APPLICATION OF ARTIFICIAL NEURAL NETWORKS IN THE INTRUSION DETECTION SYSTEM

Arslan G. Mustafaev

Department of Information technology and Information Security
Dagestan State University of National Economy
e-mail: arslan_mustafaev@mail.ru
Russian Federation

Abstract: Intrusion detection systems classify network traffic into two main categories: normal activity and the actions of an attacker. Currently, intelligent data processing and machine learning play an important role in many areas of activity, not excluding intrusion detection systems. One of the main steps in data mining is the identification of an optimal data set that helps to improve the efficiency, performance and speed of predicting intrusion detection systems. For the experimental analysis, a NSL-KDD database used. The results of the experiments show that the approach proposed in the paper is accurate enough, with a low number of false positives and high sensitivity, requiring less training time than using a complete set of data.

Key words: Intrusion detection system, adaptability, classification, artificial neural networks, analysis of network traffic, computer networks.

INTRODUCTION

Rapid development and expansion of global and local networks changed computing systems, which became more connected, and less protected from the malefactors having new potential for destructive purposes. Automation of information processing, storage and transfer leads to creating new problems related with ensuring its safety. At the same time, modern computing systems become more complex because of dynamic changes in configuration and software. Such situation creates almost unlimited opportunities for malefactors, which use software applications and operating systems vulnerabilities for successful penetration into computer systems.

At the same time, correct use of a set of organizational and technical measures enables possible protection from the majority of malicious actions of which a considerable part are remote intrusions. Today intrusion detection systems are an important element of complex system of protection of organizations networks. Intrusion detection systems allow to increase safety of a network, controlling all entering and proceeding traffic streams, as well within perimeter of the protected organization, and outside (revealing attempts of remote invasions and collecting statistics of penetrations) [1].

The main objective of intrusion detection systems is warranting detection of deliberate unauthorized access or special impacts on information from the violators acting with the use of information and telecommunication networks.

Systems of detection of invasions can be passive (find only the fact of impact on the protected system) or active (find influences and to perform reciprocal operations on counteraction to invasion) [2].

Intrusion detection systems consist of an events registration component (sensors or detectors) and a component of the events analysis and intrusion recognition (analyzers) and means of the interaction organization. The composition and structure of base of the solving rules defined by a combination of the specified detection methods. Intrusion detection systems implements one method or a set of several methods of intrusion detection, for example, the signature method based on signatures of the known intrusions or heuristic methods which use profiles of functioning of an information system or actions of information system users.

Besides above-mentioned, also other methods of intrusion detection can be realized [3, 4].

Intrusion detection can be defined as the process of intellectual monitoring of the events, which are occurring in the computer network or system, and their analysis on existence of signs of security policy violation and attempt to threaten confidentiality, integrity, availability, or to bypass mechanisms of safety of a host or network.

The intrusion detection system takes traffic from network, applies certain rules to these data and at detection of signs of an attack, reports about it to the administrator (Figure 1).

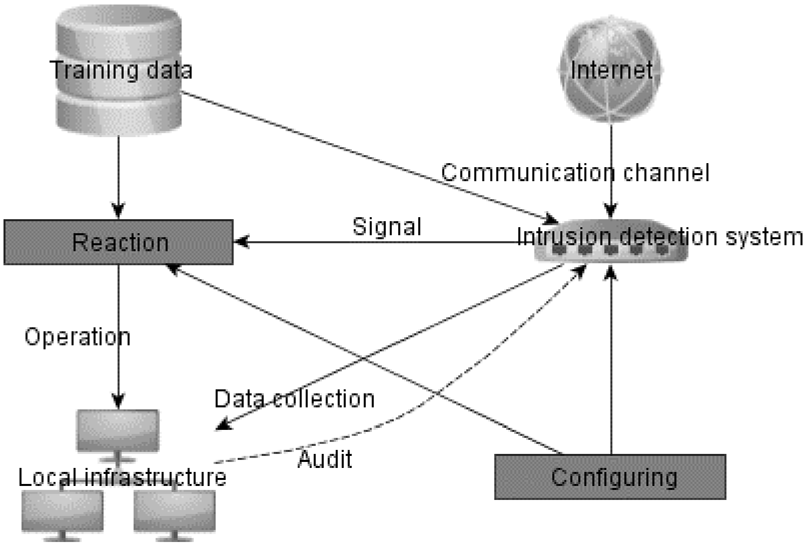

Figure 1. Structure of the intrusion detection system.

Researches and developments in this direction show that the achievement of acceptable levels of protection of information resources against more sophisticated attacks is impossible on the base of application of usual algorithmic and hardware-software decisions [5, 6]. Modern intrusion detection tools have to include intellectual subsystems, at least, as one of the components [7].

The purpose of this work is the development of the intrusion detection system, with adaptation ability to changes of behavior of the computer network based on the use of artificial neural networks.

RESEARCH METHOD

Artificial neural networks are widely used for the detection and prevention of intrusions [8]. In [9, 10] for intrusion detection use is made of a multilayered neural network with two hidden layers and the output layer containing three neurons. One of the datasets available for the evaluation of intrusion detection is the NSL-KDD data set. As a source of the training and test data, the NSL-KDD database [11] used. For neural network training, the backpropagation algorithm is used. The described system is able to recognize two types of attacks and a normal connection. A multilayer neural network is developed, where each layer represents a separate multilayered perceptron [12]. At the first layer, it is defined whether a specific connection is legal or is action of the malefactor. The second and third layers are responsible for classification according to a class and a subclass of the attack. This approach is different from others because it has the possibility of receiving the necessary degree of detail at classification of the considered connection. The three-layer neural network, trained on data of the network traffic, contains models of connections and the simulated attacks [13]. Results of experiments showed high degree of correctness of recognition. The self-organized Kohonen maps for detection of network anomalies are used [14, 15]. The training data contained the description of legitimate behavior of users.

In [16, 17] self-organized Kohonen maps used for a clustering of network traffic data. The processed data are used as input data for multilayered neural networks. For the classification of the network data the radial basis function network, in which the first two layers represent the self-organized maps [18] are also used. For the realization of the system of detection of the attacks the multilayered artificial neural network – a perceptron is used. Multilayered perceptron contains three types of layers of neurons: input, hidden and output. Each neuron of network has smooth nonlinear function of activation. Multilayered nonlinear neural networks allow to form more difficult connections between inputs and outputs, than a single-layer linear. The three-layer neural network with one hidden layer can be trained to approximate with arbitrary accuracy any continuous function [19].

ANALYSIS OF RESULTS

For construction of neural network with the good generalizing ability, it is necessary to define the Vapnik–Chervonenkis dimension (VC_{dim}) for topology of neural network [20]:

$$2\left[\frac{K}{2}\right]N \le VC_{dim} \le 2N_w(1+\log N_n),$$

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

To prevent the neural network from overtraining, the dimension of the training data has to be more or is equal to number of neurons of the hidden layer.

Training data for the neural network were taken from the NSL-KDD base containing data sets about legal network connections and the attacks (Table 1). Data on each connection contain 41 parameters and are divided into four categories corresponding to types of threats (Figure 2):

1. Denial of Service (DoS). The malefactor limits access to the verified users to specific service through a certain protocol.

2. Remote to Local (R2L). The malefactor tries to get access from the outside to the local computer of the user.

3. User to Root (U2R). The malefactor, having got access to the computer of the victim tries to acquire the rights of more exclusive user.

4. Probe. The malefactor tries to receive data on the user's infrastructure.

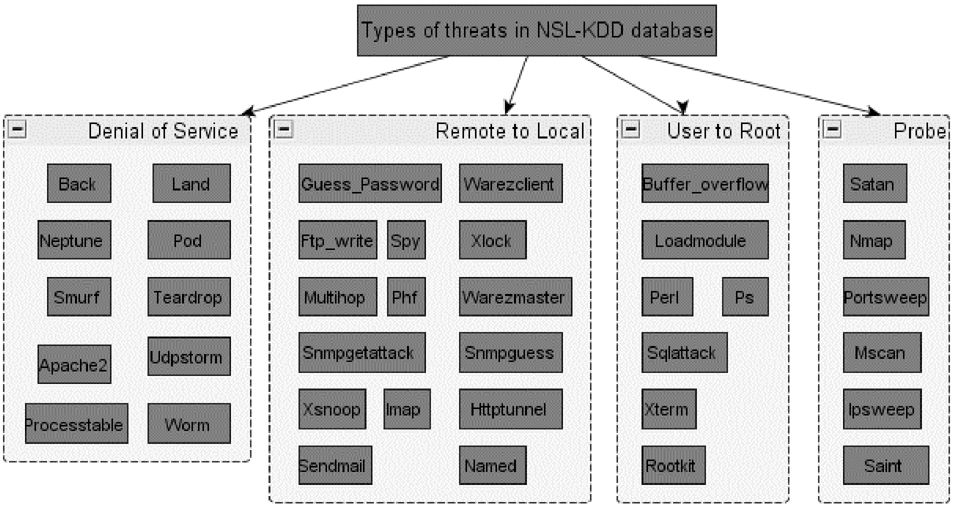

Figure 2. Types of threats in NSL-KDD database.

Table 1. Distribution of records on sets in NSL-KDD Dataset.

Dataset type	Total					
	Records	Normal	DoS	Probe	U2R	R2L
KDDTrain+20 %	25192	13449	9234	2289	11	209
		53.39%	36.65%	9.09%	0.04%	0.83%
KDDTrain+	125973	67343	45927	11656	52	995
		53.46%	36.46%	9.25%	0.04%	0.79%
KDDTest+	22544	9711	7458	2421	200	2754
		43.08%	33.08%	10.74%	0.89%	12.22%

The offered system can work in following modes: detection (for check of normal and abnormal actions), classification (if any abnormal action is revealed, to classify it by four main types of the attack: DOS, Probe, U2R or R2L) and detailed classification (classification of abnormal events in 29 subtypes of the attack).

The sequence of steps of operation of the intrusion detection system is given in Figure 3.

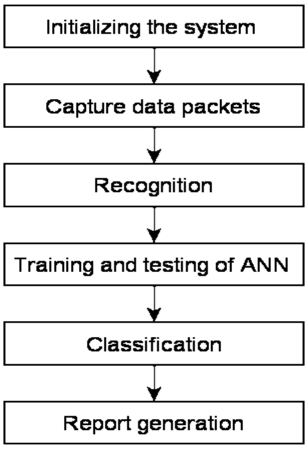

Figure 3. Chart of the sequence of operations of the intrusion detection system.

Researches and experiments show [21-24] that the use of all set of parameters does not lead to an improvement of quality of detection and gives considerable number of false positives and false negatives. A reduction of the set of parameters allows to improve quality of detection [25-27].

The approaches for estimation of informational content of big dimension data providing increase in accuracy of identification of anomalies in network traffic and significantly raise speed of classification algorithms in detail described [28-30]. Regarding the selection of features signs, they are sorted in decreasing order of their importance and the least informative are not considered.

As a result, the optimized subset of parameters of the NSL-KDD base (Table 2) is created. The initial numbering of parameters, in NSL-KDD base, in Table 2 is kept.

The designed neural network contains an input layer, one hidden layer and an output layer. The input layer of the neural network has 18 neurons, the output layer has five neurons corresponding to normal work and four types of threats (Figure 4).

The data set is divided into three subsets: training, testing and validation (60% - training, 20% - testing, and 20% - validation).

The backpropagation algorithm is applied to training of artificial neural network [31, 32]. The error of training is calculated at output layer, and distributed back to each neuron of the network, and afterwards correction of neurons weights according to their values (Figure 5) is carried out.

Table 2. A subset of the parameters considered by neural network.

№	Parameter	Description
BASIC FEATURES OF EACH NETWORK CONNECTION VECTOR		
3	service	Destination network service used
5	dst_bytes	Number of data bytes transferred from destination to source in single connection
6	flag	Status of the connection – Normal or Error
8	wrong_fragment	Total number of wrong fragments in this connection
CONTENT RELATED FEATURES OF EACH NETWORK CONNECTION VECTOR		
13	num_compromised	Number of «compromised» conditions
TIME RELATED TRAFFIC FEATURES OF EACH NETWORK CONNECTION VECTOR		
23	count	Number of connections to the same destination host as the current connection in the last two seconds
25	rerror_rate	The percentage of connections that have activated the flag (4) REJ, among the connections aggregated in count (23)
27	diff_srv_rate	The percentage of connections that were to different services, among the connections aggregated in count (23)
29	srv_serror_rate	The percentage of connections that have activated the flag (4) s0, s1, s2 or s3, among the connections aggregated in srv_count
30	srv_rerror_rate	The percentage of connections that have activated the flag (4) REJ, among the connections aggregated in srv_count
31	srv_diff_host_rate	The percentage of connections that were to different destination machines among the connections aggregated in srv_count
HOST BASED TRAFFIC FEATURES IN A NETWORK CONNECTION VECTOR		
32	dst_host_count	Number of connections having the same destination host IP address
34	dst_host_same_srv_rate	The percentage of connections that were to the same service, among the connections aggregated in dst_host_count (32)
35	dst_host_diff_srv_rate	The percentage of connections that were to different services, among the connections aggregated in dst_host_count (32)
36	dst_host_same_src_port_rate	The percentage of connections that were to the same source port, among the connections aggregated in dst_host_srv_count
37	dst_host_srv_diff_host_rate	The percentage of connections that were to different destination machines, among the connections aggregated in dst_host_srv_count
39	dst_host_srv_serror_rate	The percent of connections that have activated the flag (4) s0, s1, s2 or s3, among the connections aggregated in dst_host_srv_count
41	dst_host_srv_rerror_rate	The percentage of connections that have activated the flag (4) REJ, among the connections aggregated in dst_host_srv_count

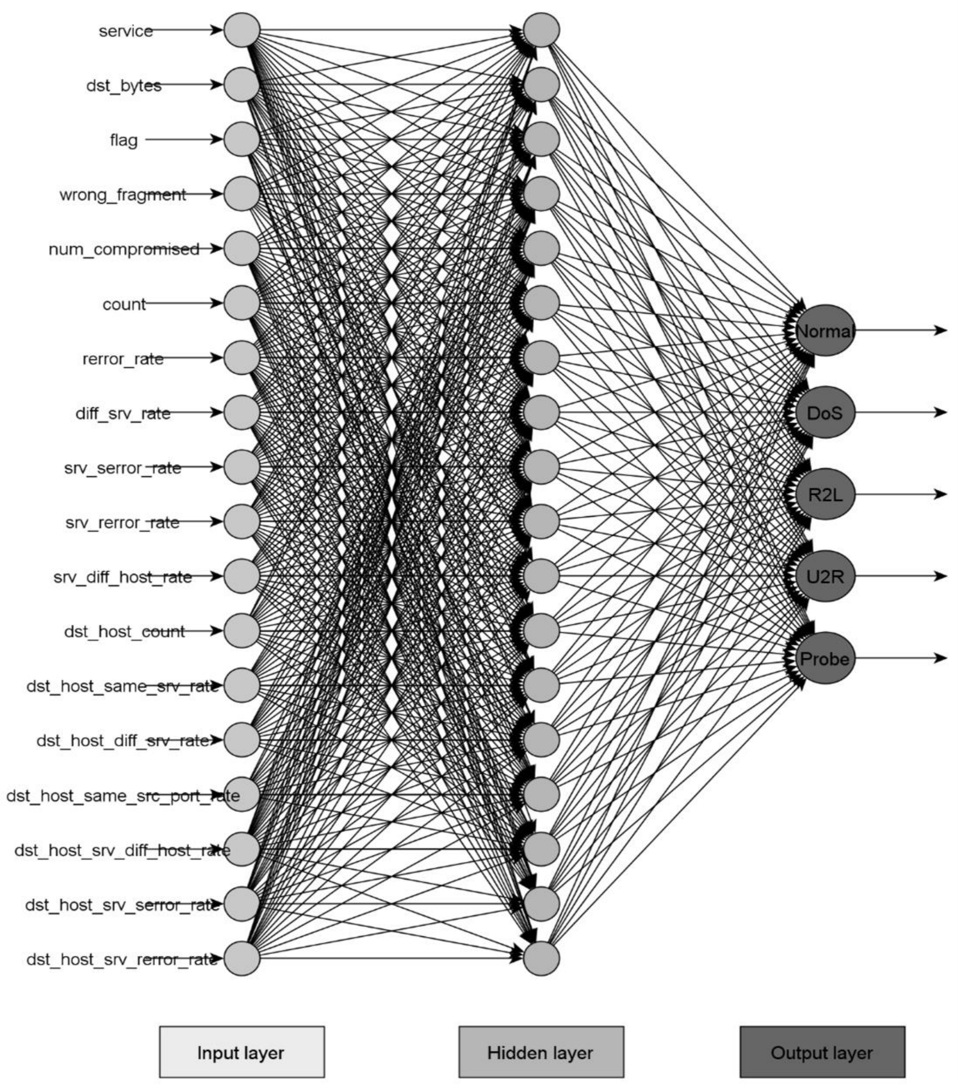

Figure 4. Architecture of neural network.

The results of training and testing of the designed neural network show a possibility of its application for the solution of a problem of detection of the network computer attacks. The neural network correctly classifies the activity in the network, in 93% of cases recognizing actions of the malefactor. Results of the research allows conclude that the offered neural network is capable of high probability to recognize the network attacks, at a rather small number of false positives (Table 3). Number epochs in Table 3 is number of neural network learning cycle.

The considered subset of parameters allowed to reduce the number of false negatives and accelerated the process of training the neural network.

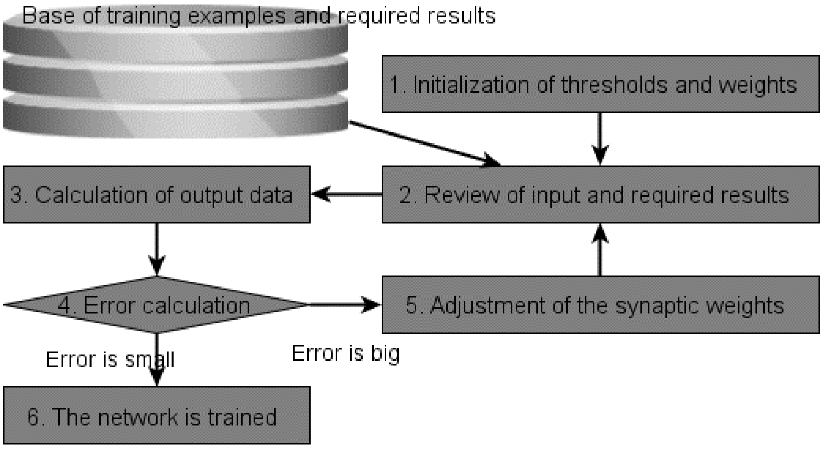
Base of training examples and required results
1. Initialization of thresholds and weights
2. Review of input and required results
3. Calculation of output data
4. Error calculation
5. Adjustment of the synaptic weights
Error is small
Error is big
6. The network is trained

Figure 5. Scheme of work of backpropagation algorithm.

Table 3. Results of work of neural network from number of the considered parameters.

Number of parameters	Accuracy	False positives	False negatives	Number of epoch
41	86.9	6.2	5.9	398
18	80.6	15.6	0.5	25

CONCLUSION

By training and testing an artificial neural network, it is possible to improve productivity of an intrusion detection system for the identification and classification practically of all events in system. However having a large amount of advantages, the artificial neural network demands time and the considerable volume of data for training to give the correct result. For achievement of the best results, it is possible to use all 41 parameter from NSL-KDD base.

REFERENCES

[1] Ushakov D.V., Development of the principles of the functioning of intrusion detection systems based on the model of a protected distributed system: abstract cand. tech. sci. diss. Moskow, MEPHI, 2005. 24 p.

[2] Polovko I.Yu., Peskova O.Yu., Analysis of functional requirements for intrusion detection systems, *Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki*, 2014, no. 2, pp. 86-92.

[3] Hofmann A., Sick B., Evolutionary Optimization of Radial Basis Function Networks for Intrusion Detection, *Proceedings, International Joint Conference on Neural Networks*. 2003. Vol.1, pp. 415- 420.

[4] Open Web Application Security Project. Available at: https://www.owasp.org/index.php/Intrusion_Detection (accessed 20.04.2018).

[5] Goncharov V.A., Przhegorlinskiy V.N., The method of detecting network attacks, based on a cluster analysis of the interaction of nodes of the computer network, *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta*, 2011, no. 36, pp. 3- 10.

[6] Middlemiss M., Dick G., Feature Selection of Intrusion detection data using a hybrid genetic of hybrid Intelligent systems, In: A. Abraham, M. Köppen and K. Franke (eds.), *Design and Application of Hybrid Intelligent Systems, IOS Press Amsterdam*, 2003. pp. 519-527.

[7] Kondrat'ev A.A., Talalaev A.A., Tishchenko I.P. et al., Methodological support of intelligent systems to protect against network attacks, *Sovremennye problemy nauki i obrazovaniya*, 2014, no. 2, p.119.

[8] Branitskiy A.A., Kotenko I.V., Analysis and classification of methods for detecting network attacks, *Trudy SPIIRAN*, 2016, no. 45, pp. 207-244.

[9] Sammany M., Sharawi M., El-Beltagy M. and Saroit I., Artificial Neural Networks Architecture for Intrusion Detection Systems and Classification of Attacks, *The 5th International Conference INFO2007*, 2007. pp. 24–26.

[10] Moradi M., Zulkernine M., A Neural Network Based System for Intrusion Detection and Classification of Attacks, *Proceedings of the IEEE International Conference on Advances in Intelligent Systems-Theory and Applications*, 2004.

[11] NSL-KDD dataset. Available at: http://www.unb.ca/cic/datasets/nsl.html (accessed 20.11.2017).

[12] Selim S., Hashem M., Nazmy T.M., Intrusion Detection using Multi-Stage Neural Network, *International Journal of Computer Science and Information Security*, 2010, vol. 8, no. 4, pp. 14–20.

[13] Cannady J., Artificial Neural Networks for Misuse Detection, *Proceedings of the 21st National Information Systems Security Conference*, 1998, pp. 368–381.

[14] Hoglund A.J., Hatonen K., Sorvari A.S., A Computer Host-Based User Anomaly Detection System Using The Self-Organizing Map, *Proceedings of the IEEE-INNSENNS International Joint Conference on Neural Networks*, 2000, vol. 5, pp. 411–416.

[15] Wang W., Guan X., Zhang X., et al., Profiling program behavior for anomaly intrusion detection based on the transition and frequency property of computer audit data, *Computers & Security*, 2006, vol. 25, Issue 7, pp. 539–550.

[16] Bivens A., Palagiri C., Smith R., Szymanski B. and Embrechts M., Network-Based Intrusion Detection Using Neural Networks, *Intelligent Engineering Systems through Artificial Neural Networks*, 2002, vol. 12, pp. 579–584.

[17] Jirapummin C., Wattanapongsakorn N., Kanthamanon P., Hybrid Neural Networks for Intrusion Detection System, *Proceedings of the 2002 International Technical Conference on Circuits, Systems, Computers and Communications*, 2002, vol. 7, pp. 928–931.

[18] Hofmann A., Horeis T., Sick B., Feature selection for intrusion detection: an evolutionary wrapper approach, *2004 IEEE International Joint Conference on Neural Networks*, 2004, vol. 2, pp. 1563-1568.

[19] Kruglov V.V., Borisov V.V., Artificial neural networks. Theory and practice, *Moskow, Goryachaya liniya – Telekom,* 2001. 382 p.

[20] Osovskiy S., Neural networks for information processing, *Moskow, Finansy i statistika*, 2002. 344 p.

[21] Mahmood, D., Feature Based Unsupervised Intrusion Detection, *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 2014, vol. 8, no. 9, pp. 1665 - 1669.

[22] Yogendra K.J., Upendra, Intrusion Detection using Supervised Learning with Feature Set Reduction, *International Journal of Computer Applications*, 2011, vol. 33, no. 6, pp. 22-31.

[23] Singh N., Kaur A., Feature selection for artificial neural network based intrusion detection system, *International Journal for Technological Research in Engineering*, 2015, vol. 2, no. 11, pp. 2681-2683.

[24] Shrivas A.K., Singhai S.K., Hota H.S., An Efficient Decision Tree Model for Classification of Attacks with Feature Selection, *International Journal of Computer Applications*, 2013, vol. 84, no. 14, pp. 42-48.

[25] Shrivas A.K., Dewangan A.K., An Ensemble Model for Classification of Attacks with Feature Selection based on KDD99 and NSL-KDD Data Set, *International Journal of Computer Applications*, 2014, vol. 99, no. 15, pp. 8-13.

[26] Mukherjee S., Sharma N., Intrusion Detection using Naive Bayes Classifier with Feature Reduction, *Procedia Technology*, 2012, vol. 4, pp. 119-128.

[27] Imamverdiev Ya.N., Sukhostat L.V., Detection of anomalies in network traffic based on informative signs, *Radioelektronika, informatika, upravlenie*, 2017, no. 3, pp. 113-120.

[28] Sethuramalingam S., Naganathan E.R., Hybrid feature selection for network intrusion detection, *International Journal of Computer Science and Engineering*, 2011, vol. 3, no. 5, pp. 1773–1780.

[29] Archer K.J., Kimes R.V., Empirical characterization of random forest variable importance measures, *Computational Statistics & Data Analysis*, 2008, no. 4, pp. 2249–2260.

[30] Feng D., Chen F., Xu W., Supervised feature subset selection with ordinal optimization, *Knowledge-Based Systems*, 2014, Vol. 56, pp. 123–140.

[31] Rojas R., Neural Networks. A Systematic Introduction, *Springer-Verlag, Berlin, New York*, 1996. 502 p.

[32] Mustafaev A.G., Neural network system for detecting computer attacks based on network traffic analysis, *Voprosy bezopasnosti*, 2016, no. 2, pp.1-7. doi:10.7256/2409-7543.2016.2.18834.

Information about the author:

Arslan Gasanovich Mustafaev– Professor at the Department of information technologies and information security, Dagestan State University of National Economy. Areas of Research are intrusion detection systems and information security.

Manuscript received on 04 September 2018