УДК 621.396

А.А. СМИРНОВ, канд. техн. наук

КРИТЕРИИ И ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Введение

Современное развитие информационных технологий привело к появлению новых угроз информационной безопасности, реализация которых может привести к непоправимым последствиям в различных сферах человеческой деятельности [1 – 4]. Следовательно, разработка перспективных технологий защиты информации, позволяющих противостоять современным угрозам, является актуальным научно-техническим заданием.

Одним из перспективных направлений в развитии современной теории защиты информации является цифровая стеганография, основной задачей которой является сокрытие не только смыслового содержания передаваемых данных, но и самого факта осуществления скрытной передачи информации [5 – 8]. Реализованные таким образом механизмы безопасности потенциально позволят обеспечить защиту от большего числа различных угроз информационной безопасности, предоставив конечному пользователю необходимые гарантии функций защиты.

В данной работе исследуется математическая модель и структурная схема стеганографической системы, вводятся критерии и показатели эффективности ее функционирования.

Структурная схема и математическая модель стеганографической системы

Основное функциональное отличие стеганографической и криптографической (секретной) систем определяется их целевым назначением. В то время как основной задачей секретной системы является сокрытие смыслового содержания передаваемых сообщений, основной задачей стеганографической системы является сокрытие самого факта организации передачи сообщений. Другими словами, противник, наблюдающий за открытым каналом связи в секретной системе, *наблюдает факт передачи данных*, и его задачей является поиск смыслового содержания этих данных. В стеганографической системе противник, наблюдая за открытым каналом связи, должен сперва *установить факт передачи данных*, после чего (при наличии такой передачи) найти смысловое содержание передаваемых данных.

Сокрытие факта организации передачи информационных сообщений безусловно обеспечивает и сокрытие их смыслового содержания. С этой точки зрения стеганографическую систему следует считать некоторым обобщением секретной системы, поскольку потеря (снижение) функции сокрытия факта организации передачи данных переводит стеганографическую систему в разряд секретной (криптографической) системы, ограничивая ее задачи до сокрытия смыслового содержания передаваемых сообщений.

Учитывая указанное функциональное отличие стеганографической системы, ее математическую опишем следующим образом.

Пусть $I = \{I_0, I_1, I_2, ..., I_m\}$ – множество возможных сообщений (событий), появляющихся на выходе источника информации, где символом I_0 формально обозначено «пустое сообщение», т.е. обозначение I_0 соответствует случаю, когда источник информации не формирует никаких сообщений, подлежащих передаче по каналам связи. Символы $I_1, I_2, ..., I_m$ соответствуют случаю формирования m различных «ненулевых» сообщений. Основной задачей секретной системы, как было показано выше, является сокрытие смыслового содержания этих информационных сообщений для любого $i = 1, 2, \ldots, m$. Сам факт передачи данных по каналам связи не скрывается и из формального описания в математической модели секретной системы случай отсутствия передачи «пустого сообщения» исключен.

Основной задачей стеганографической системы является такая организация передачи сообщений, при которой для любого $I_i, i = 0, 1, 2, ..., m$ наблюдаемый противником открытый канал связи неразличим, т.е. передача любого из сообщений $I_1, I_2, ..., I_m$ для противника неотличима от передачи «пустого сообщения» I_0, когда информационные данные вовсе не передаются. Задача распознавания передачи «пустого сообщения» I_0 и передачи любого из «ненулевых» сообщений $I_1, I_2, ..., I_m$ и есть задачей установления факта передачи данных, решаемой противником в стеганографической системе защиты информации.

Зафиксируем множество информационных данных $M = \{M_0, M_1, M_2, ..., M_m\}$, где каждое $M_i, i = 1, 2, ..., m$ соответствует результату предварительного кодирования сообщений из множества I, т.е. $M_i = f(I_i), i = 0, 1, 2, ..., m$, где $f(x)$ – формальное обозначение функции предварительного кодирования, реализуемой соответствующим устройством. Предварительное кодирование предназначено для подготовки информационного сообщения к встраиванию в контейнер (например, посредством шифрования, помехоустойчивого кодирования и/или преобразования информационного сообщения в массив специально отформатированных цифровых данных). Символом M_0 формально обозначен результат предварительного кодирования «пустого сообщения», т.е. обозначение M_0 соответствует случаю отсутствия каких-либо информационных данных, подлежащих передачи по открытым каналам связи.

Зафиксируем множество возможных пустых контейнеров $L = \{L_1, L_2, ..., L_l\}$, предназначенных для встраивания в них информационных данных. Обозначим через $E^* = \{E_1^*, E_2^*, ..., E_n^*\}$ множество возможных стеганограмм, которое содержит все элементы множества пустых контейнеров L, а также все элементы множества заполненных контейнеров $E = \{E_1, E_2, ..., E_{lm}\}$. Другими словами, каждый элемент множества E^* однозначно связан с соответствующей парой элементов из множеств L и M соответственно. При этом множество E^* должно содержать все элементы множества L, поскольку в процессе стеганографического преобразования информационные данные могут вовсе не встраиваться в какой-либо пустой контейнер из множества L. Формально этот случай соответствует встраиванию «пустого сообщения» M_0, при этом соответствующие элементы множества E будут тождественны элементам множества L. Таким образом, $E = L \cup E^*$, причем $\left|E^*\right| = ml$, $\left|E^*\right| = n = (m+1)l$.

Зафиксируем множество отображений:

$$\varphi = \{\varphi_1, \varphi_2, ..., \varphi_k\},$$

где φ_i: $(M, L) \to E^*$, $i = 1, 2, ..., k$, а также множество обратных отображений:

$$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_k^{-1}\}$$

где каждое

$$\varphi_i^{-1}: E^* \to (M^*, L),$$

которое каждому элементу множества E^* ставит в соответствие элемент множества L и элемент множества M^*, причем

$$M^* = M \cup \overline{M},$$

где $\overline{M} = \{\overline{M_1}, \overline{M_2}, ..., \overline{M_l}\}$ – множество извлеченных данных из стеганограмм, соответствующих пустым контейнерам $L = \{L_1, L_2, ..., L_l\}$.

Другими словами, при реализации обратного стеганографического преобразования информации в результате извлечения имеем некоторую «оценку» информационных данных M_j^*, которая может как относиться, так и не относиться к множеству «ненулевых» информационных данных $\{M_1, M_2, ..., M_m\}$. Задачей уполномоченного пользователя на приемной стороне стеганографической системы является детектирование сообщения, т.е. сопоставление полученной «оценки» M_j^* с одним из подмножеств.

Зафиксируем множество ключей $K = \{K_1, K_2, ..., K_k\}$ так, что для всех $i = 1, 2, ..., k$ отображение $\varphi_i \in \varphi$ однозначно задается ключом K_i, т. е.:

$$\varphi_i : (M, L) \xrightarrow{K_i} E .$$

Каждое конкретное отображение φ_i из множества φ соответствует способу встраивания сообщения из множества M в контейнер из множества L при помощи конкретного ключа K_i. На рис. 1 схематично представлено отображение $\varphi_i \in \varphi$, заданное ключом K_i.

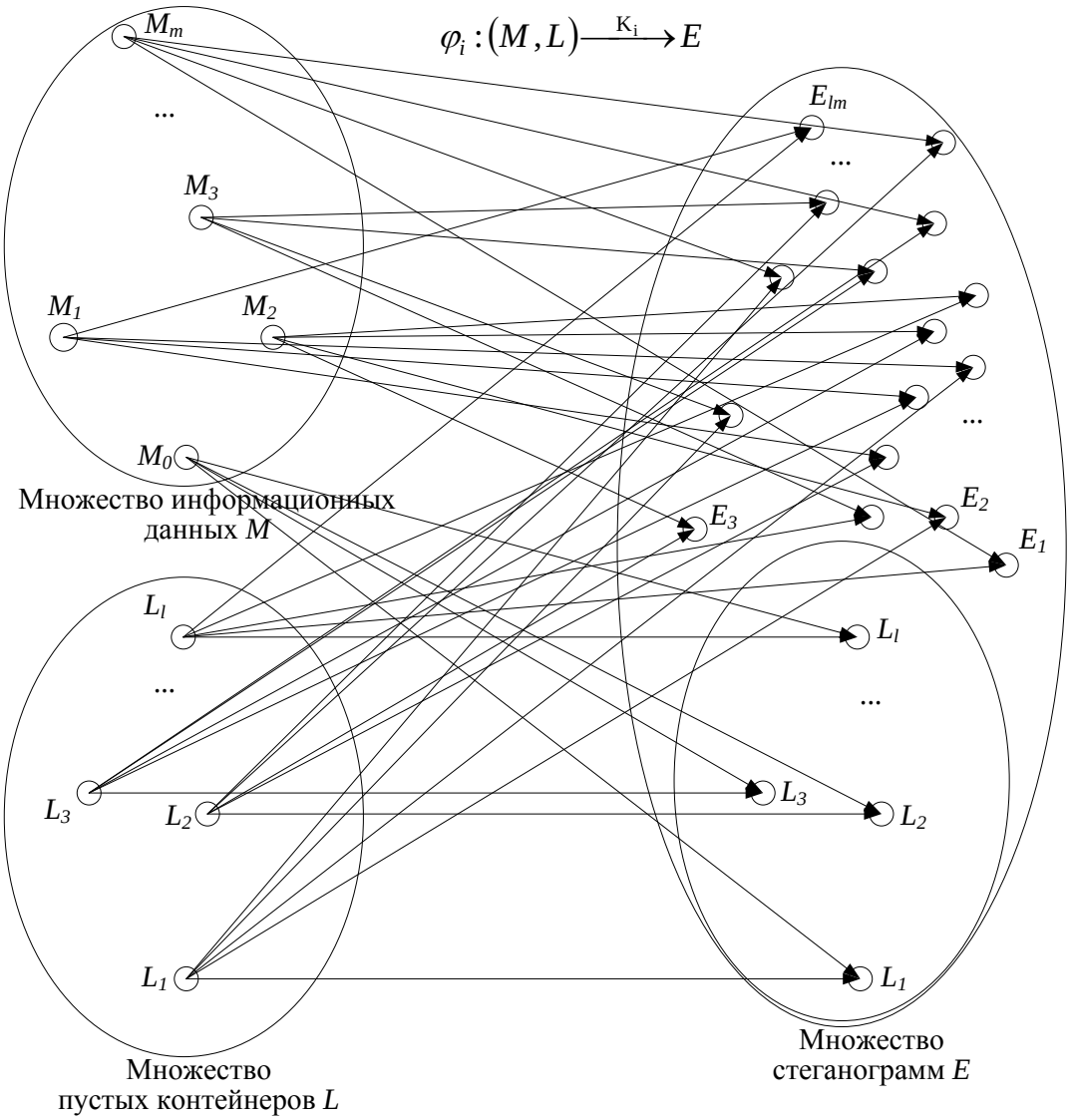

Рис. 1. Отображение $\varphi_i : (M, L) \xrightarrow{K_i} E$ множества открытых текстов и множества контейнеров в множество стеганограмм

Зафиксируем множество ключей $K^* = \{K_1^*, K_2^*, \ldots, K_k^*\}$, в общем случае $K \neq K^*$. Все элементы множества обратных отображений:

$$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_k^{-1}\}$$

задаются соответствующим ключом:

$$\varphi_i^{-1} : E \xrightarrow{K_i^*} \left(M^*, L\right).$$

Каждое конкретное отображение φ_i^{-1} из множества φ^{-1} соответствует способу извлечения сообщения из заполненного контейнера (и формирования пустого контейнера) при помощи ключа K_i^*. Если известен ключ K_i^*, то в результате выполнения операции извлечения возможен лишь единственный ответ – элемент некоторого множества M^* и элемент множества L:

$$\left(M_j^*, L_l\right) = \varphi_i^{-1}\left(E_w, K_i^*\right).$$

Множество M^* содержит все элементы множества M, кроме того, оно также содержит и другие элементы, соответствующие результату извлечения.

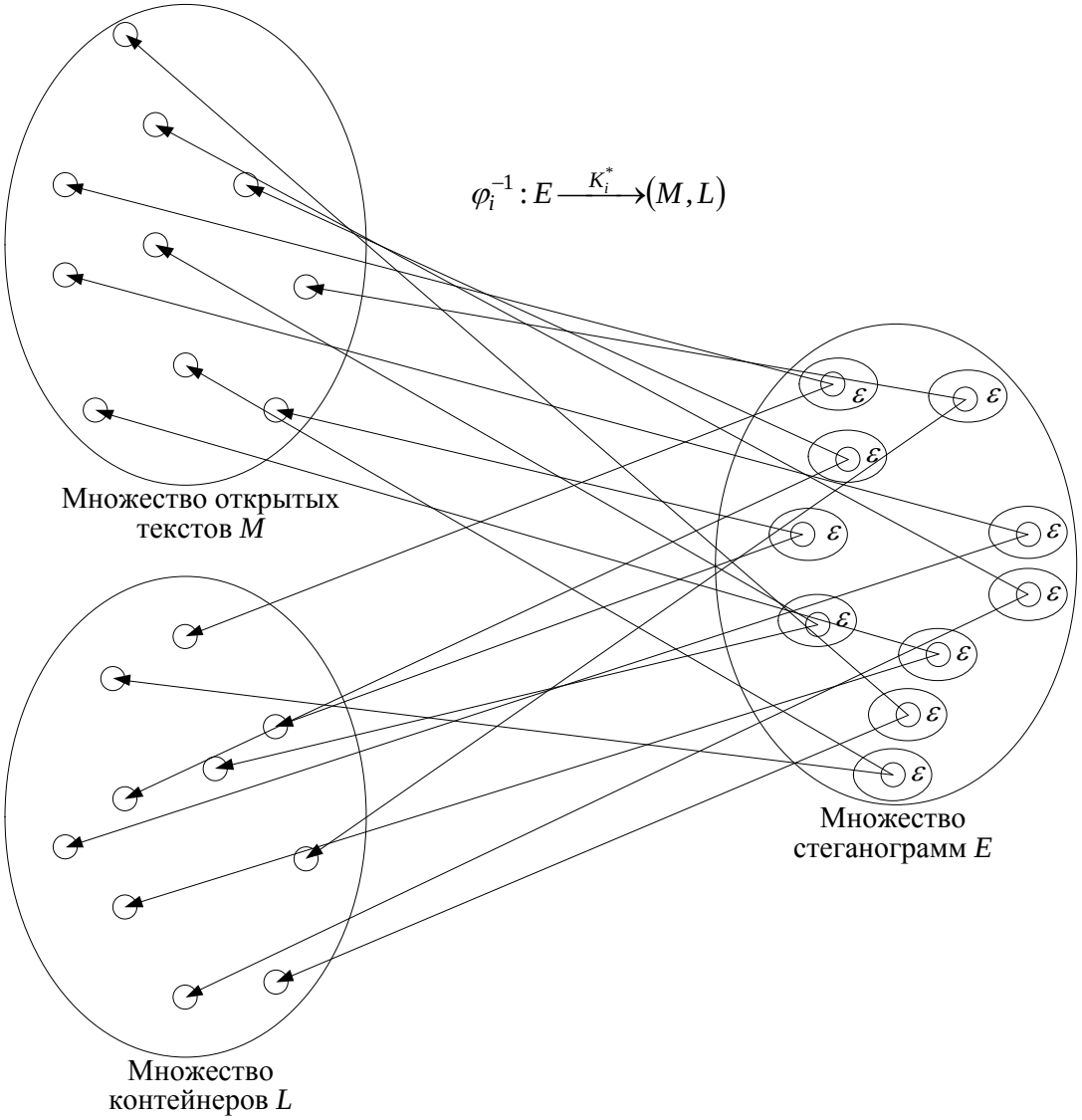

Рис. 2. Отображение $\varphi_i^{-1} : E \xrightarrow{K_i^*} (M, L)$ множества стеганограмм в множество открытых текстов и множество контейнеров

Для некоторых стеганографических систем справедливо равенство

$$\left(M_j, L_l\right) = \varphi_i^{-1}\left(E_w + \varepsilon, K_i^*\right),$$

т.е. незначительное изменение заполненного контейнера (на величину ε) не приведет к неправильному извлечению сообщения в процессе реализации отображения $\varphi_i^{-1} : E \xrightarrow{K_i^*} (M, L)$.

Этот процесс схематично представлен на рис. 2. Соответствующие указанному свойству стеганосистемы принято называть *робастными* [5 – 7].

Если для стеганосистемы характерно выполнение неравенства

$$\left(M_j, L_l\right) \neq \varphi_i^{-1}\left(E_w + \varepsilon, K_i^*\right)$$

для сколь угодно малой величины ε, тогда такие системы принято называть хрупкими.

Таким образом, в абстрактное *определение стеганографической системы* входят следующие множества M, L, E, φ, φ^{-1}, K и K^* (множества открытых текстов, пустых контейнеров и стеганограмм (заполненных контейнеров), множества прямых и обратных отображений и множества соответствующих им ключей).

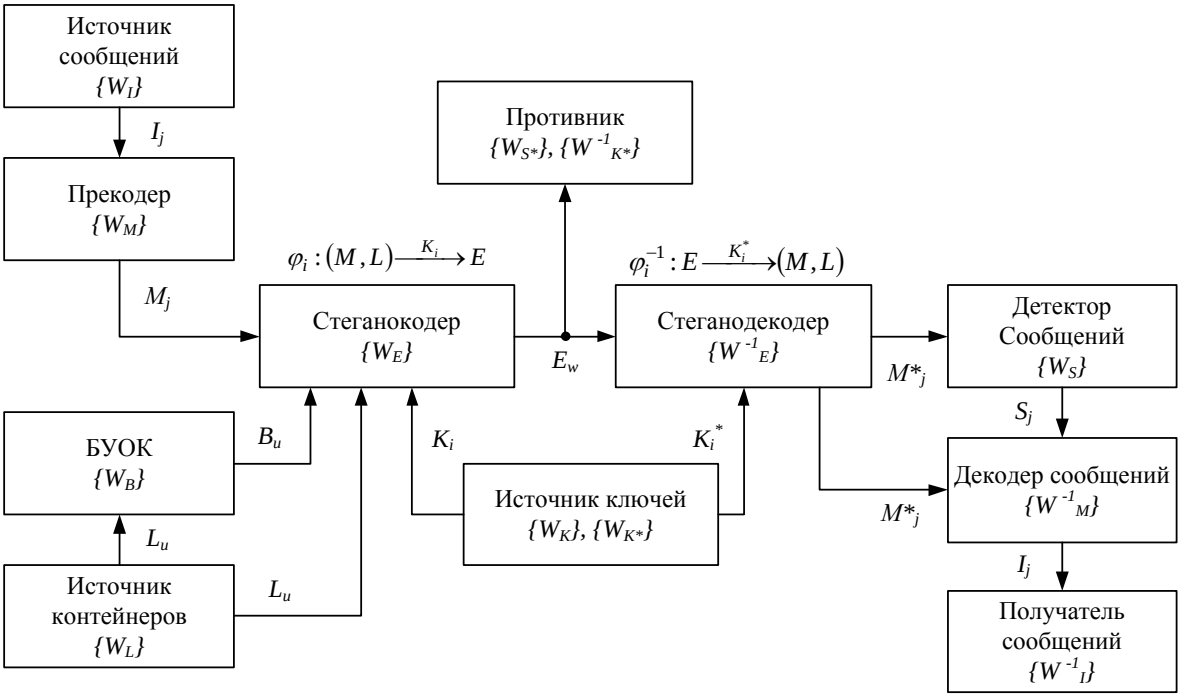

Рис. 3. Структурная схема стеганографической системы

На рис. 3 представлена структурная схема стеганографической системы. На схеме обозначены следующие элементы математической модели стеганосистемы:

– $I = \{I_1, I_2, \ldots, I_m\}$ – множество информационных сообщений, формируемых источником;

– $M = \{M_1, M_2, \ldots, M_m\}$ – множество информационных данных, полученных на выходе прекодера после соответствующего преобразования;

– $L = \{L_1, L_2, \ldots, L_l\}$ – множество пустых конейнеров, формируемых источником контейнеров и предназначенных для встраивания данных;

– $E = \{E_1, E_2, \ldots, E_n\}$ – множество возможных стеганограмм (заполненных контейнеров), формируемых устройством стеганографического кодирования (стеганокодером);

– $\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_k\}$ – множество прямых отображений множества информационных данных M и множества пустых контейнеров L в множество возможных стеганограмм E, формируемых стеганокодером, $\varphi_i: M \to E$, $i = 1, 2, \ldots, k$;

– $\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_k^{-1}\}$ – множество обратных отображений множества возможных стеганограмм E в множество информационных данных M и множество пустых контейнеров L, $\varphi^{-1}{}_i: E \to M$, $i = 1, 2, \ldots, k$;

– $K = \{K_1, K_2, \ldots, K_k\}$ – множество ключей прямого стеганографического преобразования (стеганокодирования), причем каждое отображение $\varphi_i \in \varphi$ из множества прямых отображений $\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_k\}$ задается ключом K_i;

– $K^* = \{K_1^*, K_2^*, \ldots, K_k^*\}$ – множество ключей обратного стеганографического преобразования (стеганодекодирования), причем каждое обратное отображение $\varphi_i^{-1} \in \varphi^{-1}$ из множества обратных отображений $\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_k^{-1}\}$ задается ключом K^*_i;

– $\{W_I\}$ – оператор формирования информационных сообщений $I_j \in \{M_1, M_2, \ldots, M_m\}$;

– $\{W_M\}$ – оператор предварительного кодирования информационных сообщений, результатом действия которого являются информационные данные $M_j \in \{M_1, M_2, \ldots, M_m\}$;

– $\{W_L\}$ – оператор формирования пустых контейнеров $L_u \in \{L_1, L_2, \ldots, L_l\}$, предназначенных для встраивания информационных данных;

– $\{W_B\}$ – оператор исследования и оценки особенностей формируемых контейнеров, результатом действия которого являются выработанные правила и ограничения B_u на встраивание информационных данных в сформированные контейнеры $L_u \in \{L_1, L_2, \ldots, L_l\}$;

– $\{W_E\}$ – оператор прямого стеганографического преобразования (стеганокодирования) информационных данных $M_i \in \{M_1, M_2, \ldots, M_m\}$ и пустых контейнеров $L_u \in \{L_1, L_2, \ldots, L_l\}$ в стеганограммы (заполненные контейнеры) $E_i \in \{E_1, E_2, \ldots, E_n\}$;

– $\{W^{-1}_E\}$ – оператор обратного стеганографического преобразования (стеганодекодирования) стеганограмм (заполненных контейнеров) $E_i \in \{E_1, E_2, \ldots, E_n\}$ в информационные данные $M_i \in \{M_1, M_2, \ldots, M_m\}$ и пустые контейнеры $L_u \in \{L_1, L_2, \ldots, L_l\}$;

– $\{W_K\}$ – оператор формирования ключевых данных $K_i \in \{K_1, K_2, \ldots, K_k\}$ прямого криптографического преобразования (шифрования) и ключевых данных $K^*_i \in \{K^*_1, K^*_2, \ldots, K^*_k\}$ обратного криптографического преобразования (расшифрования);

– $\{W^{-1}_{M^*}\}$ – оператор действий противника по реализации безключевого чтения, т.е. нахождения информационного сообщения $M_i \in \{M_1, M_2, \ldots, M_m\}$ без знания ключевых данных $K^*_i \in \{K^*_1, K^*_2, \ldots, K^*_k\}$ обратного криптографического преобразования (расшифрования);

– $\{W^{-1}_{K^*}\}$ – оператор действий противника по реализации поиска секретного ключа $K^*_i \in \{K^*_1, K^*_2, \ldots, K^*_k\}$ обратного криптографического преобразования (расшифрования);

– $\{W^{-1}_M\}$ – оператор обработки полученных информационных сообщений $M_i \in \{M_1, M_2, \ldots, M_m\}$ получателем информации.

Источник сообщений порождает поток информационных сообщений I_j из множества $I = \{I_1, I_2, \ldots, I_m\}$, которое, после предварительного преобразования в прекодере, формируется в виде сообщения M_j из множества M. Прекодер выполняет, таким образом, функцию предварительной подготовки информационного сообщения к встраиванию в контейнер (например, преобразование информационного сообщения в массив специально отформатированных цифровых данных и/или помехоустойчивое преобразование информации).

Источник контейнеров порождает поток пустых контейнеров L_u из множества $L = \{L_1, L_2, \ldots, L_l\}$. Сформированный контейнер L_u обрабатывается блоком учета особенностей контейнеров (БУОК). Основной функцией БУОК является выделение тех признаков (особенностей) B_u поступившего контейнера L_u, которые будут использованы при встраивании в него сообщения M_j .

Источник ключей в стеганографической системе порождает поток ключей из множества K и/или K^*. Выбор ключа K_i определяет конкретное отображение φ_i из множества отображе-

ний φ. С помощью отображения φ_i, соответствующего выбранному ключу K_i, по поступившему сообщению M_j и поступившему контейнеру L_u с учетом выявленных особенностей B_u контейнера L_u формируется стеганограмма (заполненный контейнер):

$$E_w = \varphi_i\left(K_i, M_j, L_u\right),$$
$$i \in [1,2,..., k],\ j \in [1,2,..., m],\ u \in [1,2,..., l],\ w \in [1,2,..., n],\ n \geq m.$$

Стеганограмма E_w передается в точку приема по некоторому каналу и может быть перехвачена противником. На приемном конце с помощью обратного отображения φ_i^{-1} (заданного ключом K_i^*) из стеганограммы E_w восстанавливается первоначальное сообщение и пустой контейнер:

$$\left(M_j, L_u\right) = \varphi_i^{-1}\left(K_i, E_w\right).$$

При передаче стеганограммы E_w по каналу связи и возможном воздействии противником на E_w передаваемая стеганограмма может исказиться. В этом случае на приемной стороне будет принята некоторая смесь переданного заполненного контейнера и результата воздействия на контейнер при передаче по каналу связи: $E_w+\varepsilon$. Выполнение операции обратного отображения φ_i^{-1} (заданного ключом K_i^*) в этом случае приведет к формированию некоторой оценки переданного сообщения и переданного пустого контейнера, т.е. получим:

$$\left(M_j^*, L_u^*\right) = \varphi_i^{-1}\left(K_i, E_w + \varepsilon\right).$$

Для хрупких стеганографических систем неравенство $M_j^* \neq M_j$ должно приводить к отбраковке сообщения, т.е. при малейшем искажении контейнера ($\varepsilon \neq 0$) извлеченная оценка M_j^* не должна приводить к прочтению встроенного сообщения (сообщение M_j разрушается при $\varepsilon \neq 0$).

Робастные стеганографические системы устойчивы к воздействию на заполненный контейнер. В введенных выше обозначениях это означает, что при $\varepsilon \neq 0$ извлеченная оценка M_j^* должна сопоставляться с одним из возможных сообщений (в идеальном случае, с сообщением M_j). В то же время, полученный из канала связи контейнер E_w может вовсе не содержать встроенного сообщения, т.е извлеченная из контейнера оценка M_j^* не должна быть сопоставлена ни с одним из допустимых сообщений. Функции детектирования встроенного сообщения на приемной стороне возложены на детектор сообщений, который по поступившей оценке M_j^* принимает решение о наличии или отсутствии встроенного сообщения в принятом контейнере E_w. Таким образом, оценка детектора S_j может быть интерпретирована как двоичное (да/нет) решение помехоустойчивого декодера о наличии или отсутствии неисправляемой ошибки. Само декодирование осуществляется в декодере сообщений, основными функциями которого является сопоставление извлеченной оценки M_j^* с одним из возможных сообщений M_j и преобразования последнего в информационное сообщение I_j, предоставляемое получателю информации.

Критерии и показатели эффективности стеганографических систем

Под эффективностью технической системы в широком смысле понимают соответствие результата выполнения некоторой операции требуемому [9]. При этом техническая система выступает в роли средства реализации исследуемой операции [10].

Применительно к рассматриваемому процессу стеганографическая система выступает в роли технического средства реализации операции, целью которой является сокрытие от противника факта осуществления скрытной передачи информации.

Таким образом, с учетом функционального назначения стеганосистемы, введем следующие показатели эффективности:

1. Пропускная способность – как предел отношения объема V встраиваемой в контейнер информации к общему объему D контейнера:

$$Q = \lim_{D \to \infty} \left(\frac{V}{D} \right). \quad (1)$$

2. Объем ключевых данных (в битах):

$$l_K = \log_2 \left(|K| \right), \quad (2)$$

где $|K|$ – мощность множества ключевых данных.

3. Стойкость стеганосистемы.

3.1. Вероятность нахождения противником ключа детектирования (извлечения) сообщений, оцениваемая по критерию минимального риска:

$$P_K = \max \left\{ P_K(u_1), P_K(u_2), \ldots, P_K(u_{L_K}), \right\},$$

где $P_K(u_i)$ – вероятность нахождения противником ключа детектирования (извлечения) сообщений при использовании им стратегии u_i, L_K – количество различных стратегий противника по нахождению ключа детектирования (извлечения) сообщений.

3.2. Вероятность несанкционированного детектирования (извлечения) сообщения без знания секретного ключа (вероятность безключевого детектирования (чтения) сообщений), оцениваемая по критерию минимального риска:

$$P_M = \max \left\{ P_M(v_1), P_M(v_2), \ldots, P_M(v_{L_M}), \right\},$$

где $P_M(v_i)$ – вероятность несанкционированного детектирования (извлечения) сообщения противником при использовании им стратегии v_i, L_M – количество различных стратегий противника по несанкционированногому детектированию (извлечению) сообщения.

3.3. Безопасное время работы стеганосистемы, характеризующее вычислительные возможности противника по реализации различных стратегий (атак), оцениваемое по критерию минимального риска:

$$T_Б = \min_{i,j} \left\{ T_Б(u_i), T_Б(v_j) \right\}, \quad (3)$$

где

$$T_Б(u_i) = \frac{\left(P_K(u_i) \right)^{-1}}{\Psi \gamma}, \; T_Б(v_i) = \frac{\left(P_K(v_j) \right)^{-1}}{\Psi \gamma},$$

$T_Б(u_i)$, $T_Б(v_i)$ – безопасное время работы стеганосистемы, характеризующее вычислительные возможности противника по реализации различных стратегии (атаки) u_i и v_j, $i = 1, L_K$, $j = 1, L_M$, Ψ – производительность вычислительной системы, доступная противнику, измеряемая в количестве переборных операций в единицу времени, γ – числовой показатель (константа), для пересчета в требуемые единицы измерения безопасного времени (например, при оценке безопасного времени в годах соответствующее значение $\gamma \approx 3{,}2 \cdot 10^7$).

4. Величина вносимых искажений как предел процентного отношение среднеарифметического всех абсолютных значений Δ-изменений данных контейнера к максимально возможному значению $\Delta_{\max}$:

$$I^* = \lim_{D\to\infty}\left(\frac{\Delta_{ср}}{\Delta_{\max}}\cdot 100\right) = \lim_{D\to\infty}\left(\frac{100}{\Delta_{\max}\cdot D}\cdot\sum_{i=1}^{D}|\Delta_i|\right), \quad (4)$$

где $\Delta_i - \Delta$ – изменения i-го элемента контейнера.

5. Вероятность ошибочного извлечения информационных данных сообщения как предел отношения числа ошибочно извлеченных сообщений:

$$P_{ош} = \lim_{V\to\infty}\frac{V_{ош}}{V} = 1 - \lim_{V\to\infty}\left(\frac{V - V_{ош}}{V}\right), \quad (5)$$

где $V_{ош}$ – объем ошибочно извлеченных данных.

Множество введенных показателей (1) – (5) и критериев их оценки позволяет математически формализовать постановку задачу совершенствования стеганосистемы.

Так, обобщенный показатель эффективности стеганографической системы защиты информации с учетом (1) – (5) в общем виде запишем как функционал:

$$W = F\left(Q, l_K, P_K, P_M, T_Б, I^*, P_{ош}\right),$$

где вид функционала $F\left(Q, l_K, P_K, P_M, T_Б, I^*, P_{ош}\right)$ и конкретный вклад отдельных (частных) показателей эффективности $Q, l_K, P_K, P_M, T_Б, I^*, P_{ош}$ в значении обобщенного показателя W определяется исходя из конкретного назначения системы, особенностей ее использования и условий эксплуатации.

Целевую функцию задачи совершенствования стеганосистемы в общем виде запишем через максимизацию обобщенного показателя эффективности:

$$\max\left(W\right) = \max\left(F\left(Q, l_K, P_K, P_M, T_Б, I^*, P_{ош}\right)\right).$$

Выводы

В ходе исследований введены основные элементы и математические операторы, абстрактно описывающие стеганографическую систему защиты информации. Во введенной формализации получено определение хрупких и робастных стеганосистем, а также введены критерии и показатели эффективности стеганографической защиты информации. В общем виде формализована задача совершенствования стеганосистемы через максимизацию обобщенного показателя ее эффективности. Перспективным направлением дальнейших исследований является сравнительный анализ известных стеганосистем по введенным показателям и критериям оценки эффективности, обоснование перспективных путей их дальнейшего совершенствования.

Список литературы: 1. *Final* report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 – Version 0.15 (beta), Springer-Verlag, p 829. 2. *Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone.* Handbook of Applied Cryptography – CRC Press, 1997. – 794 p. 3. *Молдовян, Н.А., Молдовян, А.А., Еремеев, М.А.* Криптография: от примитивов к синтезу алгоритмов. – СПб. : БХВ-Петербург, 2004. – 448с. 4. *Сидельников, В.М.* Криптография и теория кодирования // Материалы конференции «Московский университет и развитие криптографии в России». – МГУ, 2002. – 22 с. 5. *Конахович, Г. Ф., Пузыренко, А. Ю.* Компьютерная стеганография. Теория и практика. – К. : «МК-Пресс», 2006. – 288 с. 6. *Грибунин, В. Г , Оков, И. Н., Туринцев, И. В.* Цифровая стеганография. Серия: Аспекты защиты. – Солон-Пресс, 2002. – 272 с. 7. *Хорошко, В.А., Шелест, М.Е.* Введение в компьютерную стеганографию. – К. : НАУ, 2002. – 140 с. 8. *Хорошко,В.О., Азаров,О.Д., Шелест, М.Е., Яремчук, Ю.Е.* Основи комп'ютерної стеганографії : навч. посібник. – Вінниця : ВДТУ, 2003. – 143 с. 9. *Авдуевский, В.С.* Надежность и эффективность в технике : справочник : в 10 т. / Ред. совет: В.С. Авдуевский (пред.) и др. – М. : Машиностроение, 1986. – Т. 1 : Методология. Организация. Терминология. – 224 с. 10. *Авдуевский, В.С.* Надежность и эффективность в технике : справочник : в 10 т. / Ред. совет: В.С. Авдуевский (пред.) и др. – М.: Машиностроение, 1986. – Т. 3. Эффективность технических систем. – 328 с.

Кировоградский национальный технический университет

Поступила в редколлегию 15.09.2012