ISSN 2518-1483 (Online),
ISSN 2224-5227 (Print)

2017 • 2

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

БАЯНДАМАЛАРЫ

ДОКЛАДЫ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

REPORTS

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

ЖУРНАЛ 1944 ЖЫЛДАН ШЫҒА БАСТАҒАН
ЖУРНАЛ ИЗДАЕТСЯ С 1944 г.
PUBLISHED SINCE 1944

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ
БАЯНДАМАЛАРЫ **2017 • 2**

«Қазақстан Республикасы Ұлттық ғылым академиясының баяндамалары»
ISSN 2518-1483 (Online),
ISSN 2224-5227 (Print)

Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» Республикалық қоғамдық бірлестігі (Алматы қ.)
Қазақстан республикасының Мәдениет пен ақпарат министрлігінің Ақпарат және мұрағат комитетінде 01.06.2006 ж. берілген **№5540-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік

Мерзімділігі: жылына 6 рет.
Тиражы: 2000 дана.

Редакцияның мекенжайы: 050010, Алматы қ., Шевченко көш., 28, 219 бөл., 220, тел.: 272-13-19, 272-13-18,
http://nauka-nanrk.kz. reports-science.kz

Типографияның мекенжайы: «Аруна» ЖК, Алматы қ., Муратбаева көш., 75.

ДОКЛАДЫ **2017• 2**
НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

Доклады Национальной академии наук Республики Казахстан»
ISSN 2518-1483 (Online),
ISSN 2224-5227 (Print)

Собственник: Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№5540-Ж**, выданное 01.06.2006 г.

Периодичность: 6 раз в год.
Тираж: 2000 экземпляров

Адрес редакции: 050010, г.Алматы, ул.Шевченко, 28, ком.218-220, тел. 272-13-19, 272-13-18
http://nauka-nanrk.kz. reports-science.kz

Адрес типографии: ИП «Аруна», г.Алматы, ул.Муратбаева, 75

REPORTS **2017 • 2**
OF NATIONAL ACADEMY OF SCIENCES OF THE
REPUBLIC OF KAZAKHSTAN

Reports of the National Academy of Sciences of the Republic of Kazakhstan.
ISSN 2224-5227
ISSN 2518-1483 (Online),
ISSN 2224-5227 (Print)

Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of Information and Archives of the Ministry of Culture and Information of the Republic of Kazakhstan N 5540-Ж, issued 01.06.2006

Periodicity: 6 times a year
Circulation: 2000 copies

Editorial address: 28, Shevchenko str., of.219-220, Almaty, 050010, tel. 272-13-19, 272-13-18,
http://nauka-nanrk.kz / reports-science.kz

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

REPORTS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
ISSN 2224-5227
Volume 2, Number 312 (2017), 19 – 27

UDC 004.056.5

B. B. Akhmetov[1], A.G. Korchenko[2], I.A. Tereykovsky[2], Zh.M. Alibiyeva[3], I.M. Bapiyev[3]

[1] Kh.A.Yasawi International Kazakh-Turkish University, Kazakhstan, Turkestan;
[2] National Aviation University, Ukraine, Kiev;
[3] K.I. Satpayev Kazakh National Research Technical University, Kazakhstan, Almaty
alibieva_j@mail.ru

PARAMETERS OF EFFICIENCY ESTIMATION OF NEURAL NETWORKS OF CYBER ATTACKS RECOGNITION ON NETWORK RESOURCES OF INFORMATION SYSTEMS

Annotation. One of the main obstacles of widespread introduction of the neural network methods and models in the systems of cyber attacks recognition on network resources of information systems is the lack of parameters which are the basis of effectiveness assessment. Also, there are no mechanisms of the effectiveness evaluations of such implementation. In order to find the solution of this problem, it has been analyzed a wide spectrum of modern neural network methods and models, which used in the recognition systems. The list of parameters was found and mechanism of their usage for the evaluation of effectiveness of design and choices of these methods and models in the construction of these detection systems was worked out. The obtained results allow determining the deficiencies of modern neural network detection of cyber attacks and vulnerability of detection tools and identifying the perspective ways of their advancement. There is also defined that one of the main ways of improvements of neural network is the development of the mechanism of a constructing training sets.

Keywords: information safety, identification of cyber attacks, information system, neural network models, neural network method, safety parameter.

Introduction

In modern conditions, the effective functioning of the information safety system is impossible without the use of an intellectualized system for the recognition of cyber attacks (SRC) on the network resources of information systems (RIS) [11, 12, 22]. At the same time, one of the most promising directions of development of such RIS and SRC is the use of models and methods based on the theory of neural networks (NS). These models and methods are used in the contours of SRC recognition and, in accordance with the results of [9, 21], significantly improve the accuracy of recognition. Prospectivity of neural network tools (NNT) of recognition is confirmed by their use in well-proven SRC hardware of Cisco company and and a large number of theoretical and practical works in this direction, which review is presented in [9, 11, 12]. At the same time, the variety of solutions used in modern NNT, the large number of factors that affect their operational characteristics, the inaccessibility of the description of the commercial NNT and SRC significantly complicates the assessment of the effectiveness of their use, which in turn narrows the scope of their application in domestic information safety systems. In this case, among the analyzed works [1-24], only in [12] there was proposed a basic set of parameters and the method for assessing the effectiveness of the NNT estimating the security parameters of Internet-oriented information systems. However, the solutions of [12] have general nature, they are oriented at recognizing not only a wide range of diverse cyber attacks, but also recognizing the vulnerabilities of Internet-oriented information systems, and therefore require adaptation to the domestic conditions for recognizing cyber attacks on RIS network. In this regard, the **aim** of this article is to investigate neural networks for recognizing cyber attacks on the network resources of information systems in order to form a set of universal parameters, which values make it possible to quantify the effectiveness of using such tools.

Research of neural network tools for the recognition of cyber attacks on the network resources of information systems

The results [1, 10, 11] indicate that the neural network recognition of cyber attacks on RIS network consists of the evaluation of security parameters (SPs) that are monitored during operation. In this case, the term SP RIS characterizes a physical value that allows evaluating the security of RIS network [12], and the term cyber attacks on RIS network means the realization in cybernetic space of threats to the security of its components (namely, confidentiality, integrity and accessibility) RIS, taking into account their vulnerabilities. The main difference of this kind of cyberattacks is the network mechanism for their implementation. We have to note that in the literature such cyberattacks are often called network attacks. The NNT are intended for their recognition and should be designed to evaluate the SPs, which correspond to the parameters of network connections that are monitored during operation. These prerequisites allowed limiting the list of studies works only by those papers that deal with the use of the NS for detecting network attacks. Let us describe the obtained results.

Methods of simple and semantic classification of network attacks. The methods are developed within the framework of neural network technology for determining network computer attacks using the "Snort" software package described in [25]. The technology provides the use of two neural network methods for determining attacks – **simple classification** and **semantic classification**. As the input parameters there are used parameters of network packets of the transport of degree protocol stack TCP / IP. The simple classification method uses a multilayered persppetron (MSP) with 10 input neurons and 2 neurons in the output layer. In order to optimize the number of hidden neurons, the use of so-called "constructive algorithms" is proposed. The mathematical expression for calculating the correction of the weight coefficients of the neurons of the output layer is given

$$\Delta w_{jk}(i) = -\eta(y_n(i) - f(x_i))\varphi'(v_n(i))y_n,$$

where η – speed coefficient of learning, η – neuron number in the output layer, i – training iteration number, v_n – information field obtained at the input of the activation function, y_n – output signal of n output neuron, φ' –derivative function of activation, $f(x_i)$ – expected reaction of i neuron.

We have to note the lack of a detailed description of the process of optimizing the M structure. The CCA method proposes the use of the Kohonen topographic map (TM). The choice of TM is justified by its low resource intensity. In both methods, a technique for processing the input parameters in order to reduce the number of input parameters of the NS is provided.

Neural Network System of Intrusion Detection (NNSID) is described in [24]. The system is oriented to the use of MSP type NS for detecting network attacks. The results of experiments confirming the effectiveness of the system for detecting attacks which signatures are presented in the KDD-99 database are presented. The choice of the NS type is justified from the point of view of maximum computing power. One-criterion optimization of the architecture of MSP was also carried out.

Binary neural network method (BNM) is described in [15]. The method is used to solve the tasks of detecting network attacks. The method is based on a special binary neural network (BNN), which has two important properties. First, the model is adapted to solve problems which input information has a complex, multiply connected, and even fractal structure. Secondly, the method of training the model is a direct computational procedure and does not require the search for a global extremum of a complex nonlinear function, does not impose any fundamental limitations on the dimensionality of the task. Thus, the method considers a choice of the type of the neural network architecture by the criterion of probability in tasks of the type and by the criterion of minimizing the duration of learning. Unfortunately, there are no experimental data in the work, which makes comparative analysis difficult. The method is not intended to optimize the structure of the NS, and does not comprise the application of the procedure for processing the input data.

The method for isolating network attacks from typical network traffic (INA) is described in [13]. The method is used to recognize network attacks. The use of aMSP with 2 hidden layers of neurons is suggested. The input layer of such an MSP consists of 9 neurons, and the output layer is made up of 1 neuron. It is noted that the choice of MSP with such structure is explained by the requirements of flexibility and functionality. That is, multi-criteria optimization of the structure of NS is used. The need

for preliminary processing of the statistics used for the training and test sample is indicated.

The method for detecting DDoS attacks (MDD) is given in [18]. The use of inaccurate NS is proposed. The proposal is based on the prospective of NS nature of this type. The emphasis is on recognizing the SYN Flood type DDoS attack. In order to formalize the knowledge of experts about the DDoS attack, five linguistic variables were created, each of them characterizes one of the components of vectors of the network traffic parameters, and is used to form the input parameters of the NS. These linguistic variables include:

X_1 - time of receiving data packets, X_2 - percentage of packets from different external ip-addresses, X_3 - percentage of packets from different ports, X_4 - percentage of packages with damaged headings, S - confidence level. Predicate rules of the form were developed: if X_1 = is «big» $\rightarrow Y \rightarrow$ is «high». The structure of the classifier is shown in Figure 2.

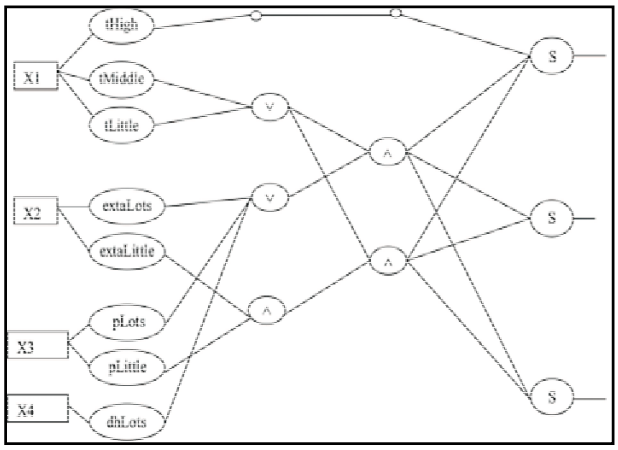

Figure 2 - Inaccurate classifier scheme for detecting SYN Flood attacks

In Figure 2, the symbol indicates the inaccurate neuron "OR", the symbol – the inaccurate neuron "AND", and the notation tLittle, tMiddle, tHigh, extraLittle, extraLots, pLittle, pLots, dhLots correspond to the activation functions of inaccurate variables. It is proposed to present inaccurate classifier in the form of NS with direct propagation of the signal, which is learned with the help of a modified algorithm for back propagation of the error. The modification consists of adapting the classical algorithm to the inaccurate "AND" and "OR" neurons. Thus, the main difference between the proposed method of detection is the possibility of using expert knowledge for NS learning.

The method of using a neural network of a hybrid structure of CounterPropagation type (NNHS) is described in [5, 21]. The method is designed to detect network attacks on a Web server. A feature of the CounterPropagation network is the combination of TM with MSP. The input data of the method are parameters of network traffic transmitted over IP, TCP, HTTP, HTTPS, CGI, and SQLNet protocols. The method provides for the preliminary processing of the input parameters of the NS by representing them in the form of graphic images (pythograms), which are used in the cognitive graph. The aim of the preliminary processing is to minimize the dimension of the input data. The graphic representation determined the necessity of using the Kohonen layer in this method. The use of the perceptron layer is justified from the position of computational efficiency. Thus, the method provides multicriteria optimization of the NS type and one-criterion optimization of the parameters of its architecture. Also, the method provides a procedure for searching the optimal training parameters for the NS, which allows us to reduce the amount of the attack detection errors up to 10 times.

The method of constructing the aggregate traffic classifier (CATC) is proposed in [9]. The method is intended for hierarchical classification of computer attacks on information and telecommunication networks. A special feature of this method is the use of the mathematical method of the main components for the compression of statistical data used as a training sample of NS. The method uses a combination of 22 neural network detectors; each of them is trained to recognize a particular attack

type, given in the KDD-99 database. The detector is a three-layer NS with 12 input neurons and 2 output neurons, one of them is responsible for the presence, and the second for the absence of the attack. As a hidden layer, the Kohonen layer was used. We have to note that the justification for the architecture and parameters of the neural network detector is not given. When the detector detects an attack, the output of the first output neuron is 1. In order to prevent a situation where several detectors simultaneously signal their own type of attack, the minimum euclidean distance between the input image (input parameters - x_i) and the weight coefficients ($w_{i,j}$) of the hidden neurons is transmitted to the second output of each of them:

$$E_j = \min_i \sqrt{\left(x_1 - w_{1,j}\right)^2 + \ldots \left(x_{12} - w_{12,j}\right)^2} .$$

Further, an attack which detector has a minimum Euclidean distance is classified. The CATC method also implicitly provides the optimization of the training and functioning of the neural network detector.

Neural network approach to the detection of network attacks (ADNA) on computer systems is given in [16]. The emphasis is on the recognition of attacks, which signatures are presented in the KDD-99 database. According to the data of this database, the number of input parameters is 41. As a criterion for choosing the optimal type of neural network model, it is suggested to use a minimum of the training sample volume. By means of the analysis of literature sources, it is determined that the admissible types of NS include TN, BSP with one hidden layer of neurons and a network of radial basis function (RBF). It is noted that the minimum amount of training sample (L) for TM should be 2 times higher than the number of input neurons (n), that is $L \approx W / \varepsilon$. For BSP and RBF, the amount of the training sample is calculated as follows $L \approx W / \varepsilon$: where W is the number of synaptic connections ε is the allowable training error. In what follows, an attempt was made in [12] to determine the optimal structure of the BSP. It is stated that the number of hidden neurons determined experimentally is equal to $m = 10$. In this case, the number of output neurons is 2. Accordingly, the required volume of the training sample of the TM is $L = 82$ examples, and for BSP and RBF at $\varepsilon = 0{,}1$ is $L = (m(n+3)+2)/\varepsilon = 4420$. Therefore, the optimal type of neural network model is TM. We have to note that the correctness of the calculated values raises doubts, because according to the NS theory [17], given the accuracy of training, the number of hidden BSP neurons directly depends on the size of the training sample. Later in [12], the structure of the TM is optimized. The criterion for maximizing the accuracy of training is implicitly used. The procedure for preliminary processing of input parameters is also used.

Adaptive system for the detection of attack (ASDA) is described in [19]. The system is designed to recognize network attacks and is based on the joint work of the TM and MSP performing the tasks of clustering and classification of data. Detection of attacks, which is carried out in several stages, became possible due to the fact that the database of the expert system was updated with information about changes in the behavior of a particular object for a certain period of time. It is proved that the optimization of the architecture will improve the accuracy and efficiency of recognition. As the input data, the parameters of the network traffic using the TCP protocol are used. In order to process the input data, a sliding time window method was used. TM is used for preliminary processing of data arriving at the MSP input in order to compress and increase the information content. A mathematical expression for calculating the neuron detection frequency in position (i, j) as the winner neuron is given:

$$\beta_{i,j} = f_{i,j} + \sum_{x=1}^{r} \left(\frac{f_{i-x,j} + f_{i,j-x} + f_{i+x,j} + f_{i,j+x}}{1+x} \right)$$

where $f_{i,j}$ - the number when the neuron at position *(i, j)* was the winner neuron, *r* - distance between cluster centers, *x* - length of input vector.

In the future, this frequency is used to determine the centers and boundaries of clusters. The structure of MSP is optimized in terms of the volume of controlled resources.

Neural network technology for detection and classification of network attacks (VKMA) is described in [23]. In this technology, the use of a three-layer NS is suggested, which is trained by the method of back propagation of the error. In this case, a separate NS is used to recognize each type of

network attacks. As input parameters it is suggested to use the parameters of network traffic on the TCP / IP protocols. As a training sample, it is proposed to use data from the KDD-99 database. The verbal description and fragments of the program code for preparation of the input data from this database to the type of the input parameters of the NS are given. At the same time, one of the training objectives is to reduce the volume of the training sample of the NS. There are no descriptions of approaches on optimizing the architecture and parameters of the neural network model.

The method for recognizing anomalies of network traffic (PANT) is developed in [1]. The method provides the use of the MSP type NS. As input NS data, IP headings datagram parameters are used. The choice of the architecture of the NS is based on the statement about the high approximation possibilities of MSP. The MSP consists of three layers of neurons. The number of neurons of the first (input) layer is 18, which is equal to the number of parameters of the headings of the IP datagram. The number of neurons in the output layer is 2. The output of neuron №1 is responsible for the presence of an anomaly, and the output of neuron №2 for the safe state of network traffic. Expressions for calculating the number of neurons in a hidden layer are given. Thus, the method provides for optimization of the architecture parameters of the NS. In order to simplify the creation of a representative sample, a method for specifying signatures was developed, which aim is to introduce additional artificially created signatures that describe a priori anomalous traffic. Thus, in this method, it is possible to implicitly use expert data on network attacks.

Algorithm of traffic parameters transformation (ATPT) is described in [2]. The algorithm is designed to obtain input data from the network traffic for a neural network system for detecting network attacks. As the input information of the specified algorithm, the parameters of the TCP session are used. Transformation of traffic parameters is used to reduce the number of input parameters of the NS and increase their informative content and is implemented using a mathematical apparatus based on the method of main components. In ATPT, the optimization of the architecture and parameters of the neural network model is not provided. We also note that works [3, 11] have a similar character.

Neural network technology for detecting network attacks (TOMA) on information resources is described in [8, 9, 19]. The technology provides a compression module for input data, which is based on the application of the neural network analogue of the main component method – a recirculating neural network (RNN) with two layers of neurons. The structure of the RNN is shown in Figure 2.

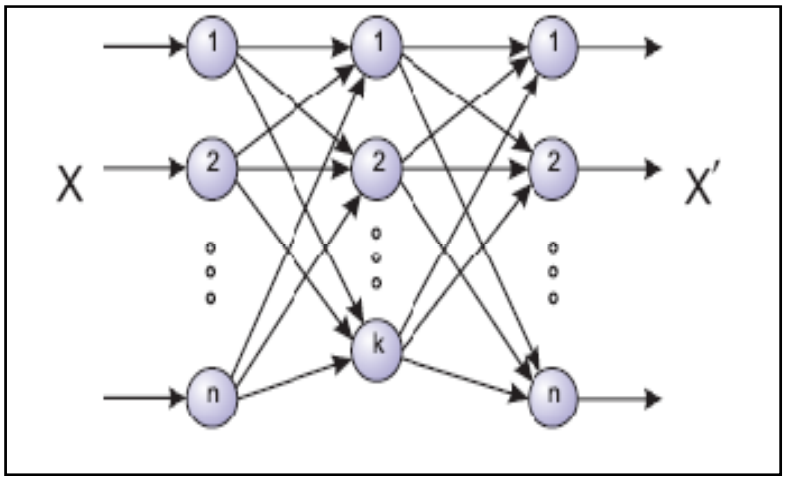

Figure 2 - The structure of the recirculating neural network

The first layer, consisting of k neurons, allows us to control the number of information signs (x), and the second layer of n neurons allows us to filter data (x'). The settings of the first layer allow us to obtain a form of representation of the input n-dimensional object compressed to k attributes, that is, to determine the k principal components.

In the method, by means of numerical experiments, the possibility of using TM and MSP to detect network attacks, which signatures are presented in the KDD-99 database is proved.

Neural network system for detecting computer attacks based on the analysis of network traffic (NNSDC) is described in [16].

The development of a method for analyzing input traffic based on a three-layer NS is declared. It is shown that the calculation of the topology of the NSM should be implemented taking into account the Vapnik-Chervonenkis measure of the form:

$$K \times N \le VC_{\dim} \le N_w \times \left(1 + \lg N_n\right),$$

where N – size of the data at the input; K – number of neurons in the hidden layer; N_w – total number of network weights; N_n – total number of network neurons.

The results of training and testing of the projected NS are given, which show the possibility of its successful application for solving the problem of detection of network computer attacks. It has been suggested that the best results can be obtained in computer systems using a limited set of network software, which makes it possible to form the signs of normal behavior for detecting attacks more effectively.

In [16], a **method for detecting intrusions into an information system based on neural networks (MDI)** was proposed. This method is based on a combined application of methods of searching for an attack signature and detecting anomalies in the user's work. In the process of developing the method, an approach to solve the problem of classifying images is proposed, which consists of presenting input data in the form of signatures and assigning them to attack classes or to safe user actions using the NS. Based on the model of safe operation of the user in the IS and the proposed approach to simplifying the task of processing information, the structure of the neural network attack detection system was synthesized. Also, research was carried out to determine the optimal parameters of NS training algorithms, including the choice of methods for the formation of representative training sets, the assessment of the quality of NS functioning, and the search for optimal parameter values.

A scheme for detecting network attacks based on the combination of neural, immune and neuron-inaccurate classifiers (SDNA) was proposed in [3]. The main features of the proposed scheme are a multilevel analysis of network traffic, as well as the use of various adaptive in the detection of attacks, including neural network and modules. In order to reduce the number of features used for the analysis, it is suggested to apply the principal component method. Computational experiments on two open data sets using various methods of combining classifiers were performed.

Neural network methodology for assessing the safety parameters of Internet-oriented information systems (NISM) is presented in [12]. Among the analyzed papers, this work is the most fundamental. It comprises the further development of theoretical propositions of constructing the NNT for assessing the SP, which aims at the developed approaches to the recognition of gradual and unexpected cyber attacks, the determination of the optimal type of NSM, the appropriateness of using the NNT, the classification of statistically similar cyber attacks, the application of production rules for the presentation of expert knowledge, parameters of NNT effectiveness assessment. Also, models for the creation and use of the NNT for assessing the SP have been developed, which allow us (through the application of the developed theoretical provisions): to determine the list of assessed SP, to create behavior templates adapted to the complex nature of the SP, and to reduce the resource intensity of the creation of the NSM. On the basis of these models, a number of methods that make it possible to increase the efficiency of the use of the NNT have been developed. So the method of representation of expert knowledge for the NNT for assessing the SP allows us to provide prompt recognition and expand many types of cyberattacks for which there are no statistical data. The method for determining the time characteristics of the use of the N NNT for assessing the SP due to the use of the developed analytical dependencies of the determination between the expected and permissible development periods provides the opportunity to determine the appropriateness of using these means. The method of designing a behavior pattern makes it possible to reduce the error in the training of the NSM in 1.5-2 times. The method for determining the effectiveness of developing neural network tools for assessing safety parameters through the application of the proposed parameters for assessing the effectiveness and the formed integral indicator of efficiency allows us to choose the most effective means. The application of the method enabled to determine that the typical shortcomings of the known NNT are the insufficient validity of the use expediency, the inability to use expert data, and the empirical choice of the type of NSM.

Based on the interconnected use of the developed approaches, models and methods, a comprehensive methodology for the neural network estimation of the SP has been developed, which allows us to significantly expand the NNT functional capabilities and to select the most effective means.

From the position of the aim of the research, the proposed list of parameters characterizing the effectiveness of the NNT is the most interesting in this work. We have to note that the lack of this list is caused from the rather general character of the paper [12], which is aimed at evaluating the SP for recognizing a wide range of cyber attacks and vulnerabilities of Internet-oriented IP. Therefore, taking into account the above limitations, proposed list is largely superfluous at evaluating the NNT for recognizing cyber attacks on RIS network. At the same time, it does not fully take into account the specifics of assessing the effectiveness of the NNT in the recognition of network cyber attacks.

The basic characteristics of the analyzed neural network methods and models are given in Table 1. Analysis of the data in this table indicates that BSP and TM are used as the basic types of neural network models in most of the known neural network systems for recognizing network attacks.

In addition, as a result of the analysis it was established that the efficiency of modern neural network methods and models is improved by providing them with certain capabilities that are characterized by the following parameters: $P_{по}$ - preliminary processing of incoming parameters, $P_{ота}$ - optimization of the architecture type, $P_{омн}$ - optimization of the training method, $P_{веп}$ - the possibility of using expert rules, $P_{мна}$ - the possibility of using classical and perspective types of neural network architectures in method, $P_{одв}$ - the possibility of a principled assessment of the appropriateness of using the NS for the solution of the task.

Also, the conclusion that the effectiveness of neural network recognition tools depends on the completeness and representativeness of the training sample was made, which is used to train the basic neural network models. This conclusion is formulated on the basis of an analysis of the results of [21], which substantiates the method of using NS to recognize voice signals. Due to this, the use of the $P_{ов}$ parameter, which is intended to assess the mechanism of formation of the training sample, which is used in the NNT, is suggested.

The values of the proposed parameters in the first approximation can be estimated by a binary scale of 0 or 1. The parameter is equal to 0 when the corresponding possibility in the NNT is not provided and 1 is in the opposite case. For the analyzed cases, the values of these parameters are given in Table. 2. At the same time, $P_{ов} = 0$ for all analyzed methods. That is, in most of the analyzed methods, the procedure for forming the sampling sample has not been implemented. In addition, the use of the proposed criteria enables to determine the integral indicator of the effectiveness of the NNT (E_{Σ}) using the following expression:

$$E_{\Sigma} = \sum_{i=1}^{8} \alpha_i E_i \,, \tag{1}$$

where α_i – weight coefficient of i criterion.

In general, the definition of weight coefficients requires a separate study, and in the basic version we assume that $\alpha_i = 1$. Also we have to note that the basic list of parameters can be further extended.

We note that the practical value of the data in Table 2 consists in outlining the shortcomings and prospects for improving modern neural network methods and models. For example, the values of $P_{по} = 0$ indicate that the shortcomings of the NNSID method include an inadequate optimization of the architecture type of the neural network model. This indicates the possibility of appropriate improvement of these methods. In this case, the value of the parameter P_{Σ} enables to estimate the integral efficiency of the neural network method. Also, as a result of the analysis proved that in modern SRC, classical types of neural network models are mainly used, which are adapted to the conditions of the task to some extent. This allows us to narrow the range of permissible neural network models, which in turn enables to increase the efficiency of determining the neural network model, which is optimal from the point of view of the task. Thus, it becomes possible to increase the efficiency of the establishment of appropriate SRC.

Table 1 - Basic parameters of neural network tools

№	Method	NM type								
		BSP	KN	TM	NMD, NME	ANM	NNM	BNNM	RNN	All types
1	ATPT	-	-	-	-	-	-	-	-	+
2	Simple classification	+	-	-	-	-	-	-	-	-
3	NNSID									
4	TDNA									
5	RANT									
6	Semantic classification	-	-	+	-	-	-	-	-	-
7	NNHS	+	-	+	-	-	-	-	-	-
8	CATC									
9	ADNA									
10	ASDA									
11	MDD	-	-	-	-	-	+	-	-	-
12	BNNM	-	-	-	-	-	-	+	-	-
13	NTDCNA	-	-	-	-	-	-	-	+	-
14	**MDI**	+	-	-	-	-	-	-	-	-
15	**NNSDC**	+	-	-	-	-	-	-	-	-
16	**NNHS**	+	-	+	-	-	-	-	-	-
17	**SDNA**	-	-	+	-	-	-	-	-	-
18	**NNMASP**	+	+	+	+	+	+	+	+	+

Table 2 - The parameters characterizing neural network methods and models

№	Method	Parameter									
		$P_{по}$	$P_{ота}$	$P_{опа}$	$P_{омн}$	$P_{веп}$	$P_{мна}$	$P_{одв}$	$P_{ов}$		P_{Σ}
1	ATPT	1	0	0	0	0	0	0	0		1
2	Simple classification, Semantic classification	1	0	0	0	0	0	0	0		1
3	NNSID	0	1	0	0	0	0	0	0		1
4	TDNA	1	1	0	0	0	0	0	0		2
5	RANT	0	1	1	0	0	0	0	0		2
6	INA	0	1	1	0	0	0	0	0		2
7	INA	1	1	0	0	0	0	0	0		2
8	CATC	1	0	0	0	0	0	0	0		1
9	ADNA	1	1	0	1	0	0	0	0		3
10	ASDA	1	1	1	0	0	0	0	0		3
11	MDD	0	1	0	1	0	0	0	0		2
12	BNNM	0	1	0	1	0	0	0	1		3
14	NTDCNA	1	0	0	0	0	0	0	1		2
15	**MDI**	1	0	0	0	0	0	0	0		1
16	**NNSDC**	1	0	0	0	0	0	0	0		1
17	**NNHS**	1	0	0	0	0	0	0	1		2
18	**SDNA**	1	0	0	0	0	0	0	1		2
19	**NNMASP**	1	1	1	1	1	1	1	0		8

Conclusions

The list of parameters is determined and the mechanism of their use for an assessment of integrated efficiency of development of modern neural network methods of recognition of cyber attacks is formed. This allows us to determine the shortcomings of these methods and models, identify promising directions for their improvement, and increase the effectiveness of the systems created on their basis. In addition, the possibility of limiting the range of permissible neural network architectures that are used in detection systems is shown, which makes it possible to increase the efficiency of the creation of these systems. It has also been determined that one of the most important areas for improving the neural network methods of recognizing cyberattack is the development of the procedure for forming a training sample.

REFERENCES

[1] Abramov E. S. Development and research of methods of creation of systems of detection of the attacks: thesis of Candidate of Technical Sciences: 05.13.19, Abramov E. S., Taganrog, 2005,199 pages. (in Russ.)

[2] Bolshev A. K. Algorithms of transformation and classification of a traffic for detection of invasions into computer networks: the abstract of the thesis on a competition of scientific degree of Candidate of Technical Sciences: specialty 05.13.19, Methods and systems of information security, information security, A. K. Bolshev, St. Petersburg, 2011, 36 pages. (in Russ.)

[3] Branitsky A. A. Detection of the network attacks on the basis of a kompleksirovaniye of neural, immune and neuroindistinct qualifiers, A. A. Branitsky, I. V. Kotenko. Management information systems, 2015, No. 3. C. 69-77. (in Russ.)

[4] Vasilyev V. I. Neural networks at detection of the attacks in Internet network (on the example of SYNFLOOD attack), V. I. Vasilyev, A. F. Hafizov. Neurocomputers in information and expert systems. M.: Radio engineering, 2007, No. 6. Page 34-38. (in Russ.)

[5] Grishin A. V. Neural network technologies in problems of detection of the computer attacks. A. V. Grishin. Information technologies and computing systems, 2011, No. 1. Page 53 - 64. (in Russ.)

[6] Yemelyanova Yu. G. Analysis of problems and prospect of creation of the intelligent detection system and prevention of the network attacks to cloud computing. Yu. G. Yemelyanova, V. P. Fralenko. Program systems: theory and applications: online scientific magazine. 2011, No. 4(8). Page 17-31. [Electronic resource]. URL: http://psta.psiras.ru/read/psta2011_4_17-31.pdf. (in Russ.)

[7] Yemelyanova Yu. G. Neural network technology of detection of the network attacks to information resources. Yu. G. Yemelyanova, A. A. Talalayev, I. P. Tyshchenko, V. P. Fralenko. Program systems: theory and applications. 2011, No. 3(7). Page 3-15. (in Russ.)

[8] Hares of the Lake. Neuronets in security systems. O. Zaytsev. IT Specialty. 2007, No. 6. Page 54-59. (in Russ.)

[9] Mosquito M. P. Metod of creation of the cumulative qualifier of a traffic of information and telecommunication networks for hierarchical classification of the computer attacks. M. P. Komar. Sistemi information processing. 2012. Release 3 (101), volume 1. Page 134-138. (in Russ.)

[10] M.P's mosquito. Neural network approach to detection of the network attacks to computer systems. M. P. Komar, I. O. Paly, R. P. Shevchuk, T. B. Fedysiv. informatics and mathematics methods in modeling. 2011. Volume 1, No. 2. Page 156-160. (in Russ.)

[11] Korchenko O. G. Methods of assessment of neural network ways of opportunities of identification of the Internet focused cyber attacks / O. G. Korchenko, I. A. Tereykovsky, S. V. Kazimirchuk//Messenger of engineering academy of Sciences. – 2014. – Release 2. – Page 87-93. (in Ukr.)

[12] Kryzhanovsky A. V. Application of artificial neural networks in systems of detection of the attacks. A. V. Krzhyzhanovsky. Reports Tomsk state university of control systems and radio electronics. 2008. No. 2 (18), part 1. Page 37-41. (in Russ.)

[13] Magnitsky Yu. N. Use of binary neural network for detection of the attacks to resources of the distributed information systems. Yu. N. Magnitsky. Dynamics of non-uniform systems. 2008. Page 200-205. (in Russ.)

[14] Mustafayev A. G. The neural network system of detection of the computer attacks on the basis of the analysis of a network traffic. Safety issues. 2016. No. 2. Page 1-7. DOI: 10.7256/2409-7543.2016.2.18834. URL: http://e-notabene.ru/nb/article_18834.html. (in Russ.)

[15] Polikarpov S. V., Dergachyov V. S., Rumyantsev K. E., Golubchikov D. M. New model of artificial neuron: cyberneuron and fields of its application. Electronic resource: http://arxiv.org/ftp/arxiv/ papers/0907/0907.0229.pdf. (in Russ.)

[16] Rudenko of O. G. Shtuchni neural networks. Education guidance. / O. G. Rudenko, Є. V. Bodyansky. – Harkov: TOV "SM_T Company", 2006. – 404 pages. (in Ukr.)

[17] Slepovichev I. I. Detection of the DDoS-attacks by indistinct neural network. I. I. Slepovichev, P. V. Irmatov, M. S. Komarova, A. A. Bezhin. News of the Saratov university. 2009. T. 9, Mathematics series. Mechanics. Informatics, release 3. Page 84-89. (in Russ.)

[18] Talalayev A.A.Razrabotka of the neural network module of monitoring of abnormal network activity. A. A. Talalayev, I. P. Tyshchenko, V. P. Fralenko, V. M. Hachumov. Neurocomputers: development and application. 2011. No. 7. Page 32-38. (in Russ.)

[19] Tereykovsky I. Neural networks of a security measure of computer information. I. Tereykovsky. To.: Poligrafkonsalting. 2007. 209 pages. (in Ukr.)

[20] Tereykovska L. O. Neural network models and methods розпізнавання phonemes on a voice signal in systems of distantsinny training. L. O. Tereykovska, Kiev. National university of a stroytelstvo and architecture. To.: 2016. 21 pages. (in Ukr.)

[21] Timofeev A. Research and modeling of a neural network method of detection and classification of the network attacks. A. Timofeev, A. Branitsky. International Journal Information Technologies & Knowledge. 2012. Vol.6, Number 3. P. 257-265 (in Russ.)

[22] A.F. hafizes. Neural network system of detection of the attacks to the WWW server: thesis of Candidate of Technical Sciences: 05.13.11. A. F. Hafizov, Ufa, 2004, 172 with. (in Russ.)

[23] Du Toit T., Kruger H. Filtering spam e-mail with Generalized AdditiveNeural Networks. Information Security for South Africa. 2012., P.1-8. (in Eng.)

[24] Hnatiuk S. Cyberterrorism: History of current trends and countermeasures. S. Hnatiuk. Privacy Notice. 2013. Volume 9, № 2. C.118 - 129. (in Eng.)

CONTENT

Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the work described has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the originality detection service Cross Check http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

ISSN 2518-1483 (Online), ISSN 2224-5227 (Print)

http://www.reports-science.kz/index.php/ru/

Редакторы *М. С. Ахметова, Д. С. Аленов, Т.А. Апендиев*
Верстка на компьютере *А.М. Кульгинбаевой*

Подписано в печать 15.04.2017.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
5,25 п.л. Тираж 2000. Заказ 2.