РАДІОТЕХНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

УДК 691.321.25

Захарченко Н.В., Корчинский В.В., Радзимовский Б.К.
Захарченко М.В., Корчинський В.В., Радзімовський Б К.
Zaharchenko M.V., Korchinsky V.V., Radzimovsky B.K.

ОЦЕНКА ИНФОРМАЦИОННОЙ СКРЫТНОСТИ ТАЙМЕРНЫХ СИГНАЛЬНЫХ КОНСТРУКЦИЙ В СИСТЕМАХ ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

ОЦІНКА ІНФОРМАЦІЙНОЇ ПРИХОВАНОСТІ ТАЙМЕРНИХ СИГНАЛЬНИХ КОНСТРУКЦІЙ В СИСТЕМАХ ПЕРЕДАЧІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

THE EVALUATION OF THE INFORMATIONAL HIDING OF THE TIMER SIGNAL CONSTRUCTIONS IN THE CONFIDENTIAL DATA TRANSMISSION SYSTEMS

Аннотация. Дана оценка структурной и информационной скрытности таймерных сигнальных конструкций. Определены вероятности раскрытия структуры сигнала и информационной скрытности таймерных сигнальных конструкций.

Анотація. Дана оцінка структурної та інформаційної прихованості таймерних сигнальних конструкцій. Визначено ймовірності розкриття структури сигналу та інформаційної прихованості таймерних сигнальних конструкцій.

Summary. The evaluation of the structural and informational hiding of the timer signal constructions was made. The probabilities of the exposure of the signal structure and informational hiding of the timer signal constructions were determined.

В современных системах конфиденциальной передачи информации проблемой является обеспечение противодействия средствам несанкционированного доступа (НСД) [1]. Несанкционированный доступ к передаваемой информации предполагает обнаружение сигнала, определение структуры обнаруженного сигнала и раскрытие содержащейся в сигнале информации**.** Перечисленным задачам НСД противопоставляются три вида скрытности сигналов: энергетическая, структурная и информационная.

Энергетическая скрытность характеризует способность противостоять мерам, направленным на обнаружение сигнала средствами НСД. Известно [2], что одним из путей повышения энергетической скрытности является увеличение ширины спектра используемых сигналов, что достигается применением шумоподобных (ШПС) и хаотических сигналов в системах конфиденциальной передачи информации.

Структурная скрытность характеризует способность противостоять мерам НСД, направленным на раскрытие структуры 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 передаваемых символов. Очевидно, что для увеличения структурной скрытности необходимо иметь по возможности бóльший ансамбль используемых сигналов с изменяемыми во времени параметрами.

Информационная скрытность определяется способностью системы связи противостоять мерам, направленным на раскрытие смыслового содержания сообщения, передаваемого с помощью сигналов [1]. Раскрытие смыслового содержания означает отождествление каждого принятого сигнала или их множества с тем сообщением, которое передавалось.

Противодействие средствам НСД является важнейшей задачей, поэтому следует осуществлять поиск и исследование методов передачи, позволяющих увеличить скрытность сигналов в конфиденциальных системах связи. Оценка скрытности сигналов в бинарном канале в основном проводилась для двоичных кодов. В частности, такие исследования были выполнены для систем передачи с кодовым разделением каналов [1]. Однако в литературе отсутствует оценка скрытности таймерных сигнальных конструкций (ТСК). В данной работе рассматривается возможность повышения скрытности сигналов бинарного канала за счет применения ТСК [3].

Цель работы – дать оценку структурной и информационной скрытности ТСК.

Как отмечалось выше, определению информационной скрытности предшествует оценка структурной скрытности сигналов. Рассмотрим возможность увеличения ансамбля передаваемых сигналов при использовании ТСК.

Известно [3], что множество реализаций бинарных ТСК формируется на интервале времени $T_c = nt_0$, где n – количество элементарных посылок, а t_0 – их длительность. Базовым элементом при формировании является $\Delta = t_0/s$, где $s \in 1, 2, 3, \ldots, l$ – целые числа. В отличие от разрядно-цифрового кода (РЦК), когда информация о передаваемом разряде определяется уровнем сигнала элементарной посылки, в ТСК информация заложена в нескольких отдельных (временных) интервалах сигнала $t_c = t_0 + k\Delta$, где $k \in 0, 1, 2, \ldots, s\cdot(n-2)$, и их на интервале T_c взаимном положении. С одной стороны такой метод формирования дает возможность передавать в канал отрезки сигнала длительностью $t_c \geq \Delta\cdot(s+i)$, где $i = 0, 1, 2, 3\ldots$, что исключает межсимвольные искажения в каналах с базой $B = 1$. С другой стороны, не кратность t_c величине t_0 позволяет уменьшить расстояния между сигнальными конструкциями до величины $\Delta < t_0$ и получить число реализаций ТСК $N_{\text{рТСК}}$ на интервале nt_0 значительно больше 2^n [3]

$$N_{\text{рТСК}} = \sum_{i=1}^{n} \frac{[(n\cdot s)-[(s-1)\cdot i]]!}{i!\cdot[[(n\cdot s)-[(s-1)\cdot i]]-i]!}. \qquad (1)$$

Число реализаций ТСК с учетом значений s, n и $i = 1\ldots n$ приведено в табл. 1. Анализ таблицы показывает, что кодек ТСК позволяет сформировать значительно больше разрешенных ТСК на одном и том же интервале, чем кодовых слов РЦК, где число реализаций $N = 2^n$. Например, при формировании ТСК на интервале $T_c = 5t_0$ и $s = 7$ число возможных реализаций $N_{\text{р}} = 1293$. Такое количество реализаций можно получить только с помощью простого двоичного кодового слова с длиной $n = \lceil \log_2 1293 \rceil = 11$ элементов.

Таблица 1 − Количество реализаций ТСК при различных значениях s и n

s / n	1	2	3	4	7	10	15	20
5	31	88	188	344	1293	3310	10475	24940
8	255	1596	5895	16492	153400	735450	4952841	20628612
10	1023	10945	58424	217224	3705000	27042520	$3{,}02\cdot10^8$	$1{,}83\cdot10^9$

На рис. 1 показана упрощенная структурная схема системы передачи конфиденциальной информации с использованием ТСК. Источник информации выдает непрерывную последовательность информационных двоичных элементов РЦК, которая кодеком ТСК разбивается на блоки некоторой длины $k_{\text{РЦК}}$. Длина блока $k_{\text{РЦК}}$ определяется из условия максимально возможного числа реализаций $N_{\text{рТСК}}$, сформированных на некотором интервале n при выбранных параметрах s и i, тогда

$$k_{\text{РЦК}} \leq \log_2 N_{\text{рТСК}}. \qquad (2)$$

Каждой длине блока $k_{\text{РЦК}}$ соответствует число, определяющее номер реализации РЦК. Кодер ТСК осуществляет кодирование сигнала РЦК $S_{\text{РЦК}}$ в сигнал ТСК $S_{\text{ТСК}}$ по правилу

$$S_{\text{РЦК}j} \rightarrow S_{\text{ТСК}z}(n, s, i), \qquad (3)$$

т.е. каждый сигнал $S_{\text{РЦК}j}$ представляется определенной конструкцией $S_{\text{ТСК}z}$., где j и z − соответственно номера реализаций.

Изменение параметров n, s и i дает возможность на выходе кодера ТСК получать различные множества сигнальных конструкций, каждое из которых может отличаться длительностями, зависящими от значений n, числом базовых элементов s и числом переходов i, т. е. структурой сигнала.

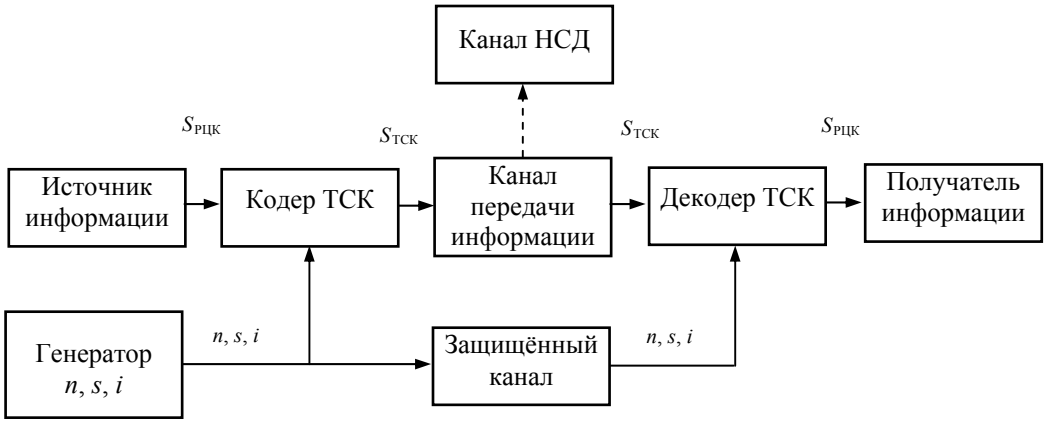

Рисунок 1 − Упрощенная структурная схема системы передачи конфиденциальной информации

Например, при определенных значениях n и s можно формировать различные множества конструкций $S_{ТСКz}$ изменением только числа переходов i, где каждому его значению будет соответствовать множество со своей структурой сигнала. Аналогично, изменением s и n или различных допустимых комбинаций n, s, i можно на выходе кодера ТСК получать множества $S_{ТСКz}$ с разной формой сигнала. Частота смены параметров кодером ТСК выбирается такой, чтобы объем перехваченных станцией НСД реализаций ТСК определенной формы с заданными параметрами был недостаточен для раскрытия структуры сигнала в пределах интервалов времени, представляющих практический интерес. Так как параметры n, s и i должны быть известны приемной стороне, то их передача обычно осуществляется по отдельному достаточно защищенному каналу.

Наличие априорной и апостериорной неопределенностей делает задачу определения структуры сигнала вероятностной, поэтому количественной мерой структурной скрытности ТСК может служить вероятность раскрытия структуры сигнала $p_{стр}$ при условии, что сигнал уже обнаружен. Следовательно, $p_{стр}$ представляет собой условную вероятность, и ее определение заключается в нахождении параметров n, s и i.

Для получения максимально возможной структурной скрытности, т. е. достижения минимальной $p_{стр}$, последовательность символов сообщения в кодере должна подлежать такому преобразованию, при котором различные символы в его выходной последовательности появлялись бы по возможности равновероятно. Следовательно, при передаче, например, текста, использующего алфавит из 32 букв, каждая из которых появляется с разной вероятностью, необходимо кодировать не отдельные буквы, а последовательности из различных (учитывающих и порядок) сочетаний букв, чем можно обеспечить достаточно равновероятное появление сигналов на выходе кодера. Но увеличение алфавита приводит к возрастанию ансамбля реализаций, что требует дополнительных затрат, например, увеличения длительности передачи или расширения ширины спектра канала связи, что не всегда желательно. Например, при кодировании последовательностей из двух букв первичный ансамбль реализаций $N = 31$ увеличивается и принимает значение $N_р = 992$, что приводит к необходимости использования для передачи такого ансамбля 10-элементного РЦК вместо 5-элементного.

Применение кодера ТСК дает возможность на интервале 5-элементного РЦК при параметрах $n = 5$, $s = 7$ и $i = 1 \ldots n$ (табл. 1) сформировать достаточный ансамбль реализаций $N_{рТСК} = 1293 > N_р = A_{32}^2 = 992$, чтобы оставить длительность передачи без изменений.

Значение $p_{стр}$ определяется с учетом минимального ансамбля реализаций $A_{ТСК}$, который требуется проанализировать методом полного перебора для нахождения ключей n, s и i при несанкционированном доступе

$$p_{\text{стр}} = \frac{1}{A_{\text{ТСК}}}, \tag{4}$$

где

$$A_{\text{ТСК}} = \sum_{n}\sum_{s}\sum_{i=1}^{n} \frac{[(n\cdot s)-[(s-1)\cdot i]]!}{i!\cdot[[(n\cdot s)-[(s-1)\cdot i]]-i]!}. \tag{5}$$

На рис. 2 приведен график вероятностей раскрытия структуры ТСК в зависимости от значений n при s=1 … 12 и i=1 … n. Как видно из рисунка, вероятности раскрытия структуры сигнала $p_{\text{стр}}$ существенно уменьшаются с ростом интервала (T_c) формирования ТСК.

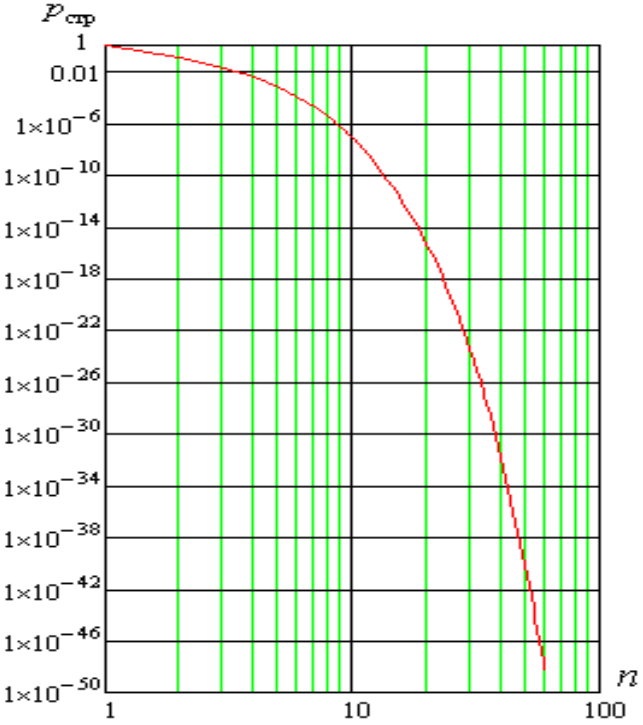

Рисунок 2 – График вероятностей раскрытия структуры ТСК в зависимости от значений n при s=1 … 12 и i=1 … n

Раскрыв структуру сигнала, станция НСД располагает набором параметров n, s и i для определения его информационной скрытности. Предположим, что система передачи использует простой двоичный код, тогда смысловое содержание может быть раскрыто путем анализа соответствий реализаций ТСК реализациям РЦК. Количество сравнений для одной реализации с учетом известных n, s и i определяется выражением

$$N_{\text{РЦК}} = N_{\text{ТСК}} = \frac{[(n\cdot s)-[(s-1)\cdot i]]!}{i!\cdot[[(n\cdot s)-[(s-1)\cdot i]]-i]!}, \tag{6}$$

где $N_{\text{ТСК}}$ и $N_{\text{РЦК}}$ − соответственно число реализаций ТСК и РЦК.

Однако для определения смыслового содержания информации необходимо анализировать не одну ТСК, а совместно некоторое их количество $N_{\text{а ТСК}}$. В этом случае необходимое число сравнений $A_{\text{инф}}$ будет определяться формулой

$$A_{\text{инф}} = C_{N_{\text{ТСК}}}^{N_{\text{а ТСК}}}. \tag{7}$$

Задача определения информационной скрытности сигнала также является статистической, поэтому в качестве количественной меры информационной скрытности можно принять условную вероятность раскрытия смыслового содержания передаваемой информации $p_{\text{инф}}$, заложенной в обнаруженном сигнале с раскрытой структурой. Учитывая, что таймерные конструкции на выходе кодера ТСК равновероятны, а их таблицы перекодировки в РЦК меняются по определенному (известному на приемной стороне) алгоритму, значение $p_{\text{инф}}$ определяется формулой

$$p_{\text{инф}} = \frac{1}{\text{A}_{\text{инф}}}. \qquad (8)$$

Например, на приемной стороне для каждого числа переходов i в принятой реализации ТСК при определенных значениях n и s используется своя таблица перекодировки в РЦК. Также разным s или некоторым комбинациям параметров n, s и i могут соответствовать другие таблицы, что повышает информационную скрытность передаваемых сигналов. Частота смены параметров n, s, i и соответствующих им таблиц перекодировки выбирается такой, чтобы накопленные станцией НСД статистические данные по числу перехваченных реализаций ТСК не давали возможности достаточно быстро распознать смысловое содержание передаваемого сообщения.

На рис. 3 приведены графики вероятностей информационной скрытности ТСК в зависимости от количества анализируемых ТСК при различных значениях n, s и i. Как видно из рисунка, увеличение ансамбля реализаций $N_{\text{ТСК}}$ и рост числа совместно анализируемых конструкций $N_{\text{а ТСК}}$ уменьшает вероятность $p_{\text{инф}}$.

Дополнительно повысить информационную скрытность ТСК можно за счет шифрования, например, используя алгоритм RSA [4]. Каждый абонент системы передачи при шифровании выбирает случайно собственных два больших простых числа p и g. После чего вычисляет числа $n = pg$ и $v = (p-1)(g-1)$, затем выбирает некоторое число $d < v$ взаимно простое с v и находит число c из условия $cd \bmod v = 1$. Ключи каждого абонента d и n являются открытыми, а ключи c – секретными. Пусть один из абонентов передает другому сообщение m, причем сообщение m рассматривается как число, удовлетворяющее неравенству $m < n_2$. Индекс указывает на принадлежность указанных параметров конкретному абоненту. Используя открытые ключи получателя сообщения, число m шифруется по формуле $e = m^{d_2} \bmod n_2$. Абонент, получивший зашифрованное сообщение e, используя свой секретный ключ c_2, вычисляет исходящее сообщение передающего абонента $m = e^{c_2} \bmod n_2$. Допустим, требуется передать $m = 27$, т.е. двадцать седьмую реализацию ТСК. Зная открытые ключи получателя, например, $d_2 = 5$ и $n_2 = 85$, в результате шифрования m получаем значение реализации ТСК под номером $e = 27^5 \bmod 85 = 57$ для передачи по каналу связи. Получатель, используя свой секретный ключ $c_2 = 13$, расшифровывает принятое сообщение $m = 57^{13} \bmod 85 = 27$ и тем самым находит исходящую реализацию ТСК.

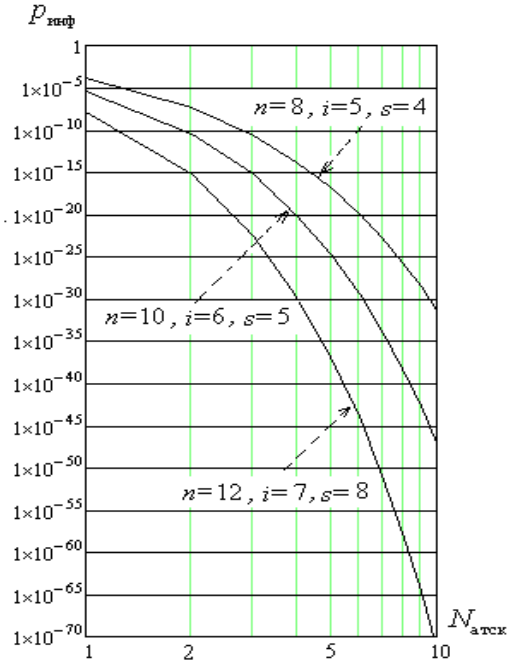

Рисунок 3 – Графики вероятностей информационной скрытности ТСК в зависимости от $N_{\text{а ТСК}}$ при различных значениях n, s и i

Следует заметить, что в зашифрованном тексте статистические свойства исходного сообщения сохраняются, но ансамбль требуемых ТСК значительно увеличивается. Станции НСД, перехватившей сообщение и знающей открытые ключи, трудно найти за приемлемое время без секретного ключа c исходное сообщение при больших значениях p и g.

Вероятность полного раскрытия ТСК $p_{\text{Р}}$ при условии обнаружения станцией НСД передаваемого сигнала определяется с учетом вероятностей $p_{\text{стр}}$ и $p_{\text{инф}}$

$$p_{\text{Р}} = p_{\text{стр}} \cdot p_{\text{инф}}. \qquad (9)$$

Представленные в работе результаты по оценке структурной и информационной скрытности ТСК показали целесообразность их применения в конфиденциальной системах передачи. В заключение можно сделать следующие выводы:

1) использование ТСК в конфиденциальных системах связи повышает структурную и информационную скрытности передаваемой информации;

2) применение ТСК позволяет уменьшить вероятность раскрытия структуры сигнала $p_{\text{стр}}$ до значений 10^{-48}, а вероятность информационной скрытности $p_{\text{инф}}$ – до 10^{-70}.

3) шифрование ТСК дополнительно повышает информационную скрытность передаваемых сообщений.

Литература

1. *Куприянов А.И.* Теоретические основы радиоэлектронной борьбы / А. И. Куприянов, А. В. Сахаров. – М.: Вузовская книга, 2007. – 356 с.
2. *Помехозащищенность* систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью / [Борисов В. И., Зинчук В. М., Лимарев А. Е. и др.]; под ред. В. И. Борисова. – М.: Радио и связь, 2003. – 640 с.
3. *Захарченко Н.В.* Основы кодирования: учебное пособие / Захарченко Н.В., Крысько А.С., Захарченко В.Н. – Одесса: УГАС им. А. С. Попова, 1999. – 240 с.
4. *Мао В.* Современная криптография; пер. с англ. – М.: Вильямс, 2005. – 768 с.