ATLANTIS PRESS

Advances in Intelligent Systems Research, volume 166

7th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS 2019)

Distributed Intelligent System of Network Traffic Anomaly Detection Based on Artificial Immune System

Vladimir Vasilyev
Ufa State Aviation Technical University
Ufa, Russia
vasilyev@ugatu.ac.ru

Rinat Shamsutdinov
Ufa State Aviation Technical University
Ufa, Russia
shamsutdinov.rinat.r@gmail.com

***Abstract*—The paper analyzes the essence of intrusion detection systems, identifies the relevance of detecting unknown attacks with a low number of False Positives, and identifies the significant parameters of the NSL-KDD dataset network connections. The authors have developed a distributed system for detecting network anomalies, using the mechanisms of an artificial immune system. A series of computational experiments was conducted that demonstrated a high level of efficiency of the developed system and a low percentage of False Positives.**

Keywords—information security, network attack, intrusion detection system, artificial immune system, network security.

I. INTRODUCTION

According to Positive Technologies Report [1], in 2018 the amount of organizations financial investments in ensuring information security significantly increased. This is facilitated by high profile public incidents of recent years, formed personal experience of companies, demonstrating in practice the results of neglecting information protection – the consequences of sensational epidemics, for example, WannaCry, NotPetya, BadRabbit.

The total number of companies that faced targeted attacks in 2017 almost doubled, every second large organization found traces of the intruders presence in its infrastructure. According to CISCO [2], the complexity and resilience of network attacks has increased significantly in recent years.

According to the results of the penetration testing series conducted by Positive Technologies [3], it was possible to overcome the network perimeter and gain access to local network resources in 92% of external penetration testing projects. In the half of companies, an attacker can overcome the network perimeter in one step. According to the Central Bank of the Russian Federation, the damage only to Russian banks from cyber attacks in 2018 amounted to 76.49 million rubles [4].

All of the above causes the urgency of the detecting newest and unknown network attacks problem. The goal of this work is to build and test a network attack detection system based on the artificial immune system mechanisms.

The paper is organized as follows. Section 2 is devoted to general issues of intrusion detection systems construction. Section 3 describes mechanisms of artificial immune system behavior. The procedure of data preprocessing is described in Section 4. The description of developed system and results of computational experiments are presented in Sections 5 and 6, and the paper is finished by conclusion.

II. INTRUSION DETECTION SYSTEMS

Intrusion Detection Systems (IDS) are designed to detect certain types of activity related to the threat of unauthorized access to the protected information, and information processing systems, and in case of IPS systems (Intrusion Prevention Systems) also to prevent from intrusions [5].

IDSs contain the sensory subsystem, analytical subsystem, system log, and management console [6]. There are host-based and network-based IDS, active and passive IDS, and IDS based on the protocol [7]. One can use various methods for detecting incidents using IDS technologies, among which the most popular are signature-based attack detection and attack detection by anomalous behavior elicitation [8].

As noted in [2], systems based on detection of anomalies using unsupervised machine learning are characterized by the highest probability of detecting previously unknown network attacks. The disadvantage of such systems is a high level of False Positives. However, the mechanisms of the artificial immune systems significantly reduce the level of False Positives. This is the reason for the choice of this machine learning method for the designed system.

III. ARTIFICIAL IMMUNE SYSTEM

Artificial immune systems and immunocomputing are developing in the framework of computational intelligent approaches like genetic algorithms and artificial neural networks, also known as neurocomputing [9]. In [10] the construction of a system for protecting the distributed computing environment with use of an artificial immune system is considered.

Immunocomputing technology is based on principles (especially – mathematical models) of information processing by proteins and immune networks. Table 1 shows a clarifying analogy between neurocomputing and immunocomputing.

TABLE I. ANALOGY BETWEEN NEUROCOMPUTING AND IMMUNOCOMPUTING

Approach	Neurocomputing	Immunocomputing
Basic element	Artificial neuron	Formal protein
Network	Artificial neural network	Formal immune network
Hardware	Neurochip	Immunochip

Since artificial neural network is formed as a "hardwired" network of artificial neurons, the essential difference between neural and immune computing is that a formal immune network represents a network of free interactions (bindings) between formal proteins [9].

But as it was presented in [11, 12], in real recognition tasks immunocomputing exceeds its main competitors (artificial neural networks and genetic algorithms), at least 40 times in speed and 2 times in recognition error-free.

The basis of the immune system is its ability to distinguish between "self" (the body's own molecules, cells, and tissues) and "nonself" (foreign substances, such as viruses or bacteria) [13].

In the human body while ingesting harmful microorganisms (antigens) an immune response occurs. The main participants in the immune response are lymphocytes that are able to recognize antigens and destroy them, and also under certain conditions undergo mutations in order to acquire the ability to quickly distinguish hostile cells from the cells of their bodies [14].

This discrimination ability is associated with the mechanism of positive and negative selection in the thymus. This discrimination between self and nonself is based on the affinity between lymphocyte receptors and major histocompatibility complex (MHC) molecules. In the thymus, T-cell gene rearrangements generate diverse T-cell receptors, and T-cells that recognize MHC molecules are positively selected [15]. Then the T-cell is subjected to negative selection – those T-lymphocytes that react to the body's own cells are destroyed.

Formal immune system is defines as a set of cells. Every cell has real-valued point (vector) of multi-dimensional Euclidean space. Let cell V_1 "recognize" cell V_2 if the distance between them is lower than some threshold. The distance between cells is determined by the number of element-wise matching the vector-row values – the affinity.

IV. DATA PREPROCESSING

To test the effectiveness of the real network attacks detection by the developed system, it was decided to use NSL-KDD dataset [16]. NSL-KDD is an improved KDD Cup 99 dataset generated by emulating the military network environment in 1999. NSL-KDD is the set of data strings characterizing normal and abnormal network connections, each string contains 41 parameters. The analysis of such data would take a long time, so it was necessary to reduce the length of the analyzed strings.

Consider the parameter sets proposed in the scientific literature. In [17], the DPSO algorithm was used to find the significant parameters. The idea of this algorithm is to solve the optimization problem by modeling the particles population behavior in the parameter space. In [18], the SVDF algorithm was used. It is a variation of the support vector method. First, the initial data set was fed to the input of the classifier for training. Then, to determine the importance of the parameters, the classifier's decision function was used.

In [19], the 5 most significant parameters for each type of attack were obtained by removing one parameter at a time. A set of parameters proposed in [20] was also considered. However, the parameters proposed in [17-20] are different for each type of attack, but we need here a universal set of parameters.

The paper [21] suggests 11 specific parameters, but it was not possible to detect threats using it. In [22], the compression of the KDD set using the singular decomposition of matrices was proposed. This compression is effective and supports full recovery with a slight error, however it allows as the classification of simultaneously compressed data and does not allow analyzing all new and new strings of network activity. In this regard, it was decided to independently allocate significant parameters of the network connections NSL-KDD.

First of all, the NSL-KDD dataset was divided into normal activity data and anomaly data, and then each parameter was encoded in a range of values not exceeding the value range of one byte. Thus, the data were pre-processed. The pre-processed data were recorded in a binary file.

The corresponding elements of each string of anomalous activity A_j and each string of normal activity N_i are compared to find a pair of strings with the maximum number of matching elements for A_j with the strings of the set N. When such a pair of strings is found, each matching element is replaced by a one, each not matching element replaced by zero, and the resulting string is recorded in a separate file, on the basis of which the percentage of matches for each parameter between the strings of normal and anomalous activity was calculated. The results obtained are ranked by the lowest percentage of matches.

It is better to choose the parameters with the minimum number of matches. It was decided to conduct a series of computational experiments with the first 16 ranked parameters, then gradually reduce the number of parameters, and in case of unsatisfactory analysis result with 16 parameters gradually increase parameters quantity.

The initial NSL-KDD dataset was divided into 4 sets as follows:

- the first set is the half of attack data contained in NSL-KDD, intended for training the system;
- the second set is the other half of attack data contained in the NSL-KDD, intended for testing the system;
- the third set is the half of normal activity data contained in the NSL-KDD, intended to train the system;

- the fourth set is the other half of normal activity data contained in NSL-KDD, intended for testing the system.

Each such data set was saved in a separate binary file.

V. Description of Developed System

The immune system is a distributed multi-level mechanism of protection against foreign microorganisms, viruses and pathogens [22]. An artificial immune system, by analogy with the natural immune system, consists of a variety of artificial lymphocytes, each of which contains a detection field and is tolerant to the normal state of the controlled system. For the representation of formal lymphocytes, the class "*Lymphocyte*" was described, with the features:

- the feature "*Value*" is a byte array and serves as a detection field;
- the "*ReactionCount*" feature is the number of True Positives;
- the "*FalseReactionCount*" feature is the number of False Positives;
- the feature "*Age*" represents the age of the lymphocyte;
- the "*IsClone*" feature determines whether a lymphocyte is a newly created clone;
- the feature "*Type*" is the type of anomaly detected;
- the "*TypeCode*" feature is the coded numeric value of the "*Type*" feature.

Data for analysis by an artificial immune system should be a set of strings. The length of the detection string of each lymphocyte is identical to the length of the analyzed string. The main mechanisms of the developed system include:

- lymphocyte generation subsystem;
- subsystem of lymphocyte negative selection;
- subsystem of lymphocyte reaction determination;
- subsystem of lymphocyte clonal selection;
- lymphocyte renewal subsystem with preservation of immune memory.

The scheme of interaction between the modules of the developed system is shown in Fig. 1.

A. Lymphocyte Generation

It should be noted that before starting the lymphocyte generation subsystem, the limits of the generated values should be determined, according to the maximum value for each parameter after its preprocessing. Since the maximum number of different protocols in NSL-KDD is 65, it does not make sense to create detectors with a value of 255 for this parameter.

The system is primarily aimed at identifying unknown network attacks, but it would not be superfluous to add the ability to classify known attacks. This complicates the generation process. A total of 500,000 lymphocytes were generated.

In order to train the system to detect and classify known network attacks, for each string of training data about attacks an instance of the "*Lymphocyte*" class was created with the value of detection field identical to that string.

The values of "*Type*" and "*TypeCode*" of such a lymphocyte correspond to the type of attack that the training string contains. The number of True and False Positives of such a lymphocyte initially is zero.

After generation, such a lymphocyte was transferred to the negative selection subsystem, and if it successfully passed a negative selection, it was added to the lymphocyte array. If not, the lymphocyte was destroyed and no further was created for this string.

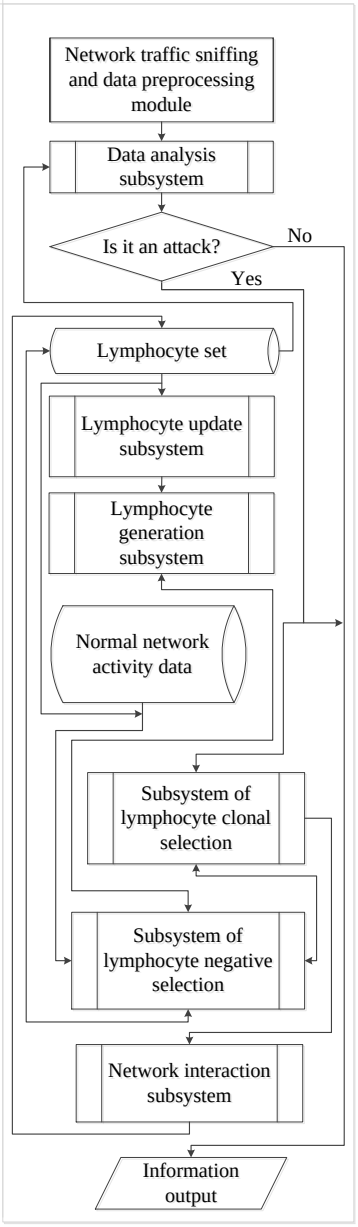

Fig. 1. The modules interaction scheme of the developed system

In order to train the system in detecting unknown attacks, a random number in the range from zero to a certain maximum is determined for each element of the detection string. An instance of the class "*Lymphocyte*" is created with

the obtained value of the detection string, zero number of true and False Positives, and zero age. The value of the "*Type*" feature of such a lymphocyte is "*new*". After which the lymphocyte was transferred to the negative selection subsystem. If the lymphocyte successfully passed a negative selection, it was added to the lymphocyte array, otherwise it was destroyed, a new lymphocyte was generated in its place.

B. Determination of the Lymphocyte Reaction

The lymphocyte reaction is determined as follows. Calculate the number of element-wise matching the values between the analyzed string and the field "*Value*" of the lymphocyte. This number is referred to as affinity. If affinity reaches a threshold defined here by one less than the number of parameters, it is considered that the lymphocyte has reacted. Lymphocytes that have detected an attack are subject to clonal selection, with the exception of their reaction during the negative selection procedure. The lifespan of the reacted lymphocytes is significantly increased.

C. Lymphocyte Negative Selection

One of the most important components of the artificial immune system, ensuring the tolerance of lymphocytes to normal activity, is the subsystem of negative selection, to the input of which the analyzed lymphocyte is fed. The subsystem selects the feature "*Value*" of the lymphocyte and compares it element-wise with feature "*Value*" of each lymphocyte that have been generated before, as well as with each string of normal activity.

If the lymphocyte at least once reacted to the normal behavior of the controlled system or to the other lymphocytes, it is destroyed. Otherwise it is considered that he underwent a negative selection procedure.

D. Lymphocyte Clonal Selection

The clonal selection subsystem first selects one of the worst lymphocytes to replace with a clone. Then it creates a clone of a lymphocyte fed into the input of the subsystem and replaces two random parameters in it with new random values ranging from zero to maximum.

The resulting clone is sent to the negative selection subsystem. If the lymphocyte successfully passed it, the clone is added to the set of lymphocytes to the place of the worst lymphocyte, otherwise another clone is created [23, 24].

It should be noted that the number of clones created for one reacted lymphocyte is determined by the administrator independently. In this study, 3 clones were created for a single lymphocyte.

E. Lymphocyte Update With Preservation of Immune Memory

The subsystem of lymphocyte renewal with preservation of immune memory with a certain frequency checks the number of reactions and the age of each lymphocyte. If the lifetime of any lymphocytes is over, they are destroyed, in their place new lymphocytes are generated. Immune memory is provided by a significantly increased life span of the reacted lymphocytes.

VI. Results of Computational Experiments

Evaluation of the system effectiveness includes 2 series of experiments. The first series was conducted to assess the effectiveness of detection and classification of known attacks by the system, as well as to assess the significant parameters of NSL-KDD. 10 iterations of the analysis of the same data were performed, since the system is independently trained during the analysis process. The analysis was conducted with the use of lymphocytes, both with random values of the detection field and with fully relevant training strings of data about attacks. Each iteration of the analysis was conducted alternately on two different hosts, which exchanged training information after each analysis iteration.

The second series of experiments was carried out to assess the effectiveness of the unknown attack detection. In this case, only lymphocytes with random values of the detection field were used, so all the attacks contained in NSL-KDD were unknown to the system. 19 iterations of analysis were performed.

According to the results of the first 16 parameters analysis, the efficiency of the system turned out to be high; therefore the number of analyzed parameters gradually decreased. The False Negative errors following the results of each iteration of the analysis using lymphocytes, including trained to classification of known attacks are summarized in Table 2.

TABLE II. The False Negative Errors Percentage

Iteration Number	Number of Parameters						
	9	***10***	***11***	***12***	***13***	***14***	***16***
1	0.16%	0.19%	0.19%	0.14%	0.15%	0.13%	0.02%
2	0.11%	0.14%	0.14%	0.13%	0.11%	0.11%	0.014%
3	0.11%	0.11%	0.10%	0.10%	0.10%	0.10%	0.013%
4	0.11%	0.11%	0.10%	0.10%	0.08%	0.08%	0.012%
5	0.11%	0.11%	0.10%	0.10%	0.05%	0.05%	0.011%
6	0.11%	0.11%	0.10%	0.10%	0.04%	0.04%	0.010%
7	0.11%	0.11%	0.10%	0.10%	0.04%	0.03%	0.009%
8	0.11%	0.11%	0.10%	0.10%	0.03%	0.03%	0.008%
9	0.11%	0.11%	0.10%	0.10%	0.02%	0.02%	0.007%
10	0.11%	0.11%	0.10%	0.10%	0.01%	0.01%	0.006%

According to Table 2, for the number of parameters less than 13 a certain limit was determined for reducing the percentage of the False Negative errors, the limiting values are highlighted in color. However, with the number of parameters from 13 and more, the percentage of the False Negative errors continues to decrease from iteration to iteration.

The False Positive errors based on the results of each iteration of the analysis using lymphocytes, including the trained to classification of known attacks are summarized in Table 3.

TABLE IV. THE FALSE POSITIVE ERRORS PERCENTAGE

Iteration Number	Number of Parameters						
	9	*10*	*11*	*12*	*13*	*14*	*16*
1	3.42%	4.96%	4.99%	6.13%	5.80%	5.80%	5.93%
2	2.80%	3.40%	3.45%	4.31%	4.16%	4.09%	4.29%
3	2.80%	2.40%	2.37%	2.52%	1.75%	1.69%	2.12%
4	2.80%	2.40%	2.37%	1.73%	1.46%	1.39%	1.46%
5	2.80%	2.40%	2.37%	1.73%	0.73%	0.70%	0.63%
6	2.80%	2.40%	2.37%	1.73%	0.68%	0.67%	0.56%
7	2.80%	2.40%	2.37%	1.73%	0.56%	0.55%	0.52%
8	2.80%	2.40%	2.37%	1.73%	0.50%	0.47%	0.43%
9	2.80%	2.40%	2.37%	1.73%	0.36%	0.36%	0.34%
10	2.80%	2.40%	2.37%	1.73%	0.28%	0.26%	0.21%

When choosing the number of parameters less than 13, the limit for reducing the False Positive errors is similarly observed. It would be logical to assume that not the thirteen parameters selected are significant, but the thirteenth parameter, however the percentage of matches between the the corresponding strings of normal and anomalous activity on it is 99.3%.

Thus, by the selected 13 parameters NSL-KDD (23; 24; 3; 30; 33; 29; 34; 35; 32; 4; 36; 40; 5), the system demonstrates the high level of detection of known attacks with its classification.

The results of the analysis using only the lymphocytes with randomly generated detection fields, for which each attack from NSL-KDD is unknown, are presented in Fig. 2.

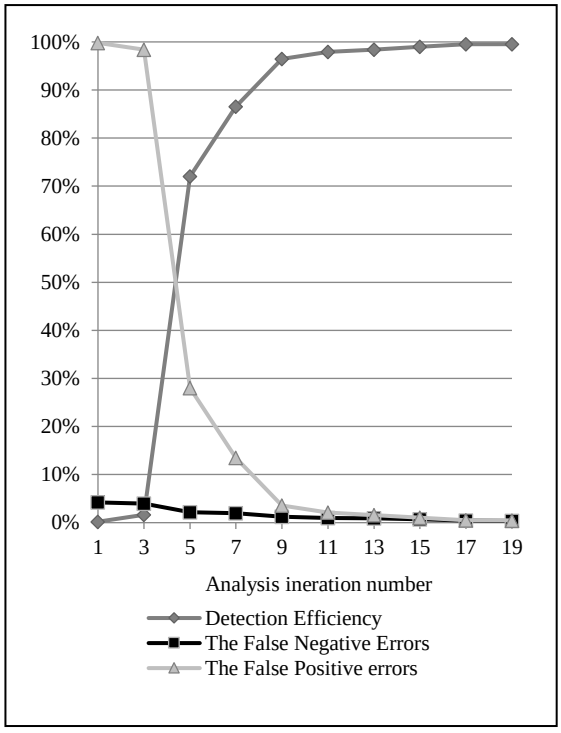

Fig. 2. The lymphocyte analysis results for which all NSL-KDD attacks were unknown

As it can be seen from Figure 2, the system demonstrates the high efficiency of detecting unknown attacks for it. According to the results of the nineteenth iteration of the analysis, the detection efficiency exceeded 99%; the level of the False Negative and the False Positive errors does not exceed 0.5%.

VII. CONCLUSION

Thus, the significant parameters of the NSL-KDD network connection dataset were defined, that is the parameters: 3, 4, 5, 23, 24, 29, 30, 32, 33, 34, 35, 36, 40. The distributed attack detection system has been developed using the mechanisms of an artificial immune system, which has demonstrated a high efficiency in detecting both known and unknown network attacks. Moreover, each host with an installed system upon detecting an attack not only independently trained to better detect similar attacks, but also taught this to other hosts of the distributed system.

ACKNOWLEDGMENT

The work was supported by the Russian Basic Research Foundation (RBRF) grant №17-48-020095.

REFERENCES

[1] Kiberbezopasnost' 2017–2018: cifry, fakty, prognozy [Cybersecurity 2017-2018: numbers, facts, forecasts], Positive Technologies, available at: http://permsite.ru/files/2017/12/cybersecurity-2017-2018-rus.pdf (accessed 12.02.2019). (in Russian).

[2] CISCO 2018 Annual Cybersecurity Report, CISCO, available at: https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2 (accessed 10.02.2019). (in Russian).

[3] Uyazvimosti korporativnyh informacionnyh sistem, 2019 [Corporate Information System Vulnerabilities, 2019], Positive Technologies, available at: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019 (accessed 09.02.2019). (in Russian).

[4] CB nazval ushcherb rossijskih bankov ot kiberatak v 2018 godu [Central Bank called the damage to Russian banks from cyber-attacks in 2018], RBC, available at: https://www.rbc.ru/rbcfreenews/5bc881ea9a7947189fe00a9a (accessed 09.02.2019). (in Russian).

[5] V. I. Vasilyev, R. R. Shamsutdinov, Distributed Intrusion Detection System Based on Immune System Mechanisms, Proceedings of the 6th All-Russian Scientific Conference «Information Technologies for Intelligent Decision Making Support», vol. 1, may 28-31, Ufa-Stavropol, Russia, 2018, pp. 237-244. (in Russian).

[6] A. A. Kornienko, I. M. Slyusarenko, Intrusion Detection Systems and Methods: Current State and Directions for Improvement, CIT Forum, available at: http://citforum.ru/security/internet/ids_overview/ (accessed 14.11.2018). (in Russian).

[7] V. I. Vasilyev, V. D. Kotov, Sovremennoe sostoyanie problemy obnaruzheniya setevyh vtorzhenij [The Current State of Network Intrusion Detection Problems], Vestnik Ufimskogo gosudarstvennogo aviacionnogo tekhnicheskogo universiteta [Bulletin of Ufa State Aviation Technical University], Ufa, 2012, no. 3, pp. 198-204. (in Russian).

[8] A. A. Branitsky, A. V. Kotenko, Analysis and Classification of Methods for Network Attack Detection, SPIIRAS Proceedings, St. Peterburg, 2016, no 2, pp. 207-244. (in Russian).

[9] A. O. Tarakanov, Immunocomputing for Intelligent Inrusion Detection, IEEE Computational Intelligence Magazine, 2008, vol. 3, no. 2, pp. 22-30.

[10] A. A. Krasnopevtsev, Yu. M. Tumanov, Primenenie iskusstvennoj immunnoj sistemy dlya zashchity sredy raspredelennyh vychislenij [The Use of an Artificial Immune System to Protect the Distributed Computing Environment], Bezopasnost` Informatsionnykh

Tekhnologiy [Information Technology Security], 2013, vol. 20, no. 1, pp. 63-65. (in Russian).

[11] A. O. Tarakanov, Y. A. Tarakanov, A Comparison of Immune and Genetic Algorithms for Two Real-Life Tasks of Pattern Recognition, Int. J. of Unconventional Computing, 2004, vol. 1.4, pp. 357-374.

[12] A. O. Tarakanov, Y. A. Tarakanov, A Comparison of Immune and Neural Computing for Two Real-Life Tasks of Pattern Recognition, International Conference on Artificial Immune Systems, Catania, 2004, pp. 236-249.

[13] T. Okamoto, Y. Ishida, Towards an Immunity-Based Anomaly Detection System for Network Traffic. In: Gabrys B., Howlett R. J., Jain L. C. (eds) Knowledge-Based Intelligent Information and Engineering Systems. KES 2006. Lecture Notes in Computer Science, 2006, vol 4252. Springer, Berlin, Heidelberg, pp. 123-130

[14] V. D. Kotov, Sistema obnaruzheniya atak na osnove tekhnologij iskusstvennyh immunnyh sistem [Attack Detection System Based on Artificial Immune System Technologies], Materialy dokladov Vserossijskoj nauchno-tekhnicheskoj konferencii studentov, aspirantov i molodyh uchenyh "Nauchnaya sessiya TUSUR-2009", Tomsk, 12-15 maya 2009, [Proceedings of the All-Russian Scientific and Technical Conference of Students, Postgraduates and Young Scientists "Scientific session TUSUR-2009", Tomsk, 12-15 may 2009], V-Spektr Publ, Tomsk, 2009, pp. 371-381. (in Russian)

[15] T. Okamoto, Y. Ishida, Framework of an Immunity-Based Anomaly Detection System for User Behavior. In: Apolloni B., Howlett R.J., Jain L. (eds) Knowledge-Based Intelligent Information and Engineering Systems. KES 2007. Lecture Notes in Computer Science, 2007, vol 4694. Springer, Berlin, Heidelberg, pp. 821-829.

[16] NSL-KDD dataset, available at: https://www.unb.ca/cic/datasets/nsl.html (accessed 25.02.2019).

[17] A. Zaind, M. Maarof, S. Shamsnddin, A. Abraham, Ensemble of One-class Classifiers for Network Intrusion Detection System, available at: http://www.softcomputing.net/ias08_1.pdf (accessed: 29.02.2018).

[18] S. Mukkamala, A. H. Sung, Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques, International Journal of Digital Evidence, 2003, vol. 1, no. 4, pp. 1-17.

[19] S. Mukkamala, A. H. Sung, A. Abraham, Modeling Intrusion Detection Systems Using Linear Genetic Programming Approach, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.83.544&rep=rep1&type=pdf (accessed: 29.02.2018).

[20] T. S. Chou, K. K. Yen, and J. Luo, Network Intrusion Detection Design Using Feature Selection of Soft Computing Paradigms, International Journal of Computational Intelligence, 2008, vol. 4, no. 3, pp. 196-208..

[21] R. V. Meshcheryakov, I. A. Khodashinsky, E. N. Gusakova, Evaluation of feature space for intrusion detection system, Izvestiya YUFU. Tekhnicheskie nauki [Transactions of SFedU. Technical Science], Taganrog, 2013, no. 12, pp. 57-63. (in Russian).

[22] V. I. Vasilyev, V. D. Kotov, Network Attacks Detection System Based on the Mechanisms of Immune Model, Izvestiya YUFU. Tekhnicheskie nauki [News of SFedU. Technical Science], Taganrog, 2011, no. 12, pp. 180-189. (in Russian).

[23] L. N. De Castro, F.J. Von Zuben, Learning and optimization using the clonal selection principle, IEEE Transactions on Evolutionary Computation. 2002, vol. 6, no. 3, pp. 239-251.

[24] V. I. Vasilyev, Intellektual'nye sistemy zashchity informacii [Intelligent information security systems], in Vasilyev V.I. (ed.), Innovatsionnoe mashinostroenie Publ., Moscow, 2017, 201 p. (in Russian).