В настоящее время широко распространено использование интернет-сервисов, которые позволяют загружать и скачивать неподвижные изображения. Некоторые из этих сервисов при загрузке на них изображений стирают всю пользовательскую информацию из файла, следовательно, для подтверждения авторских прав необходимо разработать алгоритм, при использовании которого встроенный ЦВЗ сохранится в условиях снижения качества изображений пережатием.

Были проанализированы существующие алгоритмы внедрения ЦВЗ в область преобразования, используемого в формате JPEG [2], — дискретного косинусного преобразования (ДКП). Внедрение информации в коэффициенты ДКП характеризуется наличием заметных искажений изображения или, в случае незаметных искажений, малой устойчивостью к воздействиям. Учитывая особенности формата JPEG, ДКП, а также системы человеческого зрения, можно внедрить ЦВЗ в изображение, сделав его более устойчивым и менее заметным.

Модифицирован один из методов внедрения ЦВЗ в область преобразования — метод Коха и Жао [3. С. 130–135]. ЦВЗ, встроенный таким образом, извлекается из изображений с разной степенью сжатия.

Разработанные алгоритмы позволяют внедрять в изображения информацию, сохраняющуюся при JPEG-сжатии с наиболее распространенными параметрами, что дает возможность извлекать данные об авторе изображения даже после ухудшения его качества и удаления метаданных.

СПИСОК ЛИТЕРАТУРЫ:

1. *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. М.: СОЛОН-Пресс, 2002. — 272 с.
2. ISO/IEC 10918-1:1994. Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines.
3. *Коханович Г. Ф., Пузыренко А. Ю.* Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. — 288 с.

REFERENCES:

1. *Gribunin V. G., Okov I. N., Turintsev I. V.* Tsifrovaya steganografiya. M.: SOLON-Press, 2002. — 272 p.
2. ISO/IEC 10918-1:1992. Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines.
3. *Kokhanovich G. F., Puzyrenko A. U.* Kompjuternaya steganografiya. Teoriya I praktika. K.: MK-Press, 2006. — 288 c.

S. D. Kulik

Ensuring Information Security and Factographic Systems

Key words: *information security, factographic system, factographic information retrieval system*

This article is about methods of information security. These methods are a part of the automated tools of ensuring the information security. It is offered to use a factographic information retrieval. The results are protected with patents.

С. Д. Кулик

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ФАКТОГРАФИЧЕСКИЕ СИСТЕМЫ

В области информационных технологий специалисты среди информационных систем выделяют класс систем, которые получили название автоматизированные фактографические информационно-поисковые системы (АФИПС) [1]. Для повышения эффективности работы автоматизированных средств обеспечения информационной безопасности (АСОИБ) предлагается использовать в составе этих средств фактографическую информационно-поисковую подсистему. Существенное отличие АФИПС от автоматизированной информационно-поисковой системы (АИПС) состоит в том, что АФИПС позволяют получать ответы на фактографические запросы. Одной из главных задач, решаемых этой подсистемой, является ответ на фактографические запросы пользователя АСОИБ и реализация специализированного фактографического поиска по запросу оператора АСОИБ.

Предлагается ввести следующие частные показатели, связанные с оценкой эффективности защиты информации в данных фактографических информационных системах:

A_1 – оценка вероятности неискажения информации от внутреннего злоумышленника;

A_2 – оценка вероятности неискажения информации от внешнего злоумышленника;

A_3 – оценка вероятности неискажения информации от вредоносного *программного обеспечения* (например, вредоносного компьютерного вируса);

A_4 – оценка вероятности неискажения информации от вредоносного *аппаратного обеспечения* (например, закладочных устройств, аппаратных закладок, то есть устройств в электронной схеме, скрытно внедряемых к остальным элементам);

A_5 – оценка вероятности неискажения информации от внешнего вредоносного воздействия на *аппаратуру*, *программное обеспечение*, *фактографические данные* (например, электромагнитное воздействие).

С опорой на эти введенные показатели и на работы [2–6] была разработана аналитическая модель для оценки эффективности работы АФИПС в АСОИБ.

Подход к оценке информационной безопасности для фактографических систем с помощью набора показателей $\{A_1, A_2, A_3, A_4, A_5\}$ ранее не использовался. На практике злоумышленник может частично разрушить (исказить) содержимое записи данных в фактографической БД, при этом цель АФИПС – найти фактографические данные, необходимые для эффективного функционирования АСОИБ.

В процессе работы поискового блока АФИПС сравнение поискового образа запроса и поискового образа объекта выполняется с применением алгоритма распознавания образов или нейросетевого алгоритма [2, 6, 7, 8], который характеризуется вероятностями пропуска цели и ложной тревоги. Так как это сравнение поисковым блоком характеризуется этими вероятностями, то это позволяет учитывать эффективность защиты информации в фактографических данных в АСОИБ. В составе АСОИБ есть человек-оператор, эффективная работа которого сильно зависит от эффективности работы АФИПС. Разработанная аналитическая модель опирается на теорию вероятностей [4, 5, 6] и позволяет учесть этот факт. Экспериментальное исследование этой модели показало, что она адекватна для выбранной прикладной области.

По результатам проведенных исследований намечены пути применения фактографического поиска с помощью АФИПС в АСОИБ. Была кратко представлена идея АСОИБ с элементами фактографических систем, что способствует эффективному решению задачи обеспечения информационной безопасности. Разработана аналитическая модель для оценки (по введенным

показателям) эффективности фактографического поиска в АСОИБ. Проведено исследование полученных оценок и выявлены их свойства. В процессе выполненной работы и проведенных исследований были успешно получены необходимые охранные документы Федеральной службы по интеллектуальной собственности (Роспатент).

СПИСОК ЛИТЕРАТУРЫ:

1. *Кулик С. Д.* Информационная безопасность АФИПС // Известия Южного федерального университета. Технические науки. 2003. Т. 33. № 4. С. 238.
2. *Salton G.* Automatic information organization and Retrieval. New York: McGraw-Hill, 1968. — 514 р.
3. *Fukunaga K.* Introduction to Statistical Pattern Recognition. Elsevier Academic Press. San Diego, San Francisco, New York, Boston, London, Sydney, Tokyo, 1990. — 592 p.
4. *Вентцель Е. С.* Теория вероятностей. М.: Высшая школа, 2001. — 575 с.
5. *Колмогоров А. Н.* Основные понятия теории вероятностей. М.: ФАЗИС, 1998. — 144 с.
6. *Feller W.* An introduction to probability theory and its applications. Vol. 1. 3rd ed. John Wiley & Sons. New York, 1968. — 509 p.
7. *Галушкин А. И.* Теория нейронных сетей: Учебное пособие для вузов. Кн. 1. М.: ИПРЖР, 2000. — 416 с.
8. *Haykin S.* Neural Networks — A Comprehensive Foundation. Second Edition. Pearson Education, Inc., 1999. Reprint: 2005.

REFERENCES:

1. *Kulik S. D.* Informatsionnaya bezopasnost' AFIPS // Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskiye nauki. 2003. T. 33. № 4. P. 238.
2. *Salton G.* Automatic information organization and Retrieval. New York: McGraw-Hill, 1968. — 514 p.
3. *Fukunaga K.* Introduction to Statistical Pattern Recognition. Elsevier Academic Press. San Diego, San Francisco, New York, Boston, London, Sydney, Tokyo, 1990. — 592 p.
4. *Wentzel E. S.* Teoriya veroyatnostey. M.: Vysshaya shkola, 2001. — 575 p.
5. *Kolmogorov A. N.* Osnovnyye ponyatiya teorii veroyatnostey. M.: FAZIS, 1998. —144 p.
6. *Feller W.* An introduction to probability theory and its applications. Vol. 1. 3rd ed. John Wiley & Sons. New York, 1968. — 509 p.
7. *Galushkin A. I.* Teoriya neyronnykh setey: Uchebnoye posobiye dlya vuzov. Kn. 1. M.: IPRZHR, 2000. — 416 p.
8. *Haykin S.* Neural Networks — A Comprehensive Foundation. Second Edition. Pearson Education, Inc., 1999. Reprint: 2005.

M. A. Kupriyashin, G. I. Borzunov

Evolution of Knapsack Ciphersystems

Key words: knapsack problem, knapsack ciphersystems

The knapsack problem is known to be used in numerous public key ciphersystems designs. These ciphersystems have been receiving increased attention from analytics, resulting in many being compromised. Therefore, modern systems incorporate new algorithms making them at least partially immune to known attacks. In this paper, three types of knapsack ciphersystems are introduced. The difference between types is how the keys are generated and used. Classical systems, being the first type, use superincreasing sequences and low-density knapsacks and are therefore vulnerable. Modern cryptosystems are based on high-density knapsacks. That makes them difficult to analyze. Hybrid cryptosystems incorporate several security mechanisms (not only trapdoor knapsacks) that makes analysis, as well as implementation, even more complicated.