УДК 681.3:519.72:003.26

В.К. ЗАДИРАКА, А.М. КУДИН

НОВЫЕ МОДЕЛИ И МЕТОДЫ ОПРЕДЕЛЕНИЯ СТОЙКОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. Предложен новый подход к оценке стойкости систем защиты информаци для современных информационно-коммуникационных систем на базе общей теории оптимальных алгоритмов. Показана связь между качеством информации и стойкостью криптографических и стеганографических систем. Обоснован выбор радиуса информации как показателя стойкости для различных систем защиты информации.

Ключевые слова: безопасность информации, криптология, стеганография, общая теория оптимальных алгоритмов, радиус информации.

ВВЕДЕНИЕ. СОВРЕМЕННЫЕ ПРОБЛЕМЫ КРИПТОЛОГИИ И СТЕГАНОГРАФИИ. ПОИСК АДЕКВАТНЫХ МОДЕЛЕЙ ОЦЕНКИ СТОЙКОСТИ

Большинство из существующих результатов прикладной криптографии и стеганографии получено для информационно-коммуникационных систем, не в полной мере соответствующих современным. Повсеместное применение технологий распределенной и децентрализованной обработки информации определяет особенности современных грид, облачных и блокчейн информационно-коммуникационных систем (ИКС). По сравнению с используемыми ранее в этих ИКС имеется ряд существенно отличающихся особенностей процессов обработки информации, а именно: распределенное применение гетерогенных вычислительных ресурсов, гибкое наращивание вычислительных возможностей для пользователей, постоянное повторное использование типовых информационных ресурсов различными потребителями, сокращение функций центров обработки данных (ЦОД) вплоть до их полного отключения (как в блокчейнах), обработка огромных массивов информации (концепция «BigData») и широкое применение концепции «Open Source Software» [1]. Такие особенности обусловливают новые постановки задач защиты информации, среди которых оценка уровня защищенности и построение систем защиты распределенных и децентрализованных ИКС, проектирование и реализация криптографических и стеганографических систем с доказуемой стойкостью.

Несмотря на многочисленные исследования, упомянутые проблемы [2–21] окончательно не решены. Причинами этого являются: отсутствие математических моделей оценки безопасности информации в системах с заранее неизвестными множествами информационных и вычислительных ресурсов; нерешенность проблемы получения нетривиальных нижних оценок стойкости асимметричных криптосистем и стеганосистем вследствие сложности доказательств гипотез существования односторонних функций и односторонних функций с лазейкой; незначительное количество исследований обеспечения защиты криптосистем от атак на реализацию для распределенных систем, в том числе облачных ИКС, и методов эффективной реализации асимметричных криптосистем для распределенных систем.

Таким образом, основными отличиями современных систем, которые оказали наибольшее влияние на изменения постановок задач защиты информации, являются применение технологий распределенной и децентрализованной обработки данных, облачных и грид вычислений, технологий блокчейн и интеллектуальных контрактов, а также методов работы с «большими данными» (BigData) и использование концепции «Open Source Software».

Другой тенденцией развития современных информационных технологий является применение принципов построения информационно-коммуникационных

систем общего назначения для автоматизированных систем управления инфраструктурой (в том числе критической) и технологических процессов реального мира — «Интернет вещей» [22]. В результате снижается стоимость систем управления (в том числе стоимость эксплуатации систем), повышается их интеллектуальность, расширяется круг потенциальных уязвимостей, угроз и нарушителей. Последнее происходит в основном вследствие двух причин: унификации технологий обработки информации в системах и повышения адаптивности киберсистем. Примерами упомянутых тенденций являются инциденты со злонамеренным кодом BlackEnergy и атаками на сеть SWIFT [22].

Таким образом, описанные тенденции обусловливают переход от информационно-коммуникационного к киберпространству. В последнем в отличие от информационно-коммуникационного пространства формируются и передаются сигналы управления, способные придать данной области киберпространства некий «интеллектуальный» характер поведения и устойчивость к угрозам. Архитектура киберпространства изменяется во времени, так же как ценность информации и угрозы. Исходя из этого, традиционные подходы к оценке показателей безопасности информации киберпространства, которые рассматривают его как совокупность ИКС традиционной архитектуры [23], недопустимы. Изменение информационной среды обусловливает и изменение стратегии и тактики проведения атак на информационные ресурсы. Современные «интеллектуальные» атаки (APT-атаки) в киберпространстве могут осуществляться длительное время, имея «латентный» период, который очень сложно обнаружить, а подготовка к проведению APT-атаки включает как технические методы, так и методы социальной инженерии.

Известно, что методы атаки и защиты информации должны быть адекватными. Поэтому необходимо, чтобы киберпространство имело центры, постоянно управляющие его адаптацией к угрозам (сейчас такую функцию выполняют CSIRT — группы реагирования на киберинциденты). Единственным методом построения системы защиты киберпространства является передача управления ею непосредственно системе защиты, т.е. построение интеллектуальной системы автоматизированного управления защитой информации, центральное место в которой занимают системы поддержки принятия решений (СППР). В работе [12] показано, что формальные постановки задач оценки безопасности информации в киберпространстве и технической исправности объекта диагностирования совпадают. Однако проблемой применения известных методов технической диагностики является сложность введения метрики на пространстве диагностических признаков для задачи оценки безопасности информации. В этом случае предпочтительнее методы, связывающие показатели безопасности информации с качеством информации для работы СППР и сложностью алгоритма ее работы.

Еще одной тенденцией развития ИКС является появление новых моделей вычислений и их практической реализации — квантовые вычисления и квантовая криптография. Перспективы создания квантового компьютера [24] определяют актуальность исследований построения практических криптосистем с теоретико-информационной стойкостью. Другим важным направлением является построение и поиск односторонних преобразований в квантовой модели вычислений (так называемых «постквантовых» криптосистем). Таким образом, актуально исследование методов анализа и синтеза криптосистем, позволяющих с единой точки зрения оценивать качество и полноту информации для алгоритма криптоанализа и его сложность.

Очевидно, что для решения различных задач оценки стойкости систем защиты информации необходимо применять модели и методы, с помощью которых в рамках единой модели можно оценивать сложность алгоритма и качество информации, необходимой для его работы. Такую возможность дают методы общей теории оптимальных алгоритмов [25, 26], рассмотренные далее.

ОБЩАЯ ТЕОРИЯ ОПТИМАЛЬНЫХ АЛГОРИТМОВ В ЗАДАЧАХ ОЦЕНКИ СТОЙКОСТИ КРИПТО- И СТЕГАНОСИСТЕМ

Представим операторную модель вычислений [26] в виде, удобном для описания криптосистем и стеганосистем. Введем следующие обозначения. Пусть заданы множества X, Y, а 2^Y — класс всех подмножеств множества Y. В работе [26] рассматривается оператор $S: X \times R_+ \to 2^Y$, где $R_+ = [0, \infty)$, называемый оператором решения и имеющий два свойства:

$$S(x, 0) \neq \varnothing \quad \forall x \in X,$$

$$\delta_1 \le \delta_2 \Rightarrow S(x, \delta_1) \subset S(x, \delta_2) \quad \forall \delta_1, \delta_2 \in R_+, \ x \in X.$$

Для заданного $\varepsilon \ge 0$ элемент $y \in Y$, удовлетворяющий условию $y \in S(x, \varepsilon)$, называется ε-приближением. Задача поиска ε-приближения решается в случае отсутствия полной (и в общем случае точной) информации об элементе x, о котором имеется некоторая информация $N(x)$, где $N: X \to Y$ — информационный оператор в терминологии общей теории оптимальных алгоритмов (ОТОА), а Y — образ множества X. Зная $N(x)$, необходимо найти ε-приближение к x (рис. 1).

Если множество $V(N, x) = \{\widetilde{x} \in X : N(\widetilde{x}) = N(x)\}$ всех элементов $\widetilde{x}$, неотличимых с помощью информационного оператора N от x, одноточечно, то оператор N устанавливает взаимно-однозначное соответствие между множествами X, Y и называется полным (в противном случае — неполным). Оператор решения, примененный к неполному информационному оператору, порождает множество $A(N, f, \varepsilon) = \bigcap_{\widetilde{x} \in V(N, x)} S(\widetilde{x}, \varepsilon)$, при этом для $\delta_1 \le \delta_2 \Rightarrow A(N, x, \delta_1) \subset A(N, x, \delta_2)$.

Тогда величины $r(N, x) = \inf\{\delta : A(N, x, \delta) \neq \varnothing\}$ и $r(N) = \sup_{x \in X} r(N, x)$ ($r(N, x) = \inf\{\delta : A(N, x, \delta) \neq \varnothing \ \forall x \in X\}$) определяют нижние оценки точности решений, которые можно достичь при неполном информационном операторе. В работе [26] доказано, что в классе идеальных алгоритмов $\Phi(N): N(x) \to G$ с введенными определениями локальной $e(\varphi, N, x) = \inf\{\delta : \varphi(N(x)) \in A(N, x, \delta)\}$ и глобальной $e(\varphi, N) = \sup_{x \in X} \varepsilon(\varphi, N, x)$ погрешностей информация $N(x)$ позволяет найти ε-приближение для произвольного $x \in X$ тогда и только тогда, когда выполняется одно из условий:

$$r(N) < \varepsilon,$$

$$r(N) = \varepsilon, \ \exists \varphi : \varphi(N(x)) \in S(x, e(\varphi, N)) \quad \forall x \in X.$$

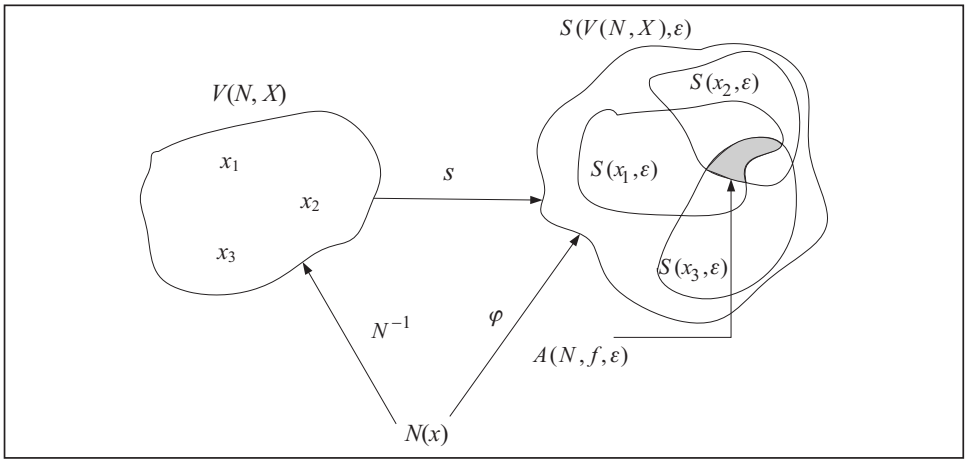

Рис. 1. Информационный оператор и оператор решения

В случае приближенной информации N_ρ (ρ — мера погрешности) результаты для нижних оценок определяются аналогично

$$r(N_\rho) < \varepsilon,$$

$$r(N_\rho) = \varepsilon,\ \exists \varphi : \varphi(N_\rho(x)) \in S(x, e(\varphi, N_\rho))\ \ \forall x \in X.$$

Оператор N_ρ в отличие от точного информационного оператора определяется через оператор информационной ошибки $E : H \times R_+ \to 2^H$, имеющий два свойства:

$$E(h, 0) = \{h\}\ \ \forall h \in H,$$

$$\delta_1 \le \delta_2 \Rightarrow E(h, \delta_1) \subset E(h, \delta_2)\ \ \forall \delta_1, \delta_2 \in R_+,\ h \in H.$$

Приближенный оператор $N_\rho : X \to H$ удовлетворяет условию

$$N_\rho(x) \in E(N(x), \rho)\ \ \forall x \in X.$$

Заметим, что если точный информационный оператор N неполон, то N_ρ тоже неполон, и если N полон, то N_ρ может оказаться как полным, так и неполным. Если оператор N_ρ полон, то $r(N_\rho) = 0$.

Для построения математической модели криптосистемы с введенными в [8, 10] обозначениями информационный оператор используется нестандартно, т.е. как оператор прямого криптографического преобразования. Это обусловлено тем, что при шифровании нарушителю известен не открытый текст, а некоторая информация о нем, заключенная в криптограммах. Тогда X — источник открытых сообщений, а $N : X \to Y$ — оператор, описывающий прямое криптографическое преобразование, $S : X \times R_+ \to 2^G$ — оператор криптографического анализа, G — множество оценок «истинности» открытых текстов. В зависимости от ситуации в качестве множества G можно использовать, например, апостериорные вероятности элементов множества X (как в теории информации Шеннона); множество предполагаемых открытых текстов или множество состояний конечного автомата, описывающего источник открытых сообщений X. Заметим, что для достижения идеальной стойкости криптосистемы оператор N должен быть неполным. Для такой модели «вычислительной стойкости» получены следующие результаты [10]:

— условие идеальной стойкости определяется как $r(N(X)) \ge \varepsilon > 0$, где $r(N(X))$ — радиус информации $N(x)$;

— модель с неточным информационным оператором N_ρ позволяет описывать внесение ошибок в процесс шифрования, при этом существуют идеально стойкие криптосистемы, которые по классификации Шеннона относятся к «практически стойким»;

— для криптосистем, идеально стойких в вычислительной модели стойкости, все криптографические преобразования имеют свойство не сохранять гомоморфизм;

— криптосистема, идеально стойкая в вычислительной модели стойкости, также является стойкой в смысле полиномиальной неразличимости.

Заметим, что подобное применение информационного оператора не всегда оправданно. Рассмотрим традиционное использование информационного оператора для оценки стойкости криптосистем на примере оценки стойкости с помощью ОТОА схем двуфакторной аутентификации на одноразовых паролях. Системы многофакторной аутентификации пользователей — одни из самых популярных и эффективных методов для защиты пользователей от несанкционированного доступа к персональным данным, контента и т.д. Главная идея многофакторной аутентификации заключается в использовании дополнительного фактора аутентификации: чаще всего одноразового пароля, генерируемого датчиком псевдослучайных чисел и распределяемого по защищенному каналу между

участниками схемы аутентификации (такие схемы применяются, например, в Gmail, социальных сетях Twitter и Facebook).

Для анализа уязвимостей систем многофакторной аутентификации пользователей традиционно проводятся исследования статистических свойств одноразовых паролей (их длина обычно варьируется от 6 до 10 десятичных знаков), используемых в данных системах. Такой подход имеет ряд недостатков. Рассмотрим их на примере анализа схемы двуфакторной аутентификации системы Gmail.

В данной схеме используется алгоритм TOTP (RFC 6238), являющийся улучшенным вариантом алгоритма HOTP (RFC 4226). Проведенные экспериментальные исследования статистических свойств пароля показали, что из 3246 полученных одноразовых паролей только 30 % уникальны. Для последовательности попыток аутентификации от одного пользователя Gmail повторно создает такой же одноразовый пароль, который аннулируется только по истечении 30 мин после первой попытки аутентификации или ее успешного завершения. Это позволяет сделать вывод о недостаточной длине периода датчика псевдослучайных чисел. Последовательность уникальных паролей (после исключения повторов) не проходит стандартных тестов на случайность, рекомендованных NIST. Однако получение выборки требуемой длины из одноразовых паролей связано со значительными технологическими трудностями, которые не позволяют применять большинство из существующих статистических методов. В итоге использование статистических подходов практически не дает какой-либо информации о верхних и нижних границах стойкости схем аутентификации с одноразовыми паролями.

Сформулируем задачу оценки стойкости схем аутентификации с одноразовыми паролями в терминах OTOA. Рассмотрим частный случай задачи бинарного поиска, описанной в [26]. Пусть $S(f,\varepsilon)=\{g\in G:|f-g|\le \varepsilon m\}$, где $F=\{1,2,\dots,m\}$ и $G=\{1,2,\dots\}$, $R_+=[0,\infty)$ — множество целых чисел, отличающихся от f не более чем на εm, $\varepsilon\ge 0$. Очевидно, что свойства оператора решения, описанные ранее, выполнены. Пусть T_i, $i=1,\dots,n$, — заданные подмножества в F, а также далее $H=\{0,1\}^n$ и $N(f)=[Q(f,T_1),\dots,Q(f,T_n)]$, где $Q(f,T_i)=\begin{cases}1, & \text{если } f\in T_i\\ 0, & \text{если } f\notin T_i\end{cases}$.

Требуется найти неизвестное число f с точностью до εm, зная только его принадлежность множествам T_i, $i=1,\dots,n$. При этом задача состоит в определении минимального объема информации для получения точного одноразового пароля, т.е. $\varepsilon=0$. Тогда положим $S(f,\varepsilon)=\{S(f)\}$ для $\varepsilon\ge 0$, т.е. $S(f,\varepsilon)$ не зависит от ε и для каждого f существует единственное ε-приближение к $x=S(f)$. Показано [26], что

$$r(N)=\begin{cases}0, & \text{если } S(V(N,f)) \text{ одноточечно}\\ +\infty & \text{в противном случае}\end{cases}.$$

Здесь радиус информации определяет возможность решения задачи при нахождении точного одноразового пароля и невозможность ее решения в случае неопределенности (т.е. существования более чем одного одноразового пароля). Задача таким образом сводится к определению «минимального количества» информации, при котором $r(N)=0$. Заметим, что верхней границей этой информации является период датчика псевдослучайных чисел, используемого для генерации одноразовых паролей, а нижней — колмогоровская сложность [10] множества $S(V(N,f))$.

Вернемся к использованию информационного оператора для описания некоторого преобразования, а именно стеганографической системы. Представим стеганосистему как совокупность множеств (C, S, M, K, Q) соответственно контейнеров, стеганограмм, открытых сообщений, ключей и сообщений, наблюдаемых нарушителем. Для встраивания сообщения используется оператор

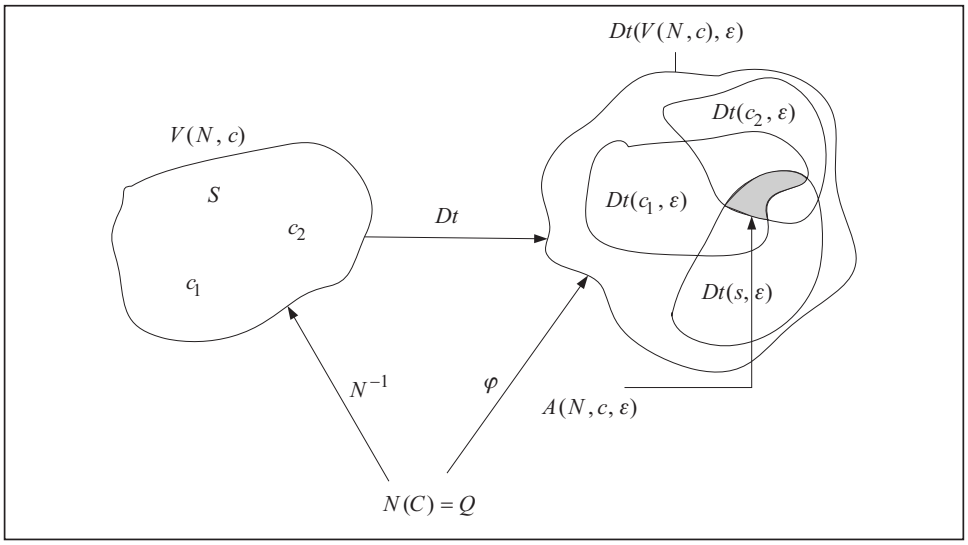

Рис. 2. Операторы стеганографический и стеганоанализа

$E:C\times M\times K\to N(C)=Q$, который можно также рассматривать в виде $E_{K\times M}:C\to N(C)$, где $M\times K$ — составной ключ. Тогда стеганосистему можно рассматривать как криптосистему с составным ключом, оператор $Dt:C\times\Re_+\to 2^M$, где $\Re_+=[0,\infty)$ — оператор стеганоанализа (рис. 2).

Построение модели стеганосистемы осуществляется аналогично построению модели криптосистемы. Пусть оператор стеганоанализа имеет два свойства:

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

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

Для заданного значения $\varepsilon\ge 0$ элемент $c\in C$, удовлетворяющий условию $c\in Dt(c,\varepsilon)$, называется ε-приближением. Задача поиска ε-приближения решается в случае отсутствия полной информации об элементе c, о котором имеется некоторая информация $N(c)=q\in Q$, где $N:C\to Q$ — информационный оператор или информация о контейнерах (заполненных и пустых), которой владеет нарушитель. Зная q, необходимо найти ε-приближение к $m\in Dt(c,0)$. Очевидно, что условия (1), (2) выполняются для любого метода стеганографического анализа. Рассмотрим множество $V(N,c)=\{\widetilde{c}\in C:N(\widetilde{c})=N(c)\}$ всех элементов $\widetilde{c}$, неотличимых с помощью информационного оператора $N(c)$. Если оператор N не является биекцией [9], то множество $V(N,c)$ неодноточечное. Можно считать, что множество $V(N,c)$ является классом эквивалентности на множестве Q, а разбиение контейнеров на классы эквивалентности порождает информационный оператор N, который называется неполным оператором. Оператор стеганоанализа, примененный к неполному информационному оператору, порождает множество $A(N,c,\varepsilon)=\bigcap_{\widetilde{c}\in V(N,c)} Dt(\widetilde{c},\varepsilon)$. Исходя из условия (2), величины $r(N,c)=\inf\{\delta:A(N,c,\delta)\neq\varnothing\}$ и $r(N)=\sup\limits_{c\in C} r(N,c)$ определяют нижние оценки точности решений, которые можно достичь при неполном информационном операторе.

Используя результаты работы [26], получаем, что в 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 $e(\varphi,N)=\sup\limits_{c\in C} e(\varphi,N,c)$ погрешностями,

где φ — алгоритм реализации оператора стеганоанализа (см. рис. 2), информация Q позволяет найти ε-приближение для произвольного $c \in C$ тогда и только тогда, когда выполняется одно из условий:

$$r(N) < \varepsilon,$$

$$r(N) = \varepsilon,\ \exists \varphi : \varphi(Q) \in Dt(c, e(\varphi, N))\ \ \forall c \in C.$$

Таким образом, для оценки стойкости к стеганоанализу можно использовать радиус информации. С помощью данной модели для оценки стойкости стеганосистем получены следующие результаты [8, 9, 16–20]:

— формально доказано, что построение совершенно стойкой стегосистемы возможно или при применении селективного метода, или при отсутствии полной информации об «эталонном» незаполненном контейнере (при применении контейнеров произвольного доступа, например, метода LSB). В этом случае оператор N должен быть неполным, а стойкость не зависеть от оператора стеганоанализа;

— показано, что теоретико-информационная стойкость по отношению к выбранному критерию распознавания скрытого сообщения достигается, если $r(N) \to \infty$, т.е. множество $Dt(V(N, c), \varepsilon)$ распадается на непересекающиеся подмножества при любом $\varepsilon > 0$. Такой случай в методе LSB соответствует встраиванию в контейнеры бессмысленных сообщений или сообщений, зашифрованных совершенно стойким шифром;

— доказано, что стойкость стеганографической системы, предложенной в [20], определяется радиусом информации алгоритма генерации CAPTCHA-изображения.

Использование информационного оператора как традиционным (в смысле модели, приведенной в [26]), так и нетрадиционным способами позволяет также получать нижние оценки показателей безопасности информации для распределенных, облачных и децентрализованных информационно-коммуникационных систем. Так, в работе [12] доказано:

— надежность распознавания безопасного состояния ИКС не превышает вероятности осуществления APT-атаки в промежутке времени, меньшем Δt — периодичности срабатывания сенсоров систем мониторинга безопасности информации (например, времени обработки события SIEM-системой);

— надежность распознавания сигнатурного метода не превышает вероятности коллизии применяемой в нем хеш-функции.

ЗАКЛЮЧЕНИЕ. ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ОТОА В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

Особенностью ОТОА является возможность связывания сложности вычислительных алгоритмов с качеством информации о задаче. Эта уникальная возможность позволяет применять элементы этой теории для решения разнообразных задач защиты информации:

— получение нижних оценок надежности распознавания уровня безопасности информации в любых распределенных системах независимо от степени их неоднородности;

— разработка и исследование методов построения с информационно невычислимой лазейкой однонаправленных функций и нового класса асимметричных криптосистем;

— нахождение более точных и комплексных (относительно сложности алгоритмов криптоанализа и необходимого количества шифртекста) оценок стойкости криптографических систем;

— определение более точных оценок стойкости стеганографических систем без привязки к виду стеганографических контейнеров;

— получение более точных оценок стойкости средств криптографической защиты информации к атакам на реализацию, учитывающих неоднородность и

распределенность вычислительных и информационных ресурсов и не требующих ввода меры на множестве оценочных параметров.

СПИСОК ЛИТЕРАТУРЫ

1. The Open Source Definition (Annotated). URL: https://opensource.org/docs/definition.php.
2. Maurer U. Information-theoretic cryptography. *Advances in Cryptology — CRYPTO'99, Proc.* Springer Verlag, 1999. P. 47–64.
3. Abadi M., Rogaway P. Reconciling two views of cryptography (The computational soundness of formal encryption). *Journal of Cryptology.* 2002. Vol. 15, N 2. P. 103–127.
4. Алексейчук А.Н. Математическая модель и задачи анализа стойкости вероятностно-криптографических систем в системах защиты информации. *Захист інформації*. 2001. № 3. С. 5–12.
5. Богуш В.М., Довидьков О.А., Кудін А.М. Перспективи розвитку автоматизованих систем обробки конфіденційної інформації загального призначення. *Вісн. Державного ун-ту інформаційно-комунікаційних технологій.* 2003. Т. 1, № 1. С. 42–46.
6. Задірака В.К., Кудін А.М., Людвиченко В.О., Олексюк О.С. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: Навчальний посібник. Київ; Тернопіль: Підручники та посібники, 2007. 272 с.
7. Задирака В.К., Кудин А.М., Людвиченко В.А., Олексюк А.С. Специальные цифровые носители информации. Теория, технология, применение. *Искусственный интеллект*. 2008. № 3. С. 631–638.
8. Задирака В.К., Кудин А.М. Анализ стойкости криптографических и стеганографических систем на основе общей теории оптимальных алгоритмов. *Journal of Qafqaz University Mathematics and Computer Science*. 2010. N 2. P. 47–57.
9. Кудин А.М. Математическая модель стеганографической системы на базе общей теории оптимальных алгоритмов. *Математичне та комп'ютерне моделювання.* Кам'янець-Подільський: Вид-во Кам.-Под. нац. ун-ту, 2010. № 4. С. 136–143.
10. Кудин А.М. Криптографические преобразования нешенноновских источников информации. *Кибернетика и системный анализ*. 2010. № 5. С. 143–149.
11. Кудін А.М. Порівняльний аналіз математичних моделей стійкості криптосистем. *Наукові вісті НТУУ «КПІ»*. 2010. № 4(72). С. 86–90.
12. Кудін А.М. Створення систем підтримки прийняття рішень для управління захистом інформації в хмарних обчислювальних системах. *Зб. наук. пр. Національної академії державної прикордонної служби імені Б. Хмельницького. Сер. військові та технічні науки.* Хмельницький: Вид-во НА ДПС, 2010. № 54. С. 70–72.
13. Кудин А.М. Алгоритмические аспекты реализации модулей защиты для распределенных вычислительных систем. *Вісн. Державного ун-ту інформаційно-комунікаційних технологій*. 2011. Т. 9, № 2. С. 142–147.
14. Кудин А.М. Модель оценки стойкости модулей криптографической защиты информации к криптоанализу по побочным каналам. *Компьютерная математика*. 2011. № 2. С. 59–66.
15. Кудин А.М. Однонаправленные функции с информационно невычислимой лазейкой. *Прикладная радиоэлектроника.* 2012. Т. 11, № 2. С. 245–249.
16. Задирака В.К., Кудин А.М. Особенности реализации криптографических и стеганографических систем по принципу облачных вычислительных технологий. *Искусственный интеллект*. 2012. № 3. С. 438–444.
17. Задирака В.К., Кудин А.М. Облачные вычисления в криптографии и стеганографии. *Кибернетика и системный анализ*. 2013. № 4. С. 113–119.
18. Задирака В.К., Кудин А.М., Швидченко И.В. Стеганография в облачных информационно-коммуникационных системах. *Компьютерная математика*. 2014. № 1. С. 54–60.
19. Zadiraka V., Kudin A., Shvidchenko I., Bredelev B. Cryptographic and steganographic protocols for cloud systems. *Computer Technologies in Information Security.* V. Zadiraka, Y. Nykolaichuk (Eds). Ternopil, 2015. P. 9–41.
20. Задирака В.К., Кудин А.М., Бределев Б.А., Швидченко И.В. Применение CAPTCHA в компьютерной стеганографии. *Кибернетика и системный анализ*. 2015. Т. 51, № 5. С. 149–156.

21. Задирака В.К., Кудин А.М., Селюх П.В., Швидченко И.В. Облачные технологии: новые возможности для вычислительного криптоанализа. *Проблемы управления и информатики*. 2016. № 1. С. 148–155.
22. Итоги киберактивности в 1 квартале 2017 года. URL: https://habrahabr.ru/company/panda/blog/328324.
23. Mell P., Grance T. Effectively and securely using the cloud computing paradigm. URL: http://csrc.nist.gov/groups/SNS/cloud-computing/index.html
24. Simonite T. Google's new chip is a stepping stone to quantum computing supremacy URL: https://www.technologyreview.com/s/604242/googles-new-chip-is-a-stepping-stone-to-quantum-computing-supremacy.
25. Трауб Д., Вожьняковский Х. Общая теория оптимальных алгоритмов. Москва: Мир, 1983. 382 с.
26. Трауб Д., Васильковский Г., Вожьняковский Х. Информация, неопределенность, сложность. Москва: Мир, 1988. 184 с.

Надійшла до редакції 29.06.2017

В.К. Задірака, А.М. Кудін

НОВІ МОДЕЛІ ТА МЕТОДИ ВИЗНАЧЕННЯ СТІЙКОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Анотація. Запропоновано новий підхід до оцінки стійкості систем захисту інформації для сучасних інформаційно-комунікаційних систем на базі загальної теорії оптимальних алгоритмів. Наведено зв'язок між якістю інформації та стійкістю криптографічних та стеганографічних систем. Обґрунтовано вибір радіуса інформації як показника стійкості для різних систем захисту інформації.

Ключові слова: безпека інформації, криптологія, стеганографія, загальна теорія оптимальних алгоритмів, радіус информації.

V.K. Zadiraka, A.M. Kudin

NEW MODELS AND METHODS OF INFORMATION SECURITY ESTIMATES

Abstract. The new approach for information security estimate for modern information and communication systems based on the general theory of optimal algorithms is proposed. The relationship between the quality of information and the cryptographic and steganographic systems security is shown. The choice of the radius of information as an index of security for various information security systems is justified.

Keywords: information security, cryptology, steganography, the general theory of optimal algorithms, information radius.

Задирака Валерий Константинович,
академик НАН Украины, доктор физ.-мат. наук, профессор, заведующий отделом Института кибернетики им. В.М. Глушкова НАН Украины, Киев, e-mail: zvk140@ukr.net.

Кудин Антон Михайлович,
доктор техн. наук, старший научный сотрудник, профессор Физико-технического института Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского», e-mail: pplayshner@gmail.com.