

## МЕТОД СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ ИНФОРМАЦИИ В НЕПОДВИЖНЫЕ ИЗОБРАЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ СЛОЖНЫХ ДИСКРЕТНЫХ СИГНАЛОВ И ПРЯМОГО РАСШИРЕНИЯ СПЕКТРА

Представлен метод стеганографического встраивания информации в неподвижные изображения с использованием сложных дискретных сигналов и прямого расширения спектра. Описан процесс извлечения информации из неподвижных изображений с использованием корреляционного приема сложных дискретных сигналов.

Ключевые слова: стеганография, сложный дискретный сигнал, прямое расширение спектра

**1. Постановка проблемы в общем виде и анализ литературы.** Методы стеганографической защиты информации развиваются в последние годы очень интенсивно [1-7]. В их основе лежит сокрытие не только смыслового содержания передаваемой информации, но и самого факта организации передачи данных. Другими словами, основной задачей методов стеганографической защиты информации является организация скрытного канала передачи данных посредством встраивания передаваемых информационных сообщений в объекты (контейнеры), обладающие высокой естественной избыточностью.

Одним из наиболее удобных способов организации цифровых стеганографических каналов скрытной передачи информации является использование в качестве цифровых контейнеров неподвижных изображений [1-7]. Обладая высоким уровнем естественной избыточности подобные контейнеры являются наиболее перспективным направлением исследований в современной стеганографии. В тоже время подавляющее большинство известных методов встраивания информации в неподвижные изображения используют простейшие процедуры кодирования наименее значимых бит и/или особенности форматирования растровых данных изображения [1-3].

В данной работе представлен метод стеганографического встраивания информации в неподвижные изображения с использованием сложных дискретных сигналов и прямого расширения спектра. Для реализации стеганографической защиты информации используются теоретические положения и вычислительные методы цифровой связи, в частности, методы теории сложных дискретных сигналов, корреляционного и спектрального анализа. Показано, что использование технологии прямого расширения спектра позволяет осуществить встраивание информационных данных в неподвижные изображения для скрытной передачи и реализовать, таким образом, стеганографическую защиту информации.

**2. Встраивание информации в неподвижные изображения с использованием сложных дискретных сигналов и технологии прямого расширения спектра.**

Введем некоторые условные обозначения и математические соотношения, которые, по аналогии с системами широкополосной цифровой связи, позволят исследовать особенности построения и информационного обмена данных в стеганографической системе, формализовать процессы встраивания и извлечения сообщений в пространственной области неподвижных изображений [4-7].

Представим информационное сообщение  $m$ , подлежащее встраиванию в цифровой контейнер-изображение, последовательностью данных из  $Nk$  бит. Представим  $m$  в виде  $N$  блоков  $m_i$  равной длины, т.е.  $m = (m_0, m_1, \dots, m_{N-1})$ , где каждый  $m_i$  – блок данных, последовательность (вектор) из  $k$  бит:  $m_i = (m_{i_0}, m_{i_1}, \dots, m_{i_{k-1}})$ . Другими словами, информационное сообщение запишем в виде:

$$m = (m_0, m_1, \dots, m_{N-1}) = ((m_{0_0}, m_{0_1}, \dots, m_{0_{k-1}}), (m_{1_0}, m_{1_1}, \dots, m_{1_{k-1}}), \dots, (m_{N-1_0}, m_{N-1_1}, \dots, m_{N-1_{k-1}}))$$

где каждый символ  $m_{ij} \in [0,1]$  представляет собой отдельный бит информационных данных.

Контейнер-изображение будем рассматривать как массив данных  $C$  размерностью  $V \cdot U$ , разбитый на подблоки размером  $v \cdot u = n$ . В случае, когда размер исходного контейнера-изображения не кратен величине  $n$  последние справа и последние снизу подблоки дополним нулевыми значениями до длины, кратной  $n$ . Таким образом, формально контейнер  $C$  запишем в виде объединения соответствующих подблоков  $C_i, i = 0, \dots, N-1$ :

$$C = C_0 \cup C_1 \cup \dots \cup C_{U/u} \cup \dots \cup C_{N-1},$$

$$C_0 = \begin{pmatrix} c_{0,0} & c_{0,1} & \dots & c_{0,u-1} \\ c_{1,0} & c_{1,1} & \dots & c_{1,u-1} \\ \dots & \dots & \dots & \dots \\ c_{v-1,0} & c_{v-1,1} & \dots & c_{v-1,u-1} \end{pmatrix}, C_1 = \begin{pmatrix} c_{0,u} & c_{0,u+1} & \dots & c_{0,2u-1} \\ c_{1,u} & c_{1,u+1} & \dots & c_{1,2u-1} \\ \dots & \dots & \dots & \dots \\ c_{v-1,u} & c_{v-1,u+1} & \dots & c_{v-1,2u-1} \end{pmatrix}, \dots,$$

$$C_{U/u-1} = \begin{pmatrix} c_{0,U-u} & c_{0,U-u+1} & \dots & c_{0,U-1} \\ c_{1,U-u} & c_{1,U-u+1} & \dots & c_{1,U-1} \\ \dots & \dots & \dots & \dots \\ c_{v-1,U-u} & c_{v-1,U-u+1} & \dots & c_{v-1,U-1} \end{pmatrix}, C_{U/u} = \begin{pmatrix} c_{v,0} & c_{v,1} & \dots & c_{v,u-1} \\ c_{v+1,0} & c_{v+1,1} & \dots & c_{v+1,u-1} \\ \dots & \dots & \dots & \dots \\ c_{2v-1,0} & c_{2v-1,1} & \dots & c_{2v-1,u-1} \end{pmatrix}, \dots,$$

$$C_i = \begin{pmatrix} c_{v,0} & c_{v,1} & \dots & c_{v,u-1} \\ c_{v+1,0} & c_{v+1,1} & \dots & c_{v+1,u-1} \\ \dots & \dots & \dots & \dots \\ c_{2v-1,0} & c_{2v-1,1} & \dots & c_{2v-1,u-1} \end{pmatrix}, \dots, C_{N-1} = \begin{pmatrix} c_{V-v,U-u} & c_{V-v,U-u+1} & \dots & c_{V-v,U-1} \\ c_{V-v+1,U-u} & c_{V-v+1,U-u+1} & \dots & c_{V-v+1,U-1} \\ \dots & \dots & \dots & \dots \\ c_{V-1,U-u} & c_{V-1,U-u+1} & \dots & c_{V-1,U-1} \end{pmatrix}.$$

В качестве элементов массива  $C$  могут выступать, например, растровые данные используемого изображения.

В качестве секретных ключевых данных будем использовать ансамбль слабокоррелированных дискретных сигналов (базисных векторов)  $Key = \Phi = \{\Phi_0, \Phi_1, \dots, \Phi_{M-1}\}$  мощности  $|\Phi| = M \geq k$ . Другими словами, число элементов  $k$  в каждом блоке информационного сообщения не превышает мощности  $M$  ансамбля  $\Phi$  используемых дискретных сигналов. Все базисные вектора  $\Phi_i$  представляют собой дискретные последовательности  $\Phi_i = (\varphi_{i_0}, \varphi_{i_1}, \dots, \varphi_{i_{n-1}})$  с длиной, равной размеру  $n$  блоков контейнера  $C$ . Т.е. запишем:

$$Key = \Phi = \left\{ \begin{array}{l} (\varphi_{0_0}, \varphi_{0_1}, \dots, \varphi_{0_{n-1}}) \\ (\varphi_{1_0}, \varphi_{1_1}, \dots, \varphi_{1_{n-1}}) \\ \dots \\ (\varphi_{M-1_0}, \varphi_{M-1_1}, \dots, \varphi_{M-1_{n-1}}) \end{array} \right\}.$$

Свойство слабокоррелированности элементов множества  $\Phi = \{\Phi_0, \Phi_1, \dots, \Phi_{M-1}\}$  формально запишем через ограничение на значения коэффициентов взаимной корреляции, т.е. для любых  $i, j \in [0, \dots, M-1]$  справедливо соотношение:

$$\rho(\Phi_i, \Phi_j) = \frac{1}{n} \sum_{z=0}^{n-1} \Phi_{i_z} \Phi_{j_z} = \begin{cases} +1, & \text{при } i = j; \\ \approx 0, & \text{при } i \neq j. \end{cases}$$

В случае использования ансамблей ортогональных (некоррелированных) сигналов выполняется равенство:

$$\rho(\Phi_i, \Phi_j) = \frac{1}{n} \sum_{z=0}^{n-1} \Phi_{i_z} \Phi_{j_z} = \begin{cases} +1, & \text{при } i = j; \\ 0, & \text{при } i \neq j. \end{cases}$$

Целью стеганографического преобразования информации является встраивание каждого отдельного блока сообщения  $m_i$  в соответствующий подблок  $C_i$  контейнера-изображения, т.е. в каждый подблок контейнера встраивается до  $k \leq n$  бит информационных данных. Таким образом, цифровой контейнер-изображение размерностью  $V \cdot U$  элементов может содержать до  $V \cdot \frac{U}{n}$  блоков информационного сообщения, т.е. до  $V \cdot \frac{U}{n} \cdot k$  информационных битов.

В качестве ключевых данных (массива базисных векторов  $Key = \Phi$ ) будем использовать большие ансамбли шумоподобных сложных дискретных сигналов.

Встраивание информационного сообщения осуществляется следующим образом. Каждый блок сообщения  $m_{i_j}, j = 0, \dots, n-1$  сопоставляется с отдельным блоком контейнера-изображения. Каждый информационный бит блока  $m_{i_j}, j = 0, \dots, n-1$  представляется в виде информационного сигнала:

$$m_{i_j}(t) = \begin{cases} +1, & m_{i_j} = 1; \\ -1, & m_{i_j} = 0; \end{cases}$$

и по аналогии с модуляцией шумоподобными сигналами в теории цифровой связи модулируется расширяющим кодовым сигналом (базисными векторами), т.е. псевдослучайной последовательностью (ПСП)  $\Phi_j \in \Phi$  [8-9].

В результате для каждого информационного блока  $m_i$  формируется блок модулированного информационного сигнала:

$$E_i(t) = \sum_{j=0}^{k-1} m_{i_j}(t) \Phi_j.$$

Для встраивания информационных данных полученный блок модулированного информационного сигнала  $E_i(t)$  попиксельно суммируется с подблоком контейнера. Для формализации этой процедуры представим соответствующие блоки модулированного информационного сигнала  $E_i(t)$  в виде двумерного массива данных:

$$E_i = \begin{pmatrix} c_{0,u} & c_{0,u+1} & \dots & c_{0,2u-1} \\ c_{1,u} & c_{1,u+1} & \dots & c_{1,2u-1} \\ \dots & \dots & \dots & \dots \\ c_{v-1,u} & c_{v-1,u+1} & \dots & c_{v-1,2u-1} \end{pmatrix}, i = 0, \dots, N-1.$$

Тогда стеганограмма (заполненный контейнер)  $S$  формируется посредством объединения массивов данных  $S_i, i = 0, \dots, N-1$ . Формально такое объединение запишем в виде:  $S = S_0 \cup S_1 \cup \dots \cup S_{N-1}, S_i = C_i + E_i \cdot G$ , где  $G > 0$  – коэффициент усиления расширяющего сигнала, задающий «энергию» встраиваемых бит информационной последовательности. Каждый подблок  $S_i$  стеганограммы  $S$  с учетом приведенных выше выражений запишем в виде:

$$S_i = \begin{pmatrix} S_{i_0} & S_{i_1} & \dots & S_{i_{n-1}} \\ S_{i_u} & S_{i_{u+1}} & \dots & S_{i_{2u-1}} \\ \dots & \dots & \dots & \dots \\ S_{i_{n-u}} & S_{i_{n-u+1}} & \dots & S_{i_{n-1}} \end{pmatrix} =$$

$$= \begin{pmatrix} C_{i_0} + G \sum_{j=0}^{k-1} m_{i_j}(t) \Phi_{j_0} & C_{i_1} + G \sum_{j=0}^{k-1} m_{i_j}(t) \Phi_{j_1} & \dots & C_{i_{n-1}} + G \sum_{j=0}^{k-1} m_{i_j}(t) \Phi_{j_{n-1}} \\ C_{i_u} + G \sum_{j=0}^{k-1} m_{i_j}(t) \Phi_{j_u} & C_{i_{u+1}} + G \sum_{j=0}^{k-1} m_{i_j}(t) \Phi_{j_{u+1}} & \dots & C_{i_{2u-1}} + G \sum_{j=0}^{k-1} m_{i_j}(t) \Phi_{j_{2u-1}} \\ \dots & \dots & \dots & \dots \\ C_{i_{n-u}} + G \sum_{j=0}^{k-1} m_{i_j}(t) \Phi_{j_{n-u}} & C_{i_{n-u+1}} + G \sum_{j=0}^{k-1} m_{i_j}(t) \Phi_{j_{n-u+1}} & \dots & C_{i_{n-1}} + G \sum_{j=0}^{k-1} m_{i_j}(t) \Phi_{j_{n-1}} \end{pmatrix}$$

Таким образом, заполненный контейнер  $S$  образуется посредством объединения сформированных блоков  $S_i$ ,  $i = 0, \dots, N - 1$ .

Структурная схема процесса встраивания данных в пространственную область неподвижных изображений с использованием сложных дискретных сигналов и технологии прямого расширения спектра представлена на рис. 1.

Таким образом, процесс встраивания сообщения состоит из последовательно выполняемых операций форматирования контейнера, ключевых и информационных данных, модуляции информационных сигналов с помощью ПСП, формирования блоков стеганограммы и их объединения в общий стегоконтейнер.

**3. Извлечение информации из неподвижных изображений с использованием корреляционного приема сложных дискретных сигналов.** Для извлечения информационных данных из стеганографического контейнера на приемной стороне следует реализовать корреляционный прием информационных сигналов из аддитивной смеси усиленного в  $G$  раз модулированного сообщения  $E_i(t)$  и данных контейнера  $C_i$ . При этом для реализации извлечения данных нет необходимости владеть информацией о первичном контейнере  $C$ . Данные контейнера  $C_i$  интерпретируются как воздействие случайных помех в канале связи, а операция извлечения информационных данных из стеганодетектора тождественна задаче приема сообщения из аддитивной смеси информационных сигналов и случайного шума в канале связи.

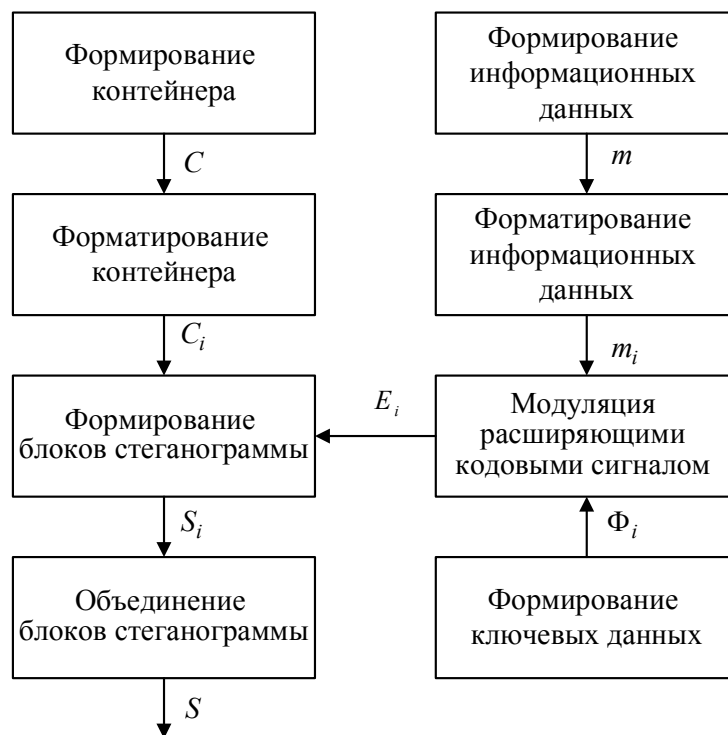


Рис. 1. Структурная схема процесса встраивания данных в пространственную область неподвижных изображений с использованием сложных дискретных сигналов и технологии прямого расширения спектра

Операция декодирования заключается в восстановлении скрытого сообщения путем проецирования каждого блока  $S_i$ , полученного стеганоизображения  $S$  на все базисные вектора  $\Phi_j \in \Phi, i = 0, \dots, N - 1$ . Для этого каждый блок  $S_i$  представляется в форме вектора  $S_i = (S_{i_0}, S_{i_1}, \dots, S_{i_{n-1}})$ ,  $i = 0, \dots, N - 1$ .

Чтобы извлечь  $j$ -ый бит сообщения из  $i$ -го блока стеганоизображения необходимо вычислить коэффициент корреляции между  $\Phi_j$  и принятым блоком  $S_i$  (представленного в виде вектора):

$$\rho(S_i, \Phi_j) = \frac{1}{n} \sum_{z=0}^{n-1} S_{i_z} \Phi_{j_z} = G \cdot \frac{1}{n} \sum_{z=0}^{n-1} E_{i_z} \Phi_{j_z} + \frac{1}{n} \sum_{z=0}^{n-1} C_{i_z} \Phi_{j_z}, \quad (1)$$

где под  $C_i$  понимается одномерный массив, т.е. соответствующий блок контейнера, представленный в форме вектора.

Предположим, что массив  $C_i$  имеет случайную статистическую структуру, т.е. положим, что второе слагаемое в правой части выражения (1) близко к нулю и им можно пренебречь. Тогда имеем:

$$\rho(S_i, \Phi_j) \approx G \cdot E_i \cdot \Phi_j = G \cdot \sum_{l=0}^{n-1} \sum_{z=0}^{n-1} m_{i_x}(t) \cdot \Phi_{l_z} \Phi_{j_z}. \quad (2)$$

Отметим, что все последовательности из множества  $\Phi$  слабокоррелированы, т.е. при  $l \neq j$  имеем  $\rho(\Phi_i, \Phi_j) \approx 0$ . Следовательно, всеми слагаемыми в правой части равенства (2) при  $l \neq j$  можно пренебречь. Отсюда имеем:

$$\rho(S_i, \Phi_j) \approx G \cdot m_{ij}(t) \cdot \frac{1}{n} \sum_{z=0}^{n-1} (\Phi_{jz})^2 = G \cdot m_{ij}(t). \quad (3)$$

Значения  $m_{ij}(t)$  могут быть легко восстановлены с помощью знаковой функции. Поскольку  $G > 0$  и  $n > 0$  знак  $\rho(S_i, \Phi_j)$  в (3) зависит только от  $m_{ij}(t)$ , откуда имеем:

$$m_{ij}(t) = \text{sign}(\rho(S_i, \Phi_j)) = \begin{cases} -1, & \text{при } \rho(S_i, \Phi_j) < 0; \\ +1, & \text{при } \rho(S_i, \Phi_j) > 0; \\ ?, & \text{при } \rho(S_i, \Phi_j) = 0; \end{cases} \quad (4)$$

Если  $\rho(S_i, \Phi_j) = 0$  в (4) будем полагать, что встроенная информация была утрачена (стерта).

На рис. 2. представлена структурная схема процесса извлечения данных из пространственной области неподвижных изображений с использованием корреляционного приема сложных дискретных сигналов.

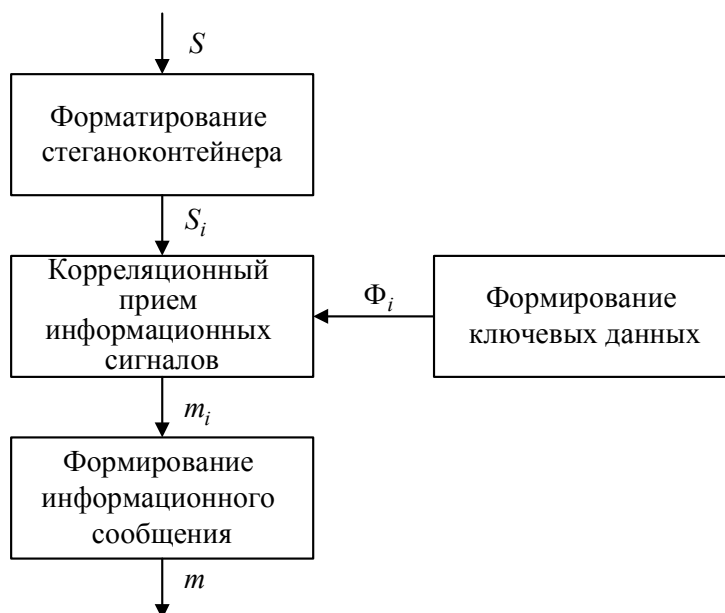


Рис. 2. Структурная схема процесса извлечения данных из пространственной области неподвижных изображений с использованием корреляционного приема сложных дискретных сигналов

Структурная схема передачи информации в стеганографической системе с использованием сложных дискретных сигналов и технологии прямого расширения спектра представлена на рис.3.

Из рисунка следует, что процесс встраивания информационных сообщений для скрытной передачи подобен процессу расширения спектра дискретных сигналов в системах связи. Поэлементное сложение модулированного сообщения  $E(t)$  с контейнером-изображением  $C(t)$  следует интерпретировать как наложение ошибок  $e(t)$  на полезный сигнал в канале связи  $y(t)$ . Задача извлечения сообщения  $m(t)$  из  $S(t)$  на приемной стороне стеганосистемы эквивалентна задаче детектирования  $x(t)$  из смеси полезного сигнала и помехи  $y'(t) = y(t) + e(t)$  в широкополосной системе связи. Другими словами, рассмотренная стеганосистема наследует все преимущества широкополосных систем связи: устойчивость к

несанкціонованому извлечению встроенных сообщений (аналог скрытности в системе связи), устойчивость к разрушению или модификации встроенных сообщений (аналог помехозащищенности), устойчивость к навязыванию ложных сообщений (аналог имитостойкости в системе связи).

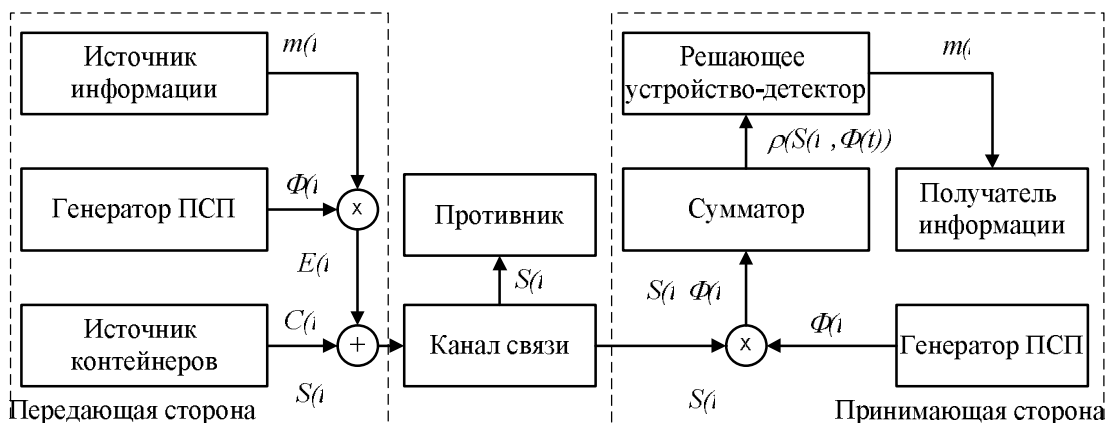


Рис. 3. Структурная схема передачи информации в стеганографической системе с использованием сложных дискретных сигналов и технологии прямого расширения спектра

**4. Выводы.** Таким образом, использование прямого расширения спектра дискретных сигналов позволяет осуществить встраивание информационных данных в неподвижные изображения для скрытной передачи и реализовать, таким образом, стеганографическую защиту информации. *Перспективным направлением дальнейших исследований* является экспериментальная оценка эффективности стеганографического встраивания информации в неподвижные изображения с использованием сложных дискретных сигналов и технологии прямого расширения спектра.

#### ЛИТЕРАТУРА

1. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Конахович Г. Ф., Пузыренко А. Ю. – К.: «МК-Пресс»б 2006. - 288 с., ил.
2. Грибунин В.Г. Цифровая стеганография / Грибунин В.Г., Оков И.Н., Туринцев И.В. – М.: Солон-Пресс, 2002. – 272 с.
3. Хорошко В.А. Введение в компьютерную стеганографию / Хорошко В.А., Шелест М.Е. – К., 2002. – 140 с.
4. J. Smith. Modulation and Information hiding in Image / J. Smith, B. Comiskey // Information hiding: First Int. Workshop “InfoHiding’96”, Springer as Lecture Notes in Computing Science, vol 1174. 1996. – pp. 207-227.
5. Кузнецов А.А. Встраивание данных в контейнеры-изображения с использованием сложных дискретных сигналов / Кузнецов А.А., Смирнов А.А. // Радиотехника: Всеукр. межвед. науч.-техн. сб. – Харьков: ХТУРЭ.–2011. – Вып. 166. – С. 134-141.
6. Kuznetsov A. Use of Complex Discrete Signals for Steganographic Information Security / Kuznetsov A., Serhiienko R., Kovtun V., Botnov A // Statistical Methods of Signal and Data Processing (SMSDP-2010): Proceedings. – Kiev: National Aviation University “NAU-Druk” Publishing House – 2010. – pp. 143 – 146.
7. Стасев Ю.В. Использование сложных дискретных сигналов для стеганографической защиты информации / Стасев Ю.В., Кузнецов А.А., Смирнов А.А.// Системи управління, навігації та зв’язку. – Київ: Центральний науково-дослідний інститут навігації і управління. – 2011. – Вип. 3 (19). – С. 110-114.
8. Цифровые методы в космической связи / Под ред. С. Голомба.- М.: Связь, 1969. – 272 с.
9. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.

Надійшла: 17.12.2011

Рецензент: д.т.н., проф. Корченко О.Г.