ISSN 2226-3780

УДК 621.391

Корчинский В. В.

МЕТОД ФОРМИРОВАНИЯ ГРУППОВОГО СИГНАЛА НА ОСНОВЕ ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТАНОВКИ РЕАЛИЗАЦИЙ ХАОТИЧЕСКИХ СИГНАЛОВ

Для конфиденциальных систем связи с кодовым разделением каналов предложен метод формирования группового сигнала на основе множества взаимно-ортогональных последовательностей хаотических реализаций. С целью повышения структурной скрытности передачи в системе связи предлагается периодически выполнять по некоторому заданному закону перестановку ортогональных псевдослучайных хаотических последовательностей для каждого индивидуального канала.

Ключевые слова: *хаотический сигнал, ортогональность, конфиденциальный, сигнатура, несанкционированный доступ, скрытность, канал, защита.*

1. Введение

В последнее десятилетие особый интерес приобретают методы защиты информации применительно к первому уровню эталонной модели OSI [1, 4]. Немаловажную роль в этом играет появление сложных видов модуляции, развитие широкополосных систем передачи и внедрение явления динамического хаоса в современную теорию информации и связи. Как результат, становится возможным создание сигнальных конструкций, которым присущи свойства скрытности передачи, т. е. маскировки, что направлено на существенное снижение эффективности средств несанкционированного доступа (НСД) по перехвату сообщений на уровне физического канала [3].

Качество защиты передаваемой информации от средств НСД на уровне физического канала оценивается показателем энергетической скрытности, который характеризует способность системы противостоять мерам НСД, направленным на обнаружение самого факта передачи сигнала. Если станцией НСД сообщение перехвачено, то структурная скрытность должна противостоять мерам, направленным на распознавание формы сигнала и измерение его параметров, т. е. отождествление обнаруженного сигнала с одним из множеств априорно известных сигналов. Показатель информационной скрытности оценивает качество защищаемой информации в инфокоммуникациях на верхних уровнях модели OSI [2]. Защита информации в этом случае осуществляется с помощью различных криптографических систем [7–12].

В настоящее время большой интерес представляют методы передачи, в которых в качестве носителей информации используются не гармонические колебания, а шумовые сигналы. Особенность такого вида переносчика информации, как шум, объясняется новой перспективой их применения в различных информационных технологиях.

Первоначально практическое использование шумов имело два основных направления, связанных с маскировкой работы собственных информационных систем, и созданием помех для дестабилизации работы подобных систем вероятного противника [1].

Для современных систем связи реальный интерес представляют шумовые сигналы с воспроизводимостью генерируемых процессов, примером которых являются реализации на основе динамического хаоса [3, 4].

Использование возможностей динамического хаоса в инфокоммуникациях открывает широкие перспективы по практическому их применению в следующих направлениях: синхронизация приемника и передатчика [3]; маскировка и восстановление сообщений [4]; фильтрация шумов [3]; восстановление информационных сигналов [2], создание алгоритмов кодирования и декодирования цифровых сообщений на основе реализаций хаотической системы [4, 5, 6].

Шумовые сигналы на основе динамического хаоса по своей сути являются шумоподобными сигналами (ШПС). Такие сигнальные конструкции обладают свойствами случайных шумовых сигналов (широкий спектр, меняющаяся по внешнему виду при каждой выборке реализация такого сигнала и др.) и имеет главную особенность, которая отличает их от обычных шумов: они реализуются с использованием разработанного математического алгоритма, т. е. обладают свойством воспроизводимости.

В работе [6] рассмотрена возможность создания многоканальной системы передачи на основе динамического хаоса с кодовым разделением каналов. Представляет интерес дальнейшее развитие этого метода с целью повышения структурной скрытности передачи формируемых сигнальных конструкций группового сигнала.

Целью статьи является разработка метода формирования группового сигнала на основе множества взаимно-ортогональных последовательностей хаотических реализаций с псевдослучайной их перестановкой при выборе индивидуального канала.

2. Алгоритм формирования группового сигнала

Пусть в системе с кодовым разделением каналов (КРК) имеется некоторое количество источников цифрового сигнала $x_1, x_2, ..., x_N$, использующих избыточные коды, и соответствующее им количество двоичных каналов

с ограниченной полосой пропускания ΔF и минимальной базой сигнала $B = \Delta F t_0 = 1$. Сигналы абонентов объединяются в групповой сигнал и им предоставляется возможность одновременной работы в общей полосе частот. Для возможности разделения каналов каждый двоичный элемент исходного сигнала в индивидуальных каналах заменяется соответствующей дискретной реализацией псевдослучайной хаотической последовательности (ПХП) c_i, называемой сигнатурой, разной по структуре, но равной по длительности в чипах для каждого канала. В ПСП длительность отдельного чипа (сигнала минимальной длительности) $t_ч$ намного меньше времени передачи бита сообщения t_0 в индивидуальном канале. Следовательно, ширина спектра группового сигнала определяется длительностью $t_ч$. Вид многоуровневой сигнатурной последовательности приведен на рис. 1.

Надежность разделения каналов на приемной стороне зависит от длины сигнатуры (числом реализаций ПХП) на интервале единичного элемента в индивидуальных каналах и ортогональности сигнатур $c_1, c_2, \ldots, c_N$, которые предназначены для формирования группового сигнала. В работе [6] рассмотрены вопросы выбора и обеспечения ортогональности сигнатур.

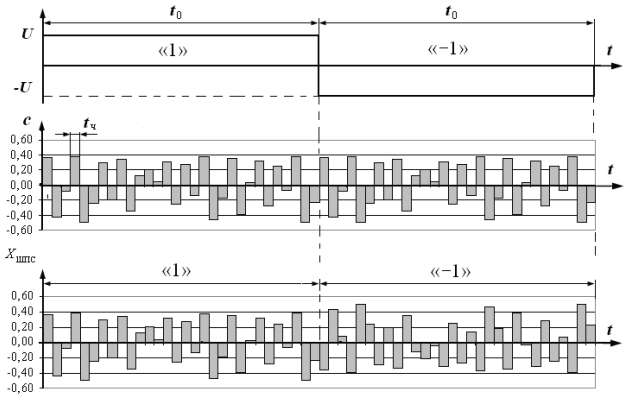

Рис. 1. Правило кодирования последовательности «1» и «–1» индивидуального канала с помощью сигнатуры ПХП

Алгоритм кодирования последовательности «1» и «–1» индивидуального канала с помощью хаотической последовательности в одноканальной системе передачи следующий: 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 чипов в данной ПХП, т. е.

$$X_{\text{ШПС}\,i}(t_0) = x_i(t_0)c_i(t_0). \qquad (1)$$

Использование прямой и инвертированной сигнатуры обеспечивает не только определение полярности передаваемых посылок, но и позволяет регистрировать их значащие моменты модуляции при корреляционном приеме в каждом индивидуальном канале.

Групповой сигнал $X_{\text{ГР}}(t_0)$ формируется в результате суммирования чиповой последовательности каждого индивидуального канала

$$X_{\text{ГР}}(t_0) = \sum_{i=1}^{N} x_i(t_0)c_i(t_0). \qquad (2)$$

Многопозиционный сигнал с выхода сумматора поступает на формирователь прямохаотического сигнала $X_{\text{ГР}}(t_0)$, а затем в канал.

На рис. 2 представлена структурная схема предлагаемой конфиденциальной системы передачи, для правильной работы которой необходимы наличие системы синхронизации и согласованная смена ключей в передатчике и приемнике.

Для повышения структурной скрытности передачи в системе связи предлагается периодически выполнять по некоторому заданному закону смену (перестановку) ортогональных ПХП для каждого индивидуального канала. Смена комбинаций ортогональных ПХП при передаче и приеме осуществляется по командам устройства управления (УУ) передатчика через коммутатор с учетом ключа A_k, формируемого генератором ключа (ГК) на каждый сеанс передачи.

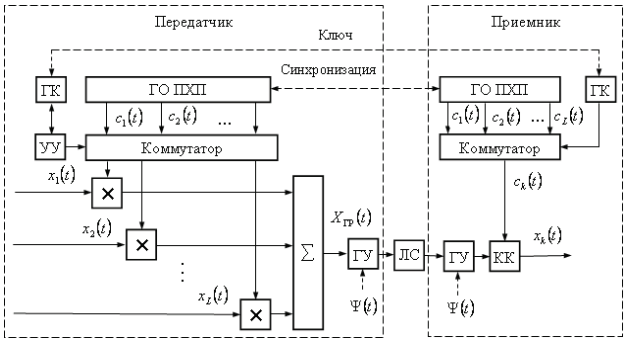

Рис. 2. Структурная схема системы с ХС: ГОС — генератор ортогональных сигналов; × — схема умножения; ГУ — групповое устройство; ГК — генератор ключей; S — сумматор; ГО ПХП — генератор опорных псевдослучайных хаотических последовательностей

Для согласования сигнал $X_{\text{ГР}}(t)$ со средой передачи он поступает на вход ГУ, а затем в линию связи (ЛС). Если в системе связи не используется прямохаотическая передача [3], то в ГУ может выполняться повторная модуляция сигнала $Y_{\text{К}}(t)$ с помощью носителя $\psi(t)$. В приемнике на основе ключа A_k задается опорная ПХП, поступающая через коммутатор на корреляционный приемник (КК), с помощью которого осуществляется выделение информационного сигнала индивидуального канала.

3. Выводы

В заключение можно сделать следующие выводы.

В данной статье предложен метод формировании группового сигнала на основе множества взаимно-ортогональных последовательностей хаотических реализаций с псевдослучайной их перестановкой при выборе индивидуального канала. Данный метод позволяет повысить структурную скрытность передаваемых сигнальных конструкций, что особенно важно при построении конфиденциальных систем связи многопользовательского доступа.

Литература

1. Куприянов, А. И. Теоретические основы радиоэлектронной борьбы [Текст] / А. И. Куприянов, А. В. Сахаров. – М. : Вузовская книга, 2007. – 356 с.

2. Шаньгин, А. И. Информационная безопасность компьютерных систем и сетей [Текст] / А. И. Шаньгин. — М. : ИД «Форум»: ИФРА-М, 2008. — 416 с.
3. 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.
4. Корчинский, В. В. Повышение структурной скрытности передачи систем с хаотическими сигналами [Текст] / В. В. Корчинский // Восточно-Европейский журнал передовых технологий //научный журнал. —2013. — № 1/9(61). — С. 53.
5. Захарченко, Н. В. Эффективность использования таймерных сигнальных конструкций в системах передачи с кодовым разделением каналов [Текст] / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Наукові праці ДонНТУ. — 2011. — Випуск № 20(182). — С. 145—151.
6. 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.
7. Richard, K. Recommendations of the National Institute of Standards and Technology [Text] / K. Richard, T. Walsh, W. Fries. — NIST SP 800-58. — 2005. — P. 93.
8. Базова модель ВВС. — Geneva. Recomendation CCITT X.200. Reference Model of open systems interconnection for CCITT applications // Стандарт ISO 7498-1:1984. — 1991. — P. 31.
9. Carvalho, M. Using Mobile Agents as Roaming Security Guards to Test and Improve Security of Hosts and Networks Proceedings of the 2004 ACM Symposium on Applied Computing (SAC'04) [Text] / M. Carvalho, T. Cowin, N. Suri, M. Breedy, K. Ford. — ACM. — 2004.
10. Pedireddy, T. Prototype Multi Agent Network Security System. Proceedings of the AAMAS'03. [Text] / T. Pedireddy, J. Vidal. — ACM. — 2003.
11. Menezes, R. Self-Organization and Computer Security Proceedings of the 2005 ACM Symposium on Applied Computing (SAC'05) [Text] / R. Menezes. — ACM. — 2004.
12. Valeyev, S. Multiagent Technology and Information System Security Proceedings of the 7th International Workshop on Computer Science and Information Technologies CSIT'2005 [Text] / S. Valeyev, T. Bakirov, D. Pogorelov, I. Starodumov. — Ufa, Russia, 2005. — Vol. 1. — P. 195—200.

МЕТОД ФОРМУВАННЯ ГРУПОВОГО СИГНАЛУ НА ОСНОВІ ПСЕВДОВИПАДКОВОЇ ПЕРЕСТАНОВКИ РЕАЛІЗАЦІЙ ХАОТИЧНИХ СИГНАЛІВ

Для систем зв'язку з кодовим розподілом каналів запропоновано метод формування групового сигналу на основі множини взаємно-ортогональних послідовностей хаотичних реалізацій. З метою підвищення структурної скритності передачі в системі зв'язку пропонується періодично виконувати за деяким законом перестановку ортогональних псевдовипадкових хаотичних послідовностей для кожного індивідуального каналу.

Ключові слова: хаотичний сигнал, ортогональність, конфіденційний, сигнатура, несанкціонований доступ, скритність, канал, захист.

***Корчинский Владимир Викторович**, кандидат технических наук, доцент, кафедра информационной безопасности и передачи данных, Одесская национальная академия связи им. А. С. Попова*

***Корчинський Володимир Вікторович**, кандидат технічних наук, доцент, кафедра інформаційної безпеки та передачі даних, Одеська національна академія зв'язку ім. О. С. Попова*

***Korchinsky Vladimir**, Odessa National Academy of Telecommunications*

УДК 536.248.2

Кравец В. Ю.,
Кравец Д. В.

МЕХАНИЧЕСКИЕ СВОЙСТВА КАПИЛЛЯРНЫХ СТРУКТУР ПРИМЕНИТЕЛЬНО К УСЛОВИЯМ ФУНКЦИОНИРОВАНИЯ В ТЕПЛОВЫХ ТРУБАХ

Представлены результаты исследования предельных механических нагрузок металло-волокнистой капиллярно-пористой структуры из нержавеющей стали в диапазоне пористости от 88 до 99 %. Исследовались на разрыв образцы с диаметрами волокон 8 мкм и 30 мкм. Показано, что на прочность капиллярной структуры влияют как пористость и диаметр волокон, так и температурный диапазон работы в тепловых трубах.

Ключевые слова: *капиллярная структура, предел прочности, предел пропорциональности, тепловая труба.*

1. Введение

Одной из важных характеристик капиллярно-пористых структур, используемых в качестве фитилей тепловых труб, является их механические свойства. В различных условиях эксплуатации пористые структуры могут подвергаться как сжимающим, так и растягивающим воздействиям. Это связано с процессом кипения в зоне нагрева тепловых труб, когда внутри капиллярной структуры активизируются центры парообразования. В процессе возникновения и роста парового пузыря его межфазная поверхность механически воздействует на волокна капиллярной структуры, что, в конечном счете, может привести к их разрушению [1]. Снижение массогабаритных характеристик тепловых труб существенно усложняет выход паровых пузырей из капиллярной