УДК 04.004

В.Е. Мухин, Я.И. Корнага, В.В. Стешин

АДАПТИВНЫЕ СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНЫХ СИСТЕМ НА ОСНОВЕ МОДИФИЦИРОВАННЫХ НЕЙРОННЫХ СЕТЕЙ КОХОНЕНА

V.Ye. Mukhin, Ya.I. Kornaga, V.V. Steshyn

ADAPTIVE SAFETY MECHANISMS FOR COMPUTER SYSTEMS BASED ON THE MODIFIED KOHONEN NEURAL NETWORKS

Предложен новый подход к обеспечению безопасности распределенных компьютерных систем на основе механизма нейронных сетей. Представлена комплексная адаптивная система защиты с интеллектуальным агентом на основе модифицированных нейронных сетей. Данная система позволяет реализовать адаптивное управление системой защиты информационной системы, обеспечить своевременное реагирование на угрозы безопасности, и оперативное автоматическое принятие решений по управлению параметрами системы защиты. Проведены экспериментальные исследования по определению уровня правильности обнаружения и распознавания угроз безопасности.

РАСПРЕДЕЛЕННЫЕ КОМПЬЮТЕРНЫЕ СИСТЕМЫ; НЕЙРОННАЯ СЕТЬ; ИНТЕЛЛЕКТУАЛЬНЫЙ АГЕНТ; КОМПЛЕКСНЫЕ АДАПТИВНЫЕ СИСТЕМЫ; ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ.

In the paper we propose a new approach to the safety ensurance for the distributed computer systems based on the neural network mechanism. There is described a complex adaptive safety support system with the intelligent agent based on the modified neural networks. This system allows to implement the adaptive control for the security mechanisms and to provide the in-time reaction to the security threats, and also to support the fast decisions making on the security mechanisms parameters modification. Also, we perform the experimental researches to evaluate the correctness level of the threats detection and recognition.

DISTRIBUTED COMPUTER SYSTEM; NEURAL NETWORK; INTELLECTUAL AGENT; COMPLEX ADAPTIVE SYSTEM; SAFETY ENSHURANCE.

Для работы с большими объемами данных и в случаях, когда требуется механизм быстрой обработки информации, используются распределенные компьютерные системы (РКС), структура которых во многом определяется отсутствием центра управления и распределения функций и ресурсов между всеми узлами системы. Типичный пример такой системы – сеть Интернет, обеспечивающая открытую и масштабируемую коммуникационную среду. Данный принцип является базовым для всех распределенных систем, что в целом снижает общий уровень их безопасности. В сети любой субъект может отправить пакет данных любому приемнику, при этом получатель должен обработать соответствующим образом полученный пакет данных.

Снижение уровня безопасности заключается в том, что злоумышленник может сформировать фальшивую учетную запись и практически безнаказанно генерировать и передавать вредоносный трафик. Таким образом, все соединенные узлы системы находятся в состоянии потенциальной опасности, поскольку присущее им свойство открытости делает их доступными для атакующей стороны. Методы обеспечения безопасности распределенных компьютерных систем, базирующиеся на стандартных методах проверки авторизационных данных, не могут в полной мере противодействовать этим угрозам.

Как свидетельствует статистика «Лаборатории Касперского» большинство атак в последние годы направлены на получение доступа к распределенной системе и запуск процессов с правами зарегистрированного пользователя, а также на специальную модификацию данных, генерацию DDoS-атак для отказа системных ресурсов или для создания эффекта перегрузки в системе. Также распространены атаки на уязвимости, позволяющие изменять данные, обходить систему защиты и проводить XSS-атаки [1].

Особенностями современных атак является увеличение сложности комплекса атакующих действий и соответствующего технологического уровня атак. Чаще всего атаки реализуют многоуровневый алгоритм и имеют распределенную структуру, что существенно увеличивает их опасность и последствия реализации. В результате особой задачей современных систем обеспечения безопасности распределенных систем является обработка и анализ большого объема данных, в частности, с использованием интеллектуального подхода. Системы защиты должны поддерживать распознавание и классификацию угрозы, а в случае отсутствия информации о типе атаки, адаптироваться к новому типу атакующих действий. Таким образом, ввиду приведенных выше требований к построению механизмов защиты распределенных систем, для повышения их защищенности предлагается использовать механизм нейронных сетей на основе интеллектуальных агентов.

Особенности и основные принципы построения адаптивных систем обеспечения защиты РКС

Обеспечение защиты распределенной компьютерной системы реализуется двумя путями. Первый путь заключается в попытке построения т. н. абсолютно защищенной системы, в которой постоянно усложняются процессы аутентификации, механизмов разграничения прав доступа и т. д. Однако данный путь имеет ряд недостатков. Во-первых, возникает проблема защиты от локальных легальных субъектов; во-вторых, сами протоколы аутентификации имеют уязвимости, а пароли могут быть похищены либо подобраны. Второй путь состоит в усложнении механизмов выявления аномалий в действиях субъектов по отношению к ресурсам и другим субъектам.

Среди существующих методов защиты распределенных компьютерных систем, предложенных в других работах, выделяются следующие: деревья принятия решения, Байесовская сеть, скрытая Марковская сеть, нечеткая логика, метод опорных векторов. Все данные методы подразумевают выполнение анализа исходных данных и реализуют алгоритм реагирования на угрозы, при этом наилучшие результаты по распознаванию новых и модифицированных угроз показывают системы на основе нейронных сетей, т. е. такие, в которых используется интеллектуальный подход к выявлению угроз в РКС [2, 3].

Одним из базовых компонентов таких систем является прототип биологического нейрона. На основе полученных входных данных и предыдущего опыта, полученного в виде заданных весов связей между входным и промежуточным слоями, генерируется результат, являющийся следствием активации нейрона [4, 5].

На рис. 1 изображен формальный нейрон как элемент нейронной сети. Объединение данной структуры в единую систему позволяет проанализировать входные параметры и с некоторой вероятностью ответить на вопрос, к какому классу или типу относится входная информация [6].

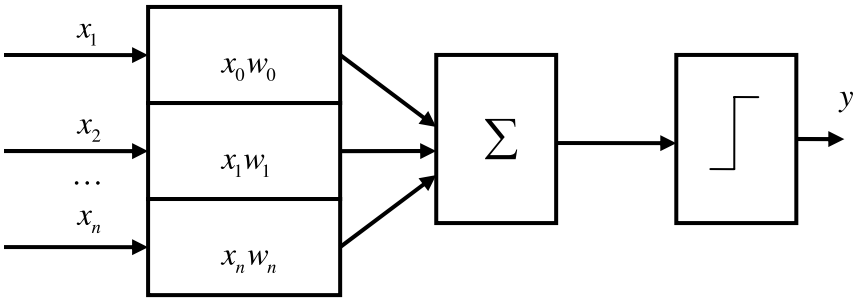

Рис. 1. Нейрон как элемент нейронной сети

Механизм обнаружения вторжений на основе модифицированной нейронной сети Кохонена

В целом нейронные сети характеризуются возможностью обучения. В отличие от обычных механизмов, они не имеют стандартного алгоритма выполнения и могут обучаться путем изменения коэффициентов связей между нейронами. В процессе обучения нейронная сеть способна выявлять сложные зависимости между входными и выходными данными и выполнять обобщение полученного образа [7]. По методу обучения нейронные сети делятся на требующие предварительного обучения и самообучающиеся сети. К числу последних относятся сети Кохонена, характеризующиеся структурно распределенной памятью, что позволяет избежать отказа сети в целом в случае отказа одного из нейронов. Данный эффект достигается за счет того, что классификацию входных данных выполняет не один нейрон, а целый кластер нейронов. Каждый входной вектор сигналов $X = \{x_1, x_2, ..., x_n\}$ поступает на вход каждого нейрона двумерной матрицы нейронов, а множество весов связей представляется в виде матрицы [8]:

$$W = \begin{pmatrix} w^{11} & w^{12} & w^{1j} \\ w^{21} & w^{22} & w^{2j} \\ w^{i1} & w^{i2} & w^{ij} \end{pmatrix}. \qquad (1)$$

Элементами данной матрицы являются векторы весовых коэффициентов связей $w^{ij} = \{w_1^{ij}, w_2^{ij}, ..., w_n^{ij}\}$. В начале обучения весовые коэффициенты нейронной сети задаются случайным образом из некоторого диапазона, далее вычисляется расстояние между входным вектором сигналов и множеством нейронов сети:

$$d_{ij} = \sum_{p=1}^{n} (x(t) - w_p^{ij}(t))^2, \qquad (2)$$

где $x(t)$ – входной вектор данных в момент времени t; $w_p^{ij}(t)$ – вектор весовых коэффициентов связей в момент времени t.

На третьем этапе выполняется поиск нейрона с координатами (i, j), для которого это расстояние является наименьшим. Далее выполняется изменение весов связей для обучения сети:

$$w^{ij}(t+1) = w^{ij}(t) + k(t)(x(t) - w^{ij}(t)), \qquad (3)$$

где $k(t)$ – коэффициент обучения (или скорость обучения), который уменьшается со временем.

Таким образом, сеть Кохонена обучается методом последовательных приближений. В процессе обучения на ее входы подаются данные, но при этом сеть подстраивается не под эталонное значение выхода, а под определенные закономерности во входных данных. Обучение начинается с выбранного случайным образом исходного расположения центров.

В процессе последовательной подачи на вход нейронной сети обучающих наборов определяется наиболее похожий нейрон, т. е. тот, у которого скалярное произведение весов и поданного на вход вектора является минимальным. Этот нейрон объявляется победителем и становится центром при подстройке весов соседних нейронов. Такое правило обучения предполагает «соревновательное» обучение с учетом расстояния нейронов от «нейрона-победителя». Суть

обучение при этом состоит не в минимизации ошибок распознавания, а в подстройке весов – внутренних параметров нейронной сети – для наиболее полного совпадения с входными данными.

Основой сети является скрытый слой Кохонена. Однако для улучшения результата анализа состояния системы и обнаружения вторжений предложена модификация нейронной сети Кохонена. При этом, как показано на рис. 2, скрытый слой нейронной сети Кохонена предложено разделить на две части или набора. Первый набор нейронов [1...f] отвечает за определение типа и класса атак, при этом изменение входных весов на выходном слое вызывает активацию линейной функции Y_1, значение нуль соответствует разрешенному состоянию системы, а единица – соответственно, атаке. Второй набор нейронов [n...m] анализирует нормальное состояние системы Y_2, что позволяет дополнить и уточнить результат выходного слоя класса атаки Y_1.

Модель данного механизма изображена на рис. 2.

Основой данной сети является скрытый слой Кохонена. Параметрами, которые используются в качестве входных данных для распознавания системных атак, являются:

сетевые записи и события;

данные о времени входа субъектов в систему и выхода из нее;

количество процессов;

индикаторы доступа к файлам;

временные интервалы доступа к ресурсам;

запросы к ресурсам и объектам компьютерной системы.

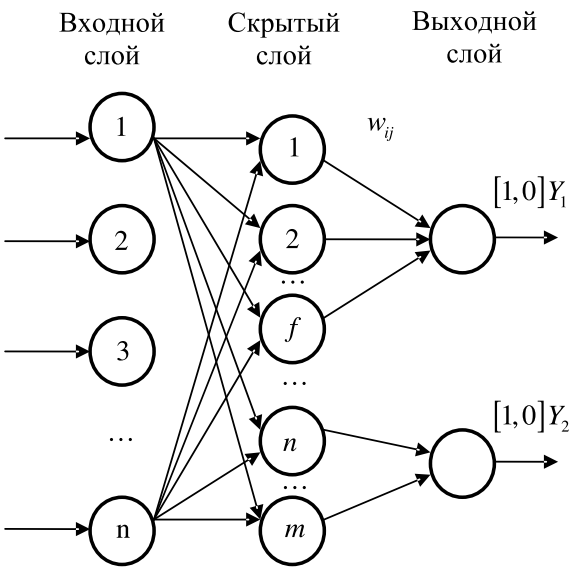

Рис. 2. Нейронная сеть для определения атаки

Далее интеллектуальный агент комплексной адаптивной системы защиты компьютерных систем использует механизм модифицированной нейронной сети для обнаружения и классификации потенциальных угроз безопасности. Входные параметры системы попадают на сенсор агента, который непрерывно считывает данные из соответствующей среды и передает их на входы нейронной сети. Кроме данных системы, интеллектуальный агент в качестве входной информации также может подавать данные о самом субъекте, его активностях и др.

После получения результата анализа нейронной сети по типу и классу атаки или по констатации нормального состояния системы данная информация передается через связи агента другим агентам, а также главному агенту администратора безопасности системы. Таким образом, информация о потенциальных угрозах анализируется всей структурой механизма обеспечения безопасности, что в целом повышает точность анализа возможности реализации угроз.

Поскольку мы используем нейронную сеть Кохонена в качестве скрытого слоя, все входные параметры подаются на матрицу нейронов, формируя полносвязную нейронную сеть. Важно отметить, что данный тип нейронной сети характеризуется значительным числом связей, следовательно, целесообразно выполнить некоторое упрощение и вербализацию нейронной сети за счет того, что элементы (входные параметры, нейроны, оказывающие минимальное влияние на корректность распознавания состояний) могут быть исключены из сети без существенного снижения качества распознавания [9].

Для выявления уязвимостей данный механизм может использовать настройки компьютерной сети, число ее пользователей, права пользователей, параметры их до-

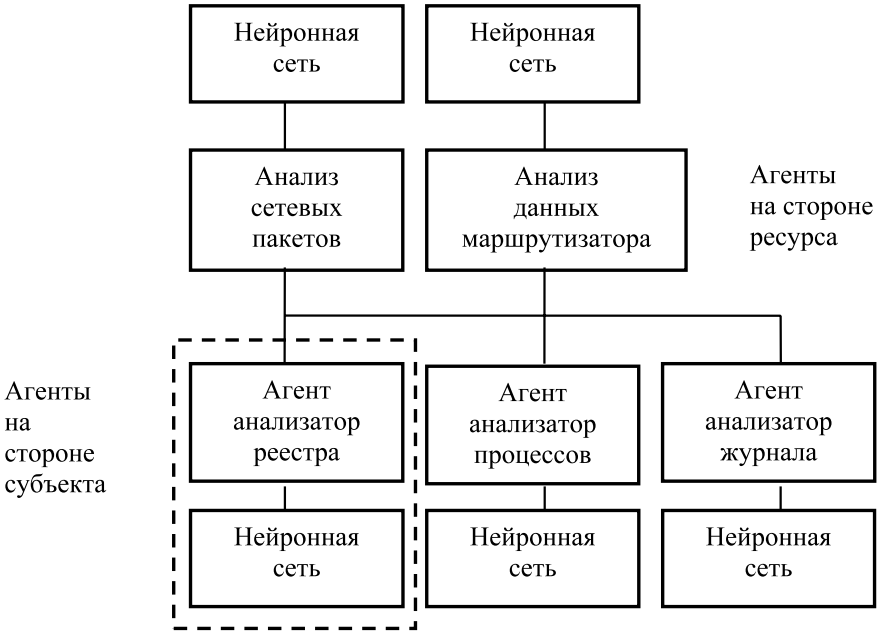

Рис. 3. Общая архитектура системы выявления атаки

ступа, число и типы портов, сетевые службы и настройки администратора.

Для выявления атакующих действий анализ и сбор данных требуется выполнять на нескольких уровнях распределенной компьютерной системы. Таким образом, использованы следующие исходные данные: данные о сетевых пакетах; данные журнала маршрутизатора; данные журнала безопасности операционной системы; данные реестра операционной системы и данные о процессах операционной системы.

Далее, на каждом уровне сбора информации прикрепляется выделенный интеллектуальный агент, как показано на рис. 3.

На рисунке изображена общая архитектура системы выявления атаки на основе механизма нейронной сети и интеллектуальных агентов. Каждый из прикрепленных интеллектуальных агентов включает свою собственную нейронную сеть, которая в рамках своего анализа выполняет классификацию угроз и атак. Соответственно, для повышения корректности распознавания

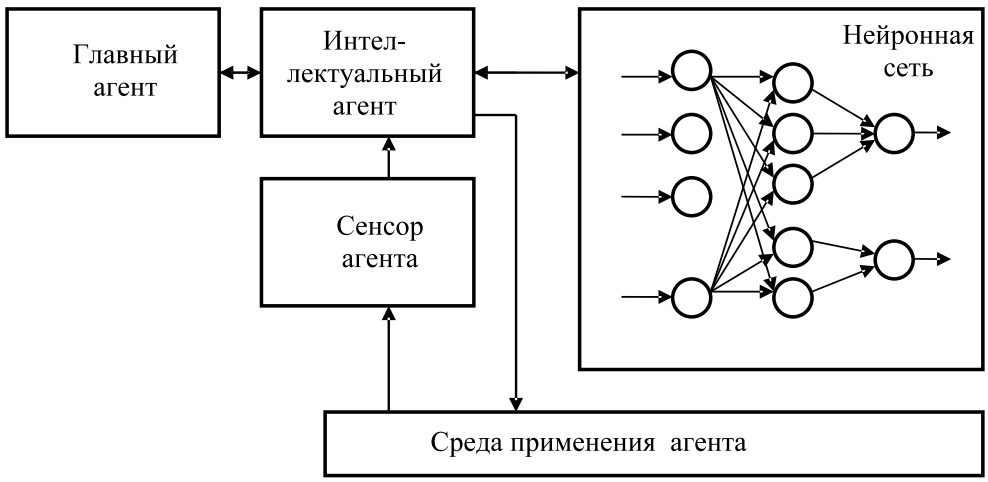

Рис. 4. Архитектура комплексной адаптивной системы защиты с интеллектуальным агентом на основе модифицированной нейронной сети

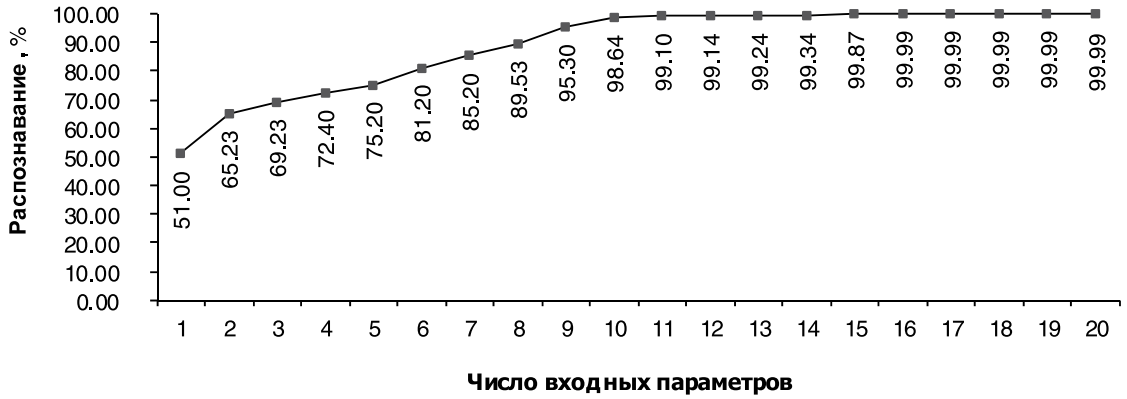

Рис. 5. Анализ результатов распознавания состояния РКС в зависимости от входных параметров

атак предлагается использование взаимодействующих между собой и с нейронной сетью интеллектуальных агентов. Схема взаимодействия интеллектуальных агентов и нейронной сети показана на рис. 4.

Экспериментальные исследования параметров адаптивной системы защиты

Проведены экспериментальные исследования корректности распознавания ситуации типа атака как числа выявленных вторжений со стороны предложенной адаптивной системы защиты на основе нейронной сети с интеллектуальным агентом. Для этого на вход нейронной сети, моделируемой с использованием специализированной среды, подавались различные наборы входных параметров, отражающих факт нарушения безопасности РКС. Число параметров в наборе изменялось от 1 до 20.

В ходе экспериментальных исследований установлено, что, в частности, при анализе выбранных DDoS-атак некоторые из параметров не имеют существенной роли в процессе распознавания. Как показывает рис. 5, при наличии более 11 входных параметров нейронной сети результаты распознавания незначительно отличаются друг от друга и, следовательно, их общее количество может быть снижено до этого числа.

Однако при появлении новых входных параметров для обучения при использовании данного метода могут измениться функции нейронной сети, и она может лишиться свойства обобщения. Таким образом, данный алгоритм снижения входных параметров целесообразно использовать именно в статических задачах, а не в задачах с динамически изменяющимися условиями.

В ситуации, когда число атак и их сложность постоянно увеличивается, организация безопасности распределенных компьютерных систем требует специального интеллектуального подхода, при котором система защиты способна обучаться и принимать решения по обеспечению безопасности автономно, при этом выявляя угрозы, классифицируя их по определенным признакам.

Разработан специальный программный комплекс на основе механизма нейронных сетей с использованием интеллектуальных агентов, позволяющий выявлять и классифицировать атаки на РКС. Предложенный механизм основан на модифицированных нейронных сетях Кохонена и характеризуется повышенной корректностью обнаружения атак, в т. ч. в условиях, когда отказал один из нейронов нейронной сети, ввиду того что классификацию атаки выполняет несколько нейронов – кластер нейронов. Кроме того, способность предложенного механизма анализировать состояние РКС без наличия полного набора параметров системы, как показали экспериментальные исследования, позволяет избежать некорректного результата в случае отсутствия ряда параметров или некорректного изменения их значений.

СПИСОК ЛИТЕРАТУРЫ

1. [Электронный ресурс] / URL: http://www.securelist.com/ru/analysis/208050810/DDoS_ataki_pervogo_polugodiya_2013_goda (дата обращения 2013)

2. **Андон Ф.И., Игнатенко А.П.** Атаки на отказ в сети Интернет: описание проблемы и подходов к ее решению. Киев, Препринт. НАН Украина. Ин-т программных систем, 2008. 50 с.

3. **Уланов А.В., Котенко И.В.** Защита от DDoS-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия // Защита информации INSIDE. 2007. № 1–3.

4. **Pushnoi G.S., Bonser G.L.** Method of Systems Potential as «Top-Bottom» Technique of the Complex Adaptive Systems Modelling // Intelligent Complex Adaptive Systems. Hershey-London, IGI-Publishing, 2008. Pp. 26–73.

5. Artificial Neural Networks for Misuse Detection. StudyMode.com [электронный ресурс] / URL: http://www.studymode.com/essays/Artificial-Neural-Networks-For-Misuse-Detection-63716.html (дата обращения Aug. 2005)

6. **Нестеренко Б.Б., Новотарский М.А.** Дискретные клеточные нейронные сети с обобщенным нейроном // Искусственный интеллект. 2007. № 4.

7. **Хайкин С.** Нейронные сети. 2-е изд. М.: ИД «Вильямс», 2008. 1103 с.

8. **Kohonen T.** Self-Organized Formation of Topologically Correct Feature Maps // Biological Cybernetics. 1982. No. 43(1). Pp. 59–69.

9. **Pham D.T., Ghanbarzadeh A., Koc E., Otri S., Rahim S., Zaidi M.** The Bees Algorithm – A Novel Tool for Complex Optimisation Problems Cardiff: Cardiff University, 2006. Pp. 454–459.

REFERENCES

1. Available: http://www.securelist.com/ru/analysis/208050810/DDoS_ataki_pervogo_polugodiya_2013_goda (Accessed 2013)

2. **Andon F.I., Ignatenko A.P.** *Ataki na otkaz v seti Internet: opisanie problemy i podhodov k ee resheniyu*. Kiev, Preprint, NAN Ukrainy, Institute porgrammnykh system, 2008, 50 p. (rus)

3. **Ulanov A.V., Kotenko I.V.** Zaschita ot DDoS-atak: mechanismy preduprezdenia, obnaruhenia, otslezhivania istochnika i protivodeistvia. *Zaschita informacii INSIDE*, 2007, No. 1–3. (rus)

4. **Pushnoi G.S., Bonser G.L.** Method of Systems Potential as «Top-Bottom» Technique of the Complex Adaptive Systems Modelling, *Intelligent Complex Adaptive Systems*, IGI-Publishing, Hershey-London, 2008, Pp. 26–73.

5. *Artificial Neural Networks for Misuse Detection. StudyMode.com* Available: http://www.studymode.com/essays/Artificial-Neural-Networks-For-Misuse-Detection-63716.html (Accessed Aug. 2005)

6. **Nesterenko B.B., Novotarsky M.A.** Discretnye kletochnye neironnye seti s obobschenym neironom, *Iskusstvennyi intellekt*, 2007, No. 4. (rus)

7. **Haykin S.** *Neironnye seti*, 2-e izd, ID «Willams» Publ., 2008, 1103 p. (rus)

8. **Kohonen T.** Self-Organized Formation of Topologically Correct Feature Maps, *Biological Cybernetics*, 1982, No. 43(1), Pp. 59–69.

9. **Pham D.T., Ghanbarzadeh A., Koc E., Otri S., Rahim S., Zaidi M.** *The Bees Algorithm – A Novel Tool for Complex Optimisation Problems*, Cardiff: Cardiff University, 2006, Pp. 454–459.

МУХИН Вадим Евгеньевич – *доцент кафедры вычислительной техники Национального технического университета Украины «Киевский политехнический институт», кандидат технических наук.*
02098, Украина, Киев, пр. Победы, д. 37.
E-mail: v_mukhin@mail.ru

MUKHIN, Vadym Ye. *National Technical University of Ukraine «Kiev Polytechnic Institute».*
02098, Pobedy Ave. 37, Kiev, Ukraine.
E-mail: v_mukhin@mail.ru

КОРНАГА Ярослав Игоревич – *старший преподаватель кафедры вычислительной техники Национального технического университета Украины «Киевский политехнический институт».*
02098, Украина, Киев, пр. Победы, д. 37.
E-mail: slovyan_k@ukr.net

KORNAGA, Yaroslav I. *National Technical University of Ukraine «Kiev Polytechnic Institute».*
02098, Pobedy Ave. 37, Kiev, Ukraine.
E-mail: slovyan_k@ukr.net

СТЕШИН Виктор Васильевич – *аспирант кафедры вычислительной техники Национального технического университета Украины «Киевский политехнический институт».*
02098, Украина, Киев, пр. Победы, д. 37.
E-mail: mail@webmarker.com.ua

STESHYN, Viktor V. *National Technical University of Ukraine «Kiev Polytechnic Institute».*
02098, Pobedy Ave. 37, Kiev, Ukraine.
E-mail: mail@webmarker.com.ua