

## СКРЫТНОСТЬ ПЕРЕДАЧИ В СИСТЕМАХ СВЯЗИ С ХАОТИЧЕСКИМИ СИГНАЛАМИ

*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.* Скрытность, база, канал, хаос, сигнал, сигнатура

M.V. ZAKHARCHENKO, S.M. HOROKHOV, V.V. KORCHYNSKII, B.K. RADZYMOVSKI

Odessa National Academy of Telecommunications named after O.S.Popov

### STEALTH OF TRANSMISSION IN COMMUNICATION SYSTEMS WITH CHAOTIC SIGNALS

*The condition of ensuring energy stealth transmission of confidential communications system based on the signal designs implementations of dynamic chaos is considered. The possibility of using multi-level sequences as the spreading sequence of information signal to improve the stealth of transmission is shown. Simulation modeling of communication systems with chaotic signals is conducted.*

**Keywords.** Stealth, base, channel, chaos, signal, signature

#### Вступление

Актуальным направлением современной науки и техники является исследование конфликта информационных систем и, в частности, радиотехнических систем. С учетом выполняемых задач радиотехнические системы можно классифицировать на три основных класса: системы разрушения информации, системы несанкционированного доступа и конфиденциальные системы связи [ ]. Системы разрушения информации специально организуются противником в процессе радиоэлектронного противодействия (РЕП) с целью постановки преднамеренных помех, имитации ложных информационных сигналов и др. Системы несанкционированного доступа (НСД) решают задачи по несанкционированному перехвату передаваемых сообщений, определению структуры и параметров сигналов, дешифрированию криптотекстов и т.д.

#### Обоснование требования по обеспечению энергетической скрытности передачи

С учетом противоречивости информационного конфликта к конфиденциальной системе связи (КСС) предъявляется важное требование по обеспечению заданной помехозащищенности, которая характеризует способность системы выполнять свои задачи с заданным качеством в условиях радиоэлектронного подавления и несанкционированного доступа [1].

Одним из важных показателей помехозащищенности является скрытность. В соответствии с задачами радиотехнической разведки различают энергетическую, структурную, информационную и другие виды скрытности [1,2]. Не менее важным показателем помехозащищенности является помехоустойчивость, которая характеризуется способностью системы связи нормально функционировать, выполняя задачи по приему информации в условиях действий радиопомех, в том числе, преднамеренных.

Качество защиты передаваемой информации от средств НСД на уровне физического канала оценивается показателем энергетической скрытности [1], который характеризует способность системы противостоять действиям РЕП и НСД, направленным на обнаружение самого факта передачи сигнала и его перехвата. Известно [1,3], что перспективным решением проблемы энергетической скрытности являются методы передачи с помощью шумоподобных сигналов, при формировании которых осуществляется преднамеренное расширение спектра информационного сигнала: псевдослучайная перестройка рабочей частоты (ППРЧ) (FHSS – Frequency Hopping Spread Spectrum); расширение спектра методом прямой последовательности (ПСП) (DSSS – Direct Sequence Spread Spectrum) и др. Первоначально системы связи на основе ППРЧ и ПСП применялись после второй мировой войны в военных целях странами СССР и США для решения различных задач разведывательного характера. В настоящее время эти методы передачи заложены при построении современных коммерческих систем связи многопользовательского доступа.

Одним из путей решения проблемы обеспечения энергетической скрытности 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 конструкций 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.

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  $h^2 \leq 1$ . Тогда работа станции РЭП по обнаружению передаваемого сигнала будет существенно затруднена. Однако при  $h^2 \rightarrow 0$  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.

### Аналитическая часть исследования

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

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

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

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

где  $F$  – нелинейный оператор;  $m$  – управляющий параметр.

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

$$x_{n+1} = ax_n(1 - x_n), \quad (3)$$

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

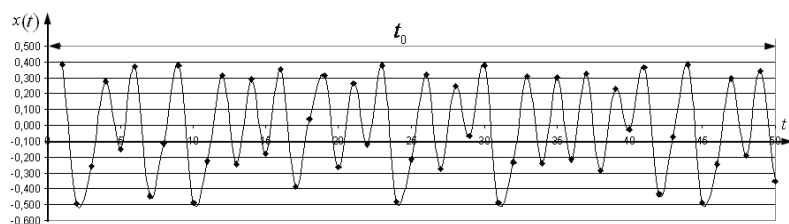


Рис. 1. Реализация хаотического сигнала  $x(t)$

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.

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  $\xi(t)$ , представляющую собой случайную величину с нормальным законом распределения. Тогда на входе приёмника КСС будет наблюдаться случайный процесс

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

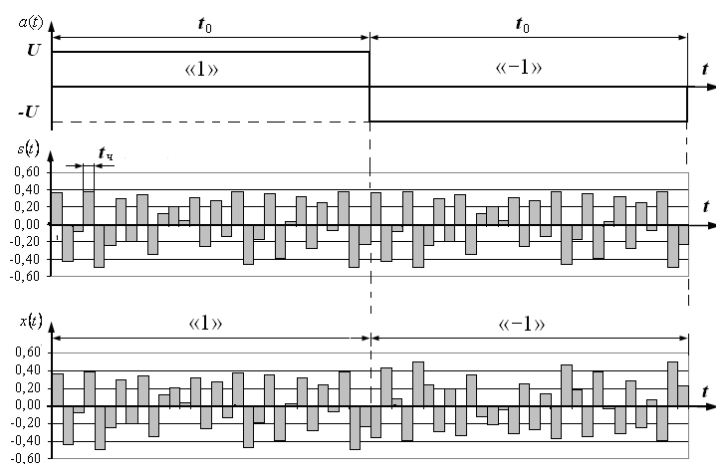


Рис. 2. Кодирование двоичной информационной последовательности  $a(t)$  с помощью расширяющей многоуровневой последовательности  $s(t)$

расширяющей последовательности многоуровневого сигнала с  $B$  и  $h^2$  (рис. 3).

Результаты моделирования показывают, что высокая энергетическая скрытность передачи ( $h^2 \leq -10$  дБ) может быть достигнута при достаточно больших значениях базы, т.е.  $B \rightarrow \infty$ , 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  $h=-5$  дБ вероятность  $p_0=5 \cdot 10^{-2}$  может быть снижена до значения  $2 \cdot 10^{-3}$  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.

Представляет интерес оценка возможностей по обеспечению скрытности передачи на основе хаотических сигналов с большими значениями базы  $B \geq 1000$ . Рассмотрим систему связи с бинарной фазовой модуляцией (ФМ-ПСП) при гауссовой шумовой помехе в канале и корреляционном методе приема. Если на интервале времени  $t_0 T_c$ , соответствующей передаче одного бита данных, передается  $N_c$  элементов ПСП, то соотношение сигнал/шум  $h^2$  на бит на выходе коррелятора увеличивается в  $B = N$  раз. Вероятность  $p_0$  зависит от  $h^2$  и определяется известной формулой

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  $h^2 \leq 1$ , а увеличение её происходит, если  $h^2 \rightarrow 0$ . 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

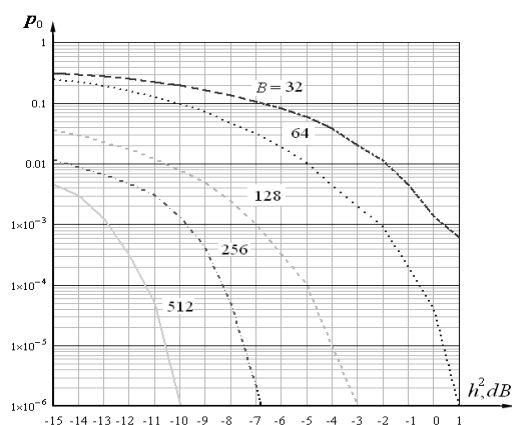


Рис. 3. Зависимость  $p_0$  от  $h^2$  при различных значениях базы  $B$  расширяющей последовательности

$$p_0 = 0,5 - \Phi_0(\sqrt{2}h), \quad (6)$$

где  $\Phi_0(z)$  – интеграл вероятности.

На рис. 4 представлены зависимости вероятности  $p_0$  в зависимости от базы сигнала. Из зависимостей видно, что вероятность ошибки не зависит от структуры ПСП, а только от базы сигнала. Уменьшить вероятность ошибки возможно путем применения помехоустойчивого кодирования. Преимущество синтезированных в работе хаотических сигналов заключается в значительном повышении их структурной скрытности.

#### Выводы

Результаты исследований показывают 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 достоверности передачи и скрытности. Повышение скрытности передачи при сохранении требуемой достоверности может быть достигнуто за счёт помехоустойчивого кодирования.

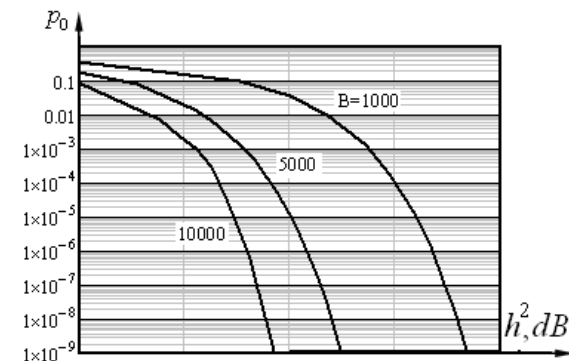


Рис. 4. Графики зависимости вероятности ошибки на бит в зависимости от базы сигнала

#### Литература

1. Куприянов А.И. Теоретические основы радиоэлектронной борьбы / А. И. Куприянов, А. В. Сахаров. – М.: Вузская книга, 2007. – 356 с.
2. 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. Корчинский В.В. Модель шумового сигнала для передачи конфиденциальной информации // Вестник НТУ «ХПИ» – Харьков, 2013. – № 11(985). – С. 89-94.
5. Корчинский В.В. Метод моделирования шумовых сигналов для систем передачи конфиденциальной информации // Вестник НТУ «ХПИ» – Харьков, 2013. – № 38(1011). – С. 99-104.
6. Корчинский В.В. Оценка структурной скрытности сигнальных конструкций на основе хаотических сигналов в системах передачи конфиденциальной информации / Корчинский 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.

#### References

1. Kuprijanov A.I. Teoreticheskie osnovy radiojelektronnoj bor'by / A. I. Kuprijanov, A. V. Saharov. – M.: Vuzovskaja kniga, 2007. – 356 s.
2. Shan'gin A.I. Informacionnaja bezopasnost' komp'juternyh sistem i setej / A.I. Shan'gin. – M.: ID «Forum»: IFRA-M, 2008. – 416 s.
3. Guljaev Ju.V. Informacionnye tehnologii na osnove dinamicheskogo haosa dlja peredachi, obrabotki, hranenija i zashhity informacii / [Ju.V. Guljaev, R.V. Beljaev, G.M. Voroncov i dr.] // Radiotekhnika i jelektronika. – 2003. – T. 48. – № 10. – S. 1157–1185.
4. Korchinsk'ij V.V. Model' shumovogo signala dlja peredachi konfidencial'noj informacii // Vestnik NTU «HPI» – Har'kov, 2013. – № 11(985). – S. 89-94.
5. Korchinsk'ij V.V. Metod modelirovanija shumovyh signalov dlja sistem peredachi konfidencial'noj informacii // Vestnik NTU «HPI» – Har'kov, 2013. – № 38(1011). – S. 99-104.
6. Korchinsk'ij V.V. Ocenka strukturnoj skrytnosti signal'nyh konstrukcij na osnove haoticheskikh signalov v sistemah peredachi konfidencial'noj informacii / Korchinsk'ij V.V. // Zbirnik naukovih prac' ONAZ im. O. S. Popova. – 2012. – № 2. – S. 77-81.
7. Korchinskij V.V. Povyshenie strukturnoj skrytnosti peredachi sistem s haoticheskimi signalami / V.V. Korchinskij // Vostochno-Evropejskij zhurnal peredovyh tehnologij // nauchnyj zhurnal. – Har'kov: Tehnologicheskij centr, 2013. – № 1/9 (61). – S.53.
8. Zaharchenko, N. V. Mnogopol'zovatel'skij dostup v sistemah peredachi s haoticheskimi signalami / N. V. Zaharchenko, V. V. Korchinskij, B. K. Radzimovskij // Vostochno-Evropejskij zhurnal peredovyh tehnologij. – 2011. – № 5/9(53). – S. 26–29.

Рецензія/Peer review : 10.7.2013 р.

Надрукована/Printed : 17.10.2013 р.