Запропоновано метод формування сигнальних конструкцій на основі хаотичних і таймерних сигналів для застосування в конфіденційних системах передачі з метою підвищення скритності сигналів

Ключові слова: шумовий сигнал, динамічний хаос

Предложен метод формирования сигнальных конструкций на основе хаотических и таймерных сигналов для использования их в конфиденциальных системах передачи с целью повышения скрытности передаваемых сигналов

Ключевые слова: шумовой сигнал, динамический хаос

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 is proposed

Keywords: noise signal, dynamic chaos

УДК 691.321.25

ПОВЫШЕНИЕ СКРЫТНОСТИ ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА БАЗЕ ХАОТИЧЕСКИХ СИГНАЛОВ И ТАЙМЕРНЫХ СИГНАЛЬНЫХ КОНСТРУКЦИЙ

Н.В. Захарченко
Доктор технических наук, профессор, проректор по учебной работе*
В.В. Корчинский
Кандидат технических наук, доцент*
Контактный тел.: (048) 7067-982
Б.К. Радзимовский
Инженер*
Контактный тел. (048) 731-73-55
В.Й. Кильдишев
Кандидат технических наук, доцент*
Контактный тел.: 067-481-22-01
*Кафедра информационной безопасности и передачи данных
Одесская национальная академия связи им. А. С. Попова
ул. Кузнечная, 1, г. Одесса, Украина, 65029

1. Введение

Одним из приемов защиты конфиденциальной информации от несанкционированного доступа (НСД) в каналах связи является использование методов передачи сигналами, обеспечивающих высокою скрытность передачи. Способность системы передачи противостоять действиям, направленным на обнаружение сигнала и измерение его параметров, определяется скрытностью. При этом различают энергетическую, структурную и информационную скрытность сигналов [1]. Энергетическая скрытность характеризует способность системы противостоять мерам НСД, направленным на обнаружение факта передачи сигнала. Если станцией НСД сообщение перехвачено, то структурная скрытность должна противостоять мерам, направленным на 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 передаваемых сообщений с помощью сигналов информации [1].

В данной работе предложен метод формирования сигнальных конструкций для повышения структурной и информационной скрытности передаваемых сигналов. Исследования в данном направлении [2, 3, 4] были выполнены для хаотических и таймерных сигнальных конструкций (ТСК). В [2] показано, что применение хаотических сигналов в качестве переносчика информационного сигнала позволяет решать задачи по обеспечению энергетической скрытности передачи. В [3, 4] была дана оценка структурной и информационной скрытности ТСК, что позволило сделать вывод о перспективности их применения в конфиденциальных системах связи. Для задачи повышения структурной и информационной скрытности в [5] впервые показана возможность совместного применения хаотических сигналов и ТСК.

В связи с тем, что в современных системах связи защите конфиденциальной информации уделяется большое внимание, актуальным является развитие методов передачи, обеспечивающих повышение скрытности передачи.

Целью данной работы является усовершенствование метода формирования сигнальных конструкций на основе ТСК и хаотических сигналов [5].

2. Формирование сигнальных конструкций

Известно [1], что потенциальную структурную скрытность сигналов S можно повысить за счет увеличения ансамбля реализаций A, которая зависит от

количества всех возможных значений каких-либо параметров сигнала (например, несущая частота, структура кода, время прихода сигнала и др), т.е. скрытность зависит от способа построения конкретного вида сигнала.

Показатель S определяется числом двоичных измерений (д.из), которое необходимо произвести для задачи раскрытия структуры сигнала без знания алгоритмов обработки. Общее выражение для потенциальной скрытности имеет вид

$$S^* = \log_2 A \qquad (1)$$

В [3] показано, что увеличение показателя скрытности S возможно за счет изменения в каждом j-ом сеансе передачи своего ансамбля реализации A_j. Тогда общий ансамбль реализаций

$$S^* = \log_2 A_{общ} , \qquad (2)$$

где $A_{общ} = \sum_{j}^{N} A_j$ – суммарный ансамбль реализаций используемых сигналов.

Рассмотрим возможность расширения ансамбля передаваемых сигналов за счет совместного применения ТСК и хаотических сигналов. Оценим возможность получения различного ансамбля реализации A_j на основе ТСК.

Построение реализаций ТСК осуществляется с учетом полосы пропускания ΔF. Для этого выбираются базовый элемент Δ и временной интервал формирования $T_c = mt_0$, где t_0 – длительность элементарной посылки РЦК; n – количество элементов t_0. В ТСК расстояние τ_c между значащими моментами модуляции (ЗММ) не меньше интервала Найквиста ($t_0 = 1/\Delta F$), но и не кратно ему. Значение τ_c кратно временному отрезку $\Delta = t_0/s$ (s ∈ 2, 3, ... k), а расстояние между ЗММ $\tau_c = t_0 + \Delta \times l$ ($l \in 0, 1, 2, 3, \ldots$). Такое расстояние обеспечивает устранение межсимвольных искажений в ТСК. Значение s показывает, насколько меньше Δ по отношению к t_0. Число переходов i в ТСК может быть различным и меняться в пределах $i = 1,2, ..., n-1$.

Выбор значений Δ, s, n и i [3, 4] может быть использовано при решении задачи:

1) обеспечения помехоустойчивой передачи с заданными корректирующими способностями ТСК [4];

2) шифрования сообщения, при котором задается определенный ансамбль реализаций сигнальных конструкций $A_j^{тск}$.

Например, для формирования различных множеств $A_j^{тск}$ могут использоваться сигнальные конструкции с постоянным или различным числом переходов. Ансамблю реализаций ТСК с постоянным ЗММ для заданного значения s на интервале n соответствует выражение [2]

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

Для сигнальных конструкций с разным числом ЗММ

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

Также возможно построение различных множеств $A_j^{тск}$ которые отличаются количеством элементов n, на котором осуществляется построение сигнальных конструкций. Таким образом, варьированием параметрами s, n и i можно сформировать исходное количество множеств $A_j^{тск}$ для передачи конфиденциальной информации [4].

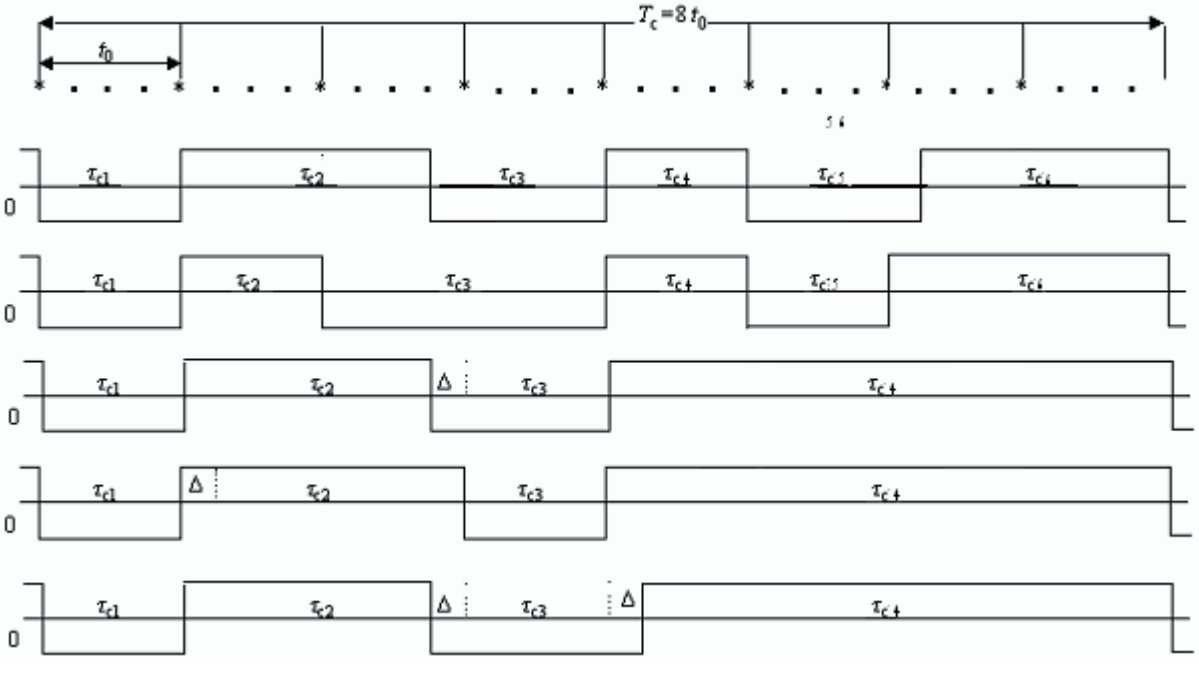

Рис. 1. Реализация таймерних сигнальных конструкций

На рис. 1 показан пример построения сигнальных конструкций с постоянным и различным числом ЗММ i при значении n = 8.

Вопросы получения различных множеств $A_j^{тск}$ в зависимости от параметров s, n и i были рассмотрены в работе [4]. Результаты исследований показали, что при увеличении значений s и n число реализаций ТСК возрастает. Для получения максимального числа реализаций желательно использовать конструкции с разным числом информационных ЗММ на интервале формирования ТСК.

Рассмотрим алгоритм формирования сигнальной конструкции на основе ТСК и хаотических сигналов на передающей стороне. Для интервала T_c выбира-

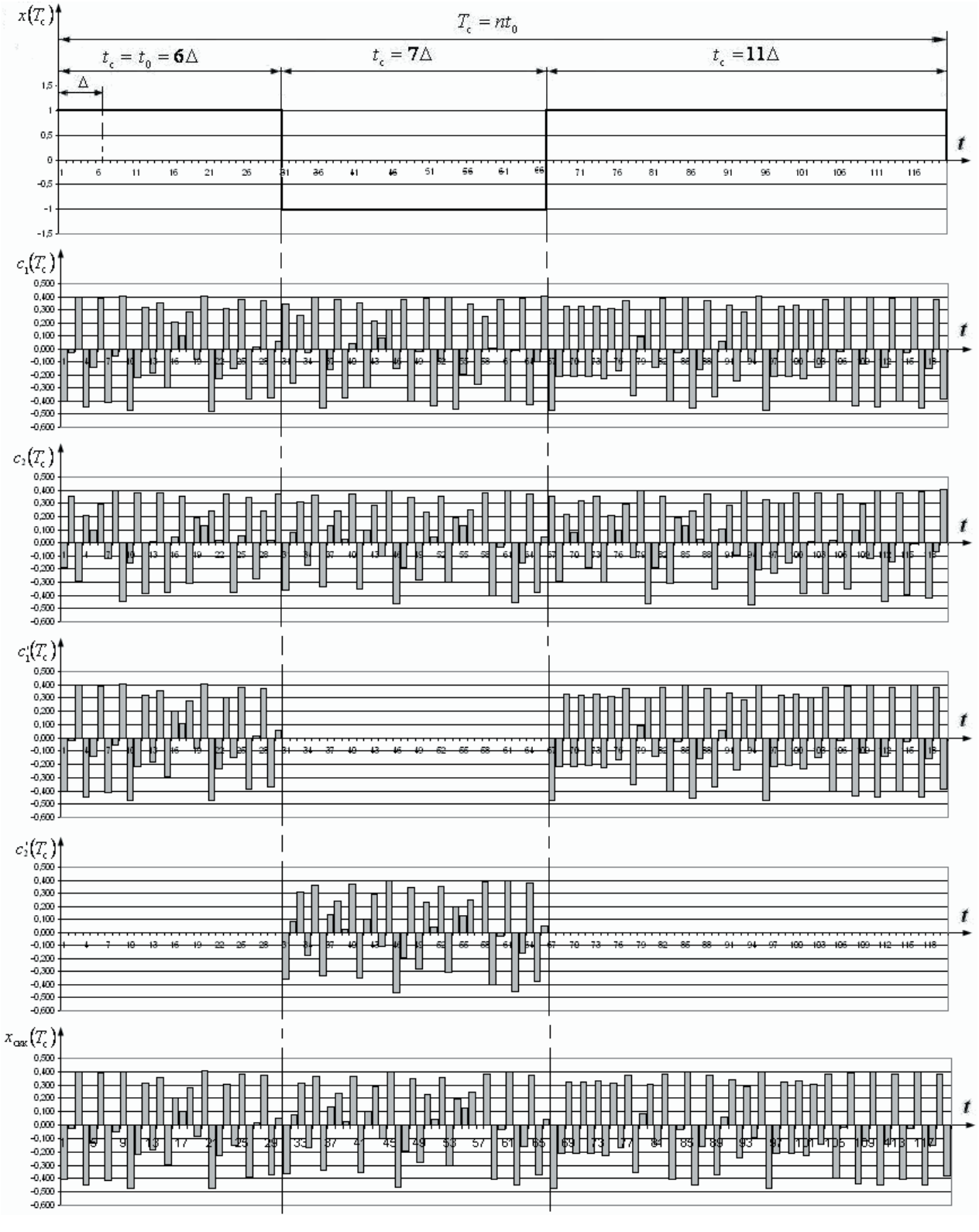

Рис. 2. Формирование выходного сигнала

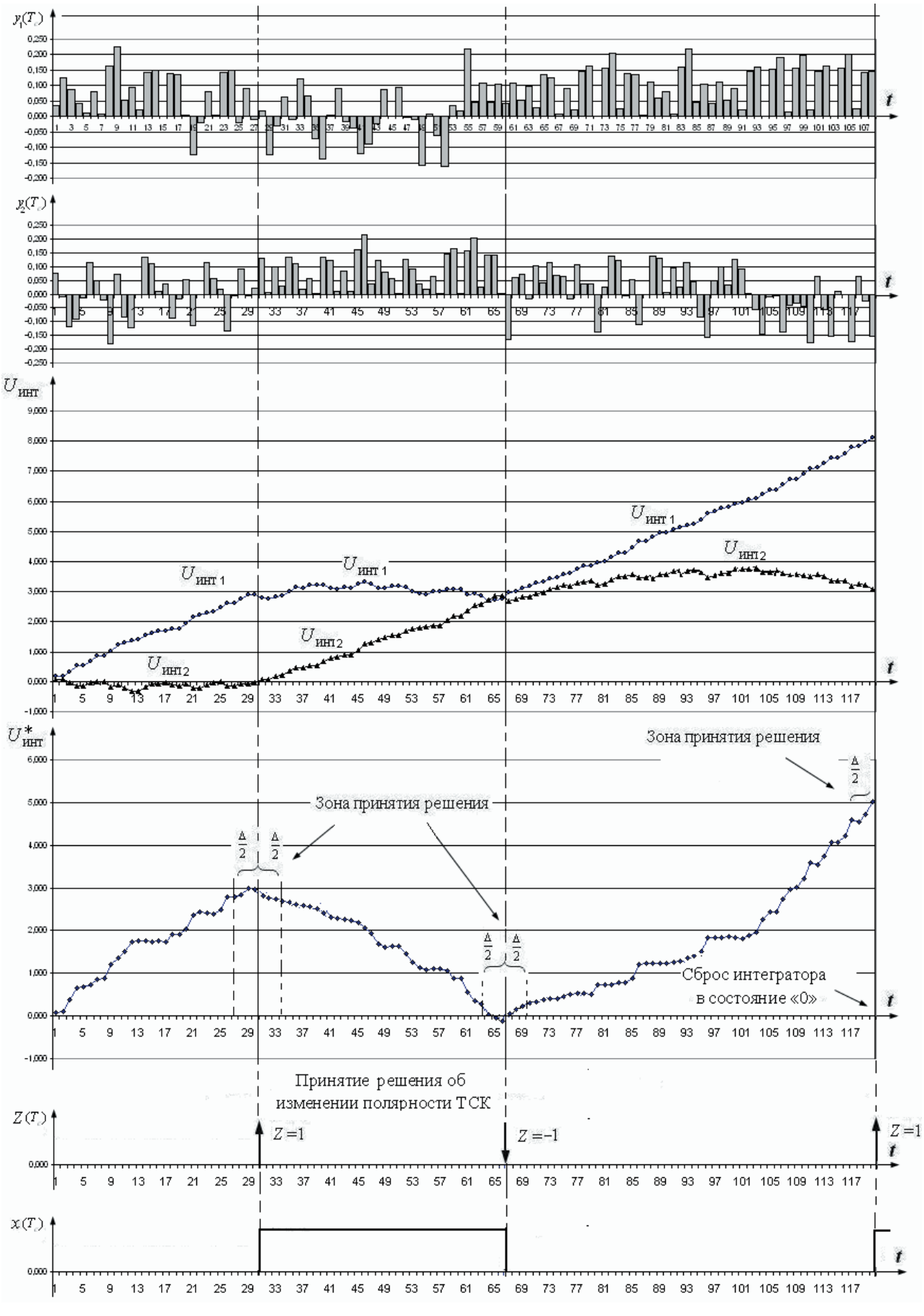

Рис. 3. Временные диаграммы корреляционного приема сигнала

ются две ортогональные по отношению друг к другу реализации хаотического сигнала c_1 и c_2 (рис. 2). На их основе формируется многоуровневые кодовые последовательности $c_1(T_c)$ и $c_2(T_c)$ (рис. 2), прошедших дискретизацию по времени (согласно теореме отсчетов) и квантование по уровню. Полученные последовательности $c_1(T_c)$ и $c_2(T_c)$ будут использоваться при построении сигнальных конструкций. Для задачи эксперимента опытным путем были подобраны слабокоррелированные последовательности $c_1(T_c)$ и $c_2(T_c)$, коэффициент корреляции которых составил $2{,}039\times10^{-4}$.

Пусть $x(T_c)$ бинарный таймерный сигнал на интервале его формирования $T_c = nt_0$, а $c_1(T_c)$ и $c_2(T_c)$ – многоуровневые кодовые последовательности на этом же временном интервале T_c. При этом длительность разрядов хаотической последовательности меньше Δ таймерного сигнала. Синтез сигнально-кодовой конструкции $x_{скк}(T_c)$ на интервале T_c осуществляется путем перемножения значения уровня каждого разряда хаотической последовательности $c_1(T_c)$ на значение положительного уровня таймерного сигнала $x_j(>0;T_c)$ на данном временном интервале, а значение отрицательного уровня $x_j(<0;T_c)$ по модулю умножается на значение разряда $c_2(T_c)$, т.е. происходит замена каждой положительной полярности («1») в бинарном таймерном сигнале выборкой сигналов из хаотической последовательности $c_1(T_c)$, а отрицательная полярность («–1») заменяется продолжением выборки из последовательности $c_2(T_c)$. Использование выборок хаотического сигнала из последовательностей $c_1(T_c)$ и $c_2(T_c)$ обеспечивает не только определение полярности в таймерном сигнале, но и позволяет регистрировать моменты смены фронтов на интервале T_c при корреляционном приеме, т.е.

$$x_{скк}(T_c) = c_{1i}(T_c)\times x_j(>0;T_c) + c_{2i}(T_c)\times\left|x_j(<0;T_c)\right| . \quad (5)$$

Временные диаграммы формирования выходного сигнала на передающей стороне системы конфиденциальной связи показаны на рис.2.

Предполагая линейность системы и наличие идеальной синхронизации в канале, рассмотрим корреляционный прием такого сигнала. Пусть $x_{скк}(T_c)$ сигнал на входе приемного устройства. Каждый разряд принятого сигнала $x_{скк}(T_c)$ умножается на соответствующий разряд хаотической последовательности $c_1(T_c)$ и $c_2(T_c)$, известных на приеме:

$$y_1(T_c) = x_{iскк}'(T_c)\times c_{1i}(T_c) \quad (6)$$

$$y_2(T_c) = x_{iскк}'(T_c)\times c_{2i}(T_c) . \quad (7)$$

Результаты каждого умножения с учетом амплитуды и значения полярности интегрируются в двух накопителях в пределах одного периода хаотической последовательности T_c. Уровни напряжения $U_{инт1}$ и $U_{инт2}$ интеграторов складываются и фиксируются в суммирующем устройстве для принятия решения о полярности принятого импульса ТСК. Решающее устройство отслеживает уровни напряжения $U^*_{инт}$ в пределах временного отрезка T_c и по его максимальному или минимальному значению выносит решение о знаке z и моменте смены полярности таймерного сигнала. По истечении интервала T_c интегратор сбрасывается в нулевое состояние, а решающее устройство выдает принятую реализацию таймерного сигнала с задержкой на тактовый интервал T_c.

На рис. 3 показаны временные диаграммы корреляционного приема сигнала.

Выводы

Анализ приема сформированной сигнальной конструкции с помощью двух корреляторов показал принципиальную возможность регистрации значащих моментов восстановления (ЗМВ) импульсов ТСК. Однако на точность принятия решения о ЗМВ могут повлиять свойства используемых последовательностей хаотического сигнала $c_1(T_c)$ и $c_2(T_c)$, ортогональность которых должна соблюдаться не только в пределах интервала T_c, но и в пределах временных интервалов τ_c между отдельными выборками. Такие требования, с одной стороны, делают достаточно трудоемкий процесс выбора последовательностей хаотического сигнала, однако, с другой стороны, позволяют существенно увеличить ансамбль используемых сигналов при передаче для задачи повышения структурной и информационной скрытности сигналов.

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. Захарченко, Н. В. Метод формирования сигнальных конструкций на основе хаотических и таймерных сигналов в системах передачи конфиденциальной информации/ Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Збірник наукових праць ОНАЗ ім.О.С.Попова. –2011. – № 2. – С. 3–7.
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.