5. Лаврентьев М. А. Методы теории функций комплексного переменного / М. А. Лаврентьев, Б. В. Шабат. — М. : Наука, 1987. — 688 с.
6. Курош А. Г. Курс высшей алгебры / А. Г. Курош. — М. : Физматгиз, 1963. — 431 с.
7. Степанов В. В. Курс дифференциальных уравнений / В. В. Степанов. — М. : Физматгиз, 1959. — 468 с.
8. Шилов Г. Е. Математический анализ. Второй специальный курс / Г. Е. Шилов. — М. : Наука, 1965. — 328 с.

By an operating method it is get the integral presentation of exact analytical solution of algorithmic character of problem about diffusion processes in non-homogeneous environments with soft bounds in the case of the modeling of diffusion processes is realized by the method of hybrid differential Legendres-Fourier-Legendres operator.

Key words: *hybrid differential operator, fundamental system of solution, Cauchy functions, Green functions, influence functions, boundary-value problem.*

Отримано: 16.09.2010

УДК 004.415.24

А. М. Кудин, канд. техн. наук
Институт кибернетики им. В. М. Глушкова НАН Украины, г. Киев

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ НА БАЗЕ ОБЩЕЙ ТЕОРИИ ОПТИМАЛЬНЫХ АЛГОРИТМОВ

Статья посвящена исследованию проблемы построения математической модели для оценки стойкости стеганографических систем, адекватной практическим приложениям. В отличии от существующих, предложенная модель не предполагает априорное знание распределения контейнеров или существование совершенного оракула.

Ключевые слова: *стеганография, стойкость стеганографических систем, общая теория оптимальных алгоритмов, радиус иформации.*

Введение. Широкое использование методов компьютерной стеганографии в современных системах защиты информации определяет актуальность задачи построения формальных методов анализа стойкости стеганографических систем к различным атакам. При этом желательно получить с одной стороны как можно более общие модели, с другой — хорошо применимые в практических ситуациях.

В общем случае неформальное описание универсальной стеганографической системы выглядит так:

- выбирается избыточная характеристика информационной системы, изменение которой не сказывается на функциональности системы (заметим, что выбор «избыточности» существенно зависит от модели нарушителя);
- определяется метод извлечения избыточной информации, избыточная информация и является контейнером;
- определяется алгоритм модификации или выбора избыточной информации для формирования скрытого сообщения.

При выборе алгоритма модификации избыточной информации существенными являются цель, с которой формируется скрытое сообщение и модель нарушителя. Варьируя эти два параметра, можно получить все существующие разновидности стеганографических систем [1]. Естественно, что и определение стойкости будет существенно зависеть и от цели, и от модели нарушителя. С другой стороны, одной из двух базовых, отправных точек для всех стеганографичсеких систем является скрытие факта наличия в контейнере скрытого сообщения и модель пассивного нарушителя. Будем называть стеганографическую систему, предназначенную для решения такой задачи «классической стеганографической системой».

Утверждение важности решения задачи скрытие факта наличия в контейнере скрытого сообщения в модели пассивного нарушителя *для всех стеганографических систем* требует некоторого пояснения в случае видимых цифровых водяных знаков и цифровых идентификаторов (fingerprints). Неформально, в случае цифровых водяных знаков решается задача обеспечения целостности скрытого сообщения, тогда как в классической стегосистеме — конфиденциальности скрытого сообщения, а в случае цифровых идентификаторов необходимо обеспечение и конфиденциальности и целостности. Тогда для построения стойких систем цифровых водяных знаков и цифровых идентификаторов нам необходимо решить задачу построения классической стеганосистемы и определить класс преобразований, которые являются инвариантными относительно выбранной нами избыточной информации.

В силу изложенного выше, в дальнейшем рассматривается решение только одной задачи — построение адекватной на практике модели оценки стойкости классической стегосистемы.

Анализ известных моделей оценки стойкости стеганографических систем. В настоящее время существует два подхода к построению метрик стойкости стеганографических систем. Первый, основой которого служит работа Качина [2], в качестве меры стойкости использует одну из вероятностных мер математической статистики — относительную энтропию. При этом стеганосистема представляется как

суперпозиция случайных величин (C,S,M,K,Q,P_C,P_S) соответственно контейнеров, стего, открытых сообщений, ключей, сообщений, наблюдаемых нарушителем, распределений контейнеров и стего. Относительная энтропия или разрешающая способность определяется как $D(P_C \| P_S) = \sum_{q\in Q} P_C(q)\log\frac{P_C(q)}{P_S(q)}$. Совершенно стойкая стеганосистема соответствует равенству $D(P_C \| P_S) = 0$, которое выполняется тогда и только тогда, когда распределения контейнеров и стего совпадают. Недостатком данного подхода является то, что введенная мера предполагает априорное знание распределения контейнеров, что редко встречается на практике. Кроме того, относительная энтропия не является метрикой: для нее не выполнено условие симметричности и неравенство треугольника.

Более адекватная модель с информационно-вероятностной мерой стойкости предложена в работе [3]. В ней стегосистема рассматривается как обобщение криптосистемы. По аналогии с теорией стойкости криптосистем Шеннона показателем стойкости считается взаимная информация $I(M;(S,C)) = H(M) - H(M \mid (S,C))$. В совершенно стойкой системе эта информация равна нулю, значит $H(M) = H(M \mid (S,C))$. Из последнего равенства ясно, что M является независимым от S,C. Для совершенно стойкой стегосистемы выполняется равенство $H(S \mid C) = H(C \mid S)$. Далее или $H(S \mid C) = H(C \mid S) = 0$ (C и S совпадают) или $H(S \mid C) = H(C \mid S) > 0$. Но последнее неравенство может выполняться только в случае $H(M) \neq H(M \mid (S,C))$, так как $S = f(C,M)$. Отсюда следует, что необходимым и достаточным условием совершенной стойкости стегосистемы является равенство $H(S \mid C) = H(C \mid S) = 0$. С другой стороны, последнее равенство означает нестойкость (в теоретико-информационном смысле) стегосистемы в случае точного знания противником пустого контейнера (эталона). Учитывая, что существуют два различных подхода к работе с контейнерами: селективный (потоковые контейнеры) и модификации (контейнеры с произвольным доступом), получаем следующее утверждение: «совершенно стойкие в теоретико-информационном смысле стегоситемы существуют только в рамках селективного метода». При этом из множества всех контейнеров случайно и равновероятно выбирается подмножество $C_r \subseteq C$, такое что выполнялось $H(C) \geq H(C_r)$ и $H(C_r \mid C) > 0$. При таком подходе условиями совершенной стойкости стегосистемы явля-

ются: $H\left(M\mid\left(S,C\right)\right)=H\left(M\mid S\right)=H\left(M\right)$ и $H\left(K\mid\left(S,C\right)\right)\geq H\left(M\right)$. Из последнего неравенства следует $H\left(K\right)\geq H\left(K\mid\left(S,C\right)\right)\geq H\left(M\right)$, откуда следует, что граница неопределенности ключа для совершенной стегосистемы по крайней мере не лучше, чем для совершенной криптосистемы. При некоторых практических допущениях можно показать, что для совершенной стегосистемы длина ключа $\left|K\right|$ (при совпадении алфавитов ключа и открытых сообщений, равномерном распределении ключа) и длина открытого (встраиваемого) сообщения $\left|L\right|$ связаны неравенством $\left|K\right|\geq c\left|L\right|$, где $c>1$. Таким образом в информационно-вероятностной модели, совершенная стегосистема менее эффективна, чем совершенно стойкая криптосистема. В работе [1] отмечаются некоторые из недостатков информационно-вероятностных моделей, однако часть из приведенных недостатков зависит друг от друга. Поэтому общими недостатками информационно-вероятностных моделей, рассмотренных выше, можно считать:

- для произвольной совершенно стойкой стегосистемы доказывается лишь факт ее существования, но не учитывается возможность и сложность решения задачи ее построения;
- для произвольной совершенно стойкой стегосистемы не рассматривается вычислительная сложность алгоритма встраивания сообщений;
- не учитываются вычислительные ресурсы нарушителя.

Первый недостаток означает, что задача построения совершенной стойкой стегосистемы может быть практически неосуществима, более того в работе [2] показано, что в общем случае эта задача эквивалентна NP-полной задаче разбиения. Практическая невозможность построения стегосистемы может также определяться неизвестностью на практике распределения контейнеров или невозможностью выбора реальных контейнеров с требуемыми в моделях характеристиками.

Второй недостаток приводит к тому, что может не существовать эффективного алгоритма встраивания (или извлечения) сообщений в контейнеры, поэтому стегосистема будет практически неэффективна.

Третий недостаток приводит к тому, что для оценки стойкости используются верхние границы оценки стойкости, что также существенно ограничивает практическое применение стегосистем.

Дальнейшие исследования моделей стегосистем и их стойкости были продолжены в рамках подхода теории сложности вычислений [4; 5]. Стегосистема в рамках данного подхода представляет собой пару вероятностных алгоритмов $\left(S_E,S_D\right)$ встраивания и извлечения сообщений. Алгоритм S_E использует для работы: ключ $K\in\left\{0,1\right\}^k$,

встраиваемое сообщение $m \in \{0,1\}^l$, историю предыдущих сообщений в канале связи h, дискретный канал с памятью на h сообщений C_h^b и оракул $M(h)$, который возвращает следующий блок b сообщения в соответствии с распределением канала C_h^b. Алгоритм извлечения скрытых сообщений S_D использует для своей работы результат работы алгоритма S_E, ключ $K \in \{0,1\}^k$, историю предыдущих сообщений в канале связи h, оракул $M(h)$ и возвращает скрытое сообщение $m \in \{0,1\}^l$.

Заметим, что, в общем случае, алгоритм S_D является вероятностным, но вероятность успеха можно обеспечить сколь угодно близкой к 1.

Стойкость в такой модели определяется подобно определению семантической стойкости [6] криптосистем, а именно с помощью величины «выигрыша противника», определяемой на основании знания выбранного скрываемого сообщения $m \in \{0,1\}^l$, следующим образом

$$Adv_{S,C}(W) = \left| \underset{K,R,M,S_E}{P}\left(W_R^{M,SE(K,*,*)} = 1\right) - \underset{R,M,O}{P}\left(W_R^{M,O(*,*)} = 1\right) \right|, \qquad \text{где}$$

$W_R^{M,SE(K,*,*)}$ — игра противника при известном ключе, $W_R^{M,O(*,*)}$ — игра противника при неизвестном ключе, $O(*,*)$ определен на множестве всех $m \in \{0,1\}^l$ как оракул $O(m,h) \leftarrow C_h^{|S_E(K,M,h)|}$.

Важный теоретический результат, полученный в рамках этой модели — доказательство эквивалентности существования стойких в этой модели стеганосистем и однонаправленных функций.

Главным недостатком данного подхода является предположение о существовании оракула $M(h)$, эффективной реализации которого может не существовать на практике. Заметим, что оракул используется не только при построении алгоритма встраивания скрытого сообщения, но и для оценки стойкости стеганографической системы.

Модель стойкости на основании общей теории оптимальных алгоритмов. Отмеченные выше недостатки существующих теоретико-информационных и теоретико-сложностных моделей стойкости стеганографических систем определяют важность решения задачи построения критерия, который связывает информацию о первоначальном, неизмененном контейнере и информацию об измененном контейнере с одной стороны, и учитывает реальные особенности противника относительно стеганоанализа, с другой. Представим стеганосистему как совокупность множеств (C,S,M,K,Q) соответственно

контейнеров, стего, открытых сообщений, ключей, сообщений, наблюдаемых нарушителем. Для встраивания сообщения используется оператор $E: C \times M \times K \to N(C) = Q$. Этот оператор можно также рассматривать в виде $E_{K \times M}: C \to N(C)$, где $M \times K$ — составной ключ. Тогда стеганосистема может рассматриваться как криптосистема с составным ключом, оператор $Dt: C \times \Re_+ \to 2^M$, где $\Re_+ = [0, \infty)$ — оператор стеганоанализа, а φ-алгоритм реализации оператора стеганоанализа. Построение модели осуществляется аналогично построению модели криптосистемы, рассмотренной автором в работах [7; 8]. Пусть оператор стеганоанализа обладает двумя свойствами:

$$Dt(c, 0) \neq \varnothing, \forall c \in C, \tag{1}$$

$$\delta_1 \leq \delta_2 \Rightarrow Dt(c, \delta_1) \subset Dt(c, \delta_2), \ \forall \delta_1, \delta_2 \in \Re_+, c \in C \tag{2}$$

Для заданного значения $\varepsilon \geq 0$ элемент $c \in C$, удовлетворяющий условию $c \in Dt(c, \varepsilon)$ называется ε-приближением. Задача поиска ε-приближения решается при отсутствии полной (и, в общем случае точной) информации об элементе *c*, о котором известна некоторая информация $N(c) = q \in Q$ где $N: C \to Q$ – информационный оператор или информация противника о контейнерах (заполненных и пустых). Зная q необходимо найти ε-приближение к $m \in Dt(c, 0)$ (рис. 1). Поскольку условия (1), (2) выполняются для любого метода стеганографического анализа, то к определенной таким образом модели стегосистемы возможно применить результаты, полученные в рамках общей теории оптимальных алгоритмов и ее развитии, изложенные в работе [9].

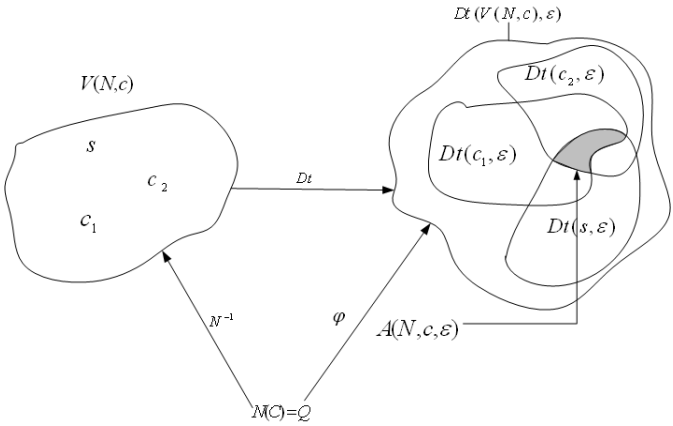

Рис. 1. *Оператор стеганографический и оператор стеганоанализа*

Рассмотрим множество $V(N,c)=\{\tilde{c}\in C: N(\tilde{c})=N(c)\}$ всех элементов $\tilde{c}$ неотличимых с помощью информационного оператора N от c. Если оператор N не есть биекция, то множество $V(N,c)$ не одноточечное. Практически можно считать, что множество $V(N,c)$ является классом эквивалентности на множестве Q, а разбиение контейнеров на классы эквивалентности порождает информационный оператор N, который в данном случае называется неполным оператором. Оператор стеганоанализа, примененный к неполному информационному оператору порождает множество $A(N,c,\varepsilon)=$ $=\bigcap_{\tilde{c}\in V(N,c)} Dt(\tilde{c},\varepsilon)$. Исходя из условия (2) величины $r(N,c)=$ $=\inf\{\delta: A(N,c,\delta)\neq\varnothing\}$ и $r(N)=\sup_{c\in C} r(N,c)$ определяют нижние оценки точности решений, которые могут быть достигнуты при неполном информационном операторе. Пользуясь результатами работы [9] получаем, что на классе идеальных алгоритмов $\Phi(N): Q\to M$, с введенными определениями локальной $e(\varphi,N,c)=\inf\{\delta:\varphi(Q)\in A(N,c,\delta)$ и глобальной $e(\varphi,N)=\sup_{c\in C} e(\varphi,N,c)$ погрешностями, информация Q позволяет найти ε-приближение для произвольного $c\in C$ тогда и только тогда, когда выполняется одно из условий:

$$r(N)<\varepsilon \tag{3}$$

$$r(N)=\varepsilon,\exists\varphi:\varphi(Q)\in Dt(c,e(\varphi,N)),\forall c\in C \tag{4}$$

Проиллюстрируем применение модели для оценки стойкости широко распространенной стеганографической схемы, использующей так называемый метод «наименьшего значащего бита» или LSB метод [1]. Контейнер $\vec{C}$ можно представить как n-мерный вектор над полем $GF(2)$. Можно рассматривать два случая: первый — отклонение контейнеров от некоторых «эталонов», второй — наличие в контейнере скрытого сообщения m, т.е. решение задачи распознавания пустых и заполненных контейнеров. Если рассматривать различие контейнеров между собой, то неравенство $V(N,c)>1$ соответствует определению совершенной стойкости стегосистемы [2]. Из него также сразу следует, что построение совершенно стойкой стегосистемы возможно или при применении селективного метода, или при отсутствии полной информации про «эталонный» незаполненный контейнер (при применении контейнеров произвольного доступа, например метода LSB). В этом случае оператор N должен быть неполным, т.е. $\vec{C}$ должен быть реализа-

цией случайной величины над $GF\left(2^n\right)$, а стойкость не зависит от оператора стеганоанализа. Во втором случае оператор стеганоанализа *Dt* можно рассматривать как критерий распознавания наличия скрытого сообщения в одном из контейнеров. При этом также можно достигать стойкости в теоретико-информационном смысле, но иной, чем совершенной, а именно — теоретико-информационной стойкости по отношению к выбранному критерию распознавания скрытого сообщения. Такая стойкость достигается, если $r\left(N\right)\to\infty$, т.е. множество $Dt\left(V\left(N,c\right),\varepsilon\right)$ распадается на непересекающиеся подмножества при любом ε. Такой случай в методе LSB соответствует встраиванию в контейнеры бессмысленных сообщений или сообщений, зашифрованных совершенно стойким шифром. Для более адекватных моделей можно рассматривать множество алгоритмов реализации оператора стеганоанализа. При этом условие стойкости на разных классах алгоритмов определяется из условий (3), (4).

Список использованной литературы:

1. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
2. Cachin, C. An information-theoretic model for steganography // Information and Computation. — 2004. — № 192 — P. 41—56.
3. Zollner J., Federrath H., Klimant H., P_tzmann A., Piotraschke R., Westfeld A., Wicke G., Wolf G.: Modeling the security of steganographic systems. In Aucsmith, D., ed.: Information Hiding (2nd International Workshop). — Berlin Heidelberg, Springer-Verlag, 1998. — P. 306—318.
4. Hopper N. J., Langford J., Ahn L.v. Provable secure steganography. In Yung, M., ed.: Proc. of CRYPTO. — Berlin Heidelberg, Springer-Verlag, 2002. P. 77—92.
5. Rainer Bohme An Epistemological Approach to Steganography Proceedings of Information Hiding 2009, July 16, 2009. — Springer Verlag, 2009. — P. 1—17.
6. Goldwasser S. Lecture Notes on Cryptography S. Goldwasser, M. Bellare. — Cambridge, Massachusetts, 2001. —283 с.
7. Кудин А.М. Об одном классе криптографических преобразований для модели источников информации Колмогорова / А. М. Кудин. — К. : Інститут кібернетики ім.. В.М. Глушкова НАН України, 2009. — Т. 1. — С. 394—399.
8. Кудин А. М. Криптографические преобразования нешенноновских источников информации / А. М. Кудин // Кибернетика и системный анализ. — 2010. —№ 5. — С.143—149.
9. Трауб Д. Информация, неопределенность, сложность / Д. Трауб, Г. Васильковский, Х. Вожьняковский. — М. : Мир, 1988. — 184 с.

The article is devoted to a problem of building mathematical model of security stegosystem estimating for practical use. The model, as opposed to existing, not requires knowledge of the covertext statistics or exist perfect oracle.

Key words: *steganography, stegosystem security, general theory of optimal algorithms, information radius.*

Отримано 23.09.2010