ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ

УДК 621.391

М. В. Захарченко, В. В. Корчинський, Б. К. Радзімовський, Ю. С. Горохов
Одеська національна академія зв'язку ім. О. С. Попова

ЕФЕКТИВНІСТЬ ПРЯМОГО РОЗШИРЕННЯ СПЕКТРА В СИСТЕМАХ ЗВ'ЯЗКУ З ТАЙМЕРНИМИ СИГНАЛАМИ

© Захарченко М. В., Корчинский В. В., Радзимовский Б. К., Горохов Ю. С., 2015

Запропоновано метод синтезу шумоподібних сигналів на основі таймерних сигнальних конструкцій (ТСК) і ортогональних псевдовипадкових послідовностей з бінарною фазовою модуляцією ФМ-2 (BPSK) у системах зв'язку з кодовим розділенням каналів (КРК). Оцінено ефективність використання ТСК в індивідуальних каналах з обмеженою смугою частот окремих абонентів системи передавання з КРК. Наведено алгоритм вибору параметрів таймерних сигналів і псевдовипадкових послідовностей у разі формування шумоподібних сигналів. Показана перспектива використання таймерних сигнальних конструкцій в конфіденційних системах зв'язку для завдання підвищення структурної прихованості шумоподібних сигналів.

Ключові слова: пряме розширення спектра, система з кодовим розділенням каналів, таймерні сигнальні конструкції, телекомунікаційна система.

N. V. Zakharchenko, V. V. Korchinskiy, B. K. Radzimovskiy, Y. S. Gorohov
Odesa National academy of Telecommunications n.a. O. S. Popov

EFFECTIVENESS OF THE DIRECT SEQUENCE SPREAD SPECTRUM FOR THE COMMUNICATION SYSTEMS BASED ON TIMING SIGNALS

© Zaharchenko M. V., Korchinsky V. V., Radzimovskiy B. K., Gorohov Y. S., 2015

Cryptographic systems are considered to be quite an effective mechanism for the protection of information, and they are used mainly in the upper levels of the reference model OSI. However, analysis of trends in cryptography and cryptanalysis confrontation shows that no matter how reliable was not used newly established cryptographic system, discrediting it eventually becomes apparent. Taking into account this fact, promising is the development of additional mechanisms for the protection of information circulating on the network. In the last decade a special interest in acquiring methods of information security, which are implemented on the ground level of the OSI reference model and are aimed at significant reduction in the effectiveness of the means of unauthorized access (unauthorized access), which include: an attempt to detect the fact of transfer and violation of the integrity of a transmitted message, intercepting communication session and recognition of the structure of the signal structures with subsequent decoding of cryptograms, etc. One of the ways of confrontation of confidential communications with NSD can use complex signals with cryptoprotection structure. A prerequisite for the formation of the requirements for the properties of structures and algorithms for signal transfer to ensure secrecy of information exchange, is the account of algorithmic and technological potential of modern means of unauthorized access. It follows that the relevant information to improve the security of information transfer is the study on the creation of algorithms of functioning of confidential communications and signal synthesis designs that enhance the various indicators of secrecy. In view of this, the aim is to develop a

method of forming a broadband noise-like signal based on the timer signal design (TSC) with binary phase demodulation. A method for synthesis of noise signals based on the TSC and orthogonal pseudorandom binary phase modulation with the FM-2 (BPSK) communication systems, code division multiplexing (AAC). The estimation had been performed of utilization efficiency of TSC in the individual channels with limited bandwidth transmission systems of individual subscribers to the CBC. An algorithm is proposed for selecting parameters of timing signals and pseudo-random sequence of the formation of noise-like signals. The prospects of using timer signal designs in confidential communication systems for the task of improving the structural stealth noise-like signals.

Key words: DSSS, CDMA, TSC, telecommunication system.

В последнее десятилетие особый интерес вызывают методы защиты информации, которые реализуются на первом уровне эталонной модели OSI [1] и направлены на существенное снижение эффективности действий средств несанкционированного доступа (НСД), к которым относятся: попытка обнаружения факта передачи и нарушение целостности передаваемого сообщения, перехват сеанса передачи и распознавание структуры сигнальных конструкций с последующей дешифрацией криптограммы и т.д. Одним из способов противоборства конфиденциальной системы связи с НСД может быть применение сложных сигналов с криптозащищаемой структурой. Обязательным условием при формировании требований к свойствам передаваемых сигнальных конструкций и алгоритмам передачи, обеспечивающим скрытность передачи, является учёт алгоритмического и технологического потенциала современных средств НСД. Из вышесказанного следует, что актуальными для повышения информационной безопасности передачи информации являются исследования по созданию алгоритмов работы конфиденциальных систем связи и синтеза сигнальных конструкций, которые обеспечивают повышение различных показателей скрытности. Учитывая сказанное, целью работы является разработка метода формирования широкополосного шумоподобного сигнала на основе таймерных сигнальных конструкции (ТСК) с бинарной фазовой демодуляцией.

Для формирования широкополосных шумоподобных сигналов (ШППС) чаще всего используется метод прямого расширения спектра, который реализуется с применением ортогональных псевдослучайных последовательностей (ПСП) и простейшей формой бинарной фазовой модуляции ФМ-2 (BPSK). В предложенном алгоритме формирования широкополосных таймерных сигналов важным является согласование параметров построения ТСК [2, 3] с особенностями структуры ортогональной ПСП и её базы $B_{\text{псп}}$ [1].

Ортогональные ПСП близки по своим свойствам к шумоподобным сигналам, в которых минимальная длительность элементарных посылок $t_{\text{ч}}$ намного меньше времени передачи информационного элемента t_0 [1], т.е. $B_{\text{инф}} >> B_{\text{псп}}$. В системе с кодовым разделением канала (КРК) информационный сигнал t_0 передается последовательностью чипов длительностью $t_{\text{ч}} << t_0$, за счет чего достигается расширение спектра передаваемого сигнала. Базовым элементом для формирования ТСК является элемент Δ, который в s раз меньше длительности элементарной посылки t_0, но в то же время больше $t_{\text{ч}}$. Такой подход позволяет исходную двоичную информационную последовательность передавать бинарной последовательностью ТСК.

Алгоритм прямого расширения спектра и выбор базы B 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 $B_{\text{ТСК}} = B_{t_0} \times n$ применительно ко всей длине временного интервала $T_{\text{с}}$ при сохранении тактовой частоты в системе связи. Значение $B_{\text{ТСК}}$ должно быть кратно числу $N_\Delta = s \times n$, где N_Δ – число Δ на интервале $T_{\text{с}}$. Например, если $s = 4$, $n = 4$, $N_\Delta = 16$, тогда для согласования ТСК и ПСП необходимо, чтобы $B = 32; 64; 128 \ldots$. Если $s = 4$, $n = 3$, $N_\Delta = s \times n = 12$, тогда $B = 12; 24; 48 \ldots$.

В качестве примера проанализируем формирование широкополосной ТСК со следующими параметрами:

1) $T = 4t_0$ – длительность элементарных посылок, на которой осуществляется построение сигнальной конструкции;

2) $s = 2$ – количество базовых элементов Δ на интервале t_0.

Обозначим через $x_k(t)$ информационный сигнал k-го пользователя. После перемежения и помехоустойчивого кодирования сигнал $x_k^{\text{ПК}}(t)$ формирователь ТСК преобразует в сигнал $x_k^{\text{ТСК}}(t)$. Сигнал $x_k^{\text{ТСК}}(t)$ умножается на сигнатуру $s_k(t)$ k-го пользователя.

Полученный сигнал

$$b_k(t) = x_k^{\text{ТСК}}(t) \cdot s_k(t) \tag{1}$$

поступает на бинарный фазовый модулятор, на выходе которого формируется сигнал

$$s_k(t; b_k) = x_k^{\text{ТСК}}(t) \cdot s_k(t) \cdot \cos(2pf_0 t). \tag{2}$$

На рис. 1 показан процесс прямого расширения спектра сигнальной конструкции $x_k^{\text{ТСК}}(t)$ сигнатурой $s_k(t)$ для одного из индивидуальных каналов.

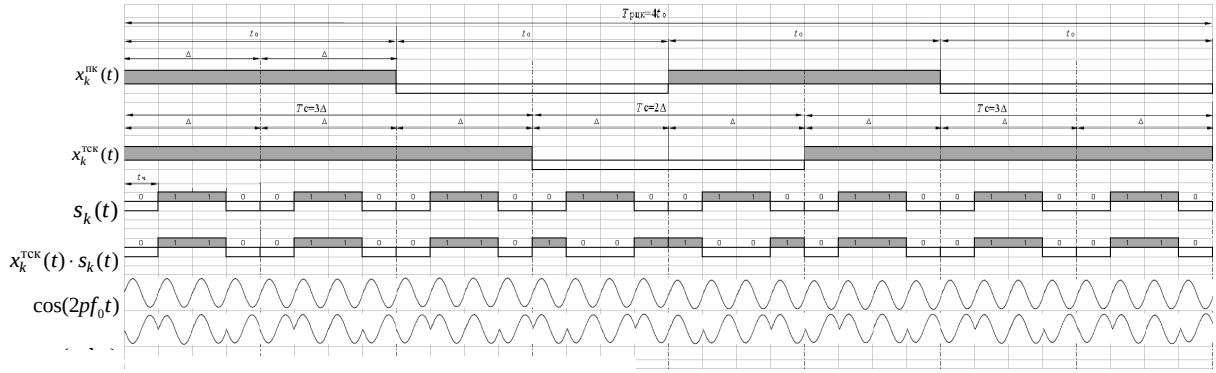

Рис. 1. Процесс прямого расширения спектра сигнальной конструкции $x_k^{\text{ТСК}}(t)$ *сигнатурой* $s_k(t)$

В результате распространения по каналу связи сигнал претерпевает ослабление, а также приобретает задержку и фазовый сдвиг. Предполагается, что их значения на приемной стороне известны, а также в приемнике обеспечены идеальная частотная, фазовая и тактовая синхронизация. На входе приемника получаем сигнал

$$s'_k(t; b_k) = x'^{\text{ТСК}}_k(t) \cdot s_k(t) \cdot \cos(2pf_0 t). \tag{3}$$

Для устранения расширения спектра сигнал $s'_k(t; b_k)$ умножается на формируемую в приемнике копию сигнатуры $s_k(t)$, синхронизированную с принимаемым сигналом. В результате сигнал представляет собой несущую $\cos(2pf_0 t)$ с бинарной фазовой манипуляцией $x_k^{\text{ТСК}}(t)$

$$s'_k(t; b_k) s_k(t) = s_k^2(t) \cdot x'^{\text{ТСК}}_k(t) \cdot \cos(2pf_0 t) = x'^{\text{ТСК}}_k(t) \cdot \cos(2pf_0 t), \tag{4}$$

где $s_k^2(t) = 1$ с учетом бинарности $s_k(t) = \pm 1$. На выходе фазового бинарного демодулятора получаем реализацию ТСК $x'^{\text{ТСК}}_k(t)$. На рис. 2 представлена упрощенная структурная схема приемной части системы с КРК. Процесс сжатия спектра сигнальной конструкции $x'^{\text{ТСК}}_k(t)$ для одного из индивидуальных каналов показан на рис. 3. Декодер ТСК осуществляет преобразование $x'^{\text{ТСК}}_k(t)$ в последовательность $x'^{\text{ПК}}_k(t)$, которая далее поступает на вход декодера помехоустойчивого кода. После декодирования и перемежения на выходе помехоустойчивого декодера получаем

информационный сигнал k-го пользователя $x'_k(t)$. Использование кодека ТСК позволяет на одном и том же интервале T_c сформировать больше разрешенных ТСК, чем сигнальных конструкций при разрядно-цифровом кодировании ($N = 2^n$).

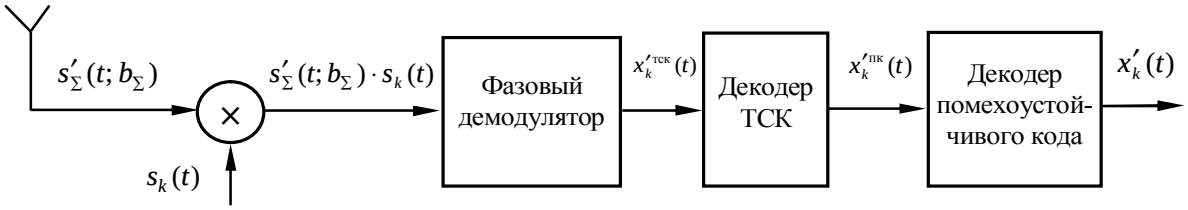

Рис. 2. Структурная схема приемной части системы с КРК

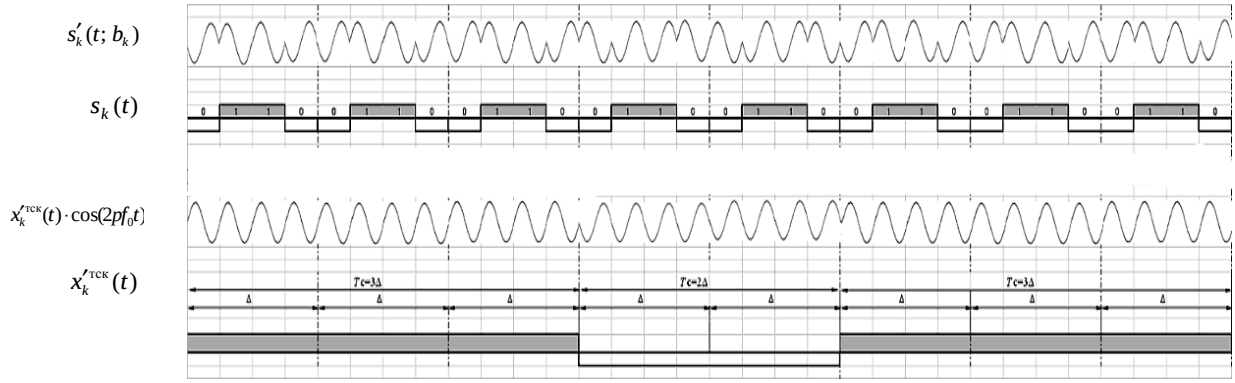

Рис. 3. Процесс сжатия спектра сигнальной конструкции $x'^{тск}_k(t)$

Предположим, что в качестве помехоустойчивого кода в индивидуальном канале на временном интервале $T_c = 9t_0$ сформирован 9-элементный код Слепяна (9, 5) с кодовым расстоянием $d = 3$, исправляющий однократные ошибки [4]. Но на этом же интервале $T_c = 9t_0$, в соответствии с [3], даже для $s = 3$ можно получить 18560 реализаций ТСК, эквивалентных 14-элементным бинарным кодовым словам. Следовательно, на интервале $T_c < 9t_0$ можно реализовать 13-элементный код Слепяна (13, 5) с кодовым расстоянием $d = 5$, позволяющий исправлять двукратные ошибки. Так как код (13, 5) позволяет исправлять двукратные ошибки, то доля неисправленных ошибок в канале Гильберта составит 0,1 от всех ошибок с учетом “плохого” состояния канала, в то время как после исправления однократных ошибок кодом (9, 5) доля неисправленных ошибок – 0,42 [3].

Вывод

В работе предложен метод формирования широкополосного шумоподобного сигнала на основе таймерных сигнальных конструкций, что позволило в каждом индивидуальном канале системы связи с КРК повысить скорость передачи системы в $1{,}4 \times N$ раз (где N − количество каналов в системе) или повысить качество приема в индивидуальных каналах.

1. Ипатов В. П. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения; пер. с англ. – М.: Техносфера, 2007. – 487 с. 2. Захарченко Н. В. Основы кодирования: учеб. пособие / Захарченко Н. В., Захарченко В. Н., Крысько А. С. – Одесса: УГАС им. А.С. Попова, 1999. – 240 с. 3. Захарченко М. В. Системи передавання даних. Том 1. Завадостійке кодування / Захарченко М. В. – Одеса: Фенікс, 2009. – 447 с. 4. Блейхут Р. Теория и практика кодов, контролирующих ошибки; пер. с англ. – М.: Мир, 1986. – 576 с.