УДК 004.056.53

О ЦЕЛЕСООБРАЗНОСТИ ИСПОЛЬЗОВАНИЯ ТАЙМЕРНЫХ СИГНАЛЬНЫХ КОНСТРУКЦИЙ В СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ю. С. Горохов, д. т. н. Н. В. Захарченко, д. т. н. В. В. Корчинский,
к. т. н. Б. К. Радзимовский

Одесская национальная академия связи им. А. С. Попова
Украина, г. Одесса
vladkorchin@rambler.ru

Обоснована целесообразность применения таймерных сигнальных конструкций в системах информационной безопасности. Дана оценка структурной и информационной скрытности таймерных сигнальных конструкций.

Ключевые слова: таймерная сигнальная конструкция, скрытность, шифрование.

Несанкционированный доступ (НСД) к передаваемой информации предполагает обнаружение и определение структуры сигнала, а также раскрытие смыслового содержания в перехваченном сообщении [1]. Перечисленным задачам НСД противопоставляются три вида скрытности сигнальных конструкций: энергетическая, структурная и информационная. Поэтому актуальной задачей является поиск и синтез сигнальных конструкций, которым присущи свойства скрытности [1]. В настоящей работе дана оценка структурной и информационной скрытности таймерных сигнальных конструкций (ТСК) в сравнении с позиционным кодированием. Таймерные сигналы [2] 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 информационной и структурной скрытности за счет синтезируемых ТСК [2] по сравнению с позиционным кодированием [3]. 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

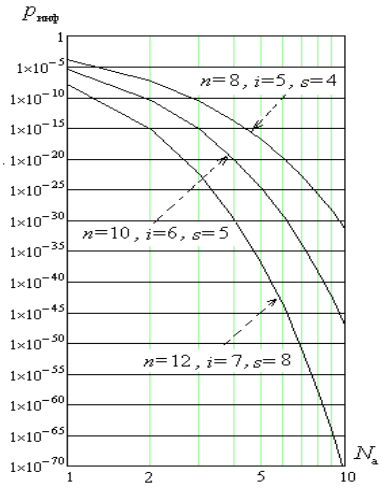
$$N_{\text{р}} = \sum_{i=1}^{n} \frac{[(n \cdot s) - [(s-1) \cdot i]]!}{i! \cdot [[(n \cdot s) - [(s-1) \cdot i]] - i]!}, \qquad (1)$$

где i – число информационных моментов модуляции. Параметры n, s и i можно рассматривать в качестве ключей системы шифрования, так как при изменении значения хотя бы одного из них формируется новое множество ТСК. Даже при использовании в системе передачи простого двоичного кода смысловое содержание может быть раскрыто только путем анализа соответствий реализаций ТСК реализациям разрядно-цифрового кода (РЦК). 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 $N_{\text{а}}$. Число реализаций ТСК с учетом значений s, n и $i = 1 \ldots n$ приведено в таблице. Анализ таблицы по-

казывает, 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.

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	$3{,}02\cdot10^8$	$1{,}83\cdot10^9$



Графики вероятностей раскрытия информационного содержания ТСК

В системе конфиденциальной связи с 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

$$k_{\text{РЦК}} \le \log_2 N_{\text{ртск}}. \qquad (2)$$

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), 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. На рисунке приведены графики вероятностей раскрытия информационного содержания ТСК в зависимости от количества совместно анализируемых реализаций при различных значениях n, s и i. Видно, что увеличение ансамбля реализаций $N_{\text{р}}$ таймерных сигналов и числа совместно анализируемых конструкций N, уменьшает вероятность $p_{\text{инф}}$ их раскрытия.

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. 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.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Куприянов А. И., Сахаров А. В. Теоретические основы радиоэлектронной борьбы.– Москва: Вузовская книга, 2007.

2. Захарченко В.М. Синтез багатопозиційних часових кодів.– Київ: Техніка, 2012.

Y. S. Horokhov, M. V. Zaharchenko, V. V. Korchinsky, B. K. Radzimovsky

On the feasibility of using timer signal constructions in information security systems.

The paper proves the feasibility of using timer signal constructions in information security systems. The estimation of the structural and informational stealth of timer signal constructions is given.

Keywords: *timer signal construction, stealth, encryption.*