УДК 621.391

В. В. Корчинский

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ЗАЩИЩЕННЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

Рассматриваются вопросы применения хаотических сигналов в современных системах связи, в частности, предложен метод организации многопользовательского доступа в системах передачи конфиденциальной информации

Ключевые слова: *хаотический сигнал, многопользовательский доступ, сигнатура*

1. Введение

Исследования, о которых идет речь в докладе, относятся к области повышения информационной безопасности в телекоммуникационных системах и сетях. Для выполнения этой задачи важным является создание новых высоконадежных технологий по защите информации не только от ошибок в канале связи, но и от несанкционированного доступа (НСД).

Противодействие средствам НСД выдвигает поиск новых методов и подходов по обеспечению безопасности конфиденциальной информации. Известно [1], что защита информации от НСД осуществляется комплексом правовых, организационных и технических мероприятий непосредственно в абонентских пунктах. Не менее важной является задача по защите конфиденциальной информации от НСД на уровне физического канала с помощью сигнальных конструкций, которым присущи свойства скрытности передачи [2, 3]. Такой подход к защите информации на этапе ее передачи по каналу связи направлен на затруднение средствами НСД самого факта обнаружения несущего сигнала, а также в случае его перехвата распознавания структуры и параметров используемых сигнальных конструкций с последующим раскрытием смыслового содержания сообщения.

2. Постановка проблемы

В работе показана возможность создания многоканальной системы передачи на основе динамического хаоса с кодовым разделением каналов (КРК).

3. Основная часть

3.1. Анализ литературных источников по теме исследования. При построении конфиденциальных систем связи в последнее время все чаще используется явление динамического хаоса [2, 3, 4]. Под динамическим хаосом понимают сложные непериодические колебания, порождаемые нелинейными системами, вид которых полностью определяется только параметрами динамической системы.

В [4] методом перебора был осуществлен поиск семи ортогональных сигнатур на базе одной из реализаций хаотического сигнала. Предварительно, прошедший дискретизацию по времени и квантование по уровню хаотический сигнал $x(t)$ преобразовывается в многоуровневую кодовую последовательность x_n. Кодовая последовательность x_n разбивается на сегменты определенной длины, например, $s = 30$ элементов (чипов), и путем их сравнения находят взаимно-ортогональные кодовые последовательности, которые и будут использоваться в качестве сигнатур.

Пусть имеется некоторое количество N источников цифрового сигнала, использующих избыточные коды, и соответствующее им количество двоичных каналов. Каждому i-му каналу присваивается своя многоуровневая кодовая последовательность в качестве сигнатуры c_i. Формирование сигнала в индивидуальном канале осуществляется путем замены единичных посылок сигнатурой, разной по структуре, но равной длительности в чипах для каждого канала (в нашем случае $s = 30$). С целью обеспечения эффективности корреляционного приема в каждом индивидуальном канале на приемной стороне отдельные элементы (посылки) индивидуальных каналов должны быть синхронизированы между собой.

Следует заметить, что 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 инвертированием значений 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 в каждом индивидуальном канале.

Так как групповой сигнал $X_{\text{ГР}}$ формируется в результате суммирования сигнатур c_i всех индивидуальных каналов

$$X_{\text{ГР}} = \sum_{i=1}^{N} x_i c_i , \qquad (1)$$

ISSN 2226-3780

то надежность разделения каналов определяется степенью ортогональности сигнатур $c_1, c_2, \ldots, c_N$.

На приемной стороне каждый разряд группового сигнала $X_{\text{ГР}}$ умножается на соответствующий элемент «своей» прямой (используемой на передаче для замены «+1») сигнатуры c_i, в результате получаем сигнал, в котором заложена информация индивидуального i канала. Результаты каждого умножения с учетом амплитуды и значения полярности интегрируются в накопителе в пределах одного периода последовательности. В конечном счете, по окончании периода сигнатуры на выходе интегратора формируется уровень напряжения, полярность которого будет соответствовать полярности принятой посылки «+1» или «−1» в каждом индивидуальном канале. При этом сигналы других пользователей с их сигнатурами воспринимаются как аддитивные шумы для данного канала. Предполагая линейность системы и наличие идеальной синхронизации в каналах на рис. 1 показано выделение элементарных посылок одного индивидуального канала из группового сигнала при корреляционном приеме. Из рисунка видно, что уровень сигнала на выходе интегратора $U_{\text{ВЫХ ИНТ}}$ значительно превышает порог принятия решения $U_{\text{макс}}/2$, чем обеспечивается надежное выделение сигнала каждого индивидуального канала. Кроме того, если $U_{\text{ВЫХ ИНТ}} > U_{\text{макс}}/2$, то принята посылка положительной полярности, если $U_{\text{ВЫХ ИНТ}} < -U_{\text{макс}}/2$, то — отрицательной.

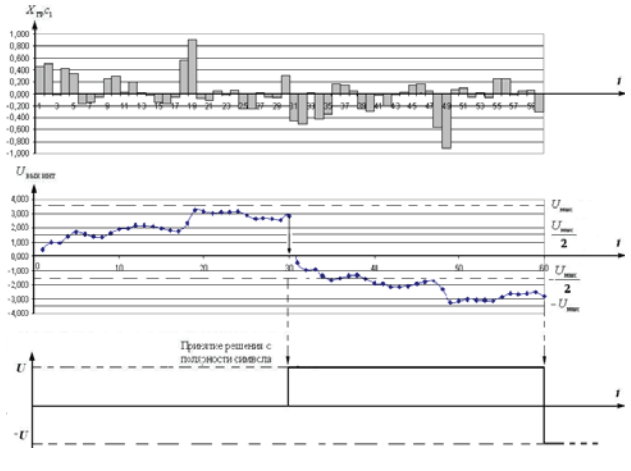

Рис. 1. Выделение элементарной посылки одного индивидуального канала из группового сигнала

3.2. Результаты исследований. Предложенные методы формирования многоуровневых ортогональных последовательностей на базе хаотического процесса и группового сигнала показали возможность организации многопользовательского доступа в современных конфиденциальных системах связи. При построении таких систем возникает задача поиска достаточного количества взаимно-ортогональных кодовых последовательностей с хорошими корреляционными свойствами.

Литература

1. Куприянов А. И. Основы защиты информации [Текст] : учебное пособие / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. — М. : Издательский центр «Академия», 2006. — 256 с.
2. 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.
3. Захарченко Н. В. Метод формирования сигнальных конструкций на основе хаотических и таймерных сигналов в системах передачи конфиденциальной информации [Текст] / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Збірник наукових праць ОНАЗ ім. О. С. Попова. —2011. — № 2. — С. 3—7.
4. Захарченко Н. В. Многопользовательский доступ в системах передачи с хаотическими сигналами [Текст] / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Восточно-Европейский журнал передовых технологий. — 2011. — № 5/9(53). — С. 26—29.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИЩЕНИХ ІНФОКОМУНІКАЦІЙНИХ СИСТЕМ

В. В. Корчинський

Розглядаються питання застосування хаотичних сигналів в сучасних системах зв'язку, зокрема, запропонований метод організації доступу з багатьма користувачами в системах передачі конфіденційної інформації.

Ключові слова: хаотичний сигнал, розрахований на багато користувачів доступ, сигнатура.

***Володимир Вікторович Корчинський**, кандидат технічних наук, доцент кафедри інформаційної безпеки і передачі даних Одеської національної академії зв'язку ім. О. С. Попова, **тел.: (095) 208-27-10, e-mail: vladkorchin@rambler.ru**.*

INCREASE THE EFFICIENCY OF SECURE INFOCOMMUNICATION SYSTEMS

V. Korchinsky

Multi-user access in the data communication systems with chaotic signals.

The problems of chaotic signals usage in modern communication systems were discussed. The method of organizing multi-user access system for transmission of confidential information was proposed.

Keywords: chaotic signal, multi-user access, signature.

***Vladimir Korchinsky**, Ph.D., Associate Professor, Department of Information Security and data transfer, Odessa National Academy of Telecommunications named after O. S. Popov, **tel.: (095) 208-27-10, e-mail: vladkorchin@rambler.ru**.*