N E W S
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
SERIES OF GEOLOGY AND TECHNICAL SCIENCES
ISSN 2224-5278
Volume 5, Number 425 (2017), 202 – 212

UDC 004.056.5

B. Aitchanov [1], A. Korchenko[2], I. Tereykovskiy[3], I. Bapiyev[1]

[1]Kazakh National Research Technical University after K. I. Satpaev, Almaty, Kazakhstan,
[2]National Aviation University, Kyiv, Ukraine,
[3]National Technikal University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.
E-mail: bapiev@mail.ru, bekait@rambler.ru, agkorchenko@gmail.com, terejkowski@ukr.net

PERSPECTIVES FOR USING CLASSICAL NEURAL NETWORK MODELS AND METHODS OF COUNTERACTING ATTACKS ON NETWORK RESOURCES OF INFORMATION SYSTEMS

Abstract. The article is devoted to the development of the methodological base for increasing the efficiency of using neural network models for the recognition of cyber-attacks on the network resources of information systems. It is shown that the efficiency of use largely depends on the type of neural network model. The list of the main conditions of the recognition problem is determined, which should be provided due to the characteristics of the type of the neural network model. A number of parameters have been developed, the values of which make it possible to determine the degree of such security. As a result of studies of the main types of classical neural network models, the values of these parameters were determined for each of them. Using the parameters obtained and taking into account the expected application conditions, the perspectives of using the main types of classical neural network models are estimated for the recognition of cyber-attacks. The ways of development of neural network systems for the recognition of cyber attacks on network resources are considered. It is shown that a promising way of such development is the rulemaking for determining effective types of neural network models.

Keywords: neural networks; cyber-attack; network resource; information system; data protection.

I. Introduction. Under current conditions, the effective functioning of the information security system is impossible without the use of an intellectualized system for the recognition of cyber-attacks (RCA) on the network resources of information systems (RIS) [1, 9]. At the same time, one of the most promising areas for the development of intelligent RSA for network RIS is the use of models and methods based on the theory of neural networks (NN). These models and methods are used in the contours of the recognition of RSA and, in accordance with the results of [14, 25], significantly improve the accuracy of recognition. Perspectives of neural network items (NNI) recognition are confirmed by their use in Cisco's well-proven software and hardware RSA and a large number of theoretical and practical works in this direction [10-13, 24]. At the same time, the variety of solutions used in modern NNI, the large number of factors that affect their operational characteristics, the inaccessibility of the description of the commercial NNI of RSA significantly complicate the estimation of the effectiveness of their use, which in turn narrows the scope of their application in domestic information security systems. Note that among the analyzed set of works [15-23, 16-28], only [4, 19] propose the basic set of parameters and the method based on them for estimating the effectiveness of estimating NNI of the security parameters of Internet-oriented information systems. However, the solutions [4, 19] are of a general nature, they are oriented to recognizing not only a wide range of various cyber-attacks, but also the recognition of the vulnerabilities of Internet-oriented information systems, and therefore require adaptation to the domestic conditions for the recognition of cyber-attacks on network RIS. Also, we note that as a result of the analysis of modern scientific works in the field of application of NNI in the domain of information protection, it is determined that in most of them are based on classical neural network models (NNM) adapted to the conditions of the task.

In this regard, the purpose of this research is to assess the perspectives for using classical neural network models for recognizing cyber attacks on network resources of information systems.

II. Approach to determining the effectiveness of the type of the neural network model. In accordance with [3, 5], the development of effective NNI is carried out by adapting certain characteristics of NNM to the significant conditions of the problem of determining cyber-attacks. Thus, we can propose the following approach: the most effective type of NNM has characteristics more fully corresponding to the significant conditions of the problem of determining cyberattacks. In the basic version, the significant conditions set is divided into categories characterizing the tutorial data, training process limitations, computing power, output information, technical implementation and the field of application of NNI.

Let's describe the specified categories.

1. The main characteristics of the tutorial data are:

– Number of parameters defining the case study;

– Type of parameters - discrete (symbolic) or continuous (numeric);

– Number of available case studies. For example, in tasks of recognizing the content of texts, the number of case studies can be considered as unlimited. For other tasks (recognition of network cyber-attacks), the number of case studies can be approximately equal to the number of input parameters;

– Presence of errors (noise) in the case studies;

– Correlation of case studies;

– Ability to pre-process input data to remove noise;

– Ability to display all aspects of the process in the training sampling. For example, the ability to reflect signatures of all types of abnormal behavior or signatures of all viruses in the training sampling;

– Proportionality of the case studies corresponding to various aspects of the process. For example, how many case studies correspond to anomalous behavior of type A, and how many case studies correspond to behavior of type B.

2. Restriction of the training process is conditioned by:

– Maximum period of the training;

– Need to present the expected output of the NN in the tutorial data. Thus, the types of training "with a teacher" or "without a teacher" is determined;

– Ability to automate the training process; It is determined by the number and importance of empirical parameters. This possibility largely determines the conditions of application of the NN. Networks where the training process is not automated can only be used in the laboratory;

– Possibility of additional training during operation;

– Training quality requirements, which are usually estimated by the maximum and average errors in the recognition of tutorial and test data. In this case, the test data should be slightly different from the tutorial data;

– Ability to study NN in the laboratory. For example, in the laboratory, it is possible to teach the NS to recognize network attacks of a certain type. At the same time, it is impossible to teach the NN to classify emails in accordance with the interests of a particular user. The expediency of training in the laboratory is explained by the needs of the optimal mechanism for creating and updating the knowledge base of the NN;

– Requirement to have the same output signal of the network for different examples with the same parameters.

3. In practice, the requirements for computing power are determined by the maximum number of case studies (memory capacity) that NN can memorize in order to achieve the required recognition accuracy. In turn, the accuracy of recognition is characterized by the values of the maximum and average NN errors on the data, which can go beyond the set of the training sampling. Accordingly, there arises a problem of extrapolating the outcomes of teaching NN beyond the training sampling of case studies.

4. The requirements to the NN output information indicate the form, in which this information should be presented. For example, when recognizing viruses, it may be necessary not only to determine a situation such as "software malfunction", but also to calculate the probability of this situation or graphically display such situations on the plane, which will allow the final classification of the user. Another requirement may be the need to determine verbal dependencies between input and output information.

5. Restrictions on the NN technical implementation concern the speed of decision-making, integration into the existing information security systems, the scope and complexity of software implementation.

6. The scope determines the systems in which the NN will be used. To date, the use of NN for image recognition, optimization and text analysis are sufficiently investigated. Note, that the system of pattern recognition is fundamentally different from the systems of text analysis, because the number of output and the number of combinations of input parameters in them is fundamentally limited. In text analysis systems, this number is not fundamentally limited. In addition, the scope of application is determined by adaptability of the network to autonomous operation. In this regard, the architecture of the NN should provide for the possibility of complete automation of the complementary training process during operation.

A possible interpretation of the approach is the expression

$$e(a_i) \to \max, a_i \in A, i = 1, 2, ..., I \ , \quad (1)$$

where e is the efficiency criterion; a_i - i-th type of NNM; A is a set of admissible type of NNM; I is the number of admissible type of NNM.

According to the results obtained in [1 - 3, 5, 7], the components of A are defined as follows:

$$A = \{MLP, RBF, PNN, TM, ART, ANN, CNN, ENN, JNN, SNN\}, \quad (2)$$

where MLP is multilayer perspeter, CNN - convolutional NN, RBF - radial basis function network, TM - Kohonen topographic map, ART - adaptive resonance theory network, PNN - probabilistic NN, ENN - Elmen's network, JNN - Jordan's network, SNN - semantic NN, ANN - associative NN.

Note that the set A determines the most approved classical types of NNM. Also, note that deep neural networks are a kind of MLP.

It is obvious that the efficiency criterion used in formula (1) requires detailed elaboration from the point of view of certain characteristics of the type of NNM. It is possible to carry out the detailed analysis keeping in mind that this criterion is calculated using a number of parameters that allow to take into account the peculiarities of the type of NNM. Besides, we should follow up that for various types of NNM, the effectiveness criterion value may be similar. Therefore, it is expedient to determine the set of effective types of NNM. This set will include NNM, for which the value of the efficiency criterion is close to the maximum. Proximity can be estimated by means of the deviation factor kE.

III. Parameters of determining the efficiency of the type of the neural network model. In order to form the effectiveness criteria for NNM type, we used the developed approach to determining the effective type of NNM, the results of research on the possibilities of using the NN theory methods for estimating security parameters, and the results of the analysis of the most approved classical neural network models. The basic list of the obtained criteria is given in Table. 1. In the future, this list can be expanded, for example, by detailing certain criteria or taking into account new areas of NN application.

Table 1 – Efficiency parameters

#	Category	Explanation of the parameter
1	2	3
$E_{1,1}$	Tutorial data	Limitation in a number of input parameters
$E_{1,2}$		Limitation in the tutorial sampling
$E_{1,3}$		Noise acceptability
$E_{1,4}$		Correlation acceptability
$E_{1,5}$		Need to reflect all the aspects of the process
$E_{1,6}$		Need to represent case studies ratably
$E_{1,7}$		Ability to use discrete input parameters
$E_{1,8}$		Ability to use continuous input parameters
$E_{1,9}$		Ability to use tutorial sampling, whose volume is less than a number of input parameters
$E_{2,1}$	Training process	Short training period
$E_{2,2}$		Need to present the expected yield
$E_{2,3}$		Automation of training
$E_{2,4}$		Option of complementary training
$E_{2,5}$		Quality of training
$E_{2,6}$		Possibility to train on the expert data
$E_{2,7}$		Inalterability of results

Continuation of table 1

1	2	3
$E_{3,1}$	Computation power	Storage capacity
$E_{3,2}$		Extrapolation of the training results
$E_{4,1}$	Initial information	Interpretability of the yield in the form of probability
$E_{4,2}$		Interpretability of the yield in graphical form
$E_{4,3}$		Possibility of verbalization
$E_{5,1}$	Technical implementation	Fast decision making
$E_{5,2}$		The amount of software implementation
$E_{6,1}$	Field of application	Recognition of patterns
$E_{6,2}$		Text analysis
$E_{6,3}$		Control of security settings
$E_{6,4}$		Adaptability to autonomous functioning
$E_{6,5}$		Time series modeling
$E_{6,6}$		Image analysis
$E_{6,7}$		Sound analysis
$E_{6,8}$		Intelligent data analysis

The results of the research carried out in subsection 1.3 allowed us to assess, as a first approximation, the conformity of NNM main types to the proposed parameters. Results of that estimation are presented on a three-point scale and are listed in Tables 2 and 3. The criterion $E_i = 1$, if the *i*-th characteristic of the estimation problem of security parameters is fully ensured in NNM, $E_i = 0$ – if provided partially and $E_i = -1$ – if not provided.

Table 2 – Parameters of the neural network criteria with direct signal propagation and ART

#	NNM type				
	MLP	CNN	RBF	ART	PNN
1	2	3	4	5	6
$E_{1,1}$	–1	–1	–1	–1	–1
$E_{1,2}$	–1	–1	–1	0	–1
$E_{1,3}$	1	1	0	–1	0
$E_{1,4}$	1	1	1	1	1
$E_{1,5}$	–1	–1	1	–1	1
$E_{1,6}$	–1	1	–1	–1	–1
$E_{1,7}$	1	1	1	1	1
$E_{1,8}$	1	1	1	1	1
$E_{1,9}$	–1	–1	1	1	1
$E_{2,1}$	–1	–1	0	1	1
$E_{2,2}$	1	1	1	–1	1
$E_{2,3}$	1	1	–1	1	1
$E_{2,4}$	0	0	1	1	1
$E_{2,5}$	1	1	0	1	1
$E_{2,6}$	–1	–1	–1	–1	1
$E_{2,7}$	1	1	1	1	1
$E_{3,1}$	1	1	–1	–1	–1
$E_{3,2}$	1	0	–1	–1	–1
$E_{4,1}$	0	–1	0	–1	1
$E_{4,2}$	–1	0	–1	–1	–1
$E_{4,3}$	1	–1	0	–1	0
$E_{5,1}$	1	1	1	1	1

Continuation of table 2

1	2	3	4	5	6
$E_{5,2}$	–1	–1	1	0	–1
$E_{6,1}$	1	0	1	1	1
$E_{6,2}$	–1	–1	–1	0	0
$E_{6,3}$	–1	–1	–1	–1	–1
$E_{6,4}$	0	–1	1	1	–1
$E_{6,5}$	1	–1	0	0	0
$E_{6,6}$	1	1	–1	–1	–1
$E_{6,7}$	1	0	–1	–1	–1
$E_{6,8}$	–1	–1	–1	–1	–1

Table 3 – Values of parameters for recurrent NC, SNN, ANN and TM

#	NNM type				
	ENN	JNN	SNN	ANN	TM
$E_{1,1}$	–1	–1	1	–1	–1
$E_{1,2}$	–1	–1	1	–1	–1
$E_{1,3}$	1	1	1	–1	1
$E_{1,4}$	1	1	1	–1	1
$E_{1,5}$	–1	–1	–1	0	1
$E_{1,6}$	1	1	–1	0	1
$E_{1,7}$	1	1	1	1	1
$E_{1,8}$	1	1	–1	0	1
$E_{1,9}$	–1	–1	1	1	1
$E_{2,1}$	–1	–1	0	1	1
$E_{2,2}$	1	1	–1	1	–1
$E_{2,3}$	–1	–1	1	0	0
$E_{2,4}$	0	0	1	0	1
$E_{2,5}$	0	0	1	1	0
$E_{2,6}$	–1	–1	–1	–1	–1
$E_{2,7}$	1	1	1	0	0
$E_{3,1}$	1	1	0	0	–1
$E_{3,2}$	1	1	0	1	0
$E_{4,1}$	0	0	–1	0	0
$E_{4,2}$	–1	–1	–1	–1	1
$E_{4,3}$	1	1	–1	–1	–1
$E_{5,1}$	1	1	0	–1	1
$E_{5,2}$	–1	–1	–1	0	–1
$E_{6,1}$	0	0	0	1	1
$E_{6,2}$	–1	–1	1	–1	1
$E_{6,3}$	–1	–1	–1	1	1
$E_{6,4}$	–1	–1	1	–1	–1
$E_{6,5}$	1	1	–1	–1	–1
$E_{6,6}$	0	–1	–1	–1	–1
$E_{6,7}$	0	0	–1	–1	0
$E_{6,8}$	–1	–1	–1	1	1

If we take into account the three-point numerical estimate, formula (1) is modified as follows:

$$E_{\Sigma} = \sum_{k=1}^{K} E_k(a_i) \to \max,\ a_i \in \boldsymbol{A},\ i = 1,2,...,7\ , \tag{3}$$

where E_{Σ} is an integral criterion for optimization of NNM type; A is the set of admissible NNM types.

For a specific task of determining a cyber attack, the significance of the efficiency parameters can be taken into account if we introduce the corresponding weight coefficients in (3):

$$E_{\Sigma} = \sum_{k=1}^{K} \left(r_k E_k(a_i)\right) \to \max,\ a_i \in \boldsymbol{A}\ , \tag{4}$$

where r_k is a weighting factor of the k-th parameter.

IV. Estimation of perspectives of using classical neural network models. As a result of the research, it can be proposed that the value of the efficiency criterion of the neural network model (4) allows estimating the perspectives of using such a model for the recognition of cyber-attacks on the network resources of information systems. In accordance with [4], in the first approximation, we can assume that the method for determining the effectiveness of use of classical neural network models consists of the following stages:

1. To determine the classical types of neural network models defined by the expression (2), which contain the estimated neural network models.
2. To use the data in Tables 2 and 3 in order to determine the values of the efficiency parameters.
3. To determine the weighting coefficients used in expression (4) by means of the expert evaluation procedure
4. To compute the effectiveness of each estimated model, and to determine the most effective neural network model by means of expression (4).

V. Rules for determining the effective types of neural networks of recognition of cyber-attacks on network resources. According to the results of [1, 2, 9], the main factor that influences the formation of a set of permissible NNM types is the provision of effective training of NNM. To do this, it is necessary to perform the following procedures in a reasonable time: to define a set of input and output parameters of NNM, to encode the input and output parameters, to create a training sampling, and to implement the training process. The first and second procedures are implemented at the preparatory stages of the RCA development, therefore their influence on the formation of many effective types of NNM is not considered. The focus is on the implementation of the second and third procedures. The eligible period for creation of the training sampling and NNM training is determined on the basis of the requirement

$$t_{\Sigma} \le t_d\ , \tag{5}$$

where t_{Σ} is the total period of NNM training, t_d is the acceptable period for the creation of NNM.

Thus, the permissibility of using the i-th type of NNM for recognizing cyber attacks on network RIS can be specified with the help of the following rule:

$$If\ \ t_{\Sigma}(net_i) \le t_d \to net_i \in \boldsymbol{Net_d}\ , \tag{6}$$

where net_i is the i-th form of NNM, $\boldsymbol{Net_d}$ is a set of admissible type of NNM.

Detailing the expression (5), we obtain:

$$t_{\Sigma}(net_i) = t_v + t_l(net_i)\ , \tag{7}$$

where t_v is time of creating the training sampling, t_l (net_i) is time of determination of the model parameters for the i-th type of NNM.

Note that, in the first approximation, the value of t_l (net_i) is approximately equal to the time of determination of the weight coefficients of the synaptic links of NNM. The creation of the training sampling is formation of such a number of case studies, which is considered sufficient for the qualitative teaching of NNM. In accordance with [2, 4, 9], this number depends on the number of input parameters of NNM and in the base case is calculated as follows:

$$P_{\min} \approx 10N_x\ , \tag{8}$$

where P_{min} is the minimum admissible number of case studies, N_x is a number of input parameters of NNM.

It can also be assumed that:

$$t_v = \bar{t}_v P_{\min}, \tag{9}$$

where $\bar{t}_v$ is average time of creating one case study.

It is possible to determine the value of $\bar{t}_v$ by expert evaluation. After substituting (8) into (9), we obtain:

$$t_v = 10\bar{t}_v N_x . \tag{10}$$

At a certain structure for NNM of the i-th type, the duration of the process of determining the weight coefficients can be estimated as follows:

$$t_l(net_i) = \tau \times L_i \times W_i \times K_{o,i}, \tag{11}$$

where τ is the duration of the training iteration for one link; W_i is a number of connections for the i-th type of NNM; L_i is a number of neurons; $K_{o,i}$ is a number of iterations.

In accordance with [1, 2, 9], with approximate calculations for a set of NNM types $\boldsymbol{net_1}$, which consists of NNMs based on PNN, an adaptive resonant theory network, a Kohonen map (TM), a radial basis function network (RBF), associative neural networks (ANS), the duration of training can be written as follows:

$$t_l(\boldsymbol{net_1}) \approx k_1 \tau e^{-\varepsilon} P(N_x + N_y), \tag{12}$$

where $t_l(\boldsymbol{net}_1)$ is the duration of the determination of the weighting coefficients for $\boldsymbol{net_1}$, k_1 is the proportionality coefficient for $\boldsymbol{net_1}$, τ is the duration of one computational operation, P, N_y is the number of case studies and output parameters; χ is an empirical coefficient.

It is possible to estimate the training duration of many types of NNM on the basis of a multi-layer perceptron (MLP) $\boldsymbol{net_2}$, as:

$$t_l(\boldsymbol{net_2}) \approx k_2 \tau e^{-\chi\varepsilon} P^2 (N_x + N_y)^2 , \tag{13}$$

where $t_l(\boldsymbol{net}_2)$ is duration of determining the weighting coefficients for $\boldsymbol{net_2}$, k_2 is a proportionality coefficient for $\boldsymbol{net_2}$.

Note that (12, 13) are obtained under the condition of sequential calculation of signals of artificial neurons that are part of NNM, which is typical for its generally accepted implementation. In addition, it is accepted to assume that the structure of NNM and the computational capabilities of the type of NNM are sufficient to obtain an allowable training error.

As the results of [1, 4, 9] show, from the point of view of the recognition of cyber attacks on network RIS, the most promising types of NNM are RBF, TM, SME, ANS, deep neural networks (DNN). For RBF, TM and ANS, the approximate duration of training can be estimated by means of (12), and for MLP and DNN it is advisable to use (13).

Given the software implementation of NNM, the duration of one computing operation of the learning process depends mainly on the computing power of the hardware of the cyber attack recognition circuit in the network security system RIS.

A permissible error in the training of NNM can be calculated on the basis of the requirements for the accuracy of the recognition of cyber attacks on network RIS. In the first approximation, the values of τ and ε can be determined by expert evaluation.

When determining the principal possibility of using NNM, it is advisable to focus on the minimum number of case studies. Taking into account (12, 13) and the dependence (8), we obtain:

$$t_l(\boldsymbol{net_1}) \approx 10 k_1 \tau e^{-\varepsilon} N_x (N_x + N_y), \tag{14}$$

$$t_l(\boldsymbol{net_2}) \approx 100 k_2 \tau e^{-\chi\varepsilon} N_x^2 (N_x + N_y)^2 . \tag{15}$$

Substituting (10, 14) and (10, 15) into (7), taking into account that $k_1 \approx 0{,}1$, $k_2 \approx 0{,}001$, $\chi \approx 1$, $\varepsilon \approx 0{,}05$, after trivial simplifications, we get:

$$t_\Sigma(\boldsymbol{net_1}) \approx 10 N_x (\bar{t}_v + 0{,}1\tau(N_x + N_y)), \tag{16}$$

$$t_{\Sigma}(\boldsymbol{net}_2) \approx 10N_x\left(\bar{t}_v + 0{,}01\tau N_x\left(N_x + N_y\right)\right), \quad (17)$$

Where $t_{\Sigma}(\boldsymbol{net}_1)$ and $t_{\Sigma}(\boldsymbol{net}_2)$ is the learning time for $\boldsymbol{net}_1$ and $\boldsymbol{net}_2$.

The data of [4] indicate that $N_x = 50...100$, and $N_x + N_y \approx 100$. These assumptions allow us to modify (16, 17) as follows:

$$t_{\Sigma}(\boldsymbol{net}_1) \approx 1000\left(\bar{t}_v + 10\tau\right), \quad (18)$$

$$t_{\Sigma}(\boldsymbol{net}_2) \approx 1000\left(\bar{t}_v + \tau\right). \quad (19)$$

Since $t_{\Sigma}(\boldsymbol{net}_2) > t_{\Sigma}(\boldsymbol{net}_1)$, then, taking into account (18, 19), rule (6) can be detailed:

$$If\ 1000\left(\bar{t}_v + 10\tau\right) \le t_d \rightarrow \boldsymbol{net}_1 \in \boldsymbol{Net}\ , \quad (20)$$

$$If\ 1000\left(\bar{t}_v + \tau\right) \le t_d \rightarrow \boldsymbol{Net} = \left\{\boldsymbol{net}_1, \boldsymbol{net}_2\right\}. \quad (21)$$

Condition (20) determines the acceptability of the use for the recognition of cyber attacks on network RIS of NNM on the basis of ANN, TM, CNN, RBF, PNN, networks of adaptive resonance theory. Condition (21) complements the admissible set by models based on MLP and DNN.

Expressions (20, 21) are the rules for determining the permissible types of NNM intended for the recognition of cyber attacks on network RIS. The application of these rules to the set of available NNM allows us to proceed to the definition of a set of effective types of NNM.

Let's assume that among the set of admissible types, the i-th type of NNM is most effective if the efficiency function takes the maximum value for it. The calculation of the efficiency function of the i-th type of NNM is performed as follows:

$$V_i = \sum_{k=1}^{K} \alpha_k R_k\left(net_i\right),\ net_i \in \mathbf{Net}_d\ , \quad (22)$$

where $\alpha_k = \left[0...1\right]$ is a weight coefficient of the *k-th* efficiency criterion, net_i is the i-th kind of NNM, K is a number of efficiency criteria, R_k is the value of the *k-th* criterion for net_i.

In accordance with the results of [1, 2, 4, 9], the *k-th* criterion for determining the most effective type of NNM is a measure of providing the *k-th* requirement of the problem of recognizing cyber attacks on network RIS in NNM. It should be noted that the requirements for NNM characterize their learning ability, computational capabilities and technical implementation. Partially the list of the developed efficiency criteria meeting the specified requirements is shown in table 4.

Table 4 – Efficiency criteria for the type of NNM

Criterion	Requirement
R_1	Ability to use case studies with various number of input parameters
R_2	Mininmization of the training sampling volume
R_3	Ability to use the training sampling with not proportional presentation of the recognized classes
R_4	Ability to use case studies without the expected output signal
R_5	Ability to use correlated case studies
R_6	Suitability to complementary training
R_7	Suitability to train in parts

The values of the proposed criteria can vary from 0 to 1. In this case, for the *i-th* type of NNM, the value of the *k-th* criterion is 1 if the corresponding *k-th* requirement is fully provided in this type of NNM, and is equal to 0, if it is not provided.

The use of the proposed criteria allows us to proceed to the calculation of the efficiency function of the type of NNM given by expression (22). In turn, this allows writing down the rule for formation of a set of effective types of NNM with the help of expression (23), and the rule for finding the most effective type of NNM can be written by means of expression (24).

$$If\ V(net) \geq \Delta_V \wedge net \in \boldsymbol{Net}_d \rightarrow net \in \boldsymbol{Net}_e, \quad (23)$$

$$If \max_i = \{V(net_i)\}_I, net_i \in \boldsymbol{Net}_e \rightarrow net_i = net_e^{\max}, \quad (24)$$

where $V(net)$ is efficiency of NNM, which is calculated by means of (22), $\boldsymbol{Net}_d$ is the admissible set of NNM, which is formed by means of rules (20, 21), Δ_V is the minimum acceptable efficiency of NNM.

Thus, we can draw the following conclusion that a set of rules (20, 21, 23, 24) has been generated, the use of which makes it possible to determine the set of permissible and effective types of neural network models designed to recognize cyber attacks on network resources of information systems.

VI. Conclusions.

- The list of the main conditions of the recognition problem is determined; these conditions should be provided due to the characteristics of the type of the neural network model.
- A number of parameters has been developed; the values of these parameters make it possible to determine the degree of such security.
- As a result of studies of the main types of classical neural network models, the values of these parameters were determined for each of them.
- Assessments of perspectives for using the main types of classical neural network models for the recognition of cyber attacks are presented.
- Perspectives for further research are the details of the proposed method for determining the effectiveness of using classical neural network models for the recognition of cyber attacks on the network resources of information systems.

REFERENCES

[1] Aytchanov BKh, Bapiyev IM (2017) Razrabotka protsedury opredeleniya ozhidayemogo vykhodnogo signala neyrosetevoy modeli raspoznavaniya kiberatak, International Journal Of Applied And Fundamental Research, 5:8-11. (In Russian) DOI: 10.17513/mjpfi.11532 Access mode: URL: https://www.applied-research.ru/ru/article/view?id=11532 (reference date: August 22, 17).

[2] Aytchanov BKh, Bapiyev IM, Korchenko AG, Tereykovskaya LA, Pogorelov VV (2017) Kontseptual'naya model' obespecheniya effektivnosti neyrosetevogo raspoznavaniya kiberatak. Mathematical Methods and Information Technologies of Macroeconomic Analysis and Economic Policy, Almaty, Kazakhstan, pp. 321-326. (In Russian)

[3] Aytchanov BKh, Bapiyev IM, Tereykovskiy IA, Tereykovskaya LA, Pogorelov VV (2017) Calculation of expected output signal of neural network model for detecting of cyberattack on network resources. Information Technologies, Management and Society, Riga, Latviya, pp. 59-62.

[4] Akhmetov BB, Korchenko AG, Tereykovskiy IA, Alibiyeva ZhM, Bapiyev IM (2017) Parameters of efficiency estimation of neural networks of cyber attacks recognition on network resources of information systems, Reports Of The National Academy Of Sciences Of The Republic Of Kazakhstan, 2:28–37.

[5] Bapiyev IM, Akhmetov BS, Korchenko AG, Tereykovskiy IA (2016) Primeneniye neyronnoy seti s radial'nymi bazisnymi funktsiyami dlya raspoznavaniya skriptovykh virusov, II International Scientific and Practical Conference "Actual issues of cybersecurity and information protection", Kyiv, Ukraine, pp. 21–24. (In Russian)

[6] Bapiyev IM (2017) Pravila dlya opredeleniya effektivnykh vidov neyrosetevykh modeley raspoznavaniya kiberatak na setevyye resursy. III International Scientific and Practical Conference "Actual Issues of Ensuring Cybersecurity and Information Protection", Kyiv, Ukraina, pp. 27–30. (In Russian)

[7] Bapiyev IM, Korchenko AG, Tereykovskiy IA (2016) Razrabotka kriteriyev otsenki effektivnosti neyrosetevykh sredstv raspoznavaniya kiberatak na setevyye resursy informatsionnykh sistem. IV International scientific conference «Global and regional problems of informatizition in society and nature using», Kyiv, Ukraine, pp. 80 – 82. (In Russian)

[8] Bapiyev IM, Korchenko AG, Tereykovskiy IA, Akhmetov BB (2016) Opredeleniye effektivnykh vidov neyrosetevykh modeley raspoznavaniya kiberatak na setevyye resursy. Legal, regulatory and metrological support of information security system in Ukraine, 2:56-63. (In Russian)

[9] Bapiyev IM, Pogorelov VV, Tereykovskiy OI (2017) Sovremennyye neyrosetevyye sredstva raspoznavaniya kiberatak na resursy komp'yuternykh setey. Global and regional problems of informatization in society and nature using, Kyiv, Ukraine, pp. 50-52. (In Russian)

[10] Branitskiy AA, Kotenko IV (2015) Obnaruzheniye setevykh atak na osnove kompleksirovaniya neyronnykh, immunnykh i neyronechetkikh klassifikatorov. Informatsionno-upravlyayushchiye sistemy, 3: 69-77. (In Russian)

[11] Vasil'yev VI, Khafizov AF (2007) Neyronnyye seti pri obnaruzhenii atak v seti Internet (na primere ataki SYNFLOOD). Neyrokomp'yutery v informatsionnykh i ekspertnykh sistemakh, 6:34-38. (In Russian)

[12] Grishin AV (2011) Neural network technology in problems of detection of computer attacks. Information technology and computer systems, 1:53-64.

[13] Yemel'yanova YuG (2011) Analiz problem i perspektivy sozdaniya intellektual'noy sistemy obnaruzheniya i predotvrashcheniya setevykh atak na oblachnyye vychisleniya. Programmnyye sistemy: teoriya i prilozheniya. 4:17-31. [Electronic resource]. (In Russian) URL: http://psta.psiras.ru/read/psta2011_4_17-31.pdf (reference date: August 22, 2017)

[14] Yemel'yanova YuG (2011) Neyrosetevaya tekhnologiya obnaruzheniya setevykh atak na informatsionnyye resursy. Programmnyye sistemy: teoriya i prilozheniya, 3:3–15. (In Russian)

[15] Zaytsev O (2007) Neyroseti v sistemakh bezopasnosti. IT-Spets, 6:54–59. (In Russian)

[16] Komar MP (2012) Metod postroyeniya sovokupnogo klassifikatora trafika informatsionno-telekommunikatsionnykh setey dlya iyerarkhicheskoy klassifikatsii komp'yuternykh atak. Sistemy obrabotki informatsii, 3:134-138. (In Russian)

[17] Komar MP (2011) Neyrosetevoy podkhod k obnaruzheniyu setevykh atak na komp'yuternyye sistemy. Informatika ta matematichní metodi v modelyuvanní, 2:156-160. (In Russian)

[18] Korchenko OG, Tereykovskiy IA, Kazimirchuk SV (2014) Metod otsínki neyromerezhevikh zasobív shchodo mozhlivostey viyavlennya ínternet-oríêntovanikh kíberatak. Vísnik ínzhenernoí akademíí nauk. 2: 87-93. (in Ukrainian)

[19] Korchenko A, Tereykovskiy I, Karpinskiy N, Tynymbayev S (2016) Neyrosetevyye modeli, metody i sredstva otsenki parametrov bezopasnosti Internet-oriyentirovannykh informatsionnykh sistem: monografiya, Kyiv, Ukraine, 276 p. (In Russian)

[20] Krzhyzhanovskiy AV (2008) Primeneniye iskusstvennykh neyronnykh setey v sistemakh obnaruzheniya atak. Doklady TUSURa, 2:37-41. (In Russian)

[21] Magnitskiy YuN (2008) Ispol'zovaniye binarnoy neyronnoy seti dlya obnaruzheniya atak na resursy raspredelennykh informatsionnykh sistem. Dinamika neodnorodnykh sistem, pp. 200-205. (In Russian)

[22] Mustafayev AG (2016) Neyrosetevaya sistema obnaruzheniya komp'yuternykh atak na osnove analiza setevogo trafika. Voprosy bezopasnosti, 2:1-7. DOI: 10.7256/2409-7543.2016.2.18834 Access mode: URL: http://nbpublish.com/library_read_article.php?id=18834 (reference date: August 22, 17)

[23] Polikarpov SV, Dergachev VS, Rumyantsev KE, Golubchikov DM Novaya model' iskusstvennogo neyrona: kiberneyron i oblasti yego primeneniya. [Electronic resource]. (In Russian) Access mode: URL: https://arxiv.org/ftp/arxiv/papers/0907/0907.0229.pdf (reference date: August 22, 2017)

[24] Rudenko OG, Bodyans'kiy YeV (2006) Shtuchní neyronní merezhí. Navch. posíb., Kharkov, Ukraine, 404 p. (in Ukrainian)

[25] Slepovichev II, Irmatov PV, Komarova MS, Bezhin AA (2009) Obnaruzheniye DDoS-atak nechetkoy neyronnoy set'yu. Izvestiya Saratovskogo universiteta, 3:84-89. (In Russian)

[26] Talalayev AA, Tishchenko IP, Fralenko VP, Khachumov VM (2011) Razrabotka neyrosetevogo modulya monitoringa anomal'noy setevoy aktivnosti. Neyrokomp'yutery: razrabotka i primeneniye, 7:32-38. (In Russian)

[27] Tereykovs'kiy Í (2007) Neyronní merezhí v zasobakh zakhistu komp'yuternoí ínformatsíí, Kyiv, Ukraine, 209 p. (in Ukrainian)

[28] Timofeyev A (2012) Issledovaniye i modelirovaniye neyrosetevogo metoda obnaruzheniya i klassifikatsii setevykh atak. International Journal Information Technologies & Knowledge, 3:257-265. (In Russian)

Б. Х. Айтчанов[1], А. Г. Корченко[2], И. А. Терейковский[3], И. М. Бапиев[1]

[1]Қ. И.Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы, Қазақстан,
[2]Ұлттық авиациялық университет, Украина, Киев,
[3]Украина ұлттық техникалық университеті «И. Сикорский атындағы КПИ», Украина, Киев

КЛАССИКАЛЫҚ НЕЙРОЖЕЛІЛІК МОДЕЛЬДЕРДІ ЖӘНЕ АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІҢ ЖЕЛІЛІК РЕСУРСТАРЫНА ШАБУЫЛДАРҒА ҚАРСЫ ӘРЕКЕТ ӘДІСТЕРІН ПАЙДАЛАНУ КЕЛЕШЕКТЕРІ

Аннотация. Мақала ақпараттық жүйелердің желілік ресурстарына кибернетикалық шабуылдарды айырып тану үшін нейрондық желілік модельдерді пайдалану тиімділігін жоғарылатудың әдіснамалық базасын дамытуға арналған. Пайдалану тиімділігі едәуір дәрежеде нейрожелілік модельдің түрінен тәуелді болатынын көрсетілген. Нейрожелілік модель түрінің сипаттамаларының есебінен қамтамасыз етілуі тиіс болатын айырып тану міндеттерінің негізгі шарттарының тізімі анықталған. Мәндері осындай қамтамасыз етудің дәрежесін анықтауға мүмкіндік беретін бірқатар параметрлер әзірленген. Классикалық нейрожелілік модельдердің негізгі түрлерін зерттеу нәтижесінде олардың әрқайсысы үшін көрсетілген параметрлердің мәндері анықталған болатын. Қолданудың күтілетін шарттарын есепке алумен алынған параметрлерді пайдалана отырып, кибершабуылдарды айырып тану үшін классикалық нейрожелілік модельдердің негізгі түрлерін пайдалану келешектерінің бағалары шығарылған. Желілік ресурстарға кибершабуылдарды айырып танудің нейрожелілік жүйелерін дамыту жолдару қарастырылған. Осындай дамытудың келешекті жолы нейрожелілік модельдердің тиімді түрлерін анықтау үшін ережелерді әзірлеу болып табылатыны көрсетілген.

Түйін сөздер: нейрондық желі, кибершабуылдау, желілік ресурс, ақпараттық жүйе, деректерді қорғау.

Б. Х. Айтчанов[1], А. Г. Корченко[2], И. А. Терейковский[3], И. М. Бапиев[1]

[1]Казахский национальный исследовательский технический университет им. К. И. Сатпаева, Алматы, Казахстан,
[2]Национальный авиационный университет, Украина, Киев,
[3]Национальный технический университет Украины «КПИ им. И. Сикорского», Украина, Киев

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ КЛАССИЧЕСКИХ НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ И МЕТОДОВ ПРОТИВОДЕЙСТВИЯ АТАКАМ НА СЕТЕВЫЕ РЕСУРСЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация. Статья посвящена развитию методологической базы повышения эффективности использования нейронных сетевых моделей для распознавания кибернетических атак на сетевые ресурсы информационных систем. Показано, что эффективность использования в значительной степени зависит от вида нейросетевой модели. Определен перечень основных условий задачи распознавания, которые должны обеспечиваться за счет характеристик вида нейросетевой модели. Разработан ряд параметров, значения которых позволяют определить степень такого обеспечения. В результате исследований основных видов классических нейросетевых моделей для каждого из них были определены значения указанных параметров. Используя полученные параметры, с учетом ожидаемых условий применения выставлены оценки перспектив использования основных видов классических нейросетевых моделей для распознавания кибератак. Рассмотрены пути развития нейросетевых систем распознавания кибератак на сетевые ресурсы. Показано, что перспективным путем такого развития является разработка правил для определения эффективных видов нейросетевых моделей.

Ключевые слова: нейронная сеть, кибератака, сетевой ресурс, Информационная система, защита данных.