Journal of Theoretical and Applied Information Technology
15th May 2022. Vol.100. No 9
© 2022 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

METHOD FOR DETERMINING EFFECTIVE TYPES OF NEURAL NETWORK MODELS FOR RECOGNITION OF CYBER ATTACKS BASED ON PROCEDURAL RULES

I. BAPIYEV [1], A. KHAMZINA [2], A. KASSYMOVA [1], G. KHAZHGALIYEVA [1], V. RAMAZANOVA [2], Zh. BAGISOV [2]

[1]Zhangir Khan West Kazakhstan Agrarian-Technical University, Uralsk, West-Kazakhstan Region, Kazakhstan

[2]Makhambet Utemisov West Kazakhstan University, Uralsk, West-Kazakhstan Region, Kazakhstan

E-mail: gulnar.khazhgaliyeva@gmail.com

ABSTRACT

The article touches upon the ways of developing neural network systems for recognizing cyber attacks on network resources of information systems. It is shown that a promising way of such development is the elaboration of rules for determining the effective types of neural network models. The expediency of determining effective types of neural network models based on the consistent application of three rules is substantiated. The first rule allows you to determine the set of valid models from the set of available types of neural network models. The definition of admissibility is implemented on the basis of comparing the minimum possible training time of the type of neural network model with the maximum admissible training time. The second and third rules, formed on the basis of a multi-criteria approach, allow us to select many effective types of neural network models from the set of valid ones, and then determine the most effective type of them.

Keywords: *Neural Network Models, Cyber Attacks, Network Resources, Procedural Rules*

1. INTRODUCTION

In modern conditions, cyber attack countermeasures systems are one of the main means of protecting information of network resources of information systems. Although such systems have been used for more than a decade, many highly qualified specialists have been developing them, and a large number of works have been devoted to the creation of an appropriate scientific and methodological base, however, practical experience indicates that there are a number of significant shortcomings in systems to counter network cyber attacks.

The main one is the insufficient accuracy of recognition of the entire range of network cyber attacks, which is confirmed by well-known cases of successful hacking of information security systems in a number of world countries [1]. In addition, the introduction of well-known means of counteracting network cyber attacks in the information security systems of domestic information systems necessitates their complex adaptation to the variability of conditions of use. Also, the disadvantages of the known means of counteracting cyber attacks on network resources of information systems are the high cost and the lack of detailed scientific and technical documentation.

The studies of scientists [2 - 5] indicate that a promising way to improve the efficiency of network cyber attack recognition tools is to use the apparatus of artificial neural networks in them. This is due to the proven effectiveness of using neural networks for solving such problems by leading developers of information security tools (Cisco, Symantec) and the proven adaptability of neural network tools to a variety of application conditions. At the same time, the results of studies [6] suggest that one of the main tasks in the development of such systems is to determine the most effective type of neural network model, on the basis of which the specified cyber attack recognition system operates. At the same time, the analysis of sources [3, 4] indicates a certain scientific reserve in this direction. A set of efficiency criteria for the type of neural network model is substantiated.

A methodology for the development of neural network tools for assessing the security parameters

of information system resources has been created. A method for evaluating neural network recognition tools for Internet-oriented cyberattacks is substantiated [6, 14]. However, the proposed solutions are of a general nature, quite complex and require adaptation for implementation in modern systems for recognizing cyber attacks on network resources of information systems. Therefore, the purpose of this study is to develop rules for determining effective types of neural network models intended for integration into systems for recognizing cyber attacks on network resources of information systems.

2. METHODS

As the results show, the main factor that influences the formation of the set of valid types of neural network models is to ensure effective training of the neural network model. To do this, it is necessary to perform the following procedures in a reasonable time: determine the set of input and output parameters of the non-network model, encode the specified input and output parameters, create a training sample, and implement the learning process [7, 9, 14].

The first and second procedures are implemented at the preparatory stages of developing a cyber attack recognition system, so their influence on the formation of many effective types of a neural network model is not considered. The main attention is focused on the implementation of the second and third procedures. The acceptable time for creating a training sample and training a neural network model is determined based on the requirement

$$t_{\Sigma} \le t_d, \quad (1)$$

where t_{Σ} – the total training time of the neural network model, t_d – an acceptable time for creating a cyber attack recognition system.

Thus, the admissibility of using the *i*-th type of neural network model for recognizing cyber attacks on network resources of information systems can be set using the following rule:

$$\text{If } t_{\Sigma}(net_i) \le t_d \rightarrow net_i \in Net_d, \quad (2)$$

where net_i – *i*-th type of neural network model, Net_d – set of valid types of neural network models.

Detailing expression (1), we obtain:

$$t_{\Sigma}(net_i) = t_v + t_l(net_i), \quad (3)$$

where t_v – training sample creation time, $t_l(net_i)$ – time to determine the model parameters for the *i*-th type of neural network model.

Note that in the first approximation, the value $t_l(net_i)$ is approximately equal to the time of determining the weight coefficients of synaptic connections of the neural network model. The creation of a training sample is led to the formation of such a number of training examples that is considered sufficient for high-quality training of a neural network model. In accordance with [2, 4, 15], this number depends on the number of input parameters of the neural network model and in the base case is calculated as follows:

$$P_{\min} \approx 10N_x, \quad (4)$$

where $P_{\min}$ – minimum allowed number of training examples, N_x – the number of input parameters of the neural network model.

It can also be assumed that:

$$t_v = \bar{t}_v P_{\min}, \quad (5)$$

where $\bar{t}_v$ – average time to create one case study.

It is possible to determine the value $\bar{t}_v$ by expert evaluation. After substituting (4) into (5), we obtain:

$$t_v = 10\bar{t}_v N_x. \quad (6)$$

With a certain structure for the neural network model of the *i*-th type, the duration of the process of determining the weight coefficients can be estimated as follows:

$$t_l(net_i) = \tau \times L_i \times W_i \times K_{o,i}, \quad (7)$$

where τ – duration of training iteration for one connection; W_i – number of connections for the *i*-th type of neural network model; L_i – number of neurons; $K_{o,i}$ – number of iterations.

In accordance with [10, 12, 16], in approximate calculations for many types of neural network models net_1, which consists of a neural network model based on a probabilistic neural network (PNN), an adaptive resonance theory network (APT), a Kohonen map (TM), a radial basis function network (RBF), associative neural networks (ANN), the duration of training can be

written as follows:

$$t_l\left(net_1\right) \approx k_1 \tau e^{-\varepsilon} P\left(N_x + N_y\right), \quad (8)$$

where $t_l\left(net_1\right)$ – the duration of determining the weighting factors for net_1, k_1 – proportionality factor for net_1, τ – duration of one computational operation, P, N_y – number of training examples and output parameters; ε – learning error.

You can estimate the training duration of many types of neural network models based on the net_2 multilayer perceptron (MLP) as follows:

$$t_l\left(net_2\right) \approx k_2 \tau e^{-\chi\varepsilon} P^2\left(N_x + N_y\right)^2, \quad (9)$$

where $t_l\left(net_2\right)$ – the duration of determining the weighting factors for net_2, k_2 – proportionality factor for net_2, χ – empirical coefficient.

Note that (8, 9) were obtained under the condition of sequential calculation of artificial neuron signals that are part of the neural network model, which is typical for its generally accepted implementation. In addition, the assumption is accepted that the structure of the neural network model and the computational capabilities of the type of neural network model are sufficient to obtain an acceptable learning error.

As evidenced by the results of [7, 9, 17], from the point of view of recognizing cyber attacks on network resources of information systems, the most promising types of neural network models are RBF, TM, MLP, ANN, deep neural networks (DNN). For RBF, TM and ANN, the approximate duration of training can be estimated using (8), and for MLP and DNN it is advisable to use (9).

With a given software implementation of the neural network model, the duration of one computational operation of the learning process mainly depends on the computing power of the hardware of the cyberattack recognition circuit in the system for protecting network resources of information systems.

The allowable learning error of a neural network model can be calculated based on the requirements for the accuracy of recognizing cyber attacks on network resources of information systems. In the first approximation, the values of τ and ε can be determined by expert evaluation.

When determining the fundamental possibility of using a neural network model, it is advisable to focus on the minimum allowable number of training examples. Taking into account (8, 9) and dependence (4), we get:

$$t_l\left(net_1\right) \approx 10 k_1 \tau e^{-\varepsilon} N_x\left(N_x + N_y\right), \quad (10)$$

$$t_l\left(net_2\right) \approx 100 k_2 \tau e^{-\chi\varepsilon} N_x^2\left(N_x + N_y\right)^2 \quad (11)$$

Substituting (6, 10) and (6, 11) into (3), 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 obtain:

$$t_\Sigma\left(net_1\right) \approx 10 N_x\left(\bar{t}_v + 0{,}1\tau\left(N_x + N_y\right)\right), \quad (12)$$

$$t_\Sigma\left(net_2\right) \approx 10 N_x\left(\bar{t}_v + 0{,}01\tau N_x\left(N_x + N_y\right)\right), \quad (13)$$

where $t_\Sigma\left(net_1\right)$ and $t_\Sigma\left(net_2\right)$ – training time for net_1 and net_2.

The data [4] indicate that $N_x = 50 \ldots 100$, a $N_x+N_y \approx 100$. These prerequisites allow us to modify (12, 13):

$$t_\Sigma\left(net_1\right) \approx 1000\left(\bar{t}_v + 10\tau\right), \quad (14)$$

$$t_\Sigma\left(net_2\right) \approx 1000\left(\bar{t}_v + \tau\right). \quad (15)$$

As $t_\Sigma\left(net_2\right) > t_\Sigma\left(net_1\right)$, then taking into account (15, 16) rule (2) can be detailed:

$$If\ 1000\left(\bar{t}_v + 10\tau\right) \le t_d \rightarrow net_1 \in Net, \quad (16)$$

$$If\ 1000\left(\bar{t}_v + \tau\right) \le t_d \rightarrow Net = \left\{net_1, net_2\right\}. \quad (17)$$

Condition (16) determines the admissibility of using neural network models based on ANN, TM, SNN, RBF, PNN, networks of adaptive resonance theory for recognizing cyber attacks on network resources of information systems. Condition (17) complements the admissible set with models based on MLP and DNN.

3. RESULTS

Expressions (16, 17) are the rules for determining the permissible types of neural network models designed to recognize cyber attacks on network resources of information systems. Applying these rules to the set of available neural network models allows us to proceed to the definition of a set of effective types of neural network models.

We will assume that among the set of admissible the *i*-th type of neural network model is the most effective if the efficiency function for it takes the maximum value. The calculation of the efficiency function of the *i*-th type of the neural network model is performed as follows:

$$V_i = \sum_{k=1}^{K} \alpha_k R_k\left(net_i\right), \quad net_i \in Net_d, \tag{18}$$

where $\alpha_k = [0 \ldots 1]$ – weight coefficient of the *k*–efficiency criterion, net_i – *i*-th type of neural network model, *K* – the number of efficiency criteria, *R* –value of the *k* criteria for net_i.

In accordance with the results of [8, 11, 18], under the *k*-th criterion for determining the most effective type of neural network model, we mean the measure of ensuring in the neural network model the *k*-th requirement of the task of recognizing cyber attacks on network resources of information systems. We should note that the requirements for a neural network model characterize their trainability, computational capabilities, and technical implementation. A partial list of developed performance criteria that meet these requirements is shown in Table 1.

Table 1: Criteria for the effectiveness of the type of neural network model

Criterion	Requirement
R_1	Ability to use a neural network of training examples with a variety of input parameters
R_2	Minimizing the volume of training sample
R_3	The possibility of using a training sample in which the number of examples is disproportionately with the number of recognized classes
R_4	Ability to use educational examples in which there is no expected output
R_5	The possibility of using a training sample with correlated examples
R_6	Advancement for adaptation without loss of initial educational information
R_7	Learning adaptation by individual parts
R_8	Ensuring a low learning error
R_9	Providing a short term of study
R_{10}	Ensuring automatic learning
R_{11}	Minimizing the volume of computing resources in training
R_{12}	Ensuring stability learning
R_{13}	The possibility of filing in NNM of explicit expert knowledge
R_{14}	Maximization of the memory ratio of NNM to the number of synaptic ties
R_{15}	Minimizing the generalization error
R_{16}	Minimizing the terms of recognition
R_{17}	Minimization of computing resources when recognizing
R_{18}	The possibility of verbalization of NNM
R_{19}	Testing the tasks of the recognition of cyber

The values of the proposed criteria may vary in the range from 0 to 1. At the same time, for the *i*-th view of the neural network model, the value of the *k*-th criterion is equal to 1, if the corresponding *k*-th requirement is fully provided in this form of the neural network model, and equal to 0, if not ensured.

The use of the proposed criteria allows you to switch to the calculation of the function of the effectiveness of the type of neural network model, given by the expression (18). In turn, this suggests a rule to form a set of effective types of neural network models using an expression (19), and a rule for finding the most efficient type of neural network model - using an expression (20).

$$If\ V(net) \geq \Delta_V \wedge net \in Net_d \rightarrow net \in Net_e, \tag{19}$$

$$If\ \max_i = \left\{V\left(net_i\right)\right\}_I, net_i \in Net_e \rightarrow net_i = net_e^{\max} \tag{20}$$

where $V(net)$ – the effectiveness of the neural network model, which is calculated using (18), Net_d – the permissible set of neural network models, which is formed using the rules (16, 17), Δ_V – the minimum permissible effectiveness of the neural network model, Net_e – many effective types of neural network models.

Thus, it is possible to make the following conclusion that a set of rules (16, 17, 19, 20) was formed, the use of which allows you to determine the set of permissible and effective types of neural network models intended for the recognition of

cyber attacks on network resources of information systems.

4. DISCUSSION:

Let's consider an approximate assessment of the permissible period of creating a neural network model of cyber attack recognition on network resources of information systems. We take into account that the development of the specified neural network model is only one of the components of the general process of creating a system for the protection of information. Therefore

$$t_d = k_{nsm} \times t_{\max}, \quad (22)$$

where t_{max} – the maximum allowable deadline for the development of the information protection system; k_{nsm} – the ratio of proportionality between t_d and t_{max}.

In accordance with [11], in estimated calculations, it can be assumed that the duration of the development of the neural network model takes about a quarter of the total period of the information protection system. Therefore:

$$k_{nsm} \approx 0{,}25. \quad (23)$$

Taking into account the one-year term for the development of the information security system [12], we obtain

$$t_d \approx 0{,}25 \times 1\,\text{year} = 7{,}5 \times 10^6\,\text{c}. \quad (24)$$

Using (24), expressions (17, 18) are modified this way:

$$If\ 1000\left(\bar{t}_v + 10\tau\right) \le 7{,}5 \times 10^6 \rightarrow net_1 \in Net, \quad (25)$$

$$If\ 1000\left(\bar{t}_v + \tau\right) \le 7{,}5 \times 10^6 \rightarrow Net = \left\{net_1, net_2\right\}. \quad (26)$$

Expressions (17, 18, 25, 26) are the rules for determining the permissible types of neural network models designed to recognize cyber attacks on network resources of information systems. The use of these rules to a variety of available neural network models allows you to define a lot of effective types of neural network models.

Table 2 shows the values of the elements of the set of criteria ($\boldsymbol{R_a}$) for tested types of neural network models.

Table 2: Efficiency criteria values for test species of neural network models

Criterion	Types of NNM				
	MLP	DNN	TM	PNN	RBF
R_1	0	0	0,2	0,2	0
R_2	0,2	0,2	0,5	0,9	0,7
R_3	0,3	0,5	0,5	0,5	0,7
R_4	0	0	1	0	0
R_5	0,8	0,8	0,3	0,5	0,5
R_6	0,2	0,9	0,2	1	0,7
R_7	0,1	0,9	0,1	0,1	0,9
R_8	0,9	0,9	0,5	0,9	0,9
R_9	0,5	0,5	0,8	0,9	0,9
R_{10}	0,9	0,9	0,7	0,9	0,7
R_{11}	0,7	0,2	0,8	0,9	0,9
R_{12}	0,8	0,8	0,7	0,9	0,9
R_{13}	0	0	0	0,9	0
R_{14}	0,9	0,9	0,4	0,3	0,5
R_{15}	0,9	0,9	0,4	0,3	0,4
R_{16}	0,7	0,7	0,4	0,9	0,5
R_{17}	0,9	0,9	0,4	0,5	0,5
R_{18}	0,5	0	0	0	0
R_{19}	0,9	0,9	0,5	0,5	0,5

5. CONCLUSION:

The experimental installation is a hardware-software complex designed to conduct experimental studies of the developed models and methods, as well as the neural network system of recognition of network cyber attacks.

Computational capabilities and configuration of hardware of the experimental installation were determined from the standpoint of providing minimally permissible requirements for universal Cyber Recognition System (CRS) type Snort adapted to unfold on Windows and Linux family operating systems [11, 12, 18].

It is also taken into account that the network capabilities of hardware must ensure the possibility

Journal of Theoretical and Applied Information Technology
15th May 2022. Vol.100. No 9
© 2022 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

for intercepting network traffic corresponding to the TCP / IP protocol stack. Therefore, in the basic configuration, a universal personal computer is used based on the Intel (R) Core (TM) 2 Quad CPU Q6600 @ 2.40GHz with RAM volume of 3.7 GB, a rigid disk of volume 1 TB and an Attansic L1 Gigabit Ethernet 10/100/1000Base-T. It should be noted that 20 GB of permanent memory is sufficient for the operation of the experimental installation.

Requirements for the functionality of the experimental installation software are defined from the provision:

– Registration of network requests transmitted according to TCP / IP protocol stack.

– Pre-processing parameters of registered network queries to bring them to the form suitable for use as NNM input parameters.

– Opportunities for the use of public databases for learning NNM network cyber attacks.

– The possibilities of using public databases for the formation of product reference rules of network cyber attacks.

– Implementation of the learning process and testing well-known NNM recognition of network cyber attacks.

– Implementation of the learning process and testing developed on the basis of DNN and PNN NNM recognition of network cyber attacks.

– Comparison of the effectiveness of developed models and methods with known similar models and methods.

The main part of the experimental installation is the developed DNETpro program in Figure 1.

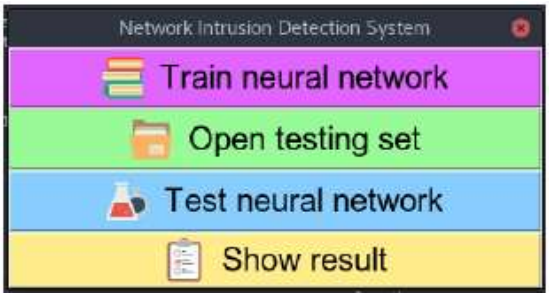

Figure 1. - Main window of the program DNET_pro

DNETpro has been developed on the basis of the proposed model of the DNN, adapted to the recognition of network cyberattack; Python Programming Language and TensorFlow Library have been used. The choice of these instrumental development tools is explained by their high efficiency in the implementation of neural network models on the basis of the DNN [8, 11, 18].

The DNETpro program allows you to train a neural network model, network testing and graphically display test results. On average, the accuracy of the recognition of the DNN was about 90%, which corresponds to the accuracy of cyber recognition with the help of known cyber defamation systems.

The DNETpro learning process is launched using the "Train neural network" button. In this case, the training sample should be located in the "\model\data\" directory, which in turn should be placed in the directory with the launch file called main.py. It should also be noted that the file with the training sample must be named train. File format .csv. The end of the learning process is signaled by the message shown in fig. 2.

Figure 2. Information message about the end of the learning process

After learning DNETpro you can use the analysis of the registered parameters of network requests. We should note that like the training test sample, it must also be written in a .csv file. To specify the target file with a test sample, use the "Open testing set" button. In response a query dialog box opens (Fig. 3, 4).

Journal of Theoretical and Applied Information Technology
15th May 2022. Vol.100. No 9
© 2022 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

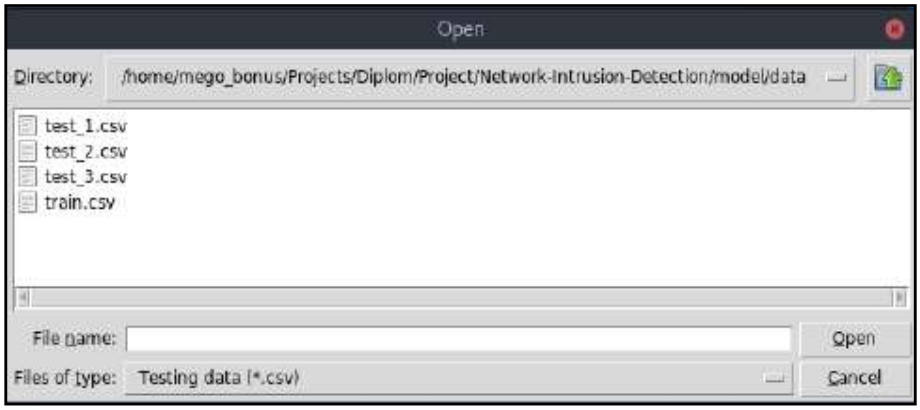

Figure 3. Dialog box for specifying a file with a test sample

Figure 4. Signaling the completion of the recognition process

The visualization of the obtained recognition results is planned to be implemented in the form of a diagram, an example of which is shown in Fig. 5. Entering the view mode is carried out using the "Show result" button. We should note that in Fig. 5. hourly diagram of recognized different types of network cyber attacks for 24 hours is displayed.

Conducted researches allowed to assert:

– The use of the developed method of creating a training sample allows to reduce the number of neural network model computing operations approximately 2.4 times to achieve a permissible learning error.

– The use of the developed method of neural network recognition of cyber attacks allows to increase the efficiency of neural network recognition of cyber attacks approximately 1.35 times.

– Under the expected application conditions, the developed neural network system will ensure an error of recognizing network cyber attacks within 0.05, which is sufficient for practical use.

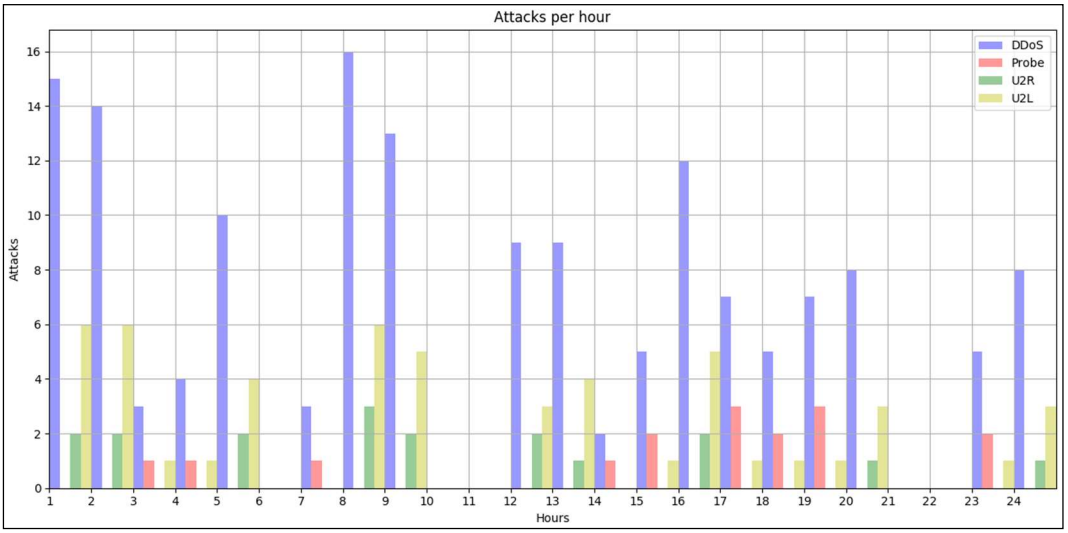

Figure 5. Displaying recognition results

Thus, this method depending on the conditions of application, as well as taking into account special criteria, allows you to choose the most effective neural network models from the many available types. The effectiveness of the selected cyber attack recognition models was proven as a result of specially conducted experiments, as well as practical approbation.

The future direction of research is the development of a technique for neural network recognition of cyber attacks on network resources of information systems. Investigation of the possibilities of reducing the error in recognizing new types of cyber attacks. Creation of new or continuous updating of old databases of signatures of cyber attacks.

REFERENCES:

[1] N. Ryabchuk, N. Grishko, V. Grishko, A. Rudenko, V. Petryk, I. Bapiyev, and S. Fedushko, "Artificial intelligence technologies using in social engineering attacks", in CEUR Workshop Proceedings, Vol. 2654, 2020, pp. 546-555.

[2] Yu.G. Yemelyanova, A.A. Talalaev, I.P. Tishchenko, and V.P. Fralenko, "Neural network technology of detection of network attacks to information resources", Program Systems: Theory and Applications, Vol. 3, № 7, 2011, pp. 3-15.

[3] A.K. Bolshev, "Algorithms of conversion and classification of traffic for intrusion detection in computer networks", Autoabstract thesis for degree of Cand. Tech. Sciences: spec. 05.13.19: Methods and systems of information security, information security, St. Petersburg. State Electrotechnical University, St. Petersburg, 2011, p. 36.

[4] A.V. Artemenko, and V.A. Golovko, "Analysis of neural network methods of computer virus detection", in Materials of section sessions. Youth Innovation Forum "INTRI" – 2010, State Educational Institution "BelISA", Minsk, Belarus, 2010, p. 239.

[5] D.Yu. Gamayunov, "Detection of computer attacks on the basis of the analysis of the network objects' behaviour", Autoabstract thesis for degree of Cand. Tech. Sciences: speciality 05.13.11: mathematical and software support of computers, complexes and computer networks, Moscow state University named after M.V. Lomonosov, Moscow, 2007, p. 11.

[6] A. Korchenko, I. Tereykovsky, N. Karpinsky, and S. Tynimbaev, Neural network models, methods and tools for assessing the security parameters of Internet-oriented information systems: monograph. Kiev, Ukraine: TOV "Our Format", 2016, 275 p.

[7] Tereykovskaya L.A. and Tereykovskiy I.A., "Using the expertise in the development of neural network model for recognition of phonemes in the voice signal" [Text] the proceedings of the II International scientific-practical conference Information and telecommunication technologies: education, science and practice, Almaty, Kazakhstan, 2015, pp. 258–261.

[8] B. Aitchanov, and I.M. Bapiyev, "Razrabotka protsedury opredeleniya ozhidayemogo vykhodnogo signala neyrosetevoy modeli raspoznavaniya kiberatak [Development of a procedure for determining the expected output signal of a neural network model for recognizing cyber attacks]", International Journal of Applied and Fundamental Research, Vol. 5, 2017, pp. 8-11. DOI 10.17513/mjpfi.11532

[9] B. Aitchanov, A. Korchenko, I. Tereykovskiy, and I. Bapiyev, "Perspectives for using classical neural network models and methods of counteracting attacks on network resources of information systems", News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences, Vol. 5, № 425, 2017, pp. 202-212.

[10] Grishin A.V., "Neural network technology in problems of detection of computer attacks", Information technology and computer systems, 2011; 1: 53-64.

[11] I.M. Bapiyev, B.H. Aitchanov, I.A. Tereikovskyi, L.A. Tereikovska, and A.A. Korchenko, "Deep neural networks in cyber attack detection systems", International Journal of Civil Engineering and Technology, Vol. 8, № 11, 2017, pp. 1086-1092.

[12] I. Bapiyev, G. Kamalova, F. Yermukhambetova, A. Khairullina, and A.

Kassymova, "Neural network model of countering network cyber attacks using expert knowledge", Journal of Theoretical and Applied Information Technology, Vol. 99, № 13, 2021., pp. 3179-3190.

[13] Vinoth Kumar R., and Kishore Kumar K., "Exploitation of content management system vulnerabilities to launch large scale cyber attacks", International Journal of Civil Engineering and Technology, Vol. 8, № 10, October 2017, pp. 1381 – 1395.

[14] Li Q., Zhang L., Zhou R., Xia Y., Gao W., Gao W., and Tai Y., "Machine learning-based stealing attack of the temperature monitoring system for the energy internet of things" Security and Communication Networks, Volume 2021, Article ID 6661954, 8 pages https://doi.org/10.1155/2021/6661954

[15] Tai Y., Gao B., Li Q., Yu Z., Zhu C., and Chang V., "Trustworthy and Intelligent COVID-19 Diagnostic IoMT through XR and Deep-Learning-Based Clinic Data Access", IEEE Internet of Things Journal, Vol. 8, № 21, November 2021, pp. 15965 – 159761.

[16] Dychka I., Tereikovskyi I., Tereikovska L., Korchenko A., and Pogorelov V., "Significant Parameters of the Keystroke for the Formation of the Input Field of a Convolutional Neural Network", Advances in Intelligent Systems and Computing, Vol. 1247 AISC, 2021, pp. 498 – 507.

[17] Hu Z., Tereikovskyi I., Korystin O., Mihaylenko V., and Tereikovska L., "Two-Layer Perceptron for Voice Recognition of Speaker's Identity", Advances in Intelligent Systems and Computing, Vol. 1247 AISC, 2021, pp. 508 – 517.

[18] Toliupa S., Tereikovskyi I., Tereikovska L., Mussiraliyeva S., and Bagitova K., "Deep Neural Network Model for Recognition of Speaker's Emotion", 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 - Proceedings, October 2021, pp. 172 - 1766 Article ID 9468017.