*УДК 004.056*

# ГЕНЕРАЦИЯ И ОБРАБОТКА ХАОТИЧЕСКИХ СИГНАЛОВ НА ОСНОВЕ ТРЕХМЕРНЫХ ФУНКЦИЙ В ПРОСТРАНСТВЕ СОСТОЯНИЙ

В.А. ЧЕРДЫНЦЕВ, С.И. ПОЛОВЕНЯ, В.В. ДУБРОВСКИЙ

*Белорусский государственный университет информатики и радиоэлектроники*
*П. Бровки, 6, Минск, 220013, Беларусь*

*Поступила в редакцию 14 февраля 2014*

Рассмотрен новый класс хаотических генераторов, хаотический процесс в которых формируется на основе распределенных во времени отображений. Приведены алгоритмы и структурные схемы устройств формирования, информационной модуляции и обработки сигнала. Численным моделированием системы получено семейство кривых помехоустойчивости для различных условий работы генератора хаотических процессов.

*Ключевые слова:* хаос-процесс, нелинейная формирующая функция, помехоустойчивость.

## Введение

Случайно-подобные, или хаотические, последовательности обладают множеством уникальных свойств и особенностей. Например, в отличие от всех известных на данный момент последовательностей они непериодичны, а значит, имеют сплошной спектр. Нелинейные системы, формирующие хаотические сигналы, допускают множество подходов к осуществлению информационной модуляции в отличие, например, от модуляции гармонического колебания, где управлению можно подвергать лишь три параметра: амплитуду, частоту и начальную фазу. Сложность фазовых траекторий хаотических сигналов делает передачу информации скрытной [1]. Такого рода сигналы можно использовать в качестве переносчиков информации в любых существующих системах телекоммуникаций, но выгоднее всего использовать их в системах передачи информации с повышенной защитой от несанкционированного доступа [2].

## Постановка задачи

Формирователь хаоса представляет собой усилитель, охваченный обратной связью с существенно нелинейной амплитудной характеристикой. Формирователь дискретных во времени хаотических сигналов есть некоторый сигнальный процессор, в котором на основе нелинейной функции рекуррентно вычисляются отсчеты процесса. В случае составных отображений формирователь представляет собой систему связанных между собой усилителей с нелинейной обратной связью. Это существенно усложняет характер отображения и структуру фазовых траекторий.

Системы передачи информации с использованием хаос-сигналов, как правило, имеют более низкую помехоустойчивость в сравнении с классическими системами. Это есть своего рода плата за все достоинства, присущие хаос-сигналам. Тем не менее, в статье предложен эффективный подход к повышению помехоустойчивости за счет распределения отображения хаотического процесса во времени.

Особенностью предлагаемых алгоритмов генерации хаос-процессов (ХП) является то, что в них не существует строго определенной нелинейной формирующей функции (НФФ). В рассматриваемом случае один или несколько параметров НФФ изменяются хаотическим

образом на каждом такте генерации. Главная цель, достигаемая при реализации алгоритмов, – это относительно малое приращение формирующей функции при внесении значительного возмущения ее аргумента с сохранением высокой степени стохастизации колебательного процесса. В результате помехоустойчивость системы существенно возрастает, но при этом сохраняется «хаотизация», или стохастизация колебаний. Это также означает, что система обладает структурной скрытностью. Как следствие, ни методом прямого перебора, ни методом статистического анализа, невозможно «вскрыть» систему и извлечь информацию без знания: 1) структуры генератора; 2) знания точной аналитической записи нелинейных формирующих функций.

**Алгоритмы формирования и обработки**

Алгоритм формирования в общем виде описывается системой уравнений:

$$\begin{cases} h'_k = p_{0,k} + \alpha p_{1,k} h_{k-1} + \alpha p_{2,k} h_{k-1} + \dots \\ \dots + \alpha p_{N,k} h_{k-N} = \mathrm{p}_{0,k} + \alpha \sum_{i=1}^{N} p_{i,k} h_{k-i}; \\ h_k = F(h'_k); \\ p_{0,k} = f_{p0}(p_{0,k-1}); \\ p_{1,k} = f_{p1}(p_{1,k-1}); \\ p_{2,k} = f_{p2}(p_{2,k-1}); \\ \quad \dots \\ p_{N,k} = f_{pN}(p_{N,k-1}). \end{cases}$$

Для системы передачи информации (СПИ) фазовые траектории имеют два важнейших свойства: экспоненциальную расходимость фазовых траекторий и перемешивание. Указанные свойства обеспечивают высокую алгоритмическую сложность динамических процессов, описывающих данные траектории и данные динамические системы

Подбирая параметры системы, можно добиться того, что такие колебательные процессы по своим статистическим характеристикам не будут отличаться от реализаций шумового процесса. При этом имеется детерминированное уравнение или алгоритм, по которому, задав начальные условия, можно полностью рассчитать хаотический процесс и воспроизвести его как эталон любое число раз.

Алгоритм формирования и реализация хаос-генератора основаны на аналогичном подходе, осуществляемом в ПК при моделировании, т. е. используют дискретное время и квантованные по уровню величины. Источники нелинейно формируемых последовательнсотей (НФП) могут быть построены на дискретных логических элементах или БИС, выполняющих роль сборок дискретных элементов (программируемые логические матрицы, FPGA – field programmable gate array, CPLD – complex programmable logic devices), универсальных микропроцессорных комплектах, а также на специализированных микропроцессорных комплектах – сигнальных процессорах.

Нелинейное подмешивание информации задается следующей системой уравнений:

$$\begin{cases} p_{0,k} = f_{p0}(p_{0,k-1}); \; p_{1,k} = f_{p1}(p_{1,k-1}); \\ p_{2,k} = f_{p2}(p_{2,k-1}); \; \dots; \; p_{N,k} = f_{pN}(p_{\mathrm{N},k-1}); \\ h'_k = p_{0,k} + \alpha p_{1,k} h_{k-1} + \alpha p_{2,k} h_{k-2} + \dots + \alpha p_{N,k} h_{k-N} = p_{0,k} + \alpha \sum_{i=1}^{N} p_{i,k} h_{k-i}; \\ h_k = (1-\gamma) F(h'_k) + \gamma \lambda_k; \; \lambda_k = \pm 1. \end{cases}$$

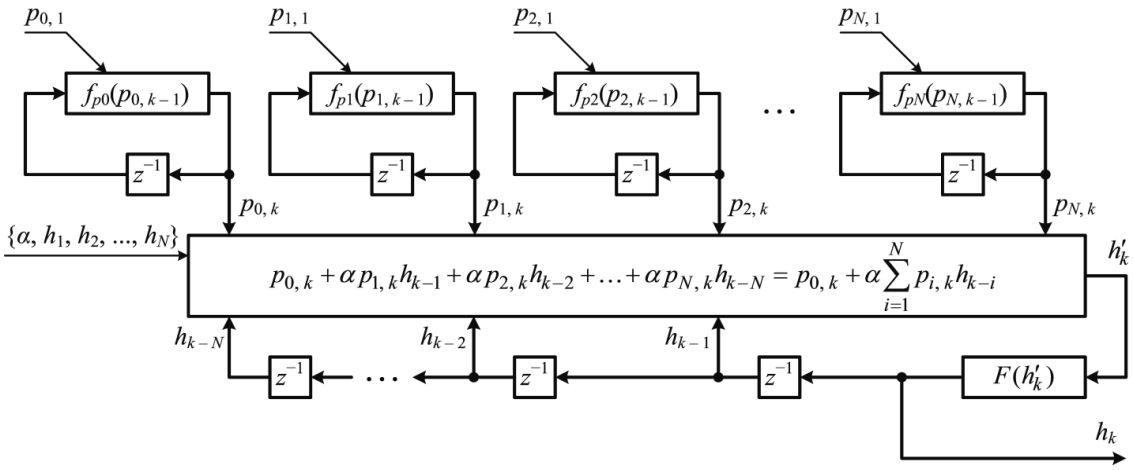


Рис. 1. Структурная схема генерации ХП

На рисунках ниже приведены некоторые результаты численного моделирования: фрагмент реализации процесса и его отображение. Исследование проводилось на 15 парах функций. Моделирование показало, что при формировании ХП на основе связанных функций отображение практически полностью размыто по пространству состояний. Этот факт подтверждает запутанность фазовых траекторий, что является положительным фактом с точки зрения структурной скрытности сигнала. В таком случае наблюдение достаточно длительной реализации хаотического сигнала делает невозможным воссоздание исходной нелинейной формирующей функции.

Аналитическая оценка качественных показателей систем формирования и обработки хаотических сигналов – задача исключительно трудоемкая и зачастую невозможная. Поэтому единственным способом проверки работоспособности предлагаемых алгоритмов и их оптимизации является численное моделирование.

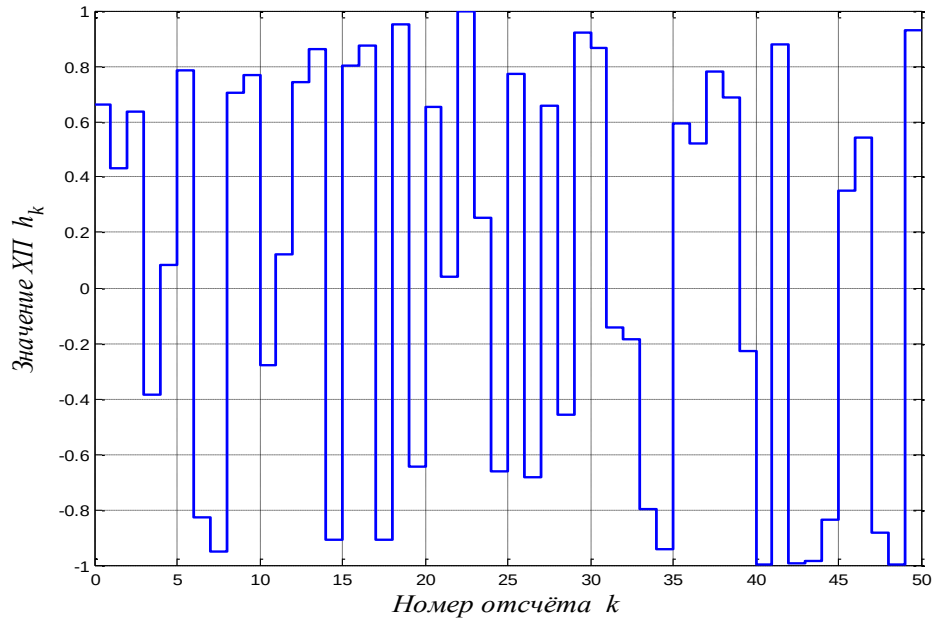


Рис. 2. Фрагмент реализации хаотического сигнала

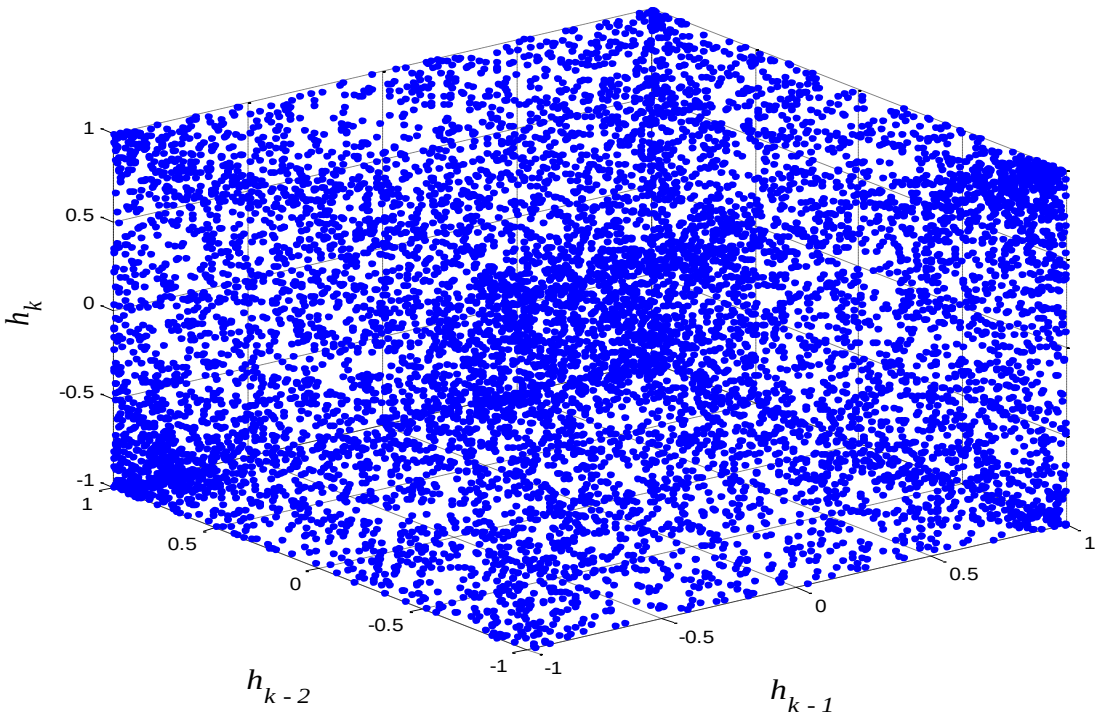


Рис. 3. Отображение хаотического сигнала

**Численное моделирование и оценка помехоустойчивости**

Сущность моделирования состоит в том, что к хаотическому сигналу добавлялся шум, полоса частот которого соответствовала полосе частот, занимаемых хаос-сигналом. В результате строились зависимости вероятности ошибки различения дискретного параметра от отношения сигнал/шум на входе устройства приема и обработки. Такие измерения проводились при различных параметрах НФФ, т.е. строилось семейство кривых помехоустойчивости.

Исследования проводились на статистике объемом 100 тыс. отсчетов хаотического процесса. Ниже приведены результаты исследования для формирующих функций:

$$\begin{cases} h'_k = p_{0,k} + 0{,}1 p_{1,k} h_{k-1} + 0{,}1 p_{2,k} h_{k-2}; \\ h_k = F(h'_k); \\ p_{0,k} = F\left\{80(p_{0,k-1} - 0{,}7)^2 - 0{,}8\right\}; \\ p_{1,k} = F\left\{10(p_{1,k-1} - 0{,}3)^2 - 0{,}8\right\}; \\ p_{2,k} = F\left\{20(p_{2,k-1} + 0{,}6)^3 + 0{,}6\right\}. \end{cases}$$

Следует отметить, что в случае нелинейного подмешивания информационный сигнал представлял собой последовательность значений $\lambda_k = \pm 1$. Это было сделано для сопоставимости результатов моделирования двух методов хаотической модуляции.

Семейство кривых помехоустойчивости при $\alpha = 1$ приведено на рис. 5 (кривая 1 снималась при $\gamma = 0{,}1$, кривая 2 – $\gamma = 0{,}2$, кривая 3 – $\gamma = 0{,}4$).

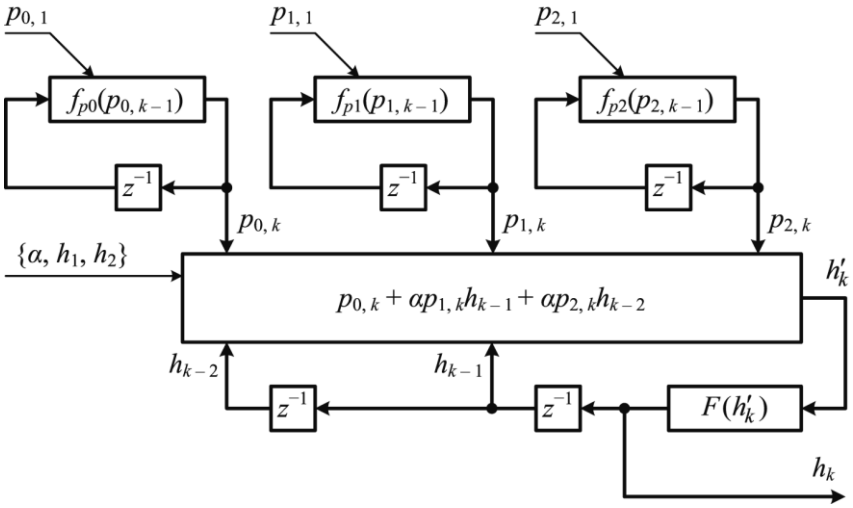


Рис. 4. Структурная схема генерации ХП

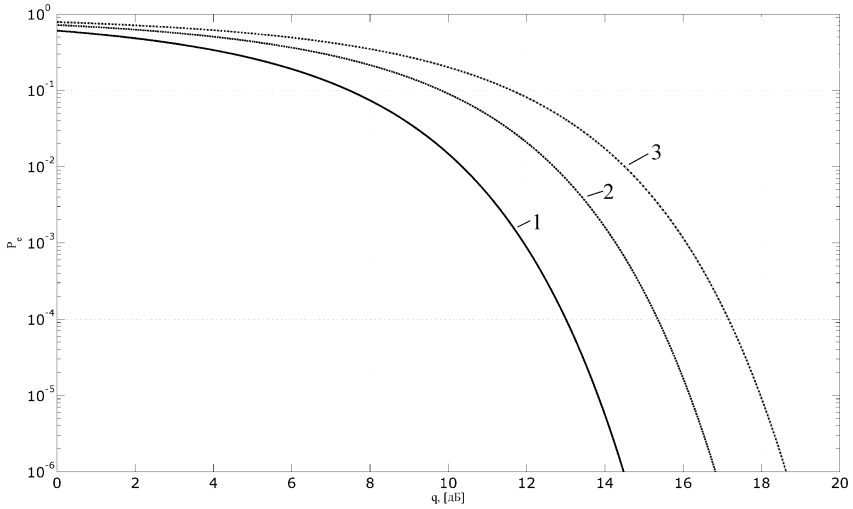


Рис. 5. Семейство кривых помехоустойчивости

**Оценка степени защиты информации в системах с распределенными отображениями**

В настоящее время микроконтроллеры, имеющиеся в продаже, имеют разрядность АЛУ не менее 12 бит с количеством общедоступных регистров от 16 до 256 и выше. Фактически эти регистры являются сверхоперативной памятью.

Функция $F(...)$ на рис. 1 в виде полинома с изменяющимися во времени коэффициентами (блок в центре схемы) определяет помехоустойчивость; вспомогательные функции, реализующие формирование последовательности коэффициентов полинома, определяют стохастизацию колебаний. На указанные функции, в силу того, что они не влияют на помехоустойчивость системы, никакие условия не налагаются, т.е. они могут быть совершенно произвольными.

Положим, что функция $F$ однозначно определяется 10 коэффициентами. Это значит, что суммарный объем «пространства параметров» составляет 120 бит. В других работах на примере многочисленных функций показано, что хаос восстановим в течение 4–5 тактов, если ошибка в параметре нелинейной формирующей функции (НФФ) не превышает 3–5 %. Это значит, что взломщик сигнальной конструкции при грубой атаке имеет возможность «ошибиться» в единственном последнем бите параметра НФФ [2]. Таким образом, объем пространства параметров, который необходимо «перебрать» для вскрытия системы, снижается до 120–12 = 108 бит. Отсюда находим количество возможных вариантов: $2^{108} = 3{,}25 \times 10^{32}$.

Если предположить, что недоброжелатель зафиксировал весь сеанс связи и имеет

возможность перебирать 1 млрд. вариантов в секунду, то получается, что на взлом сигнально-кодовой конструкции и извлечение информации ему потребуется порядка $3{,}76\times10^{18}$ суток или $1{,}03\times10^{16}$ лет. Знание начальных условий для вспомогательных генераторов (генераторов параметров) фактически составляет ключ и в нашем примере он равен 120 битам. Эффективный объем ключа, как было показано, в реальных системах составляет порядка 100–110 бит. Алгоритм обладает исключительно высокой в сравнении с известными хаотическими системами помехоустойчивостью, составляющей величину порядка 12–18 дБ. Схема реализуема на простейших контроллерах, в т.ч. и на устаревших 8-битных, даже в отсутствие внешнего оперативного запоминающего устройства.

### Заключение

Методы на основе распределенных отображений в виде кусочно-линейных плоскостей существенно более просты, нежели известные, и при этом достаточно гибки. Например, информацию в ХП можно закладывать как минимум четырьмя способами: маскировкой, нелинейным подмешиванием, манипуляцией режимами хаос-генератора, кодированием зон и областей. В настоящее время прорабатываются еще несколько уникальных подходов, касающихся повышения помехоустойчивости. В системах телекоммуникаций на основе распределенных отображений усложняется структура формирователя сигнала и его декодера.

В настоящей работе показана принципиальная возможность существенного повышения помехоустойчивости систем передачи информации на основе методов нелинейной динамики. Предложен новый алгоритм генерации хаотических последовательностей. В системе задаются распределенные во времени нелинейные формирующие функции (НФФ) в виде наклонных плоскостей в *N*-мерном пространстве фазовых состояний. Предложен эффективный с точки зрения объема вычислений алгоритм синтеза НФФ на основе полиномов не выше 3-ей степени.

Также показано, что передаваемое по каналу связи колебание по своим статистическим и спектрально−временны́м характеристикам схоже с шумом. При передаче последовательности «нулей» или «единиц» в сигнале не проявляются регулярные структуры. Определены алгоритмы информационной модуляции и достигнута помехоустойчивость системы передачи информации 15–21 дБ при вероятности ошибки $10^{-4}$. Все предложенные алгоритмы хорошо адаптированы к цифровым методам формирования и обработки сигнала, в том числе в системах с невысокой разрядностью целочисленных регистров. Предложенные алгоритмы расширяют класс сигналов с хаотической модуляцией и методов их приема и обработки на фоне шумов, что обеспечивает создание помехозащищенных и скрытных телекоммуникационных систем нового типа.

## GENERATION AND PROCESSING OF CHAOTIC SIGNALS BASED ON SIMPLE FUNCTIONS IN THREE DIMENSIONAL SPACE

V.A. CHERDYNTSEV, S.I. POLOVENYA, V.V. DUBROVSKY

### Abstract

A new class of chaotic oscillators, chaotic process that is based on distributed in time maps is considered. The algorithms and block diagrams of devices forming, information of modulation and signal processing are given. Numerical simulation of a family of curves obtained interference immunity for various operating conditions of the generator of chaotic processes is received.

### Список литературы

1. *Магницкий, Н.А., Сидоров С.В.* Новые методы хаотической динамики. М., 2004.
2. *Измайлов И.В., Коханенко А.П., Пойзнер Б.Н. и др.* // Изв. вузов. Сер. Физика. 2008. Т. 51. № 9/2. С. 178–179.