УДК 621.396

Дискретные кодирующие алгоритмы на основе динамического хаоса для широкополосных информационных технологий

В.В. Колесов, А.И. Полубехин, Е.П.Чигин

Рассмотрены перспективные направления использования информационных технологий на основе динамического хаоса для передачи, обработки, хранения и защиты информации. На основе нелинейных систем с динамическим хаосом разработаны и исследованы дискретные хаотические алгоритмы с высокой информационной ёмкостью. Проведены анализ структурной сложности и исследование статистических и корреляционных характеристик псевдослучайных целочисленных последовательностей. Разработанные хаотические кодирующие алгоритмы могут эффективно использоваться в различных радиотехнических и телекоммуникационных системах, а также в радиолокации и навигации.

Ключевые слова: широкополосные информационные технологии, динамический хаос, хаотические кодирующие алгоритмы, псевдослучайные целочисленные последовательности.

1. Введение

В настоящее время одним из перспективных направлений является применение принципов хаотической динамики при разработке современных широкополосных радиотехнических (телекоммуникационных, радиолокационных, навигационных) систем. Поиск информационных носителей (процессов и сигналов), обладающих повышенной информационной ёмкостью, и математических алгоритмов, порождающих такие процессы, является наиболее актуальной задачей при разработке новых информационных технологий.

Хаотическое поведение систем привлекает конструкторов:

- возможностью получения сложных колебаний простыми по структуре устройствами;
- реализацией в одном устройстве большого числа различных хаотических мод;
- большой информационной ёмкостью;
- разнообразием методов ввода информационного сигнала в хаотическую несущую;
- возможностью синхронизации передатчика и приёмника;
- конфиденциальностью при передаче сообщений и др.

Такое многообразие хаотических проявлений динамических систем послужило причиной различных подходов к использованию хаотических режимов динамических систем в области связи. Важным направлением при этом является разработка на основе хаотической динамики новых классов алгоритмов формирования последовательностей со свойствами случайных процессов [1]. Это открывает возможность разработки новых информационных технологий и создания новых перспективных методов применения сложных хаотических сигналов в телекоммуникационных системах для передачи, обработки, хранения и защиты информации, а также в системах радиолокации и навигации.

Радиолокационное распознавание целей при малых отношениях сигнал/шум является одной из самых сложных задач современной радиолокации. Информация, используемая для распознавания цели, содержится в структуре отражённых радиолокационных сигналов. Многофункциональность и эффективность современных радиолокационных систем может быть обеспечена только разработкой и применением нетрадиционных цифровых алгоритмов и новых адаптивных прикладных решений по обработке сигналов и изображений с целью выделения и распознавания малоконтрастных объектов [2].

В настоящее время, в связи с разработкой цифровых радиолокаторов и широким внедрением широкополосных зондирующих сигналов, интерес к этой проблеме существенно возрос. Повышение точности и разрешающей способности радиолокационных измерений связано с усложнением структуры и расширением полосы частот зондирующего сигнала. Такое расширение может быть достигнуто либо за счёт укорочения зондирующего импульса, либо при использовании шумоподобной несущей. Предельным случаем непрерывного широкополосного зондирующего сигнала является так называемый белый шум с равномерным спектром, т.е. сигнал, имеющий функцию неопределённости 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 приёмного 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.

2. Широкополосные сигналы на основе хаотических дискретных алгоритмов с нелинейной динамикой

Большая информационная ёмкость и повышенная структурная сложность широкополосных сигналов даёт возможность эффективного использования фрактальных адаптивных методов обработки таких сигналов в когерентной и некогерентной радиолокации. Такие сигналы могут формироваться в виде псевдослучайных импульсных последовательностей, которые обладают заданными спектральными и корреляционными характеристиками. В настоящее время в системах связи с расширением спектра используются псевдослучайные последовательности (ПСП) максимального периода, свойства которых хорошо изучены. М-последовательности генерируются простыми алгоритмами и поэтому успешно применяются в разработках различного назначения на протяжении более чем 40 лет. Известные методы формирования псевдослучайных последовательностей обладают определёнными недостатками и не всегда способны удовлетворить в полной мере требованиям, предъявляемым к большой системе сигналов. Так, в семействе последовательностей максимального периода на основе функций Адамара велика вероятность появления пар сегментов ПСП с высоким уровнем взаимной корреляции и большим количеством (достигающем трети длины ПСП) совпадающих символов [3].

В настоящее время наиболее перспективным методом формирования ПСП является использование хаотических алгоритмов, описывающих сложное неравновесное поведение нелинейных динамических систем. Для применения в радиотехнических системах предложен новый класс случайных последовательностей, формируемых на основе алгоритмов, описывающих поведение автоколебательных систем с запаздыванием, имеющих режимы динамического хаоса [4]. Особенностью таких систем является их нелинейность и непериодичность генерируемого ими временно́го процесса. Изменяя параметры такой динамической системы

и начальные условия, можно в широких пределах изменять характер её 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. 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.

3. Дискретные порождающие алгоритмы для формирования хаотических сигналов

Из теории информации известно, что наибольшей информационной ёмкостью обладают стохастические сигналы, порождаемые случайными процессами [5]. Основная проблема при разработке информационных носителей в цифровых телекоммуникационных каналах заключается в трудности генерирования случайных двоичных последовательностей с применением короткого задающего ключа. Требования, предъявляемые к свойствам последовательностей псевдослучайных чисел, зависят от конкретных применений и, как правило, один алгоритм не в состоянии всем этим требованиям удовлетворить [6]. Математические алгоритмы, которые на основе ключа формируют псевдослучайные последовательности (ПСП) числовых значений, должны обладать рядом необходимых свойств:

– *высокое качество*: ПСП по статистическим критериям должна быть близка к случайному процессу и иметь сколь угодно длинный период;

– *эффективность*: алгоритм должен быть быстрым и занимать возможно меньший объём 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*: математическая формула алгоритма должен быть проста в схемотехнической реализации и использовании.

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

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.

Однако попытки приспособить для цифровых алгоритмов шума операции над действительными числами оканчивались неудачами, так как для систем с динамическим хаосом замена действительного числа его приближённым значением сильно меняет статистику получаемой последовательности. Операция округления вносит непредсказуемое возмущение в порождающий алгоритм, и получаемая последовательность перестаёт быть статистически независимой, а значит, и случайной. При этом округлённый алгоритм может вывести после-

довательность на другой аттрактор, что ставит под вопрос воспроизводимость данного процесса на различной вычислительной технике.

Основной метод получения двоичных ПСП в настоящее время – это формирование М-последовательностей (последовательности максимального периода) на основе сдвиговых регистров, когда численное значение 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 – 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 закрытой.

Известные классы ПСП, как линейных (М-последовательности, последовательности Адамара, Голда, Касами и др.), так и нелинейных (последовательности Лежандра, бент-последовательности и др.), обладают определёнными недостатками и не удовлетворяют отдельным из перечисленных выше требований. Альтернативное решение проблемы даёт 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 как двоичных, так и многоуровневых сигналов больших объёмов и являются нелинейными, что затрудняет их распознавание в целях последующего воспроизведения при несанкционированном доступе к кодированной информации.

Все известные динамические системы с небольшим числом степеней свободы, которые обладают динамическим хаосом («странным аттрактором»): аттракторы Лоренца, Рёсслера, системы Чуа, кольцевые системы с запаздыванием и чисто амплитудной нелинейностью – также не обеспечивают корреляционных функций с необходимыми параметрами [7, 8, 9].

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 [10]. Схему такой системы можно представить в виде кольца из трёх блоков (рис.1).

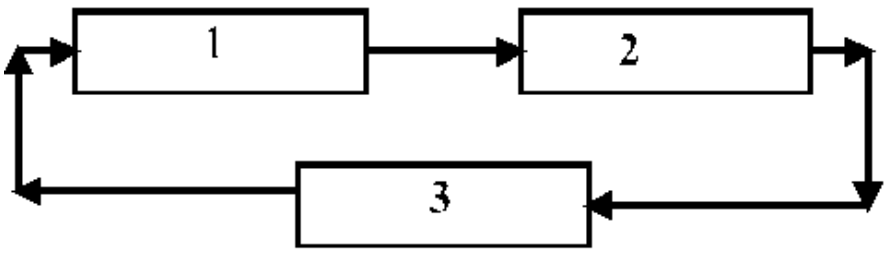

Рис.1. Модель динамической системы с хаотическим поведением:
1 – нелинейный усилитель**;** 2 – линия задержки**;** 3 – фильтр

Механизм автоколебаний в такой системе можно описать комплексным интегральным уравнением, где учтено действие всех функциональных блоков:

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

которое можно преобразовать к дискретному виду:

$$\hat{x}_k = (1-\exp(-h))\cdot \hat{F}_{k-\mathrm{Nz}} + \exp(-h)\cdot \hat{x}_{k-1}\ , \qquad (2)$$

если ввести прямоугольную фильтрацию сигнала, представить функции g и $\hat{F}$ в виде ортогональных рядов Котельникова и осуществить некоторые преобразования

Здесь: $\hat{x}=a\cdot\exp(i\varphi)$, $\hat{F}_k = F(a_k)\cdot\exp\left[\varphi_k + \Phi(a_k)\right]$, Nz – параметр запаздывания, h – шаг дискретизации, выбираемый в соответствии с теоремой Котельникова [11]. Нелинейные функции преобразования амплитуды $F(x)$ и фазы сигнала $\Phi(x)$, определяющие процесс стохастизации колебаний в данной динамической системе, могут быть достаточно сложными. Путём численного анализа на ЭВМ проведён выбор параметров системы с целью получения развитой хаотичности автоколебаний и быстрого спадания автокорреляционной функции сигнала (АКФ).

Вычисление значений взаимной корреляционной функции (ВКФ) показали, что форма ВКФ качественно аналогична виду АКФ, а её наибольшие выбросы имеют тенденцию к снижению при увеличении длительности реализаций по аналогичному закону $\alpha/\sqrt{N}$.

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 клипированием многоуровневых сигналов, полученных в результате расчётов. Как показал численный эксперимент, бинарное квантование многоуровневого сигнала практически не ухудшает его корреляционные свойства.

Второй способ представляет собой прямое построение дискретных автоколебательных систем. Например, алгоритм получения бинарного сигнала в дискретной автоколебательной системе может иметь вид

$$x_k = \mathrm{sign}[F(x_{k-N})] + x_{k-1}. \qquad (3)$$

Это 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 рекуррентно-параметрического типа с запаздыванием. Форма алгоритма этого класса в общем виде имеет вид дискретного функционального преобразования (отображения):

$$x_n = f(x_{n-1}, x_{n-2}, \ldots, x_{n-\mathrm{Nz}}), \qquad (4)$$

где x_n – вновь вычисляемый член формируемой псевдослучайной последовательности на n-ом шаге, N_z – параметр запаздывания, определяющий число членов последовательности на интервале запаздывания $x_{n-1}, x_{n-2}, \ldots, x_{n-\mathrm{Nz}}$, которые полностью определяют новое значение x_n и 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 определён на множестве M целых чисел натурального ряда, принадлежащих замкнутому числовому интервалу [M1, M2], (M2>M1, M=M2-M1+1), и формирует практически некоррелированную псевдослучайную последовательность целых чисел с распределением вероятностей, близким к равномерному.

Особенностью исследуемых алгоритмов является то, что задаваемая ими формула отображения может выводить новое значение x_n за область определения алгоритма [M1, M2]. Поэтому явный вид алгоритма (4) должен быть дополнен специальной операцией, обеспечивающей возвращение в заданный числовой интервал значения x_n каждого вновь вычислен-

ного 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 [12]. Возможны и другие виды преобразований, но среди них следует особо выделить те, которые не вносят существенных изменений в распределение вероятностей генерируемых чисел.

Фазовое пространство (ФП) 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, т.е. 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.

Мощность используемого множества целых чисел значительно меньше мощности континуума непрерывного множества, на котором определена динамическая система. Вследствие ограниченности этого множества в процессе алгоритмического формирования таких последовательностей при увеличении числа их членов имеет место неизбежный выход на цикл, являющийся аналогом предельного цикла динамических систем, определённых 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 генерирования всей последовательности необходимо задание всех Nz значений на интервале запаздывания. Отсюда следует теорема, что если в последовательности, формируемой алгоритмом, совпадают полностью два неперекрывающихся участка (сегмента) длины Nz, отстоящие на расстояние L шагов вычисления алгоритма между началами сегментов (L>Nz), то последовательность будет периодической с периодом T=L. Вероятность наступления такого события для алгоритма, заданного на целочисленном интервале [1,256], порядка обратной величины объема фазового пространства $P(256,n)\sim 1/(256)^n = 3\cdot 10^{-39}$ при n=Nz=16.

Полученный результат можно интерпретировать как оценку возможного периода формируемой алгоритмом последовательности. Таким образом, величина последнего может составлять $T\approx 10^{38}$ (при Nz=16) членов последовательности. Эту оценку следует рассматривать как вероятную величину периода в формируемой последовательности при M=256 и Nz=16. Т.е. при увеличении запаздывания Nz вероятность выхода на период в последовательности, формируемой алгоритмом, может быть сделана пренебрежимо малой. Численное моделирование показывает, что при произвольных значениях M и Nz практически всегда можно найти длинный цикл с периодом $T=(0.3\div 1.0)M^{Nz}$.

Рассматриваемый алгоритм хаотического сигнала формирует многоуровневый целочисленный сигнал $\{x_n\}\in$ [1,256]. 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 даёт анализ распределений вероятностей чисел $p(x)$ и распределений условных вероятностей $p(i+j,x_n \mid i,x_k)$, 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 [M1,M2], M=M2–M1+1, $x_n\in$[M1,M2].

Если распределение условных вероятностей при любом j практически совпадает с равномерным распределением, то отсюда следует, что все вероятности перехода $p(i+j,x_n \mid i,x_k)\approx 1/M$, $j=1,2,3\ldots$ 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 [M1, M2]. В последнем случае можно ожидать, что данная последовательность будет обладать наилучшими статистическими свойствами. Установление подобного факта позволяет выработать оценочный критерий на основе исследования распределений условных вероятностей для априорного суждения о качестве формируемых псевдослучайных последовательностей.

Для характеристики условных распределений $p(x_{i+j} \mid x_i)$ большое значение имеет вид расположения точек (x_{i+j},x_i) на плоскости отображения $x_{i+j}=\mathrm{func}(x_i)$, задаваемого дискретным алгоритмом, при соответствующих значениях $j=1,2,3,\ldots$и $i=1,2,3,\ldots,N$. Получение разброса точек (x_{i+j},x_i) и визуализация паттерна на экране не требует больших вычислительных ресурсов по сравнению с вычислением условных вероятностей, и хотя характер этого разброса не даёт непосредственно формы распределения условных вероятностей, тем не менее, визуализация разброса свидетельствует о степени регулярности этих распределений, о наличии функциональных связей, о существовании запретных переходов и запретных зон.

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 [13].

4. Фазовое пространство цифрового кодирующего алгоритма

Рассмотрим дискретный алгоритм с запаздыванием, формирующий псевдослучайную последовательность с хорошими статистическими свойствами. Основным параметром алгоритма является параметр запаздывания Nz, определяющий число запоминаемых членов последовательности и размерность фазового пространства (ФП). Алгоритм определяется на конечном множестве целых чисел натурального ряда из замкнутого интервала [1, M]. Если вновь вычисленное число последовательности выходит за пределы этого интервала, то осуществляется линейное преобразование сдвига $x_n \rightarrow x_{n\pm M}$, возвращающее это число в границы области определения. Это преобразование помимо функционального действия самого алгоритма играет существенную роль в механизме хаотизации поведения исследуемой динамической системы.

Число точек состояний системы в фазовом пространстве алгоритма конечно и равно M^{Nz}. Движение системы в ФП осуществляется путём перехода скачком из одного состояния в другое. Траектории движения системы занимают весь объём ФП, т.е. все возможные состояния. Каждая такая траектория движения системы происходит по своему замкнутому циклу, содержащему ограниченное число состояний системы. Структура ФП состоит из конечного набора циклов разного периода, поведение системы на которых носит псевдослучайный характер. Все циклы сложным образом располагаются во всем объёме ФП. Так, ФП алгоритма при Nz=4 и M=17 состоит из пяти циклов с периодом 73684, 3619, 2549, 2471, 529 и одной особой точки с координатами (17,17,17,17). Выбор цикла определяется заданием набора начальных условий.

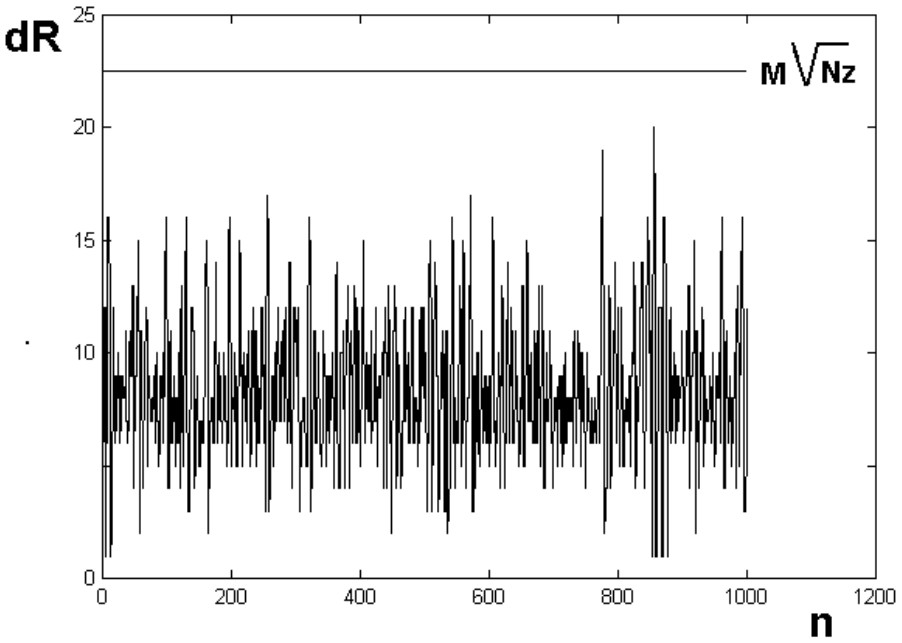

Рис.2. Расстояния в ФП между соседними точками на цикле. Nz=3, M=13

Псевдослучайный характер поведения системы на цикле на интервале, меньшем периода, подтверждается зависимостью изменения расстояний в ФП $\Delta R(n)$ между соседними точками на цикле, приведённой на рис.2 для алгоритма с Nz=3, M=13. Это расстояние на каждом шаге алгоритма изменяется случайным образом, достигая значений, близких к наибольшим геометрическим размерам ФП.

Фазовое пространство исследуемого алгоритма при Nz>2 состоит из одной особой точки с координатами (M,M,…,M) и семейства циклов разного или одного и того же периода. Каждая точка ФП принадлежит только одному конкретному циклу, при этом разные циклы не имеют ни одной общей точки.

Алгоритм выходит на тот или иной цикл в зависимости от выбора вектора начального состояния. До замыкания цикла вектор состояния описывает псевдослучайный процесс, которому соответствует непериодический сегмент формируемой алгоритмом псевдослучайной последовательности соответствующего размера.

Показано, что в ансамбле фазовых пространств алгоритмов с различными параметрами M и Nz наблюдаются как «короткие» циклы, период которых T много меньше по сравнению с полным числом точек фазового пространства M^{Nz} ($T<<M^{Nz}$), так и «длинные» циклы, период которых сопоставим с последней величиной: $T\sim M^{Nz}$. При чётных M в ФП алгоритма преобладают короткие циклы, а при нечётных M коротких циклов вообще не существует, либо они представлены в небольшом количестве, занимая малый объём ФП, что и обеспечивает возможность существования длинного цикла. Тем самым при нечётных M наблюдаются наиболее длинные циклы. Период таких циклов при определённых значениях параметров алгоритма может приближаться к максимально возможной величине $T_{max}=M^{Nz}$.

Численным экспериментом зафиксирован случай, когда ФП содержит только один длинный цикл и одну изолированную точку: M=2, Nz=15, $T/M^{Nz}=1.0$. Близкий результат получен при M=3, Nz=9, когда период длинного цикла $T/M^{Nz}=0.999$, а помимо него и одной изолированной точки в ФП системы существует только один пятитактный короткий цикл. Всё это подтверждает, что оценкой максимального непериодического сегмента формируемой алгоритмом последовательности может служить величина $T_{max}=M^{Nz}$. Следует иметь в виду, что этот максимальный период T_{max} может быть реализован лишь при определённых соотношениях параметров M и Nz.

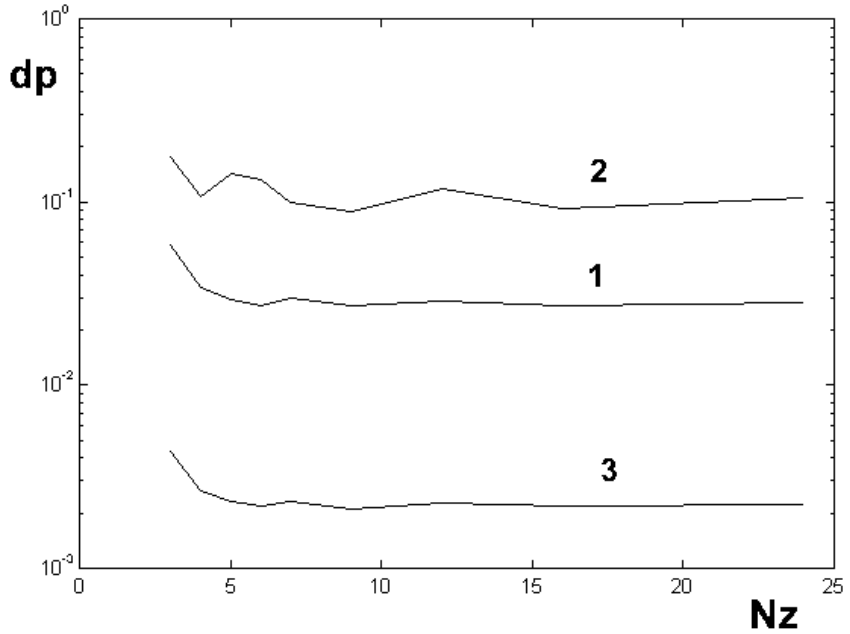

Рис.3. Отличие распределения от равномерного в зависимости от Nz (M=255).
1– $\Delta p_{ср}$, 2 – $\Delta p_{макс}$, 3 – σ

При реализации длинных циклов им соответствуют распределения генерируемых чисел, близкие к равномерному. Характер изменения функций распределения генерируемых чисел при увеличении параметра Nz (для M=255) показан на рис.3. Здесь: $\Delta p_{ср}$, $\Delta p_{макс}$, σ – среднее (1) и максимальное (2) относительные по модулю, среднеквадратичное (3) отклонения распределений от равномерного (n=210000). Видно, что алгоритм формирует последовательность с практически равномерным распределением при Nz>5. В этом случае близки к равномерному распределению и все условные вероятности $p(x_i|x_j)$. Это означает, что формируемая данным алгоритмом псевдослучайная последовательность по своим вероятностным свойствам мало отличается от последовательности независимых равновероятных чисел из интервала [1, M].

Таким образом, показано, что фазовое пространство состоит из конечного числа циклов различного периода, поведение системы на которых носит псевдослучайный характер. При соответствующем выборе параметров дискретный алгоритм формирует длинные непериодические сегменты псевдослучайных последовательностей с равномерным распределением вероятностей, которые могут эффективно использоваться при кодировании информации в телекоммуникационных системах и компьютерных сетях.

5. Структурная сложность хаотических дискретных сигналов

Для эффективной реализации хаотических сигналов в радиотехнических комплексах, телекоммуникационных системах, а также для применения их в качестве информационного носителя в широкополосных информационных технологиях нового поколения необходимо разработать методы оценки структурной сложности [14].

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

Полученные количественные значения коэффициента $K_{сс}$ для некоторых анализируемых алгоритмов приведены в табл. 1. Эти данные показывают, что структурная сложность псевдослучайных бинарных последовательностей, сформированных целочисленными алгорит-

мами с запаздыванием, 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 в пакетах Maple, Mathcad и Pascal.

Таблица 1

Алгоритм	K_{cc}	$\frac{R_{макс}}{\sqrt{N_{cod}}}$, АКФ	$\frac{R_{макс}}{\sqrt{N_{cod}}}$, ВКФ
Алгоритм с запаздыванием	0.96	1.14-4.2	1.5-4.6
RND Maple	0.96	-	-
RND Mathcad	0.95	-	-
RND Pascal	0.95	-	-
М-последовательность [3]	-	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

Алгоритмам с высокой структурной сложностью должны соответствовать корреляционные характеристики, близкие к соответствующим характеристикам случайного процесса. Для всех анализируемых алгоритмов с операцией возврата генерируемых чисел в интервал области определения в табл. 1 приведены оценки уровня $R_{макс}$ боковых выбросов апериодических авто- и взаимокорреляционных функций (АКФ, ВКФ). 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 отбора, в том числе и без отбора по сбалансированности кода. Приведённые уровни боковых выбросов корреляционных функций для сегментов бинарных ПСП, формируемых хаотическим алгоритмом с запаздыванием, достаточно хорошо соответствуют боковым выбросам корреляционных функций случайных последовательностей [3].

6. Хаотический кодирующий алгоритм с двумя параметрами запаздывания

При синтезе кодирующих алгоритмов для цифровых телекоммуникационных систем предъявляется требование достаточно высокой сложности реконструкции явного вида алгоритма по известной реализации генерируемой им кодовой последовательности. Эта задача (криптостойкость) может решаться повышением размерности алгоритма, т.е. в случае алгоритма с запаздыванием

$$x_n = f(x_{n-1}, x_{n-2}, \ldots, x_{n-Nz}, Nz, M) \qquad (5)$$

путём увеличения параметра запаздывания Nz. Увеличение параметра Nz приводит, как правило, и к улучшению статистических характеристик формируемого псевдослучайного процесса и возможности генерации более длинных непериодических сегментов, длина которых растёт в среднем пропорционально M^{Nz} [11].

Для моделирования возможности повышения «сложности» алгоритма не увеличением его размерности, а введением дополнительного параметра запаздывания, и для исследования статистических характеристик генерируемых последовательностей рассмотрим алгоритм:

$$x_n = f(x_{n-1}, x_{n-2}, \ldots x_{n-Nz1}, Nz1, Nz2, M), \quad (6)$$

$1 \le x_n \le M$, $Nz1 > Nz2$ с дополнительным преобразованием сдвига $x_n \rightarrow x_{n \pm M}$, осуществляющем при однократном или двукратном применении возврат текущего числа x_n в интервал области определения. Введение такой дополнительной обратной связи с параметром $Nz2 < Nz1$ не изменяет размерность фазового пространства (ФП), но, как показывает анализ, существенно меняет его структуру – число циклов и их периоды. При этом алгоритм с двумя запаздываниями, так же как и базовый алгоритм с одним запаздыванием, при движении по каждому циклу формирует псевдослучайный процесс. В качестве примера приведём спектры циклов базового и усложнённого алгоритмов, определённых на интервале [1;3], т.е. M=3, при небольшом объёме ФП $M^{Nz} <= 729$ (табл. 1).

У алгоритма с двумя запаздываниями, как и у базового, при нечётных значениях M все циклы – одинарной кратности, а при чётном значении M циклы в фазовом пространстве – короткие и многократные. При этом никакой чёткой закономерности между размерами циклов в фазовых пространствах той и другой систем не просматривается. Спектры циклов алгоритма с двумя запаздываниями Nz1 и Nz2 не содержат циклов алгоритмов с одним запаздыванием Nz=Nz1 и Nz=Nz2, а скорее совпадают со спектрами циклов алгоритма с параметром Nz=(Nz1+Nz2)/2 и добавлением некоторого числа циклов малого периода. При этом вне зависимости от чётности параметра M, как правило, наблюдалась картина существенного уменьшения длины наибольшего цикла.

Таблица 2

Nz=4	44, 29, 7, 1
Nz=5	118, 70, 22, 16, 13, 3, 1
Nz=6	457, 100, 61, 31, 28, 26, 25, 1
Nz1=4, Nz2=3	36, 22, 12, 8, 2, 1
Nz1=5, Nz2=3	200, 25, 12, 5, 1
Nz1=5, Nz2=4	80, 64, 26, 23, 17, 14, 11, 7, 1
Nz1=6, Nz2=4	347, 217, 106, 33, 13, 9, 3, 1

Численное моделирование показало, что порождающий алгоритм при значениях Nz, M и начальных условиях, соответствующих достаточно длинным циклам, формирует псевдослучайную последовательность с распределением вероятностей, близким к равномерному $p(x)=1/M$. Так, при Nz1=16, Nz2=11, M=255 и длине анализируемого сегмента последовательности из N=210000 чисел в эксперименте получено среднее относительное отличие по модулю от равномерного закона $\Delta p_{ср}=0.026$, что соответствует практически равномерному распределению.

В эксперименте уровень боковых выбросов авто- и взаимокорреляционных функций неклипированных и клипированных произвольных сегментов формируемой алгоритмом последовательности не превышал следующих значений: $(1.5 \div 4.0)/\sqrt{N}$ для сегментов с N=128 и $(2.3 \div 4.4)/\sqrt{N}$ для сегментов с N=1024, что согласуется с соответствующим уровнем боковых выбросов корреляционных функций случайных последовательностей. Таким образом, введение в алгоритм дополнительной обратной связи практически не влияет на форму корреляционных зависимостей сегментов генерируемой последовательности.

Блоковая структура клипированной последовательности из 270000 членов для алгоритма с теми же параметрами продемонстрировала близость к закону $p(k)=1/2^k$ вплоть до блоков

размером k=17. Результаты численного анализа представлены на рис.4 в сопоставлении с блоковой структурой последовательности, порождаемой базовым алгоритмом (M=255, Nz=16).

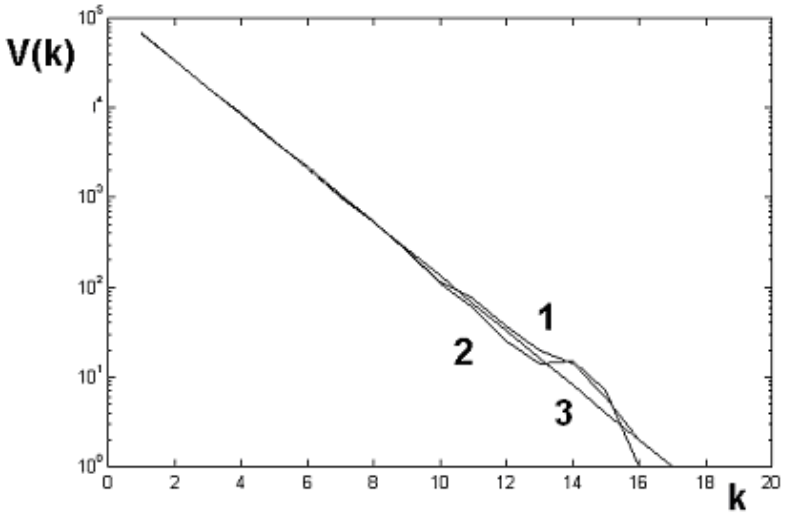

Рис.4. Вероятность появления блоков из k одинаковых символов
в последовательности из 270000 чисел:
для базового алгоритма (1), алгоритма с двумя запаздываниями (2) и $V(k)=1/2^k$(3)

Из рис. 4 видно, что вероятность появления блоков из одинаковых символов полностью совпадает с зависимостью $1/2^k$ вплоть до блока размером k=13 с небольшими отличиями от этого закона для блоков из k=14÷17 символов.

Отбор в систему сигналов кодовых сегментов с заданными корреляционными свойствами показал, что «скорость» такого отбора для алгоритма с двумя запаздываниями может оказаться в 1.5÷2 раза меньше, чем у базового алгоритма. Тем не менее, получаемый объём системы сигнала в обоих случаях оказывается одинаковым.

Таким образом, численным моделированием показано, что порождающий хаотический дискретный алгоритм с двумя параметрами запаздывания имеет хорошую криптостойкость и повышенную сложность при реконструкции явного вида алгоритма по конечной реализации формируемой последовательности. Статистические характеристики псевдослучайных последовательностей, порождаемых разработанным дискретным алгоритмом с двумя параметрами запаздывания, близки к статистическим характеристикам случайного процесса с равномерным распределением вероятностей.

6. Хаотический кодирующий алгоритм на основе двумерного отображения

При разработке дискретных хаотических алгоритмов с повышенной сложностью был предложен и исследовался хаотический кодирующий алгоритм на основе двумерного отображения.

В качестве базового дискретного алгоритма был выбран одномерный алгоритм генератора случайных чисел $x_n=f(x_{n-1},\dots x_{n-Nz},Nz,M)$. Общий вид исследуемого двумерного алгоритма:

$$x_n=f_1(x_{n-1},\dots x_{n-Nz1}, y_{n-1},\dots y_{n-Nz2}, Nz1, Nz2, M), \quad (7)$$
$$y_n=f_2(y_{n-1},\dots y_{n-Nz2}, x_{n-1},\dots x_{n-Nz1}, Nz1, Nz2, M).$$

Область определения алгоритма – замкнутый интервал целых чисел [1, M]. В процессе генерации последовательности при выходе чисел x_n, y_n из интервала [1, M] применялось преобразование возврата $x_n \rightarrow x_{n\pm M}$ и $y_n \rightarrow y_{n\pm M}$.

Фазовое пространство (ФП) алгоритма имеет размерность Nz1+Nz2. Число состояний системы в этом пространстве для алгоритма, определённого на ограниченном дискретном множестве, конечно и равно $M^{Nz1+Nz2}$. Поскольку каждое состояние системы определено на конечном и ограниченном множестве чисел и явный вид алгоритма представляет собой однозначное отображение, то система рано или поздно попадёт в первоначальное состояние и процесс станет периодическим. До выхода на период формируемая последовательность, как показывает численный эксперимент, является псевдослучайной. Появление периода в последовательности $\{x_n\}$, так же как и в последовательности $\{y_n\}$, реализуется в случае одновременного точного повторения полных наборов начальных условий из запаздывающих членов $(x_{n-1},\ldots,x_{n-Nz1})$ и $(y_{n-1},\ldots,y_{n-Nz2})$.

Исследование структуры ФП алгоритма было проведено в доступном для численного анализа диапазоне параметров M, Nz1, Nz2: $M^{Nz1+Nz2} \le 10^6 \div 10^7$. В табл. 3 и 4 приведены результаты исследования структуры ФП алгоритма при нечётном (M=3) и чётном (M=4) значениях параметра M в сопоставлении со спектрами циклов базового одномерного алгоритма с соответствующими значениями параметров, в круглых скобках указано количество циклов одинакового периода.

Таблица 3

Nz=3	18, 8, 1	$M^{Nz} = 27$
Nz=4	44, 29, 7, 1	$M^{Nz} = 81$
Nz=5	118, 70, 22, 16, 13, 3, 1	$M^{Nz} = 243$
Nz=6	457, 100, 61, 31, 28, 26, 25, 1	$M^{Nz} = 729$
Nz1=4, Nz2=3	1258, 351, 270, 88, 26, 1	$M^{Nz1+Nz2} = 2187$
Nz1=5, Nz2=3	3614, 862, 798, 645, 496, 70, 16, 1	$M^{Nz1+Nz2} = 6561$
Nz1=5, Nz2=4	8789, 5677, 2725, 1391, 613, 207, 39, 1	$M^{Nz1+Nz2} = 19683$
Nz1=6, Nz2=4	24844, 23261, 5908, 2781, 400, 1	$M^{Nz1+Nz2} = 59049$

Таблица 4

Nz=3	14(4), 7, 1	$M^{Nz} = 64$
Nz=4	30(8), 15, 1	$M^{Nz} = 256$
Nz=5	42(22), 21, 14(4), 7, 6(2), 3, 1	$M^{Nz} = 1024$
Nz=6	126(32), 63, 1	$M^{Nz} = 4096$
Nz1=4, Nz2=3	186(68), 93, 62(8), 31, 1	$M^{Nz1+Nz2} = 16384$
Nz1=5, Nz2=3	60(544), 30(8), 15, 1	$M^{Nz1+Nz2} = 65536$
Nz1=5, Nz2=4	465(412), 31(3), 1	$M^{Nz1+Nz2} = 262144$
Nz1=6, Nz2=4	84(1149), 42(43), 21, 14(4), 1	$M^{Nz1+Nz2} = 1048576$

ФП исследуемого алгоритма состоит из набора циклов разной кратности и длины и одной особой изолированной точки с координатами (M, M,…, M). Из табл. 3 видно, что при нечётных M все циклы имеют одинарную кратность, точно также как и в ФП базового алго-

ритма. При этом явная закономерность между размерами циклов в ФП сопоставляемых алгоритмов не просматривается. Размер наибольшего цикла составляет ~0.5 от полного числа состояний в фазовом пространстве $M^{Nz1+Nz2}$.

При чётных значениях M (табл. 4) циклы в ФП, как правило, короткие и многократные, как и в случае базового алгоритма. Спектры циклов двумерного алгоритма с параметрами Nz1 и Nz2 не содержат циклов парциальных базовых алгоритмов с Nz=Nz1 и Nz=Nz2, но имеют циклы базового алгоритма с Nz=(Nz1+Nz2)/2 с добавлением циклов удвоенного периода. При этом основные периоды циклов двумерного алгоритма отличаются в целое число раз от фундаментального периода в каждой из серий циклов: например, при Nz1=4, Nz2=3 спектр циклов – 31 (фундаментальный период), 62, 93, 186. Такой характер спектра циклов свойственен и одномерному алгоритму при чётных значениях M.

Из табл. 4 видно, что размер циклов наибольшей длины двумерного алгоритма почти на два порядка превышает размер цикла соответствующего одномерного алгоритма при Nz1=Nz. Но этот выигрыш обусловлен не столько специфическими особенностями двумерного отображения по сравнению с одномерным аналогом, сколько реальным увеличением размерности ФП. Соотношение между длиной цикла максимального размера и полным числом состояний в ФП остаётся прежним ~ 0.5.

Как показал предварительный анализ, оценку статистических характеристик надо проводить не при малых, а при реальных, т.е. относительно больших значениях параметров, соответствующих развитому хаосу и формированию длинных псевдослучайных последовательностей с хорошими корреляционными свойствами. Поэтому оценочные расчёты выполнены при параметрах M=255, Nz1=16, Nz2=11. Показано, что двумерный алгоритм формирует псевдослучайную последовательность с практически равномерным распределением вероятностей $p(x)=1/M$. Для сегмента последовательности с N=210000 отличие от этого распределения составляет: относительное среднее отличие по модулю $\Delta p_{ср}=0.028$ при максимальном $\Delta p_{макс} = 0.10$, среднеквадратичное $\sigma = 0.002$.

Оценка корреляционных характеристик формируемых последовательностей проводилась на основе анализа неклипированных и клипированных 100 пар сегментов размером в 128 и 1024 символа, последовательно генерируемых алгоритмом без какого-либо отбора, в том числе и без отбора по сбалансированности кодов. Получено, что уровень выбросов авто- и взаимокорреляционных функций не превышал следующих значений: $(1.5\div4.8)/\sqrt{N}$ для сегментов с N=128 и $(2.5\div4.9)/\sqrt{N}$ для сегментов с N=1024, что согласуется с соответствующим уровнем боковых выбросов корреляционных функций как чисто случайных последовательностей с равномерным распределением, так и последовательностей, генерируемых базовым алгоритмом.

Подсчёт блоков из одинаковых символов на реализации клипированной последовательности из 270000 чисел показал, что вероятность появления таких блоков полностью подчиняется закону $p(k)=1/2^k$ вплоть до блока размером k=12 с несущественными отличиями от этого закона для блоков из k = 13÷18 символов. Последние отличия обусловлены скорее недостаточностью данных для статистической обработки результатов, чем свойствами самих алгоритмов.

Оценка объёма системы сигналов, формируемых двумерным и базовым алгоритмами, производилась отбором из сформированной клипированной последовательности сбалансированных кодов с заданными корреляционными свойствами. Показано, что при одинаковых длинах реализации последовательности число отбираемых кодов и скорость их отбора близки для обоих сопоставляемых алгоритмов.

В результате анализа структуры фазового пространства двумерного алгоритма найден спектр периодов циклических траекторий в ФП, различающихся начальными условиями. Установлено, что статистические свойства псевдослучайных последовательностей, формируемых базовым дискретным алгоритмом и алгоритмом с двумерным отображением, при сопоставимых параметрах близки. Однако при этом двумерный алгоритм имеет повышенную

сложность, что значительно затрудняет его криптоаналитическую реконструкцию по реализации, сформированной алгоритмом последовательности. Таким образом, структурная сложность последовательностей, формируемых разработанными хаотическими алгоритмами, практически совпадает со сложностью случайных последовательностей.

7. Заключение

На основе нелинейных систем с хаотической динамикой разработаны дискретные хаотические алгоритмы для генерации псевдослучайных последовательностей. Исследованы статистические и корреляционные характеристики псевдослучайных дискретных кодирующих сигналов, обладающих повышенной структурной сложностью и криптостойкостью.

Численным моделированием исследована структура фазового пространства дискретного кодирующего алгоритма с запаздыванием, заданного на замкнутом интервале целых чисел. Установлено, что фазовое пространство состоит из конечного числа циклов различного периода, поведение системы на которых носит псевдослучайный характер. Показано, что при соответствующем выборе параметров дискретный алгоритм формирует длинные непериодические сегменты псевдослучайных последовательностей с равномерным распределением вероятностей, которые могут эффективно использоваться при кодировании информации в телекоммуникационных системах и компьютерных сетях.

Показано, что на основе конечномерных алгоритмов с нелинейной динамикой может быть сконструирован большой ансамбль квазиортогональных хаотических бинарных кодов, что позволяет практически осуществить эффективное кодовое разделение большого числа пользователей, работающих в общей полосе частот.

Для повышения структурной сложности и криптостойкости сигналов предложены методы модификации разработанных порождающих алгоритмов, что заметно увеличивает объём системы кодов.

Таким образом, сложные шумоподобные сигналы такого типа обладают высокой информационной ёмкостью, структурной сложностью, криптостойкостью и могут быть эффективно использованы в качестве расширяющих и кодирующих сигналов в различных широкополосных радиотехнических системах с высокой степенью скрытности, в том числе телекоммуникационных системах, а также в радиолокации и навигации.

Статья поступила в редакцию 10.03.2015

Литература

1. *Гуляев Ю.В., Кислов В.Я., Кислов В.В.* Докл. РАН, 1998, Т.359, №6, С.750.
2. *Потапов А.А.* «Фракталы в радиофизике и радиолокации» – М.: Логос, 2002. С.664.
3. *Варакин Л.Е.* «Системы связи с шумоподобными сигналами» – М.: Радио и связь. 1985.
4. *Беляев Р.В., Воронцов Г.М., Колесов В.В.* «Случайные последовательности, формируемые нелинейным алгоритмом с запаздыванием», Радиотехника и электроника, 2000, т. 45, №12, с.954-960.
5. *Shannon. C.E*. A Mathematical Theory of Communication // Bell System Techn. J., 1948. V.27, N 3, P.379-423.
6. *Kolesov V.V., Belyaev R.V., Vorontsov G.M., Popov A.M., Ryabenkov V.I.* The complex chaotic discrete signals in systems of radiolocation and navigation, XI Int. scientific-research conference «Radiolocation, navigation, communications», Voronezh, Russia, 12-14 April 2005, Proceedings, P. 292-307.

7. *Lorenz E. N.* Deterministic Nonperiodic Flow, J. Atoms. Sci., 1963, V.20, PP.130-141.
8. *Ressler O.E.* «Chemical Turbulence: Chaos in a Small Reaction-Diffusion System», Z. Naturforsch., 1976, V. 31, PP.168-172.
9. *Chua L.O., Komuro M., Matsumoto T.* «The Double Scroll Family», IEEE Transactions on Circuits & Systems,1986, vol.CAS-33, no.11, pp.1073-1118.
10. *Беляев Р.В., Воронцов Г.М., Кислов В.Я., Колесов В.В., Крупенин С.В., Попов А.М., Рябенков В.И.* Сложные хаотические дискретные сигналы в системах телекоммуникации, радиолокации и навигации, Радиотехника и электроника, 2006, т.51, № 9. С. 1116-1128.
11. *Котельников В.А.* Теория потенциальной помехоустойчивости. М.: Радио и связь,1998.
12. *Шустер Г.* Детерминированный хаос. Введение. -М.: Мир, 1988, 240с.
13. *Беляев Р.В., Воронцов Г.М., Кислов В.В., Колесов В.В., Попов А.М., Рябенков В.И.* Спектр периодов псевдослучайных последовательностей, формируемых алгоритмом с задержкой, Радиотехника и электроника, 2004, Т.49, № 3, С. 325-332.
14. *Колесов В.В.* Оценка структурной сложности псевдослучайной последовательности целых чисел, 7-я Международная конференция и выставка «Цифровая обработка сигналов и её применение», 16-18 марта 2005 г., Москва, Россия, Доклады-1, с. 3-7.

Колесов Владимир Владимирович
к.ф.-м.н., заведующий лабораторией ФГБУН Института радиотехники и электроники им. В.А. Котельникова РАН (125009, г. Москва, ул. Моховая, д. 11, стр. 7), тел. 8(495) 6293368, e-mail: kvv@cplire.ru

Полубехин Александр Иванович
к.т.н., руководитель инновационного технологического центра МГТУ им. Н.Э. Баумана (105005, г. Москва, 2-я Бауманская ул., д. 5, стр. 1), тел. 8(499) 2636846, e-mail: polub1980@mail.ru

Чигин Евгений Павлович
к.ф.-м.н., ведущий научный сотрудник ИРЭ РАН ученый секретарь Научного совета РАН по проблеме «Физическая электроника», тел.: 8(495) 6293368, e-mail: ire@cplire.ru

The discrete coding algorithms on the basis of dynamic chaos for the broadband information technologies

Vladimir V. Kolesov, Alexander I. Polubekhin, Eugene P. Chigin

Promising areas of application of information technologies on the basis of dynamic chaos for transmission, processing, storage and information security are considered. On the basis of the nonlinear systems with dynamic chaos, discrete chaotic algorithms with a high information capacity are developed and investigated. The analysis of structural complexity as well as statistical and correlated characteristics of the pseudorandom integer sequences is carried out. The developed coding chaotic algorithms can be effectively used in various radio engineering and telecommunication systems as well as in a radiolocation and navigation.

Keywords: broadband information technologies, dynamic chaos, the chaotic coding algorithms, pseudorandom integer sequences.