УДК 621.391

ДИНАМИЧЕСКИЙ ХАОС НА ОСНОВЕ НЕЛИНЕЙНОГО ПОДМЕШИВАНИЯ С КОДИРОВАНИЕМ БЛОКА ИНФОРМАЦИОННЫХ СИМВОЛОВ

С.И. ПОЛОВЕНЯ

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

Поступила в редакцию 2июля 2010

Рассмотрен метод блочного кодирования информационного потока с последующим нелинейным подмешиванием к динамическому хаосу в кольцевой динамической системе. Метод предполагает генерацию и обработку сигнала как с расширением спектра, так и без него. Предложены алгоритмы формирования сигнала и его обработки. Приведены структурно-функциональные схемы устройств и результаты численного моделирования.

Ключевые слова: хаос-процесс, нелинейная динамическая система, помехозащищенный прием.

Введение

Метод нелинейного подмешивания (НП) информации к динамическому хаосу является наиболее удобным для придания телекоммуникационной системе на его основе свойств структурной скрытности и защищённости информации от перехвата. Аналитически НП в одно-кольцевой динамической системе определяется выражением

$$h_k = (1-a)\, f(h_{k-1}, h_{k-2}, ..., h_{k-N}) + a\lambda_k, \qquad (1)$$

где h_k −последовательность отсчётов хаотического сигнала; $a \in [0;1]$ − параметр, задающий степень нелинейного подмешивания информации к хаосу; λ_k − информационное сообщение, мгновенные значения которого не превышают по модулю единицу; натуральное число N определяет память нелинейной динамической системы.

При $a = 1$ на модулятор передающего устройства подаётся лишь информационное сообщение λ_k. Если же $a = 0$, хаотический сигнал вырождается в хаотический процесс, не несущий полезной информации.

Отличительной чертой НП как метода информационной модуляции хаоса является возможность передачи информационного процесса, значения которого определены непрерывным множеством. В то время как при манипуляции хаотических режимов информационное сообщение должно иметь счётное и конечное число состояний [1]. В этой связи имеется возможность сравнительно простыми методами кодировать блок символов путём нелинейного подмешивания многоуровневой информационной последовательности к хаосу.

Генерация хаотического сигнала

Структурная схема метода, реализующего алгоритм кодирования блока информации, представлена на рис. 1.

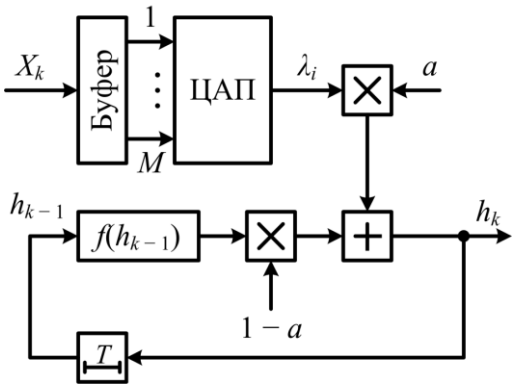

Рис. 1. Структурная схема кодера сигнала X_k – последовательность информационных символов, формирующая в буфере блоки по M бит; ЦАП – цифроаналоговый преобразователь; λ_i – многоуровневая последовательность, представляющая собой сообщение; $f(h_{k-1})$ – нелинейная формирующая функция (НФФ); T – такт формирования хаотического сигнала (ХС).

Формирователь *ХС* управляется тактовым генератором, изменяющим состояния системы каждые T секунд. На выходе ЦАП формируется многоуровневая последовательность λ_i, состояния которой равны одному из 2^M возможных значений. Так как буфер заполняется новым блоком за M тактов, то период смены состояний последовательности λ_i составляет MT секунд. Таким образом, в течение M тактов работы генератора хаотического сигнала передаётся одно и то же значение информационного сообщения, что позволяет в устройстве обработки сигнала уточнить оценку информационного параметра путём усреднения на некотором интервале времени.

Ниже приведены результаты численного моделирования генератора ХС для длины информационного блока 4 и НФФ в виде:

$$h_k = 0,67\sin(1,8\pi h_{k-1}) + 0,33\lambda_k \qquad (2)$$

Как видно из рис. 2 в отображении прослеживается «гладкий» характер формирующей функции, однако точное определение её параметров затруднительно, на фоне шумов – невозможно, т.к. состояния ХС достаточно равномерно распределены на плоскости.

Первые 50 тактов временных реализаций последовательностей λ_k и h_k приведены на рис. 3, гистограмма хаотического сигнала приведена на рис. 4.

На гистограмме прослеживается некоторое множество наиболее вероятных значений *ХС*, определяемое характером НФФ и допустимыми значениями процесса λ_k.

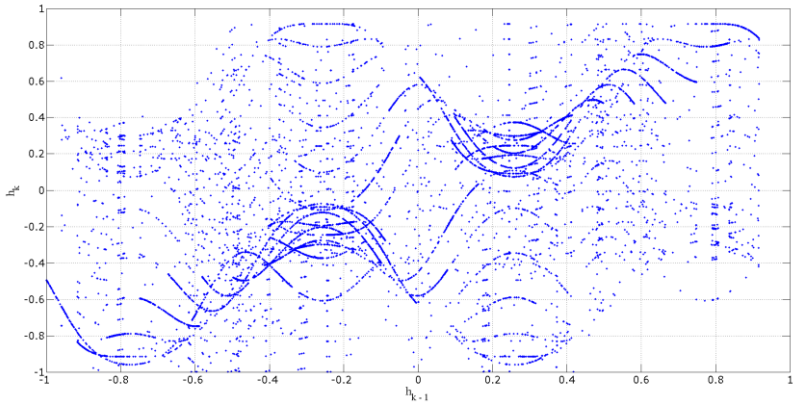

Рис. 2. Отображение хаос-сигнала для случая (2)

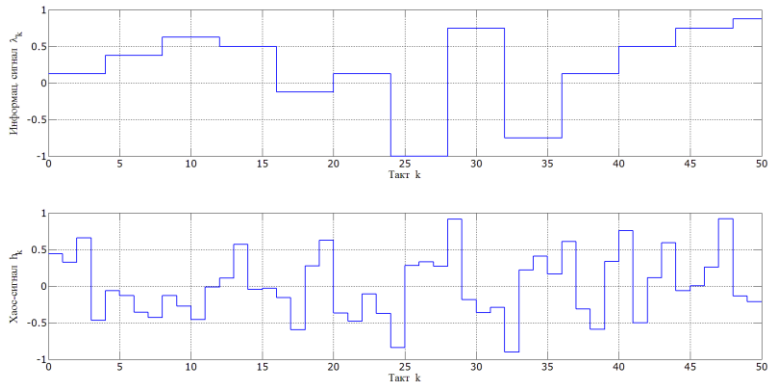

Рис. 3. Временная реализация сообщения и хаотического сигнала

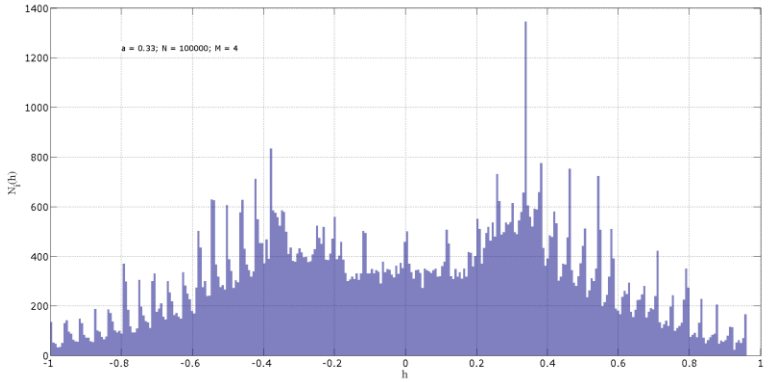

Рис. 4. Гистограмма хаос-сигнала

Обработка и декодирование информации

Алгоритм обработки также двухступенчатый и предполагает выполнение следующих процедур:

- извлечение информационного процесса λ_k из принятой хаотической последовательности;

- усреднение значений λ_k на интервале времени длительностью MT и декодирование информационного потока.

Обозначим сигнальную последовательность на выходе демодулятора устройства приёма как $r_k = h_k + n_k$, где n_k – отсчёты помехи. Оценочные значения информационной последовательности λ_k^* будут находиться согласно выражению:

$$\lambda_k^* = \frac{1}{a}\ r_k - (1-a)\, f(r_{k-1}) \quad . \qquad (3)$$

Структурная схема устройства обработки и декодирования принятого хаотического сигнала приведена на рис. 5.

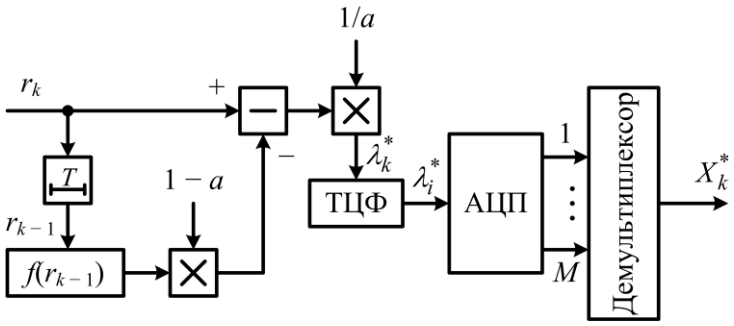

Рис. 5. Декодер хаотического сигнала ТЦФ − трансверсальный цифровой фильтр, осуществляющий усреднение последовательности λ_k^* во времени.

Сложная структура фазовых переходов принимаемого сигнала вместе с шумом показана на рис. 6, где представлена зависимость значений r_k от r_{k-1} и r_{k-2}.

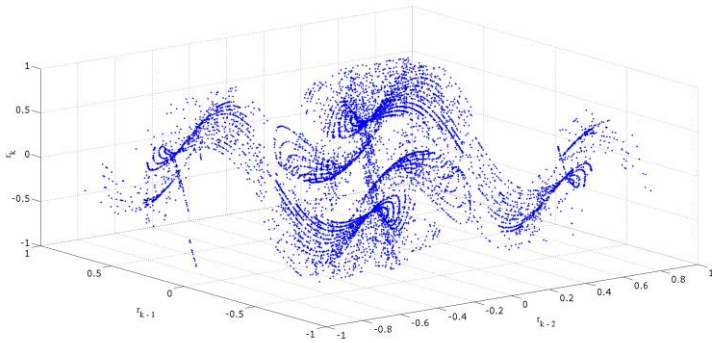

Рис. 6. Двумерное отображение последовательности r_k при отношении С/Ш равном 24 дБ

Численное моделирование системы передачи информации проводилось для четырёх функций: гладкой; гладкой с разрывами; кусочно-линейной; кусочно-линейной с разрывами. Показано, что разрывы в НФФ ухудшают помехоустойчивость на 2–3 порядка, что делает такие функции неприемлемыми для передачи информации с нелинейным подмешиванием блоков информации.

Семейство кривых помехоустойчивости для различных длин информационных блоков и кусочно-линейной формирующей функции без разрывов приведено на рис. 7.

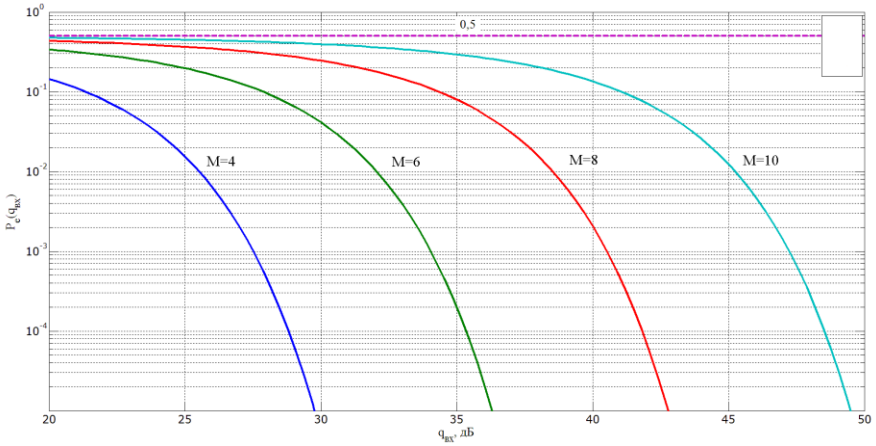

Рис. 7. Семейство кривых помехоустойчивости для M равного 4, 6, 8 и 10

Объём статистки составил 320 тыс. бит для каждого графика. Из приведённых графиков видно, что помехоустойчивость системы характеризуется некоторыми порогами, что обусловлено гранулярностью многоуровневого процесса λ_k.

Выводы и практические рекомендации

В работе показана принципиальная возможность повышения конфиденциальности передачи информации с нелинейным подмешиванием при условии, когда динамический хаос формируется на основе простейших одномерных отображений. Укажем особенности предлагаемого метода кодирования и декодирования.

1. По сравнению с манипуляцией хаотических режимов [2] отсутствует необходимость в тщательном выборе НФФ. В предлагаемом методе основным требованием к НФФ является простота и удобство её вычисления в реальном устройстве. Кроме того, в методе лишь одна формирующая функция задаёт структуру и характеристики динамического хаоса вне зависимости от длины информационного блока.

2. Для повышения помехоустойчивости системы желательно минимизировать угол наклона касательных или скорость изменения функции на всей области её определения, а также обязательно исключить разрывы в НФФ.

3. За счёт нелинейного подмешивания информационной последовательности отображение ХС является всегда достаточно сложным, что позитивно сказывается на возможности выявления характера НФФ путём длительного наблюдения реализации сигнала третьей стороной.

4. В устройстве приёма и обработки требуется точная нормировка хаос-сигнала, которая может достигаться за счёт передачи эталонного импульса единичной амплитуды через равные интервалы времени, определяемые степенью нестационарности канала связи.

5. Алгоритм формирования и обработки реализуем для многомерных и составных отображений, а также ориентирован на дискретную обработку сигнала.

DYNAMIC CHAOS NONLINEAR MIXING CODING OF INFORMATION SYMBOLS BLOCK

S.I. POLOVENYA

Abstract

Method of block coding information data stream, followed by nonlinear mixing of dynamic chaos in a circular dynamic system. The method involves the generation and signal processing, as with the expansion of the spectrum, and without it.

Литература

1. *Чердынцев В.А., Дубровский В.В.* // Материалы IX международной научно-технической конференции «Современные средства связи». Известия Белорусской инженерной академии. 2004. № 2 (18). С. 66–68.
2. *Чердынцев В.А., Дубровский В. В., Половеня С.И.* // Докл. БГУИР. 2009. № 2 (40). С. 5–11.