Медведев Михаил Юрьевич – Южный федеральный университет; e-mail: medvmihal@sfedu.ru; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: 88634371694; кафедра электротехники и мехатроники; зав. кафедрой; д.т.н.; профессор.

Рогов Владимир Александрович – e-mail: v_rogoff@mail.ru; кафедра электротехники и мехатроники; инженер.

Медведева Татьяна Николаевна – e-mail: tnikmedv@gmail.com; кафедра электротехники и мехатроники; магистрант.

Medvedev Mikhail Yur'evich – Southern Federal University; e-mail: medvmihal@sfedu.ru; 44, Nekrasovsky, Taganrog, 347928, Russia; phone: +78634371694; the department of electrical engineering and mechatronics; dr. of eng. sc.; professor.

Rogov Vladimir Alexandrovich – e-mail: v_rogoff@mail.ru; the department of electrical engineering and mechatronics; engineer.

Medvedeva Tat'yana Nikolaevna – e-mail: tnikmedv@gmail.com; the department of electrical engineering and mechatronics; undergraduate student.

УДК 004.032.26 DOI 10.18522/2311-3103-2016-7-114122

В.Н. Гридин, В.И. Солодовников

ИССЛЕДОВАНИЕ ВОПРОСОВ КРИПТОСТОЙКОСТИ И МЕТОДОВ КРИПТОАНАЛИЗА НЕЙРОСЕТЕВОГО АЛГОРИТМА СИММЕТРИЧНОГО ШИФРОВАНИЯ

Предпосылкой использования нейронных сетей в качестве математической основы при создании новых методов криптографической защиты информации может служить их способность к восстановлению искаженных сигналов и распознаванию объектов, имеющих характеристики отличные от эталонных. Дополнительным преимуществом является аппаратная реализуемость нейросетевых алгоритмов, что позволяет увеличить скорость шифрования и дешифрования данных. Одной из основных проблем, мешающих продвижению нейросетевых методов шифрования, является плохая изученность вопросов их криптостойкости, что делает актуальной задачу исследования характерных особенностей и поиска уязвимостей нейросетевых криптографических алгоритмов. В статье исследуются вопросы применения нейронных сетей для криптографической защиты информации. Были предложены алгоритмы шифрования, дешифрования и предварительной обработки данных. Алгоритм шифрования основан на генерации различных вариантов искаженного кода, который может быть восстановлен и классифицирован используемой сетью с заданными характеристиками. При построении нейронной сети учитывается информация о частотности появления символов исходного алфавита, что в дальнейшем затрудняет применение методов частотного криптоанализа. Алгоритм дешифрования заключается в распознавании элементов поступающего на вход сети шифротекста и на выходе пользователь получает набор исходных символов. Таким образом, предлагаемый алгоритм принадлежит к симметричным шифрам, так как ключом шифрования и дешифрования является сама нейросеть, а именно выбранная парадигма, ее параметры и структурные характеристики. В статье осуществляется построение математической модели нейросетевого алгоритма симметричного шифрования, а также отмечено его сходство с шифром пропорциональной замены, но с характерными особенностями, присущими методам нейросетевой обработки информации. Проведен анализ классических методов криптоанализа и их применимость по отношению к нейросетевому алгоритму. Предложены возможные направления криптоанализа, а также способы улучшения криптостойкости. Дополнительно осуществляется попытка сопоставить терминологию, принятую при работе с нейросетевыми алгоритма-

ми, и используемую в задачах криптографии. Стоит отметить, что чем более длительным и экспертным является анализ алгоритма и его реализаций, тем более достоверной можно считать его стойкость.

Нейронные сети; криптографическая защита; шифрование; дешифрование; криптостойкость; криптоанализ.

V.N. Gridin, V.I. Solodovnikov

INVESTIGATION OF A CRYPTOGRAPHIC STRENGTH AND CRYPTANALYSIS METHODS FOR THE NEURAL NETWORK ALGORITHM OF A SYMMETRIC ENCRYPTION

A prerequisite for the neural networks use as a mathematical basis for the cryptographic information protection methods could be distinguished their ability to restore the distorted signals and recognize objects with differences from the reference characteristics. An additional advantage includes the hardware realizability of neural network algorithms, which increases speed of data encryption and decryption. One of the main problems that hinder the advancement of neural network encryption methods is the insufficiently studied reliability issues that make it urgent to study the characteristic features and vulnerabilities of the neural network cryptographic algorithms. The article investigates the questions of the neural networks usage for cryptographic information protection. Algorithms for encryption, decoding and data preprocessing were proposed. The encryption algorithm is based on the generation of different variants of the distorted code that could be restored and identified by the used network. Moreover, the formation of the neural network uses the information on the frequency of occurrence of the source alphabet symbols, which makes it difficult to apply the methods of frequency cryptanalysis. At the stage of decryption the neural network classifies the input encrypted signals and converts them into source symbols. Thus, the proposed algorithm belongs to a symmetric cipher, since key encryption and decryption is a neural network itself, specifically the selected paradigm, its parameters and structural characteristics. The mathematical model of the neural network algorithm for symmetric encryption was carried out. Also it was noted the similarity of neural network algorithm with the proportional replace cipher, but with the feature characteristic of neural network data processing methods. The classical methods of cryptanalysis and their applicability in relation to the neural network algorithm were analyzed. Possible directions of cryptanalysis, as well as ways to improve the reliability have been offered. It should be noted that more prolonged and expert analysis of the algorithm and its implementation were conducted, then more accurate its cryptographic strength could be assumed.

Neural network; cryptographic protection; encryption; decryption; cryptographic strength; cryptanalysis.

Введение. В последнее время можно отметить увеличивающийся интерес в области использования математического аппарата искусственных нейронных сетей в задачах защиты информации, а именно криптографии [1–5]. Предпосылкой использования нейросетевого подхода в качестве основы при создании новых методов криптографической защиты информации может служить их способность к восстановлению искаженных сигналов и распознаванию объектов, имеющих характеристики отличные от эталонных [6–9]. Дополнительным преимуществом является аппаратная реализуемость нейросетевых алгоритмов, что позволяет увеличить скорость шифрования и дешифрования данных, а также моделировать их работу на высокопроизводительных супер-ЭВМ. Однако, одной из основных проблем, препятствующих распространению данного подхода, является плохая изученность вопросов криптостойкости, что делает актуальной задачу исследования характерных особенностей и поиска уязвимостей нейросетевых криптографических алгоритмов.

1. Нейросетевой алгоритм симметричного шифрования. Алгоритм шифрования основывается на поиске искаженного кода, который может распознать или восстановить используемая сеть с заданными характеристиками [10, 11]. Без

потери общности будем рассматривать алгоритм шифрования некоторой текстовой информации, т.е. будем оперировать символами или наборами символов и их зашифрованными соответствиями (кодами). В случае необходимости аналогичные рассуждения могут быть проведены для любых кортежей вида $(x_1,...x_S)$ состоящих из 0 и 1, где *s* – размерность блока шифруемых данных. Таким образом, предлагаемый алгоритм применим для любого потока данных.

Реализация алгоритма шифрования включает следующие основные этапы [10, 11]:

- предварительный этап, на котором осуществляется предобработка данных и формируется обучающее множество с учётом частотности появления символов из исходного алфавита (формирование кластеров в пространстве шифробозначений) [12];
- построение нейросети – выбор нейросетевой парадигмы, определение структуры нейронной сети и задание значений весовых коэффициентов (обучение) [7, 9];
- основной этап, на котором происходит процесс шифрования.

Предварительный этап и формирование нейросети обязательно должны предшествовать этапу шифрования, однако после получения обученной сети процесс шифрования может осуществляться многократно.

Алгоритм дешифрования заключается в распознавании поступающего на вход сети шифротекста. В результате на выходе пользователь получает набор исходных символов (кодов классов).

Предлагаемый алгоритм принадлежит к симметричным шифрам, т.к. ключом шифрования и дешифрования является сама нейросеть, а именно выбранная парадигма, ее параметры и структурные характеристики. Также данный алгоритм является шифром замены, т.к. в процессе функционирования осуществляет выбор некоторого кода для каждого символа исходного сообщения.

2. Построение математической модели шифра. Системы шифрования включают следующие основные компоненты [13, 14]:

- совокупность множеств возможных открытых текстов;
- ключ шифрования;
- алгоритм шифрования, который определяет способ преобразования исходного текста в зашифрованный с помощью ключа шифрования;
- совокупность множеств возможных шифротекстов;
- ключ дешифрования;
- алгоритм дешифрования, который задает, как с помощью ключа дешифрования преобразовать зашифрованные данные в исходные.

Пусть *X,K,Y* – конечные множества возможных открытых текстов, ключей и зашифрованных текстов соответственно. Через $E_k : X \to Y$ представим правило шифрования на ключе $k \in K$. Множество $\{E_k : k \in K\}$ обозначим через *E*, а множество $\{E_k(x) : x \in X\}$ – через $E_k(X)$. Тогда $D_k : E_k(X) \to X$ – это правило дешифрования на ключе $k \in K$, и *D* – множество $\{D_k : k \in K\}$ [3].

Система шифрования может быть определена через совокупность $\Sigma_A = (X, K, Y, E, D)$ введенных множеств, для которых выполняются следующие свойства:

Для любых $x \in X$ и $k \in K$ выполняется равенство $D_k(E_k(x)) = x$;

$$Y = \bigcup_{k \in K} E_k(X) \cdot$$

Условие 1) отвечает требованию однозначности дешифрования. Условие 2) означает, что любой элемент $y \in Y$ может быть представлен в виде $E_k(x)$ для подходящих элементов $x \in X$ и $k \in K$.

В качестве первичного признака, по которому производится классификация шифров, рассматривается тип преобразования, осуществляемого с открытым текстом при шифровании. Если отдельные символы или группы символов открытого текста заменяются некоторыми их эквивалентами (кодами) в шифротексте, то соответствующий шифр относится к классу шифров замены.

Для описания произвольного шифра замены в модель $\Sigma_A = (X, K, Y, E, D)$ может быть внесен ряд дополнений. Так открытые и шифрованные тексты *X* и *Y* являются словами в алфавитах *A* и *B*, где: $X \subset A^*$, $Y \subset B^*$, $|A| = n$, $|B| = m$. Знак «*» обозначает множество слов конечной длины соответствующего алфавита. Перед шифрованием открытый текст предварительно представляется в виде последовательности символов или групп символов, называемых шифрвеличинами. В процессе шифрования шифрвеличины заменяются некоторыми их эквивалентами в шифротексте или шифробозначениями. Как шифрвеличины, так и шифробозначения представляют собой слова из A^* и B^* соответственно. Пусть $U = \{u_1, ..., u_N\}$ – множество возможных шифрвеличин, $V = \{v_1, ..., v_M\}$ – множество возможных шифробозначений. Эти множества должны быть такими, чтобы любые тексты $x \in X$, $y \in Y$ можно было представить словами из U^*, V^* соответственно. Требование однозначности дешифрования влечет неравенства $N \geq n$, $M \geq m$, $M \geq N$.

Правило шифрования $E_k(x)$ заключается в выборе на каждом такте шифрования замены для очередной шифрвеличины соответствующего ей шифробозначения. Поскольку $M \geq N$, множество *V* можно представить в виде объединения $V = \bigcup_{i=1}^{N} V^{(i)}$ непересекающихся непустых подмножеств $V^{(i)}$. Произвольное семейство, состоящее из *r* таких разбиений множества *V*, имеет следующий вид:

$$V = \bigcup_{i=1}^{N} V_a^{(i)}, \; a = \overline{1, r}, \; r \in N.$$

Тогда отображение множества шифрвеличин в множество шифробозначений можно представить как семейство биекций:

$\varphi_a : U \to \{V_a^{(1)}, ..., V_a^{(N)}\}$, для которых $\varphi_a(u_i) = V_a^{(i)}$, $i = \overline{1, N}$.

Рассмотрим также произвольное отображение $\psi : K \times N \to N_r^*$, где $N_r = \{1, 2, ..., r\}$, такое, что для любых $k \in K$, $l \in N$, $\psi(k, l) = a_1^{(k)} ... a_l^{(k)}$, $a_j^{(k)} \in N_r$, $j = \overline{1, l}$. Последовательность $\psi(k, l)$ является распределителем, отвечающим данным значениям $k \in K$, $l \in N$. В случае *r=1* шифр замены называют одноалфавитным или шифром простой замены, в противном случае – многоалфавитным.

Правило шифрования произвольного шифра замены примет следующий вид: пусть $x \in X$, $x = x_1 ... x_l$, $x_i \in U$, $i = \overline{1,l}$; $k \in K$ и $\psi(k,l) = a_1^{(k)} ... a_l^{(k)}$, тогда $E_k(x) = y$, где $y = y_1 ... y_l$, $y_j \in \varphi_{a_j^{(k)}}(x_j)$, $j = \overline{1,l}$ [3].

В качестве y_j можно выбрать любой элемент множества $\varphi_{a_j^{(k)}}(x_j)$. Всякий раз при шифровании этот выбор можно производить случайно, например, с помощью некоторого рандомизатора типа игровой рулетки. Подчеркнем, что такая многозначность при зашифровании не препятствует расшифрованию, так как $V_a^{(i)} \bigcap V_a^{(j)} = 0$ при $i \neq j$.

Шифры замены могут быть разделены на однозначные и многозначные. Для однозначных шифров замены справедливо свойство:

$$\forall \alpha, i : \left| V_\alpha^{(i)} \right| = 1.$$

Для многозначных шифров замены:

$$\exists \alpha, i : \left| V_\alpha^{(i)} \right| > 1.$$

Одним из наиболее известных шифров многозначной замены является шифр пропорциональной замены [13, 14]. В нем уравнивается частота появления зашифрованных знаков для защиты от раскрытия с помощью частотного анализа. Для знаков, встречающихся часто, используется относительно большое число возможных эквивалентов. Для менее используемых исходных знаков может оказаться достаточным одного или двух эквивалентов. При шифровании замена для символа открытого текста выбирается либо случайным, либо определенным образом (например, по порядку). Пропорциональные шифры более сложны для вскрытия, чем шифры простой одноалфавитной замены.

3. Соотнесение нейросетевого алгоритма с шифром пропорциональной замены. Рассматриваемый алгоритм во многом подобен шифру пропорциональной замены, что обусловлено предобработкой данных и формированием обучающего множества на предварительном этапе, а также алгоритмом формирования нейронной [10, 11].

Для создания обучающего множества используется информация о частотности появления символов (групп символов) из исходного алфавита A. В случае, если такие данные отсутствуют, необходимо произвести анализ исходного текста и рассчитать частоты вхождения каждого символа в шифруемом сообщении $x(n_1 ... n_t)$, где t – количество различных символов в исходном тексте, n_i – число вхождения i-го символа в исходный текст. В дальнейшем осуществляется формирование областей (кластеров) пространства шифрования, в границах которых будет осуществляться выбор шифробозначений (кодов символов). Данная особенность гарантирует равномерное распределение символов входной последовательности $x = x_1 ... x_l$ в области шифрования, что делает затруднительным применение к алгоритму методов частотного криптоанализа. Режим работы распределителя $\psi(k,l)$ состоит из следующих шагов:

1. Выделение очередного символа или группы символов (шифрвеличины) используемого алфавита A.
2. Для шифрвеличины осуществляется выбор соответствующей ей области (кластера) в пространстве шифрования. Если таких областей несколько, выбор может осуществляться, либо случайным образом, либо последовательно.

3. В полученном кластере генерируется случайная точка, которая является шифром (шифробозначением) исходной шифрвеличины.

Результатом работы алгоритма будет вектор $y = y_1 ... y_l$, где $y_j \in \varphi_{a_j^{(k)}}(x_j)$, который соответствует полученному зашифрованному тексту. Данный подход позволяет шифровать одни и те же символы или группы символов различными кодовыми последовательностями, причем находиться они могут в несвязанных областях пространства шифрования.

4. Криптоанализ нейросетевого алгоритма. В качестве основных подходов криптоанализа симметричных шифров можно выделить: метод грубой силы, частотный анализ, методы разностного (дифференциального) и линейного криптоанализа [15–17].

Атака методом грубой силы, которая предполагает полный перебор всех возможных ключей шифрования, применима для всех типов криптографических алгоритмов. Ее эффективность зависит от размера ключа шифрования и связана с количеством вычислений, требуемых для подбора ключей, соотношением $N_{операций} = 2^N$. В алгоритме шифрования с использованием нейронных сетей в качестве ключа шифрования выступает сама нейронная сеть, т.е. необходимо знать значения всех ее структурных характеристик и параметров. Для хранения этих значений необходимы тысячи, а то и десятки тысяч бит (в зависимости от размера сети), поиск которых с помощью полного перебора недостижим.

Частотный анализ базируется на статистических закономерностях появления отдельных символов и их сочетаний в словах и фразах естественного языка. Анализируя достаточно длинный текст, зашифрованный методом замены, можно по частотам появления символов произвести обратную замену и восстановить исходный текст. Как уже упоминалось ранее нейросетевой алгоритм шифрования учитывает частотность появления символов на предварительном этапе при построении нейронной сети, что гарантирует равномерное распределение символов входной последовательности в области шифрования, т.е. делает затруднительным применение к алгоритму методов частотного криптоанализа.

Метод разностного анализа сочетает в себе обобщение идеи общей линейной структуры с применением вероятностно-статистических методов исследования. Этот метод относится к атакам по выбранному открытому тексту и основан на использовании неравновероятности в распределении значений разности двух шифртекстов, полученных из пары открытых текстов, имеющих некоторую фиксированную разность.

Подобно разностному, линейный криптоанализ является комбинированным методом, сочетающим в себе поиск линейных статистических аналогов для уравнений шифрования. Он основан на применении статистического анализа имеющихся открытых и шифрованных текстов, алгоритмов согласования и перебора.

Логично предположить, что для криптоанализа нейросетевого алгоритма шифрования целесообразно учитывать основные свойства, присущие нейронным сетям. Также стоит обратить внимание на методы, используемые для анализа данных, в частности кластерный анализ, что связано с внутренним представлением информации нейросетью. Общим является то обстоятельство, что нейросеть разбивает все множество шифробозначений на области, каждая из которых в свою очередь соотносится с некоторым значением шифрвеличины.

Исходя из вышесказанного, основное направление криптоанализа будет заключаться в поиске областей в множестве шифробозначений, т.е. решении задачи кластеризации. Для осуществления подобного рода атаки потребуется наличие,

как открытых текстов, так и соответствующих им шифротекстов. Чем большим объемом данных обладает криптоаналитик, тем с большей точностью он сможет выделить необходимые области и построить некоторый функциональный эквивалент исследуемого алгоритма и использованного ключа.

Улучшения криптостойкости алгоритма можно добиться путем увеличения размера ключа, который зависит от размерности элементов множества шифробозначений, и от количества кластеров (областей), характеризующих символ или группу символов. Однако, необходимо учитывать тот факт, что с ростом размерности, так же увеличивается и длинна получаемого шифротекста. Увеличение длинны получаемого шифротекста может быть компенсировано с помощью введения дополнительных классов, которые будут включать не единичные символы, а часто встречающиеся в тексте цепочки символов, но это потребует дополнительных вычислительных затрат на предварительном этапе в процессе построения сети.

Еще одним способом улучшить криптостойкость может служить использование комитетов нейронных сетей. Данный подход подразумевает, что для шифрования очередного символа или группы символов используется выбранная по некоторому правилу сеть из имеющегося набора. В этом случае области шифробозначений у разных нейросетей будут накладываться друг на друга, что способно существенно повысить криптостойкость.

Заключение. В основу предложенного подхода положена способность ряда нейронных сетей к восстановлению искаженных сигналов и распознаванию объектов, имеющих характеристики отличные от эталонных. Алгоритм шифрования основан на генерации различных вариантов искаженного кода, который может распознать или восстановить используемая сеть. Причем при формировании нейронной сети использует информация о частотности появления символов исходного алфавита, что делает затруднительным применение методов частотного криптоанализа. На этапе дешифрования нейросеть осуществляет классификацию поступающих на вход сигналов и преобразует шифробозначения в шифрвеличины. Эти особенности определяют схожесть нейросетевого алгоритма с шифром пропорциональной замены, но с характерными особенностями, присущими методам нейросетевой обработки информации. Также предложен основной подход криптоанализа алгоритма шифрования, а также способы улучшения его криптостойкости. Стоит отметить, что чем более длительным и экспертным является анализ алгоритма и его реализаций, тем более достоверной можно считать его стойкость.

Благодарности. Работа выполняется в рамках программы № IV.3.4. фундаментальных научных исследований ОНИТ РАН «Архитектурно-программные решения и обеспечение безопасности суперкомпьютерных информационно-вычислительных комплексов новых поколений» проект «Использование крупномасштабной проблемы криптоанализа и криптостойкости алгоритмов на основе нейронных сетей для обеспечения безопасности информационно-вычислительных комплексов новых поколений», а также по теме № ГР 115020410096 «Разработка комплексного подхода на основе совместного использования методов интеллектуального анализа данных для выявления скрытых закономерностей и защиты информации».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Ido Kanter, Wolfgang Kinzel, Eran Kanter.* Secure exchange of information by synchronization of neural networks // Europhys., Lett. 57, 141, 2002.
2. *Kinzel W., Kanter I.* Interacting neural networks and cryptography // Advances in solid state physics, Springer Verlag. – 2002. – Vol. 42. – P. 383-391.
3. *Michal Rosen-Zvi, Ido Kanter*. Wolfgang Kinzel Cryptography based on neural networks–analytical results // Journal of Physics A: Mathematical and General. – 2002. – Vol. 35, № 47.

4. *Klimov Alexander, Mityaguine Anton, and Shamir Adi.* "Analysis of Neural Cryptography", Computer Science department, The Weizmann Institute, Rehovot 76100 Israel.
5. *Червяков Н.И., Галушкин А.И., Евдокимов А.А., Лавриненко А.В., Лавриненко И.Н.* Применение искусственных нейронных сетей и системы остаточных классов в криптографии. – М.: Физматлит, 2012. – 280 с.
6. *Каллан Р.* Основные концепции нейронных сетей. – М.: Изд. дом «Вильямс», 2001. – 287 с.
7. *Ежов А., Шумский С.* Нейрокомпьютинг и его применение в экономике и бизнесе. – М.: МИФИ, 1998. – 224 с.
8. *Рассел С., Норвиг П.* Искусственный интеллект: современный подход. – М.: Изд. дом «Вильямс», 2007. – 1408 с.
9. *Медведев В.С., Потемкин В.Г.* Нейронные сети. MATLAB 6. – М.: Диалог МИФИ, 2002. – 496 с.
10. *Гридин В.Н., Солодовников В.И., Евдокимов И.А.* Нейросетевой алгоритм симметричного шифрования // Информационные технологии. – 2015. – Т. 21. № 4. – С. 306-311.
11. *Гридин В.Н., Солодовников В.И., Евдокимов И.А.* Применение нейросетевого подхода на основе LVQ-сети для шифрования текстовой информации // Системы высокой доступности. – 2011. – Т. 7, № 1. – С. 65-68.
12. *Евдокимов И.А., Гридин В.Н., Солодовников В.И., Солодовников И.В.* Предобработка данных с учетом заданных значений отдельных признаков // Информационные технологии и вычислительные системы. – 2009. – № 1. – С. 14-17.
13. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. – М.: Гелиос АРВ, 2005. – 480 с.
14. *Бауэр Ф.* Расшифрованные секреты. Методы и принципы криптологии. – М.: Мир, 2007. – 550 с.
15. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2003. – 610 с.
16. *Шнайер Б., Фергюсон Н.* Практическая криптография. – М.: Вильямс, 2005. – 424 с.
17. *Панасенко С.П.* Современные методы вскрытия алгоритмов шифрования. Ч. 1. CIO-World. – 23.10.2006.
18. *Stinson D.R.* Cryptography: Theory and Practice. – CRC Press, 1995.
19. *Аграновский А.В., Хади Р.А.* Практическая криптография: алгоритмы и их программирование. – М.: Солон-Пресс, 2009. – 258 с.
20. *Смарт Н.* Криптография. – М.: Техносфера, 2005. – 528 с.
21. *Рябко Б.Я., Фионов А.Н.* Криптографические методы защиты информации. – М.: Горячая Линия – Телеком, 2005. – 229 с.

REFERENCES

1. *Ido Kanter, Wolfgang Kinzel, Eran Kanter.* Secure exchange of information by synchronization of neural networks, *Europhys., Lett.* 57, 141, 2002.
2. *Kinzel W., Kanter I.* Interacting neural networks and cryptography, *Advances in solid state physics*, 2002, Vol. 42, зз. 383-391.
3. *Michal Rosen-Zvi, Ido Kanter*. Wolfgang Kinzel Cryptography based on neural networks–analytical results, *Journal of Physics A: Mathematical and General*, 2002, Vol. 35, No. 47.
4. *Klimov Alexander, Mityaguine Anton, and Shamir Adi.* "Analysis of Neural Cryptography", Computer Science department, The Weizmann Institute, Rehovot 76100 Israel.
5. *Chervyakov N.I., Galushkin A.I., Evdokimov A.A., Lavrinenko A.V., Lavrinenko I.N.* Primenenie iskusstvennykh neyronnykh setey i sistemy ostatochnykh klassov v kriptografii [Application of artificial neural networks and the system of residual classes in cryptography]. Moscow: Fizmatlit, 2012, 280 p.
6. *Kallan R.* Osnovnye kontseptsii neyronnykh setey [Basic concepts of neural networks]. Moscow: Izd. dom «Vil'yams», 2001, 287 p.
7. *Ezhov A., Shumskiy S.* Neyrokomp'yuting i ego primenenie v ekonomike i biznese [Neurocomputing, and its application in Economics and business]. Moscow: MIFI, 1998, 224 p.
8. *Rassel S., Norvig P.* Iskusstvennyy intellekt: sovremennyy podkhod [Artificial intelligence: a modern approach]. Moscow: Izd. dom «Vil'yams», 2007, 1408 p.
9. *Medvedev V.S., Potemkin V.G.* Neyronnye seti. MATLAB 6 [Neural network. MATLAB 6]. Moscow: Dialog MIFI, 2002, 496 p.

10. *Gridin V.N., Solodovnikov V.I., Evdokimov I.A.* Neyrosetevoy algoritm simmetrichnogo shifrovaniya [Neural network symmetric encryption algorithm], *Informatsionnye tekhnologii* [Information Technology], 2015, Vol. 21, No. 4, pp. 306-311.
11. *Gridin V.N., Solodovnikov V.I., Evdokimov I.A.* Primenenie neyrosetevogo podkhoda na osnove LVQ-seti dlya shifrovaniya tekstovoy informatsii [Application of neural network approach based on the LVQ network to encrypt text information], *Sistemy vysokoy dostupnosti* [System High Availability], 2011, Vol. 7, No. 1, pp. 65-68.
12. *Evdokimov I.A., Gridin V.N., Solodovnikov V.I., Solodovnikov I.V.* Predobrabotka dannykh s uchetom zadannykh znacheniy otdel'nykh priznakov [Preprocessing given the values of individual traits], *Informatsionnye tekhnologii i vychislitel'nye sistemy* [Information Technologies and Computing Systems], 2009, No. 1, pp. 14-17.
13. *Alferov A.P., Zubov A.Yu., Kuz'min A.S., Cheremushkin A.V.* Osnovy kriptografii [The basics of cryptography]. Moscow: Gelios ARV, 2005, 480 p.
14. *Bauer F.* Rasshifrovannye sekrety. Metody i printsipy kriptologii [Decrypted secrets. Methods and principles of cryptology]. Moscow: Mir, 2007, 550 p.
15. *Shnayer B.* Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si [Applied cryptography. Protocols, algorithms, and source code in C language]. Moscow: Triumf, 2003, 610 p.
16. *Shnayer B., Fergyuson N.* Prakticheskaya kriptografiya [Practical cryptography]. Moscow: Vil'yams, 2005, 424 p.
17. *Panasenko S.P.* Sovremennye metody vskrytiya algoritmov shifrovaniya [Modern methods of opening the encryption algorithms]. Part 1. CIO-World. 23.10.2006.
18. *Stinson D.R.* Cryptography: Theory and Practice. CRC Press, 1995.
19. *Agranovskiy A.V., Khadi R.A.* Prakticheskaya kriptografiya: algoritmy i ikh programmirovanie [Practical cryptography: algorithms and their programming]. Moscow: Solon-Press, 2009, 258 p.
20. *Smart N.* Kriptografiya [Cryptography]. Moscow: Tekhnosfera, 2005, 528 p.
21. *Ryabko B.Ya., Fionov A.N.* Kriptograficheskie metody zashchity informatsii [Cryptographic methods of information protection]. Moscow: Goryachaya Liniya – Telekom, 2005, 229 p.

Статью рекомендовал к опубликованию д.т.н., профессор Ю.И. Митропольский.

Гридин Владимир Николаевич – Учреждение Российской академии наук Центр информационных технологий в проектировании РАН; e-mail: info@ditc.ras.ru; 143000, Московская область, Одинцово, ул. Маршала Бирюзова, 7а; тел.: 84955960219; д.т.н.; профессор.

Солодовников Владимир Игоревич – тел.: 84955964427; к.т.н.; с.н.с.

Gridin Vladimir Nikolaevich – Design information technologies Center Russian Academy of Sciences (DITC RAS); e-mail: info@ditc.ras.ru; 7a, Marshal Biryuzova street, Odintsovo, Moscow region, Russia; phone: +74955960219; dr. of eng. sc.; professor.

Solodovnikov Vladimir Igorevich – phone: +74955964427; cand. of eng. sc.; senior researcher.

УДК 004.853 DOI 10.18522/2311-3103-2016-7-122136

О.И. Федяев

ПРОГНОЗИРОВАНИЕ ОСТАТОЧНЫХ ЗНАНИЙ СТУДЕНТОВ ПО ОТДЕЛЬНЫМ ДИСЦИПЛИНАМ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ

Научная работа посвящена разработке нейросетевой модели процесса обучения студентов для агентной системы моделирования рынка труда. Эта модель позволит имитировать процесс передачи профессиональных навыков и знаний по отдельным дисциплинам в зависимости от личностных характеристик студентов. Система моделирования на осно-