REPORTS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
ISSN 2224-5227
Volume 2, Number 312 (2017), 19 – 38

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.

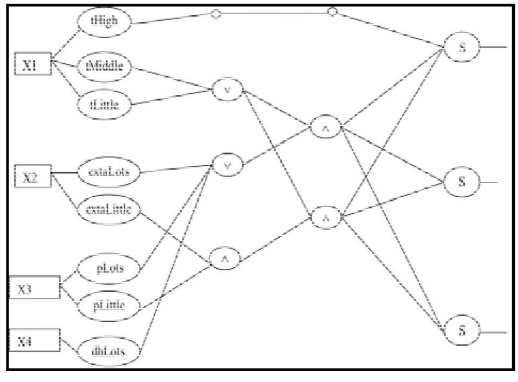

Figure 2 - Inaccurate classifier scheme for detecting SYN Flood attacks

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