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.

МЕТОД ФОРМИРОВАНИЯ СИГНАЛЬНЫХ КОНСТРУКЦИЙ НА ОСНОВЕ ХАОТИЧЕСКИХ И ТАЙМЕРНЫХ СИГНАЛОВ В СИСТЕМАХ ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

МЕТОД ФОРМУВАННЯ СИГНАЛЬНИХ КОНСТРУКЦІЙ НА ОСНОВІ ХАОТИЧНИХ І ТАЙМЕРНИХ СИГНАЛІВ У СИСТЕМАХ ПЕРЕДАЧІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

THE SYNTHESIS OF SIGNAL CONSTRUCTIONS, BASED ON CHAOTIC AND TIMER SIGNALS IN CONFIDENTIAL INFORMATION TRANSMISSION SYSTEM

Аннотация. Предложен метод формирования сигнальных конструкций на основе хаотических и таймерных сигналов для использования их в конфиденциальных системах передачи с целью повышения скрытности передаваемых сигналов. Приведен алгоритм формирования сигнала для передачи и показан метод его приема.

Анотація. Запропоновано метод формування сигнальних конструкцій на основі хаотичних і таймерних сигналів для застосування в конфіденційних системах передачі з метою підвищення скритності сигналів. Наведено алгоритм формування сигналу для передачі і показаний метод його прийому.

Summary. The method of signal constructions synthesis, based on chaotic and timer signals for use in confidential communication systems to improve the secrecy of transmitted signals was proposed. The algorithm of waveform shaping for signal transmission and method of signal reception was shown.

Надежная защита передаваемых данных от несанкционированного доступа (НСД) является одним из главных критериев эффективности конфиденциальных систем связи [1]. Поэтому поиск и исследование методов передачи, направленных на увеличение скрытности (энергетической, структурной и информационной) передаваемой информации является актуальной проблемой.

Известно [1], что применение в системах связи широкополосных сигналов с большой базой $B >> 1$ при разрядно-цифровых методах кодирования обеспечивает значительное повышение скрытности передачи, по сравнению с сигналами $B = 1$. В свою очередь, исследования, проведенные в работах [2, 3], показали, что структурная и информационная скрытность таймерных сигнальных конструкций (ТСК) выше, чем при разрядно-цифровых методах кодирования. В этих работах дана оценка структурной и информационной скрытности передаваемого сигнала при совместном использовании ТСК и широкополосных сигналов на основе псевдослучайных последовательностей. Это позволило увеличить структурную скрытность при $B = 64$ в 1,5 и более раз по сравнению с разрядно-цифровым кодированием. Показано, что вероятность информационной скрытности можно уменьшить до значений 10^{-70}.

В [4] показана перспективность использования широкополосных сигналов на основе динамического хаоса для новых систем, обладающих повышенной информационной емкостью, высокой помехозащищенностью и обеспечивающих конфиденциальность передаваемого сообщения. Появляется возможность получения сложных широкополосных хаотических сигналов со сплошным спектром в заданном диапазоне частот с помощью простых по структуре электронных устройств и управление хаотическими режимами путем малых изменений параметров системы, и наличие значительного количества методов модуляции хаотического сигнала.

Однако в литературе отсутствуют исследования о возможности использования ТСК в системах связи с широкополосными хаотическими сигналами. Поэтому *целью статьи является разработка метода формирования сигнальных конструкций* на основе широкополосных хаотических [4] и информационных таймерных сигналов.

В предлагаемых алгоритмах передачи [4] на основе широкополосных хаотических сигналов среди разнообразия методов модуляции сигнала можно выделить:

1) хаотическую маскировку, при которой информационный сигнал суммируется с хаотическим сигналом и передается в канал связи;

2) переключение хаотических режимов, когда, например, в случае бинарного информационного сигнала символ «1» кодируется одним типом хаотического сигнала, а символ «0» – другим.

В таких алгоритмах формирование выходного сигнала осуществляется модуляцией информационной последовательностью хаотического сигнала на каждом единичном интервале t_0 разрядно-цифрового кода. Если в качестве информационной последовательности использовать ТСК, то применить такие алгоритмы не представляется возможным, так как значения моментов модуляции таймерного сигнала, сформированного на интервале времени $T_c = nt_0$ (где n – количество элементарных посылок; t_0 – их длительность), кратны не t_0, а некоторому базовому элементу Δ (где $\Delta = t_0/s$; $s = 1, 2, 3, ..., l$ – целые числа).

Так как в таймерных сигналах [2,3] расстояния между сигнальными конструкциями определяется величиной $\Delta < t_0$, то число реализаций $N_р$ ТСК на интервале T_c значительно увеличивается по сравнению с разрядно-цифровым кодом. В канал передаются отрезки сигнала длительностью

$$t_c = t_0 + k\Delta , \tag{1}$$

где $k = 0, 1, 2, ..., s \cdot (n - 2)$. Как следует из (1), таймерные сигналы представляют собой некоторый вид разрядно-цифровых кодов, в которых разрешенные для передачи сигнальные конструкции имеют не менее s (где $s = t_0/\Delta$) подряд передаваемых элементов Δ одного знака (1 или −1).

Для заданного значения s на интервале n единичных элементов число реализаций ТСК равно [2]

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

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

Для сигнальных конструкций с разным числом ЗММ

$$N_р = \sum_{i=1}^{n} \frac{[(n \cdot s) - [(s-1) \cdot i]]!}{i! \cdot [[(n \cdot s) - [(s-1) \cdot i]] - i]!} . \tag{3}$$

Изменяя параметры n, s и i можно получить различные множества таймерных сигналов, каждое из которых отличается длительностями, зависящими от значений n, числом базовых элементов s и числом переходов i, т. е. структурой сигнала на интервале времени T_c, чем достигается значительное повышение структурной и информационной скрытности передаваемых сигналов [2, 3].

На рис. 1 и 2 показаны графики числа реализаций в зависимости от значений s и n соответственно.

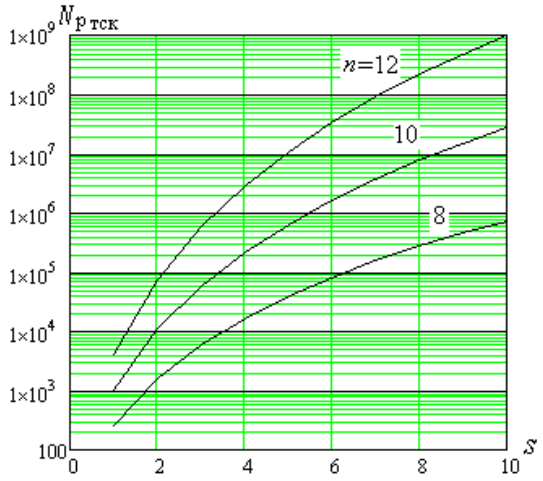

Рисунок 1 – Число реализаций ТСК в зависимости от значений при =8, 10, 12 и

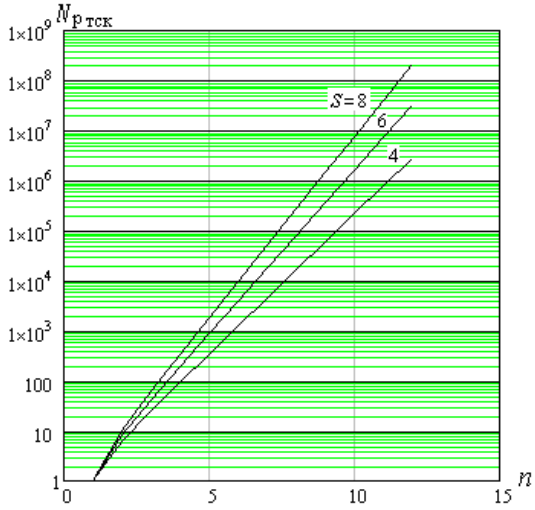

Рисунок 2 – Число реализаций ТСК в зависимости от значений при =4, 6, 8 и

Из рисунков видно, что при увеличении значений s и n число реализаций ТСК возрастает.

Графики числа реализаций в зависимости от значений i показаны на рис. 3.

Из приведенных графиков видно, что для получения максимального числа реализаций желательно использовать конструкции с разным числом информационных ЗММ на интервале формирования ТСК.

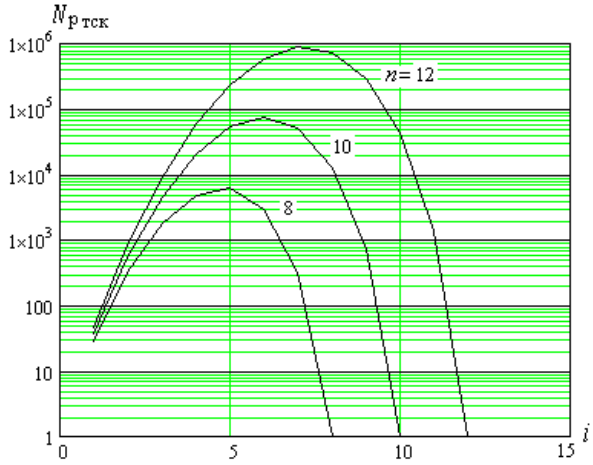

Рисунок 3 – Число реализаций ТСК в зависимости от значений (= 4) при = 8, 10, 12

Следуя [5], сформируем многоуровневую кодовую последовательность c_n на основе одной из реализаций хаотического сигнала $c(t)$, прошедшего дискретизацию по времени (используется теорема отсчетов) и квантование по уровню. Полученная последовательность c_n разбивается на сегменты определенной длины, равной длительностям таймерных сигналов $T_{\text{с}}$, которые и будут использоваться при построении сигнальных конструкций.

Пусть $x(T_{\text{с}})$ бинарный таймерный сигнал на интервале его формирования $T_{\text{с}} = nt_0$, а $c(T_{\text{с}})$ – многоуровневая кодовая последовательность c_n на этом же временном интервале $T_{\text{с}}$, которая характеризуется определенным количеством разрядов k, каждому из которых соответствует свой уровень. При этом длительность разрядов хаотической последовательности меньше Δ таймерного сигнала. Тогда синтез сигнально-кодовой конструкции $x_{\text{скк}}$ на интервале $T_{\text{с}}$ осуществляется путем перемножения значения уровня каждого разряда хаотической последовательности на значение уровня таймерного сигнала на данном временном интервале:

$$x_{\text{скк}}(T_{\text{с}}) = c_i(T_{\text{с}}) \times x_j(T_{\text{с}}), \tag{4}$$

т.е. происходит замена каждой положительной полярности («1») в бинарном таймерном сигнале отрезком прямой хаотической последовательности, а отрицательная полярность (−1)

заменяется продолжением той же последовательности, но с инвертированием значений ее разрядов. Использование прямой и инвертированной хаотической последовательности обеспечивает не только определение полярности в таймерном сигнале, но и позволяет регистрировать моменты смены фронтов на интервале T_c при корреляционном приеме.

На рис. 4 показано формирование выходного сигнала на передающей стороне системы конфиденциальной связи.

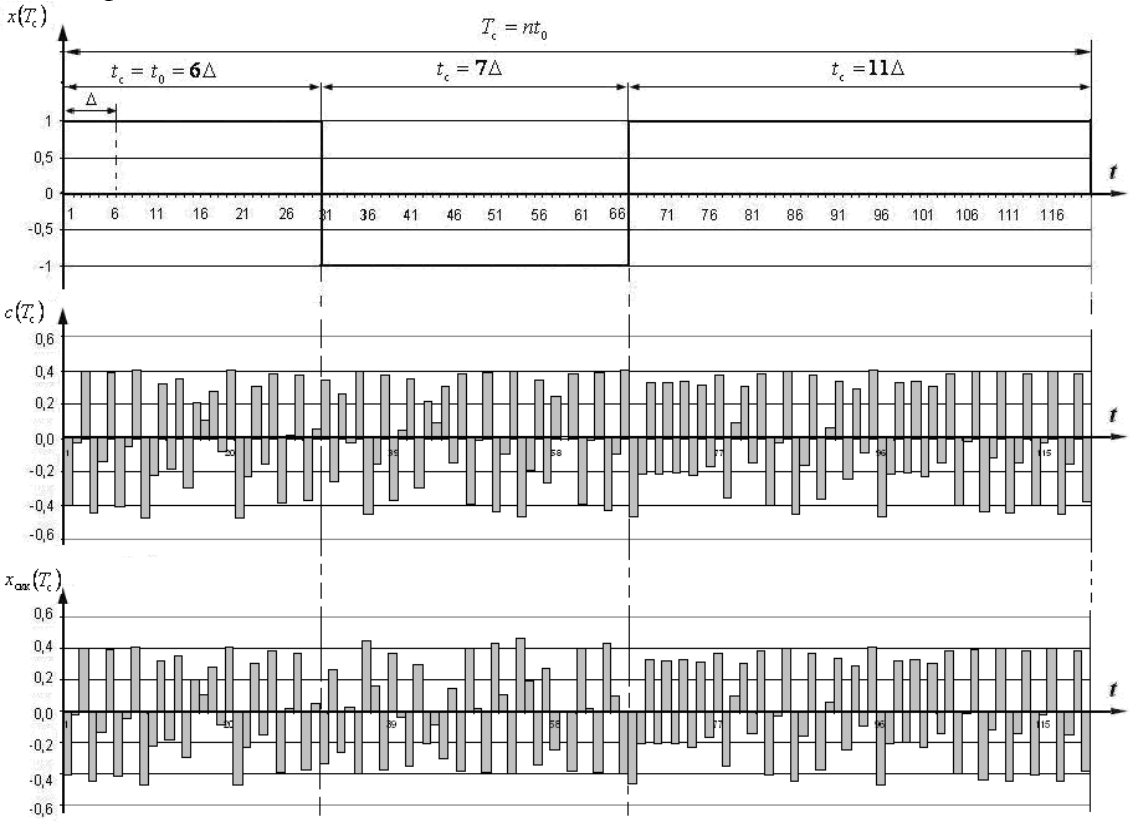

Рисунок 4 – Формирование выходного сигнала

Предполагая линейность системы и наличие идеальной синхронизации в канале, рассмотрим корреляционный прием такого сигнала. Пусть $x_{\text{скк}}'(T_c)$ сигнал на входе приемного устройства. Каждый разряд принятого сигнала $x_{\text{скк}}'(T_c)$ умножается на соответствующий разряд исходной прямой хаотической последовательности, известной на приеме:

$$y(T_c) = x_{i\,\text{скк}}'(T_c) \cdot c_i(T_c). \qquad (5)$$

Результаты каждого умножения с учетом амплитуды и значения полярности интегрируются в накопителе в пределах одного периода хаотической последовательности T_c. Решающее устройство отслеживает, уровни напряжения $U_{инт}$ в пределах этого периода, и по его максимальному или минимальному значению выносит решение о моменте и знаке z – смены полярности таймерного сигнала. После чего интегратор сбрасывается в нулевое состояние, а решающее устройство выдает принятую реализацию таймерного сигнала с задержкой на тактовый интервал T_c.

На рис. 5 показаны временные диаграммы корреляционного приема сигнала.

В работе [6] доказано, что сформированная на основе хаотической реализации кодовая последовательность обладает свойствами случайной последовательности, а в работах [2,3] показано, что при кодовом разделении сигналов использование ТСК (вместо

разрядно-цифрового кода) и сигнатуры со случайным чередованием 1 и −1 повышает структурную и информационную скрытность передаваемого сигнала.

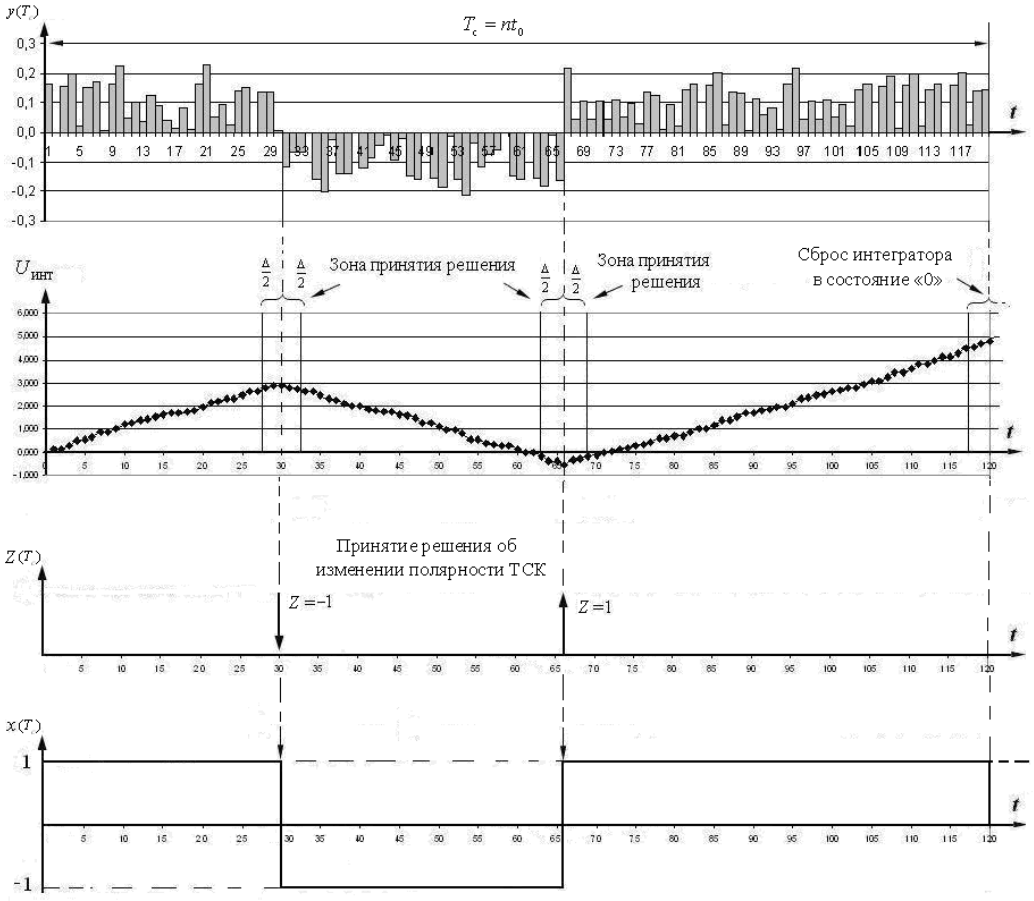

Рисунок 5 – Временные диаграммы корреляционного приема сигнала

В заключение можно сделать следующие выводы.

В статье разработан метод формирования сигнально-кодовых конструкций, который позволяет использовать корреляционный прием, а также повышает структурную и информационную скрытность передаваемых сигналов в системах конфиденциальной связи.

Литература

1. *Помехозащищенность* систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / [В.И. Борисов, В.М. Зинчук, А.Е. Лимарев и др.]; под ред. В.М. Борисова. – М.: Радио и связь, 2000. – 384 с.
2. *Захарченко Н.В.* Структурная скрытность таймерных сигналов в системах с кодовым разделением каналов / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Восточно-Европейский журнал передовых технологий. – 2011. – № 2/9(50). – С. 7–9.
3. *Захарченко Н.В.* Оценка информационной скрытности таймерных сигнальных конструкций в системах передачи конфиденциальной информации / Н.В. Захарченко, В.В. Корчинский, Б.К. Радзимовский // Збірник наукових праць ОНАЗ ім. О.С. Попова. – 2011. – № 1. – С. 3–8.
4. *Капранов М.В.* Регулярная и хаотическая динамика нелинейных систем с дискретным временем / М.В. Капранов, А.И. Томашевский. – М.: Издательский дом МЭИ, 2010. – 256 с.
5. *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.
6. *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.