УДК 621.391

МЕТОД ПОВЫШЕНИЯ СКРЫТНОСТИ ПЕРЕДАЧИ ТАЙМЕРНЫМИ СИГНАЛАМИ В СИСТЕМАХ СВЯЗИ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ

Корчинский В.В.

METHOD OF INCREASE OF RESERVE OF TRANSFER BY TIMER SIGNALS IN COMMUNICATION SYSTEMS WITH CODE DIVISION OF CHANNELS

Korchinskiy V.

Дана оценка эффективности использования таймерных сигнальных конструкций в индивидуальных каналах с ограниченной полосой частот отдельных абонентов системы связи с кодовым разделением каналов и рассмотрена возможность повышения структурной скрытности передачи при формировании группового сигнала.

Ключевые слова: *криптографические системы, информационная скрытность, групповой сигнал, таймерные сигналы.*

Криптографические системы считаются достаточно эффективным механизмом по защите информации и используются они в основном на верхних уровнях эталонной модели OSI. Однако анализ тенденции противостояния криптографии и криптоанализа показывает, что какой бы надежной не была б вновь созданная криптографическая система, её дискредитация [1] со временем становится очевидной. Принимая во внимание данный факт, перспективным является развитие дополнительных механизмов по защите информации, циркулирующей в сети.

Постановка проблемы в общем виде. В последнее десятилетие особый интерес приобретают методы защиты информации, которые реализуются на первом уровне эталонной модели OSI [2, 3] и направлены на существенное снижение эффективности действий средств несанкционированного доступа (НСД), к числу которых 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, обеспечивающих скрытность передачи, является учёт алгоритмического и технологического потенциала современных средств НСД.

Известно [7], что свойства сигнальных конструкций могут оцениваться по одному или нескольким показателям скрытности: энергетической, структурной, информационной и др.

Информационная скрытность [7] определяется способностью противостоять мерам, направленным на раскрытие смысла передаваемых сообщений с помощью сигналов информации. Этот показатель скрытности реализуется в основном на верхних уровнях эталонной модели OSI [1].

Качество защиты передаваемой информации от средств НСД на уровне физического канала оценивается показателем энергетической скрытности [2,7], который характеризует способность системы противостоять действиям НСД, направленным на обнаружение самого факта передачи сигнала и его перехвата. Известно [2-4], что перспективным решением проблемы энергетической скрытности являются методы передачи с помощью шумоподобных сигналов, при формировании которых осуществляется преднамеренное расширение спектра информационного сигнала таких как: псевдослучайная перестройка рабочей частоты (ППРЧ) (FHSS – Frequency Hopping Spread Spectrum); расширение спектра методом прямой псевдослучайной последовательности (ПСП) (DSSS – Direct Sequence Spread Spectrum) и др. Первоначально системы связи на основе ППРЧ и ПСП применялись после второй мировой войны в военных целях странами СССР и США для решения различных задач разведывательного характера. В настоящее время эти методы передачи используются при построении современных коммерческих систем связи многопользовательского доступа. В данной работе рассматривается метод расширения спектра информационного сигнала с помощь ПСП. В случае перехвата сообщения структурная скрытность должна противостоять мерам НСД, которые направлены на раскрытие структуры сигнала и измерение его параметров.

В работах [8, 9] был проведен анализ некоторых методов формирования сигнальных конструкций с иных теоретических позиций для оценки их возможностей по обеспечению функций защиты информации. Раздел теории информации и кодирования, рассматривающий методы формирования сигнальных конструкций на основе таймерного кодирования акцентировал своё научное внимание на вопросах повышения скорости передачи в бинарных каналах и обеспечения требуемой помехоустойчивости [5]. Однако таймерные сигнальные конструкции (ТСК) также представляют научный и практический интерес с точки зрения задачи повышения структурной и информационной скрытности передачи. Объясняется это большими вариационными возможностями построения различных множеств кодовых конструкций таймерных сигналов при несущественном комбинаторном изменении одного или нескольких из её параметров. Анализ методов формирования ТСК с учетом их свойств позволил сделать вывод о целесообразности их применения при разработке новых криптографических приемов шифрования и методов передачи информации по каналах связи. Также появилась возможность объединения процедур помехоустойчивого кодирования и шифрования на основе ТСК в единую задачу.

В работе [8] рассмотрена возможность увеличения структурной скрытности сигналов в каждом индивидуальном канале системы за счет совместного использования ТСК и псевдослучайных последовательностей. Представляет интерес дальнейшее развитие этого направления для задачи повышения структурной скрытности формируемых сигнальных конструкций группового сигнала в системах связи с кодовым разделением канала.

Таким образом, скрытность передачи является одним из важных показателей помехозащищенности. Другим не менее важным показателем помехозащищенности является помехоустойчивость [5], которая характеризует способность системы работать с заданным качеством в условиях воздействия различного рода помех. Связь этих двух показателей очевидна, так как при решении вопросов, направленных на повышение скрытности синтезируемых сигнальных конструкций, в первую очередь необходимо выполнить условие по обеспечению заданной верности передачи.

Из вышесказанного следует, что актуальным для повышения информационной безопасности передачи информации являются исследования по созданию алгоритмов работы конфиденциальных систем связи и синтезу сигнальных конструкций, которые обеспечивают повышение различных показателей скрытности.

Цель статьи. Учитывая сказанное, статья посвящена разработке метода формирования группового сигнала на основе ТСК в индивидуальных каналах с ограниченной полосой частот отдельных абонентов системы связи с кодовым разделением каналов (КРК).

Изложение основного материала. Потенциальная структурная скрытность определяется количеством двоичных измерений (д.из), которое необходимо выполнить для раскрытия структуры перехваченного сигнала без учёта алгоритмов его обработки на станции НСД [7]. Общее выражение для потенциальной скрытности имеет вид

$$S = \log_2 A, \qquad (1)$$

где А – множество реализаций, определяемый количеством всех возможных значений каких-либо параметров сигнала. Такими параметрами могут быть несущая частота, структура кода, время прихода сигнала и др. В общем случае скрытность зависит от способа построения конкретного вида сигнала.

Для увеличения структурной скрытности необходимо по возможности расширять множество используемых сигналов [7]. Известно, что в бинарном канале увеличить количество реализаций кодовых последовательностей на некотором интервале времени можно за счет применения ТСК [5].

Множество бинарных ТСК формируется на интервале времени $T_c = nt_0$ (n – количество элементарных посылок, t_0 – их длительность) при базовом элементе Δ ($\Delta = t_0/s$, $s \in 1, 2, 3, ..., l$ – целые числа).

В отличие от разрядно-цифрового кодирования, когда информация о передаваемом разряде определяется уровнем сигнала элементарной посылки, в ТСК информация заложена в нескольких отдельных временных интервалах сигнала $t_c = t_0 + k\Delta$ ($k \in 0, 1, 2, ..., s \cdot (n-2)$) и их взаимном положении на интервале формирования T_c. Пример формирования нескольких реализаций бинарных ТСК на интервале времени $T_c = 4t_0$ при базовом элементе Δ показан на рис. 1.

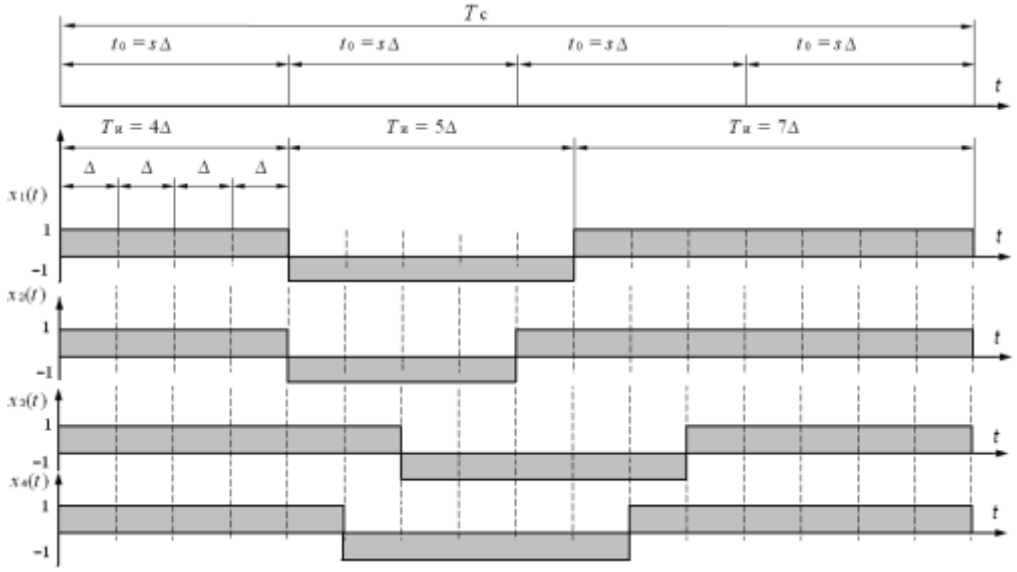

Рис. 1. Формирование реализаций бинарных ТСК на интервале времени $T_c = 5t_0$ при базовом элементе Δ

Из рисунка следует, что таймерные сигналы представляют собой вид разрядно-цифровых кодов (РЦК), в которых разрешенные для передачи сигнальные конструкции имеют не менее S подряд передаваемых элементов Δ одного знака («1» или «−1»).

Такой метод формирования позволяет передавать в канал отрезки сигнала длительностью $t_c \geq \Delta \cdot (s+i)$, где $i = 0,1,2,3\ldots$, что исключает межсимвольные искажения. С другой стороны не кратность t_c величине t_0 позволяет уменьшить расстояния между сигнальными конструкциями до величины Δ.Это позволяет получить число реализаций ТСК $N_{\text{р}}$ на интервале nt_0 больше 2^n. При заданном s ($s = t_0/\Delta$) на интервале n единичных элементов число реализаций сигнального алфавита бинарных ТСК равно [9]

$$N_{\text{р}} = \frac{\left[(n \cdot s) - \left[(s-1) \cdot i\right]\right]!}{i! \cdot \left[\left[(n \cdot s) - \left[(s-1) \cdot i\right]\right] - i\right]!}, \quad (2)$$

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

При применении сигнальных конструкций с разным числом ЗММ

$$N_{\text{р}} = \sum_{i=1}^{n} \frac{\left[(n \cdot s) - \left[(s-1) \cdot i\right]\right]!}{i! \cdot \left[\left[(n \cdot s) - \left[(s-1) \cdot i\right]\right] - i\right]!}. \quad (3)$$

Оценим изменение ансамбля реализаций ТСК $N_{\text{р тск}}$ в зависимости от параметров n, s и i. На рис. 2 приведены зависимости $N_{\text{р тск}}$ от n, s и $i = 1\ldots n$.

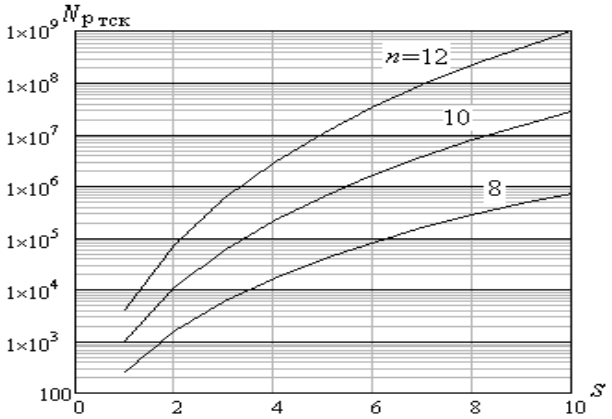

Рис. 2. Количество реализаций ТСК в зависимости от s при значениях n=8, 10, 12

Из рисунка видно, что количество реализаций ТСК существенно увеличивается с ростом n и s при $i=1\ldots n$ по сравнению с РЦК.

На рис. 3 представлены зависимости структурной скрытности ТСК от изменения параметров n, s и i. Как видно из рисунка структурная скрытность ТСК увеличивается с ростом n и s при $i=1\ldots n$.

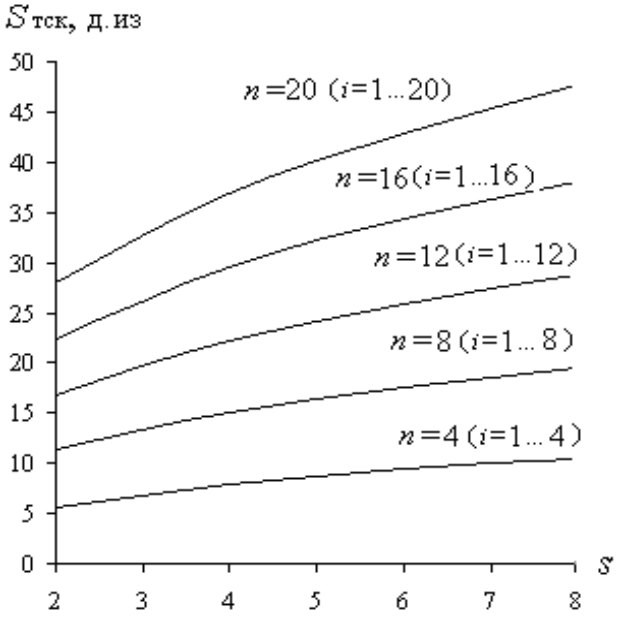

Рис. 3. Зависимости структурной скрытности ТСК от параметров n, s и i

Рассмотрим формирование широкополосного сигнала (ШПС) методом прямого расширения спектра (ПРС) с применением ортогональных псевдослучайных последовательностей (ПСП). Такие последовательности близки по своим свойствам к шумоподобным сигналам, в которых длительность элементов $t_ч$, называемых чипами, намного меньше времени передачи бита сообщения t_0 [4].

Анализ построения ТСК [5] и ШПС [4] на базе ортогональных псевдослучайных послідовательностей для систем с КРК позволил выделить следующие особенности по их формированию. В системе с КРК сигнал t_0 передается последовательностью чипов длительностью $t_ч < t_0$, 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 при этом больше $t_ч$.

В качестве примера проанализируем передачу одной из возможных реализаций ТСК с помощью ШПС в системе с КРК на интервале $T = 4t_0$ при $s = 2$.

Обозначим через $x_k(t)$ информационный сигнал k–го пользователя. После перемежения и помехоустойчивого кодирования сигнал $x_k^{пк}(t)$ преобразуется формирователем ТСК в сигнал $x_k^{тск}(t)$. Сигнал $x_k^{тск}(t)$ умножается на сигнатуру $s_k(t)$ k–го пользователя. Полученный сигнал

$$b_k(t) = x_k^{тск}(t) \cdot s_k(t) \quad (4)$$

поступает на фазовый модулятор, на выходе которого формируется сигнал

$$s_k(t; b_k) = x_k^{тск}(t) \cdot s_k(t) \cdot \cos(2\pi f_0 t) \quad (5)$$

На рис. 4 представлена упрощенная структурная схема передающей части системы с КРК. Для наглядности на рис. 5 показан процесс прямого расширения спектра сигнальной конструкции $x_k^{тск}(t)$ сигнатурой $s_k(t)$ для одного из индивидуальных каналов.

В результате распространения по каналу связи сигнал претерпевает ослабление, а также приобретает задержку и фазовый сдвиг. Предполагаем, что их значения на приемной стороне известны, а также в приемнике обеспечены идеальная частотная, фазовая и

тактовая синхронизация. На входе приемника получаем сигнал

$$s'_k(t;b_k) = x'^{\text{тск}}_k(t)\cdot s_k(t)\cdot\cos(2\pi f_0 t). \quad (6)$$

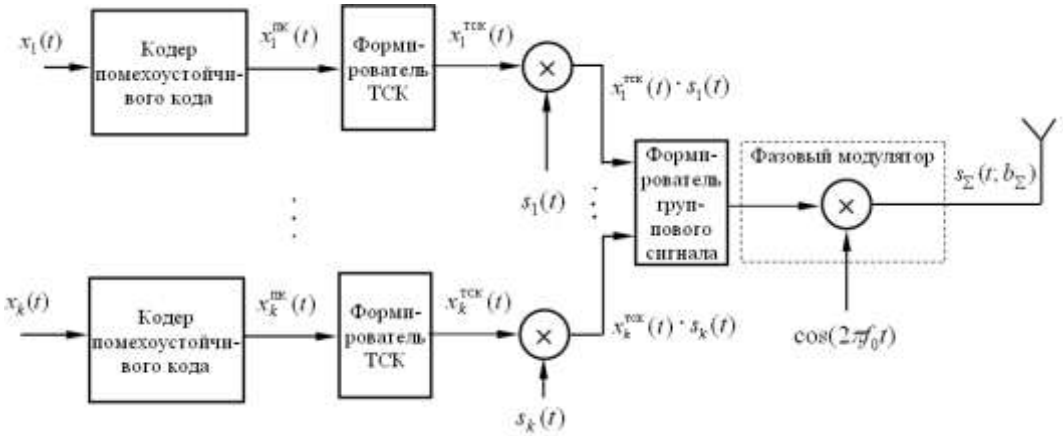

Рис. 4. Структурная схема передающей части системы с КРК

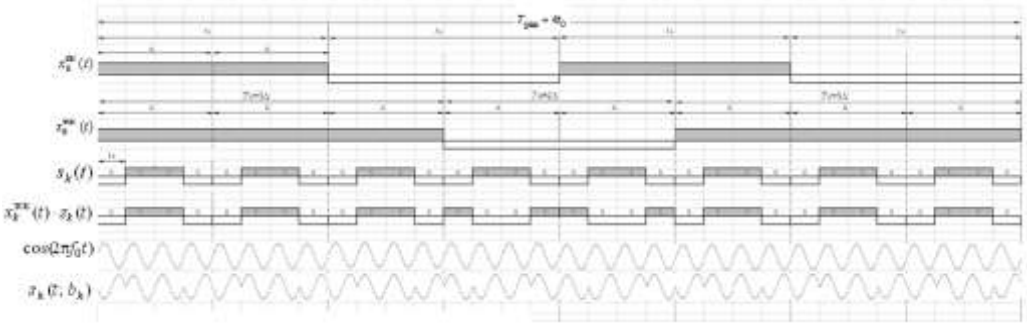

Рис. 5. Процесс прямого расширения спектра сигнальной конструкции $x_k^{\text{тск}}(t)$ сигнатурой $s_k(t)$

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 $\cos(2\pi f_0 t)$ с бинарной фазовой манипуляцией $x_k^{\text{тск}}(t)$:

$$\begin{aligned} &s'_k(t;b_k)s_k(t) = \\ &= s_k^2(t)\cdot x'^{\text{тск}}_k(t)\cdot\cos(2\pi f_0 t) = \\ &= x'^{\text{тск}}_k(t)\cdot\cos(2\pi f_0 t) \end{aligned} \quad ,(7)$$

где $s_k^2(t)=1$ с учетом бинарности $s_k(t)=\pm 1$. На выходе фазового демодулятора получаем переданную реализацию ТСК $x'^{\text{тск}}_k(t)$.

На рис. 6 представлена упрощенная структурная схема приемной части системы с КРК. Декодером ТСК осуществляется преобразование $x'^{\text{тск}}_k(t)$, в последовательность $x'^{\text{пк}}_k(t)$, которая дальше поступает на вход декодера помехоустойчивого кода. После декодирования и перемежения на выходе помехоустойчивого декодера получаем информационный сигнал *k*-го пользователя $x'_k(t)$.

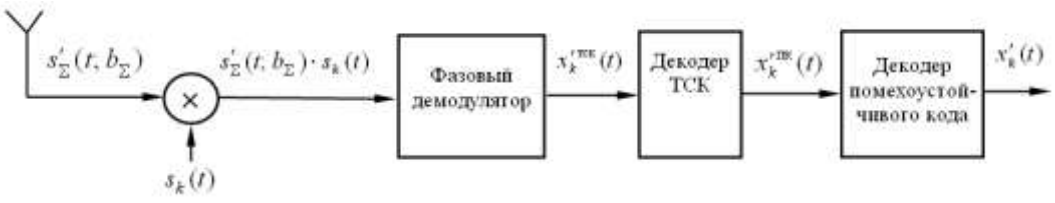

Рис. 6. Структурная схема приемной части системы с КРК

На рис. 7 показан процесс сжатия спектра сигнальной конструкции $x_k'^{\text{тск}}(t)$ для одного из индивидуальных каналов. Использование кодека ТСК позволяет на одном и том же интервале T_c сформировать больше разрешенных ТСК, чем сигнальных конструкций при РЦК ($N = 2^n$).

Предположим, что в качестве помехоустойчивого кода в индивидуальном канале на временном интервале $T_{\text{с}} = 9t_0$ сформирован 9-элементный код Слепяна (9, 5) [5] с кодовым расстоянием $d = 3$, исправляющий однократные ошибки [4]. Но, на этом же интервале $T_{\text{с}} = 9t_0$, в соответствии с [5], даже для $s = 3$ можно получить 18560 реализаций ТСК, эквивалентных 14-элементным бинарным кодовым словам. Следовательно, на интервале $T_{\text{с}} < 9t_0$ 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 (10%) от всех ошибок с учетом «плохого» состояния канала, в то время как после исправления однократных ошибок кодом (9, 5), доля неисправленных ошибок была 0,42 (42%) [5].

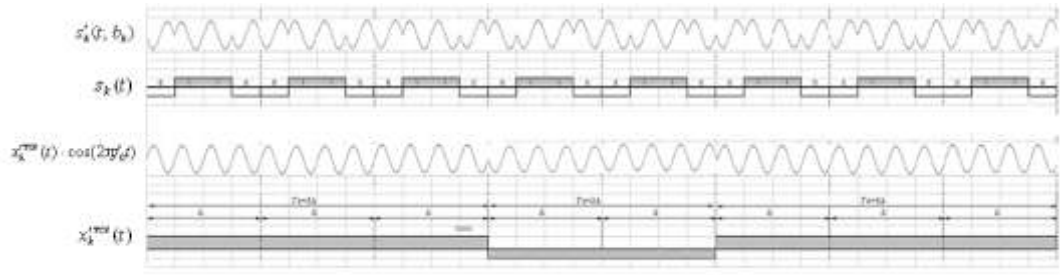

Рис. 7. Процесс сжатия спектра сигнальной конструкции $x_k'^{\text{тск}}(t)$

Выводы. В работе предложен метод формирования группового сигнала на основе ТСК в системе связи с КРК, что позволило повысить структурную скрытность сигнальных конструкций и качество приема в индивидуальных каналах.

Литература

1. Шаньгин, А.И. Информационная безопасность компьютерных систем и сетей [Текст] / А.И. Шаньгин. – М.: ИД «Форум»: ИФРА-М, 2008. – 416 с.

2. 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.

3. Куприянов, А.И. Теоретические основы радиоэлектронной борьбы [Текст] / А. И. Куприянов, А. В. Сахаров. – М.: Вузовская книга, 2007. – 356 с.

4. Ипатов В. П. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения; пер. с англ. – М.: Техносфера, 2007. – 487 с.

5. Захарченко М. В. Системи передавання даних. Том 1. Завадостійке кодування / Захарченко М. В. – Одеса: Фенікс, 2009. – 447 с.

6. Блейхут Р. Теория и практика кодов, контролирующих ошибки; пер. с англ. – М.: Мир, 1986. – 576 с.

7. Каневский З. М. Теория скрытности / З. М. Каневский, В.П. Литвиненко – Воронеж : ВГУ, 1991. – 144 с.

8. 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.

9. Захарченко, Н. В. Эффективность использования таймерных сигнальных конструкций в системах передачи с кодовым разделением каналов / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Наукові праці ДонНТУ. – 2011. – Випуск № 20(182). – С. 145–151.

References

1. Shan'gin, A.I. Informacionnaja bezopasnost' komp'juternyh sistem i setej [Tekst] / A.I. Shan'gin. – M.: ID «Forum»: IFRA-M, 2008. – 416 s.

2. Pomehozashhishhennost' sistem radiosvjazi s rasshireniem spektra signalov metodom psevdosluchajnoj perestrojki rabochej chastoty / V.I. Borisov, V.M. Zinchuk, A.E. Limarev i dr.; pod red. V.M. Borisova. – M.: Radio i svjaz', 2000. – 384 s.

3. Kuprijanov, A.I. Teoreticheskie osnovy radiojelektronnoj bor'by [Tekst] / A. I. Kuprijanov, A. V. Saharov. – M.: Vuzovskaja kniga, 2007. – 356 s.

4. Ipatov V. P. Shirokopolosnye sistemy i kodovoe razdelenie signalov. Principy i prilozhenija; per. s angl. – M.: Tehnosfera, 2007. – 487 s.

5. Zaharchenko M. V. Sistemi peredavannja danih. Tom 1. Zavadostijke koduvannja /

Zaharchenko M. V. – Odesa: Feniks, 2009. – 447 s.

6. Blejhut R. Teorija i praktika kodov, kontrolirujushhih oshibki; per. s angl. – M.: Mir, 1986. – 576 s.

7. Kanevskij Z. M. Teorija skrytnosti / Z. M. Kanevskij, V.P. Litvinenko – Voronezh : VGU, 1991. – 144 s.

8. Zaharchenko, N. V. Strukturnaja skrytnost' tajmernyh signalov v sistemah s kodovym razdeleniem

kanalov / N. V. Zaharchenko, V. V. Korchinskij, B. K. Radzimovskij // Vostochno-Evropejskij zhurnal peredovyh tehnologij. – 2011. – № 2/9(50). – S. 7–9.

9. Zaharchenko, N. V. Jeffektivnost' ispol'zovanija tajmernyh signal'nyh konstrukcij v sistemah peredachi s kodovym razdeleniem kanalov / N. V. Zaharchenko, V. V. Korchinskij, B. K. Radzimovskij // Naukovi praci DonNTU. – 2011. – Vipusk № 20(182). – S. 145–151.

Корчинський В.В.

МЕТОД ПІДВИЩЕННЯ СКРИТНОСТІ ПЕРЕДАЧІ ТАЙМЕРНИМИ СИГНАЛАМИ В СИСТЕМАХ ЗВ'ЯЗКУ З КОДОВИМ РОЗДІЛЕННЯМ КАНАЛІВ

Дана оцінка ефективності використання таймерних сигнальних конструкцій в індивідуальних каналах з обмеженою смугою частот окремих абонентів системи зв'язку з кодовим розділенням каналів та розглянуто можливість підвищення структурної скритності передачі при формуванні групового сигналу.

Ключові слова: *криптографічні системи, інформаційна скритність, груповий сигнал, таймерні сигнали.*

Korchinskiy V.V.

METHOD OF INCREASE OF RESERVE OF TRANSFER BY TIMER SIGNALS IN COMMUNICATION SYSTEMS WITH CODE DIVISION OF CHANNELS

Efficiency assessment of using the timer signal constructions in individual channels with limited frequency band individual subscriber of communication system with code division multiplexing is presented. The possibility of increasing the structural stealth transmission in forming of a group signal is considered.

Keyword: *cryptographic systems, information reserve, group signal, timer signals.*

Корчинский В.В. – доцент кафедры информационной безопасности и передачи данных, кандидат технических наук, ОНАС им. А. С. Попова

Рецензент: Осенин Юрий Иванович, доктор технических наук, профессор, проректор по научной работе Восточноукраинского национального университета имени Владимира Даля.