УДК 003.26
DOI: 10.21122/2309-4923-2022-3-67-74

Е. А. БЛИНОВА

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ НА ОСНОВЕ КЛЮЧЕВОЙ ИНФОРМАЦИИ В ВИДЕ СТЕГОНАБОРОВ

Белорусский государственный технологический университет

Приведено формальное описание математической модели стеганографической системы, основанной на ключе-вой информации в виде стегонаборов. Математическая модель стеганографической системы предназначена как для размещения скрытых меток для контроля целостности документов, выступающих в качестве контейнера, так и для скрытой передачи данных. Существующие математические модели не полностью удовлетворяют требованиям, предъявляемым к стеганографическим системам. Предлагаемая модель строится на основе поня-тий трехуровневого ключа, стегонабора, компонента контейнера, блока сообщения и контрольного числа. Трехуровневый ключ представляет собой множество фактических стеганографических преобразований в зави-симости от типа контейнера. Стегонабор представляет собой элемент множества ключа. Компонентом сте-гоконтейнера является такое его подмножество, что для него существует стегонабор. Блоком сообщения яв-ляется такая последовательная часть сообщения, что для нее существуют компонент контейнера, в котором она может быть скрыта при помощи соответствующего стегонабора. Модель реализует применение различных стегонаборов к различным компонентам контейнера, причем сообщение может разбиваться на блоки. Модель позволяет контролировать целостность цифровых меток и скрытого сообщения. Предлагаются возможные варианты практического применения математической модели, такие как контроль целостности сообщения при вычислении контрольного числа, разбиение сообщения на блоки и последовательный контроль их целостно-сти по аналогии с системой блокчейн.

Ключевые слова: *стеганография; математическая модель; авторское право.*

Введение

Математическому моделированию стеганографических систем уделяется значительное внимание в работах [1-3]. В настоящее время в качестве общепринятой математической модели стеганографической системы принята следующая. Пусть:

$\boldsymbol{M}$ – это конечное множество сообщений, которые могут быть размещены в контейнере:

$$\boldsymbol{M} = \{M_1, M_2, \ldots, M_N\}, \quad (1)$$

где N – количество сообщений;

$\boldsymbol{C}$ – это конечное множество всех потенциальных контейнеров:

$$\boldsymbol{C} = \{C_1, C_2, \ldots, C_Q\}, \quad (2)$$

где Q – количество потенциальных контейнеров;

$\boldsymbol{K}$ – это конечное множество всех допустимых потенциальных ключей:

$$\boldsymbol{K} = \{K_1, K_2, \ldots, K_P\}, \quad (3)$$

где P – количество допустимых потенциальных ключей;

$\boldsymbol{S}$ – множество заполненных контейнеров (стегоконтейнеров):

$$\boldsymbol{S} = \{S_1, S_2, \ldots, S_R\}, \quad (4)$$

где R – количество заполненных контейнеров.

Произвольное тайное сообщение M_i можно скрыть в контейнере C_j при использовании ключа K_m, где $M_i \in \boldsymbol{M}$, $i \in [1, N]$; $C_j \in \boldsymbol{C}$, $j = [1, Q]$; $K_m \in \boldsymbol{K}$, $m = [1, P]$. Результатом такого преобразования будет стегоконтейнер S_q, $S_q \in \boldsymbol{S}$, $q \in [1, R]$.

Функция $\boldsymbol{F}$, определенная на $\boldsymbol{M} \times \boldsymbol{C} \times \boldsymbol{K}$ со значениями в $\boldsymbol{S}$, отождествляется со скрытием сообщения M_i из множества $\boldsymbol{M}$ в контейнер C_j из множества $\boldsymbol{C}$ на основе ключа из множества $\boldsymbol{K}$:

$$\boldsymbol{F}: \boldsymbol{M} \times \boldsymbol{C} \times \boldsymbol{K} \longrightarrow \boldsymbol{S}. \quad (5)$$

Функция $\boldsymbol{F}^{-1}$, определенная на $\boldsymbol{S} \times \boldsymbol{K}$ со значениями в $\boldsymbol{M}$, отождествляется с извлечением тайного сообщения $M_i \in \boldsymbol{M}$ из стегоконтейнера $S_q \in \boldsymbol{S}$:

$$\boldsymbol{F}^{-1}: \boldsymbol{S} \times \boldsymbol{K} \longrightarrow \boldsymbol{M}, \boldsymbol{C}. \quad (6)$$

Соотношение (5) формально описывает процедуру скрытия сообщения M_i в контейнер C_j на основе выбранного ключа K_m.

Соотношение (6) формально описывает процедуру извлечения сообщения M_i из стегоконтейнера S_q, используя ключ K_m.

Таким образом, стеганографическая

система представляет собой поле $\boldsymbol{SF}$, в котором определены как стеганографические объекты, так и функции преобразования:

$$\boldsymbol{SF} = (\boldsymbol{C}, \boldsymbol{M}, \boldsymbol{K}, \boldsymbol{F}, \boldsymbol{F^{-1}}). \quad (7)$$

Авторы работы [4] вводят понятие дополнительного ключа $\boldsymbol{K_д}$, который представляет собой криптографическое преобразование или преобразование для помехоустойчивого кодирования. Таким образом, стеганографическая система представляет собой совокупность сообщений, контейнеров, ключей и преобразований, которые их связывают:

$$\boldsymbol{\Sigma} = (\boldsymbol{C}, \boldsymbol{M}, \boldsymbol{K}, \boldsymbol{K_д}, \boldsymbol{F}, \boldsymbol{F^{-1}}) \quad (8)$$

Авторы работе [5] вводят понятие стеганографического канала $\boldsymbol{SC}$ – такой пространственной, временной или частотной области данных, которая пригодна для стеганографической передачи сообщений:

$$\boldsymbol{F}: \boldsymbol{C} \longrightarrow \boldsymbol{SC} \quad (9)$$

и стеганографическую систему определяют, как:

$$\boldsymbol{SF} = (\boldsymbol{SC}, \boldsymbol{C}, \boldsymbol{M}, \boldsymbol{K}, \boldsymbol{F}, \boldsymbol{F^{-1}}). \quad (10)$$

В [6] вводится понятие многоключевой стеганографической системы. Авторы работы полагают, что стеганографическая система, описываемая соотношением (7), может считаться одноключевой, где в качестве ключа выступает алгоритм скрытия/извлечения информации. Анализируя дополнительные меры по защите стеганографической системы, авторы предлагают ввести понятие многоключевой стеганографической системы. Причем в качестве дополнительного ключа первого рода выступает криптографическое преобразование или преобразование для помехоустойчивого кодирования, а в качестве дополнительного ключа второго рода выступает порядок выбора элементов контейнера (пикселей, цветовых компонентов, отдельных символов текста и др.) при реализации процедур скрытия/извлечения сообщения. Таким образом, стеганографическая система может быть пред-ставлена в виде пары преобразований:

$$\boldsymbol{F}: \boldsymbol{M} \times \boldsymbol{K_{Д1}} \times \boldsymbol{C} \times \boldsymbol{K_0}, \boldsymbol{K_{Д2}} \longrightarrow \boldsymbol{S}, \quad (11)$$

$$\boldsymbol{F^{-1}}: \boldsymbol{S} \times \boldsymbol{K_0}, \boldsymbol{K_{Д2}} \times \boldsymbol{K_{Д1}}^* \longrightarrow \boldsymbol{M}, \boldsymbol{C}, \quad (12)$$

где K_0 – основной ключ, $K_{Д1}$ – дополнительный ключ первого рода для шифрования/кодирования сообщения, $K_{Д2}$ – дополнительный ключ второго рода для выбора элементов контейнера для встраивания, $K_{Д1}^*$ – дополнительный ключ первого рода для расшифрования/раскодирования сообщения.

Однако существующие математические модели не учитывают важные, на наш взгляд, особенности, такие как необходимость множественного внедрения сообщения и распределение сообщения в контейнере для контроля его целостности, что является основанием для разработки более детализированной математической модели стеганографической системы.

Основная часть

По аналогии с правилами Кергхоффса к стеганографической системе можно предъявить набор требований. Такая система должна:

1) быть многопараметрически стойкой;
2) быть максимально незаметной;
3) иметь секретный ключ;
4) позволять осуществление передачи, хранения и замены ключа;
5) быть совместимой с современными технологиями передачи и хранения данных;
6) быть простой в использовании;
7) не может быть универсальной;
8) ее надежность может быть проверена при помощи стеганографического анализа.

Определение 1

Многопараметрической стойкостью для стеганографической системы называется стойкость к обнаружению, извлечению и модификации скрытой информации, к раскрытию реализации стеганографической системы и ее ключа.

Сформулируем математическую модель стеганографической системы, удовлетворяющей данным требованиям. Для начала моделирования предлагаем взять общепринятую математическую модель, описанную соотношениями (1) - (6). Предлагаемая модель строится на основе понятий *трехуровневого ключа*, *стегонабора*, *компонента контейнера*, *блока сообщения* и *контрольного числа*. Далее дадим определения этим понятиям.

Множество $\boldsymbol{K}$ из соотношения (3) и преобразования $\boldsymbol{F}$ и $\boldsymbol{F^{-1}}$ из соотношений (5) и (6) могут быть детализированы следующим образом.

Определение 2

Ключом первого уровня называется такое конечное множество $\boldsymbol{K^1}$, что существует такое преобразование $\boldsymbol{F_1}$, определенное на $\boldsymbol{C}$, что:

$$\boldsymbol{F_1}: \boldsymbol{C} \longrightarrow \boldsymbol{K^1}, \qquad (16)$$

Множество ключей первого рода $\boldsymbol{K^1}$ будем отождествлять с стеганографическими преобразованиями, возможными для определенного типа контейнеров. Поскольку стеганографическая система, в первую очередь, представляет собой скрытое размещение сообщения в данных, то допустимо в качестве одного из компонентов ключевой информации рассматривать метод размещения скрытого сообщения. Для разных типов контейнеров эти методы и их количество различны. Например, для электронных документов в формате DOCX во множество $\boldsymbol{K^1}$ среди прочих входят: метод *Word-shift coding*, метод *Line-shift coding*, метод изменения цветовых характеристик и др.

Функцию $\boldsymbol{F_1}$, определенную на $\boldsymbol{C}$ со значениями в $\boldsymbol{K^1}$, будем отождествлять с выбором ключа первого уровня K^1_i из множества $\boldsymbol{K^1}$ для контейнера C_j из множества $\boldsymbol{C}$.

Определение 3

Ключом второго уровня называется такое конечное множество $\boldsymbol{K^2}$, что существует такое преобразование $\boldsymbol{F_2}$, определенное на декартовом произведении $\boldsymbol{C} \times \boldsymbol{K^1}$, что:

$$\boldsymbol{F_2}: \boldsymbol{C} \times \boldsymbol{K^1} \longrightarrow \boldsymbol{K^2}, \qquad (17)$$

Функцию $\boldsymbol{F_2}$, определенную на $\boldsymbol{C} \times \boldsymbol{K^1}$ со значениями в $\boldsymbol{K^2}$, будем отождествлять с выбором ключа второго уровня K^2_i из множества $\boldsymbol{K^2}$ для контейнера C_j из множества $\boldsymbol{C}$ на основе ключа из множества $\boldsymbol{K^1}$.

Множество ключей второго уровня $\boldsymbol{K^2}$ будем отождествлять с определенными особенностями реализации стеганографического преобразования. Например, если в качестве множества контейнеров выбраны электронные документы в формате DOCX, а в качестве множества ключей первого рода $\boldsymbol{K^1}$ выбран метод *Word-shift coding*, то множество $\boldsymbol{K^2}$ будет включать: *замену символов* символами другого алфавита, изменение *величины апроша*, изменение *контура буквы* и др.

Определение 4

Ключом третьего уровня называется такое конечное множество $\boldsymbol{K^3}$, что существует такое преобразование $\boldsymbol{F_3}$, определенное на $\boldsymbol{C} \times \boldsymbol{K^2}$, что:

$$\boldsymbol{F_3}: \boldsymbol{C} \times \boldsymbol{K^2} \longrightarrow \boldsymbol{K^3}, \qquad (18)$$

Функцию $\boldsymbol{F_3}$, определенную на $\boldsymbol{C} \times \boldsymbol{K^2}$ со значениями в $\boldsymbol{K^3}$, будем отождествлять с выбором ключа третьего уровня K^3_i для контейнера C_j из множества $\boldsymbol{C}$ на основе множества $\boldsymbol{K^3}$ на основе ключа из множества $\boldsymbol{K^2}$:

Множество ключей третьего уровня $\boldsymbol{K^3}$ будем отождествлять с определенными значениями реализации стеганографического преобразования. Например, если в качестве множества контейнеров выбраны электронные документы в формате DOCX, в качестве множества ключей первого рода $\boldsymbol{K^1}$ выбран метод *Word-shift coding*, в качестве множества $\boldsymbol{K^2}$ выбран метод изменения кернинга, то в качестве элементов множества $\boldsymbol{K^3}$ перечисляются *фактические кернинговые пары*. С учетом определений 1 – 4 соотношение (3) можно переписать следующим образом.

Следствие 1

Трехуровневым ключом является такое конечное множество $\boldsymbol{K}$, которое представляет собой набор $\{\boldsymbol{K^1}, \boldsymbol{K^2}, \boldsymbol{K^3}\}$, где $\boldsymbol{K^1}$

ключ первого уровня, $\boldsymbol{K^2}$ – ключ второго уровня, $\boldsymbol{K^3}$ ключ третьего уровня, такой, что для набора $\{\boldsymbol{C}, \boldsymbol{M}, \boldsymbol{K^1}, \boldsymbol{K^2}, \boldsymbol{K^3}, \boldsymbol{S}\}$ существует преобразование $\boldsymbol{F}$, определенное на декартовом произведении множеств $\boldsymbol{M}$, $\boldsymbol{C}$, $\boldsymbol{K^1}$, $\boldsymbol{K^2}$, $\boldsymbol{K^3}$, что:

$$\boldsymbol{F}: \boldsymbol{M} \times \mathbf{C} \times \boldsymbol{K^1} \times \boldsymbol{K^2} \times \boldsymbol{K^3} \longrightarrow \boldsymbol{S}, \quad (19)$$

и может существовать такое преобразование $\boldsymbol{F^{-1}}$, определенное на декартовом произведении $\boldsymbol{S}$, $\boldsymbol{K^1}$, $\boldsymbol{K^2}$, K^3, что:

$$\boldsymbol{F^{-1}}: \boldsymbol{S} \times \boldsymbol{K^1} \times \boldsymbol{K^2} \times \boldsymbol{K^3} \longrightarrow \boldsymbol{M}, \boldsymbol{C}. \quad (20)$$

Функцию $\boldsymbol{F}$, определенную на $\boldsymbol{M} \times \boldsymbol{C} \times \boldsymbol{K^1} \times \boldsymbol{K^2} \times \boldsymbol{K^3}$ со значениями в $\boldsymbol{S}$, будем отождествлять со скрытием сообщения M_i из множества $\boldsymbol{M}$ в контейнер C_j из множества $\boldsymbol{C}$ на основе ключа из множеств $\boldsymbol{K^1}$, $\boldsymbol{K^2}$, $\boldsymbol{K^3}$. Функцию $\boldsymbol{F^{-1}}$, определенную на $\boldsymbol{S} \times \boldsymbol{K^1} \times \boldsymbol{K^2} \times \boldsymbol{K^3}$ со значениями в $\boldsymbol{M}$, будем отождествлять с извлечением тайного сообщения $M_i \in \boldsymbol{M}$ из стегосообщения $S_q \in \boldsymbol{S}$. Таким образом, каждый ключ K_i представляет собой набор из трех уровней ключевой информации:

$$K_i = \{K^1_m, K^2_j, K^3_l\}, \quad (21)$$

где

K^1_m – ключ первого уровня, $m \in [1, P^1_i]$; (22)

K^2_j – ключ второго уровня, $j \in [1, P^2_i]$; (23)

K^3_l – ключ третьего уровня, $l \in [1, P^3_i]$; (24)

Значения P^1_i, P^2_i и P^3_i определяют количество ключей соответствующего уровня для элемента C_k множества $\boldsymbol{C}$.

Определение 5

Стегонабором называется элемент K_i множества ключа $\boldsymbol{K}$.

Определение 6

Стегонабор K_i *доступен* для контейнера C_j из множества $\boldsymbol{C}$, если существует преобразование $\boldsymbol{F}$, позволяющее скрыть сообщение M_k в контейнере C_j с использованием стегонабора K_i.

Определение 7

Стегонаборы $\{K^1_i, K^2_i, K^3_i\}$ и $\{K^1_j, K^2_i, K^3_j\}$ называются *пересекающимися*, если $\exists \alpha$, такое что $K^{\alpha}_i = K^{\alpha}_j$.

Стегонаборы могут пересекаться на одном уровне или на нескольких. Если стегонаборы пересекаются на трех уровнях, то они совпадают. Представление ключевой информации в виде стегонабора позволит в дальнейшем описать взаимодействие участников стеганографической системы.

Дадим формальное описание *компонента контейнера стеганографической системы*. Пусть $\boldsymbol{C}$ – это множество всех контейнеров, как определено в (2), а $C_j \in \boldsymbol{C}$, $j = [1, P_C]$.

Определение 8

Компонентом стеганографического контейнера C_j назовем такое $\boldsymbol{C_{ij}}$, $\boldsymbol{C_{ij}} \in \boldsymbol{C_j}$, $i = [1, N_j]$, что для набора $\{\boldsymbol{C_{ij}}, \boldsymbol{M}, \boldsymbol{S}\}$, где $\boldsymbol{M}$ определено в (3), $\boldsymbol{S}$ определено в (4), существует стегонабор $\{\boldsymbol{K^1_i}, \boldsymbol{K^2_i}, \boldsymbol{K^3_i}\}$, где $\boldsymbol{K^1_i}$ – ключ первого уровня, $\boldsymbol{K^2_i}$ – ключ второго уровня, $\boldsymbol{K^3_i}$ – ключ третьего уровня, и существует функция прямого стеганографического преобразования $\boldsymbol{F_i}$, такая что:

$$\boldsymbol{F_i}: \boldsymbol{M} \times \boldsymbol{C_{ij}} \times \boldsymbol{K^1_i} \times \boldsymbol{K^2_i} \times \boldsymbol{K^3_i} \longrightarrow \boldsymbol{S}, \quad (25)$$

и может существовать функция обратного $\boldsymbol{F^{-1}_i}$ стеганографического преобразования, такая что:

$$\boldsymbol{F^{-1}_i}: \boldsymbol{S} \times \boldsymbol{K^1_i} \times \boldsymbol{K^2_i} \times \boldsymbol{K^3_i} \longrightarrow \boldsymbol{M}, \boldsymbol{C_{ij}}. \quad (26)$$

В математической модели, принятой за основу, сообщение $\boldsymbol{C_j}$ множества сообщений $\boldsymbol{C}$ рассматривается как единичный контейнер, в который можно внедрить скрытую информацию, и к этому контейнеру применяется стеганографическое преобразование. Однако элемент $\boldsymbol{C_j}$ зачастую не является неделимым. В большинстве контейнеров мы можем выделить различные области, внедрение скрытого сообщения в которые может проводиться по различным алгоритмам. Если мы рассмотрим, например, в качестве контейнера электронный документ в формате DOCX, то в качестве компонентов контейнера могут быть выделены: текст электронного документа; описание

электронного документа в формате XML; история редактирования электронного до-кумента; стилевые, цветовые, размерные и прочие параметры оформления документа и др. Если мы рассмотрим в качестве контейнера электронные карты в формате SHP, то в каче-стве компонентов стеганографического контейнера могут быть выделены отдельные про-странственные области или наборы пространственных областей. Для векторных изображе-ний элементами могут являться отдельные фигуры, линии и их наборы. Можно отметить, что содержимое компонентов стегоконтейнера может пересекаться.

Исходя из требований, выдвигаемых к стегосистемам, необходимо реализовать вариативность стеганографической системы в зависимости от условий ее применения. Выделение компонентов контейнера может быть проведено различными способами. Пусть $\boldsymbol{G_j}$ – набор функций, реализующих *выделение компонентов контейнера* $\boldsymbol{C_j}$, причем

$$\boldsymbol{G_j}: \boldsymbol{C_j} \longrightarrow \{\boldsymbol{C_{j1}}, \boldsymbol{C_{j2}}, \ldots, \boldsymbol{C_{jNj}}\}, \qquad (27)$$

где N_j – количество компонентов в контейнере $\boldsymbol{C_j}$ при разбиении $\boldsymbol{G_j}$.

Для каждого компонента стегоконтейнера $\boldsymbol{C_j}$ могут существовать стегонаборы $\{\boldsymbol{K^1_{ij}}, \boldsymbol{K^2_{ij}}, \boldsymbol{K^3_{ij}}\}$, $i = [1, N_j]$, где N_j – количество компонентов в контейнере $\boldsymbol{C_j}$. Например, если в качестве множества стегоконтейнеров $\boldsymbol{C}$ выбраны электронные документы в формате DOCX, то в некотором электронном документе в формате DOCX могут быть выделены только два компонента: размерные параметры оформления документа и текст электронного документа. Для компонента, представляющего собой размерные параметры оформления документа, может применяться стегонабор {метод *Word-shift coding*, метод изменения кернинга, пары AV и LW}, а для текста электронного документа может быть применен стегонабор {метод *Word-shift coding*, метод замены символов символами другого алфавита, замена символов **A**, **B** и **K**}. Эти стегонаборы пересекаются на первом уровне. Таким образом, для дальнейшего моделирования отметим, что единичный стегоконтейнер C_j из множества $\boldsymbol{C}$ представлен в виде набора компонентов $\boldsymbol{C_{ij}}$, $i = [1, N_j]$, для каждого из которых может быть определено стегонабор $\{\boldsymbol{K^1_{ij}}, \boldsymbol{K^2_{ij}}, \boldsymbol{K^3_{ij}}\}$, причем стегонаборы из разных множеств могут пересекаться частично или полностью.

Дадим формальное описание *блока сообщения стеганографической системы*. Пусть $\boldsymbol{M}$ определено в (1), а $M_i \in M$, $i = [1, N]$. Будем предполагать далее, что сообщение M_i может быть представлено в виде битовой последовательности.

Определение 9

Блоком M_{ik} скрытого сообщения M_i, $k = [1, N_{Mi}]$, назовем такую часть сообщения M_i, которая может быть скрыта в компоненте C_{jl}, $l = [1, N_{Cj}]$, с использованием стегонабора K_{qjl}, $q = [1, N_{Cjl}]$, где:
N_{Mi} – количество блоков сообщения M_i;
N_{Cj} – количество компонентов стеганографического контейнера C_j, $j = [1, N_C]$;
N_C – количество контейнеров в $\boldsymbol{C}$;
N_{Cjl} – количество стегонаборов, доступных для компонента C_{jl}.

Сообщение может быть разбито на блоки различными способами. Блок должен быть выделен таким образом, чтобы иметь возможность быть скрытым в одном из компонентов. Однако могут существовать как «пустые» компоненты, в которые не внедряется какой-либо блок, так и «большие» компоненты, вмещающие несколько блоков. Таким образом, разбиение сообщения на блоки зависит от компонентов контейнера, используемых для скрытия сообщения, и исходного сообщения. Пусть $\boldsymbol{H_i}$ – преобразование разбиения сообщения M_i на блоки:

$$\boldsymbol{H_i}: M_i \times C_j \longrightarrow \{M_{1i}, M_{2i}, \ldots, M_{jNi}\}, \quad (28)$$

Таким образом, определение стеганографической системы $\boldsymbol{SF}$ из (7) может быть переписано следующим образом:

$$\boldsymbol{SF} = (\boldsymbol{C'}, \boldsymbol{M'}, \boldsymbol{K'}, \boldsymbol{F}, \boldsymbol{F^{-1}}, \boldsymbol{G}, \boldsymbol{H}), \qquad (29)$$

где $\boldsymbol{C'}$ – множество компонентов стегоконтейнеров, определяемых преобразованием $\boldsymbol{G}$, реализующим выделение компонентов контейнера; $\boldsymbol{M'}$ – множество сообщений,

состоящих из блоков, определяемых преобразованием ***H***, реализующим разбиение сообщения на блоки; ***K'*** – множество стегонаборов.

При построении стеганографической системы требуется обеспечить стойкость к обнаружению и модификации скрытой информации, для чего воспользуемся *контрольным числом*.

Определение 10

Контрольным числом скрытого сообщения M_i называется значение, рассчитанное путем применения определенного алгоритма Z и используемое для проверки целостности сообщения M_i. В качестве такого алгоритма могут использоваться как различные алгоритмы хэширования, так и алгоритмы вычисления контрольной суммы.

Пусть V_i – функция вычисления контрольного значения сообщения M_i: (30)

$$h_i = V_i (M_i, Z_i).$$

Можем рассматривать h_i как еще один блок сообщения M_i. Для скрытия этого блока следует выделить компонент контейнера и стегонабор. Таким образом, определение стеганографической системы ***SF*** из (28) может быть записано следующим образом: (31)

$$\boldsymbol{SF} = (\boldsymbol{C'}, \boldsymbol{M'}, \boldsymbol{K'}, \boldsymbol{F}, \boldsymbol{F^{-1}}, \boldsymbol{G}, \boldsymbol{H}, \boldsymbol{Z}),$$

где ***C'*** – множество компонентов стегоконтейнеров, определяемых преобразованием ***G***, реализующим выделение компонентов контейнера; ***M'*** – множество сообщений, состоящих из блоков, определяемых преобразованием ***H***, реализующим разбиение сообщения на блоки; ***K'*** – множество стегонаборов, ***Z*** – набор алгоритмов для вычисления контрольных чисел.

Заключение

Полученная математическая модель стеганографической системы позволяет обеспечить контроль целостности внедряемых скрытых сообщений. Опишем некоторые схемы ее практического использования.

1) Контейнер C разделяется на два компонента C_1 и C_2; сообщение M воспринимается как единый блок и скрывается при помощи стегонабора K_1 в компоненте C_1; контрольное число h, вычисленное как значение хэш-функции ***Z***, скрывается при помощи стегонабора K_2 в компоненте C_2. Таким образом, при извлечении сообщения M и контрольного числа h, возможно повторное вычисление хэш-функции и проверка целостности сообщения, что было реализовано в [7].

2) Сообщение M разделяется на блоки M_i, а контейнер C – на подходящее число компонентов C_i, для каждого из которых выбирается стегонабор K_i. Для каждого блока M_i вычисляется контрольное число h_i. Контрольное число h_{i-1} добавляется к следующему блоку M_i и скрывается в следующем компоненте C_i по принципу блокчейн. В результате формируется контейнер S, содержащий скрытую информацию и отдельно пользователю предоставляется последнее контрольное значение h_n. Извлечение происходит, начиная с последнего компонента, целостность сообщения проверяется последовательно по блокам, как описано в [8].

ЛИТЕРАТУРА

1. **Урбанович П. П.** Защита информации методами криптографии, стеганографии и обфускации. – Минск: БГТУ, 2016. 220 с.

2. **21 Cachin C.** An Information-Theoretic Model for Steganography, Information and Computation, Proc. 2nd International Workshop on Information Hiding, 1998, LNCS, v.1525, pp. 306-318.

3. **Конахович, Г. В.** Компьютерная стеганография. Теория и практика / Г. В. Конахович, А. Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.

4. **Шутько Н.П.** МОДЕЛИРОВАНИЕ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ В ЗАДАЧАХ ПО ОХРАНЕ АВТОРСКИХ ПРАВ // Н.П. Шутько, Н.И. Листопад, П.П. Урбанович / Восьмая Международная научно-техническая конференция «Информационные технологии в промышленности» (ITI-2015) : тезисы докладов (2-3 апреля 2015 года, Минск). - Минск : ОИПИ НАН Беларуси, 2015. – 128 с. - ISBN 978-985-6744-87-0.

5. **Чернявский, А.Ф.** Оценка информационных потерь при фильтрации изображений/ А.Ф. Чернявский, И.Л. Чваркова, В.С. Садов. Информатика, № 2, 2008. – с. 119-128.

6. **Pavel Urbanovich, Nadzeya Shutko** Theoretical Model of a Multi-Key Steganography System // Recent De-

velopments in Mathematics and Informatics.Contemporary Mathematics and Computer Science. Part II Computer Science/ Wydawnictwo KUL, 2016. – стр. 181-202.

7. **Блинова, Е.А.** Применение нескольких стеганографических методов для осаждения скрытых данных в электронных текстовых документах // Блинова Е.А., Сущеня А.А. «Системный анализ и прикладная информатика», №2. Минск, БНТУ. – 2019. – стр. 32-38 .

8. **Блинова, Е.А.** Приложение для нанесения стеганографического водяного знака на электронную карту / Блинова Е.А., Сташевская И.Ю. // Материалы докладов VIII МНТК «Информационные технологии в образовании, науке и производстве», 20-22 ноября 2021 года, Международный институт дистанционного образования Белорусского национального технического университета. Минск, МИДО БНТУ. – 2021. – стр. 193-198.

REFERENCES

1. **Urbanovich P. P.** *Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii* [The protection of information based on the methods by cryptography steganography and obfuscation]. Minsk. BGTU Publ., 2017. 220 p.

2. **Cachin C.** An Information-Theoretic Model for Steganography, Information and Computation, Proc. 2nd International Workshop on Information Hiding, 1998, LNCS, v.1525, pp. 306-318.

3. **Konahovich G.V.** *Komputernaya steganografia. Teoria i praktika* [Computer steganography. Theory and practice] G.V. Konahovich, A. U. Puzyrenko. K.: MK-Press, 2006. 288 p.

4. **Shutko N.P.** *Modelirovanie steganographicheskoy systemy v zadachah po ohrane avtorskih prav* [The modeling of the steganographic system in copyright tasks]. N. P. Shutko, N. I. Listopad, P. P. Urbanovich, 8th International scientific and technical conference “Information technologies in industry”(ITI-2015) (2-3 April 2015), Minsk. UIIP NAS of Belarus Publ., 2015. 128 p. ISBN 978-985-6744-87-0.

5. **Chernyavsky A.F.** *Ocenka informacionnyh poter pri filtracii izobrazheniy* [Estimation of Information Losses in Image Filtering] A. F. Chernyavsky, I. L. Chvarkova, V.S. Sadov. Minsk. BSU Publ. Informatics, № 2, 2008. 119-128 pp.

6. **Pavel Urbanovich, Nadzeya Shutko** Theoretical Model of a Multi-Key Steganography System // Recent Developments in Mathematics and Informatics.Contemporary Mathematics and Computer Science. Part II Computer Science/ Wydawnictwo KUL, 2016, pp. 181-202.

7. **Blinova E.A., Sushchenia A.A.** Several steganographic methods using for embedding of hidden data in electronic text documents. «System analysis and applied information science». 2019;(2):32-38. (In Russ.) https://doi.org/10.21122/2309-4923-2019-2-32-38

8. **Blinova E.A.** Prilozhenie dlya naneseniya steganograficheskogo vodyanogo znaka na elektronnuyu kartu [An application for applying a steganographic watermark to an electronic card] / Blinova E.A., Stashevskaya I.U. // Proc. 8th International scientific and technical conference “Information technologies in education, science and industry” (20-22 November 2021), Minsk. MIDO BNTU Publ., 2021. pp. 193-198.

E. A. BLINOVA

MATHEMATICAL MODEL OF A STEGANOGRAPHIC SYSTEM BASED ON KEY INFORMATION IN THE FORM OF STEGOSETS

Belarusian State Technological University

A formal description of the mathematical model of a steganographic system based on key information in the form of stegosets is given. The mathematical model of the steganographic system is intended both for placing hidden marks to control the integrity of documents acting as a container, and for covert data transmission. Exist-ing mathematical models do not fully meet the requirements for steganographic systems. The proposed model is based on the concepts of a three-level key, a stegoset, a container component, and a message block. The three-level key is a set of actual steganographic transformations depending on the type of container. A stegoset is an element of a key set. A component of a container is such a subset of it that there is a stegoset for it. A message block is such a sequential part of the message that there is a container component for it, in which it can be hidden using the appropriate stegoset. The model implements the application of different stegosets to different container compo-nents, and the message can be divided into blocks. The model allows controlling the integrity of the message and adapts to different types of containers. Possible options for the practical application of the mathematical model are proposed, such as monitoring the integrity of the message when calculating the control number, splitting the message into blocks and sequentially monitoring their integrity by analogy with the blockchain system.

Keywords: *steganography; copyright; mathematical model.*

Блинова Евгения Александровна, старший преподаватель кафедры ИСИТ Белорусского государственного технологического университета. Научные интересы: стеганография, базы данных, обработка данных.
Evgenia Blinova, senior teacher at Information systems and technolo-gies Department at Belorussian State Technological University. Scientific interests: Ste-ganography, Database Administration, Programming and Security.

Email: eugenia.blinova@gmail.com