5. Кулаков Ю. А. Иерархический способ планирования для Grid / Ю. А. Кулаков // Вісник НТУУ «КПІ» Інформатика, управління та обчислювальна техніка. – 2011. - № 50. – С. 13-21.
6. Матов О. Я. Перспективні інформаційні технології та розвиток GRID-систем у високопродуктивних глобально-розподілених обчислювальних інфраструктурах корпоративної співпраці / О. Я. Матов, І. О. Храмова // Реєстрація, зберігання і обробка даних. – 2004. - Т. 6, № 1. – С. 85-98.
7. Мухин В. Е. Средства защиты GRID-систем на основе дифференцирования уровня доверия к узлам системы / В. Е. Мухин // Штучний інтелект. – 2008. - №3. – С. 187-196.
8. Про затвердження Державної програми «Інформаційні та комунікаційні технології в освіті і науці» на 2006-2010 роки: Кабінет Міністрів України; Постанова від 07.12.2005 р. № 1153.
9. Про затвердження Державної цільової науково-технічної програми впровадження і застосування грід-технологій на 2009-2013 роки: Кабінет Міністрів України; Постанова від 23.09.2009 р. № 1020.
10. Шелестов А. Ю. Реалізація Grid-інфраструктури для розв'язання задач обробки супутникових даних / А. Ю. Шелестов // Проблеми програмування. - 2006. - № 2-3. - С. 94-101.
11. Шелестов А. Ю. К вопросу информационной безопасности Grid-систем / А. Ю. Шелестов та інші // Наукові праці ДонНТУ. – 2009. - Випуск 10 (153). – С. 121-130.

Розглядається можливість збільшення структурної скритності сигнальних конструкцій, які передаються, сформованих на основі змінної кількості взаємно-ортогональних послідовностей хаотичних реалізацій. Запропонований метод може бути рекомендований для задачі побудови конфіденційної системи зв'язку, в якій необхідно забезпечити високу структурну скритність передачі на рівні фізичного каналу

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

Рассматривается возможность повышения структурной скрытности передаваемых сигнальных конструкций, формируемых на основе переменного количества взаимно-ортогональных последовательностей хаотических реализаций. Предложенный метод может быть рекомендован для задачи построения конфиденциальной системы связи, в которой требуется обеспечить высокую структурную скрытность передачи на уровне физического канала

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

УДК 621.391

МЕТОД ФОРМИРОВАНИЯ СИГНАЛЬНЫХ КОНСТРУКЦИЙ НА ОСНОВЕ МНОЖЕСТВА ВЗАИМНО-ОРТОГОНАЛЬНЫХ ХАОТИЧЕСКИХ СИГНАЛОВ

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

1. Введение

Большинство современных методов защиты информации от несанкционированного доступа (НСД) реализуется на разных уровнях эталонной модели OSI [1,5,6]. Протоколы туннелирования канального уровня PPTP (Point-to-Point Tunneling Protocol), L2F (Layer-2 Forwarding) и L2TP (Layer-2 Tunneling Protocol) предназначены для организации защищенного многопротокольного удаленного доступа к ресурсам корпоративной сети через открытую сеть, например, через Интернет. На сеансовом уровне решается задача формирования защищенных виртуальных сетей с помощью криптографической защиты информационного обмена, включая аутентификацию, а также выполняется ряд функций посредничества между взаимодействующими сторонами. Криптографические методы защиты информации также используются и на некоторых более старших уровнях модели OSI. Они направлены на повышение информационной скрытности конфиденциальных данных сети, которые предназначены для хранения или передачи по каналу связи [5-10].

Не менее важной является задача по защите передаваемой информации от НСД на первом уровне модели OSI [2]. Эта проблема особо актуальна при обеспечении безопасности беспроводной сети (например, для стандарта RadioEthernet), так как на физическом уровне она наиболее уязвима для перехвата передаваемых сообщений средствам НСД [1, 2].

Внедрение явления динамического хаоса в область инфокоммуникационных технологий открыло новые перспективы не только по созданию эффективных систем криптокодирования, но и расширило возможности по синтезу сигнальных конструкций, с помощью которых можно обеспечить потенциально высокую структурную скрытность передачи на уровне физического канала [3]. В работе [4] предложен метод формирования сигнальных конструкций на базе заданного множества взаимно-ортогональных хаотических сигналов. Однако исследования в этом направлении показали новую перспективу по совершенствованию данного метода для задачи повышения структурной скрытности передаваемых сигнальных конструкций.

Целью статьи является разработка метода формирования сигнальных конструкций на основе переменного множества комбинаций взаимно-ортогональных хаотических последовательностей.

2. Метод формирования сигнальных конструкций

Рассмотрим алгоритм повышения структурной скрытности передачи на основе сигнальных конструкций, полученных с помощью некоторого количества взаимно-ортогональных хаотических сигналов, взятых из некоторого заданного множества F. В качестве исходного множества носителей F будут использоваться взаимно-ортогональные реализации хаотического процесса $c_1(t), c_2(t), \ldots, c_L(t)$, т.е.

$$\int c_i(t)c_{i+1}(t)dt = 0. \quad (1)$$

В алгоритме [4] для усложнения задачи распознавания параметров сигнальной конструкции в случае перехвата сообщения средствами НСД её формирование осуществлялось в два этапа. Сначала из L последовательностей множества $F(c_i)$ с учетом вектора текущего ключа A_k выбирается одна из последовательностей $c_i(t)$, с помощью которой на длительности элементарной посылки информационного сигнала t_0 формируется сигнальная конструкция

$$X_i(t_0) = x_k(t)c_k(t), \quad (2)$$

где $c_k(t)$ – ортогональная последовательность под номером k.

Например, пусть длина вектора ключа A_k =5 и состоит из пяти двоичных элементов. Для упрощения примера допустим, что длина вектора A_k совпадает с числом L. Тогда, если $A_k = \{10000\}$, выбирается первая последовательность $c_{k=1}(t)$. Остальные $L-1$ последовательности $c_2(t), c_3(t), c_4(t), c_5(t)$ используются для завершения процедуры синтеза сигнальной конструкции

$$Y_K(t) = x_k(t)c_1(t) + \sum_{i=2}^{L} c_i(t). \quad (3)$$

Частотно-временное представление формируемой сигнальной конструкции показано на рис. 1.

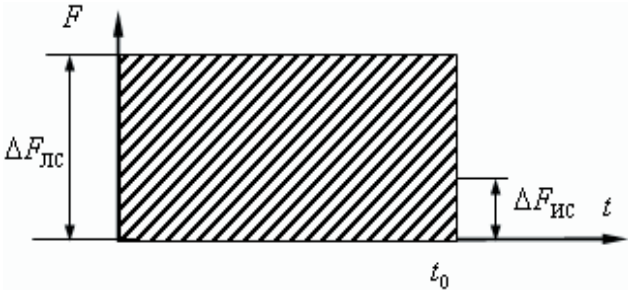

Рис. 1. Частотно-временное представление сигнальной конструкции

В этом алгоритме количество N сигнальных конструкций $Y_K(t)$, которое можно получить на основе множества F, определяется числом L. Очевидно, что для повышения структурной скрытности передачи система связи должна манипулировать как можно с большим количеством сигналов с изменяемыми во времени параметрами. Чтобы увеличить множество формируемых сигнальных конструкций $Y(t)$ предлагается использовать переменное количество ортогональных сигналов

$$N' = \sum_{i=1}^{L} C_i^1. \quad (4)$$

На рис. 2 показаны зависимости множества сигнальных конструкций N и N' от числа используемых ортогональных последовательностей хаотических реализаций L. По этой зависимости видно, что процедура комбинирования количеством c_i для формирования $Y_K(t)$ позволяет существенно увеличить множество формируемых сигнальных конструкций, т.е. $N' >> N$.

Рассмотрим процесс распознавания сигнала $x_k(t)$ из $Y_k(t)$ при условии, что на перовом этапе формирования этой сигнальной конструкции использовалась ортогональная последовательность под номером k. В приемнике сигнал $x_k(t)$ можно разделить, используя условие ортогональности (1):

$$\begin{aligned} x_k(t) &= \int_0^{t_0} Y_k(t)c_k(t)dt = \\ &= \int_0^{t_0} \left[X_1(t) + X_2(t) + \ldots + X_L(t)\right]c_k(t)dt = \\ &= \int_0^{t_0} \left[x_1(t)c_1(t) + \ldots + x_k(t)c_k(t) + \ldots + x_L(t)c_L(t)\right]c_k(t)dt. \end{aligned} \quad (5)$$

В рассматриваемом алгоритме только сигнал $x_k(t)$ является информационным, а остальные $x_i(t)$ равны единице. Если $x_i(t)$ задавать случайные значения бинарной последовательности, то существенно усиливается эффект по маскировке передаваемого информационного сигнала $x_k(t)$.

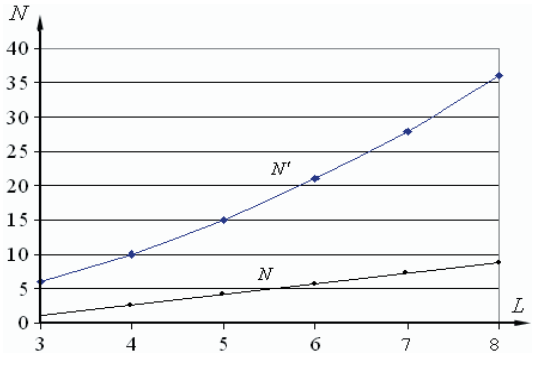

Рис. 2. Зависимость множества формируемых сигнальных конструкций N и N′ от числа L

В (5) с учетом условия (1) произведение $x_i(t)\times c_i(t)\times c_k(t)=0$,
тогда

$$x_k(t)=\int_0^{t_0} x_k(t)c_k{}^2(t)dt. \qquad (6)$$

Обычно $x_K(t)\approx x_K=\text{const}$ за время передачи t_0. Тогда

$$\int_0^{t_0} x_k(t)c_k^2(t)dt\approx x_k(t)\int_0^{t_0} c_k^2(t)dt=x_k(t). \qquad (7)$$

Данный алгоритм реализуется канальным корреляторо м (КК) [2] (рис. 3)

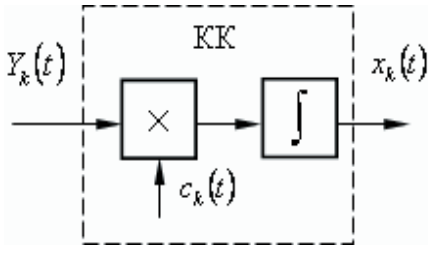

Рис. 3. Схема канального коррелятора

На рис. 4 представлена структурная схема предлагаемой конфиденциальной системы передачи, для правильной работы которой необходимы наличие системы синхронизации и согласованная смена ключей в передатчике и приемнике. Выбор комбинации ортогональных последовательностей осуществляется с помощью коммутатора с учетом ключа A_k на текущий сеанс передачи.

Сформированный сигнал $Y_K(t)$ поступает на ГУ, а затем в линию связи (ЛС). В ГУ осуществляется согласование сигнала $Y_K(t)$ со средой передачи, а также, если в системе связи не используется прямохаотическая передача [3], то может выполняться повторная модуляция сигнала $Y_K(t)$ с помощью носителя $\psi(t)$.

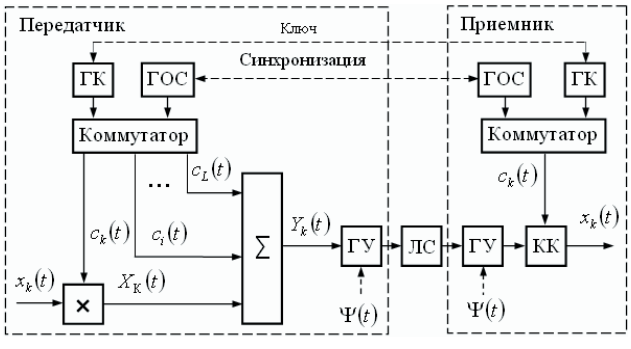

Рис. 4. Структурная схема системы с ХС: ГОС – генератор ортогональных сигналов; × – схема умножения; ГУ – групповое устройство; ГК – генератор ключей; Σ – сумматор

3. Выводы

В заключение можно сделать следующие выводы.

В данной статье разработан метод формирования сигнальных конструкций на основе переменного множества комбинаций взаимно-ортогональных хаотических последовательностей.

Данный метод может быть рекомендован для задачи построения конфиденциальной системы связи, в которой требуется обеспечить высокую структурную скрытность передачи на уровне физического канала.

Литература

1. Шаньгин, А.И. Информационная безопасность компьютерных систем и сетей [Текст] / А.И. Шаньгин. – М.: ИД «Форум»: ИФРА-М, 2008. – 416 с.
2. Куприянов, А.И. Теоретические основы радиоэлектронной борьбы [Текст] / А. И. Куприянов, А. В. Сахаров. – М.: Вузовская книга, 2007. – 356 с.
3. Гуляев, Ю.В. Информационные технологии на основе динамического хаоса для передачи, обработки, хранения и защиты информации / [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. – Харьков: Технологический центр, 2013. – № 1/9 (61). – С.53.
5. D. Richard Kuhn, Thomas J. Walsh, Steffen Fries. «Security Considerations for Voice Over IP Systems». Recommendations of the National Institute of Standards and Technology. – NIST SP 800-58, January 2005. – S. 93.
6. Recomendation CCITT X.200. Reference Model of open systems interconnection for CCITT applications. Geneva, 1991; Стандарт ISO 7498-1:1984. Базова модель ВВС. – С. 31.

7. Carvalho, M. Using Mobile Agents as Roaming Security Guards to Test and Improve Security of Hosts and Networks [Текст] / Carvalho M., Cowin T., Suri N., Breedy M., Ford K. // Proceedings of the 2004 ACM Symposium on Applied Computing (SAC'04). – **ACM**. – 2004.
8. Pedireddy, T. A Prototype Multi Agent Network Security System [Текст] / Pedireddy T., Vidal J. // Proceedings of the AAMAS'03. – **ACM**. – 2003.
9. Menezes, R. Self-Organization and Computer Security [Текст] / Menezes R. // Proceedings of the 2005 ACM Symposium on Applied Computing (SAC'05). – **ACM**. – 2005.
10. Valeyev S.S. Multiagent Technology and Information System Security [Текст] / S.S.Valeyev, T.K. Bakirov, D.N. Pogorelov, I.V. Starodumov // Proceedings of the 7th International Workshop on Computer Science and Information Technologies CSIT'2005. – Vol.1, Ufa, Russia, 2005. – P. 195-200.

Проведено комп'ютерне моделювання різних методів модуляції та демодуляції для системи передачі інформації. Визначено якісні характеристики в умовах впливу адитивного білого гаусового шуму. Зроблені рекомендації щодо використання методів для умов метеорного каналу

Ключові слова: цифрова модуляція, АБГШ, метеорна система передачі інформації

Проведено компьютерное моделирование различных методов модуляции и демодуляции для системы передачи информации. Определены качественные характеристики в условиях влияния аддитивного белого гауссового шума. Сделаны рекомендации по использованию методов для условий метеорного канала

Ключевые слова: цифровая модуляция, АБГШ, метеорная система передачи информации

УДК 621.391

ИССЛЕДОВАНИЕ ЦИФРОВЫХ МЕТОДОВ МОДУЛЯЦИИ ДЛЯ МЕТЕОРНОЙ СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

А. В. Воргуль
Кандидат технических наук, доцент*
E-mail: alvorgul@gmail.com
Ю. Х. Сулейман
Аспирант*
*Кафедра основ радиотехники
Харьковский национальный университет радиоэлектроники
пр. Ленина, 14, г. Харьков, Украина, 61166

1. Введение

Целью работы является проверка в ходе компьютерного моделирования характеристик цифровой системы передачи информации (ЦСПИ) в целом в случае использования разных методов модуляции.

В качестве методов модуляций рассматривается амплитудная манипуляция (АМ), амплитудная манипуляция с подавленной несущей (БАМ), частотная манипуляция (ЧМан), минимальная частотная манипуляция (МЧМ), фазовая манипуляция (ФМан), квадратурная манипуляция.

В качестве проверяемых характеристик рассматривается доля ошибочно принятых бит (bit error rate – BER), дисперсия ошибки на входе квантователя, скорость модуляции [1–3], полоса частот, занимаемая модулированным сигналом при заданной полосе информационного сигнала.

2. Моделируемая ЦСПИ

Структурная схема части ЦСПИ, рассматриваемая в работе, имеет вид, рис. 1 [4]:

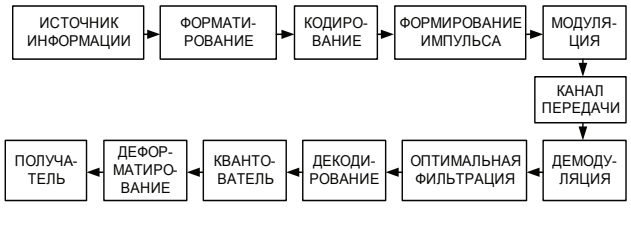

Рис. 1. Структурная схема исследуемой цифровой системы передачи информации

Согласно структурной схеме, выходной сигнал блока «источник информации» представляет собой поток битов. Формирователь преобразует битовый поток в последовательность символов. Число битов на один