствующим быстродействием.

Следует особо отметить, что при генерации псевдослучайных последовательностей одна из основных проблем заключается в необходимости формирования длинных реализаций при использовании короткого задающего ключа, определяющего начальные условия.

При программной реализации алгоритмов генерации псевдослучайных процессов ЭВМ оперирует с дискретными числами в бинарном представлении с конечным числом разрядов. Учитывая это ограничение на конечную разрядность чисел в ЭВМ, полный объем фазового пространства (ФП), любая точка которого соответствует однозначному состоянию системы, ограничен, и соответственно любой алгоритмический метод формирования должен рано или поздно выйти на периодическое повторение одних и тех же сегментов формируемой последовательности, то есть выйти на цикл, хотя его период и может быть очень большим и даже бесконечным с точки зрения ряда практических применений [8].

Требования, предъявляемые к свойствам последовательностей псевдослучайных чисел, зависят от конкретных применений и, как правило, один алгоритм не в состоянии всем этим требованиям удовлетворить. В общем случае можно сформулировать основные требования, предъявляемые к ПСП [9]:

- высокое качество: ПСП по статистическим критериям должна быть близка к случайному процессу и иметь возможно более длинный период;
- эффективность: алгоритм должен быть быстрым и занимать возможно меньший объем памяти;
- воспроизводимость: при точном воспроизведении начальных условий алгоритма должна формироваться одна и та же ПСП на реализациях любой длительности, а незначительные изменения в начальной процедуре должны приводить к генерации качественно различных последовательностей;
- простота: формула алгоритма должен быть проста в реализации и использовании.

Все сказанное подчеркивает актуальность поиска новых детерминированных алгоритмов, обеспечивающих формирование потоков псевдослучайных чисел, удовлетворяющих различным системам требований.

В общедоступной литературе практически отсутствуют сведения о методах разработки алгоритмов генерации псевдослучайных чисел. Разработка новых алгоритмов требует понимания закономерностей формирования ПСП чисел с определенными заданными статистическими свойствами.

С точки зрения практического применения в цифровых информационных технологиях интерес представляют алгоритмы, определенные на замкнутом интервале целых чисел. Их достоинство связано с отсутствием необходимости использовать какое-либо округление в процессе вычисления членов последовательности. Соответственно результаты вычисления в этом случае не будут зависеть от разрядности шины данных в конкретной ЭВМ и числа значащих цифр в представлении чисел с фиксированной запятой [10].

Несмотря на то, что известно довольно много алгоритмов генерации ПСП, на практике для генерации двоичных ПСП, как правило, используется рекуррентный алгоритм, когда на основании линейного рекуррентного соотношения и некоторых начальных значений строится бесконечная последовательность, каждый последующий член которой определяется из предыдущих. Двоичные последовательности на основе рекуррентных соотношений достаточно легко реализуются на ЭВМ в виде программ и схемотехнически на основе быстродействующих многоразрядных двоичных сдвиговых регистров.

Попытки приспособить для цифровых алгоритмов операции над действительными числами оканчивались неудачами, так как замена действительного числа его приближенным значением сильно меняет

статистику получаемой последовательности. Операция округления вносит непредсказуемое возмущение в порождающий алгоритм, и получаемая последовательность перестает быть статистически независимой, а значит, и случайной.

Основной метод получения ПСП в настоящее время – это формирование М-последовательностей (последовательности максимального периода) на основе сдвиговых регистров, когда численное значение последовательности в данный момент определяется линейными соотношениями с некоторым весом (кодом) по отношению к предыдущим членам последовательности. При этом весовые коэффициенты подбирают таким образом, чтобы обеспечить быстрый спад корреляционной функции до значений порядка $1/\sqrt{N}$, где N – длина периода М-последовательности. Самый большой недостаток данного метода – это отсутствие математического аппарата, позволяющего получать алгебраические многочлены, порождающие последовательности максимального периода сколь угодно большой степени, к тому же информация о полиномах высокой степени, пригодных для помехоустойчивого кодирования, является исключительно секретной [11].

Известные классы ПСП, как линейных (М-последовательности, последовательности Адамара, Голда, Касами и др.), так и нелинейных (последовательности Лежандра, бент-последовательности и др.), обладают определенными недостатками и не удовлетворяют отдельным из перечисленных выше требований. Определенное решение проблемы дает применение шумоподобных сигналов (ШПС), формируемых нелинейными системами с динамическим хаосом. Такие ШПС, обладая корреляционными свойствами не хуже, чем у М-последовательностей, имеют практически неограниченный набор длин, могут образовывать ансамбли сигналов больших объемов и являются нелинейными, что затрудняет их распознавание в целях последующего воспроизведения.

Все известные динамические системы с небольшим числом степеней свободы, которые обладают динамическим хаосом ("странным аттрактором") – аттрактор Лоренца, Ресслера, системы Чуа, кольцевые системы с запаздыванием и чисто амплитудной нелинейностью – также не обеспечивают корреляционных функций с необходимыми параметрами [12].

Хорошими статистическими свойствами обладают динамические системы, в которых одновременно присутствует и диссипативная (амплитудная) нелинейность, и реактивная (фазовая) нелинейность. В автоколебательных системах с фазовой нелинейностью и задержкой в результате существования нелинейности фазы нарушаются условия баланса фаз, условия синхронизации мод, и в процессе хаотизации колебаний происходит ослабление внутриспектральных связей и более быстрое (по сравнению с другими автостохастическими системами) расщепление корреляций в генерируемом сигнале. Сигналы с хорошими корреляционными свойствами могут быть получены в классе нелинейных кольцевых систем с запаздыванием, в которых одновременно присутствуют и активная (амплитудная), и реактивная (фазовая) нелинейности.

При этом принципиальной особенностью алгоритмов, описывающих систему с динамическим хаосом, является их нелинейность, а особенностью генерируемого временного процесса – его непериодичность.

Системы с хаотической нелинейной динамикой отличаются от традиционных автоколебательных систем, образом которых в фазовом пространстве являются предельные циклы в виде замкнутых непересекающихся кривых на плоскости или многомерных торов в случае большого числа степеней свободы системы. Траектории системы с хаотической динамикой стягиваются в фазовом пространстве не к предельным циклам, а к сложным многомерным поверхностям, которые принято называть "странными аттракторами" и которые являются канторовыми множествами с фрактальной (дробной) размерностью [13].

Динамические системы имеют различные аттракторы, а следовательно, соответствующие им генерируемые процессы и построенные на их основе системы сигналов будут иметь разные свойства [14]. Алгоритмический подход, основанный на использовании явления динамического хаоса, позволит целенаправленно формировать системы шумоподобных сигналов с нужными заданными свойствами.

Применение данного подхода позволяет создать новый класс псевдослучайных последовательностей для применения в радиотехнических системах передачи информации – широкополосных хаотических сигналов, которые в полной мере отвечают всем перечисленным выше требованиям.

Цель данной работы – разработка и исследование свойств псевдослучайных кодирующих сигналов, формируемых порождающими рекуррентными алгоритмами на основе систем с хаотической динамикой, для создания расширяющих функций в широкополосных информационных технологиях Spread Spectrum.

2. ШИРОКОПОЛОСНЫЕ СИГНАЛЫ НА ОСНОВЕ ХАОТИЧЕСКИХ ДИСКРЕТНЫХ АЛГОРИТМОВ С НЕЛИНЕЙНОЙ ДИНАМИКОЙ

В настоящее время наиболее перспективным методом формирования ПСП является использование хаотических алгоритмов, описывающих сложное неравновесное поведение нелинейных динамических систем. Нелинейные динамические системы, генерирующие хаос, обладают чрезвычайно высокой информативностью, позволяющей реализовать в одной и той же аналоговой либо цифровой схеме множество различных типов колебаний с широким спектром.

Для применения в радиотехнических системах предложен новый класс случайных последовательностей, формируемых на основе алгоритмов, описывающих поведение автоколебательных систем с запаздыванием, имеющих режимы динамического хаоса. Особенностью таких систем является их нелинейность и непериодичность генерируемого ими временного процесса. Изменяя параметры такой динамической системы и начальные условия, можно в широких пределах изменять характер ее поведения и тем самым целенаправленно управлять видом и свойствами генерируемого хаотического сигнала.

Предложенные алгоритмы формирования хаотического сигнала моделируют поведение кольцевых автоколебательных систем с запаздывающей обратной связью и сильной амплитудно-фазовой нелинейностью [15]. При циркуляции сигнала по цепи обратной связи нелинейность системы приводит к расширению спектра сигнала. Ширина этого спектра ограничивается фильтрующими свойствами автоколебательной системы. Соотношение между этими двумя конкурирующими факторами – нелинейностью, расширяющей спектр, и фильтрацией, сужающей спектр, – позволяет создавать хаотический сигнал с заданной шириной спектра. Формируемые при этом сигналы относятся к классу широкополосных хаотических сигналов. Схему такой системы можно представить в виде кольца из трех блоков:

$\rightarrow$ (1 нелинейность) $\rightarrow\left[\hat{F}\right]\rightarrow$, (2 задержка) $\rightarrow[T]\rightarrow$, (3 оператор фильтра) $\rightarrow\left[\hat{\Phi}\right]\rightarrow$

Блок-схема такой системы представлена на **Рис. 1**. Механизм автоколебаний в такой системе, сопровождающийся стохастизацией, можно описывать интегральным уравнением, где последовательно учтено действие всех трех указанных функциональных блоков [16]:

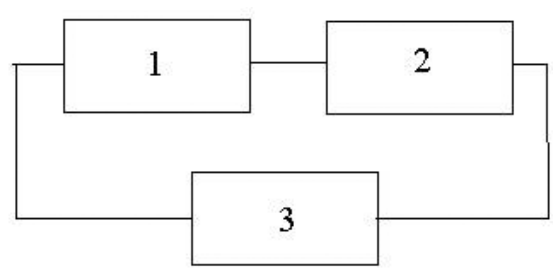

Рис. 1. *Блок-схема нелинейной кольцевой системы с запаздыванием, в которой одновременно присутствуют и активная (амплитудная), и реактивная (фазовая) нелинейности.*

$$\hat{x}(t) = \int_{-\infty}^{\infty} g(t-\tau)\,\hat{F}(\tau - T)d\tau, \quad (1)$$

которое может быть преобразовано к дискретному виду, если ввести прямоугольную фильтрацию сигнала, представить функции g и $\hat{F}$ в виде ортогональных рядов Котельникова и осуществить некоторые преобразования [17]:

$$\hat{x}_k = [1-\exp(-h)]\hat{F}_{k-Nz} + \exp(-h)\hat{x}_{k-1}, \quad (2)$$

где: $x = a\exp(i\varphi)$, a – амплитуда, φ – фаза сигнала, $F_k = F(a_k)\exp\{i[\varphi_k + \Phi(a_k)]\}$, $F(a)$ и $\Phi(a)$ – функции нелинейного преобразования амплитуды и фазы сигнала, h – дискретизация, выбираемая в соответствии с теоремой Котельникова, $N\tau$ – параметр задержки (количество отсчетов на интервале длительности запаздывания).

Вид функций $F(a)$ и $\Phi(a)$ в совокупности со значениями параметров h и $N\tau$ определяет характер формируемого хаотического процесса и его статистические свойства. Нелинейные функции преобразования амплитуды и фазы сигнала $F(a)$ и $\Phi(a)$, определяющие процесс стохастизации колебаний в данной динамической системе, в зависимости от выбора типа нелинейного усилителя могут быть достаточно сложными. Определяющим фактором для получения сигналом нужных статистических свойств является наличие крутого наклона фазовой характеристики по отношению к значению сигнала на входе нелинейного элемента.

Фазовое пространство динамической системы с запаздыванием является n-мерным, где n – число значений, однозначно определяющих поведение системы на каждом следующем шаге. Для системы с запаздыванием размерность фазового пространства определяется числом динамических переменных и длительностью задержки в обратной связи, представленной в дискретном виде.

Особое место среди алгоритмов формирования случайных последовательностей занимают алгоритмы формирования целочисленных последовательностей. Обычно они определяются на конечном множестве целых чисел, что связано с ограничением разрядности, используемым для представления целых чисел в цифровой технике. Преимущество целочисленных последовательностей состоит в том, что они идентично воспроизводятся на различных типах вычислительных устройств и при аппаратной реализации легко воспроизводятся схемотехнически.

При практической реализации нового класса сигналов в цифровой технике связи, которая основана, главным образом, на двоичном коде, имеются две возможности получения бинарных сигналов. Первый способ связан с клиппированием многоуровневых сигналов, полученных в результате расчетов. Этот метод связан с большой потерей информации, заложенной в исходном многоуровневом сигнале, но, к счастью, корреляционные свойства сигналов при этом практически не ухудшаются.

Второй способ представляет собой прямое построение дискретных автоколебательных систем. Алгоритм получения бинарного сигнала в автоколебательной системе имеет вид:

$$\begin{aligned} x_k &= (1-e^{-h})sign[F(x_{k-N})] + e^{-h}x_{k-1}, \\ F(x_k) &= sign[x_k], \end{aligned} \quad (3)$$

Соотношение получено непосредственно из уравнения (2).

На основе математической модели кольцевой автоколебательной системы с сильной амплитудно-фазовой нелинейностью, фильтрацией и запаздыванием разработан и исследован дискретный порождающий алгоритм хаотического сигнала, относящийся к классу алгоритмов реккурентно-параметрического типа с запаздыванием. Форма алгоритма этого класса в общем виде имеет вид дискретного функционального преобразования (отображения) вида

$$x_n = f(x_{n-1}, x_{n-2}, ..., x_{n-Nz}), \quad (4)$$

где x_n и x_{n-1} – соответственно вновь вычисляемые члены формируемой псевдослучайной последовательности на n-ном шаге и предыдущий член этой последовательности на $(n-1)$-м шаге, $N\tau$ – параметр запаздывания, определяющий число членов последовательности на интервале запаздывания $x_{n-1}, x_{n-2}, ..., x_{n-Nz}$, которые полностью определяют новое значение x_n и которые

должны быть заданы в качестве начального условия на первом шаге, а функция $f(x)$ отражает преобразования амплитуды и фазы в порождающей кольцевой автоколебательной системе в режиме хаоса. Алгоритм определен на множестве M целых чисел натурального ряда, принадлежащих замкнутому числовому интервалу $[M_1, M_2]$, $(M_2 > M_1, M = M_2 - M_1 + 1)$, и формирует практически некоррелированную псевдослучайную последовательность целых чисел с распределением вероятностей, близким к равномерному, и корреляционными характеристиками, соответствующими требованиям, предъявляемым к кодирующим сигналам.

Особенностью алгоритмов с запаздыванием является то, что задаваемая им формула отображения может выводить новое значение x_n за область определения алгоритма $[M_1, M_2]$. Поэтому формула алгоритма (4) должна быть дополнена специальной операцией, обеспечивающей возвращение в заданный числовой интервал значение x_m каждого вновь вычисленного члена последовательности в случае, если он оказался вне его границ. Преобразования подобного рода с отображением числового множества «в себя» известны давно. Примером может служить хорошо известное преобразование "пекаря" [18]. Возможны и другие виды преобразований, но среди них следует особо выделить те, которые не вносят существенных изменений в распределение вероятностей генерируемых чисел.

Мощность используемого множества целых чисел значительно меньше мощности континуума непрерывного множества, на котором определена динамическая система. Вследствие этого ограничения в процессе алгоритмического формирования таких последовательностей при увеличении числа их членов имеет место неизбежный выход на цикл, являющийся аналогом предельного цикла динамических систем, определенных на непрерывном числовом множестве. При этом важно, чтобы на интервале до выхода на период повторения, соответствующий этому циклу, реализуемые алгоритмически последовательности имели статистические свойства, близкие к свойствам истинно случайных последовательностей.

Используемый алгоритм с запаздыванием обладает тем свойством, что для однозначного определения всей последующей "траектории" необходимо задание всех N_τ значений на интервале запаздывания. Отсюда следует, что если в последовательности, формируемой алгоритмом, совпадают полностью два неперекрывающихся участка (сегмента) длины N_τ, отстоящие на расстояние L шагов вычисления алгоритма между началами сегментов ($L > N_\tau$), то последовательность будет периодической с периодом $T = L$. Вероятность наступления такого события для алгоритма, заданного на целочисленном интервале [0, 255], порядка обратной величины объема фазового пространства

$P(256, n) \sim 1/(256)n = 3 \cdot 10^{-39}$ при $n = N_\tau = 16$.

Полученный результат можно интерпретировать как оценку возможного периода формируемой алгоритмом последовательности. Величина последнего, таким образом, может составлять $T \approx 10^{38}$ (при $N_\tau = 16$) членов последовательности. Эту оценку следует рассматривать как вероятную величину существования периода в формируемой последовательности при $M = 256$ и $N_\tau = 16$. Отсюда следует, что при увеличении запаздывания N_τ вероятность появления периода в последовательности, формируемой алгоритмом, может быть сделана пренебрежимо малой.

Рассматриваемый алгоритм хаотического сигнала формирует многоуровневый целочисленный сигнал $\{x_n\} \in [0, 255]$. На практике широко используются также системы бинарных сигналов. Такой сигнал можно получить из многоуровневого, используя операцию клипирования.

Наиболее полную информацию о статистических свойствах дискретных последовательностей дает анализ распределений вероятностей чисел $p(x)$ и распределений условных вероятностей $p(i + j,\ x_n / ix_k),\ j = 1, 2, 3, ..., N, n, k = 1, 2, 3, ..., M,$ т.е. вероятности генерации числа x_n на $(i+j)$-том

шаге алгоритма, если на i-том шаге было получено число x_k. При этом областью определения дискретного алгоритма является произвольный замкнутый целочисленный интервал $[M_1, M_2]$, $M = M_2 - M_1 + 1$, $x_n \in [M_1, M_2]$.

Если распределение условных вероятностей при любом j практически совпадает с равномерным распределением, то отсюда следует, что все вероятности перехода $p(i+j, x_n / ix_k) \approx 1/M$, $j = 1,2,3,...$ при произвольном выборе i. В то же время, если распределение вероятностей генерируемых чисел $p(x)$ близко к равномерному, то вероятность значения x_n практически также равна $1/M$. Тем самым вероятности перехода в состояние x_n на j-том шаге совпадают с вероятностью этого значения на этом шаге независимо от значений последовательности на предыдущих шагах алгоритма, что характерно для случайных последовательностей при независимых испытаниях. Более того, формируемая таким алгоритмом псевдослучайная последовательность по своим вероятностным характеристикам будет близка к последовательности независимых равновероятных чисел из интервала $[M_1, M_2]$. В последнем случае можно ожидать, что данная последовательность будет обладать наилучшими статистическими свойствами. Установление подобного факта подчеркивает важность исследования распределений условных вероятностей для априорного суждения о качестве формируемых псевдослучайных последовательностей.

Для характеристики условных распределений $p(x_{i+j}/x_i)$ большое значение имеет вид расположения точек (x_{i+j}, x_i) на плоскости для отображения $x_{i+j} = func(x_i)$, задаваемого дискретным алгоритмом, при соответствующих значениях j = 1, 2, 3,…и i = 1, 2, 3,…N. Получение разброса точек (x_{i+j}, x_i) и визуализация на экране не требует больших вычислительных ресурсов по сравнению с непосредственным вычислением условных вероятностей, и хотя характер этого разброса не дает непосредственно формы распределения условных вероятностей, тем не менее визуализация разброса свидетельствует о степени регулярности этих распределений, наличии функциональных связей, существовании запретных переходов, а то и целых запретных зон, что неизбежно сказывается на корреляционных и других статистических свойствах последовательности.

Было показано, что при соответствующем выборе параметров дискретные алгоритмы с запаздыванием формируют длинные непериодические сегменты псевдослучайных последовательностей с равномерным распределением вероятностей, которые по статистическим и корреляционным параметрам близки к характеристикам случайного равновероятного процесса.

3. СТРУКТУРНАЯ И ФРАКТАЛЬНАЯ СЛОЖНОСТИ ХАОТИЧЕСКИХ ДИСКРЕТНЫХ СИГНАЛОВ

Для эффективной реализации хаотических сигналов в радиотехнических комплексах, телекоммуникационных системах, а также для применения их в качестве информационного носителя в информационных технологиях нового поколения необходимо разработать методы оценки структурной сложности и фрактальной размерности этих сигналов.

С этой целью в настоящей работе анализировались простейшие алгоритмы формирования псевдослучайных последовательностей целых чисел $\{x_n\}$ с запаздыванием, использующие отображение Фибоначчи и его модификации:

Алгоритм Ф-1 $\tilde{x}_n = x_{n-1} + (-1)^{x_{n-Kz}} x_{n-Nz}$ (1)

Алгоритм Ф-2 $\tilde{x}_n = x_{n-1} + (-1)^{x_{n-Nz}} x_{n-Nz}$ (2)

Алгоритм Ф-3 $\tilde{x}_n = x_{n-1} + x_{n-Nz}$ (3)

где $N\tilde{z}$ и $K\tilde{z}$ – параметры алгоритмов, $2 \le K\tilde{z} \le (N\tilde{z} - 1)$. В отличие от работы [6] знак перед запаздывающим членом в Ф-1, Ф-2 изменяется не случайным независимым образом, а определяется внутренней динамикой системы. Параметр обратной связи $N\tilde{z}$ определяет размерность фазового пространства алгоритма и, соответственно, размерность радиус-вектора $R_n(x_{n-1}, x_{n-2}, ..., x_{n-Nz})$ состояния дискретной динамической системы на каждом шаге.

Фазовое пространство (ФП) отображения Фибоначчи размерности N_z не ограничено. Для практического применения алгоритмов ПСП в радиотехнических системах и формирования модулирующих цифровых сигналов конечной разрядности необходимо задать область определения алгоритма на конечном множестве чисел замкнутого интервала натурального ряда [1, M], где $M > 1$. Для этого отображения (1-3) должны быть дополнены операцией преобразования числового интервала [1, M] самого в себя, например, следующего вида:

$$x_n = \tilde{x}_n, \qquad if\ \tilde{x}_n \in [1, M]$$
$$x_n = \tilde{x}_n - M,\ if\ \tilde{x}_n > M$$
$$x_n = \tilde{x}_n + M,\ if\ \tilde{x}_n < 1.$$

Это преобразование, соответствующее свертыванию отрезка [1, M] в кольцо, играет важную роль в механизме хаотического поведения данных динамических систем. Во-первых, эта операция ограничивает объем фазового пространства, делая его конечным, равным $V_{ФП} = M^{N_z}$ точек состояний, а, во-вторых, обеспечивает дополнительное перемешивание траекторий в фазовом пространстве. Необходимо отметить, что одного преобразования числового интервала самого в себя недостаточно для эффективного перемешивания траекторий в фазовом пространстве. Определенный механизм хаотизации должен уже содержаться в функции отображения. В данном случае это обеспечивается свойствами отображения Фибоначчи. Эти два условия – ограниченность объема фазового пространства и наличие мощного механизма перемешивания – являются необходимыми условиями хаотического поведения любой динамической системы.

В качестве альтернативы также рассматривался алгоритм (Ф-4) на основе отображения Фибоначчи (3), но с другой операцией преобразования числового интервала [1, M] самого в себя – типа отражающей границы [19]:

$$x_n = \tilde{x}_n, \qquad if\ \tilde{x}_n \in [1, M]$$
$$x_n = M, \qquad if\ \tilde{x}_n = 2M$$
$$x_n = 2M - \tilde{x}_n,\ if\ M < \tilde{x}_n < 2M.$$

В зависимости от выбора начальных условий радиус-вектор R_n описывает в фазовом пространстве алгоритма траекторию, представляющую собой последовательные дискретные переходы из одной точки состояния динамической системы (ДС) в другую по случайному закону. Эти "траектории" движения дискретной ДС в ФП из-за ограниченности объема ФП образуют замкнутые циклы, которые, вследствие однозначности преобразований, не пересекаются и не имеют общих точек. Кроме того, в ФП могут существовать бассейны циклов и изолированные точки. Так, например, при $N_z = 4$, $K_z = 3$ и $M = 5$ ФП алгоритма Ф-1 имеет три однократных цикла с периодами 526, 27 и 8 и одну изолированную точку, ФП алгоритма Ф-2 содержит один 13-тактный цикл с траекторией бассейна из 611 точек, выходящей на этот цикл, плюс одну изолированную точку, ФП алгоритма Ф-3 состоит из двух циклов с периодом 312 и одной изолированной точки. Спектр периодов алгоритма Ф-4 (в скобках указана кратность цикла): T = 36(1), 15(3), 5(1), 1(1) и 538 точек бассейна циклов.

Циклы алгоритмов Ф-1, Ф-2, Ф-3, Ф-4 имеют важную отличительную особенность: поведение динамической системы до замыкания цикла (равным образом и на траектории бассейна, если он существует) имеет хаотический характер, а порождаемая при этом алгоритмом непериодическая последовательность – псевдослучайного типа. Множество точек в ФП, объединенных в цикл, назовем псевдослучайным циклом (ПСЦ), если формируемый алгоритмом непериодический процесс до замыкания цикла имеет хаотический характер, в отличие от регулярного цикла, которому до замыкания соответствует регулярный процесс. Псевдослучайному циклу соответствует нерегулярное движение в фазовом пространстве, а регулярному циклу – регулярное. Конечно, в том и другом случае поведение динамической системы на цикле полностью детерминировано. Траектория псевдослучайного цикла представляет собой детерминированное множество хаотически следующих одна за другой точек состояний

дискретной динамической системы во всем объеме фазового пространства алгоритма. Аналогом псевдослучайного цикла дискретной системы является странный аттрактор непрерывной динамической системы.

В зависимости от значений параметров $N\chi \geq 3$, $K\chi$ и M в фазовом пространстве алгоритмов Ф-1, Ф-2, Ф-3 существует целый ряд циклов различного периода, из которых каждому длинному ($N \sim V_{\text{ФП}}$) циклу до его замыкания соответствует непериодическая ПСП с практически равномерным распределением генерируемых чисел в заданном интервале области определения $p(x) \cong 1/M$ и с равномерными распределениями условных вероятностей. Лишь для алгоритма Ф-2 в распределениях условных вероятностей $p(i + 1, x_n/i, x_k)$ имеют место запретные переходы для четных, либо нечетных чисел в зависимости от четности числа на предыдущем шаге. Будем рассматривать процессы только до замыкания циклов, т.е. непериодические сегменты формируемой алгоритмом ПСП. Эти сегменты могут быть любой (сколь угодно большой) длины при соответствующем выборе параметров алгоритма и начальных условий. Так у алгоритма Ф-1 при значениях параметров $N\chi = 3$, $M = 63$ длина непериодической ПСП равна $N = 7.8317 \cdot 10^4$ ($N/V_{\text{ФП}} = 0.31$), при $N\chi = 5$, $M = 63$ длина непериодической ПСП равна $N = 3.3174 \cdot 10^8$ ($N/V_{\text{ФП}} = 0.33$), при $N\chi = 7$, $M = 63$ $N = 1.676 \cdot 10^{12}$ ($N/V_{\text{ФП}} = 0.425$), при $N\chi = 9$, $M = 63$ длина непериодической ПСП более $5 \cdot 10^{12}$ шагов алгоритма, в последнем случае объем фазового пространства равен $V_{\text{ФП}} = 1.56 \cdot 10^{16}$. Длинные и сверхдлинные кодирующие последовательности нужны для обеспечения работы сложных навигационных комплексов типа NAVSTAR и ГЛОНАСС.

Для сопоставления в качестве примера ПСП с неравномерной функцией распределения вероятностей генерируемых чисел приводятся результаты исследования алгоритма Ф-4. Показано, что для ПСП, формируемой алгоритмом Ф-4, плотность распределения вероятностей p(x) монотонно спадает к началу интервала области определения [1, M].

Для характеристики фрактальных свойств хаотического множества точек на ПСЦ ограничимся анализом геометрической (эвклидовой) и корреляционной размерностей. Численный эксперимент был проведен для малых значений параметров алгоритмов $N\chi = 4$, $M = 11$, длине исследуемой ПСП из $N = 500$ чисел, что имеет принципиальное значение для оценки мажоритарных свойств псевдослучайных циклов. При увеличении размерности алгоритмов характер поведения дискретной ДС существенно усложняется, а статистические характеристики формируемых ПСП улучшаются.

Оценку корреляционной размерности D_2 исследуемого псевдослучайного цикла можно дать на основе вычисления корреляционного интеграла $C(l)$, заданного на множестве расстояний l между всеми парами векторов состояний на цикле в ФП, построения зависимости $\log_2 C(l) = f(\log_2 l)$, показанной на **Рис. 2**, и определения на ней углового коэффициента прямолинейного участка [20].

Для алгоритма Ф-1 с параметрами $N\chi = 4$, $K\chi = 2$, $M = 11$ корреляционная размерность множества точек на цикле с начальным вектором $R_0(8, 6, 7, 1)$ (кривая 1) равна $D_2 = 3.3$. Полученное значение согласуется с геометрической размерностью $D_0 = 4$, $D_2/D_0 = 0.83$. Величина последнего отношения может

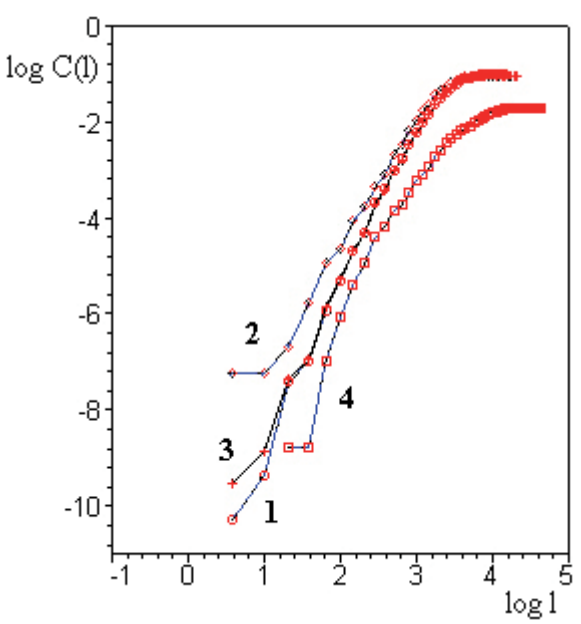

Рис. 2. *Зависимость $\log_2 C(l)$ от $\log_2 l$ для алгоритмов Ф-1, Ф-2, Ф-3 и Ф-4.*

служить характеристикой степени однородности заполнения точками цикла полного объема ФП. Как показал анализ, исследованному циклу с начальным вектором $R_0(8, 6, 7, 1)$ соответствует непериодическая ПСП длиной $N = 14030$ с распределением генерируемых чисел, близким к равномерному.

Линейный участок графика (кривая 2), полученного для множества точек траектории бассейна и цикла в фазовом пространстве алгоритма Ф-2 ($N\tau = 4$, $M = 11$, $R_0(1,1,1,1)$, $N = 500$), имеет несколько меньший наклон, которому отвечает значение корреляционной размерности около $D_2 = 3.0$. Кривая 3 на Рис. 2 соответствует логарифму корреляционного интеграла для псевдослучайного цикла с $R_0(1,6,6,7)$ тестируемого алгоритма Ф-3, $N\tau = 4$, $M = 11$, $N = 500$. Графики 1 и 3 функции $\log_2 C(l) = f(\log_2 l)$ на Рис. 2 почти в точности повторяют друг друга и имеют протяженный прямолинейный участок с наклоном $D_2 = 3.3$, что и позволяет получить количественную оценку однородности заполнения пространства точками состояний ДС на псевдослучайных циклах. Отметим, что алгоритмам Ф-1 и Ф-3 соответствуют ПСП с хорошими статистическими и корреляционными свойствами, особенно при увеличении запаздывания N_z больше 5.

Для цикла алгоритма Ф-4 с параметрами $N\tau = 4$, $M = 17$, длине последовательности $N = 500$, начальный радиус-вектор $R_0(7,14,6,15)$, период $T = 613$, зависимость $\log_2 C(l) = f(\log_2 l)$ (кривая 4 на Рис. 2) не имеет четко выраженного прямолинейного участка. Это означает, что у корреляционного интеграла существенные отклонения от закона $C(l) \sim l^{-D}$ и, следовательно, точки данного псевдослучайного цикла расположены в ФП неравномерно.

Для оценки степени сложности хаотического процесса, формируемого алгоритмом, необходимо определить однородность аттрактора в ФП на всех масштабах дискретного времени. Определение корреляционной размерности аттракторов требует большого объема вычислительных ресурсов особенно в случае ДС высокой размерности, поэтому имеет смысл исследовать структурные свойства реализации псевдослучайного процесса, являющегося проекцией траектории движения ДС в ФП на одно из направлений в этом пространстве.

Фрактальный анализ может быть применен не только к хаотическому множеству точек в многомерном ФП, но и к одномерному множеству чисел реализации ПСП. Определение по стандартной методике корреляционной размерности, примененное к одномерному ($D_0 = 1$) хаотическому массиву из $N = 1000$ чисел ПСП, сформированному алгоритмами Ф-1, Ф-2, Ф-3, Ф-4 при параметрах $N\tau = 16$, $M = 21$ дало следующие результаты. Для всех тестируемых алгоритмов значение корреляционной размерности находится в пределах $D_2 = D_2/D_0 = 0.91 \div 0.96$, в том числе для генератора случайных чисел RND(Maple) ($M = 21$). Полученные значения отношения D_2/D_0 свидетельствует о достаточно хорошей однородности заполнения интервала [1, M] генерируемыми числами. Это подтверждается анализом одномерного распределения вероятностей чисел в последовательности. Но на основе этих данных ничего нельзя сказать о структурной сложности ПСП и, главное, насколько она близка к последовательности независимых случайных событий, что можно рассматривать как эталон хаотического поведения. С этой целью исследуем локальную структуру ПСП на основе анализа фрактальной геометрии.

Случайную последовательность целых чисел можно рассматривать как дискретную топологию сложного геометрического рельефа («береговой линии»). Для оценки геометрической структурной сложности исследуем изменения расстояния последовательно между соседними точками такого рельефа в окне заданного масштаба. Другими словами, на основе данных реализации ПСП длиной N перейдем к анализу алгебраической последовательности

$$\{y_n = |x_n - x_{n-N}|\},\ n = 1, 2, ..., (N-1),$$
$$y_n \in [0,\ (M-1)].$$

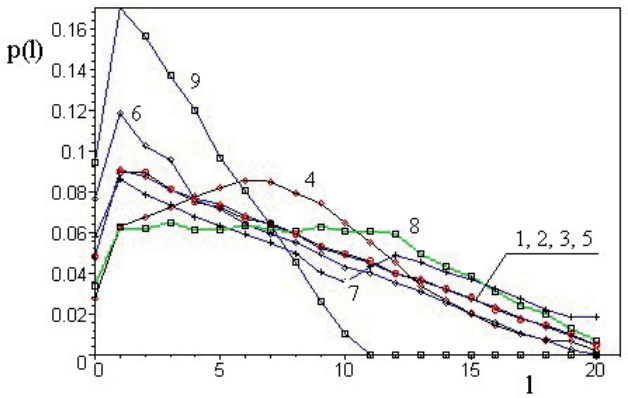

Рис. 3. *Вероятности разностей чисел* $l = |x_n - x_{n+1}|$ *в реализациях последовательностей.*

Следуя методике вычисления корреляционного интеграла, подсчитаем число $N(l)$ наступления одинаковых событий $y_n = l$, $l = 0, 1, 2,\ldots (M-1)$ в последовательности из $(N-1)$ членов и построим график частоты наступления таких событий $p(l) = N(l)/(N-1)$ в зависимости от l (**Рис. 3**).

Расчеты выполнены для ПСП длиной $N = 50000$. Кривая 1 соответствует алгоритму Ф-1 с параметрами $N\chi = 16$, $K\chi = 9$, $M = 21$. Этот график почти в точности повторяет соответствующую теоретическую зависимость для последовательности статистически независимых равновероятных чисел – $p_э(l)$, которая принимается за эталонную. В качестве последней можно использовать и экспериментально полученные значения $p(l)$ для ПСП в случае близости их к теоретическим, например, для ПСП, формируемой генератором случайных чисел RND или алгоритмом Ф-1. Суммарный модуль отклонений значений $p_i = p(l_i)$, полученных для анализируемого процесса, от эталонных – $s = \sum |p_i - p_{эi}|$. Величину $S = 1/(s+1)$ можно принять за меру структурной сложности этого процесса $\{x_n\}$. Кривые 2, 3 и 5, полученные при анализе алгоритмов Ф-2, Ф-3 с той же большой размерностью ФП ($N\chi = 16$, $M = 21$) и генератора случайных чисел RND(Maple) с $M = 21$, также мало отличаются от эталонного графика. Кривая 4 соответствует алгоритму Ф-4 с неравномерным распределением генерируемых чисел $p(x)$.

Графики 6, 7, 8 и 9 построены для модифицированных ПСП алгоритма Ф-1 с целью моделирования дискретных процессов с разным видом функции распределения чисел $p(x)$ (среднее значение $x_{ср}$, среднеквадратичное отклонение σ, коэффициенты асимметрии γ_1 и эксцесса γ_2) и интервала автокорреляции $\tau_{кор}$. Кривые 4, 6, 7, 8 и 9 заметно отличаются от эталонной, что свидетельствует о высокой информативности предложенного метода оценки структурной сложности алгоритмов путем построения графика относительной частоты наблюдения величины разности соседних чисел в реализации ПСП $p(l) = f(l)$. Данный метод не требует больших объемов вычислительных ресурсов по сравнению с методами статистического, корреляционного и фрактального анализа.

В **Таблицу 1** сведены результаты численных экспериментов для всех тестируемых алгоритмов (параметры алгоритмов типа Фибоначчи: $N\chi = 16$, $M = 21$, длина реализаций $N = 50000$).

Из приведенных данных видно, что все три алгоритма Ф-1, Ф-2 и Ф-3 на основе отображения Фибоначчи, так же как и сертифицированный генератор случайных чисел RND, демонстрируют достаточно высокое структурное качество формируемых последовательностей. При изменении функции распределения генерируемых чисел $p(x)$ и коэффициента корреляции предложенная методика оценки степени структурной сложности эффективно фиксирует соответствующее изменение статистических свойств ПСП.

Таблица 1

График на Рис.2	Алгоритм	$p(x)$ тестируемой ПСП				$\tau_{кор}$	Отличие $p(l) = f(l)$ от эталона	
		$x_{ср}$	σ	γ_1	γ_2		s	S
1	Ф-1	10.9	6.07	$1.08\cdot10^{-2}$	-1.21	1	$4.50\cdot10^{-2}$	0.96
2	Ф-2	11.0	6.05	$-1.97\cdot10^{-3}$	-1.20	1	$4.70\cdot10^{-2}$	0.96
3	Ф-3	11.0	6.07	$1.85\cdot10^{-2}$	-1.25	1	$4.80\cdot10^{-2}$	0.96
4	Ф-4	8.29	5.04	-1.21	-0.40	1	0.22	0.82
5	RND	11.0	6.06	$1.0\cdot10^{-3}$	-1.20	1	$4.40\cdot10^{-2}$	0.96
6	Ф-1 модиф.	11.0	5.55	$8.79\cdot10^{-2}$	-1.21	2	$1.85\cdot10^{-1}$	0.85
7	Ф-1 модиф.	11.0	6.81	$-1.02\cdot10^{-2}$	-1.43	1	$2.12\cdot10^{-1}$	0.83
8	Ф-1 модиф.	7.32	5.85	0.86	-0.43	-	$1.46\cdot10^{-2}$	0.87
9	Ф-1 модиф.	11.1	5.26	$-2.14\cdot10^{-2}$	-0.88	10	0.63	0.62

4. СТРУКТУРНАЯ СЛОЖНОСТЬ ХАОТИЧЕСКИХ БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Практически все цифровые радиотехнические системы используют бинарные сигналы. Поэтому достаточно актуальной является проблема сохранения всех особенностей псевдослучайных последовательностей двоичных чисел, получаемых путем клиппирования целочисленных последовательностей, формируемых исследуемыми алгоритмами типа Фибоначчи.

Известно, что вероятность появления блока из k одинаковых символов в случайной бинарной последовательности должна подчиняться закону $p(k) = 1/2^k$. В этом случае данная бинарная последовательность обладает хорошими корреляционными свойствами. Для случайного процесса статистически независимых равновероятных событий этому же закону должна подчиняться вероятность появления любого фрагмента из k двоичных символов (не обязательно одинаковых).

Целью численного эксперимента являлась проверка справедливости данной закономерности для бинарных ПСП, формируемых различными алгоритмами с запаздыванием типа Фибоначчи, и установление на этой основе количественного критерия оценки структурной сложности соответствующей бинарной ПСП.

Поставленная цель реализовывалась путем проверки следующих положений:

- все ли возможные фрагменты двоичного кода длиной k символов присутствуют в реализации ПСП;
- какова вероятность их появления в реализации последовательности в сопоставлении с законом $p(k) = 1/2^k$, справедливым для идеального случайного процесса. Отметим, что именно такую проверку, в частности, предусматривает стандарт шифрования Advanced Encryption Standard (AES), предназначенный для статистического тестирования кодовых последовательностей применяемых для обеспечения конфиденциальности при передаче информации;
- оценка структурной сложности бинарных ПСП, формируемых алгоритмами с запаздыванием типа Фибоначчи.

В численном эксперименте последовательно определялась частота появления в формируемой алгоритмами реализациях из N членов всех возможных фрагментов длиной k из системы полного кода объемом $V(k) = 2^k$, где k = 2, 3, …, 12. Полученные в эксперименте частоты каждого i-того фрагмента полного кода $n_i(k)/N$, i = 1, 2, …, 2^k сопоставлялись с вероятностью $p(k) = 1/2^k$ фрагмента длиной k символов в последовательности независимых равновероятных испытаний. Определялась дисперсия

$$\sigma^2(k) = \frac{1}{2^k}\sum_{i=1}^{2^k}\left(\frac{n_i}{N} - \frac{1}{2^k}\right)^2$$

и среднеквадратичное отклонение от этого уровня $1/2^k$ при заданном значении k. В эксперименте размер анализируемых сегментов полного кода последовательно изменялся от значения k = 2 до k = 12. Длины анализируемых реализаций последовательностей для всех рассмотренных алгоритмов определялись соотношением $N = A \cdot 2^k$, где A выбиралась из соображений обеспечения необходимой статистической представительности выборок. В представленных ниже результатах полагалось A = 100, чтобы в реализации на каждый сегмент полного кода приходилось не менее 100 испытаний.

При численном анализе использовались следующие значения параметров алгоритмов Ф-1, Ф-2, Ф-3, Ф-4: N_Z = 16, M = 255, K_Z = 9. Для сопоставления рассматривались также стандартные генераторы случайных чисел, используемые в различных программных пакетах: Maple7, Mathcad и Pascal.

На **Рис. 4** построены графики среднеквадратичного отклонения частоты появления всех 2^k вариантов сегментов полного кода длиной k от закона $p(k) = 1/2^k$ для алгоритмов Ф-1 (кривая 1), Ф-2 (2), Ф-3 (3), Ф-4 (4), генераторов случайных чисел RND Maple (5), Mathcad (6) и Pascal (7).

Из приведенных на рисунке данных можно заключить, что в последовательностях,

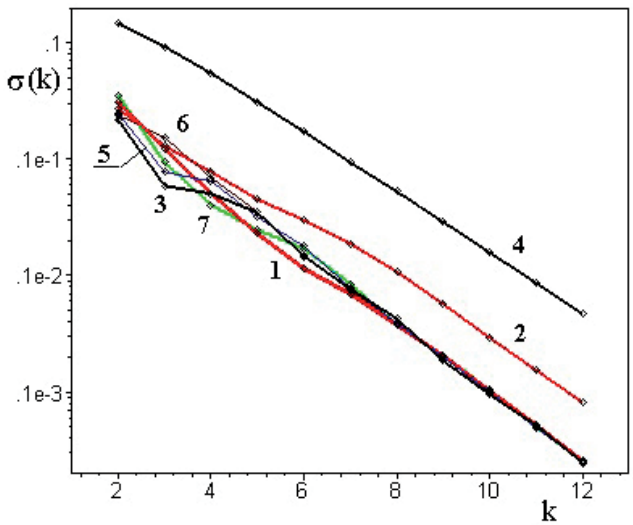

Рис. 4. *Среднеквадратичное отклонение от закона $p(k) = 1/2^k$ вероятностей сегментов полного кода в реализациях бинарных ПСП.*

формируемых алгоритмами Ф-1 и Ф-3, разброс наблюдаемых в эксперименте частот появления сегментов полного кода относительно уровня $p(k) = 1/2^k$ практически совпадает с соответствующими характеристиками последовательностей, генерируемыми датчиками случайных чисел программных пакетов Maple, Mathcad и Pascal.

Всем этим алгоритмам отвечает равномерное распределение вероятностей генерируемых чисел. У алгоритма Ф-2, формирующего целочисленную последовательность с равномерным распределением вероятностей, но с запретными переходами для четных, либо нечетных чисел на одном шаге алгоритма, разброс вероятностей появления фрагментов полного кода в 2-3 раза больше. Неравномерное распределение генерируемых чисел в последовательности, как это имеет место для алгоритма Ф-4, приводит к существенному (на порядок) отклонению от равномерности появления фрагментов полного кода в реализации формируемого двоичного процесса.

На основе полученных в численном эксперименте результатов определяем среднее значение среднеквадратичных отклонений по всем проанализированным системам полного кода ($k = 2, 3, ..., 12$):

$$\sigma_{cp} = \frac{1}{11}\sum_{i=2}^{12}\sigma_i(k).$$

Определим $K_{cc} = 1/(1 + \sigma_{cp})$ как коэффициент, характеризующий структурную сложность ПСП по отношению к сложности чисто случайной бинарной последовательности.

Полученные количественные значения коэффициента K_{cc} для всех анализируемых алгоритмов приведены в **Таблице 2.** Эти данные показывают, что структурная сложность псевдослучайных бинарных последовательностей, сформированных целочисленными алгоритмами с запаздыванием на основе отображений типа Фибоначчи с последующим клипированием, которые имеют практически равномерное распределение вероятностей генерируемых чисел $p(x)$ и близкие к равномерным же распределения условных вероятностей (вероятностей переходов), не отличается существенно от структурной сложности чисто случайных последовательностей. Точно так же как и от сложности последовательностей, генерируемых сертифицированными генераторами случайных чисел.

Алгоритмам с высокой структурной сложностью должны соответствовать корреляционные характеристики, близкие к соответствующим характеристикам случайного процесса. Для всех анализируемых алгоритмов типа Фибоначчи с операцией возврата генерируемых чисел в интервал области определения в Таблице 2 приведены оценки уровня R_{max} боковых выбросов апериодических

Таблица 2

Алгоритм	K_{cc}	$R_{max}\sqrt{N_{cod}}$, АКФ	$R_{max}\sqrt{N_{cod}}$, ВКФ
Ф-1	0.95	1.3-3.6	1.5-4.0
Ф-2	0.94	1.6-3.6	1.6-4.1
Ф-3	0.96	1.14-4.2	1.5-4.6
Ф-4	0.73	2.9-6.9	1.75-5.7
RND Maple (5)	0.96	-	-
RND Mathcad (6)	0.95	-	-
RND Pascal (7)	0.95	-	-
М-последовательность	-	0.7-1.25	1.4-5.0
Сегменты М-последовательности [3]	-	1.45-4.1	-
Случайные последовательности [3]	1.0	2.1-3.5	2.1-3.5

авто- и взаимо- корреляционных функций. В численном эксперименте апериодические корреляционные функции определялись по 100 неперекрывающимся сегментам длиной N_{cod} = 128 (что соответствует стандарту IS-95 для телекоммуникационных CDMA систем), последовательно генерируемых алгоритмами без какого-либо выбора, включая выбор по кодовому балансу. Приведенные уровни боковых выбросов корреляционных функций для сегментов бинарных ПСП, формируемых алгоритмами Ф-1, Ф-2, Ф-3, достаточно хорошо соответствуют боковым выбросам корреляционных функций случайных последовательностей.

Таким образом, структурная сложность последовательностей, формируемых разработанными хаотическими алгоритмами, практически совпадает со сложностью случайных последовательностей. Такие последовательности могут быть использованы в качестве расширяющих сигналов в радиотехнических и навигационных системах с шумоподобными сигналами.

5. ЗАКЛЮЧЕНИЕ

Прикладное применение информационных технологий предполагает физическую реализацию конкретного кодирующего процесса при передаче, обработке и хранении информации в телекоммуникационных системах и компьютерных сетях. В работе рассмотрены перспективные направления использования информационных технологий на основе динамического хаоса для передачи, обработки, хранения и защиты информации. На основе нелинейных систем с хаотической динамикой разработаны конечномерные порождающие математические алгоритмы для синтеза хаотических кодирующих сигналов с повышенной структурной сложностью. Проведен анализ структурной и фрактальной сложности псевдослучайных целочисленных и бинарных последовательностей. Показано, что сложные кодирующие сигналы такого типа обладают высокой информационной емкостью и по статистическим, корреляционным и фрактальным свойствам практически совпадают с параметрами случайных последовательностей и могут эффективно использоваться в различных многопользовательских радиотехнических системах, где требуется высокая помехоустойчивость, защита от несанкционированного доступа и криптостойкость.

ЛИТЕРАТУРА

1. Тузов ГИ. *Помехозащищенность радиосистем со сложными сигналами*. М., Радио и связь, 1985, 264 с.
2. Morsy MA and Alsayyar AS. Performance analysis of OCDMA wireless communication system based on double length modified prime code for security improvement. *IET Communications*, 2020, 14(7):1139-1146. DOI 10.1049/iet-com.2019.0533.
3. Пестряков ВБ, Афанасьев ВП, Гурвич ВЛ, Зайцев ДЛ, Зеликман ЛИ, Пестряков АВ, Сенявский АЛ, Смирнов НИ, Судовцев ВА. *Шумоподобные сигналы в системах передачи информации*. М., Сов. радио, 1973, 424 с.
4. Qi LL, Yao Y and Wu GX. Radar and communication integration based on complete complementary codes. *Journal of Engineering,* 2019, 21:7730-7733, DOI: 10.1049/joe.2019.0754.
5. Belyaev RV, Kalinin VI, Kolesov VV. Formation of a noise-like carrier in spread spectrum communication systems. *Journal of Communications Technology and Electronics,* 2001, 46(2):214.
6. Варакин ЛЕ. *Системы связи с шумоподобными сигналами*. М., Радио и связь, 1979.
7. Shannon CE. A Mathematical Theory of Communication. *Bell System Technical Journal,* 1948, 27(3):379-423.
8. Кнут ВЭ. Искусство программирования. Том 2. Получисленные алгоритмы. М., Мир, 1977, 812 с.
9. Ye Q, Ke PH and Shen J. Linear complexity of a class of pseudorandom sequences over a general finite field. *Soft Computing*, 2018, 22(13):4335-4346, DOI: 10.1007/s00500-017-2870-6.
10. Ипатов ВП. *Периодические дискретные сигналы с оптимальными корреляционными свойствами*. М., Радио и связь, 1992, 152 с.
11. Аграновский АВ, Хади РА. *Практическая криптография*. М., Солон-Пресс, 2002, 256 с.
12. Schuster HG. *Deterministic Chaos: an Introduction*.

Weinheim, Physik-Verlag, 1984, 220 p.

13. Takens F. Detecting Strange Attractors in Turbulence. *Lecture Notes in Mathematics,* Vol. 898, 1981, pp. 366-381; doi:10.1007/BFb0091924.
14. Кузнецов СП. *Динамический хаос.* М., Физматлит, 2001, 296 с.
15. Беляев РВ, Воронцов ГМ, Колесов ВВ. Случайные последовательности, формируемые нелинейным алгоритмом с запаздыванием. *Радиотехника и электроника,* 2000, 45(12):954.
16. Колмогоров АН, Фомин СВ *Элементы теории функций и функционального анализа.* М., Наука, 1972.
17. Котельников ВА. *Теория потенциальной помехоустойчивости.* М., Радио и связь, 1998.
18. Мун Ф. *Хаотические колебания.* М., Мир, 1990, с. 312.
19. Hayes Brian. Computing Science: The Vibonacci Numbers. *American Scientist,* 1999, 87(4):296-301.
20. Пуанкаре А. *О кривых, определяемых дифференциальными уравнениями.* М.-Л., Гостехтеорлит, 1947, 392 с.

Агейкин Никита Алексеевич
аспирант
ИРЭ им. В.А. Котельникова РАН
11/7, ул Моховая, Москва 125009, Россия
E-mail: ageykin_niki@mail.ru.

Грачев Владимир Иванович
научный сотрудник
ИРЭ им. В.А. Котельникова РАН
11/7, ул Моховая, Москва 125009, Россия
E-mail: grachev@cplire.ru

Рябенков Виктор Иванович
к.т.н., с.н.с.
ИРЭ им. В.А. Котельникова РАН
11/7, ул Моховая, Москва 125009, Россия
E-mail: ryabenkov.vi@list.ru

Колесов Владимир Владимирович
к.ф.-м.н., с.н.с.
ИРЭ им. В.А. Котельникова РАН
11/7, ул Моховая, Москва 125009, Россия
E-mail: kvv@cplire.ru.