Дана оцінка структурної скритності таймерних сигнальних конструкцій. Проведено розрахунок структурної скритності шумоподібної псевдовипадкової послідовності в поєднанні з таймерними сигналами в системах з кодовим розділенням каналів

Ключові слова: структурна скритність, таймерний сигнал, сигнатура

Дана оценка структурной скрытности таймерных сигнальных конструкций. Проведен расчет структурной скрытности шумоподобной псевдослучайной последовательности в сочетании с таймерными сигналами в системах с кодовым разделением каналов

Ключевые слова: структурная скрытность, таймерный сигнал, сигнатура

Evaluation of structural secrecy of timer signal constructions was given. Calculation of structural secrecy noise-like pseudo-random sequence in combination with timer signals in the system with code division multiple access was made

Keywords: structural secrecy, timer signal, signature

УДК 691.321.25

СТРУКТУРНАЯ СКРЫТНОСТЬ ТАЙМЕРНЫХ СИГНАЛОВ В СИСТЕМАХ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ

Н.В. Захарченко
Доктор технических наук, профессор, проректор по учебной работе*

В.В. Корчинский
Кандидат технических наук, доцент*
Контактный тел.: (048) 788-3-582

Б.К. Радзимовский
Преподаватель*
*Кафедра информационной безопасности и передачи данных
Контактный тел. (048) 731-73-55
Одесская национальная академия связи им. А. С. Попова
ул. Кузнечная, 1, г. Одесса, Украина, 65029

1. Введение

Одним из наиболее важных параметров, характеризующих системы передачи информации с шумоподобными сигналами, в том числе с кодовым разделением каналов (КРК), является помехозащищенность, которая определяет способность системы противостоять воздействию помех и включает в себя понятие скрытности и помехоустойчивости [1].

Способность системы противостоять действиям, направленным на обнаружение сигнала и измерение его параметров, определяется скрытностью, а способность системы работать с заданным качеством в условиях воздействия различного рода помех – помехоустойчивостью.

Скрытность сигналов можно классифицировать как энергетическую, структурную и информационную [1].

Энергетическая скрытность характеризует способность системы противостоять мерам, направленным на обнаружение сигнала.

Структурная скрытность характеризует способность противостоять мерам несанкционированного доступа, направленным на раскрытие сигнала при условии, что сигнал уже обнаружен. Это означает распознавание формы сигнала и измерение его параметров, т. е. отождествление обнаруженного сигнала с одним из множества априорно известных сигналов.

Информационная скрытность определяется способностью противостоять мерам, направленным на раскрытие смысла передаваемой с помощью сигналов информации [1].

Метод определения потенциальной структурной скрытности сигналов, не требующий знания алгоритмов обработки на станции несанкционированного доступа, изложен в работе [2]. Структурная скрытность определяется числом двоичных измерений (д.из), которые необходимо осуществить для раскрытия структуры сигнала. Общее выражение для потенциальной скрытности имеет вид

$$S = \log_2 A, \qquad (1)$$

где A – ансамбль реализаций, определяемый количеством всех возможных значений каких-либо параметров сигнала. Такими параметрами могут быть несущая частота, структура кода, время прихода сигнала и др. В общем случае скрытность зависит от способа построения конкретного вида сигнала. В системах передачи с КРК для расширения спектра и разделения каналов используются сигнатуры – ортогональные псевдослучайные последователь-ности (ПСП).

Повышение помехозащищенности передаваемой информации является важнейшей задачей в системах КРК, поэтому актуален поиск и исследование методов передачи, позволяющих увеличить скрытность сигналов.

В статье рассмотрена возможность увеличения структурной скрытности сигналов в каждом индивидуальном канале системы за счет совместного исполь-

зования ПСП и таймерных сигнальных конструкций (ТСК).

2. Увеличение ансамбля используемых сигналов

Для увеличения структурной скрытности необходимо по возможности расширять ансамбль используемых сигналов [1]. Известно, что в бинарном канале увеличить количество реализаций кодовых последовательностей на некотором интервале времени можно за счет применения ТСК [3].

Ансамбль бинарных ТСК формируется на интервале времени $T_c = nt_0$ (n – количество элементарных посылок, t_0 – их длительность) при базовом элементе Δ ($\Delta = t_0/s$, $s \in 1,2,3,...,l$ – целые числа).

В отличие от разрядно-цифрового кодирования, когда информация о передаваемом разряде определяется уровнем сигнала элементарной посылки, в ТСК информация заложена в нескольких отдельных временных интервалах сигнала $t_c = t_0 + k\Delta$ ($k \in 0,1,2,...,s\cdot(n-2)$) и их взаимном положении на интервале формирования T_c . Пример формирования нескольких реализаций бинарных ТСК на интервале времени $T_c = 5t_0$ при базовом элементе Δ показан на рис. 1.

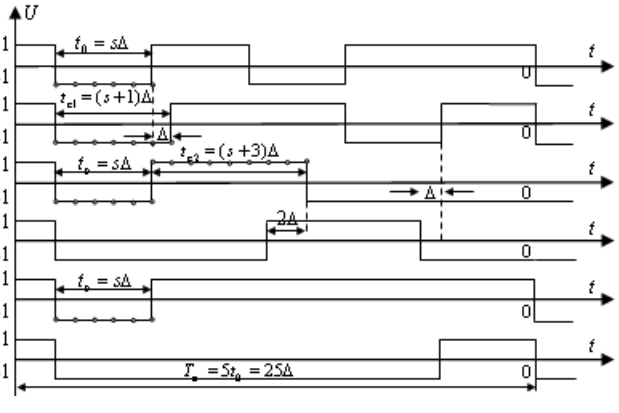

Рис. 1. Формирование реализаций бинарных ТСК на интервале времени $T_c = 5t_0$ при базовом элементе Δ

Из рисунка следует, что таймерные сигналы представляют собой вид разрядно-цифровых кодов (РЦК), в которых разрешенные для передачи сигнальные конструкции имеют не менее s подряд передаваемых элементов Δ одного знака («1» или «–1»).

Такой метод формирования позволяет передавать в канал отрезки сигнала длительностью $t_c \geq \Delta\cdot(s+i)$, где $i = 0,1,2,3...$, что исключает межсимвольные искажения. С другой стороны не кратность t_c величине t_0 позволяет уменьшить расстояния между сигнальными конструкциями до величины Δ. Это позволяет получить число реализаций ТСК N_p на интервале nt_0 больше 2^n. При заданном s ($s = t_0/\Delta$) на интервале n единичных элементов число реализаций сигнального алфавита бинарных ТСК равно [3]

$$N_p = \frac{\left[\left(n\cdot s\right)-\left[\left(s-1\right)\cdot i\right]\right]!}{i!\cdot\left[\left[\left(n\cdot s\right)-\left[\left(s-1\right)\cdot i\right]\right]-i\right]!}, \qquad (2)$$

где i – число информационных значащих моментов модуляции (ЗММ) в сигнале.

При применении сигнальных конструкций с разным числом ЗММ

$$N_p = \sum_{i=1}^{n} \frac{\left[\left(n\cdot s\right)-\left[\left(s-1\right)\cdot i\right]\right]!}{i!\cdot\left[\left[\left(n\cdot s\right)-\left[\left(s-1\right)\cdot i\right]\right]-i\right]!}. \qquad (3)$$

Оценим изменение ансамбля реализаций ТСК $N_{p\,тск}$ в зависимости от параметров n , s и i . На рис. 2 приведены зависимости $N_{p\,тск}$ от n , s и $i = 1...n$.

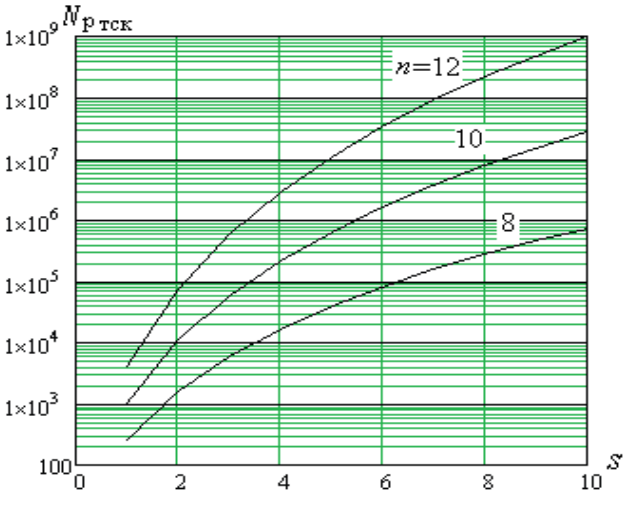

Рис. 2. Количество реализаций ТСК в зависимости от s при значениях n =8, 10, 12

Из рисунка видно, что количество реализаций ТСК существенно увеличивается с ростом n и s при $i = 1...n$ по сравнению с РЦК.

3. Повышение структурной скрытности передаваемых сигналов

Потенциальная структурная скрытность сигналов является одним из важнейших требований информационной безопасности телекоммуникационных систем. При этом задачи по скрытности формулируется, как правило, на сигнальном уровне, что предполагает выбор соответствующих характеристик и параметров сигнала. Оценим структурную скрытность таймерных сигнальных конструкций для бинарного канала при изменении параметров n, s и i .

Для расчета потенциальной структурной скрытности ТСК определим минимальный ансамбль $A_{тск}$, который требуется при несанкционированном доступе, чтобы проанализировать перехваченный сигнал

$$A_{тск} = \sum_{n}\sum_{s}\sum_{i=1}^{n} \frac{\left[\left(n\cdot s\right)-\left[\left(s-1\right)\cdot i\right]\right]!}{i!\cdot\left[\left[\left(n\cdot s\right)-\left[\left(s-1\right)\cdot i\right]\right]-i\right]!}, \qquad (4)$$

где n, s и i – текущие значения параметров.

Тогда структурная скрытность ТСК

$$S_{тск} = \log_2 A_{тск} \qquad (5)$$

На рис. 3 представлены зависимости структурной скрытности ТСК от изменения параметров n, s и i. Как видно из рисунка структурная скрытность ТСК увеличивается с ростом n и s при i=1...n.

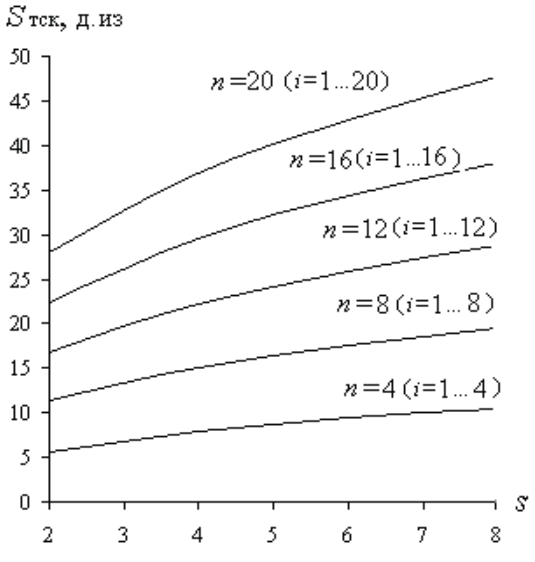

Рис. 3. Зависимости структурной скрытности ТСК от параметров n, s и i

Во введении отмечалось, что в системах с КРК для разделения каналов используются ортогональные псевдослучайные последовательности. Для ПСП со случайным чередованием «1» и «-1» $A_{псп}$ [1] принимает значение

$$A_{псп} = 2^B , \qquad (6)$$

где B – база сигнала, определяемая длиной сигнатуры (числом чипов – разрядов ПСП) на интервале единичного элемента в индивидуальных каналах.

Для оценки структурной скрытности ПСП в сочетании с ТСК формулу (1) преобразуем к виду

$$S_{шпс} = \log_2(A_{тск} \cdot A_{псп}) . \qquad (7)$$

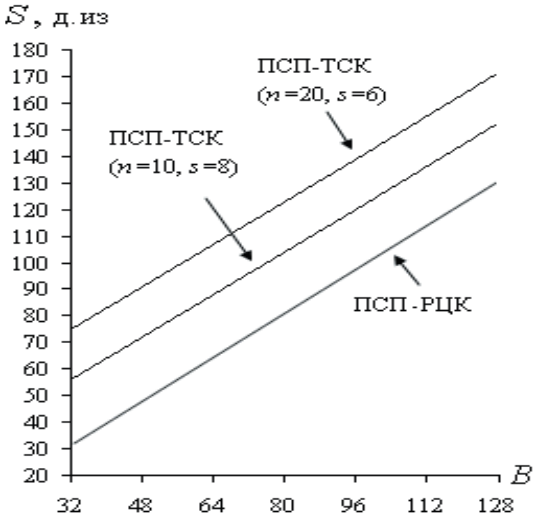

Рис. 4. Зависимости структурной скрытности ПСП-ТСК от базы B

На рис. 4 представлены зависимости потенциальной структурной скрытности сигналов ПСП от их базы B для случаев:

1) ПСП-РЦК в каждом индивидуальном канале;

2) ПСП совместно с ТСК в каждом индивидуальном канале.

Из рисунка видно, что потенциальная структурная скрытность сигналов ПСП-ТСК выше, чем у сигналов ПСП-РЦК.

4. Вывод

Проведенный анализ и расчет показали, что совместное использование ПСП и ТСК в системах передачи информации с КРК повышает потенциальную структурную скрытность передаваемого сигнала в каждом индивидуальном канале (при B=64 в 1,5 и более раз) по сравнению с ПСП-РЦК.

Литература

1. Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью / В. И. Борисов, В. М. Зинчук, А. Е. Лимарев и др. ; под ред. В. И. Борисова. - М. : Радио и связь, 2003. - 640 с.
2. Каневский, З. М. Теория скрытности / З. М. Каневский, В. П. Литвиненко. - Воронеж : ВГУ, 1991. - 144 с.
3. Захарченко, Н. В. Основы кодирования : учеб, пособие / Н. В. Захарченко, А. С. Крысько, В. Н. Захарченко. - Одесса : УГАС им. А. С. Попова, 1999. - 240 с.