її роботи. Механізми безпеки мають бути адаптивними для динамічно змінних потоків інформації.

Розглянуті підходи до забезпечення інформаційної безпеки у відкритих системах співзвучні новій парадигмі інформаційної безпеки інформаційно-телекомунікаційних систем. Системи безпеки майбутнього повинні не тільки і не стільки обмежувати допуск користувачів до програм і даних, скільки визначати і делегувати їх повноваження у корпоративному вирішенні задач, виявляти аномальне використання ресурсів, прогнозувати аварійні ситуації й усувати їх наслідки, гнучко адаптуючи структуру в умовах відмов, часткової втрати або тривалого блокування ресурсів. Вирішення такої задачі дасть можливість оптимізувати також й існуючі системи інформаційної безпеки закритих систем, сучасна теорія яких частково вирішує задачу захисту відкритих систем.

Результати та висновки

В цій частині роботи вирішені такі задачі, об'єднані поставленою метою вироблення науково-методичних основ системи інформаційної безпеки відкритих систем:

- розглянуто принципові структурні властивості відкритих систем;
- роз'яснена роль інтелектуального управління у відкритих системах та їх органічна єдність з процесами забезпечення безпеки; зроблено висновок щодо співпадання цілей, методів контролю, механізмів забезпечення безпеки, які мають системи управління та системи інформаційної безпеки; знайдено висновок, що системи інтелектуального управління за своїм принципом дії виконують певну частину задач інформаційної безпеки, зокрема повну спостережність системи та утримання системи в стані гомеокінетичного плато, тобто забезпечують фізичну безпеку;
- сформульовано цілі інформаційної безпеки та вимоги до системи інтелектуального управління з позицій інформаційної безпеки; сформульовані гіпотези щодо системи інформаційної безпеки, споріднені з аналогічними гіпотезами щодо інтелектуального управління.

Крім того, намічені шляхи до створення технології й архітектури інформаційної безпеки відкритих систем та побудови системи інформаційної безпеки на законах функціонування відкритих систем. Напрямом подальшої роботи може бути: обґрунтування способу побудови інтегрованої в систему управління чи окремої системи інформаційної безпеки відкритих систем; розробка комплексної системи вимог до власне системи інформаційної безпеки відкритих систем. Важливим напрямком досліджень є розробка принципів і реалізація адаптивних систем захисту інформації та розробки систем інформаційної безпеки в зовнішньому контурі управління відкритою системою.

Література: ***1.*** *Кононович В., Тардаскіна Т. Основні принципи інформаційної безпеки відкритих системою Частина 1. Міри інформації та властивості інформаційних процесів відкритих систем. // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 1 (12), К: 2006. С. 44 – 55.* ***2.*** *Потий А. Эталонная модель системы процессов защиты информации. // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 1 (12), К: 2006. С. 31 – 43.* ***3.*** *В. М. Лачинов, А. О. Поляков. Информодинамика или Путь к Миру открытых систем. Санкт-Петербург, Издат. СПбГТУ, 1999. – С. 364. (http//www.polyakov.com/informodynamiks).* ***4.*** *Чаки Ф. Современная теория управления. Нелинейные, оптимальные и адаптивные системы. Пер. с английского. – М.: Мир, 1975. 424 с.* ***5.*** *Леваков А. Анатомия информационной безопасности США. Jet Info online #6(109), 2002, http://daily.sec.ru/dailypblshow.cfm?rid=9&pid=5503&pos=13&stp=10. – 74 с.* ***6.*** *Кононович В., Тардаскін М. Парадигма інформаційної безпеки телебіомерики та сенсорних телекомунікаційних мереж. // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 1 (12), К: 2006. С 56 – 65.* ***7.*** *Колмогоров А. Н. Жизнь и мышление как особые формы существования материи. // О сущности жизни. М.: Наука 1964, с. 48 – 57.*

УДК 004.82, 007.04, 681.3, 681.518.54

ПРИМЕНЕНИЕ ПРИНЦИПА БИОАНАЛОГИИ ДЛЯ СИНТЕЗА СИСТЕМ ИНТЕЛЛЕКТУАЛЬНОГО УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ТЕЛЕКОММУНИКАЦИЙ

Сергей Гладыш

Одесская национальная академия связи им. А. С. Попова

Анотація: **Досліджено можливості застосування методів штучного інтелекту у процесах керування інформаційною безпекою телекомунікаційних систем. Як новий методологічний підхід**

запропоновано принцип біологічної та медичної аналогії як стосовно архітектури вбудованих засобів захисту телекомунікаційних систем, так і процесів проектування, адаптації та оптимізації систем інтелектуального керування безпекою телекомунікацій. Пропонується проектувати телекомунікаційні системи в єдиному процесі з вбудованими засобами захисту інформації, спроможними адаптуватись до зміни поля загроз з використанням імуноподібних механізмів для розпізнавання та нейтралізації атак на інформаційні ресурси телекомунікаційних систем.

Summary: **Possibilities of artificial intelligence methods integration in the information security management processes of telecommunication systems are researched. A principle of biological and medical analogy as a new methodological approach is offered both as it applies to the telecommunication and information security systems architecture and to the processes of developing, adaptation and optimization of the telecommunication security intellectual control systems. It is suggested to design telecommunication systems in a single process with built-in intellectual security facilities, able to adaptation to the dynamic changeable field of threats and using immune-similar mechanisms for recognition and neutralization of attacks on the informative resources of telecommunication systems.**

Ключевые слова: **Интеллектуальное управление, информационная безопасность, телекоммуникационная система, принцип биоаналогии, организмический подход, адаптация.**

I Введение. Постановка задачи

К современным тенденциям развития телекоммуникационных технологий можно отнести следующие: цифровизацию, разнородность и многопротокольность на базе модели взаимодействия открытых систем [1], распространение спутниковых и беспроводных технологий, конвергенцию и переход к сетям нового поколения (NGN) [2], широкое использование в сетях связи компьютерной вычислительной техники и специализированного управляющего программного обеспечения (программно-управляемых цифровых АТС, программных коммутаторов Softswitch и т. д.), интеграцию информационных и коммуникационных систем в пакетную мультисервисную информационно-телекоммуникационную сеть, появление телебиометрических и сенсорных сетей [3]. Следствием данных тенденций является необходимость пересмотра постановки проблемы обеспечения безопасности телекоммуникаций [4] и поиска новых адекватных подходов к ее решению. Одним из таких подходов, учитывающих отмеченные тенденции, является, по мнению автора, интеллектуальное управление (ИУ) ресурсами информационной безопасности (ИБ).

Проблема применения технологий искусственного интеллекта, в частности систем интеллектуального управления (СИУ), для решения задач обеспечения ИБ телекоммуникационных систем (ТКС) является актуальной и до конца не решенной [5, 6]. Особое значение приобретают задачи разработки моделей представления знаний в СИУ ИБ, которые уже рассматривались автором в работах [7 – 9]. Результаты исследований [9, 10] свидетельствуют о назревшей необходимости унификации моделей представления знаний (МПЗ) путем разработки метамоделей представления знаний (ММПЗ), универсализации систем управления, программного и алгоритмического обеспечения для работы с базами знаний. Причем степень абстрагирования при решении задачи унификации должна быть ограничена определенными классами задач, которые могут оказаться относящимися к различным предметным областям или же быть общими для различных сфер деятельности.

Целью статьи является разработка и обоснование нового методологического подхода к синтезу СИУ ИБ ТКС, основанного на применении принципа биологической и медицинской аналогии («организмического» подхода) применительно к построению ММПЗ [9]. Такой подход вписывается в русло передовых междисциплинарных научных направлений, таких как: синергетика [11], коэволюция инфосферы [12, 13], «artifical life» [14], системология [15].

Для реализации поставленной цели в рамках исследования необходимо решить следующий круг задач:

- рассмотреть особенности применения ММПЗ в рамках предметной области ИУ ИБ ТКС, проанализировать структуру изучаемой предметной области;
- сформулировать основные постулаты «организмического подхода»; раскрыть сущность биомедицинской метафоры в рамках предлагаемого подхода;
- представить формализованное математическое описание предлагаемого решения проблемы;
- дать рекомендации к синтезу СИУ ИБ ТКС с использованием разработанного подхода.

В иследовании использованы методы искусственного интеллекта (data mining, knowledge engineering); методы бионики и кибернетики (принцип биомедицинской аналогии, «организмический подход»).

II Онтология проблемной области ИУ ИБ ТКС и особенности применения унифицированных ММПЗ

Рассматривая реализацию поставленных задач как решение единой проблемы синтеза СИУ ИБ ТКС,

сформулируем некоторые особенности теоретического и практического применения унифицированных метамоделей представления знаний.

Постановка и решение любой проблемы всегда связаны с ее «погружением» в соответствующую предметную область. Так, исследуя проблему синтеза СИУ ИБ ТКС, мы вовлекаем в предметную область такие объекты, как конкретное телекоммуникационное оборудование, линейно-кабельные сооружения, абонентское оборудование, конкретные организационные, технические и криптографические средства защиты информации, протоколы, структурные элементы и подсистемы различного уровня иерархии, интервалы времени, а также общие понятия «оборудование», «линия связи», «протокол», «политика информационной безопасности» и т. п.

Все предметы и события, которые составляют основу информации, необходимой для решения данной изучаемой проблемы, будем называть предметной областью интеллектуального управления ИУ ИБ ТКС. Предметную область ИУ ИБ ТКС будем представлять состоящей из реальных или абстрактных объектов или сущностей. В базе знаний сущности будет соответствовать некоторое описание, полнота которого определяется имеющейся информацией.

Между сущностями ИУ ИБ ТКС наблюдаются различные отношения подобия. Совокупность подобных сущностей составляет класс сущностей, являющийся новой сущностью предметной области ИУ ИБ ТКС.

Отношения между сущностями ИУ ИБ ТКС выражаются с помощью суждений. Суждение - это мысленно возможная ситуация, которая может иметь место для предъявляемых сущностей или не иметь места. В языке представления знаний суждениям отвечают предложения. Суждения и предложения также нужно рассматривать как сущности и включать в предметную область ИУ ИБ ТКС.

Очевидно, что сущности предметной области ИУ ИБ ТКС находятся в определенных отношениях друг к другу (ассоциациях), которые также можно рассматривать как сущности более высокого уровня абстракции, являющиеся общими и для других предметных областей.

Предметными областями со сходными классами задач диагностики и обеспечения защищенности объекта исследования от множества угроз различной природы являются ИБ, биология, иммунология, медицинская диагностика и др.

III Концепция и основные постулаты «организмического подхода»

Рассмотренные выше современные тенденции развития ТКС и соответствующая им сетецентрическая парадигма ИБ [4] приводят, по мнению автора [9], к необходимости применения в рамках методов ИУ ИБ так называемого «организмического подхода», предложенного академиком Н. Н. Моисеевым [12, 13]. Новые угрозы ИБ ставят на повестку дня проблемы моделирования выживания, эволюции и адаптации ТКС. Это означает переход от «механицизма» к биологической и медицинской аналогии, когда ТКС понимается как развивающаяся интеллектуальная система, рассматриваемая сквозь призму эволюционной теории. В соответствии с данной метафорой ТКС уподобляется биологическому организму, который стремится выжить в определенном биоценозе.

При этом ТКС обладает собственными целями и средствами их достижения в соответствии с определением организма по Моисееву [13]. Ресурсы ИБ и элементы ТКС (организмы нижнего уровня) для того, чтобы составит единый организм должны обладать способностью обеспечивать гомеостатическое регулирование ТКС в целом и эффективно функционировать для его обеспечения. Под гомеостатическим регулированием понимается управление, поддерживающее характеристики внутренней среды, в данном случае ТКС, в пределах, обеспечивающих ее безопасность, устойчивость и жизнеспособность.

«Организмический подход» предполагает применение принципов и механизмов адаптации и эволюции при анализе и синтезе СИУ ИБ ТКС как структурно-сложной нелинейной системы управления, деятельность которой должна быть всегда направлена на обеспечение гомеостаза и выживания в динамически меняющейся внешней среде. Применение эволюционной теории для нужд ИУ ИБ ТКС должно осуществляться с учетом ее основных постулатов, которые применительно к изучаемой проблеме можно сформулировать следующим образом:

- **целесообразность**: выживают (т. е. эффективно поддерживают полную нормальную функциональность, качество обслуживания и гарантированную надежность системы с обеспечением всех характеристик защищенности информации) лишь те ТКС, которые в наибольшей степени соответствуют (т. е. не имеют уязвимостей) условиям (угрозам) внешей среды;
- **адаптация**: любое изменение в архитектуре средств защиты информации и функционировании ТКС направлено на приспособление к динамически изменяющимся внешним условиям (угрозам);
- **самоорганизация**: процесс эволюции ТКС приводит к непрерывному усложнению ее структуры в связи с перераспределением функций и ресурсов.

Таким образом, при использовании «организмического подхода» и принципа биологической и

медицинской аналогии в соответствии с приведенными постулатами сутью ИУ ИБ ИТС является установление генетической связи распределения ресурсов ИБ путем выявления в них остатков прошлого (свойств защищенности исходной информации), основы настоящего (имеющимся уязвимостям системы защиты информации) и зародыша будущего (угрозам ИБ, атакам и соответствующим адаптивным механизмам противодействия, механизмам и сервисам безопасности), т. е. определение тенденций эволюционного развития в соответствии с запросами надсистем (рынка, глобальной информационно инфраструктуры – GII и т. п.)

IV Формализованное математическое описание проблемы

Пусть решение множества проблем $\{\mathrm{PR}_x\}, \quad x \in X$ обеспечения защищенности объекта X определяет потребности $\{\mathrm{PN}_j\}, \; j \in J$ на заданных предметных областях $\{\mathrm{PA}_l\}, \quad l \in L$ со сходнями классами задач.

На предметной области ИБ $\mathrm{PA}_{\mathrm{ISec}} \in \{\mathrm{PA}_l\}, \quad ISec \in L$ определим подмножество потребностей:

$$\{\mathrm{PN}_{j\mathrm{ISec}}\} \subseteq \{\mathrm{PN}_j\}, \quad jISec \in J_{ISec}, \quad J_{ISec} \subseteq J \; . \tag{1}$$

Тогда $\{\mathrm{PN}_j\}$ будет представлено в базе знаний СИУ в общем случае в виде некоторого класса метамоделей представления знаний $\{\mathrm{PM}_q\} \subseteq \{\mathrm{PM}_Q\}, \quad q \in Q$, являющегося подмножеством всех моделей и языков представления знаний.

В свою очередь, подмножество потребностей ИУ ИБ ТКС $\{\mathrm{PN}_{j\mathrm{ISec}}\}$ может быть представлено подклассом метамоделей представления знаний:

$$\mathrm{PM}_{q\mathrm{ISec}} \subseteq \{\mathrm{PM}_q\}, \quad qISec \in Q_{ISec}, \quad Q_{ISec} \subseteq \mathrm{q}, \quad \mathrm{q} \in \mathrm{Q} \, , \tag{2}$$

отражающих специфику подмножества проблем обеспечения защищенности объекта на заданном множестве предметных областей, в том числе и ИУ ИБ ТКС.

Критерии эффективности $\{\mathrm{CR}_k\}, \quad k \in K$ СИУ определим на множестве реализуемых целей $\{\mathrm{GP}_r\}, \quad r \in R$, а также особенностями предметной области, в частности $\mathrm{PA}_{\mathrm{ISec}}$.

Множество $\{\mathrm{CR}_k\}, \quad k \in K$ порождает некоторое подмножество комплекса решаемых задач $\{\mathrm{PZ}_m\}, \quad m \in M$ на множестве метамоделей представления знаний $\{\mathrm{PM}_q\}$.

Следовательно, для целей создания и развития СИУ ИБ ТКС необходимо предложить и определить пути решения комплекса задач ИУ ИБ ТКС:

$$\mathrm{PZ}_{m\mathrm{ISec}} \subseteq \{\mathrm{PZ}_m\}, \quad mISec \in M_{ISec}, \quad M_{ISec} \subseteq m, \quad m \in M \tag{3}$$

и соответствующих ММПЗ:

$$\mathrm{PM}_{q\mathrm{ISec}} \subseteq \{\mathrm{PM}_q\}, \quad qISec \in Q_{ISec}, \quad Q_{ISec} \subseteq \mathrm{q}, \quad \mathrm{q} \in \mathrm{Q} \, . \tag{4}$$

V Рекомендации к синтезу СИУ ИБ ТКС на основе «организмического подхода»

При синтезе СИУ ИБ ТКС на основе биомедицинской метафоры и «организмического» подхода весьма рациональным оказывается применение новых математических подходов к задачам медицинской диагностики [16].

Проблема выявления профессионального знания врача математическими методами, рассмотренная в [16], является аналогичной проблеме выявления знаний эксперта по ИБ [17]. В обоих случаях знание, первоначально присутствующее в скрытом, неосознанном виде, предстоит сформулировать в виде проверяемых утверждений, имеющих точный смысл. Набор точных утверждений полезен, например, для интенсификации процесса обучения нового поколения специалистов.

При сравнительном анализе и моделировании действий врача и специалиста по ИБ возникает противоречие между традиционным недостаточно строгим описанием ситуации принятия решения и необходимостью строгого выбора действия в этой ситуации. Для преодоления этого противоречия будем использовать метод построения моделей описания ситуации в том виде, как она воспринимается специалистом с точки зрения его профессиональных задач.

Как и для информации в сфере ИБ, для медицинской информации принципиальны: сравнительно небольшое количество больных (или инцидентов ИБ) в исследовании, неполнота доступных сведений о

каждом больном (соответственно – об инциденте ИБ), многочисленность возможных вариантов описания ситуации ("множественные описания"), взаимодействие этих вариантов в процессе принятия решения, постепенное увеличение объема и изменение формы представления знаний врача (эксперта по ИБ) о больном (инциденте ИБ) по мере продолжающегося их контакта.

Математические методы, описанные в [16], в отличие от традиционных статистических подходов, позволяют решать как информационные задачи медицинской диагностики, так и ИУ ИБ ТКС, несмотря на перечисленные затруднения.

Поясним сказанное конкретными примерами. Так, при построении модели представления знаний в адаптивной системе обнаружения вторжений возможно в качестве биологической аналогии использовать результаты исследования характеристик нелинейной динамики и хаоса модели противоопухолевого иммунитета [18].

В экспертной системе оценки рисков ИБ можно предложить использовать формальные структуры и языки представления знаний, используемые в медицинских экспертных системах, интеллектуальных системах поддержки принятия решений, прогноза и диагностики заболеваний [19], информационных системах медицинских исследований [20, 21].

Объектами исследования для данных классов задач применительно к соответствующим предметным областям являются: ТКС, живая природа (биосфера), биологический организм, человек и др.

В таком случае анализируемыми характеристиками могут являться соответственно: используемые коммуникационные протоколы и технологии передачи данных, тип коммутационного оборудования, программное обеспечение; биологический вид, генетический код ДНК; группа крови человека и т. п.

Применительно к каждому объекту исследования в соответствии с рассматриваемой задачей могут иметь место следующие угрозы: несанкционированный доступ к ресурсам ТКС, нарушение целостности, конфиденциальности или доступности информации; вирусное заболевание, раковая опухоль и т. п.

Уязвимостями будут являться: недостатки в реализации криптографических средств защиты информации либо слабые криптоалгоритмы (DES), незащищенные протоколы и технологии (TCP/IP, Bluetooth), ПЭМИН; ослабленная иммунная система, отсутствие иммунитета к определенным заболеваниям, генетическая предрасположенность и т. п.

Средствами реализации угроз будут: программные и аппаратные закладки, компьютерные вирусы, «жучки»; возбудители заболеваний, неблагоприятные факторы внешней среды и т. п. Средствами защиты от угроз будут: межсетевые экраны, антивирусы, иммунная система, антитела, лимфоциты, лекарства и т. п.

Рассмотренные выше классы задач имеют сходную структуру ММПЗ. Отмеченное сходство выражается в похожих наборах понятий, терминов, анализируемых характеристик исследуемых объектов и схем их описания, а также, как следствие, в некоторой аналогии процессов и алгоритмов экспертной оценки, что может быть использовано для определения единого конечного набора понятий, стандартизации процессов экспертизы, унификации алгоритмов ИУ.

В качестве общих рекомендаций по ИУ ИБ ТКС на основе «организмического подхода», обеспечивающго их выживание и долгосрочную устойчивость в условиях внешних и внутренних угроз безопасности можно предложить:

- адаптивное динамическое распределение ресурсов ИБ ТКС, направленное на их оптимизацию к хаотически изменяющемуся полю угроз безопасности;
- построение СИУ на базе управляемого совокупностью нечетких гибридных сетевых моделей проектирования и перепроектирования ключевых процессов ИБ ТКС.

Выводы

В данном исследовании в качестве нового методологического подхода предложен принцип биологической и медицинской аналогии как применительно к архитектуре ТКС и систем защиты информации, так и к процессам проектирования (зарождения, наследования), адаптации, развития и оптимизации систем интеллектуального управления безопасностью телекоммуникаций.

Предлагается проектировать ТКС в едином процессе со встроенными интеллектуальными средствами защиты информации, способными к адаптации к изменению поля угроз и использующими иммунно-подобные механизмы для распознавания и нейтрализации атак на информационные ресурсы ТКС.

Эффективность СИУ ИБ ТКС может быть значительно повышена за счет использования метазнаний, т. е. знаний о знаниях, которые как показано в данной работе, могут быть общими для таких предметных областей как ИБ, биология, медицина, иммунология. При этом метазнания не представляют некоторую единую сущность, а являются составными элементами метамоделей знаний различных предметных областей. Они могут применяться для достижения различных целей ИУ ИБ ТКС, таких как:

- метазнания в виде стратегических метаправил используются для выбора релевантных правил ИУ;
- метазнания используются для обоснования целесообразности применения правил из области экспертизы ИБ;
- метаправила используются для обнаружения синтаксических и семантических ошибок в предметных правилах ИУ;
- метаправила позволяют системе защиты информации адаптироваться к окружению путем перестройки предметных правил и функций ИУ;
- метаправила позволяют явно указать возможности и ограничения системы защиты информации, т. е. определить, что система знает, а что не знает.

Вопросы организации знаний в СИУ ИБ ТКС необходимо рассматривать комплексно и в любом представлении. Их решение в значительной степени не зависит от выбранной модели представления знаний и от конкретной задачи, но является общим по отношению к целому классу сходных задач и видов деятельности в рамках рассмотренных выше предметных областей. Это позволяет говорить об эффективности использования принципа биологической и медицинской аналогии в моделях представления знаний СИУ ИБ ТКС.

Направлениями дальнейшего исследования рассматриваемой проблемы будут являться: детализация и конкретизация предложенного методологического подхода путем разработки и практической реализации реальной СИУ ИБ ТКС, в МПЗ которой будет использован принцип биологической и медицинской аналогии.

Литература: ***1.*** *Recomendation CCITT X.200. Reference Model of open systems interconnection for CCITT applications. - Geneva. – 1991.* ***2.*** *Кучерявый А. Е., Кучерявый Е. А. От Е-России к U-России. Тенденции развития электросвязи // Электросвязь. - № 5. - 2005. - с. 10 - 12.* ***3.*** *Кононович В. Г., Тардаскін М. Ф. Парадигма інформаційної безпеки телебіометрики та сенсорних телекомунікаційних мереж // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - № 12. – 2006. – с. 56 – 66.* ***4.*** *Леваков А. Анатомия информационной безопасности США // JetInfo. - №6. – 2002.* http://www.jetinfo.ru/2002/6/1/article1.6.2002.html ***5.*** *Варламов О. О., Локотков А. А., Журавлева Э. М., Адамова Л. Е., Межуев Н. В. Системы искусственного интеллекта и компьютерные угрозы информационной безопасности // Искусственный интеллект.- №3. – 2004.* ***6.*** *Варламов О. О., Амарян М. Р., Адамова Л. Е., Межуев Н. В., Кузьменко Г. Н., Котов К. Ю., Кашинцева И. Ю. Роль интеллектуальных систем информационной безопасности для Рунета // Искусственный интеллект.- № 4. – 2005.* ***7.*** *Гладыш С. В. Модель нечеткой экспертной системы поддержки принятия решений по распределению ресурсов информационной безопасности // Сборник докладов X Международного молодежного форума «Радиоэлектроника и молодежь в XXI веке». - Харьков. - 2006.* ***8.*** *Гладыш С. В. Представление знаний в экспертной системе поддержки принятия решений по распределению ресурсов информационной безопасности информационно-телекоммуникационных сетей // Сборник докладов IV Международного молодежного форума «Информационные технологии и кибернетика». - Днепропетровск. - 2006.* ***9.*** *Гладыш С. В. Принцип биологической и медицинской аналогии в моделях представления знаний систем интеллектуального управления безопасностью телекоммуникаций // Сборник докладов международной научно-практической конференции «Информационные технологии и кибернентика на службе здравохранения ’2006». – Днепропетровск. – 2006.* ***10.*** *Провотар Я. Спосіб уніфікації форм подання знань в експертних системах // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - № 6. - 2003.* ***11.*** *Чернавский Д. С. Синергетика и информация: Динамическая теория информации. – Москва: Едиториал УРСС. – 2004 г. – 288 с.* ***12.*** *Моисеев Н. Н. Универсальный эволюционизм и коэволюция // Природа. – 1989. - №4. – с. 3 – 8.* ***13.*** *Моисеев Н. Н. Коэволюция природы и общества. Пути ноосферогенеза // Экология и жизнь. - 1997. - № 2.* ***14.*** *Pfeifer R., Scheier C. Understanding Intelligence. – The MIT Press, Cambridge MA. – 1999.* ***15.*** *Бондаренко М. Ф., Маторин С. И., Соловьева Е. А. Моделирование и проектирование бизнес-систем: методы, стандарты, технологии. – Харьков: СМИТ. – 2004. – 272 с.* ***16.*** *Котов Ю. Б. Новые математические подходы к задачам медицинской диагностики. – Москва: Едиториал УРСС. – 2004 г. – 328 с.* ***17.*** *Гладыш С. В. Организационно-методические аспекты экспертной оценки информационной безопасности телекоммуникационных систем // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - 2006. - № 12.* ***18.*** *Марценюк В. П. Исследование характеристик нелинейной динамики и хаоса в модели противоопухолевого иммунитета // Искусственный интеллект. - №3. - 2004.* ***19.*** *Кузнецов Д. А. Интеллектуальная система поддержки принятия решений прогнозирования заболеваний на основе нечёткой логики // Искусственный интеллект. - №3. - 2004.* ***20.*** *Короткова Т. И., Куртасова А. А. Интерактивный алгоритм обработки базы данных информационной системы медицинских исследований // Искусственный интеллект. - №4. - 2005.* ***21.*** *Марценюк В. П. Модели*

популяционной динамики в программной среде поддержки системных медицинских исследований // Искусственный интеллект. - №4. - 2005.

УДК: 621.391.7

ВИКОРИСТАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ ДЛЯ ЗАХИСТУ АВТОРСЬКОГО ПРАВА В ЗОБРАЖЕННЯХ

Юрій Яремчук, Василь Карпінець
Вінницький національний технічний університет

Анотація: **Запропоновано стеганографічний метод забезпечення захисту авторських прав в зображеннях за допомогою цифрових водяних знаків. Розроблений метод базується на дискретному косинус-перетворенні і згідно з методом цифровий водяний знак вбудовується в частотну область зображення шляхом зміни значень коефіцієнтів. Завдяки використанню низькочастотних коефіцієнтів та особливостям зміни їх значень метод має низку переваг над існуючими методами вбудовування цифрових водяних знаків.**
Summary: **In the given work is offered steganographic method for providing protection of the copyright in images by digital watermarks. The developed method is based on discrete cosine-transformation and according to method digital watermark embed in frequency area of the image by changing values of coefficients. Owing to use of low-frequency coefficients and insignificant changing of their values the method has a number of advantages before existing approaches of embedding digital watermarks.**
Ключові слова: **Стеганографія, цифровий водяний знак, захист авторського права, дискретне косинус-перетворення, JPEG.**

I Вступ

Завдяки масовому поширенню мультимедійних технологій і засобів телекомунікації розвиток комп'ютерної стеганографії вийшов на принципово новий рівень. Стеганографія включає в себе такі напрямки, як вбудовування інформації з метою її прихованої передачі, цифрових водяних знаків (ЦВЗ), ідентифікаційних номерів тощо. Одною з ключових задач, де активно використовуються стеганосистеми, є захист авторського права від так званого «піратства» [1]. При цьому на комп'ютерні графічні зображення наноситься спеціальна мітка (ЦВЗ), яка залишається невидимою для людини, але розпізнається спеціалізованим програмним забезпеченням.

Існуючі методи, що вирішують задачу захисту авторського права шляхом вбудовування ЦВЗ, можна розділити на дві групи [2]: група методів, які приховують інформацію в просторовій області зображення та методи, що вбудовують ЦВЗ в частотну область. Методи першої групи вбудовують інформацію безпосередньо в первинну область даних зображення, що робить їх нестійкими до багатьох спотворень, особливо до компресії з втратами (наприклад JPEG-компресія). Це призводить до часткового чи навіть повного знищення вбудованого ЦВЗ. Більш стійкими до різного роду спотворень та компресії є методи другої групи. До відомих методів відносяться методи на основі використання дискретного косинус перетворення (ДКП), дискретного перетворення Фур'є (ДПФ), вейвлет-перетворення, перетворення Карунена-Лоєва та ін. [2]. Найбільш поширеними перетвореннями в стеганографії є ДКП та вейвлет-перетворення, тому що крім можливості використання в стеганографічних перетвореннях, вони ефективно використовуються під час ущільнення зображень.

Основною вимогою вбудовування ЦВЗ є та, що стеганосистема повинна забезпечувати незмінність вбудованої інформації при спотворенні чи компресії зображення-контейнера та мінімальний вплив методу вбудовування ЦВЗ на якість самого зображення [3]. Серед стеганосистем, які вирішують ці задачі, виділяють декілька типів [2]: конфіденційні, напівконфіденційні, напіввідкриті та відкриті стеганосистеми. Така класифікація визначає, яка інформація потрібна системі для того, щоб виявити ЦВЗ – оригінал зображення, ЦВЗ, секретний ключ чи додаткова інформація. Стеганоситеми перших двох типів вимагають наявності оригіналу зображення чи ЦВЗ, та знання секретного ключа. Напіввідкриті стеганосистеми виявляють ЦВЗ за допомогою секретного ключа, який залежить від оригіналу зображення. Відкриті стеганосистеми для своєї роботи, окрім секретного ключа, не вимагають ні знання оригінального зображення, ні вбудованого ЦВЗ. Слід відзначити, що хоча більшість існуючих на сьогодні стеганосистем відносяться до конфіденційного або напівконфіденційного типу, перспективними є дослідження та розробка відкритих систем цифрових водяних знаків.

До стеганографічних методів, що представляють відкриті стеганосистеми та приховують інформацію в частотну область зображення, відносять відомі методи Коха і Жао, Бенгама-Мемона-Ео-Юнг та Фрідріха