Когнитивные информационные технологии в системах управления

УДК 004.56 DOI 10.25559/SITITO.2017.3.489

Актаева А.[1, 3], Ниязова Р.[2], Гагарина Н.[3], Бижигитова Д.[3], Кусаинова У.[1], Даутов А.[1], Шатенова Г.[4]

[1] Кокшетауский университет имени А. Мырзахметова, г. Кокшетау, Казахстан
[2] Евразийский национальный университет им. Л. Гумилева, г. Астана, Казахстан
[3] Алматинский технологический университет, г. Алматы, Казахстан
[4] Казахская академия транспорта и коммуникации им. М. Тынышбаева, г. Алматы, Казахстан

ИСКУССТВЕННЫЕ ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ДЛЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ: ПЕРСПЕКТИВЫ РАЗВИТИЯ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация

В статье обсуждается значимость в современном информационном обществе информационных ресурсов, требующих надежных методов защиты от НСД.

Рассматриваются основные принципы технологии и структура в области искусственной интеллектуальной системы для обнаружения вторжений, а также тенденция развития перспективных разработок инновационных технологии системы обнаружения вторжений. Экспериментальная разработка была реализована авторами на установке для многоканальной сети передачи данныхв рамках грантовой программы. Предложен метод повышения уровня информационной безопасности и защиты конфиденциальной информации путем разработок инновационных технологии системы обнаружения вторжений.

Ключевые слова

Информационные системы и сети; системы обнаружения вторжений; информационная безопасность; программные и аппаратно-программные средства; искусственные интеллектуальные системы.

Aktayeva A.[1,3], Niyasova A.[2], Gagarina N.[3], Bizhigitova D.[3], Kussainova U.[1], Dautov A.[1], Shatenova G.[4]

[1] Abai Myrzakhmetov Kokshetau University, Kokshetau Kazakhstan
[2] L. Gumilyiev Eurasian National University, Almaty, Kazakhstan
[3] Almaty Technological University, Almaty, Kazakhstan
[4] Kazakh Academy of Transport and Communications named after M. Tynyshpaev, Almaty, Kazakhstan

ARTIFICIAL INTELLIGENT INTRUSION DETECTION SYSTEMS: PERSPECTIVES OF INNOVATIVE TECHNOLOGIES

Abstract

The most popular development tools of the quantum cryptography technology are compared, the structure and the basic principles of its work is considered. In article the significance in the modern information society of the information resources requiring safe methods of protection against NSD is discussed. The structure and the basic principles of technology in the field of artificial intellectual system for detection of invasions and also a tendency of development of advanced developments innovative technologies of the system of detection of invasions is considered. Also describes the structure and basic principles of quantum cryptography technology based on properties of quantum systems. Quantum information are a physical quantity characterizing changes occurring in the system during the interaction between the information flow and the external environment. The exploratory

development has been experimentally realized by the authors at the facility for multi-channel data transmission network within the grant program. The method of increase in level of information security and protection of confidential information by development innovative is offered technology of the system of detection of invasions. In the article a method of increasing the level of information security and the protection of confidential information by the quantum artificial intellectual systems of quantum channels communication are considered.

Keywords

Corporate information systems and network intrusion detection systems; information security; software and hardware; anti-virus systems; artificial intellectual systems.

Введение

В настоящее время квантовая информатика представляет собой новую, быстро развивающуюся отрасль науки, связанную с использованием квантовых технологий для реализации принципиально новых методов инфо-телекоммуникации и вычислений: квантовая информация, квантовая информатика, квантовые каналы связи, квантовая криптография, квантовый компьютер, искусственные нейронные сети.

Квантовая информация — это физическая величина, характеризующая изменения, происходящие в системе при взаимодействии информационного потока с внешним окружением. Квантовая информация — это новый вид информации, который можно передавать, но нельзя размножать. Квантовый бит или кубит (qubit) описывается единичным вектором в двумерном комплексном векторном пространстве и представляет собой двухуровневую квантовую систему. В качестве кубитов могут выступать ионы, атомы, электроны, фотоны, спины атомных ядер, структуры из сверхпроводников и многие другие физические системы [8].

Квантовый бит или кубит — это вектор единичной длины в 2-мерном комплексном пространстве, в котором зафиксирован некоторый базис {|0⟩, |1⟩}, и любую комплексную линейную комбинацию 0 и 1 можно записать, как a|0⟩ +b|1⟩ [8].

Квантовые нейронные сети (КНС) являются одним из подвидов нейронных сетей и представляют собой комбинацию классических нейронных сетей и квантовых вычислений (см. рис. 1).

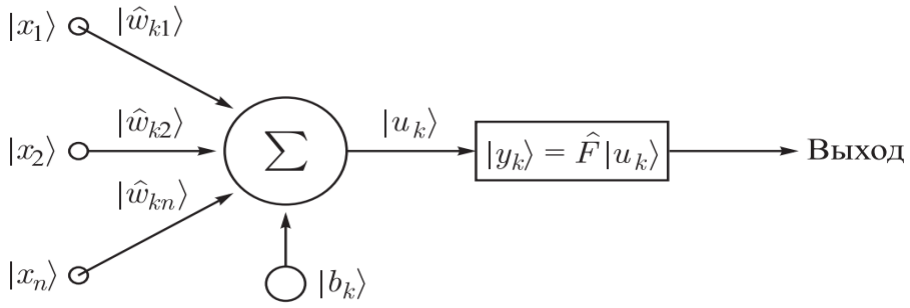

Рис. 1 – Блок-схема квантового нейрона [17]

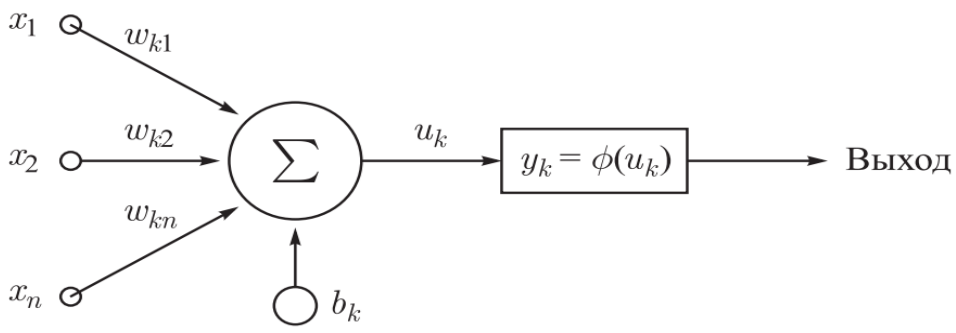

Рис. 2 – Блок-схема классической модели нейрона

Принципы построения и основные элементы КНС

Искусственные нейронные сети (ИНС) имеют некоторые привлекательные особенности: параллельность распределённой обработки, ошибкоустойчивость, способность обучаться и обобщать полученные знания. Под свойством обобщения понимается способность ИНС генерировать правильные выходы для входных сигналов, которые не были учтены в процессе обучения. Эти свойства делают ИНС системой переработки информации, которая решает сложные многомерные задачи, непосильные другим техникам [17].

Некоторая система может быть названа нейронной, если в ней удаётся идентифицировать, по крайней мере, один нейрон. Нейронная система является квантовой, если она способна реализовывать квантовые вычисления.

Существуют две главные причины интереса к квантовым нейронным сетям. Одна связана с аргументами, что квантовые процессы могут играть важную роль в работе мозга. Другая причина связана с бурным ростом квантовых вычислений, основные идеи которых вполне могли бы быть перенесены на нейро-вычисления, что открыло бы для них новые возможности. В настоящее время они обладают следующими преимуществами:

- устранение катастрофического забывания благодаря отсутствию интерференции образов;
- решение линейно-неразделимых проблем однослойной сетью;
- отсутствие соединений;
- высокая скорость обработки данных (1010 bits/s);
- миниатюрность (1011 нейронов/мм3);
- более высокая стабильность и надежность;
- экспоненциальная емкость памяти;
- лучшие характеристики при меньшем числе скрытых нейронов;
- быстрое обучение [17].

Эти потенциальные преимущества квантовых нейронных сетей мотивируют их разработку.

Существуют различные прототипы квантовых нейронных сетей. Некоторые из них очень схожи со своими классическими аналогами, в то время как другие используют квантовые операторы, которые не имеют классических эквивалентов, например, фазовые сдвиги. Различают широкий спектр различных структур КНС. Разные исследователи используют собственные аналогии для установления связи между квантовой механикой и искусственными нейронными сетями. Основные понятия этих двух областей приведены в таблице 1. Установление аналогии и является одной из главных задач теории квантовых нейронных сетей.

Эффективность использования нейронных сетей связана с массивной параллельной распределенной обработкой информации и нелинейностью преобразования векторов входов нейронами. Кроме того, квантовые системы обладают гораздо более мощным квантовым параллелизмом, выражающимся принципом суперпозиции [17].

КНС работает также, как и классическая ИНС, которая состоит из нескольких слоев персептронов – входной слой, 1 или несколько скрытых слоев и выходной слой. Каждый слой полностью связан с предыдущим слоем. Каждый скрытый слой вычисляет взвешенную сумму выходов предыдущего слоя. Если эта сумма превышает пороговое значение, узел переходит выше, иначе он остается ниже.

Таблица 1 – Аналогия между квантовой механикой и искусственными нейронными сетями

Классические нейронные сети		Квантовые нейронные сети	
Состояние нейрона	$x_j \in \{0,1\}$	Кубиты	$\|x\rangle = a\|0\rangle + b\|1\rangle$
Связь	$\{w_{ij}\}_{ij-1}^{p-1}$	Запутанность	$\|x_0 x_1 \ldots x_{p-1}\rangle$
Обучающее правило	$\sum_{s=1}^{p} x_i^s x_j^s$	Суперпозиция состояний запутанности	$\sum_{s=1}^{p} a_s \|x_0^s \ldots x_{p-1}^s\rangle$
Поиск победителя	$n = \max_i \arg(f_i)$	Интерференция как унитарное преобразование	$U : \Psi \to \Psi'$
Выходной Результат	N	Decoherence (измерение)	$\sum_s a_s \|x^s\rangle \to \|x^k\rangle$

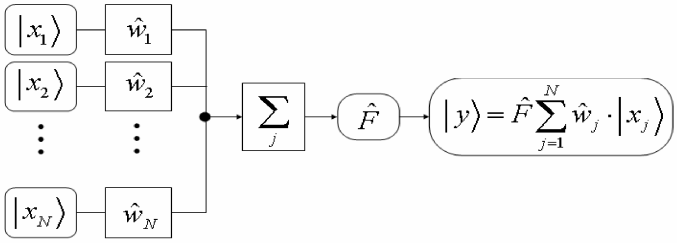

Рис. 3 – Математическая модель сигнала активации квантового нейрона [17]

Выходной слой делает то же самое, что и скрытые слои, кроме проверки точности. Сеть в целом вычисляет функцию путем проверки максимального выходного бита [17].

Определение принципа работы квантового нейрона: он получает входные сигналы или исходные данные либо выходные сигналы других нейронов КНС через несколько входных каналов. Каждый входной сигнал проходит через соединение, имеющее определенную интенсивность или вес; этот вес соответствует синаптической активности нейрона. С каждым нейроном связано определенное пороговое значение. Вычисляется взвешенная сумма входов, из нее вычитается пороговое значение и в результате получается величина активации нейрона и называется пост-синаптическим потенциалом нейрона – PSP.

Математическая модель сигнала активации квантового нейрона преобразуется с помощью функции активации и в результате получается выходной сигнал нейрона (см. рис. 3).

Математическая модель квантового нейрона $|y\rangle = F^{\wedge} \sum_{j=1}^{N} w^{\wedge} j\, |x\, j$, где $w^{\wedge}\, j$ – это матрицы 2*2, действующие на основе $\{|0\rangle, |1\rangle\}$; $F^{\wedge}$ – оператор, который может осуществлять работу сети квантовых ячеек.

Настоящее время целью и задачей системы обнаружения вторжений являются не только мониторинг и аудит событий информационных процессов, протекающих в КИСиС, а также анализ и прогнозирование этих событий в поисках признаков нарушения политики системы информационной безопасности. В зависимости от источника обнаружения вторжений различают следующие подсистемы (см. рис. 4).

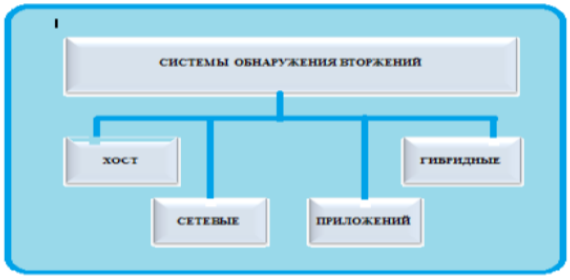

Рис. 4 – Классификация подсистем системы обнаружения вторжений

Класс задач, которые можно решить с помощью КНС, определяется тем, как сеть работает, и тем, как она обучается. При работе КНС принимает значения входных переменных и выдает значения выходных переменных. Таким образом, сеть можно применять в ситуации, когда имеется определенная известная информация и нужно из нее получить некоторую пока не известную информацию. Некоторые примеры таких задач в области защиты информации, которые можно решить с помощью КНС:

– распознавание образов и классификация;
– принятие решений и управление;
– кластеризация;
– прогнозирование;
– аппроксимация.

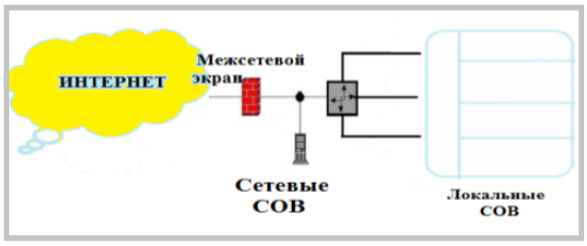

Рис. 5. Альтернативная структура компьютерной сети и системы с СОВ

Первый уровень идентифицирует вторжения, анализируя события и трафик, поступающий на отдельный компьютер, в то время как второй – исследует сетевой трафик. А системы уровня приложений, располагаются между web и SQL-серверами. На рисунке 5 представлена альтернативная структура компьютерной системы и сети с СОВ организации [2-4].

В свою очередь, как показывает практика, системы обнаружения вторжений, в зависимости от используемой технологии выявления различных типов атак и угроз, разделяют на два основных класса (см. рис. 5) [2].

Первые ориентируются на модель злонамеренного поведения (шаблон/сигнатура) и сравнивают модель с потоком событий информационного процесса. На основании сравнительного анализа система принимает решение блокировать тот или иной пакет, либо пропускать для взаимодействия непосредственно с инфраструктурой КИСиС.

Рис. 6. Классификация технологии системы обнаружения вторжений

Сигнатурные системы обнаружения вторжений обладают высокой производительностью и эффективностью обнаружения при сравнительно невысоких требованиях к аппаратному обеспечению. А недостатками сигнатурных систем обнаружения вторжений считаются:

- невозможность автоматического ввода новых сигнатур;
- отсутствие системы блокирования неизвестных сигнатур;
- отсутствие возможностей прогнозирования действий злоумышленника;
- отсутствие подсистемы мониторинга и аудита аппаратных ресурсов и др.

Главные недостаток существующих сигнатурных систем обнаружения вторжений, что они не могут профилировать перехваченный поток данных распределенных вторжений для их классификации и выработки сигнала о вторжении [1].

Для распознавания и обнаружения вторжений обычно применяются различные типы эвристических алгоритмов: комбинированные системы с эвристическим сканированием. Данный метод основанный на сигнатурах и эвристике, призван улучшить способность СОВ применять сигнатуры и распознавать модифицированные версии вторжений. Однако, данная технология, применяется очень осторожно, так как может повысить количество ложных срабатываний [1].

Системы обнаружения вторжений второго класса проектируются на основе моделей нормального поведения шаблона и ищут аномальные вхождения в поток событий информационного процесса для распознавания неизвестных вторжений. Задача исследования нормального и аномального поведения инфо-телекоммуникационных систем является очень сложной и комплексной. Поэтому ученые практики отмечают, что критериями анализа и оценки методов СОВ могут быть выбраны следующие параметры:

1) уровень наблюдения за системой;
2) верифицируемость метода (экспертная оценка корректности метода в процессе эксплуатации системы обнаружения вторжений);
3) адаптивность метода (устойчивость метода к малым изменениям при реализации атаки);
4) точность обнаружения вторжений и уровень ложных срабатываний и др [2-4].

Постановка задачи исследования

По данным материалов 7-й Международной конференции по систематизации компьютерных вирусов “VIRUS 97” еще в 1997 г была реализована искусственная иммунная система (ИИС) для киберпространства в рамках проекта фирмы IBM. На рисунке 7 представлена схема искусственной иммунной вычислительной системы [2-4].

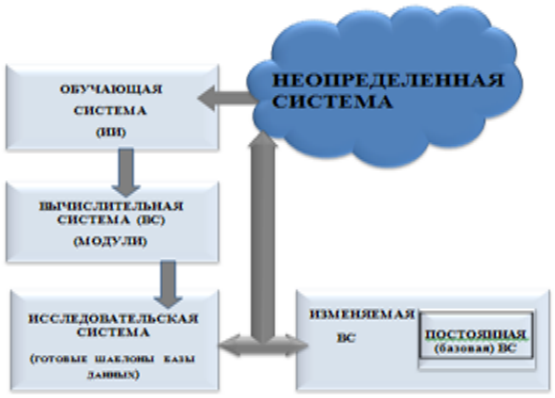

Рис 7. Схема искусственной иммунной вычислительной системы

В данной модели функционирование ИИС основывается на базовых положениях и механизмах биологической иммунной системы (генерация и детекторов, отбор нежелательных детекторов, клонирование и мутация детекторов, формирование иммунной памяти). На рисунке 8 приведена обобщенная схема механизма работы ИИС. Основные возможности ИИС предложенной модели:

1) непрерывное обновление иммунных детекторов;
2) обучение иммунных детекторов корректно классифицировать неизвестные образы;
3) автономность иммунных детекторов;
4) механизм «запрограммированной

смерти»;
5) клонирование и мутация;
6) наличие иммунной памяти адаптивной системы обнаружения вторжений.

В реализованной проекте фирмы IBM по созданию искусственной иммунной системы включены следующие этапы:

1) обнаружение неизвестных вирусов: врожденный иммунитет;
2) сбор данных образца вирусов (выделение и пересылка)
3) выработка вакцины (обновленной антивирусной базы);
4) адаптивная иммунная система;
5) доставка обновлении и распространение базы вакцинации (антител) [2-4].

Искусственная иммунная система (ИИС) должна содержать компоненты как врожденной, так и адаптивной иммунной защиты. По аналогии с врожденным иммунитетом, она должна иметь обобщенные механизмы распознавания вредных изменений, но этого недостаточно.

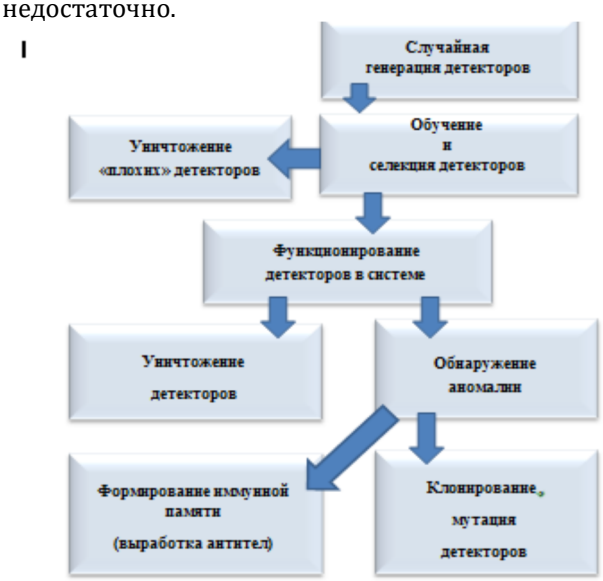

Рис. 8. Обобщенная схема механизма работы ИИС проекта «IBM – antivirus '" [2-4]

Как и адаптивный иммунитет биологической системы ИИС должна иметь в своем арсенале специфические механизмы распознавания и обнаружения вторжений. Объединяя эти весьма общие положения с рядом соображений практического характера, было сформулировано необходимый набор требований, которые должны быть выполнены для эффективного предотвращения вторжений:

1) врождённый иммунитет;
2) адаптивный иммунитет;
3) быстродействие;
4) модульное наращивание;
5) сохранность и надежность;
6) безопасность;
7) пользовательский контроль. [2-4]

Предпосылкой для создания эффективных систем обнаружения вторжений является развитие искусственных иммунных систем (ИИС) и нейросетевых технологий (ИНС), которые имеют биологические основы. Но большинство имеющихся на сегодняшний день искусственные иммунные системы обнаружения вторжений удовлетворяет лишь малой части перечисленных требований. Однако разработка и внедрение устойчивой комплексной системы защиты информации (КСЗИ) от быстро распространяющихся вторжений представляет собой трудную задачу и требует соблюдения всех перечисленных требований, ни одна из ныне существующих систем не обеспечивает такого уровня защиты [2-4].

Результаты исследований

Детальный анализ зарубежных разработок ИИС и ИНС позволил выделить основные перспективные направления развития эффективных систем обнаружения вторжений: нейропакеты, нейросетевые экспертные системы, антивирусные программы с включением ИИС и ИНС алгоритмов. Проведенный анализ литературных и открытых источников показывает отсутствие законченных решений в данном направлении. Поэтому актуальной задачей является разработка эффективных алгоритмов и методов гибридных систем обнаружения вторжений, которая позволяет обнаруживать неизвестные и базируется на интеграции искусственных иммунных систем и нейросетевых технологий на основе эволюционного программирования. Считаем, что способность таких систем к обучению и обобщению результатов позволяет создавать гибридные интеллектуальные системы обнаружения неизвестных вторжений.

В связи с интенсивным развитием инновационных технологий особое значение приобретают исследования в электронике, создании интеллектуальных программных и аппаратных продуктов прикладной информатики и квантовых технологий. Квантовая информация и технологии, основанные на ее необычных свойствах, в будущем повлияют на основы и дальнейшее развитие информационного пространства, а широкое применение квантовых технологий предполагает научно-техническую революцию, масштабы которой очень трудно представить. Распространение технологии квантовой связи является одним из перспективных и в то же

время реальных шагов в стратегических планах ряда стран Европы и США, Японии.

Теория квантовой информации кардинально изменит современные взгляды научного сообщества на основу системы информационной безопасности. Проведение экспериментов и исследований по обеспечению информационной безопасности представляет большой научный интерес по поиску решения основных задач и проблем, стоящих перед квантовыми криптографическими системами: задача детектирования единичных фотонов с высокой вероятностью в заданном квантовом состоянии при низком уровне ложных срабатываний, отсутствие управляемых источников одиночных фотонов, проблема увеличения дальности передачи и малая скорость генерации квантового ключа.

Применение квантовых технологий в области обеспечения системы информационной безопасности – одно из наиболее парадоксальных проявлений квантовой технологии, вызывающее в последние годы огромный интерес специалистов. в первую очередь, при передаче зашифрованных сообщений по двум более каналам связи – квантовому и традиционному. Квантовые нейросети является одним из самых стремительно развивающихся прикладных направлений квантовой информатики, и обеспечивает информирование о попытке перехвата передаваемой информации.

Заключение

Исследования в области квантовой информации могут привести не только к положительным последствиям, но и отрицательным. Квантовая криптография, основанная на применении квантовой нейросети, в будущем заменит используемые криптографические системы, и будет применяться наравне с обычными средствами инфотелекоммуникации. Актуальность и масштабность проблем, связанных с обеспечением информационной безопасности, с каждым днем будут возрастать, а развитие квантовой информации в ближайшем будущем принесет свои результаты и, возможно, приведет к существенному изменению научной картины мира в области ИТ.

Сегодня наблюдается тенденция перехода от программной к программно-аппаратной реализации нейросетевых алгоритмов с резким увеличением числа разработок СБИС нейрочипов с нейросетевой архитектурой. По данным открытой прессы, профинансированы исследования фирмы Microsoft по созданию искусственных иммунных и нейронных технологии по мониторингу и аудита обнаружения вторжений для будущих поколений ОС. Скорее всего, это означает, что область применения гидридных искусственных иммунно-нейронных технологии гораздо шире, поскольку большинство разработок все же засекречены. Поэтому мы считаем, что необходимо проводить весьма интенсивные и крупномасштабные исследования фундаментального и прикладного характера для решения задачи обеспечения надежной комплексной системы защиты информации в области информационной безопасности. Широкое применение квантовых информационных технологий предполагает научно-техническую революцию, масштабы которой сейчас даже трудно представить [8].

Литература

1. Искусственные иммунные системы и их применение / Под ред. Д. Дасгупты. – М.: Физматлит, 2006. – 344 с.
2. Безобразов, С.В., Головко В.А. Искусственные иммунные системы для защиты информации: обнаружение и классификация компьютерных вирусов // Материалы Всеросс. науч. конф., «Нейроинформатика», МИФИ, Москва, 20-23 янв. 2008. – Москва, 2008, 23-28 стр.
3. Безобразов С.В. Искусственные иммунные системы для защиты информации: применение LVQ сети // Нейроинформатика-2007: материалы IX Всеросс. науч.-техн. конф., Москва, МИФИ, 2007, 27-35 стр.
4. Безобразов С.В., Головко В.А. Искусственные иммунные системы для защиты информации: обнаружение и классификация компьютерных вирусов // Нейроинформатика-2008: материалы IX Всеросс. науч.-техн. конф., Москва, МИФИ, 2008, 23-27 стр.
5. Aktayeva A. and etc. *Security of information: using of quantum technologies* //International Journal of Open Information Technologies. -vol 4, № 4, 2016, 40-48 pp., – www.injoit.org
6. Актаева А.У., Илипбаева Л.И. Инновационные технологии в системе информационной безопасности: квантовые технологии // Современные инновационные технологии и ИТ- образование. -2014, том 1, № 1(9), 320-326 стр.
7. Кулик С. Классическая криптография // Фотоника 2010,2, 36-41 стр.
8. Холево А.С Математические основы квантовой информатики. – М.:2016, 125 с.
9. Курочкин В.Л. Экспериментальная установка для квантовой криптографии с одиночными поляризованными фотонами// Журнал технической физики, 2005, том 75, № 6
10. Глущенко Л.А., Моргунов К.К. Оценка защищенности информации в лазерных линиях связи // URL: http://www.oop-ros.org/maket2012/part1/ref1_2/1.3.2.pdf (дата обращения 01.10.2017)
11. Люгер Д. Ф. Искусственный интеллект, стратегии и методы решения сложных проблем. -М.: Вильямс, 2003. – 864 с.
12. Рассел С. И др. Искусственный интеллект: современный подход. – М.: Вильямс, 2007,1408 с.

13. Gorodetski V. I., Kotenko I. V., Karsaev O. Multi-agent technologies for computer network security: Attack simulation, intrusion detection and intrusion detection learning // International Journal of Computer Systems Science & Engineering. – 2003, № 4, 191–200 стр.
14. www.comsec.spb.ru
15. http://www.securitylab.ru /contest /299868.php (дата обращения 01.10.2017)
16. Aeppli G., Rosenbaum T. Quantum Annealing and Related Optimization Methods. – Heidelberg: Springer Verlag, 2007, vol.679, 159-169 pp.
17. Altaisky M., Rao V. Inverted Mexican Hat Potential in Activation of Receptor Cells // Nonlin. Analysis B. 2009, vol 10, №5, 2961-2970 pp.
18. Beck F. Synaptic Quantum Tunnelling in Brain Activity // Neuroquantology. 2008, vol 6, №2,140-151pp.
19. Beck F., Eccles J. Quantum Aspects of Brain Activity and the Role of Consciousness // PNAS. 1992, vol 89, 11357-11361pp.
20. Behera L., Kar I., Elitzur A. A Recurent Quantum Neural Network Model to Describe Eye Tracking of Moving Targets // Found. Phys. Lett. 2005. V.18, № 4, 357-370 pp

References

1. Artificial immune systems and their application / Under the editorship of D. Dasgupta. – M.: Fizmatlit, 2006. – 344 p.
2. Bezobrazov, S.V., Golovko V. A. Artificial immune systems for protection of information: detection and classification of computer viruses//Materials of Vseross. Naych.confernce Neyroinformatika, MEPhI, Moscow, 20-23 January. 2008. – Moscow, 2008. – 23-28 pp.
3. Bezobrazov S.V. Artificial immune systems for information security: application of LVQ network//Neuroinformatics-2007: materials IX of Vseross. science – tech. conference, Moscow, MEPhI, 2007, 27-35 pp.
4. Bezobrazov S.V., Golovko V. A. Artificial immune systems for information security: detection and classification of computer viruses//Neuroinformatics-2008. – Moscow, MEPhI, 2008. –23-27 pp.
5. Aktayeva A. and etc. Security of information: using of quantum technologies//International Journal of Open Information Technologies. – vol 4, №. 4, 2016, 40-48 pp. – www.injoit.org
6. Aktayeva A.U., Ilipbayeva L.I. Innovative technologies in an information security system: quantum technologies//Modern innovative technologies and IT education. -2014, vol 1, №1(9), 320-326 pp.
7. Sandpiper of Page. Classical cryptography//Photonics 2010,2, 36-41 pp.
8. Holevo A. S Mathematical fundamentals of quantum informatics. – M.:2016, 125 p.
9. Kurochkin V.L. Experimental installation for quantum cryptography with the single polarized photons//Magazine of technical physics, 2005, V.75, №6
10. Glushchenko L.A., Morgunov K.K. Cost of information security in laser communication lines// URL: http://www.oop-ros.org/maket2012/part1/ref1_2/1.3.2.pdf (circulation date 01.10.2017)
11. D. F. lugger. Artificial intelligence, strategy and methods of the solution of complex problems. – M.: Williams, 2003, 864 p.
12. Russell S. and etc. Artificial intelligence: modern approach. – M.: Williams, 2007, 1408 p.
13. Gorodetski V.I., Kotenko I.V., Karsaev O. Multi-agent technologies for computer network security: Attack simulation, intrusion detection and intrusion detection learning//International Journal of Computer Systems Science & Engineering. – 2003. – № 4,191-200 pp.
14. www.comsec.spb.ru
15. http://www.securitylab.ru/contest/299868.php (circulation date 01.10.2017)
16. Aeppli G., Rosenbaum T. Quantum Annealing and Related Optimization Methods. – Heidelberg: Springer Verlag, 2007, vol 679, 159-169 pp.
17. Altaisky M., Rao V. Inverted Mexican Hat Potential in Activation of Receptor Cells // Nonlin. Analysis B, 2009, vol 10, № 5, 2961-2970 pp.
18. Beck F. Synaptic Quantum Tunnelling in Brain Activity//Neuroquantology. 2008, vol 6, №. 2, 140-151pp.
19. Beck F., Eccles J. Quantum Aspects of Brain Activity and the Role of Consciousness// PNAS.1992, vol 89, 11357-11361 pp.
20. Behera L., Kar I., Elitzur A. A Recurent Quantum Neural Network Model to Describe Eye Tracking of Moving Targets// Found. Phys. Lett. 2005, vol 18, № 4, 357-370 pp.

Поступила: 22.10.2017

Об авторах:

Актаева Алкена, доктор Ph.D, доцент кафедры «Информационные технологии», Алматинский технологический университет, aaktaewa@list.ru

Ниязова Розамгуль, кандидат технических наук, доцент кафедры «Теоретическая информатика и информационная безопасность», Евразийский национальный университета им. Л. Гумилева, rosamgul@list.ru

Гагарина Надежда, dr.PhD, кандидат экономических наук, доцент кафедры «Информационные технологии», Алматинский технологический университет, ngagarina@mail.ru

Бижигитова Данакыз, dr.PhD, магистр технологии ИС, преподаватель кафедры «Информационные технологии», Алматинский технологический университет, bdana@mail.ru

Кусаинова Улжан, магистр технологии ИС, преподаватель «ИСИ», Кокшетауский университет им. А. Мырзахметова, aaktaewa@mail.ru

Даутов Айбек, магистр технологии ИС, преподаватель «ИСИ», Кокшетауский университет им.А. Мырзахметова, d.abeke@mail.ru

Шатенова Гульмира, магистрант, Казахская академия транспорта и коммуникации им. М. Тынышбаева, shatenova94@mail.ru

Note on the authors:

Aktayeva Alkena, doctor Ph.D, associate professor "Information technologies", Almaty technological university, aaktaewa@list.ru

Niyazova Rozamgul, Candidate of Technical Sciences, associate professor "A theoretical informatika and information security", L. Gumilyiev Eurasian National University, rosamgul@list.ru

Gagarina Nadezhda, doctor of PhD, Candidate of Economic Sciences, associate professor "Information technologies", Almaty technological university, ngagarina@mail.ru

Bizhigitova Danakyz, doctor of PhD, master of IS technology, teacher of Information Technologies department, Almaty technological university, bdana@mail.ru

Kusainova Ulzhan, master of IS technology, teacher of "ISI", Abai Myrzakhmetov Kokshetau University, ulzhan97@mail.ru

Dautov Aibek, MSc., dozent, department of Information systems and Informatics, A. Myrzakhmetov Kokshetau University, d.abeke@mail.ru

Shatenova Gulmira, undergraduate, Kazakh Academy of Transport and Communications named after M. Tynyshpaev, shatenova94@mail.ru