7. Яремчук Ю.Є. Методи автентифікації на основі рекурентних послідовностей / Ю.Є. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Випуск 1(25), 2013. – С. 39–49.

8. El Gamal, T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms / T. ElGamal // Advances in Cryptology: Proceedings of CRYPTO 84. – Springer Verlag, 1985. – P. 1–18.

Надійшла: 22.08.2013р Рецензент: д.т.н., проф. Ленков С.В

УДК 621.391

Корчинский В.В., Казакова Н.Ф.

УСЛОВИЕ ОБЕСПЕЧЕНИЯ ЭНЕРГЕТИЧЕСКОЙ СКРЫТНОСТИ ХАОТИЧЕСКИХ СИГНАЛОВ ПРИ ПЕРЕДАЧЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Рассмотрено условие обеспечения энергетической скрытности передачи конфиденциальной системы связи на основе сигнальных конструкций реализаций динамического хаоса. Показана возможность использования многоуровневых последовательностей в качестве расширяющих последовательностей информационного сигнала для повышения скрытности передачи. Проведено имитационное моделирование системы связи с хаотическими сигналами.

Ключевые слова: *с*крытность, база, канал, хаос, сигнал, сигнатура.

Обзор проблемы и постановка задачи. Одним из наиболее важных требований, предъявляемых к конфиденциальной системе связи (КСС) является обеспечение заданной помехозащищенности, которая характеризует способность системы выполнять свои задачи с заданным качеством в условиях радиоэлектронного подавления (РЭП) и несанкционированного доступа (НСД) [1]. РЭП и НСД организуется радиотехнической разведкой (РР) противоборствующей стороны, которая включает три основные задачи: обнаружения факта работы КСС; идентификация структуры и параметров сигналов-переносчиков; раскрытие смыслового содержания перехваченного сообщения.

Способность КСС противостоять мерам радиотехнической разведки (РР) называется скрытностью, которая является одним из главных показателей помехозащищенности. В соответствии с задачами радиоразведки выделяют следующие основные виды скрытности: энергетическая, структурная и информационная [1]. Другим важным показателем помехозащищенности является помехоустойчивость, которая характеризуется способностью системы связи нормально функционировать, выполняя задачи по приему информации в условиях действиях радиопомех, в том числе, преднамеренных.

Энергетическая скрытность направлена на существенное затруднение обнаружения сигнала работающей КСС средствами РЭП (разведывательным приемным устройством). Данный вид скрытности в основном обеспечивается за счет энергетической скрытности сигналов-переносчиков с базой $B >> 1$. Так в технологии многостанционного доступа с кодовым разделением каналов (Code Division Multiple Access – CDMA) для этой цели применяются шумоподобные сигналы (ШПС), формируемые на основе двоичных расширяющих последовательностей Уолша – метод DSSS (Direct Sequence Spread Spectrum). При этом закономерно, что увеличение энергетической скрытности передачи достигается за счет большей базы сигнала-переносчика, т.е. чем больше распределение энергии сигнала в большей полосе частот, тем меньше вероятность её обнаружения разведывательным приемным устройством РЭП на фоне помех.

В случае перехвата сообщения структурная скрытность направлена на затруднение измерения параметров сигнала-переносчика и идентификации структуры сигнала. Для повышения структурной скрытности целесообразно применение сигналов со сложной и изменяемой структурой, что даёт возможность, в перспективе, создавать сигналы-

переносчики с криптозащищенной структурой уже на первом уровне модели OSI. Одним из путей решения данной проблемы является использование широкополосных сигналов на основе реализаций шумового сигнала (например, динамического хаоса) [3]. В работах [4,5] для построения КСС показаны возможности по формированию множеств сигнальных конструкции с помощью шумовых сигналов, которые для противника являются сигналами с неизвестной структурой, поэтому потенциально могут обеспечивать высокую структурную скрытность, а также сохраняют свойство по обеспечению энергетической скрытности аналогично шумоподобным сигналам на основе двоичных последовательностей в системе CDMA.

Информационная скрытность в основном реализуется на верхних уровнях модели OSI и требует применения криптографической системы [2].

В данной работе в качестве расширяющих последовательностей используются многоуровневые псевдослучайные последовательности, сформированные на основе шумового сигнала, выбор которых осуществляется случайным образом методом перебора с требуемыми спектральными свойствами. Данная методика выбора рассмотрена при построении конфиденциальных систем связи в работах [4,5,8]. В [6] показано, что использование многоуровневых последовательностей по сравнению с двоичными сигналами в системах с прямым расширением спектра существенно увеличивает структурную скрытность передаваемых сигнальных конструкций.

Очевидно, что обеспечение энергетической скрытности шумового сигнала с прямым расширением спектра обосновано при условии, что полезный уровень передаваемого сигнала соизмерим с уровнем шума или меньше его, т.е. соотношение сигнал/шум $h^2 \le 1$. Тогда работа станции РЭП по обнаружению передаваемого сигнала будет существенно затруднена. Однако при $h^2 \to 0$ необходимо иметь представление о возможности системы обеспечить требуемую помехоустойчивость с учетом значения базы широкополосного сигнала B. Из вышесказанного следует, что актуальным для противодействия РР являются исследования по созданию методов передачи, которые обеспечивают повышение различных показателей скрытности.

Целью статьи является оценка взаимосвязи энергетической скрытности передачи и помехоустойчивости при различных значениях базы шумового сигнала. В качестве инструмента исследования выбран метод имитационного моделирования.

Методы модуляции на основе широкополосных хаотических сигналов. Рассмотрим шумовой сигнал на основе динамического хаоса. Формирование хаотических сигналов может быть реализовано аппаратным или программным способом с помощью соответствующих генераторов. Небольшие изменения параметров или начальных значений генератора приводят к существенному изменению формы генерируемого колебания, что дает возможность формирования и выбора различных реализаций хаотического процесса.

В работе используется программный способ генерирования хаотического колебания x_n, который может быть реализован в соответствии с некоторым разностным уравнением

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

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

$$dx(t)\big/dt = F\left[x(t); m\right], \tag{2}$$

где F нелинейный оператор; m – управляющий параметр.

Формирование хаотического сигнала осуществимо с помощью простейшего математического выражения [2]

$$x_{n+1} = a x_n \left(1 - x_n\right), \tag{3}$$

где a − управляющий параметр. На рис. 1 приведена центрированная реализация сигнала $x(t)$ на выходе генератора хаоса (3) при начальном значении $x_{n=0}$ = 0,5 и a = 3,9, который по своему алгоритму функционирования является детерминированным устройством.

Формируемые по такому алгоритму колебания обладают всеми свойствами шумоподобного сигнала, так как для них характерно:

1) непериодичность траекторий во времени;
2) экспоненциально спадающая корреляционная функция;
3) сплошной непрерывный спектр мощности.

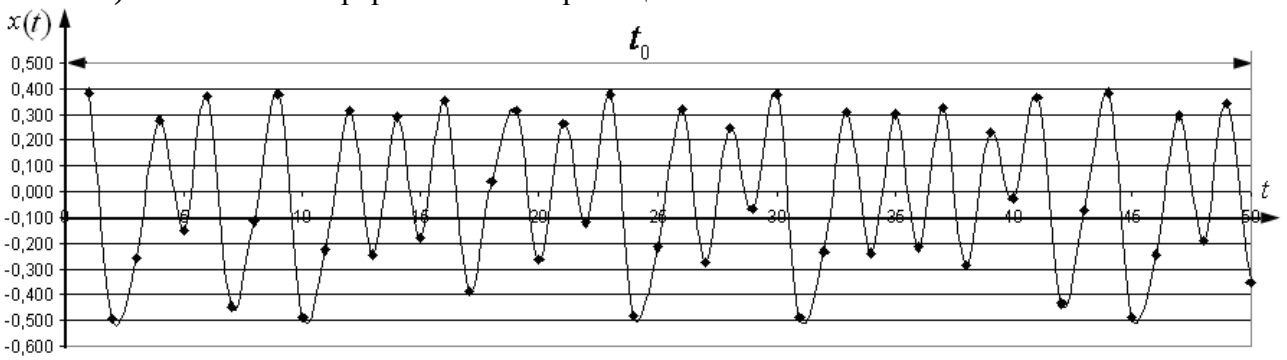

Рис. 1. Реализация хаотического сигнала $x(t)$

Среди методов модуляции сигнала на основе широкополосных хаотических сигналов можно выделить [4]:

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

2) переключение хаотических режимов – двоичный символ информационного сигнала «1» кодируется одним типом хаотического сигнала, а символ «0» – другим;

3) инвертирование хаотических сигналов – двоичный символ информационного сигнала «1» кодируется реализацией хаотического сигнала, а символ «0» – той же реализацией, но с инвертированием значений отсчетов сигнала.

Имитационное моделирование и результаты. Рассмотрим прямохаотическую систему связи. Для задачи исследования хаотический сигнал $x(t)$ предварительно проходит дискретизацию по времени (использована теорема отсчетов), квантование по уровню (в эксперименте использовалось 256 уровней) и преобразовывается в многоуровневую кодовую последовательность x_n. Кодовая последовательность x_n разбивается на сегменты определенной длины s=32, 63, 126, 256, 512, 1024 элементов (чипов), которые будут использоваться в качестве сигнатур, а также представляют собой базу расширяющей последовательности B.

Формирование сигнала в одноканальной системе (рис. 2) осуществляется путем замены единичных информационных посылок $a(t)$ сигнатурой $s(t)$ с инвертированием реализаций хаотического сигнала при передаче «1» и «−1», т.е.

$$x(t) = s(t) \times a(t). \quad (4)$$

Использование прямой и инвертированной сигнатуры обеспечивает не только определение полярности передаваемых посылок, но и позволяет регистрировать их передние и задние фронты при корреляционном приеме. С целью обеспечения эффективности корреляционного приема система связи должна быть обеспечена надежной синхронизацией.

Рассмотрим канал связи с аддитивной помехой ξ(t), представляющую собой случайную величину с нормальным законом распределения. Тогда на входе приёмника КСС будет наблюдаться случайный процесс

$$y(t) = x(t) + \xi(t). \quad (5)$$

Сигналы, излучаемые передатчиком КСС, также поступают на вход разведывательного приёмника станции РЭП, который производит их поиск, обнаружение и

оценивание. Будем считать, что энергетическая скрытность передаваемых хаотических сигналов может быть обеспечена при условии $h^2 \le 1$, а увеличение её происходит, если $h^2 \to 0$. Однако, при выполнении этого условия важно знать возможности КСС по обеспечению требуемой помехоустойчивости. Методом имитационного моделирования были получены зависимости вероятности ошибочного приема информационного элемента p_0 при различных значениях базы расширяющей последовательности многоуровневого сигнал B и h^2 (рис. 3).

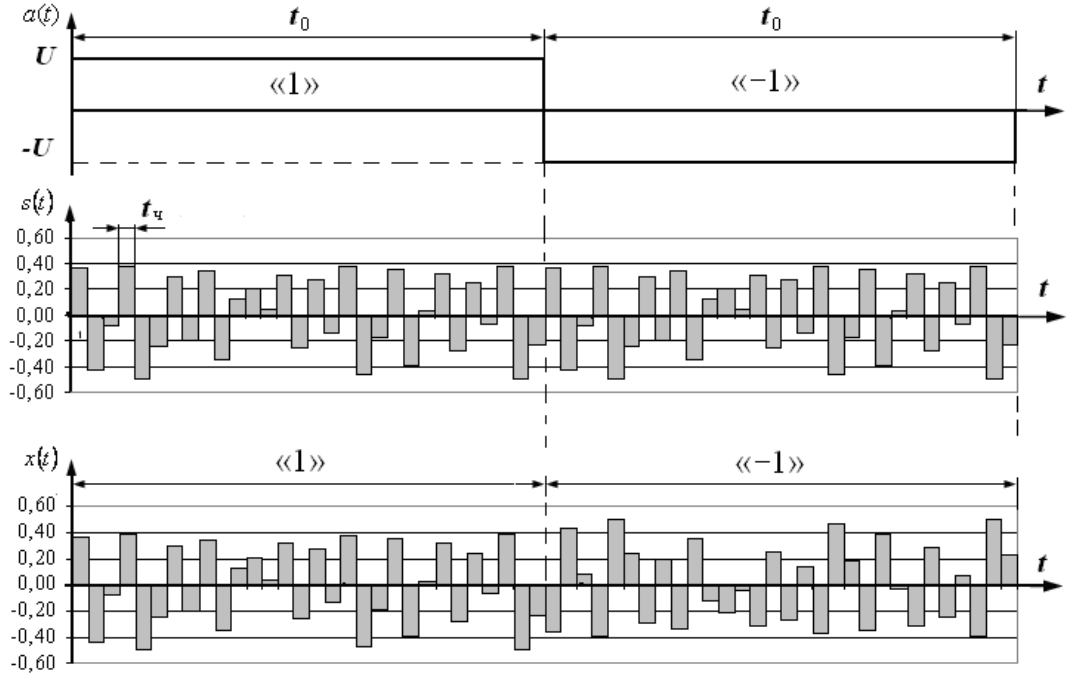

Рис. 2. Кодирование двоичной информационной последовательности $a(t)$ с помощью расширяющей многоуровневой последовательности $s(t)$

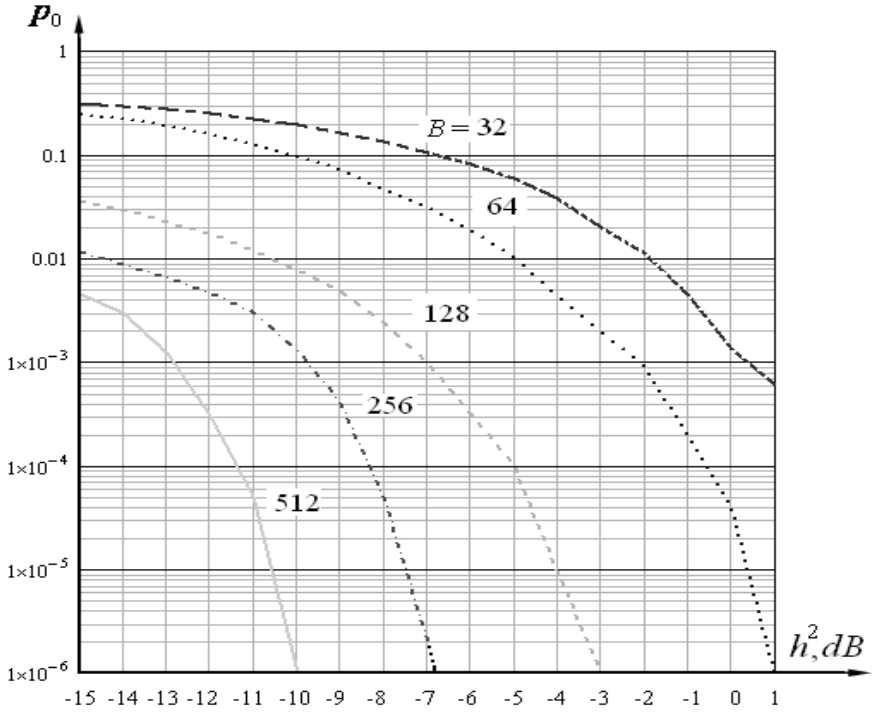

Рис. 3. Зависимость вероятности ошибочного элемента p_0 от соотношения h^2 при различных значениях базы B расширяющей последовательности

Результаты моделирования показали, что высокая энергетическая скрытность передачи ($h^2 \le -10$дБ) может быть достигнута при достаточно больших значениях базы, т.е. $B \to \infty$, что, с одной стороны, усложняет приемо-передающую аппаратуру, однако, с другой стороны, обеспечивает возможность КСС эффективно противодействовать радиотехнической разведке. Кроме этого большее значение базы сигнала обеспечивает лучший выигрыш по соотношению сигнал/шум на выходе корреляционного приемника, что повышает помехоустойчивость передачи. Так при B=32 и h=–5дБ вероятность $p_0=5\cdot10^{-2}$ может быть снижена до значения $2\cdot10^{-3}$ без применения помехоустойчивого кодирования, а только за счет базы B=128. Особый эффект достигается при значении B=256 и выше. Следует отметить, что такой выигрыш от увеличения базы происходит за счет ухудшения показателя частотной эффективности канала, так как спектр такого сигнала будет занимать большую полосу частот.

Выводы. Результаты исследований показали целесообразность использования в КСС методов передачи, основанных на хаотических сигналах, так при этом могут быть обеспечены высокие показатели, как энергетической скрытности, так и структурной. Характерна противоположная взаимосвязь между показателями энергетической скрытности и помехоустойчивости, так как улучшение одного показателя приводит к ухудшению другого. Поэтому при выборе параметров передачи КСС необходим компромисс между условием обеспечения качества передачи и скрытности. Возможным вариантом повышения скрытности передачи при сохранении требуемой помехоустойчивости может быть использование в системе помехоустойчивого кодирования.

ЛИТЕРАТУРА

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

2 Шаньгин А.И. Информационная безопасность компьютерных систем и сетей / 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 / [Ю.В. Гуляев, Р.В. Беляев, Г.М. Воронцов и др.] // Радиотехника и электроника. – 2003. – Т. 48. – № 10. – С. 1157–1185.

4. Корчинський В.В. Модель шумового сигнала для передачи конфиденциальной информации // Вестник НТУ «ХПИ» – Харьков, 2013. – № 11(985). – С. 89-94.

5. Корчинський В.В. Метод моделирования шумовых сигналов для систем передачи конфиденциальной информации // Вестник НТУ «ХПИ» – Харьков, 2013. – № 38(1011). – С. 99-104.

6. Корчинський В.В. Оценка структурной скрытности сигнальных конструкций на основе хаотических сигналов в системах передачи конфиденциальной информации / Корчинський В.В. // Збірник наукових праць ОНАЗ ім. О. С. Попова. –2012. – № 2. – С. 77-81.

7. Корчинский В.В. Повышение структурной скрытности передачи систем с хаотическими сигналами / В.В. Корчинский // Восточно-Европейский журнал передовых технологий //научный журнал. – Харьков: Технологический центр, 2013. – № 1/9 (61). – С.53.

8. Захарченко, Н. В. Многопользовательский доступ в системах передачи с хаотическими сигналами / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Восточно-Европейский журнал передовых технологий. – 2011. – № 5/9(53). – С. 26–29.

Надійшла: 12.10.2013р. Рецензент: д.т.н., професор Олійник В.Ф.