

**МЕТОД ФОРМИРОВАНИЯ СИГНАЛЬНЫХ КОНСТРУКЦИЙ НА ОСНОВЕ  
ТАЙМЕРНЫХ СИГНАЛОВ И ПОСЛЕДОВАТЕЛЬНОСТЕЙ УОЛША**

*Корчинский В. В.*

*Одесская национальная академия связи им. А.С. Попова,  
65029, Украина, г. Одесса, ул. Кузнечная, 1.  
vladkorchin@rambler.ru*

**МЕТОД ФОРМУВАННЯ СИГНАЛЬНИХ КОНСТРУКЦІЙ НА ОСНОВІ ТАЙМЕРНИХ  
СИГНАЛІВ І ПОСЛІДОВНОСТЕЙ УОЛША**

*Корчинський В. В.*

*Одеська національна академія зв'язку ім. О.С. Попова,  
65029, Україна, м. Одеса, вул. Ковальська, 1.  
vladkorchin@rambler.ru*

**THE METHOD OF FORMING SIGNAL CONSTRUCTIONS BASED ON TIMER  
SIGNALS AND THE WALSH SEQUENCE**

*Korchynskii V.V.*

*O.S. Popov Odessa national academy of telecommunications,  
1 Kovalska St., Odessa, Ukraine, 65029  
vladkorchin@rambler.ru*

**Аннотация.** Противодействие средствам радиотехнической разведки и несанкционированного доступа является важнейшей задачей при построении конфиденциальных систем связи, поэтому актуальным является разработка и исследование методов передачи, которые позволяют увеличить скрытность передаваемых сигналов в канале связи. Для увеличения структурной скрытности предлагается усложнять структуру передаваемых сигналов. Одним из путей решения данной проблемы является применение таймерных сигнальных конструкций, на основе которых можно создавать различные множества сигнальных конструкций. Такие свойства сигналов особенно важны при разработке алгоритма сигнальных конструкций с изменяемой структурой.

Предложен метод формирования широкополосных сигналов на основе таймерных сигнальных конструкций и последовательностей Уолша. Рассмотрены особенности корреляционного приема широкополосных таймерных сигнальных конструкций. Показаны возможности улучшения основных качественных показателей системы связи с кодовым разделением каналов.

**Ключевые слова:** таймерная сигнальная конструкция, скрытность, канал, энергетическое расстояние, база.

**Анотація.** Протидія засобам радіотехнічної розвідки і несанкціонованого доступу є найважливішим завданням при побудові конфіденційних систем зв'язку, тому актуальним є розробка і дослідження методів передавання, які дозволяють збільшити скритність передаваних сигналів в каналі зв'язку. Для збільшення структурної скритності пропонується ускладнювати структуру передаваних сигналів. Одним зі шляхів вирішення даної проблеми є застосування таймерних сигнальних конструкцій, на основі яких можна створювати числені сигнальні конструкції. Такі властивості сигналів особливо важливі при розробці алгоритму сигнальних конструкцій зі змінюваною структурою.

Запропоновано метод формування широкосмугових сигналів на основі таймерних сигнальних конструкцій і послідовностей Уолша. Розглянуто особливості кореляційного прийому широкосмугових таймерних сигнальних конструкцій. Показано можливості поліпшення основних якісних показників системи зв'язку з кодовим розділенням каналів.

**Ключові слова:** таймерна сигнальна конструкція, прихованість, канал, енергетична відстань, база.

**Abstract.** Counteraction of radio electronic intelligence tools and unauthorized access is a major task in the construction of confidential communication systems, so actual is the development and research of methods of transmission, which allow to increase the secrecy of the transmitted signals in the communication channel. To increase the structural stealth proposed to complicate the structure of the transmitted signals.

One way to solve this problem is the use of timer signal constructions on which you can create different sets of signal constructions. Such signals properties are especially important in the design of algorithm signal constructions with variable structure.

Proposed the method of forming noise signals based on the timer signal constructions and Walsh sequences. The features of the correlation reception broadband timer signal constructions is considered. The possibilities of improving the basic quality indicators of the communication system with code division multiplexing is shown.

**Key words:** timer signal constructions, stealth, channel, energetic distance, base.

Одним из наиболее важных требований, предъявляемых к конфиденциальной системе связи (КСС) является обеспечение заданной помехозащищенности [1], которая характеризует способность системы выполнять свои задачи с заданным качеством в условиях радиоэлектронного подавления (РЭП) и несанкционированного доступа (НСД). РЭП и НСД организуется радиотехнической разведкой (РР) противоборствующей стороны, которая включает три основные задачи: обнаружение факта работы КСС; идентификация структуры и параметров сигналов-переносчиков; раскрытие смыслового содержания перехваченного сообщения.

Способность КСС противостоять мерам радиотехнической разведки (РР) называется скрытностью, которая является одним из главных показателей помехозащищенности. В соответствии с задачами радиоразведки выделяют следующие основные виды скрытности: энергетическая, структурная и информационная [1]. Другим важным показателем помехозащищенности является помехоустойчивость, которая характеризуется способностью системы связи нормально функционировать, выполняя задачи по приему информации в условиях действия радиопомех, в том числе преднамеренных.

Энергетическая скрытность направлена на существенное затруднение обнаружения сигнала работающей КСС средствами РЭП (разведывательным приемным устройством). Данный вид скрытности в основном обеспечивается за счет энергетической скрытности сигналов-переносчиков с базой  $B \gg 1$ . Так в технологии многостанционного доступа с кодовым разделением каналов (Code Division Multiple Access – CDMA) для этой цели применяются шумоподобные сигналы (ШПС), формируемые на основе двоичных расширяющих последовательностей Уолша – метод DSSS (Direct Sequence Spread Spectrum). При этом закономерно, что увеличение энергетической скрытности передачи достигается за счет большей базы сигнала-переносчика, т.е. чем больше распределение энергии сигнала в большей полосе частот, тем меньше вероятность её обнаружения разведывательным приемным устройством РЭП на фоне помех.

В случае перехвата сообщения структурная скрытность направлена на затруднение измерения параметров сигнала-переносчика и идентификации структуры сигнала. Для повышения структурной скрытности целесообразно применение сигналов со сложной и изменяемой структурой, что даёт возможность, в перспективе, создавать сигналы-переносчики с криптозащищенной структурой уже на первом уровне модели OSI. Одним из путей решения данной проблемы является применение таймерных сигнальных конструкций (ТСК). Исследования, проведенные в [2, 3] показали, что за счет изменения параметров ТСК можно синтезировать различные множества сигнальных конструкций. Такие вариационные возможности ТСК позволяют усложнять и менять структуру сигнала, обеспечивая увеличение показателей структурной и информационной скрытности.

Дальнейшее увеличение структурной скрытности возможно за счет усложнения структуры сигнала, что осуществимо за счет увеличения базы сигнала  $B = t_0 \Delta F$  (где  $t_0$  – длительность сигнала;  $\Delta F$  – эффективное значение ширины спектра этого сигнала). Следовательно, для задачи противодействия средствам РР актуальным является исследование и развитие методов передачи, обеспечивающих скрытность передачи.

**Целью статьи** является разработка метода формирования сигнальных конструкций с базой  $B \gg 1$  на основе ТСК и последовательностей Уолша.

В данной статье в качестве расширяющих последовательностей предложено использовать последовательности Уолша [2]. Известно [2], что прямое расширение спектра информационного позиционного кода сигнала осуществляется модуляцией псевдослучайной последовательности на каждом единичном интервале  $t_0$  позиционного кода. Однако применить такой алгоритм расширения спектра к непозиционному коду не представляется возможным. Объясняется это тем, что значения моментов модуляции таймерных сигналов, которые формируются на интервале времени  $T_c = nt_0$  (где  $n$  – количество элементарных посылок;  $t_0$  – их длительность), кратны не  $t_0$ , а некоторому базовому элементу  $\Delta$  (где  $\Delta = t_0/s$ ;  $s = 1, 2, 3, \dots, l$  – целые числа).

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

$$t_c = t_0 + k\Delta, \quad (1)$$

где  $k = 0, 1, 2, \dots, s \cdot (n - 2)$ . 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  $\Delta$  одного знака («1» или «-1»).

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

$$N_p = \frac{[(n \cdot s) - [(s - 1) \cdot i]]!}{i! \cdot [(n \cdot s) - [(s - 1) \cdot i] - i]!}, \quad (2)$$

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

Для сигнальных конструкций с разным числом ЗММ

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

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 скрытности передаваемых сигналов [2, 3].

На рис. 1 приведен пример формирования нескольких реализаций бинарных ТСК на интервале времени  $T_c = 4t_0$  при базовом элементе  $\Delta$ .

Алгоритм прямого расширения спектра и выбор базы  $B$  псевдослучайной последовательности (ПСП) основан на особенностях построения таймерных сигналов. Если для позиционного кода бинарные ПСП применяются для расширения спектра сигнала на интервале  $t_0$  с базой  $B_{t_0}$ , то для непозиционных таймерных сигналов требуется база расширяющей последовательности  $B_{ТСК} = B_{t_0} \times n$  применительно ко всей длине временного интервала  $T_c$  при сохранении тактовой частоты в системе связи. Значение  $B_{ТСК}$  должно быть кратно числу  $N_\Delta = s \times n$ , где  $N_\Delta$  – число  $\Delta$  на интервале  $T_c$ . Например, если  $s = 4$ ,  $n = 4$ ,  $N_\Delta = 16$ , тогда для согласования ТСК и ПСП необходимо, чтобы  $B = 32; 64; 128 \dots$ . Если  $s = 4$ ,  $n = 3$ ,  $N_\Delta = s \times n = 12$ , тогда  $B = 12; 24; 48 \dots$ .

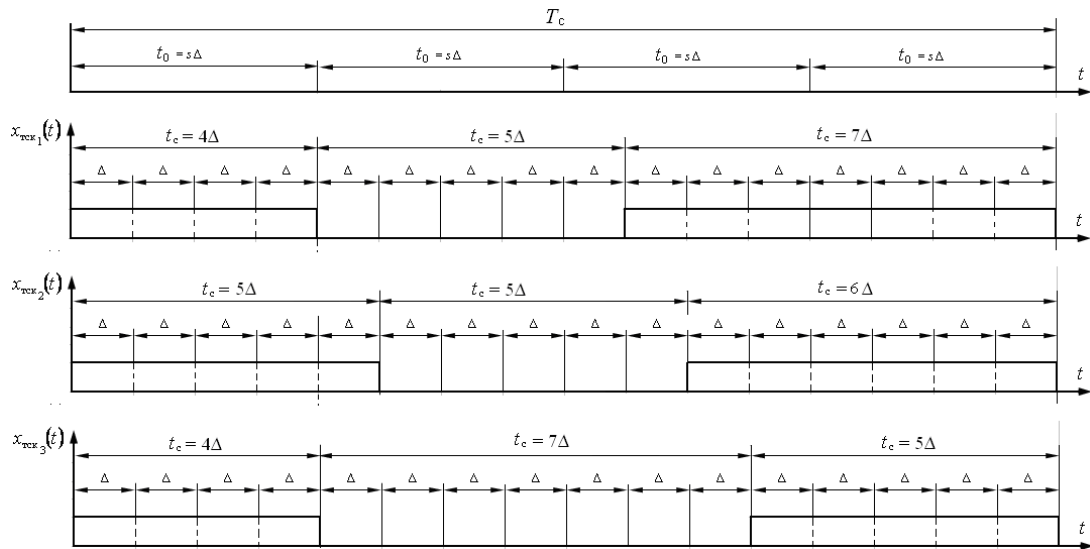


Рисунок 1 – Формирование трех реализаций ТСК на интервале времени  $T_c = 4t_0$  при базовом элементе  $\Delta$

Сформируем широкополосную последовательность  $x_{\text{срк}}(T_c)$  на основе ТСК. Пусть  $x(T_c)$  – бинарный таймерный сигнал на интервале его формирования  $T_c = nt_0$ , а  $c(T_c)$  – последовательность Уолша на этом же временном интервале  $T_c$ . При этом длительность элементов  $\tau$  последовательности  $c(T_c)$  меньше или равно  $\Delta$ . Синтез сигнально-кодовой конструкции  $x_{\text{срк}}(T_c)$  на интервале  $T_c$  осуществляется путем перемножения значения уровня каждого  $i$ -го разряда последовательности  $c(T_c)$  на  $j$ -е значение уровня таймерного сигнала на данном временном интервале:

$$x_{\text{срк}}(T_c) = c_i(T_c) \times x_j(T_c), \quad (4)$$

т.е. происходит замена каждой положительной полярности («1») в бинарном таймерном сигнале отрезком прямой последовательности  $c(T_c)$ , а отрицательная полярность («-1») заменяется продолжением той же последовательности, но с инвертированием значений ее разрядов. Использование прямой и инвертированной последовательности  $c(T_c)$  обеспечивает не только определение полярности в таймерном сигнале, но и позволяет регистрировать моменты смены фронтов на интервале  $T_c$  при корреляционном приеме.

На рис. 2 показано формирование выходного сигнала на передающей стороне системы конфиденциальной связи.

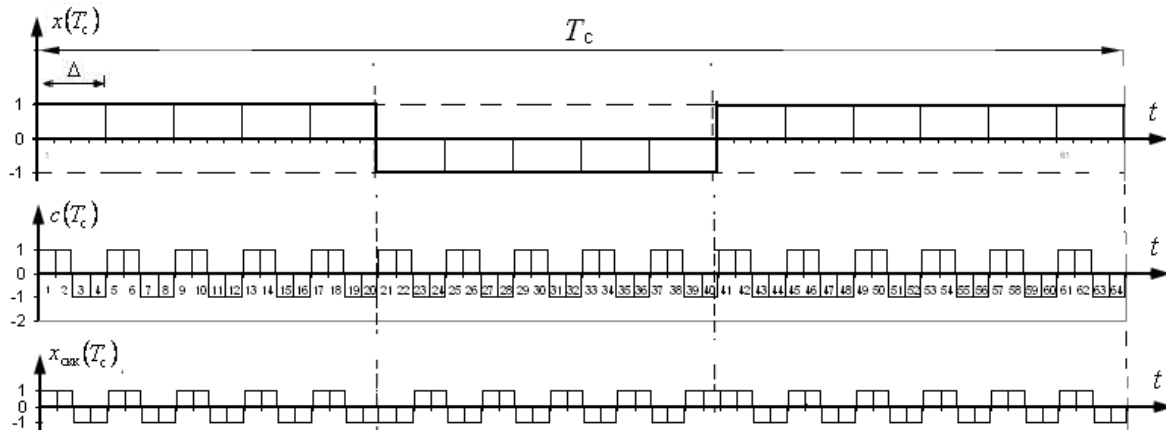


Рисунок 2 – Формирование выходного сигнала

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 последовательности  $c(T_c)$ , известной на приеме:

$$y(T_c) = x_{i_{\text{СКК}}}'(T_c) \times c_i(T_c). \quad (5)$$

Результаты каждого умножения с учетом амплитуды и значения полярности интегрируются в накопителе в пределах одного периода псевдослучайной последовательности  $c(T_c)$ . Решающее устройство отслеживает уровни напряжения  $U_{\text{инт}}$  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. 3 показаны временные диаграммы корреляционного приема сигнала.

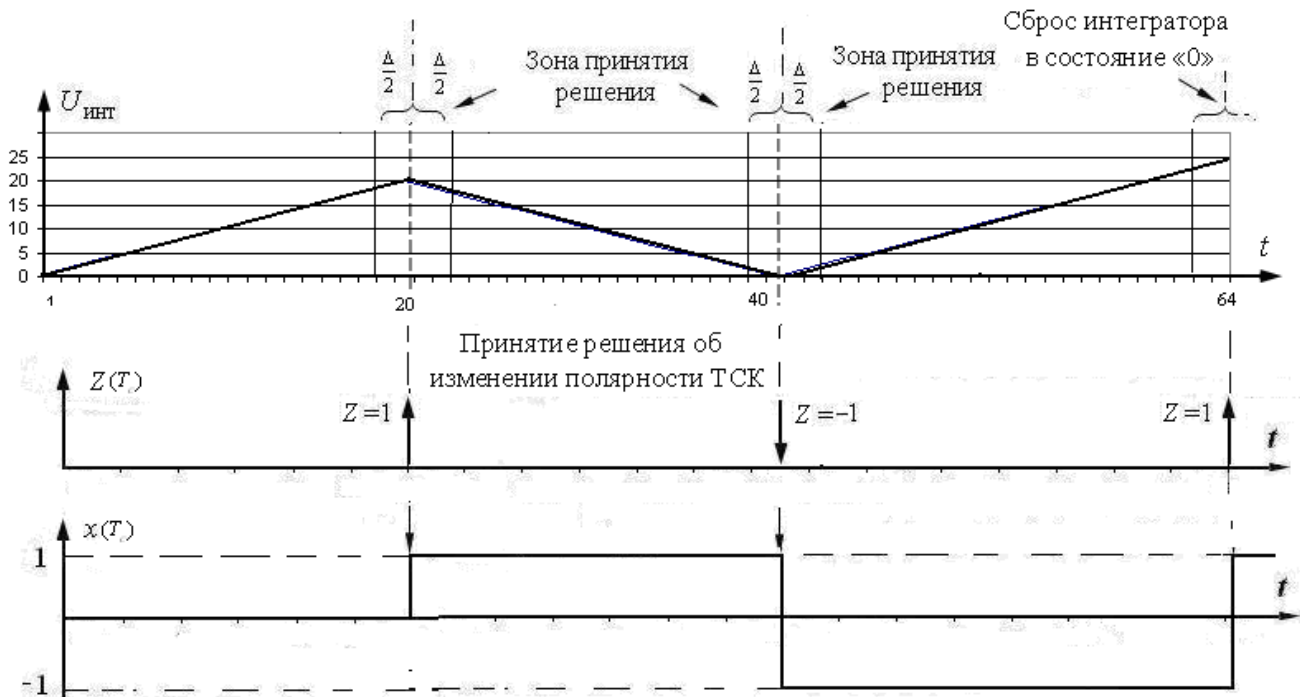


Рисунок 3 – Временные диаграммы корреляционного приема сигнала

В заключение можно сделать следующие выводы.

Предложенный метод формирования широкополосных сигналов на основе ТСК и последовательностей Уолша позволяет повысить не только структурную скрытность передаваемых сигналов, но и число используемых абонентов в системе с кодовым разделением или скорость передачи в индивидуальных каналах. В этом случае требуется увеличение длины расширяющей ПСП в  $n$  раз при сохранении тактовой частоты их следования.

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.

REFERENCES:

1. Pomehozaschischnost sistem radiosvyazi s rasshireniem spektra signalov metodom psevdosluchainoi perestroiki rabochei chastoti / [V.I. Borisov, V.M. Zinchuk, A.E. Limarev i dr.]; pod red. V.M. Borisova. – M.: Radio i svyaz, 2000. – 384 s.
2. Zaharchenko N. V. Strukturnaya skritnost taimernih signalov v sistemah s kodovim razdeleniem kanalov / N. V. Zaharchenko, V. V. Korchinskii, B. K. Radzimovskii // Vostochno-Evropeiskii jurnal peredovih tehnologii. – 2011. – № 2/9 (50). – S. 7–9.
3. Zaharchenko N. V. Ocenka informacionnoi skritnosti taimernih signalnih konstrukcii v sistemah peredachi konfidencialnoi informacii/ N. V. Zaharchenko, V. V. Korchinskii, B. K. Radzimovskii // Zbirnik naukovih prac ONAZ im.O.S.Popova. – 2011. – № 1. – S. 3–8.