державної академії технічного регулювання та якості. - 2014.- № 2(5).- с. 88 – 93

8. Allflex [Електронний ресурс] / Allflex USA Inc. - Режим доступу : http://www.allflexusa.com - 17.02.2015. - Заголовок з екрану

9. RFID Journal [Електронний ресурс] / RFID journal LLC. - Режим доступу : http://www.rfidjournal.com - 17.02.2015. - Заголовок з екрану

10. Bryant, A.M. Performance of ISO 11785 low-frequency radio frequency identification devices for cattle [Text] : M.S. Thesis, Kansas State Univ., Manhattan : 2007

References

1. ISO 11784/85. Radio frequency identification of animals [Elektronnij resurs] / International Standard Organization. - Rezhim dostupu : http: // www.iso.org - 17.02.2015. - Zagolovok z ekranu

2. Tehnologii i oborudovanie dlja zhivotnovodstva VAT "Braclav" [Tekst] / 2010. - 27 s.

3. GEA [Elektronnij resurs] / GEA Westfalia Separator Group - Rezhim dostupu : www.westfalia-separator.com - 05.03.2015. - Zagolovok z ekranu

4. Afimilk [Elektronnij resurs] / Afimilk - Rezhim dostupu : www.afimilk.com - 05.03.2015. - Zagolovok z ekranu

5. DeLaval [Elektronnij resurs] / Tetra Laval Group. - Rezhim dostupu : www.delaval.com - 05.03.2015. - Zagolovok z ekranu

6. Coj, Ju. A. Processy i oborudovanie doil'no-molochnyh otdelenij zhivotnovodcheskih ferm [Tekst] / Ju. A. Coj. – M. : GNU VIJeSH, 2010. – 424 s.

7. Kucheruk, V. Ju. Sistema radiochastotnoї identifikacії tvarin dlja stijlovoї doїl'noї ustanovki [Tekst] / V. Ju. Kucheruk, Є. A. Palamarchuk, P. I. Kulakov, T. V. Gnes' // Zbirnik naukovih prac' odes'koї derzhavnoї akademії tehnichnogo reguljuvannja ta jakosti. - 2014.- № 2(5).- s. 88 – 93

8. Allflex [Elektronnij resurs] / Allflex USA Inc. - Rezhim dostupu : http://www.allflexusa.com - 17.02.2015. - Zagolovok z ekranu

9. RFID Journal [Elektronnij resurs] / RFID journal LLC. - Rezhim dostupu : http://www.rfidjournal.com - 17.02.2015. - Zagolovok z ekranu

10. Bryant, A.M. Performance of ISO 11785 low-frequency radio frequency identification devices for cattle [Text] : M.S. Thesis, Kansas State Univ., Manhattan : 2007

Рецензія/Peer review : 6.1.2015 р. Надрукована/Printed :25.1.2015 р.
Стаття рецензована редакційною колегією

УДК 004.056.53

Н.В. ЗАХАРЧЕНКО, В.В. КОРЧИНСКИЙ, Б.К. РАДЗИМОВСКИЙ, Ю.С. ГОРОХОВ
Одесская национальная академия связи им. А.С.Попова

ТАЙМЕРНЫЕ СИГНАЛЬНЫЕ КОНСТРУКЦИИ – КАК ИНСТРУМЕНТ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье обоснована целесообразность применения таймерных сигнальных конструкций в системах информационной безопасности. Дана оценка структурной и информационной скрытности таймерных сигнальных конструкций. Определены вероятности раскрытия структуры сигнала и информационной скрытности таймерных сигнальных конструкций.

Ключевые слова: таймерная сигнальная конструкция, скрытность, шифрование.

M.V. ZAHARCHENKO, V.V. KORCHINSKY, B.K. RADZIMOVSKY, Y.S. GOROHOV
Odessa national academy of telecommunication by O. S. Popov

TIMER SIGNAL DESIGN AS A - TOOL OF INFORMATION SECURITY SYSTEMS

In the article proved the feasibility of using a timer signal constructions in information security systems. The estimation of the structural and informational stealth of timer signal designs is given. The probability of disclosure of signal structure and information stealth of a timer signal constructions is defined.

Keywords: timer signal constructions, stealth, encryption.

Вступление

Несанкционированный доступ (НСД) к передаваемой информации предполагает обнаружение и определение структуры сигнала, а также раскрытие смыслового содержания сообщения в случае его перехвата [1]. Перечисленным задачам НСД противопоставляются три вида скрытности сигнальных конструкций: энергетическая, структурная и информационная. В связи с этим актуальной задачей является поиск и синтез сигнальных конструкций, которым присущи свойства скрытности [1]. В работе дана оценка структурной и информационной скрытности таймерных сигнальных конструкций (ТСК).

Обоснование использования таймерных сигнальных конструкций в системах информационной безопасности

Таймерные сигналы [2, 3] были предложены в 80-е годы прошлого века для задачи повышения скорости передачи информации в бинарном канале. Также на их основе были разработаны и получили дальнейшее развитие новые принципы и алгоритмы помехоустойчивого кодирования, в которых дополнительные проверочные символы не требовались. Анализ вариационных возможностей таймерного кодирования по синтезу различных множеств сигнальных конструкций позволил выдвинуть гипотезу о

целесообразности использования их в системах информационной безопасности. Таким образом, появилась возможность интегрировать процесс обеспечения верности передачи и процесс защиты информации от НСД в одну общую задачу.

Проанализируем возможность увеличения ансамбля передаваемых сигналов с помощью ТСК [2] по сравнению с позиционным кодированием [3], а также покажем свойства таймерного кодирования по обнаружению и/или исправлению ошибок. Значения моментов модуляции таймерного сигнала, сформированного на интервале времени $T_{\text{с}} = nt_0$ (где n – количество найквистовых элементов; t_0 – их длительность), в отличие от разрядно-цифрового сигнала кратны не t_0, а некоторому базовому элементу Δ (где $\Delta = t_0 / s$; $s = 1, 2, 3, ..., l$ – целые числа). В канал передаются отрезки сигнала длительностью $t_{\text{с}} = t_0 + k\Delta$ (где $k = 0, 1, 2, ..., s \cdot (n-2)$). В таймерных сигналах энергетическое расстояние между сигнальными конструкциями определяется величиной $\Delta < t_0$, поэтому число их реализаций $N_{\text{р}}$ на интервале $T_{\text{с}}$ значительно больше по сравнению с позиционным кодом

$$N_{\text{р}} = \sum_{i=1}^{n} \frac{\left[(n \cdot s) - \left[(s-1) \cdot i\right]\right]!}{i! \left[\left[(n \cdot s) - \left[(s-1) \cdot i\right]\right] - i\right]!}, \tag{1}$$

где i – число информационных моментов модуляции.

Основная задача при синтезе ТСК, которые обнаруживают и исправляют ошибки, состоит в том, что необходимо найти зависимости весовых коэффициентов $A_k (k = 1, i)$ и модуля A_0 в уравнении качества [2]

$$\sum_{k=1}^{i} A_k x_k \equiv 0 \bmod A_0 \tag{2}$$

с учётом свойств того или иного кода.

Рассмотрим две теоремы, согласно которым обосновывается возможность синтеза ТСК с обнаружением и/или исправлением ошибок.

Теорема 1. Если коэффициенты A_k уравнения (2) определены так, что

$$A_k = (e_0 + 1)^{k-1},$$
$$A_0 = (e_0 + 1)^{i},$$

то ошибки кратности меньшей или равной i величиной $[-e_1, ..., e_0]$ обнаруживаются с вероятностью 1.

Теорема 2. Если коэффициенты A_k уравнения (2) определены так, что

$$A_k = (2e_0 + 1)^{k-1},$$

то ошибки кратности меньшей или равной i величиной $[-e_1, e_0]$ обнаруживаются и исправляются с вероятностью 1.

Доказательства этих теорем приведено в [2].

Путем изменения параметров n, s и i можно получать различные множества таймерных сигналов, каждое из которых отличается длительностями, зависящими от значений n, числом базовых элементов s и числом переходов i, т. е. формой сигнала на интервале времени $T_{\text{с}}$. Изменением параметров n, s и i достигается значительное повышение информационной скрытности передаваемых сигналов. В перехваченном сообщении смысловое содержание может быть раскрыто путем анализа соответствий реализаций таймерного сигнала реализациям позиционного кода. Количество сравнений для одной реализации с учетом известных n, s и i определяется выражением (1), однако для определения смыслового содержания необходимо анализировать не одну реализацию, а совместно некоторое их количество $N_{\text{а}}$.

Таблица 1

Количество реализаций ТСК при различных значениях s и n.

n \ s	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	$3{,}02 \cdot 10^8$	$1{,}83 \cdot 10^9$

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.

В конфиденциальной системе связи с ТСК (рис. 1) 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 максимального возможного числа реализаций $N_{\text{р тск}}$, сформированных на некотором интервале n при выбранных параметрах s и i, тогда

$$k_{\text{РЦК}} \le \log_2 N_{\text{р тск}}. \tag{3}$$

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

$$S_{\text{РЦК}j} \rightarrow S_{\text{ТСК}z}(n, s, i), \tag{4}$$

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

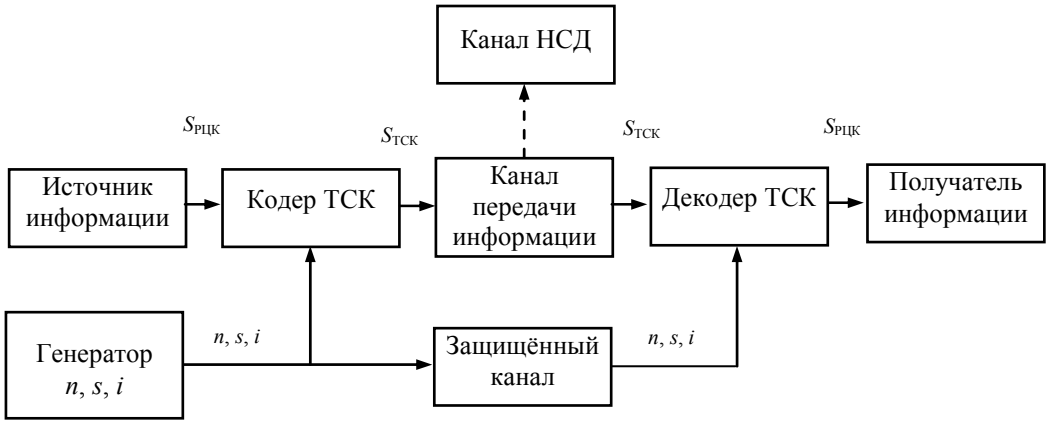

Рис. 1. Структура конфиденциальной системы связи с ТСК

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. На рис. 2 приведены графики вероятностей раскрытия информационного содержания таймерных сигналов в зависимости от количества совместно анализируемых реализаций при различных значениях n, s и i. Как видно из рисунка, увеличение ансамбля реализаций $N_{\text{р}}$ таймерных сигналов и числа, совместно анализируемых конструкций N_a, уменьшает вероятность $p_{\text{инф}}$ их раскрытия.

Например, при определенных значениях n и s можно формировать различные множества конструкций $S_{\text{ТСК}z}$ 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 $S_{\text{ТСК}z}$ с разной формой сигнала. Частота смены параметров кодером ТСК выбирается такой, чтобы объем перехваченных станцией НСД реализаций ТСК определенной формы 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 $p_{\text{стр}}$ при условии, что сигнал уже обнаружен. Следовательно, $p_{\text{стр}}$ представляет собой условную вероятность, и ее определение заключается в нахождении параметров n, s и i.

Свести к минимуму вероятность раскрытия структуры сигнала можно при условии, что $p_{\text{стр}} \rightarrow 0$. Тогда 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 сочетаний букв, за счёт чего можно обеспечить более 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 $N_{\text{р}} = 992$, что приводит к необходимости использования для передачи такого ансамбля 10-ти элементного РЦК вместо 5-ти элементного.

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

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

$$p_{\text{стр}} = \frac{1}{A_{\text{тск}}}, \tag{5}$$

где

$$A_{\text{тск}} = \sum_{n}\sum_{s}\sum_{i=1}^{n} \frac{[(n \cdot s) - [(s-1) \cdot i]]!}{i! \cdot [[(n \cdot s) - [(s-1) \cdot i]] - i]!}. \tag{6}$$

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

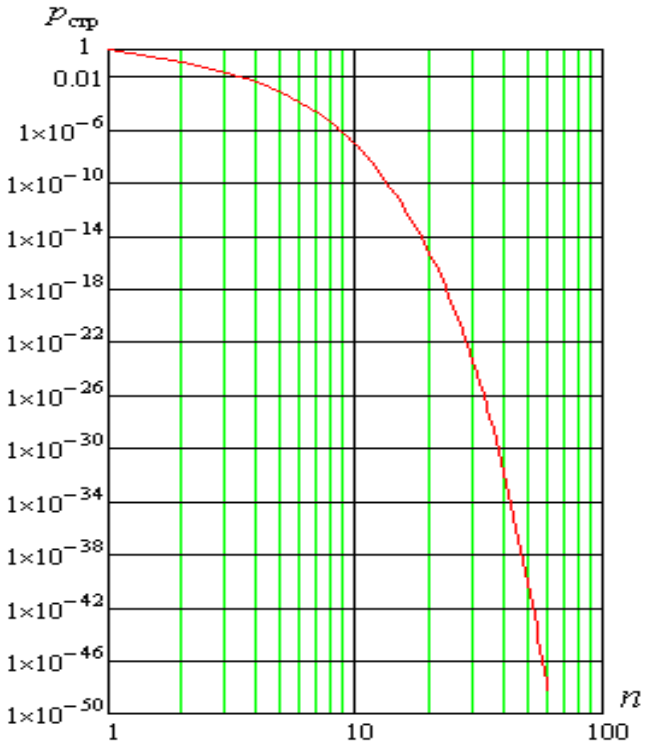

Рис. 2. График вероятности раскрытия структуры ТСК в зависимости от значений n при $s = 1 \div 12$ и $i = 1 \div n$.

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

$$N_{\text{рцк}} = N_{\text{тск}} = \frac{[(n \cdot s) - [(s-1) \cdot i]]!}{i! \cdot [[(n \cdot s) - [(s-1) \cdot i]] - i]!}, \tag{7}$$

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 будет определяться формулой

$$A_{\text{инф}} = C_{N_{\text{ТСК}}}^{N_{\text{а тск}}}. \quad (8)$$

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 разрядно-цифровой код меняются по определенному (известному на приемной стороне) алгоритму, значение $p_{\text{инф}}$ определяется формулой

$$p_{\text{инф}} = \frac{1}{\text{A}_{\text{инф}}}. \quad (9)$$

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.

Выводы

Результаты исследования показывают, что применение ТСК в системах информационной безопасности позволяет не только обнаруживать и исправлять ошибки за счет корректирующего таймерного кодирования, но и повышает структурную и информационную скрытность передаваемых сигнальных конструкций. При этом вероятность раскрытия структуры сигнала $p_{\text{стр}}$ обеспечивается в пределах порядка 10^{-48}, а вероятность информационной скрытности $p_{\text{инф}}$ – 10^{-70}. Кроме того, применяя криптографическое шифрование совместно с таймерным кодированием, можно существенно повысить информационную скрытность передаваемых сообщений.

Литература

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

Захарченко В.М. Синтез багатопозиційних часових кодів / В.М. Захарченко. – Київ: Техніка, 2012. – 284 с.

Захарченко Н. В. Основы кодирования: учебное пособие / Н. В. Захарченко, А. С. Крысько, В.Н. Захарченко – Одесса: УГАС им. А. С. Попова, 1999. – 240 с.

References

1. Kuprijanov A.I. Teoreticheskie osnovy radiojelektronnoj bor'by / A. I. Kuprijanov, A. V. Saharov. – M.: Vuzovskaja kniga, 2007. – 356 s.

2. Zaharchenko V.M. Syntez bagatopozycijnyh chasovyh kodiv / V.M. Zaharchenko. – Kyi'v: Tehnika, 2012. – 284 s.

3. Zaharchenko N. V. Osnovы kodyrovanyja: uchebnoe posobye / N. V. Zaharchenko, A. S. Krы'ko, V.N. Zaharchenko – Odessa: UGAS ym. A. S. Popova, 1999. – 240 s.

Рецензія/Peer review : 14.1.2015 р. Надрукована/Printed :25.1.2015 р.
Стаття рецензована редакційною колегією