Abstract

The article concerns an experimental study of the efficiency of statistical processing of phase characteristics of signals to solve the problem of identification of the useful component of signals of ultrasonic nondestructive control against the background of considerable noises. The method consists in processing of the signal, received experimentally; in detection of its phase characteristics and their statistical treatment. Identification of information signals is caused by one of circular features, which is the resulting length of a vector, and which is obtained during the analysis of time-limited area of values of the phase characteristic of the signal in the sliding mode.

The data, obtained during the experiment, shows that on the time intervals, where information signals are present, the values of the resulting length of a vector increase, but outside these time intervals they reduce. Therefore, the sign of the radio signal is the excess of a certain vector P by the resulting length of a vector. The value of the level of detection of the P signals is chosen, according to given levels of errors of the first and second kind.

The considered method of signal processing can be used in precision ultrasonic flaw detectors and ultrasonic thickness meters while controlling products, which materials are characterized by significant signal extinction, heterogeneity and anisotropy.

It was shown that the use of statistical methods of processing of phase characteristics of signals allowed us to solve the problem of detection of signals of ultrasonic nondestructive control against the background of noises, comparable according to the level with a signal that increases the possibility of control of new structural materials, which are characterized by a significant exctintion of ultrasonic vibrations

Keywords*: ultrasonic nondestructive control, statistical processing, phase characteristics of signals, envelope of a signal, selective resulting length*

Розглядаються питання застосування хаотичних сигналів в сучасних конфіденційних системах зв'язку. Запропоновано метод підвищення структурної скритності сигнальних конструкцій, що сформовані на безлічі взаємно-ортогональних хаотичних послідовностей. Показано, як за допомогою кореляційного прийому здійснюється виділення інформаційного сигналу

Ключові слова: хаотичний сигнал, ортогональність, конфіденційний, сигнатура

Рассматриваются вопросы применения хаотических сигналов в современных конфиденциальных системах связи. Предложен метод повышения структурной скрытности сигнальных конструкций, формируемых на множестве взаимно-ортогональных хаотических последовательностей. Показано, как с помощью корреляционного приема осуществляется выделение информационного сигнала

Ключевые слова: хаотический сигнал, ортогональность, конфиденциальный, сигнатура

УДК 621.391

ПОВЫШЕНИЕ СТРУКТУРНОЙ СКРЫТНОСТИ ПЕРЕДАЧИ СИСТЕМ С ХАОТИЧЕСКИМИ СИГНАЛАМИ

В. В. Корчинский
Кандидат технических наук, доцент
Кафедра информационной безопасности и передачи данных
Одесская национальная академия связи им. А. С. Попова
ул. Кузнечная, 1, г. Одесса, Украина, 65029
Контактный тел.: 063-631-83-77

1. Введение

Большинство современных систем связи в качестве носителя информации использует в основном гармоническое колебание, с помощью которого реализуются различные виды модуляции. В таких системах защита информации от несанкционированного доступа чаще всего осуществляется на старших уровнях эталонной модели OSI. Внедрение явления динамического хаоса в область инфокоммуникационных технологий открывает новые перспективы не только по созданию эффективных систем криптокодирования, но и расширяет возможности по синтезу сигнальных конструкций, обеспечивающих потенциально высокую скрытность передачи на первом физического уровне модели OSI. Исследования, проведенные в [1, 2, 3], по-

казали целесообразность использования хаотических колебаний в качестве носителей информации для задачи построения конфиденциальных систем передачи информации.

Решение этой задачи особенно актуально при организации многопользовательского доступа.

В [1] показано, что защита конфиденциальной информации в каналах связи от НСД обеспечивается за счет различных показателей скрытности передаваемой сигнальной конструкции: энергетической, структурной, информационной и др.

Известно, что одним из методов достижения скрытности передачи является расширение спектра информационного сигнала, например, с помощью хаотических сигналов. Такой подход формирования сигнальных конструкций позволит решать задачу по обеспечению энергетической скрытности передачи, которая включает меры, направленные на противодействия факта обнаружения передаваемого сигнала в канале.

Многообразие форм хаотического сигнала, вырабатываемых генераторами хаоса, дает возможность создавать на их базе сигнальные конструкции с переменной структурой и решать проблему по обеспечению структурной скрытности передачи, которая должна в случае перехвата сообщения средствам НСД противостоять действиям, направленным на распознавание формы сигнала и измерение его параметров.

Информационная скрытность определяется способностью противостоять мерам, направленным на раскрытие смысла передаваемых сообщений с помощью сигналов информации [1].

В данной статье предложен метод формирования сигнальных конструкций для задачи повышения структурной скрытности передаваемых сигналов. Исследования в данном направлении были выполнены в работах [2, 3], в которых были показаны методы кодирования информационной двоичной последовательности хаотическим сигналом. Среди разнообразия используемых методов передачи информации на основе динамического хаоса можно выделить [2]:

1) хаотическую маскировку, при которой информационный сигнал суммируется с хаотическим сигналом и передается в канал связи;

2) переключение хаотических режимов, когда, например, в случае бинарного информационного сигнала символ «1» кодируется одним типом хаотического сигнала, а символ «0» – другим;

3) нелинейное подмешивание, когда информационный сигнал непосредственно участвует в формировании хаотического сигнала.

Приведенные примеры методов передачи на основе динамического хаоса демонстрируют лишь простейшие возможности и приёмы по обеспечению скрытности передачи в канале связи. Очевидно, что усложнение алгоритма кодирования позволит существенно увеличить структурную скрытность передачи.

В связи с тем, что в современных системах связи защите конфиденциальной информации уделяется всё больше внимания, актуальным является совершенствование методов передачи, обеспечивающих повышение скрытности передачи.

Целью работы является разработка метода повышения структурной скрытности сигнальных конструкций, формируемых на основе множества взаимно-ортогональных хаотических последовательностей.

2. Формирование взаимно-ортогональных кодовых последовательностей

В системах связи для формирования хаотических сигналов используются аппаратные или программные генераторы хаотических колебаний [2]. Особенность этих генераторов заключается в том, что небольшие изменения их параметров или начальных значений приводят к существенному изменению формы генерируемого колебания, что дает возможность формирования и выбора различных реализаций хаотического процесса.

Программный способ генерирования хаотического колебания x_n осуществим в соответствии с некоторым разностным уравнением

$$x_{n+1} = f(x_0; x_n; a), \quad (1)$$

где $f(\cdot)$ – нелинейная функция отображения; a – управляющий параметр, x_0, x_n, x_{n+1} – начальное, текущее и последующее значения соответственно или $x(t)$ в соответствии с дифференциальным уравнением вида

$$dx(t)/dt = F[x(t); m], \quad (2)$$

где F – нелинейный оператор; m – управляющий параметр.

Одна из реализаций хаотического сигнала $x(t)$ приведена на рис. 1, которая обладает всеми свойствами шумоподобного сигнала: непериодичность траекторий во времени; экспоненциально спадающая корреляционная функция; сплошной непрерывный спектр мощности.

Данные свойства сигналов свидетельствуют о целесообразности использования их в системах конфиденциальной связи.

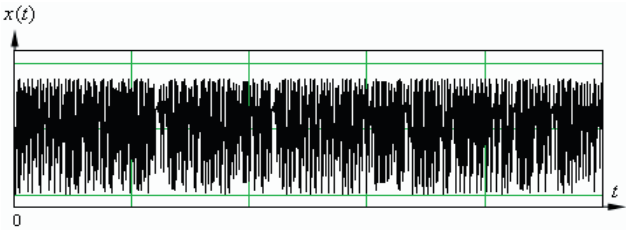

Рис. 1. Реализация хаотического сигнала $x(t)$ от времени t

Для задачи исследования в работе методом перебора был осуществлен поиск пяти ортогональных сигнатур на базе одной из реализаций хаотического сигнала. Хаотический сигнал, предварительно прошедший дискретизацию по времени (использована теорема отсчетов) и квантование по уровню $x(t)$ (в эксперименте использовалось 256 уровней), преобразовывается в многоуровневую кодовую последовательность x_n. Кодовая последовательность x_n разби-

ваетсянасегментыопределеннойдлины,например, $s = 30$ элементов (чипов) и путем их сравнения находятся взаимно-ортогональные кодовые последовательности c_i, которые и будут использоваться в качестве сигнатур.

В табл. 1 приведены коэффициенты взаимной корреляции r_{ij} отобранных $c_1, c_2, \ldots, c_5$ сигнатур. Как показали результаты эксперимента, обеспечить условие $r_{ij} = 0$ между сигнатурами при таком алгоритме их формирования не представляется возможным, поэтому при отборе был использован диапазон значений $-0{,}08 < r_{ij} < 0{,}08$.

Таблица 1

Коэффициенты корреляции r_{ij} между сигнатурами c_i.

№	r_{ij}			
i \ j	2	3	4	5
1	–0,00021	0,0070	–0,037	0,0091
2		–0,0081	0,011	0,0724
3			–0,080	–0,0286
4				–0,0469

3. Метод кодирования информационного сигнала

Рассмотрим метод кодирования информационного сигнала на основе множества ортогональных многоуровневых кодовых последовательностей.

Пусть имеется некоторое количество N источников взаимно-ортогональных хаотических сигналов (ВХС) и источник информации (ИИ). Для кодирования информационного сигнала на интервале времени одной или более посылок цифрового сигнала ($T_к = t_0 k$, где t_0 – длительность элементарной посылки; $k = 1, 2, \ldots$,) используется одна из числа N отобранных ортогональных последовательностей (сигнатура) c_i. Управление источниками ВХС осуществляется устройством управления (УУ) через коммутатор К (рис. 2). На выходе умножителя (×) схемы формируется сигнал

$$X_i(T_к) = x c_i, \qquad (3)$$

что равносильно замене единичных посылок на интервале t_0 сигнатурой c_i. При этом, если для замены каждой «1» в исходном двоичном потоке данных используется некоторая сигнатура определенной длины, то для замены «–1» применяют ту же сигнатуру, но с инвертированным значением чипов. Использование прямой и инвертированной сигнатуры обеспечивает не только определение полярности передаваемых посылок, но и позволяет регистрировать их передние и задние фронты при корреляционном приеме.

Сформированный таким образом сигнал источника ЦИ суммируется на интервале $T_к$ с остальными сигнатурами c_i.

Покажем формулу кодирования цифрового сигнала x, при условии, что в качестве сигнатуры была использована последовательность c_1

$$X_K(T_к) = x c_1 + \sum_{i=2}^{N} c_i \ . \qquad (4)$$

Очевидно, что надежность выделения на приемной стороне информационного сигнала x из $X_K(T_к)$ определяется ортогональностью сигнатур $c_1, c_2, \ldots, c_N$.

С целью обеспечения эффективности корреляционного приема в канале на приемной стороне отдельные элементы (посылки) должны быть строго синхронизированы между собой.

На рис. 2 показана структурная схема формирования сигнала $X_K(T_к)$ с помощью пяти взаимно-ортогональных сигнатур с числом чипов $s = 30$ на одну элементарную посылку.

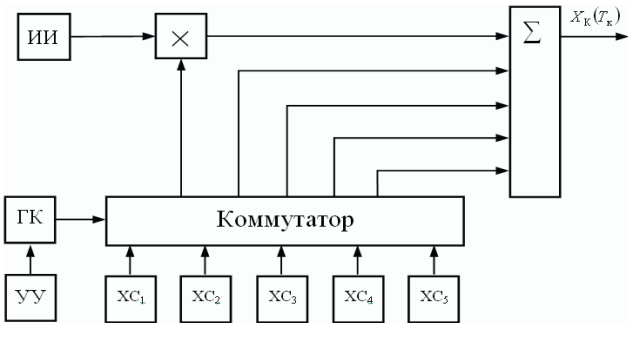

Рис. 2. Структурная схема формирования сигнала $X_K(T_к)$

Генератор ключей ГК по команде устройства управления (УУ) задаёт правило подключения источников XC_i с помощью коммутатора к перемножителю и линейному сумматору. Как видно из представленного алгоритма умножение информационного сигнала может быть осуществлено одним из источников XC_i, а остальные подключаются к входам сумматора Σ.

Таким образом, меняя через определенные интервалы времени опорную сигнатуру информационного сигнала и с учетом суммирования различных составляющих других сигнатур, можно менять структуру формируемого сигнала на выходе сумматора для задачи повышения структурной скрытности передаваемых сигнальных конструкций.

4. Выделение информационного сигнала на приемной стороне

На основе корреляционного приема покажем процесс выделения информационного сигнала из сигнальной конструкции $X_K(T_к)$. Для этого каждый разряд сигнала $X_K(T_к)$ умножается на соответствующий элемент опорной сигнатуры c_i (используемой на передаче для замены «+1»). Результаты каждого умножения с учетом амплитуды и значения полярности интегрируются в накопителе в пределах периода времени t_0.

Решающие устройство в конце каждого периода анализирует уровень напряжения с выхода интегратора и принимает решение о полярности принятой посылки «1» или «–1» информационного сигнала. Кроме этого, в конце каждого периода осуществляется сброс в ноль уровень выходного напряжения интегратора.

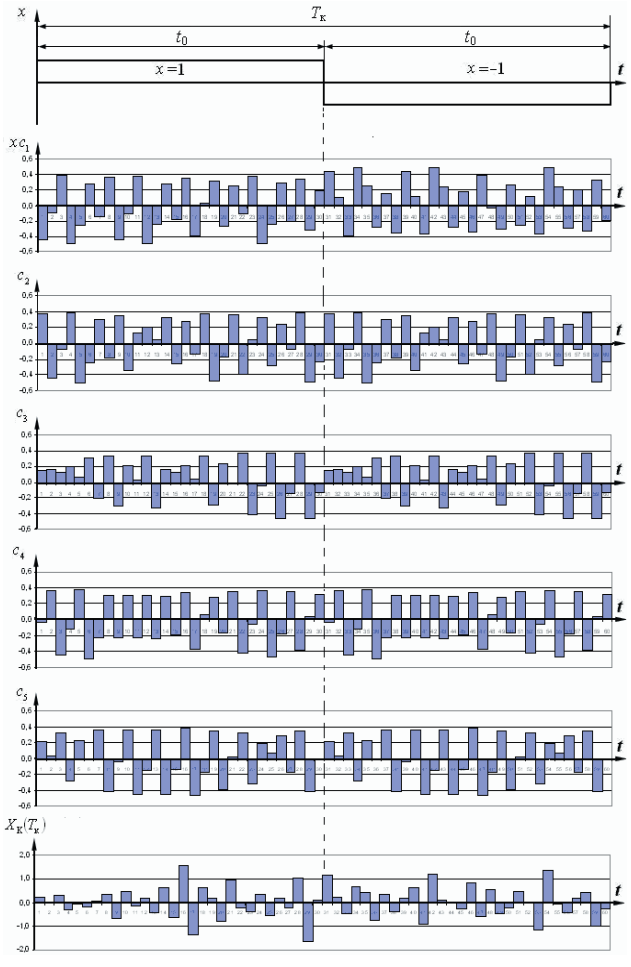

Рис. 3. Формирование зашифрованной сигнальной конструкции $X_K(T_к)$ от времени t

Если предположить, что канальный сигнал $X_K(T_к)$ средствами НСД перехвачен, то попытка выделения информационного сигнала с использованием другой сигнатуры не приведет к положительному результату, так как значения уровня напряжения каждого периода интегрирования будут близкими к нулю или распределяться случайным образом.

Подбор соответствующей сигнатуры средствами НСД будет затруднен из-за модулирования информационным сигналом хаотических сигналов, формируемых от различных генераторов, период подключения ($T_к$) которых известен только на приемной стороне конфиденциальной системы передачи.

На рис. 4 показано выделение информационных элементов из группового сигнала при корреляционном приеме, предполагая линейность системы и наличие идеальной синхронизации в канале.

Из рисунка видно, что уровень сигнала на выходе интегратора $U_{вых\,инт}$ превышает порог принятия решения $U_{макс}/2$, чем обеспечивается надежное выделение сигнала информационного сигнала.

Кроме того, если $U_{вых\,инт} > U_{макс}/2$, тогда посылка x′ принята положительной полярности, если $U_{вых\,инт} < -U_{макс}/2$, то – отрицательной.

5. Вывод

В данной статье предложен метод повышения структурной скрытности сигнальных конструкций, который реализован на множестве взаимно-ортогональных хаотических последовательностей. Данный метод позволяет повысить структурную скрытность передачи за счет переменной структуры сигнальных конструкций.

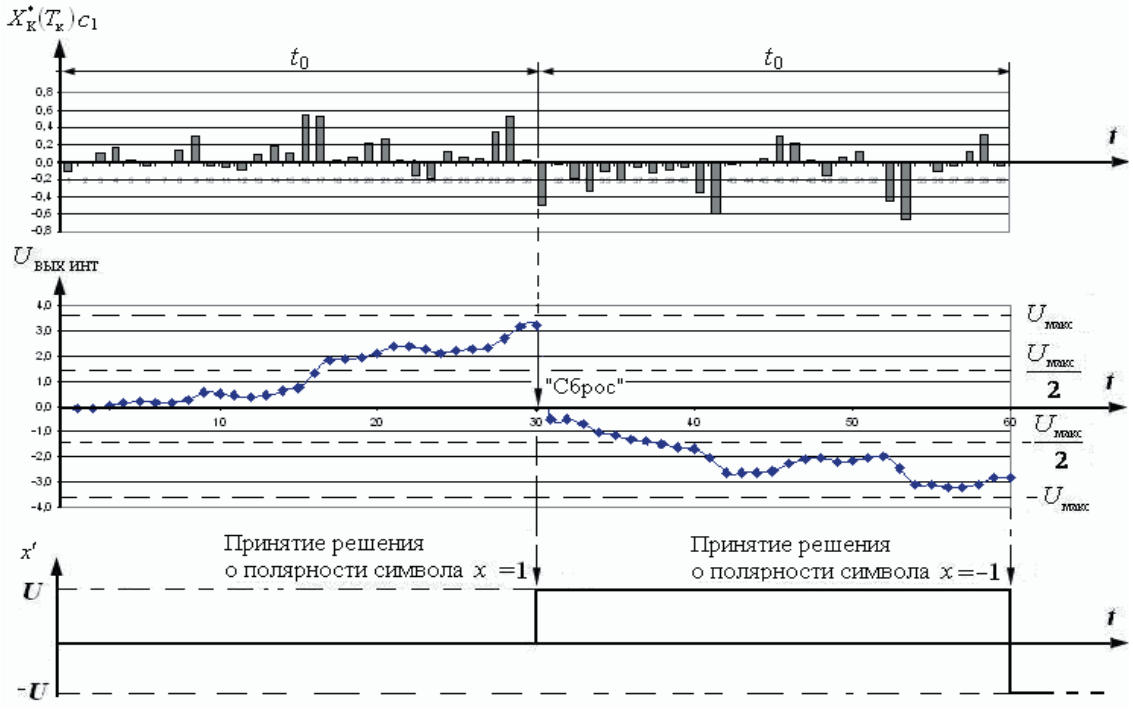

Рис. 4. Зависимости $X_K(T_к)$ c_1, $U_{вых\,инт}$ и x′ от времени t

Литература

1. Гуляев, Ю.В. Информационные технологии на основе динамического хаоса для передачи, обработки, хранения и защиты информации [Текст] / Ю.В. Гуляев, Р.В. Беляев, Г.М. Воронцов и др. // Радиотехника и электроника. - 2003. - Т. 48, №10. - С 1157-1185.
2. Капранов, М. В. Регулярная и хаотическая динамика нелинейных систем с дискретным временем [Текст] / М. В. Капранов, А. И. Томашевский. - М.: Издательский дом МЭИ, 2010. - 256 с.
3. Захарченко, Н. В. Структурная скрытность таймерных сигналов в системах с кодовым разделением каналов [Текст] / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Восточно-Европейский журнал передовых технологий. - 2011. - № 2/9(50). - С. 7-9.

Abstract

The majority of modern communication systems use a harmonic motion as an information carrier, which helps to implement various types of modulation. In such systems, the information is often protected from unauthorized access by encrypting of the information message at a link layer. The introduction of the phenomenon of dynamical chaos in the area of information and communication technologies has showed new prospects for the creation of the efficient encryption, as well as has increased the possibility of the synthesis of signal structures, providing potentially high secrecy at the layer of physical link. The variety of forms of chaotic signal, produced by chaos generators permits to create on their basis the signal structures with variable structure and to solve the problem of the secrecy of transmission, which in case of interception of a message through unauthorized access should resist actions, directed to the recognition of the form of a signal and measurement of its parameters. Due to the fact that in modern communication systems the protection of confidential information has been receiving more attention, it is important to improve the methods of transmission that enhance stealthiness of transmission. The article considers the use of chaotic signals in the modern confidential communication systems. A method of increase of the structural stealthiness of signal structures formed on a set of mutually orthogonal chaotic sequences was suggested. It was shown how to use the correlation method to select information signal

Keywords*: chaotic signal orthogonality, confidential, stealthiness*

Описано створення моделі фрагмента розподіленої інформаційної системи - grid-системи в спеціалізованій програмі GridSim. Наводиться схема побудови моделі, її основні параметри. Виконана формалізація системних ситуацій в grid-системи, наведені результати моделювання

Ключові слова: симуляція, grid-система, системні ситуації

Описано создание модели фрагмента распределенной информационной системы - grid-системы в специализированной программе-симуляторе GridSim. Приводится схема построения модели, ее основные параметры. Выполнена формализация системных ситуаций в grid-системе, приведены результаты моделирования

Ключевые слова: симуляция, grid-система, системные ситуации

УДК 004.75

СИТУАЦИОННОЕ МОДЕЛИРОВАНИЕ ФРАГМЕНТОВ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Ю.В. Сосновский
Кандидат технических наук
Кафедра компьютерной инженерии и моделирования
Таврический национальный университет
им. В.И. Вернадского
пр. Вернадского, 4, г. Симферополь, Украина, 95000
Контактный тел.: 050-984-35-55
E-mail: yuri.sosnovskij@mail.ru

1. Введение

В настоящее время, как известно, распределенные информационные системы обеспечивают основную долю роста вычислительной мощности и дискового пространства предоставляемых сервисов в сетях интернет и интранет. В то же время, актуальной остается проблема обеспечения необходимого уровня качества