УДК 621.396

О.А. Смірнов

Кіровоградський національний технічний університет, Кіровоград

СТЕГАНОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ ІЗ ВИКОРИСТАННЯМ ПРЯМОГО РОЗШИРЕННЯ СПЕКТРУ

Розглядаються стеганографічні системи захисту інформації, в яких вирішується завдання скритної передачі інформації не тільки шляхом приховування змістовної частини повідомлень, але й шляхом приховування самого факту організації каналів скритної передачі даних. Досліджуються основні стеганографічні перетворення із застосуванням технології прямого розширення спектру. Запропоновано структурні схеми пристроїв стеганографічного приховування та вилучення даних в просторовій області нерухомих зображень із використанням прямого розширення спектру.

Ключові слова: *стеганографія, захист інформації, стеганоконтейнер.*

Вступ

Стеганографічні системи та протоколи є технологічною основою щодо побудови новітніх засобів захисту інформації та інформаційних ресурсів, забезпечення певного рівня їх безпеки [1 – 5]. Тому дослідження стеганографічних систем та протоколів при вирішенні завдань стеганографічного захисту інформації та інформаційних ресурсів є надзвичайно важливим науково-практичним завданням, яке тісно пов'язане із розвитком певного напрямку теорії захисту інформації.

Розвиток засобів обчислювальної техніки останнім часом дав новий поштовх для розвитку комп'ютерної або цифровий стеганографії. При цьому секретне повідомлення у вигляді цифрових інформаційних даних вбудовується в масив та/або інформаційний потік, які володіють високою внутрішньою природною надмірністю, наприклад, в просторову область нерухомих зображень. Найбільш обґрунтованим підходом щодо побудови стеганографічних систем захисту інформації є застосування розвиненого математичного апарату теорії дискретних сигналів та технології прямого розширення спектру сигналів [4, 5]. Побудовані таким чином засобі стеганографічного перетворення інформації мають всі переваги широкосмугових систем зв'язку, а саме: високу перешкодостійкість, імітостійкість та скритність передачі інформаційних повідомлень.

Метою цієї роботи є дослідження основних стеганографічних перетворень із застосуванням технології прямого розширення спектру, обґрунтування структурних схем відповідних пристроїв стеганографічного приховування та вилучення даних

Приховування та вилучення даних в стаганосистемі

В основі стеганографічного приховування даних лежить модуляція інформаційних повідомлень шумоподібними дискретними сигналами (псевдовипадковими послідовностями) та додавання звормованих модульованих повідомленнь до даних контейнеру-зображання. При вилученні даних застосовується кореляційних приймач, який обчислює коефіцієнт кореляції прийнятого контейнеру і псевдовипадковими послідовностями, які тотожні тим, що застосовувалися на передавальній стороні. За обрахованим значенням коефіцієнту кореляції приймається рішення щодо даних, які передавалися у контейнеру.

Покладемо, що на передавальній стороні після шифрування та перешкодостійкого кодування окремі блоки $m_i = \left(m_{i_0}, m_{i_1}, ..., m_{i_{k-1}}\right)$, $i = 0, ..., N-1$ даних інформаційного повідомлення $m = \left(m_0, m_1, ..., m_{N-1}\right)$ за допомогою відповідних пристроїв модулюються шумоподібними дискретними сигналами:

$$\Phi_i = \left(\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}}\right);$$

$$\Phi_i \in \Phi = \left\{\Phi_0, \Phi_1, ..., \Phi_{M-1}\right\}$$

із базою $B = TF$, де T – тривалість елемента сигналу φ_{i_j}, F – полоса частот сигналу Φ_i. Оскільки $F = n \cdot (1/T)$ маємо $B = n >> 1$ і база сигналу задає кратність розширення полоси частот сигналу Φ_i по відношенню до елементарних сигналів φ_{i_j} та/або m_{i_j}.

В результаті для кожного інформаційного блоку m_i формується блок модульованого інформаційного сигналу:

$$E_i = \sum_{j=0}^{k-1} m^*_{i_j} \Phi_j =$$

$$= \left(\sum_{j=0}^{k-1} m^*_{i_j} \varphi_{j_0}, \sum_{j=0}^{k-1} m^*_{i_j} \varphi_{j_1}, ..., \sum_{j=0}^{k-1} m^*_{i_j} \varphi_{j_{n-1}} \right),$$

де $m^*_{i_j} = \begin{cases} +1, m_{i_j} = 1; \\ -1, m_{i_j} = 0; \end{cases}$

який за статистичними властивостями приймає вигляд випадкової послідовності, а за рахунок великої бази дискретних сигналів досягається розширення

спектру частот в $B = n$ разів.

Отримане модульоване повідомлення E_i подається на пристрій перемежування, на якому елементи E_i за допомогою таємного ключа K_1 перемішуються за відповідним правилом f. Отримані данні $\overline{E_i} = f(E_i, K_1)$ за допомогою відповідного пристрою поелементо додаються до даних контейнера C_i (даних цифрового зображення в просторовій області) за правилом:

$$S_i = C_i + \overline{E_i} \cdot G,$$

де $G > 0$ – коефіцієнт підсилення розширювального сигналу, який задає «енергію» вбудованих блоків інформаційного повідомлення.

Отримані дані S_i подаються на пристрій квантування, який виконує певне перетворення для збереження початкового динамічного діапазону зображення-контейнеру, в результаті чого формуються окремі блоки стеганограми $\overline{S_i}$ та заповнений контейнер $\overline{S} = \overline{S_0} \cup \overline{S_1} \cup ... \cup \overline{S_{N-1}}$, який передається приймальній стороні.

На приймальній стороні отримані блоки стеганограми $\overline{S_i}$ після фільтрації подаються на пристрій зворотного перемежування, на якому елементи відфільтрованих блоків стегенограми $\overline{\overline{S_i}}$ за допомогою таємного ключа перемішуються за правилом f^{-1}, яке інверсне правилу перемежування f на передавальній стороні. Вилучення блоків інформаційних даних виконується за допомогою кореляційного приймача, який обраховує значення коефіцієнту кореляції отриманих після зворотного перемежування даних $S^*_i = f^{-1}(\overline{\overline{S_i}}, K_1)$ та відповідних дискретних сигналів Φ_j, тотожних тим, що застосовувалися на передавальній стороні:

$$\rho(S^*_i, \Phi_j) = \frac{1}{n}\sum_{z=0}^{n-1} S^*_{i_z}\, \varphi_{j_z} \approx$$
$$\approx G \cdot \frac{1}{n}\sum_{z=0}^{n-1} E_{i_z} \varphi_{j_z} + \frac{1}{n}\sum_{z=0}^{n-1} C_{i_z} \varphi_{j_z}. \qquad (1)$$

Припустимо, що масив даних блоку контейнера C_i має випадкову статистичну структуру, тобто покладемо, що другий доданок в правій частині виразу (1) близький до нуля і їм можна знехтувати. Тоді маємо:

$$\rho(S^*_i, \Phi_j) \approx G \cdot \frac{1}{n}\sum_{z=0}^{n-1} E_{i_z} \varphi_{j_z} =$$
$$= G \cdot \frac{1}{n}\sum_{z=0}^{n-1}\left(\sum_{u=0}^{k-1} m^*_{i_u}\, \varphi_{u_z}\right)\varphi_{j_z} = \qquad (2)$$
$$= G \cdot \sum_{u=0}^{k-1} m^*_{i_u} \sum_{z=0}^{n-1} \varphi_{u_z} \varphi_{j_z} = G \cdot \sum_{u=0}^{k-1} m^*_{i_u}\, \rho(\Phi_u, \Phi_j).$$

Оскільки всі послідовності із множини Φ формуються за допомогою генератора псевдовипадкових послідовностей, ініційованого таємним ключем K_2, відповідні дискретні сигнали є слабокорельованими, тобто при $u \neq j$ маємо $\rho(\Phi_u, \Phi_j) \approx 0$. Відповідно до цього всіма доданками, окрім випадку $u = j$, в правій частині рівняння (2) можна знехтувати. Звідки маємо:

$$\rho(S^*_i, \Phi_j) \approx G \cdot m^*_{i_j} \cdot \frac{1}{n}\sum_{z=0}^{n-1}(\varphi_{j_z})^2 = G \cdot m^*_{i_j} = \begin{cases} +G; \\ -G. \end{cases} \qquad (3)$$

Відповідне значення вилучених даних приймається за допомогою порогового пристрою відповідно до обрахованого коефіцієнта кореляції. Оскільки $G > 0$ і $n > 0$ знак $\rho(S^*_i, \Phi_j)$ в (3) залежить тільки від $m^*_{i_j}$, звідки маємо:

$$m^*_{i_j} = \operatorname{sign}(\rho(S^*_i, \Phi_j)) = \begin{cases} -1, & \rho(S_i, \Phi_j) < 0; \\ +1, & \rho(S_i, \Phi_j) > 0. \end{cases} \qquad (4)$$

Якщо $\rho(S^*_i, \Phi_j) = 0$ в (4) будемо вважати, що вбудована інформація була втрачена (стерта).

З вилучених даних на приймальній стороні формуються окремі блоки даних $m_i = (m_{i_0}, m_{i_1}, ..., m_{i_{k-1}})$, $i = 0, ..., N-1$ інформаційного повідомлення $m = (m_0, m_1, ..., m_{N-1})$, де:

$$m_{i_j} = \begin{cases} 1, & m^*_{i_j} = +1; \\ 0, & m^*_{i_j} = -1, \end{cases}$$

з яких після перешкодостійкого декодування та розшифрування вилучених даних формуються інформаційні повідомлення. Секретний ключ K_2 задає правило формування псевдовипадкових послідовностей $\Phi_i = (\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}})$, які формуються відповідним генератором та використовуються у якості шумоподібних дискретних сигналів $\Phi_i \in \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$ з ансамблю Φ потужності M. Правило шифрування та розшифрування на передавальній та приймальній стороні ініціюється секретним ключем K_3.

Обґрунтування пристроїв стеганографічного захисту

Розглянемо введену вище формалізацію на предмет практичної реалізації пристроїв стегано_графічного захисту інформації. На рис. 1 зображено структурну схему пристрою стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектру.

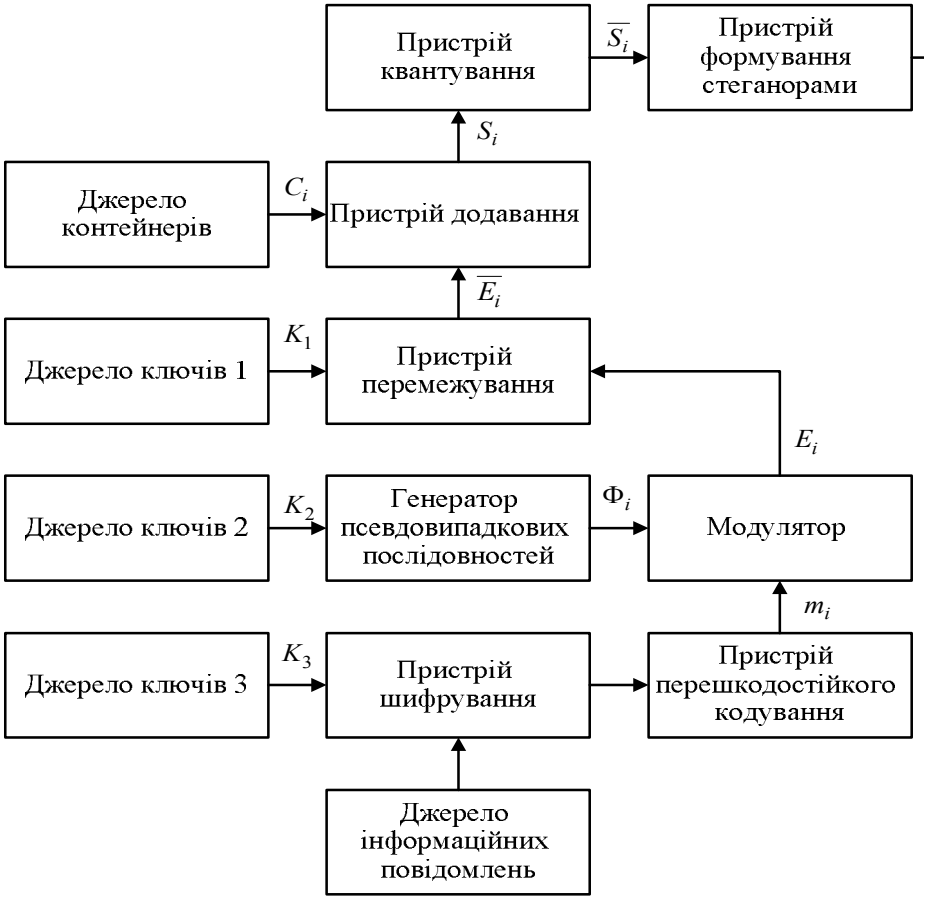

Рис. 1. Структурна схема пристрою стеганографічного приховування даних в просторовій області зображень із використанням прямого розширення спектру

Пристрій працює наступним чином.

Джерело інформаційних повідомлень формує послідовність інформаційних даних, які подаються пристрій шифрування, ініційований таємним ключем K_3, що формується джерелом ключів 3.

Зашифровані інформаційні повідомлення подаються на пристрій перешкодостійкого кодування, в якому виконується внесення спеціально формованої надмірності для підвищення достовірності інформаційних зашифрованих даних.

Джерело ключів 2 формує таємний ключ K_2, який ініціює генератор М от источника сообщений (ИС), поступают на аппаратуру сопряжения (АС), где происходит согласование выходных параметров ИС и входных параметров СОКИ.

По совокупности данных об ансамблях рабочих $\left\{p_i^{п}(z)\right\}$ и избыточных (контрольных и резервных) оснований $\left\{p_i^{к+r}(z)\right\}$ модулярного кода полиномиальной МСС (ПМСС), где $p_i(z)$ – минимальные многочлены расширенного поля Галуа $GF(2^v)$, обосновываются математические модели прямого преобразования ПСС – ПМСС и обратного преобразования из ПМСС в ПСС:

$$\begin{cases} V_{\text{ПСС–ПМСС}}\left(\left\{p^{п}(z), p^{к+r}(z)\right\}, s_j\right) \to \min, \\ T_{\text{ПСС–ПМСС}}\left(\left\{p^{п}(z), p^{к+r}(z)\right\}, s_j\right) \to \min, \\ Q_{\text{ПМСС}}\left(\left\{p^{п}(z), p^{к+r}(z)\right\}, s_j\right) \ge Q_{\text{доп}}; \end{cases}$$

$$\begin{cases} V_{\text{ПМСС–ПСС}}\left(\left\{p^{п}(z), p^{к+r}(z)\right\}, u_i\right) \to \min, \\ T_{\text{ПМСС–ПСС}}\left(\left\{p^{п}(z), p^{к+r}(z)\right\}, u_i\right) \to \min, \\ Q_{\text{ПМСС}}\left(\left\{p^{п}(z), p^{к+r}(z)\right\}, u_i\right) \ge Q_{\text{доп}}, \end{cases}$$

где $s_j \in S = [s_1, s_2, ..., s_x]$ – j-й алгоритм преобразования ПСС-ПМСС; $u_l \in U = \left[u_1, u_2, ..., u_y\right]$ – *l*-й алгоритм преобразования ПМСС-ПСС; Q – точность выполнения преобразования; T – временные затраты на реализацию преобразований.

Реализация прямого преобразования информации представленной в позиционном коде в непозиционный код ПМСС, осуществляется в соответствии с известными алгоритмами реализации данной немодульной процедуры.

Далее, на передающей стороне, с использованием известной совокупности моделей, методов и алгоритмов осуществляется реализации непосредст-

венно процесса шифрования, связанного с решением уравнения $E_e(M) = c$ и расшифрования на приёмной стороне – $D_d(c) = M$.

Открытый ключ шифрования e от генератора ключей (ГК), посредством многоканальной СПД поступает на СОКИ передающей стороны. Закрытый ключ расшифрования d после выполнения прямого преобразования ПСС-ПМСС поступает в СОКИ приёмной стороны.

Непосредственно реализация операций криптопреобразования осуществляется в трактах обработки криптографической информации (ТОКИ) выполняющих арифметические операции по строго определённому рабочему $\left\{p_i^{п}(z)\right\}$ или избыточному основанию $\left\{p_i^{к+r}(z)\right\}$ модулярного кода ПМСС

Устройство контроля возникновения ошибок и реконфигурации структуры системы (УКОРС) осуществляет контроль, диагностику и исправления ошибок в ПМСС, поиск и локализацию местоположения отказа. При необходимости, с целью сохранения работоспособного состояния, за счет перераспределения или снижения в допустимых пределах основных показателей качества функционирования псевдовипадкових послідовностей. Результатом роботи генератору псевдовипадкових послідовностей є дискретні сигнали, тобто дискретні послідовності, елементи яких сформовано псевдовипадковим чином.

Сформовані псевдовипадкові послідовності Φ_i та послідовності m_i, які було отримано на виході пристрою перешкодостійкого кодування, подаються на модулятор, в якому виконується формування модульованого повідомлення E_i за розглянутим вище правилом. Модульоване повідомлення E_i подається на пристрій перемежування, ініційований таємним ключем K_1, який сформовано джерелом ключів 1. Пристрій перемежування обробляє модульоване повідомлення E_i, тобто за правилом, яке задає таємний ключ K_1, псевдовипадковим чином переставляє місцями елементи E_i. Отримані дані $\overline{E_i}$ подаються на пристрій додавання, у якому виконується по елементне додавання з даними контейнеру C_i. Контейнер формується джерелом контейнерів. Отримані дані S_i подаються на пристрій квантування, який виконує певне перетворення для зберігання початкового динамічного діапазону зображення-контейнеру, в результаті чого формуються окремі блоки стеганограми $\overline{S_i}$ та заповнений контейнер $\overline{S} = \overline{S_0} \cup \overline{S_1} \cup ... \cup \overline{S_{N-1}}$, який передається приймальній стороні.

На рис. 2 зображена структурна схема пристрою стеганографічного вилучення даних з просторовій області зображень із використанням прямого розширення спектру.

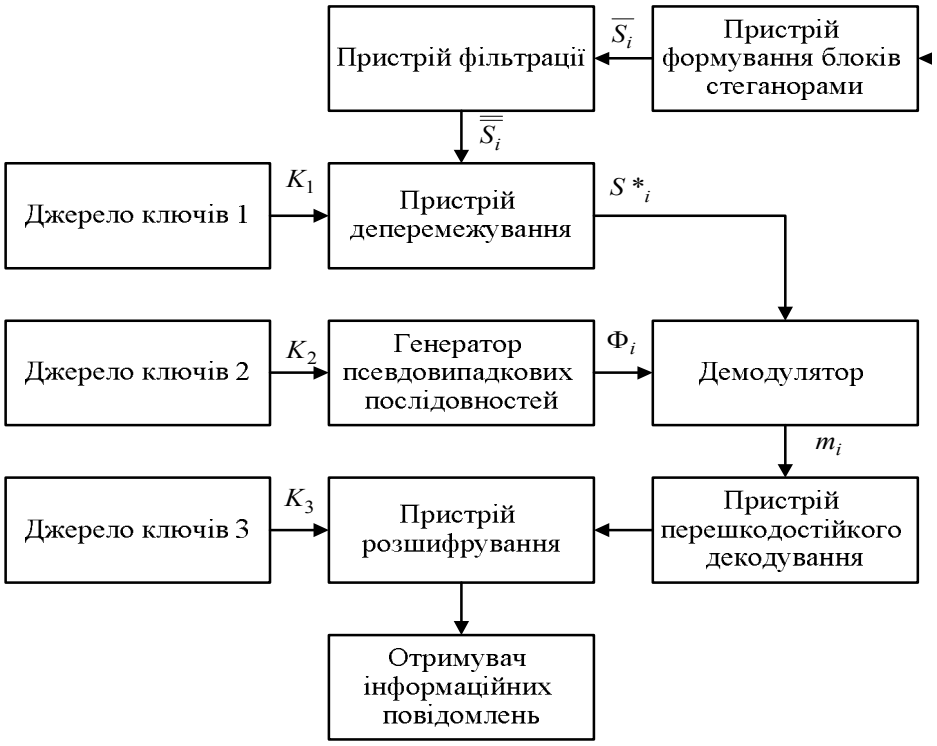

Рис. 2. Структурна схема пристрою стеганографічного вилучення даних з просторової області зображень із використанням прямого розширення спектру

На приймальній стороні отримана стеганограмма $\overline{S}$ подається на пристрій формування блоків стеганограми, в якому формуються блоки $\overline{S_i}$ та подаються на пристрій фільтрації. Після фільтрації

отримані дані $\overline{\overline{S_i}}$ подаються на пристрій зворотного перемежування, на якому виконується дія, інверсна перемежуванню на передавальній стороні.

Пристрій деперемежування ініційовано секретним ключем K_1, який сформовано джерелом ключів 1. Отримані після деперемежування дані S^*_i подаються на демодулятор, який виконує функцію кореляційного приймача дискретних сигналів за розглянутим вище правилом. Тобто в демодуляторі обчислюється значення коефіцієнту кореляції даних S^*_i та псевдовипадкових послідовностей Φ_i, які формуються відповідним генератором, що ініційований секретним ключем K_2. Секретний ключ K_2 формується джерелом ключів 2. Таким чином, в демодуляторі обчислюється значення коефіцієнту кореляції між отриманими даними S^*_i та послідовностями, які застосовувалися при вбудовуванні інформації.

Рішення, стосовно значення вбудованих даних, приймається відповідно до значення обрахованого коефіцієнту кореляції за правилом (4).

Вилучені дані m_i подаються на пристрій перешкодостійкого декодування, в якому за визначеним правилом із використанням внесеної надмірності виправляються деякі помилки, відповідно до корегуючої здатності коду.

Це призводить до деякого підвищення достовірності переданих даних, які після декодування подаються на пристрій розшифрування, ініційований таємним ключем K_3, що формується джерелом ключів 3. Розшифровані повідомлення подаються отримувачу інформаційних повідомлень.

Застосування пристроїв шифрування та перемежування у процесі приховування та вилучення даних дозволяє покращити статистичні властивості модульованого повідомлення E_i, тобто наблизити його вигляд до випадкової послідовності. Застосування пристроїв перешкодостійкого кодування дозволяє підвищити достовірність передачі інформаційних повідомлень під час стеганографічних перетворень.

Висновки

В ході проведених досліджень було розглянуто стеганографічні системи захисту інформації, в яких завдання приховування факту організації каналів скритної передачі даних вирішується із застосуванням технології прямого розширення спектру.

Досліджено основні математичні перетворення та співвідношення, що застосовуються при приховуванні та вилученні інформаційних повідомлень.

Обгрунтовано структурні схеми пристроїв стеганографічного приховування та вилучення даних в просторовій області нерухомих зображень із використанням прямого розширення спектру.

Перспективним напрямком подальших досліджень є практична реалізація розглянутих стеганосистем та експериментальна перевірка отриманих результатів та зроблених висновків.

Список літератури

1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: «МК-Пресс», 2006. – 288 с., ил.

2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-Пресс, 2002. – 272 с.

3. Хорошко В.А. Введение в компьютерную стеганографию / В.А. Хорошко, М.Е. Шелест. – К., 2002. – 140 с.

4. Smith J.R. and Comisky B.O. Modulation and information hiding in images. In R. Anderson, editor, Information Hiding, First International Workshop, volume 1174 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1996, pages 207-226.

5. Marvel L.M., Boncelet C.G., Jr. and C.T. Retter. Spread Spectrum Image Steganography, IEEE Transactions on Image Processing, Vol 8, No 8, August 1999, pages 1075-1083.

Надійшла до редколегії 12.10.2011

Рецензент: д-р техн. наук, проф. О.О. Кузнецов, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

СТЕГАНОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ПРЯМОГО РАСШИРЕНИЯ СПЕКТРА

А.А. Смирнов

Рассматриваются стегранографические системы защиты информации, в которых решается задача скрытной передачи информации не только путем утаивания содержательной части сообщений, но и путем утаивания самого факта организации каналов скрытной передачи данных. Исследуются основные стегранографические преобразование с применением технологии прямого расширения спектра. Предложены структурные схемы устройств стеганографического утаивания и изъятия данных в пространственной области неподвижных изображений с использованием прямого расширения спектра.

Ключевые слова: *стеганография, защита информации, стеганоконтейнер.*

STEGANOGRAPHY PRIV WITH THE USE OF DIRECTEXPANSION OF SPECTRUM

A.A. Smirnov

The steganography systems of priv are examined, inthat the task of secretive information transfer decides not only by the concealment of rich in content part of reports but also by the concealment of fact of organization of channels of secretive data. The basic are investigated steganography transformation with the use of technology of direct expansion of spectrum. The flow diagrams of devices of steganography concealment and withdrawal of data are offered in the spatial area of immobile images with the use of direct expansion.

Keywords: *steganography, protection to information, steganocontainer.*