УДК 004.056
doi:10.15217/issn1684-8853.2018.3.69

МЕТОД ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ НА ОСНОВЕ АНАЛИЗА ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ

И. С. Козин[a], *ведущий специалист, van@trioptimum.com*
[a]*АО «Кронштадт Технологии», Малый пр. В. О., 54, корп. 5, лит. П, Санкт-Петербург, 199178, РФ*

Постановка проблемы: *с развитием информационных технологий появляются новые классы средств защиты персональных данных при их обработке в информационных системах. Одним из классов средств защиты информации являются системы анализа поведения пользователей. При разработке средств анализа поведения все большее распространение получают методы машинного обучения, в том числе с применением математического аппарата теории искусственных нейронных сетей. Однако подходы к разработке средств защиты информации, основанные на машинном обучении, на сегодня изучены недостаточно.* ***Цель:*** *разработка метода создания искусственной нейронной сети, обеспечивающей проведение анализа санкционированного поведения пользователей информационной системы и выявление аномалий в поведении, сигнализирующих о совершении противоправных действий.* ***Результаты:*** *обзор подходов к обеспечению безопасности информации с применением искусственных нейронных сетей показал активное их развитие по разным направлениям, в том числе в направлении выявления аномалий. Разработан метод создания искусственной нейронной сети, включающий предложения по определению типа нейронной сети, области числовых значений входных и выходного сигналов, количества слоев и нейронов в слоях, метода обучения, а также типа активационных функций. В качестве входных значений предложено использовать характеристики поведения пользователя: набор данных, с которыми работает пользователь; место доступа к информационной системе; набор действий, которые совершает пользователь; время, в которое осуществляются доступ или определенные действия; общая продолжительность проводимых в течение определенного времени работ. На примере времени выполнения доступа пользователя предложен подход к присвоению характеристике пользователя числовых значений, основанный на применении математического аппарата теории нечетких множеств.* ***Практическая значимость:*** *обученная нейронная сеть обеспечивает более оперативное выявление аномалий в поведении пользователя, чем анализ специалиста по обеспечению безопасности информации без использования специальных средств автоматизации.*

Ключевые слова *— информационная безопасность, персональные данные, анализ поведения, искусственная нейронная сеть, теория нечетких множеств.*

Цитирование: Козин И. С. Метод обеспечения безопасности персональных данных при их обработке в информационной системе на основе анализа поведения пользователей// Информационно-управляющие системы. 2018. № 3. С. 69–78. doi:10.15217/issn1684-8853.2018.3.69
Citation: Kozin I. S. Providing Personal Data Protection in an Information System based on User Behavior Analytics. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 3, pp. 69–78 (In Russian). doi:10.15217/issn1684-8853.2018.3.69

Введение

Неблагоприятная геополитическая обстановка и активизация действий террористов обусловливают актуальность проблем обеспечения безопасности, одним из важнейших аспектов которой является информационная безопасность. С учетом положений Указа Президента [1] в качестве одного из основных направлений обеспечения безопасности информации можно выделить защиту персональных данных. Под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [2]. Примерами персональных данных являются паспортные данные, сведения о состоянии здоровья, политических взглядах, религиозных и философских убеждениях. Нарушение безопасности персональных данных может привести к материальному и моральному ущербу как для субъекта персональных данных, так и для организации-оператора персональных данных.

В настоящее время существует множество технических решений по обеспечению безопасности информации при ее обработке в информационной системе. Одним из таких решений являются системы управления информационной безопасностью (СУИБ). СУИБ начали получать активное распространение примерно с 2012 г., во время динамичного развития технологий аналитической работы с большими объемами данных и машинного обучения.

Одним из направлений развития СУИБ стала разработка систем анализа поведения пользователей (САПП). В задачи САПП входит анализ

действий пользователей (состав обрабатываемых данных, контроль используемых устройств и приложений, учет взаимодействий с другими пользователями и т. п.) и выявление аномалий в их поведении. В общем случае в ходе работы САПП каждому пользователю присваивается определенный уровень надежности, отражающий общую адекватность его поведения в удобном для восприятия администратором безопасности виде. Примерами практического применения САПП являются выявление аномальных действий, совершаемых от имени:

— служебных учетных записей (например, использование учетных записей, предназначенных для обеспечения определенных сервисов, в иных целях);

— привилегированных учетных записей (администратор домена осуществляет массовый сбор рабочих материалов пользователей и т. п.);

— учетных записей обычных пользователей (активный анализ доступных сетевых ресурсов, доступ в несвойственное для пользователя время или из несвойственного места, параллельный доступ из нескольких мест, резко возросшие объемы исходящего в Интернет трафика и т. п.).

Выявление аномалий, распределенных во времени или среди нескольких пользователей, как правило, затруднительно, если оно основано на применении экспертных систем, и требует значительных временных и вычислительных ресурсов. Из-за большого разнообразия действий пользователей даже регулярные обновления базы данных правил экспертной системы не способны гарантировать точной идентификации всего диапазона аномалий. Одним из подходов к устранению указанных затруднений может быть использование в составе САПП интеллектуальных подсистем, разработанных с помощью методик машинного обучения.

Машинное обучение является одним из направлений развития искусственного интеллекта и за счет применения различных математических аппаратов (таких как математическая статистика, теория вероятностей, численные методы оптимизации и т. п.) позволяет решать задачи классификации, кластеризации, систематизации, предсказания и регрессии. В направлении машинного обучения можно выделить искусственные нейронные сети (ИНС).

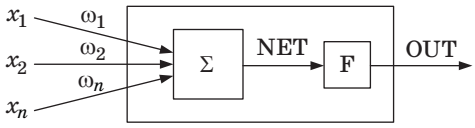
Развитие ИНС вдохновляется биологией. При работе с ИНС, рассматривая различные сетевые конфигурации и алгоритмы, исследователи применяют термины, заимствованные из принципов организации мозговой деятельности. В силу ограниченности знаний о работе мозга разработчикам ИНС приходится выходить за пределы современных биологических знаний в поисках структур, способных выполнять полезные функции [3]. Элементарной структурной единицей ИНС является искусственный нейрон [4–6], схематично представленный на рис. 1.

В общем случае основными элементами искусственного нейрона являются: входные сигналы x (соответствующие сигналам, приходящим в синапсы биологического нейрона), веса ω_n (на которые умножаются входные сигналы, соответствуют «силе» биологических синаптических связей), суммирующий блок $\sum$ (принимающий и суммирующий входные сигналы, соответствует телу биологического нейрона), выходной сигнал NET (создается суммирующим блоком, является алгебраической суммой взвешенных входов), активационная функция F (преобразующая выходной сигнал NET) и непосредственно выходной нейронный сигнал OUT. Математически нейрон может быть представлен формулой

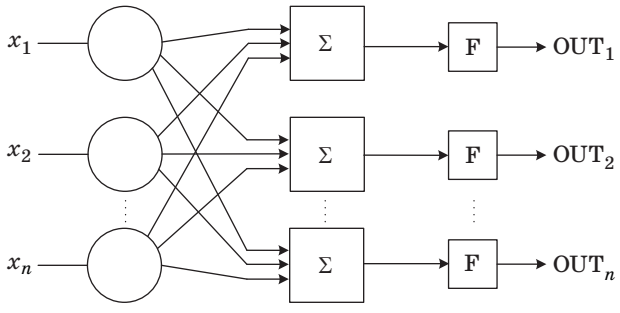
$$\mathrm{OUT} = f\left(\sum_{n=1}^{m}(x_n\omega_n)\right).$$

Один нейрон способен выполнять простейшие процедуры распознавания, однако для серьезных нейронных вычислений необходимо соединять нейроны в сети (рис. 2).

Способность ИНС обучаться, адаптироваться под новые типы поведений и распознавать их, даже если ранее она с ними не сталкивалась, придает системе защиты информации, разработанной с их применением, определенную гибкость. Обучают ИНС на определенной выборке приме-



■ ***Рис. 1.*** Обобщенная схема нейрона
■ ***Fig. 1.*** General scheme of the neuron



■ ***Рис. 2.*** Обобщенная схема однослойной ИНС
■ ***Fig. 2.*** General scheme of the one-layer neural network

ров, после чего ее реакция анализируется, и ИНС настраивается таким образом, чтобы достичь удовлетворительных результатов.

Обзор подходов к обеспечению безопасности с применением ИНС

Универсальность, которая изначально была заложена в ИНС, обусловливает активное развитие этого направления как в целом [4, 5, 7–9], так и в области обеспечения информационной безопасности: при защите от сетевых атак и вторжений [10–14], антивирусной защите [15], фильтрации спама [16, 17], анализе безопасности [18–20], анализе угроз [21, 22], разработке адаптивных средств защиты [23–25], выявлении аномалий [26] и пр. [27, 28]. В настоящее время существует большое количество разных конфигураций нейронных сетей с различными принципами функционирования [10]. Однако практически все они связаны с выбором и анализом некоторых частных видов структур с известными свойствами (сети Хопфилда, Гроссберга, Кохонена) [4, 29]. Как отмечается в работе [11], наиболее популярными и изученными являются следующие: многослойный персептрон, сети Кохонена, нейронные сети встречного распространения, сети Хопфилда и Хэмминга, сеть с радиальными базисными элементами (RBF), вероятностная нейронная сеть (PNN), обобщенно-регрессионная нейронная сеть (GRNN) и линейные нейронные сети. Использование существующих ИНС открывает широкие возможности в области обеспечения информационной безопасности, но вместе с тем оно связано и с рядом проблемных вопросов [4, 7, 30, 31].

Постановка задачи определения типа и основных характеристик ИНС

В настоящей статье предлагается метод обеспечения безопасности персональных данных при их обработке в информационной системе, основанный на проведении анализа санкционированного поведения пользователей информационной системы персональных данных с применением ИНС.

Предполагается, что каждый пользователь информационной системы персональных данных обладает набором характеристик, совокупность которых выражает его уникальное типовое поведение. К таким характеристикам предлагается отнести:

— набор данных, с которыми работает пользователь (файлы, папки, сетевые объекты, интернет-сайты и т. п.);

— место осуществления доступа к информационной системе персональных данных (конкретный компьютер, № помещения, здание, город, страна и т. п.);

— набор действий, которые выполняет пользователь (чтение, запись, копирование, модификация и т. п.);

— время, в которое осуществляется доступ или выполняются определенные действия (время суток, день недели, определенные числа и т. п.);

— общую продолжительность выполняемых в течение определенного времени действий.

Предложенный набор характеристик не является исчерпывающим, но позволяет построить уникальную модель поведения пользователя. Отступление от модели поведения (выявление аномалий в поведении) может свидетельствовать о совершении противоправных действий. Примерами таких действий являются:

— массовое удаление материалов, к которым имеет доступ пользователь (практикуется многими недовольными работниками при увольнении);

— использование чужой учетной записи (практикуется пользователями, несерьезно относящимися к правилам разграничения доступа);

— беспорядочное ознакомление или копирование корпоративной информации (практикуется любопытными пользователями и инсайдерами).

Каждая из представленных характеристик пользователя может быть рассмотрена применительно к группе пользователей. Таким образом, появляется возможность выявлять аномалии в поведении не только пользователя, но и групп. Такой подход может найти применение при сговоре среди пользователей и совершении санкционированных неправомерных действий, распределенных среди нескольких человек и потому особо затруднительных в выявлении.

Каждую характеристику пользователя (или группы пользователей) можно описать в виде коэффициентов x_n, $n \in \{1; 5\}$, где n выражает порядковый номер характеристики:

x_1 — набор данных, с которыми работает пользователь;

x_2 — точка доступа пользователя к ИСПДн;

x_3 — набор совершаемых пользователем действий;

x_4 — время осуществления доступа;

x_5 — общая продолжительность проводимых работ.

Близкий по своему составу набор характеристик поведения использовался ранее [32]. Совокупность характеристик поведения x обозначим вектором поведения $\mathbf{x}$.

В качестве математического аппарата выявления аномалий в поведении пользователя предлагается использовать теорию ИНС. Таким образом, на входе нейросети должно быть пять вход-

ных сигналов x_1–x_5, и построение ИНС сводится к решению следующих задач:

— определение типа необходимой ИНС;

— определение подхода к присвоению числовых значений входным сигналам ИНС, отражающим поведение пользователя или группы пользователей (x_1–x_5);

— определение необходимого количества слоев ИНС и количества нейронов в слоях ИНС;

— выбор метода обучения ИНС;

— выбор активационных функций;

— выбор области значений выходного сигнала NET, сигнализирующего о наличии аномалий в поведении пользователя или группы пользователей.

Построение ИНС

1. *Тип искусственной нейронной сети.*

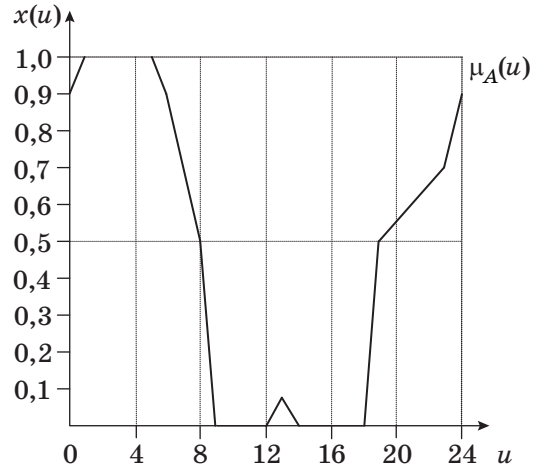
Поскольку на настоящий момент не существует строгой теории по выбору ИНС [27], за основу разрабатываемой ИНС предлагается взять хорошо изученный многослойный полносвязный персептрон без обратных связей.

2. *Вход.*

Для присвоения числовых значений входным сигналам ИНС предлагается использовать математический аппарат теории нечетких множеств, позволяющий присваивать вербальным характеристикам (более свойственно, менее свойственно и т. п.) числовые значения. Основной трудностью, мешающей применению теории нечетких множеств при решении практических задач, является то, что функция принадлежности должна быть задана вне самой теории и, следовательно, ее адекватность не может быть проверена непосредственно средствами теории. В каждом известном методе построения функции принадлежности формулируются свои требования и обоснования к выбору именно такого построения [33]. В рамках решаемой задачи предлагается рассматривать характеристики поведения пользователя x_n как характеристические функции принадлежности $\mu_A(u)$ множеству значений аномального поведения A, заданные на универсальном множестве U и принимающие значения, равные единице, на тех элементах множества U, которые принадлежат множеству A, и значения, равные нулю, на тех элементах, которые не принадлежат множеству A:

$$\mu_A(u) = \begin{cases} 1, \text{ если } u \in A \\ 0, \text{ если } u \notin A \end{cases}.$$

При этом для каждой функции принадлежности должны рассматриваться свои множества. В качестве примера на рис. 3 представлена диаграмма Заде, демонстрирующая возможную зависимость значения характеристической функции принадлежности $\mu_A(u)$ множеству значений аномального поведения A в зависимости от времени доступа пользователя к ресурсам сети, на которой:



■ ***Рис. 3.*** Диаграмма Заде

■ ***Fig. 3.*** Zade diagram

U — множество значений времени суток, в которое может быть осуществлен доступ к ресурсам сети, $U = \{u,\ u \in R : 0 \le u \le 24\}$;

A — множество значений времени суток, доступ в которое аномален для конкретного пользователя;

$\mu_A(u)$ — характеристическая функция принадлежности множеству значений времени суток, доступ в которое аномален для конкретного пользователя.

В предложенном примере предполагается следующее:

— продолжительность рабочего дня пользователя составляет девять часов (с девяти утра до шести вечера), включая перерыв на обед (в районе часа дня);

— пользователю не свойственно приходить на работу раньше начала рабочего дня, задерживаться по окончании рабочего дня и работать в околообеденное время.

Несущее множество аномального поведения можно записать следующим образом:

$$A = 0{,}9/0 + 1{,}0/1 + 1{,}0/5 + 0{,}9/6 + 0{,}5/8 + \\ + 0/9 + 0/12 + 0{,}1/13 + 0/14 + 0/18 + \\ + 0{,}5/19 + 0{,}7/23 + 0{,}9/24,$$

где запись, например, вида 0,9/0 выражает не деление на ноль, а значение функции принадлежности (в данном примере 0,9) при осуществлении доступа в полночь.

Общая форма записи нечетких подмножеств будет иметь следующий вид:

$$A = \sum_{u=0}^{24} \mu_A(u)/u = \sum_{u=0}^{0} 0{,}9/u + \sum_{u=1}^{1} 1{,}0/u + \sum_{u=5}^{5} 1{,}0/u + \sum_{u=6}^{6} 0{,}9/u + \sum_{u=8}^{8} 0{,}5/u + \sum_{u=9}^{9} 0/u + \sum_{u=12}^{12} 0/u + \sum_{u=13}^{13} 0{,}1/u + \sum_{u=14}^{14} 0/u + \sum_{u=18}^{18} 0/u + \sum_{u=19}^{19} 0{,}5/u + \sum_{u=23}^{23} 0{,}7/u + \sum_{u=24}^{24} 0{,}9/u,$$

где запись вида $\sum_{u=0}^{24} \mu_A(u)/u$ не предполагает сумму, но предполагает объединение по всем элементам конечного несущего множества значений u. Точками перехода ($x(u) = 0{,}5$) для функции принадлежности являются $u = 8$ и $u = 19$.

3. *Количество слоев и нейронов в слоях.*

Как показал А. Н. Колмогоров [34], любую непрерывную функцию n переменных на единичном отрезке [0; 1] можно представить в виде суммы конечного числа одномерных функций:

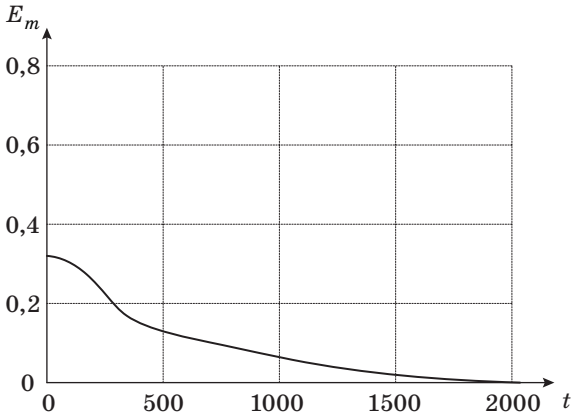
$$f(x_1, x_2, \ldots, x_n) = \sum_{p=1}^{2n+1} g\left(\sum_{i=1}^{n} \lambda_i \varphi_p(x_i)\right),$$

где функции g и φ_p являются одномерными и непрерывными; $\lambda_i = \text{const}$ для всех i. Из этого следует, что любую непрерывную функцию $f:[0;1]^n \to [0;1]$ можно аппроксимировать при помощи трехслойной нейронной сети, имеющей n входных, $2n + 1$ скрытых и один выходной нейрон. Данный результат обобщен на многослойную сеть с алгоритмом обратного распространения ошибки [35–37]. Таким образом, при построении ИНС предлагается использовать три слоя: первый слой будет включать в себя три нейрона, второй слой — семь нейронов, последний слой (выходной) — один нейрон.

4. *Метод обучения.*

В качестве метода обучения предлагается использовать алгоритм обратного распространения ошибки [38]. Данный алгоритм позволяет минимизировать среднеквадратичную ошибку ИНС. На рис. 4 продемонстрирована зависимость среднеквадратичной ошибки E_m от номера итерации t на примере прогнозирования функции $y = 0{,}1\sin(3x) + 0{,}5$ с 20 точками обучающей выборки и восемью предсказанными точками [39].

Согласно методу градиентного спуска изменение весовых коэффициентов и порогов нейронной сети происходит по следующему правилу:



■ ***Рис. 4.*** График убывания ошибки на обучающей выборке

■ ***Fig. 4.*** Graph of falling of error on the learning sample

$$\omega_{ij}(t+1) = \omega_{ij}(t) - \alpha \frac{\partial E}{\partial \omega_{ij}(t)}; \quad (1)$$

$$T_j(t+1) = T_j(t) - \alpha \frac{\partial E}{\partial T_j(t)}, \quad (2)$$

где $E = \frac{1}{2}\sum_j (y_j - t_j)^2$ — среднеквадратичная ошибка ИНС для одного образа.

В работе [40] показано, что

$$\frac{\partial E}{\partial \omega_{ki}} = \gamma_i F'(S_i)\gamma_k; \quad (3)$$

$$\frac{\partial E}{\partial T_i} = -\gamma_i F'(S_i), \quad (4)$$

где γ_i — выходное значение i-го нейрона.

В результате подстановки (3) и (4) в (1) и (2) получаются выражения, устанавливающие порядок изменения весовых коэффициентов и порогов нейронов, которого необходимо придерживаться для минимизации среднеквадратичной ошибки ИНС:

$$\omega_{ij}(t+1) = \omega_{ij}(t) - \alpha\gamma_j F'(S_j) y_i; \quad (5)$$

$$T_j(t+1) = T_j(t) + \alpha\gamma_j F'(S_j). \quad (6)$$

Выражения (5) и (6), называемые обобщенным дельта-правилом, определяют правило обучения многослойных ИНС в общем виде.

5. *Активационные функции.*

Для обеспечения сходимости алгоритма обратного распространения ошибки в качестве активационной функции предполагается использовать гиперболический тангенс. Таким образом, ИНС будет являться гомогенной, а выходное значе-

ние j-го нейрона определяться следующим образом:

$$y = \mathrm{tg}(S_j) = \frac{e^{S_j} - e^{-S_j}}{e^{S_j} + e^{-S_j}},$$

где S_j — взвешенная сумма j-го нейрона. Поскольку производная этой функции имеет вид $F'(S_j) = 1 - y_j^2$, правило обучения можно представить в виде

$$\omega_{ij}(t+1) = \omega_{ij}(t) - \alpha\gamma_j(1 - y_j^2)y_i;$$

$$T_j(t+1) = T_j(t) + \alpha\gamma_j(1 - y_j^2),$$

где t — номер итерации; α — значение шага обучения; γ_i — значение ошибки для i-го нейрона; T_j — значение порога j-го нейрона.

Ошибка для j-го нейрона выходного и скрытого слоев определяется следующим образом:

$$\gamma_j = y_j - t_j;$$

$$\gamma_j = \sum_i \gamma_i(1 - y_i^2)\omega_{ij}.$$

Для выполнения алгоритма обратного распространения ошибки необходимо выполнить следующие действия.

1. Задать значения шага обучения α $(0 < \alpha < 1)$ и желаемой среднеквадратичной ошибки E_m.

2. Придать случайные числовые значения весовым коэффициентам и пороговым значениям ИНС. В соответствии с рекомендацией, представленной в работе [41], весовым коэффициентам ω_{ij} предлагается придавать значения, примерно равные $\frac{1}{\sqrt{n(i)}}$, где $n(i)$ — число элементов в слое i.

3. Последовательно подать образы из обучающей выборки на вход ИНС. При этом для каждого входного образа необходимо выполнить следующие действия:

а) произвести фазу прямого распространения образа по ИНС, при этом вычисляется выходная активность всех нейронов ИНС

$$y_j = F\left(\sum_i \omega_{ij} y_i - T_j\right);$$

б) осуществить фазу обратного распространения сигнала, в результате которой определится ошибка нейронов γ_j для всех слоев ИНС. При этом, соответственно, для выходного и скрытого слоев

$$\gamma_j = y_j - t_j;$$

$$\gamma_j = \sum_i \gamma_i F'(S_i)\omega_{ji}, \qquad (7)$$

где i характеризует нейронные элементы следующего слоя по отношению к слою j;

в) изменить весовые коэффициенты и пороги нейронных элементов для каждого слоя ИНС в соответствии с (5) и (6):

$$\omega_{ij}(t+1) = \omega_{ij}(t) - \alpha\gamma_j F'(S_j)y_i;$$

$$T(t+1) = T_j(t) + \alpha\gamma_i F'(S_j).$$

4. Вычислить суммарную среднеквадратичную ошибку E:

$$E = \frac{1}{2}\sum_{k=1}^{L}\sum_j (y_j^k - t_j^k)^2,$$

где L — размерность обучающей выборки.

5. Если $E > E_m$, происходит переход к шагу 3, в противном случае алгоритм заканчивается. Таким образом, алгоритм функционирует до тех пор, пока суммарная среднеквадратичная ошибка ИНС не станет меньше заданной.

Для нейтрализации застраивания метода градиентного спуска в нежелательных минимумах предлагается применять метод тяжелого шарика [41]. В этом случае модификация синаптических связей ИНС будет осуществляться в соответствии с выражением

$$\Delta\omega_{ij}(t+1) = -\alpha\gamma_j F'(S_j)y_i + \xi\Delta\omega_{ij}(t),$$

где ξ — моментный параметр, выбираемый из диапазона [0; 1]. В соответствии с рекомендациями, представленными в работе [41], предлагается использовать значение $\xi = 0{,}9$.

6. *Выход.*

Для удобства интерпретации результата работы ИНС уместным является использование диапазона выходных значений от нуля (для обозначения отсутствия аномалии) до единицы (для обозначения наличия аномалии).

Однако с учетом выбора, сделанного в пользу использования в качестве метода обучения алгоритма обратного распространения ошибки (для гарантированной минимизации среднеквадратичной ошибки) и гиперболических тангенсов в качестве активационных функций (для обеспечения сходимости алгоритма обратного распространения ошибки), выходной сигнал NET будет принимать значения из диапазона от минус единицы до единицы. Таким образом, наличие аномалии в поведении пользователя предлагается интерпретировать выходом NET, равным единице, а отсутствие аномалии — выходом NET, равным минус единице.

Результаты определения типа и основных характеристик ИНС

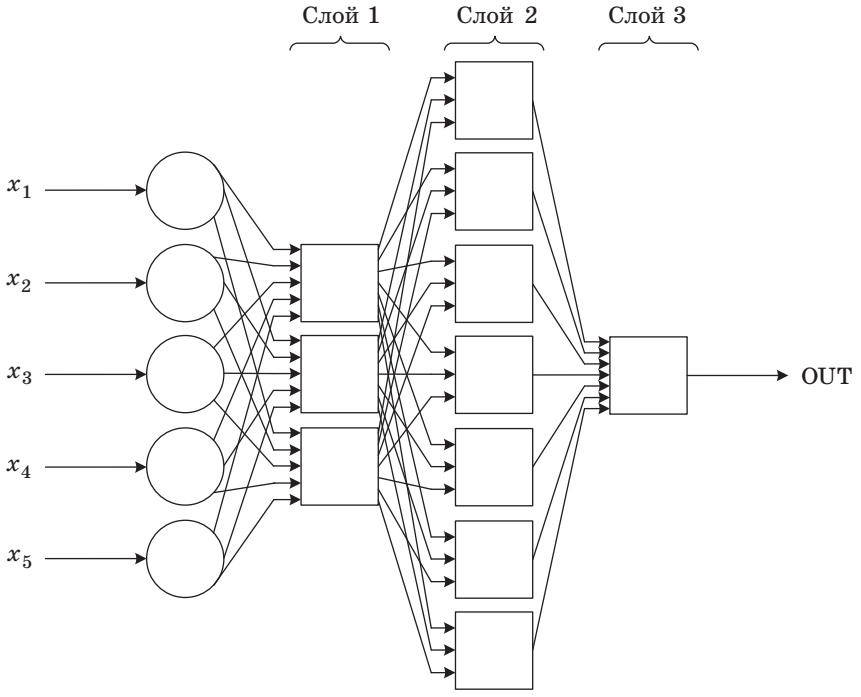
В качестве итоговой конфигурации был выбран трехслойный полносвязный гомогенный персептрон без обратных связей с пятью входными сигналами, одиннадцатью нейронами и гиперболическими тангенсами в качестве функций активации. В первом слое содержится три нейрона, в скрытом слое — семь и в выходном — один. Итоговая конфигурация подготовленной ИНС представлена на рис. 5.

При возрастании числа нейронов в скрытых слоях, с одной стороны, растет точность ИНС, но с другой — при слишком большой размерности скрытых слоев возникает явление перетренировки сети, ухудшающее обобщающие способности ИНС. Таким образом, число тренировочных образов должно быть больше числа нейронов в скрытом слое. В качестве обучающей выборки были взяты 30 комбинаций вектора **x**, выражающих наборы поведенческих характеристик пользователя и формирующих образы, подаваемые на вход ИНС. В связи с ограниченной областью значений гиперболического тангенса обучающая выборка была предварительно масштабирована к соответствующему диапазону значений. ИНС обучалась на обучающей выборке до достижения заданной среднеквадратичной ошибки. По окончании обучения для определения точности работы обученной сети использовалась тестовая выборка, состоящая из 10 комбинаций входных и выходных значений. При использовании тестовой выборки на входы сети подавались значения входов из тестовой выборки, затем значения полученных выходов сравнивались со значениями выходов тестовой выборки. В случае отличия значений полученных выходов от значений выходов тестовой выборки сеть проходила дообучение. Для итогового тестирования использовалась тестовая выборка, состоящая из пяти комбинаций.

Заключение

Рассмотрен актуальный подход к защите информации, основанный на применении технологии машинного обучения (теории искусственных нейронных сетей), отличающейся от известных уникальным составом характеристик поведения пользователя (составом входных характеристик ИНС) и подходом к выбору ИНС. Подготовлена выборка характеристик санкционированных действий пользователей. Данная выборка использовалась для обучения трехслойного персептрона. Обучение проводилось в программном обеспечении SPSS Statistics (разработка компании IBM), предназначенном для статистической обработки данных.

После обучения нейронной сети была проведена проверка эффективности ее работы с помощью контрольной выборки. Относительная погреш-



■ ***Рис. 5.*** Итоговая конфигурация ИНС
■ ***Fig. 5.*** Total configuration of neural network

ность классификации данных составила примерно 10 %, что является достаточно хорошим результатом. При обучении ИНС использовались небольшие выборки, предназначенные для демонстрации общих принципов работы ИНС. Для применения представленного подхода в решении реальных прикладных задач защиты информации выборки должны быть как можно больше.

Литература

1. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера». http://www.kremlin.ru/acts/bank/10638 (дата обращения: 20.05.2018).
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». https://rg.ru/2006/07/29/personaljnye-dannye-dok.html (дата обращения: 20.05.2018).
3. Основы теории нейронных сетей. http://www.intuit.ru/studies/courses/88/88/info (дата обращения: 06.12.2017).
4. **Круглов В. В., Дли М. И., Голунов Р. Ю.** Нечеткая логика и искусственные нейронные сети. — М.: Физматлит, 2001. — 224 с.
5. **Воронцов К. В.** Лекции по искусственным нейронным сетям. http://www.machinelearning.ru/wiki/images/c/cc/Voron-ML-NeuralNets.pdf (дата обращения: 02.04.2018).
6. **Лю Б.** Теория и практика неопределенного программирования. — М.: БИНОМ, 2005. — 416 с.
7. **Барский А. Б.** Нейронные сети: распознавание, управление, принятие решений. — М.: Финансы и статистика, 2004. — 176 с.
8. **Беркинблит М. Б.** Нейронные сети. — М.: МИРОС, 1993. — 96 с.
9. **Callan R.** The Essence of Neural Networks. — London: Prentice Hall Europe, 1999. — 248 p.
10. **Лукащик Е. П., Кочетов Д. А.** Применение нейронных сетей для обнаружения сетевых атак // Традиционная и инновационная наука: история, современное состояние, перспективы: сб. ст. по итогам Междунар. науч.-практ. конф./под ред. А. А. Сукиасяна. — Стерлитамак: Агентство международных исследований, 2017. С. 24–27.
11. **Зубков Е. В., Белов В. М.** Методы интеллектуального анализа данных и обнаружения вторжений // Вестник СибГУТИ. 2016. № 1. С. 118–133.
12. **Частикова В. А., Картамышев Д. А.** К вопросу защиты информации от сетевых атак на основе нейронных сетей // Науч. тр. Кубанского государственного технологического университета. 2014. № 6. С. 101–104.
13. **Кондратьев А. А., Талалаев А. А., Тищенко И. П., Фраленко В. П., Хачумов В. М.** Методологическое обеспечение интеллектуальных систем защиты от сетевых атак // Современные проблемы науки и образования. 2014. № 2. С. 119.
14. **Васильев В. И., Шарабыров И. В.** Обнаружение атак в локальных беспроводных сетях на основе интеллектуального анализа данных // Изв. ЮФУ. Технические науки. 2014. № 2(151). С. 57–67.
15. **Zhi-Peng Pan, Chao Feng, Chao-Jing Tang.** Malware Classification based on the Behavior Analysis and Back Propagation Neural Network. ITM Web of Conferences 7, 02001. 2016. P. 1–5. https://www.itm-conferences.org/articles/itmconf/pdf/2016/02/itmconf_ita2016_02001.pdf (дата обращения: 02.03.2018). doi:10.1051/itmconf/20160702001
16. **Ларионова А. В., Хорев П. Б.** Метод фильтрации спама на основе искусственной нейронной сети // Науковедение. 2016. Т. 8. № 3(34). https://naukovedenie.ru/PDF/04TVN316.pdf (дата обращения: 03.04.2018).
17. **Ларионова А. В., Хорев П. Б.** Оценка эффективности фильтрации спама на основе искусственной нейронной сети // Науковедение. 2016. Т. 8. № 2(33). https://naukovedenie.ru/PDF/134TVN216.pdf (дата обращения: 03.04.2018).
18. **Трапезников Е. В., Данилова О. Т.** Модель анализа защиты информации на основе нейронной сети // Динамика систем, механизмов и машин. 2016. Т. 2. № 1. С. 302–308.
19. **Данилова О. Т., Трапезников Е. В.** Разработка модели, анализирующей функцию безопасности в системе информационной защиты, на основе нейронной сети // Информационное противодействие угрозам терроризма. 2015. № 24. С. 24–29.
20. **Гильмуллин Т. М., Гильмуллин М. Ф.** Подходы к автоматизации процесса валидации уязвимостей, найденных автоматическими сканерами безопасности, при помощи нечетких множеств и нейронных сетей // Фундаментальные исследования. 2014. № 11. Ч. 2. С. 266–279.
21. **Цырульник В. Ф., Кадочникова Н. А.** Оценка актуальности угроз информационной безопасности с помощью программной реализации обученной нейронной сети // Научный альманах. 2016. № 4–3(18). С. 211–215.
22. **Соловьев С. В., Мамута В. В.** Применение аппарата нейросетевых технологий для определения актуальных угроз безопасности информации информационных систем //Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8. № 5. С. 78–82.
23. **Мухин В. Е., Корнага Я. И., Стешин В. В.** Адаптивные средства защиты компьютерных систем на основе модифицированных нейронных сетей Кохонена // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2014. № 2(193). С. 31–38.
24. **Штеренберг С. И., Виткова Л. А., Просихин В. П.** Методика применения концепции адаптивной са-

моразвивающейся системы // Информационные технологии и телекоммуникации. 2014. № 4(8). С. 126–133.
25. **Котенко И. В., Нестерук Ф. Г., Шоров А. В.** Гибридная адаптивная система защиты информации на основе биометафор «нервных» и нейронных сетей // Инновации в науке. 2013. № 16-1. С. 79–83.
26. **Вишняков В. А., Коваль О. И., Моздурани Шираз М. Г.** Использование нейронных сетей для обнаружения и распознавания аномалий в корпоративной информационной системе предприятия // Докл. Белорусского государственного университета информатики и радиоэлектроники. 2016. № 4(98). С. 86–92.
27. **Улезло Д. С., Кадан А. М.** Методы машинного обучения в решении задач информационной безопасности // Intelligent Technologies for Information Processing and Management (ITIPM'2015): Proc. of the 3rd Intern. Conf. 2015. С. 41–44.
28. **Цветкова О. Л., Крепер А. И.** О применении теории искусственных нейронных сетей в решении задач обеспечения информационной безопасности // Символ науки. 2017. № 04-2. С. 105–107.
29. **Галушкин А. И.** Нейрокомпьютеры и их применение. — М.: ИПРЖР, 2000. — 416 с.
30. **Щавелев Л. В.** Способы аналитической обработки данных для поддержки принятия решений. http://infovisor.ivanovo.ru/press/paper04.html (дата обращения: 03.04.2018).
31. **Хайкин С.** Нейронные сети: полный курс. — М.: Вильямс, 2006. — 1104 с.
32. **Shelestov A., Skakun S., Kissul O.** Complex Neural Network Model of User Behavior in Distributed System// Knowledge-Dialogue-Solutions: Intern. Conf. 2007. P. 1–8. http://inform.ikd.kiev.ua/content/ua/publications/articles/content/KDS07-Shelestov_Skakun_Kussul.pdf (дата обращения: 02.03.2018).
33. **Ronald R. Yager.** Fuzzy Set and Possibility Theory: Recent Developments. — N. Y.: Pergamon, 1982. — 408 p.
34. **Колмогоров А. Н.** О представлении непрерывных функций нескольких переменных в виде суперпозиций непрерывных функций одного переменного и сложения // Докл. АН СССР. 1957. Т. 114. С. 953–956.
35. **Hornik K., Stinchcombe M., White H.** Multilayer Feedforward Networks are Universal Approximators// Neural Network. 1989. N 2(5). P. 359–366.
36. **Rojas R.** Theorie der Neuronalen Netze: Eine Systematische Einführung. — Berlin: Springer-Verlag, 2013. — 446 p.
37. **Maxwell T., Giles C. L., Lee Y. C., Chen H. H.** Nonlinear Dynamics of Artificial Neural Systems // AIP Conf. Proc. 1986. Vol. 151. P. 299–304. doi:10.1063/1.36227
38. **Rumelhart D., Hinton G., Williams R.** Learning Representations by Back-Propagating Errors// Nature. 1986. Vol. 323. P. 533–536. doi:10.1038/323533a0
39. **Рудой Г. И.** Выбор функции активации при прогнозировании нейронными сетями // Машинное обучение и анализ данных. 2001. Т. 1. № 1. С. 16–39.
40. **Головко В. А.** Нейронные сети. Обучение, организация и применение. — М.: ИПРЖР, 2001. — 256 с.
41. **Hertz J., Krogh A., Palmer R.** Introduction to the Theory of Neural Computation. — Redwood City: Addison Wesley, 1991. — 327 p.

UDC 004.056
doi:10.15217/issn1684-8853.2018.3.69

Providing Personal Data Protection in an Information System based on User Behavior Analytics

Kozin I. S.[a], Lead Specialist, van@trioptimum.com
[a]JSC «Kronstadt Technologies», 54, Bldg 5, Litas P, Malyi Pr. V. O., 199178, Saint-Petersburg, Russian Federation

Introduction: As information technologies develop, new classes of personal data protection software come out. One of them is User Behavior Analytics. In the development of such systems, machine learning methods are widely used, including the applications of artificial neural network theory. However, the approaches to protection software development based on machine learning have not been studied well enough. **Purpose:** Developing a method of creating an artificial neural network which would provide the analysis of authorized behavior of information system users and the detection of abnormalities in their behavior signaling about criminal activity. **Results:** A review of the approaches to provide information security with artificial neural networks demonstrates their active development in several directions, including the detection of abnormalities. A new method to create an artificial neural network has been developed, including the proposals about determining the network type, the range of numeric values for the input and output signals, the number of the layers and neurons in a layer, the learning method, and the type of the activation functions. As the input values, user behavior characteristics can be used, namely: a set of the user's data, the point of access to the information system, the set of user's actions, the time of the access or time of certain actions, the general duration of runtime operations. With user's access time as an example, an approach has been proposed to assign numeric values to the characteristic of a user, based on fuzzy set theory application. **Practical relevance:** A trained neural network provides a more efficient detection of abnormalities in user behavior than an information security specialist without special automation tools.

Keywords — Information Security, Personal Data, Behavior Analytics, Artificial Neural Networks, Fuzzy Set Theory.

Citation: Kozin I. S. Providing Personal Data Protection in an Information System based on User Behavior Analytics. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 3, pp. 69–78 (In Russian). doi:10.15217/issn1684-8853.2018.3.69

References

1. Ukaz Prezidenta RF ot 06.03.1997 N 188 "Ob utverzhdenii perechnia svedenii konfidentsial'nogo kharaktera". Available at: http://www.kremlin.ru/acts/bank/10638 (accessed 20 May 2018).
2. Federal'nyi zakon ot 27.07.2006 N 152-FZ "O personal'nykh dannykh". Available at: https://rg.ru/2006/07/29/personaljnye-dannye-dok.html (accessed 20 May 2018).
3. *Osnovy teorii neironnykh setei* [The Fundamentals of the Theory of Artificial Neural Networks]. Available at: http://www.intuit.ru/studies/courses/88/88/info (accessed 6 December 2017).
4. Kruglov V. V., Dli M. I., Golunov R. Iu. *Nechetkaia logika i iskusstvennye neironnye seti* [Fuzzy Logic and Artificial Neural Networks]. Moscow, Fizmatlit Publ., 2001. 224 p. (In Russian).
5. Vorontsov K. V. *Lektsii po iskusstvennym neironnym setiam* [Lectures on Artificial Neural Networks]. Available at: http://www.machinelearning.ru/wiki/images/c/cc/Voron-ML-NeuralNets.pdf (accessed 2 April 2018).
6. Liu B. *Teoriia i praktika neopredelennogo programmirovaniia* [Theory and Practice of Indefinite Programming]. Moscow, BINOM Publ., 2005. 416 p. (In Russian).
7. Barskii A. B. *Neironnye seti: raspoznavanie, upravlenie, priniatie reshenii* [Neural Networks: Recognition, Management, Decision Making]. Moscow, Finansy i statistika Publ., 2004. 176 p. (In Russian).
8. Berkinblit M. B. *Neironnye seti* [Neural Networks]. Moscow, MIROS Publ., 1993. 96 p. (In Russian).
9. Callan R. *The Essence of Neural Networks*. London, Prentice Hall Europe, 1999. 248 p.
10. Lukashchik E. P., Kochetov D. A. The use of Neural Networks to Detect Network Attacks. *Scientific Collection "Traditsionnaia i innovatsionnaia nauka: istoriia, sovremennoe sostoianie, perspektivy"* [Traditional and Innovative Science: History, Current State, Prospects], eds. A. A. Sukiasian, Sterlitamak, Agentstvo mezhdunarodnykh issledovanii Publ., 2017, pp. 24–27 (In Russian).
11. Zubkov E. V., Belov V. M. Methods of Data Mining and Intrusion Detection. *Vestnik SibGUTI*, 2016, no. 1, pp. 118–133 (In Russian).
12. Chastikova V. A., Kartamyshev D. A. To the Issue of Protection of Information from Network Attacks based on Neural Networks. *Nauchnye trudy Kubanskogo gosudarstvennogo tekhnologicheskogo universiteta* [Scientific Collection of Kuban State Technical University], 2014, no. 6, pp. 101–104 (In Russian).
13. Kondrat'ev A. A., Talalaev A. A., Tishchenko I. P., Fralenko V. P., Khachumov V. M. Methodological Provision of Intelligent Systems to Protect against Network Attacks. *Sovremennye problemy nauki i obrazovaniia*, 2014, no. 2, p. 119 (In Russian).
14. Vasil'ev V. I., Sharabyrov I. V. Detection of Attacks in Local Wireless Networks based on Data Mining. *Izvestiia IuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, no. 2(151), pp. 57–67 (In Russian).
15. Zhi-Peng Pan, Chao Feng, Chao-Jing Tang. Malware Classification based on the Behavior Analysis and Back Propagation Neural Network. *ITM Web of Conferences 7, 02001*, 2016, pp. 1–5. Available at: https://www.itm-conferences.org/articles/itmconf/pdf/2016/02/itmconf_ita2016_02001.pdf (accessed 2 March 2018).
16. Larionova A. V., Khorev P. B. The Method of Spam Filtering based on an Artificial Neural Network. *Naukovedenie*, 2016, vol. 8, no. 3(34). Available at: https://naukovedenie.ru/PDF/04TVN316.pdf (accessed 3 April 2018) (In Russian).
17. Larionova A. V., Khorev P. B. Evaluating the Effectiveness of Spam Filtering based on an Artificial Neural Network. *Naukovedenie,* 2016, vol. 8, no. 2(33). Available at: https://naukovedenie.ru/PDF/134TVN216.pdf (accessed 3 April 2018) (In Russian).
18. Trapeznikov E. V., Danilova O. T. The Model of the Analysis of Protection of the Information on the basis of a Neural Network. *Dinamika sistem, mekhanizmov i mashin*, 2016, vol. 2, no. 1, pp. 302–308 (In Russian).
19. Danilova O. T., Trapeznikov E. V. Development of a Model Analyzing the Security Function in the Information Protection System, on the Neural Network. *Informatsionnoe protivodeistvie ugrozam terrorizma*, 2015, no. 24, pp. 24–29 (In Russian).
20. Gil'mullin T. M., Gil'mullin M. F. Approaches to Automating the Validation Process of Vulnerabilities Found by Automatic Security Scanners, using Fuzzy Sets and Neural Networks. *Fundamental'nye issledovaniia*, 2014, no. 11, part 2, pp. 266–279 (In Russian).
21. Tsyrul'nik V. F., Kadochnikova N. A. Assessment of the Urgency of Information Security Threats through the Implementation of a Trained Neural Network. *Nauchnyi al'manakh*, 2016, no. 4-3(18), pp. 211–215 (In Russian).
22. Solov'ev S. V., Mamuta V. V. Application of the Apparatus of Neural Technologies for Determining the Urgency of Information Security Threats to Information Systems. *Naukoemkie tekhnologii v kosmicheskikh issledovaniiakh Zemli*, 2016, vol. 8, no. 5, pp. 78–82 (In Russian).
23. Mukhin V. E., Kornaga Ia. I., Steshin V. V. Adaptive Means of Protection of Computer Systems based on Modified Neural Networks of Kohonen. *Nauchno-tekhnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Informatika. Telekommunikatsii. Upravlenie* [St. Petersburg Polytechnic University Journal of Engineering Science and Technology], 2014, no. 2(193), pp. 31–38 (In Russian).
24. Shterenberg S. I., Vitkova L. A., Prosikhin V. P. The Method of Application of the Concept of Adaptive Self-Developing System. *Informatsionnye tekhnologii i telekommunikatsii*, 2014, no. 4(8), pp. 126–133 (In Russian).
25. Kotenko I. V., Nesteruk F. G., Shorov A. V. Hybrid Adaptive Information Protection System based on the Biometaphors of "Nervous" and Neural Networks. *Innovatsii v nauke*, 2013, no. 16-1, pp. 79–83 (In Russian).
26. Vishniakov V. A., Koval' O. I., Mozdurani Shiraz M. G. The Use of Neural Networks to Detect and Recognize Anomalies in the Corporate Enterprise Information System. *Doklady Belorusskogo gosudarstvennogo universiteta informatiki i radioelektroniki*, 2016, no. 4(98), pp. 86–92 (In Russian).
27. Ulezlo D. S., Kadan A. M. Methods of Machine Learning in Solving Information Security Problems. *Proc. of the 3rd Intern. Conf. "Intelligent Technologies for Information Processing and Management"* (ITIPM'2015), 2015, pp. 41–44 (In Russian).
28. Tsvetkova O. L., Kreper A. I. On the Application of the Theory of Artificial Neural Networks in Solving Problems of Providing Information Security. *Simvol nauki*, 2017, no. 04-2, pp. 105–107 (In Russian).
29. Galushkin A. I. *Neirokomp'iutery i ikh primenenie* [Neurocomputers and their Application]. Moscow, IPRZhR Publ., 2000. 416 p. (In Russian).
30. Shchavelev L. V. *Sposoby analiticheskoi obrabotki dannykh dlia podderzhki priniatiia reshenii* [Methods of Analytical Data Processing to Support Decision Making]. Available at: http://infovisor.ivanovo.ru/press/paper04.html (accessed: 3 April 2018).
31. Khaikin S. *Neironnye seti: polnyi kurs* [Neural Networks: Full Course]. Moscow, Vil'iams Publ., 2006. 1104 p. (In Russian).
32. Andrii Shelestov, Serhiy Skakun, Olga Kissul. Complex Neural Network Model of User Behavior in Distributed System. *Intern. Conf. "Knowlegge-Dialogue-Solutions"*, 2007, pp. 1–8. Available at: http://inform.ikd.kiev.ua/content/ua/publications/articles/content/KDS07-Shelestov_Skakun_Kussul.pdf (accessed 2 March 2018).
33. Ronald R. Yager. *Fuzzy Set and Possibility Theory: Recent Developments*. Pergamon, New York, 1982. 408 p.
34. Kolmogorov A. N. On the Representation of Neural Functions of Several Variables in the Form of Superpositions of Continuous Functions of One Variable and Addition. *Doklady AN SSSR* [Reports of the USSR Academy of Sciences], 1957, vol. 114, pp. 953–956 (In Russian).
35. Hornik K., Stinchcombe M., White H. Multilayer Feedforward Networks are Universal Approximators. *Neural Networks*, 1989, no. 2(5), pp. 359–366.
36. Rojas R. *Theorie der Neuronalen Netze: Eine Systematische Einführung*. Springer-Verlag, Berlin, 2013. 446 p. (In German).
37. Maxwell T., Giles C. L., Lee Y. C., Chen H. H. Nonlinear Dynamics of Artificial Neural Systems. *AIP Conf. Proc.*, 1986, vol. 151, pp. 299–304. doi:10.1063/1.36227
38. Rumelhart D., Hinton G., Williams R. Learning Representations by Back-Propagating Errors. *Nature*, 1986, vol. 323, pp. 533–536. doi:10.1038/323533a0
39. Rudoi G. I. Selecting the Activation Function when Predicting Neural Networks. *Mashinnoe obuchenie i analiz dannykh*, 2001, vol. 1, no. 1, pp. 16–39 (In Russian).
40. Golovko V. A. *Neironnye seti. Obuchenie, organizatsiia i primenenie* [Neural Networks. Training, Organization and Application]. Moscow, IPRZhR Publ., 2001. 256 p. (In Russian).
41. Hertz J., Krogh A., Palmer R. *Introduction to the Theory of Neural Computation*. Addison Wesley, Redwood City, 1991. 327 p.