УДК 004.056
DOI: 10.26102/2310-6018/2022.39.4.020

Hybrid intrusion detection system with the use of a classifiers committee

V.I. Vasilyev, A.M. Vulfin, V.E. Gvozdev, R.R. Shamsutdinov✉

Ufa University of Science and Technology, Ufa, Russian Federation
shrr2019@yandex.ru✉

Abstract. The issues of detecting network attacks to Industrial Internet of Things (IIoT) systems are analyzed. Existing approaches for detecting such attacks based on the use of artificial intelligence methods are considered. The high interest to integration of machine learning and artificial intelligence methods as a part of hybrid systems is emphasized. Such integration makes it possible to compensate the shortcomings of some algorithms due to the advantages of others. The goal of this research is to improve the efficiency of network attacks detection. The paper proposes the implementation of a multi-level hybrid attack detection system on the basis of combining several classifiers in the committee including the artificial immune system, the multilayer perceptron, and the random forest algorithm. The choice of these classifiers is due to their high classification efficiency and the ability of artificial immune system to detect unknown network attacks. The decision is made on the basis of the conclusion of each expert (classifiers) with the use of voting mechanism. Such approach provides more accurate result in accordance with the Condorcet's jury theorem. To carry out computational experiments for assessing the effectiveness of the proposed system, the NSL-KDD network traffic data set was employed. The results of experiments carried out demonstrate the high efficiency of the proposed hybrid attack detection system based on use of classifiers committee.

Keywords: information security, Industrial Internet of Things, intrusion detection system, network attack, NSL-KDD dataset.

Acknowledgments: the reported research was supported by RFBR grants No. 20-37-90024 and No. 20-08-00668.

For citation: Vasilyev V.I., Vulfin A.M., Gvozdev V.E., Shamsutdinov R.R. Hybrid intrusion detection system with the use of a classifiers committee. *Modeling, Optimization and Information Technology*. 2022;10(4). Available from: https://moitvivt.ru/ru/journal/pdf?id=1267 DOI: 10.26102/2310-6018/2022.39.4.020

Гибридная система обнаружения атак на основе комитета классификаторов

В.И. Васильев, А.М. Вульфин, В.Е. Гвоздев, Р.Р. Шамсутдинов✉

Уфимский университет науки и технологий, Уфа, Российская Федерация
shrr2019@yandex.ru✉

Резюме. В статье проанализированы вопросы обнаружения сетевых атак на системы промышленного Интернета вещей (Industrial Internet of Things, IIoT), рассмотрены существующие подходы к обнаружению таких атак, основанные на применении методов искусственного интеллекта. Подчеркнут высокий интерес к интеграции машинного обучения и методов искусственного интеллекта в составе гибридных систем. Такая интеграция позволяет компенсировать недостатки одних алгоритмов преимуществами других. Целью работы является повышение эффективности обнаружения сетевых атак. В статье предложено применение многоуровневой гибридной системы обнаружения атак на IIoT, основанной на комбинации нескольких классификаторов в составе комитета, включающего искусственную иммунную систему, многослойный персептрон, алгоритм случайного леса. Выбор этих классификаторов обусловлен их высокой эффективностью решения задач классификации, а также способностью искусственной иммунной системы обнаруживать неизвестные сетевые атаки. Решение принимается в результате вывода каждого эксперта (классификатора) на основе голосования. В соответствии с теорией присяжных Кондорсе такой подход обеспечивает более точный результат. Для проведения вычислительных экспериментов по оценке эффективности предлагаемой системы использовался набор данных сетевых соединений NSL-KDD. Результаты экспериментов демонстрируют высокую эффективность предлагаемой гибридной системы обнаружения атак на основе комитета классификаторов.

Ключевые слова: информационная безопасность, промышленный Интернет вещей, система обнаружения атак, сетевая атака, NSL-KDD.

Благодарности: работа выполнена при поддержке грантов РФФИ №20-37-90024 и №20-08-00668.

Для цитирования: Васильев В.И., Вульфин А.М., Гвоздев В.Е., Шамсутдинов Р.Р. Гибридная система обнаружения атак на основе комитета классификаторов. *Моделирование, оптимизация и информационные технологии.* 2022;10(4). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1267 DOI: 10.26102/2310-6018/2022.39.4.020 (на англ.).

Introduction

At present, Industrial Internet of Things (IIoT) systems are widely used, including a lot of different heterogeneous devices. A widespread use of such systems is accompanied by an increase in risks of violating their security. According to a 2020 Nokia Threat Intelligence Lab Report [1], IIoT devices account for 32.72 % of all infections on mobile networks. In 2019, this number was 16.17 %. According to [2], in 2015-2020 there was a significant increase in new samples of malware for IIoT.

There are variety of approaches to detecting network attacks on these systems, including behavioral methods, knowledge-based methods, machine learning, computational intelligence, etc. described in [3,4]. One of the promising areas is the development of Intrusion Detection Systems (IDSs) in a class of Hybrid Intelligent Systems (HISs) combining different Artificial Intelligence (AI) methods to achieve a synergistic effect and compensating the shortcomings of some algorithms due to the advantages of others.

For example, fuzzy logic systems are understandable and transparent for the user, but they are usually incapable of learning. Artificial neural networks (ANNs), otherwise, are capable of learning, but are opaque to the user. Their joint use as the parts of fuzzy neural network makes it possible to obtain an adaptive system capable of learning and at the same time transparent to the user [5].

According to [6], hybrid use of fuzzy cognitive maps and neuro-fuzzy network (ANFIS) improves forecasting accuracy of multivariate time series. In [7] joint application of ANN and Artificial Immune System (AIS) for diagnosis of sensor nodes faults in Wireless Sensor Networks (WSNs) is considered. The simulation results demonstrate the high efficiency of combined algorithm, its high diagnostic accuracy and low error rate.

In [8] other combinations of AI methods are considered such as ANN and evolutionary algorithms, fuzzy logic and evolutionary algorithms, machine learning and fuzzy logic, machine learning and evolutionary algorithms, etc.

The general idea of constructing IDS in the class of HIS is discussed in a number of publications [9-14]. The construction of such systems, as a rule, is based on a combination of ANN, cluster analysis, decision trees, support vector machine (SVM), different in their ideology. A separate promising group of IDS is presented by IDSs based on AIS technology in addition to other AI technologies.

The paper is organized as follows. Section 2 is devoted to related works analysis. Section 3 describes the proposed approach. The results of the conducted computational experiments are presented in Section 4, and the paper is finished by Conclusion.

Related work

AISs are used in IDS development because of their adaptability, high accuracy, low error rate, and the ability to detect unknown anomalies. In [15] the multilevel IDS based on the immune theory is proposed. The system includes blocks of B-cells, T-cells, dendritic cells and basophils. Here B-cells carry out the primary analysis of data. Further analysis of data is performed by dendritic cells; if any anomaly is detected, a signal is transmitted to the T-cell block, which generates a reaction and isolates the anomaly node.

In [16] the IDS for WSN is proposed that uses such AIS algorithms as negative selection, which ensures the system tolerance to the normal state, and clonal selection, which ensures an adaptability of the system, and a possibility of its self-learning. The LEACH protocol was employed in modeling. The following types of attacks were analyzed: Resource Depletion, Sinkhole, Wormhole, Sybil, and Selective Forwarding Attack. The architecture of IDS is built by means of the Immune Danger Theory.

AISs are used in separate publications as a part of Hybrid IDSs. In [17] a joint application of Deep Learning and Dendritic Cell Algorithm (DeepDCA) is proposed. The BoT-IoT dataset is used to evaluate the IDS performance. In this paper, the compression of the parameter space is implemented. A self-organizing ANN is used, which performs primary data processing and categorization of the input signal into signals about danger and safe state. Further analysis is carried out by dendritic cells. The results of comparison with such classifiers as k-nearest neighbors, SVM, multilayer perceptron, Naive Bayes are presented. The DeepDCA demonstrates the best detection accuracy.

The joint use of AIS and self-organizing Kohonen map in [18] made it possible to increase the efficiency of detecting Denial-of-Service and User-to-Root attacks with a low level of False Positives. In this case, the work of IDS occurs in 2 stages:

- filtering features of network connections using immune detectors trained by the method of negative selection; thereby eliminating those samples that correspond to normal connections;
- anomalous samples are processed by self-organizing Kohonen map and are grouped into separate clusters with similar features.

In [19] a constructive virus detection algorithm based on combination of AIS and Deep Belief Network (DBN) is proposed. It includes:

- formation of feature vectors;
- formation of two datasets: R_1 – ‘Benign’ and R_2 – ‘Virus’;
- randomly generating a set of detectors (they have the same length as the vectors in R_1 and R_2);
- negative selection and clonal selection: removal from the set of detectors R' the vectors having the maximum affinity (similarity) in relation to vectors from R_1, i.e. construction of a set of R_2', consisting of vectors “most likely a virus”;
- selection from the set R_2' vectors having maximum affinity to vectors from R_2;
- the resulting set R_2'' is used as a training set for the DBN;
- using DBN as a classifier; the problem of recognizing a specific virus is solved, i.e. for each input feature vector a decision is made: ‘Benign’ or ‘Virus’.

In [20], the unification of the theory of negative selection with the construction of production rules for knowledge processing is considered. The results of the experiments on the

DARPA KDD-99 dataset are presented. The proposed approach allows detecting various types of attacks; production rules are generated using the WEKA package in the form of decision trees.

In [21-23], multilayer ANNs, which are generated using the clonal selection method, were selected as immune detectors.

In [24], Kohonen's ANNs are used as detectors which respond to changes in network traffic statistics. The block for forming the immune memory implements the operations of cloning and mutating detectors. The mutation consists in random changing of the weights of the ANN detector by a small amount; the mechanism for cloning the detectors consists in creating 5 copies of the detector that detected the anomaly.

In [25], an Artificial Neural Immune Network (ANIN) is proposed, which is a combination of an ANN and an Artificial Immune Network (AiNet). In ANIN, each ANN is a detector and many of them are used in such a way that they can cooperate to solve a problem. AiNet is used to train ANN-based detectors both in terms of adjusting weights and their structure. Experimental results showed the network attack detection accuracy up to 87.98 % with low false alarms.

A combination of AI algorithms allows us to provide higher accuracy. According to [26] Condorcet's Jury Theorem, experts having the similar competence above 0.5 make collective decision using a majority rule which approaches to 1 if a number of experts increases. According to [27], the combined algorithm error is guaranteed to be lower than the average error of these algorithms.

Proposed approach

As it is shown in [28-29], Random Forest (RF) classifier and ANN demonstrate a high level of attacks detection. This paper proposes the construction of the committee of classifiers, containing ANN, AIS and RF. Each classifier analyzes data independently of others. As it can be seen in Figure 1, the final decision is made based on the totality of the opinions of all classifiers.

To assess the effectiveness of the proposed approach, NSL-KDD dataset was chosen [30]. The dimension of the feature space was reduced from 41 to 16 by the way described in [31]. Further, the quantitative features were scaled by bringing them to zero mean value and single deviation, the categorical features were recoded to the uniform numerical scale. The analysis of network traffic is carried out as follows. The information contained in the headers of the network traffic packets is transferred to the Feature Extraction block, where the above-defined features are selected, a feature vector is formed, which is transferred to the Classifier Committee. The following measures were used to assess the effectiveness of IDS:

– *False Negatives* (*FN*) – a number of abnormal activity samples determined as normal ones;

– *False Positives* (*FP*) – a number of normal activity patterns identified as anomalies;

– *True Negatives* (*TN*) – a number of correctly identified samples of normal activity;

– *True Positives* (*TP*) – a number of correctly detected anomalies;

– *False Negatives Rate* (*FNR*) calculated as

$$FNR = \frac{FN}{FN + TP}; \tag{1}$$

False Positives Rate (*FPR*) calculated as

$$FPR = \frac{FP}{FP + TN}; \tag{2}$$

True Negatives Rate (*TNR*) calculated as

$$TNR = \frac{TN}{TN + FP}; \tag{3}$$

True Positives Rate (*TPR*) or *Recall* is the proportion of correctly detected anomalies among all anomalies calculated as

$$TPR = \frac{TP}{TP + FN}; \tag{4}$$

Precision is the proportion of correctly identified anomalies among all samples identified as anomalies calculated as

$$Precision = \frac{TP}{TP + FP}; \tag{5}$$

Accuracy – the proportion of correctly classified samples among all samples calculated as

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}; \tag{6}$$

F_1 score is harmonic means of Precision and Recall calculated as

$$F_1 score = \frac{2 \times Precision \times TPR}{Precision + TPR}. \tag{7}$$

Results of computational experiments

Computational experiments were conducted as follows. Feature preprocessing, i.e. scaling and coding of numerical and categorical variables, was performed. Then the attack classes with less than 800 examples were removed from dataset. The dataset balancing procedure was performed using resampling operation (SMOTE [32]) with KNN for augmentation of small classes up to 5000 examples and selection of 15000 examples from two classes with a significantly large amount of initial data.

Then the initial dataset was divided into training, test and validation datasets. RF with hyperparameter optimization (cross validation, selection by metric F_1 score) was built. Its parameters were estimated on the test dataset that did not participate in hyperparameter optimization.

ANN was created and trained on data with overfitting control and early shutdown. Then, similarly to RF, ANN was tested on the test dataset. AIS was trained not only to detect unknown attacks, but also to classify known ones using the method described in [31].

After that, the analysis procedure was started. The data were submitted to each of the classifiers. The opinions of each of them were aggregated and transmitted to the Expert block, where voting was held using the majority principle.

It should be noted that ANN architecture parameters such as a number of neurons in the hidden layer and the coefficient of thinning connections were checked. It was shown that the optimal ANN architecture with 32 neurons in the hidden layer had been used.

The experiments showed that Classifiers Committee results were worse than AIS results in 4 measures out of 7. It is because AIS, due to negative selection, has a significantly lower FPR measure and higher TNR value than ANN and RF. And several times, for instance, normal sample was categorized as normal one by AIS and as anomalous one by ANN and RC. Finally, the sample was considered as anomalous one by majority of votes.

To solve this problem, the Expert block was reconfigured as follows. In determining whether a sample is normal or anomalous one, the priority has become not as the opinion of the majority, but as the opinion of AIS. The class of attack was still determined on the basis of majority voting. The results are summarized in Table 1.

As we can see, the Classifiers Committee results after that became better than the results of each single classifier. Thus, the use of the committee of classifiers makes it possible to compensate the shortcomings of some algorithms due to the advantages of others, and to obtain better results in network attacks detection and classification. The proposed approach can be applied to ensure the security of various types of networks, including IIoT.

Table 1 – Findings
Таблица 1 – Полученные результаты

Measure	ANN	RFC	AIS	Average Value	Classifiers Committee
FNR	0,003	0,001	0,002	0,002	0,001
FPR	0,013	0,003	0,001	0,006	0,001
TNR	0,987	0,997	0,999	0,994	0,999
TPR (Recall)	0,997	0,999	0,998	0,998	0,999
Precision	0,985	0,996	0,999	0,993	0,999
Accuracy	0,992	0,998	0,999	0,996	0,999
$F_1 score$	0,991	0,997	0,998	0,996	0,999

Conclusion

Industrial Internet of Things (IIoT) systems are widely used, including a lot of different heterogeneous devices. An important issue in this field is the issue of ensuring their safety. One of the promising areas here is the development of Intrusion Detection Systems in the class of Hybrid Intelligent Systems combining different Artificial Intelligence methods to achieve a synergistic effect and compensating the shortcomings of some algorithms due to the advantages of others.

A combination of algorithms allows increasing system accuracy. According to [26], Condorcet's Jury Theorem shows that under a dichotomous choice experts who all have the similar competence above 0.5 can make collective decisions using the majority rule with a competence that approaches 1 as either the size of the group or the experts competence goes up.

This paper proposes the construction of the Committee of Classifiers, including ANN, AIS and RF. Each classifier analyzes data independently of others. The final decision is made based on the totality of the opinions of all classifiers.

Computational experiments showed that Classifiers Committee results were better than the results of each single classifier. Thus, the use of the committee of classifiers makes it possible to obtain better results in network attacks detection and classification. This approach can be applied in the field of IIoT security.

REFERENCES

1. Threat Intelligence Report 2020. *NOKIA*. Available from: https://pages.nokia.com/T005JU-Threat-Intelligence-Report-2020.html?_ga=2.216248470.16 53315497.1608038999-829562352.1608038999 (accessed on 23.09.2021).
2. Chto ugrozhaet promyshlennomu internetu veshchej i kak ot etogo zashchitit'sya. *Kaspersky Lab, Vc.ru*. Available from: https://vc.ru/kaspersky/265770-chto-ugrozhaet-

promyshlennomu-internetu-veshchey-i-kak-ot-etogo-zashchititsya (accessed on 23.09.2021). (In Russ.).

3. Branitskiy A.A., Kotenko I.V. Analysis and classification of methods for network attack detection. *Trudy SPIIRAN = SPIIRAS Proceedings*. 2016;2(45):207–244. DOI: 10.15622/sp.45.13. (In Russ.).
4. Dobkach L. An analysis of methods for identifying computer attacks. *Legal Informatics*. 2020;1:67–75.
5. ICT219 Lecture 11 – Hybrid Intelligent Systems. *StuDocu*. Available from: https://www.studocu.com/en-au/document/murdoch-university/intelligent-systems/ict219-lecture-11-hybrid-intelligent-systems/1280311 (accessed on 23.09.2021).
6. Averkin A.A., Yarushev S.A., Pavlov V.U. Cognitive hybrid systems for decision support and forecasting. *Programmnye produkty i sistemy = Software & Systems*. 2017;4(30):632–642. DOI: 10.15827/0236-235X.120.632-642. (In Russ.).
7. Lin L. An intelligent fault diagnosis model of WSN based on artificial immune system. *2020 5th International Conference on Smart Grid and Electrical Automation (ICSGEA)*. 2020:405–408. DOI: 10.1109/ICSGEA51094.2020.00093.
8. Dounias G. Hybrid computational intelligence in medicine. Available from: http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=EE461823CC470C45FC8909C60AC93956?doi=10.1.1.71.6170&rep=rep1&type=pdf (accessed on 25.07.2021).
9. Panda M., Abraham A., Patra M.R. Hybrid intelligent systems for detecting network intrusions. *Security and Communication Networks*. 2012;8(16). Available from: https://www.researchgate.net/publication/260408971_Hybrid_intelligent_systems_for_detecting_network_intrusions. DOI: 10.1002/sec.592 (accessed on 15.08.2021).
10. Salama M.A., Ramadan R., Darwish A., Eid H.F. Hybrid intelligent intrusion detection scheme. *Advances in Intelligent and Soft Computing*. 2011;96:295–302. DOI: 10.1007/978-3-642-20505-7_26.
11. Khan M.A., Kim Y. Deep learning-based hybrid intelligent intrusion detection system. *Computers, Materials & Continua*. 2021;1(68):671–687. DOI: 10.32604/cmc.2021.015647.
12. Panda M., Abraham A., Patrac M.R. A hybrid intelligent approach for network intrusion detection. *Procedia Engineering*. 2012;30:1–9. DOI: 10.1016/j.proeng.2012.01.827.
13. Chavez A., Lai C., Jacobs N., Hossain-McKenzie S., Jones C.B., Johnson J., Summers A. Hybrid intrusion detection system design for distributed energy resource systems. *IEEE CyberPELS;* 2019. Available from: https://ieeexplore.ieee.org/document/8925064 (accessed on 28.07.2021).
14. Alem S., Espes D., Martin E., Nana L., De Lamotte F. A Hybrid Intrusion Detection System in Industry 4.0 Based on ISA95 Standard. *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, 2019:1–8, DOI: 10.1109/AICCSA47632.2019.9035260.
15. Alaparthy V., Morgera S. A multi-level intrusion detection system for wireless sensor networks based on immune theory. *IEEE Access*. 2018;6:47364–47373. DOI: 10.1109/ACCESS.2018.2866962.
16. Xiao X., Zhang R. A danger theory inspired protection approach for hierarchical wireless sensor networks. *KSII Transactions on Internet and Information Systems*. 2019;5(13):2732-2753.
17. Aldhaheri S., Alghazzawi D., Cheng L., Alzahrani B., Al-Barakat A., DeepDCA: novel network-based detection of IoT attacks using artificial immune system. *Applied Sciences*. 2020;10:1909–1932.

18. Powers S.T., He J. A hybrid artificial immune system and Self Organising Map for network intrusion detection. *Information Sciences.* 2008;178(15):3024–3042. DOI: 10.1016/j.ins.2007.11.028.
19. Nguyen V.T., Dung L.H., Le T.D. A combination of artificial immune system and deep learning for virus detection. *International Journal of Applied Engineering Research*. 2018;13(22):15622–15628.
20. Mahboubian M., Hamid N.A.W.A. A machine learning based AIS IDS. *International Journal of Machine Learning and Computing*. 2013;3(3):259–262.
21. Vaitsekhovich L. Intrusion detection in TCP/IP networks using immune systems paradigm and neural network detectors. *XI International PhD Workshop OWD.* 2009:219–224. Available from: https://www.researchgate.net/publication/306194779_Intrusion_detection_in_TCPIP_networks_using_immune_systems_paradigm_and_neural_network_detectors (accessed on 25.08.2021).
22. Komar M., Golovko V., Sachenko A., Bezobrazov S. Development of neural network immune detectors for computer attacks recognition and classification. *2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS).* 2013:665-668. DOI: 10.1109/IDAACS.2013.6663008.
23. Golovko V., Komar M., Sachenko A., Principles of neural network artificial immune system design to detect attacks on computers. *International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*. 2010:237–237. Available from: https://ieeexplore.ieee.org/document/5446089 (accessed on 12.08.2021).
24. Sukhov V.E. Network traffic anomaly detection system based on artificial immune systems and neural networks approach. *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta = Vestnik of Ryazan State Radio Engineering University*. 2015;54-1:84–90. (In Russ.).
25. Khang M.T., Nguyen V.T., Le T.D. A combination of artificial neural network and artificial immune system for virus detection. *Journal on Electronics and Communications*. 2015;(5)3-4:52–57. DOI: 10.21553/rev-jec.133.
26. Estlund D.M. Opinion leaders, independence, and Condorcet's Jury Theorem. *Theory and Decision.* 1994;36:131–162. DOI: 10.1007/BF01079210.
27. Combining multiple learners, Lecture Notes for E Alpaydın 2004 Introduction to Machine Learning, *The MIT Press (V1.1).* Available from: http://people.sabanciuniv.edu/berrin/cs512/lectures/9-i2ml-chap15-classifier-combination-short.pdf (accessed on 24.09.2021).
28. Le T.-T.-H., Park T., Cho D., Kim H. An effective classification for DoS attacks in wireless sensor networks. *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN).* 2018:689–692. DOI: 10.1109/ICUFN.2018.8436999.
29. Alsulaimanand L., Al-Ahmadi S. Performance evaluation of machine learning techniques for DoS detection in wireless sensor network. *International Journal of Network Security & Its Applications (IJNSA).* 2021;13(2):21–29.
30. NSL-KDD. *University of New Brunswick.* Available from: https://www.unb.ca/cic/datasets/nsl.html (accessed on 25.09.2022).
31. Vasilyev V.I., Shamsutdinov R.R. Intelligent network intrusion detection system based on artificial immune system mechanisms. *Modeling, Optimization and Information Technology*. 2019;7(1). Available from: https://moit.vivt.ru/wp-content/uploads/2019/01/VasilyevShamsutdinov_1_19_1.pdf DOI: 10.26102/2310-6018/2019.24.1.010 (In Russ) (accessed on 23.09.2021).

32. Han H., Wang W.Y., Mao B.H. Borderline-SMOTE: a new over-sampling method in imbalanced data sets learning. *International conference on intelligent computing, Springer, Berlin, Heidelberg*. 2005:878-887.

СПИСОК ИСТОЧНИКОВ

1. Threat Intelligence Report 2020. *NOKIA*. Доступно по: https://pages.nokia.com/T005JU-Threat-Intelligence-Report-2020.html?_ga=2.216248470.16 53315497.1608038999-829562352.1608038999 (дата обращения: 23.09.2021).
2. Что угрожает промышленному интернету вещей и как от этого защититься. *Kaspersky Lab, Vc.ru*. *Kaspersky Lab, Vc.ru*. Доступно по: https://vc.ru/kaspersky/265770-chto-ugrozhaet-promyshlennomu-internetu-veshchey-i-kak-ot-etogo-zashchititsya (дата обращения: 23.09.2021).
3. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак. *Труды СПИИРАН*. 2016;2(45):207–244. DOI: 10.15622/sp.45.13.
4. Dobkach L. An analysis of methods for identifying computer attacks. *Legal Informatics*. 2020;1:67–75.
5. ICT219 Lecture 11 – Hybrid Intelligent Systems. *StuDocu*. Доступно по: https://www.studocu.com/en-au/document/murdoch-university/intelligent-systems/ict219-lecture-11-hybrid-intelligent-systems/1280311 (дата обращения: 23.09.2021).
6. Аверкин А.А., Ярушев С.А., Павлов В.У. Когнитивные гибридные системы поддержки принятия решений и прогнозирования. *Программные продукты и системы*. 2017;4(30):632–642. DOI: 10.15827/0236-235X.120.632-642.
7. Lin L. An intelligent fault diagnosis model of WSN based on artificial immune system. *2020 5th International Conference on Smart Grid and Electrical Automation (ICSGEA)*. 2020:405–408. DOI: 10.1109/ICSGEA51094.2020.00093.
8. Dounias G. Hybrid computational intelligence in medicine. Доступно по: http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=EE461823CC470C45FC8909C60AC93956?doi=10.1.1.71.6170&rep=rep1&type=pdf (дата обращения: 25.07.2021).
9. Panda M., Abraham A., Patra M.R. Hybrid intelligent systems for detecting network intrusions. *Security and Communication Networks*. 2012;8(16). Доступно по: https://www.researchgate.net/publication/260408971_Hybrid_intelligent_systems_for_detecting_network_intrusions. DOI: 10.1002/sec.592 (дата обращения: 15.08.2021).
10. Salama M.A., Ramadan R., Darwish A., Eid H.F. Hybrid intelligent intrusion detection scheme. *Advances in Intelligent and Soft Computing*. 2011;96:295–302. DOI: 10.1007/978-3-642-20505-7_26.
11. Khan M.A., Kim Y. Deep learning-based hybrid intelligent intrusion detection system. *Computers, Materials & Continua*. 2021;1(68):671–687. DOI: 10.32604/cmc.2021.015647.
12. Panda M., Abraham A., Patrac M.R. A hybrid intelligent approach for network intrusion detection. *Procedia Engineering*. 2012;30:1–9. DOI: 10.1016/j.proeng.2012.01.827.
13. Chavez A., Lai C., Jacobs N., Hossain-McKenzie S., Jones C.B., Johnson J., Summers A. Hybrid intrusion detection system design for distributed energy resource systems. *IEEE CyberPELS;* 2019. Доступно по: https://ieeexplore.ieee.org/document/8925064 (дата обращения: 28.07.2021).
14. Alem S., Espes D., Martin E., Nana L., De Lamotte F. A Hybrid Intrusion Detection System in Industry 4.0 Based on ISA95 Standard. *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA),* 2019:1–8, DOI: 10.1109/AICCSA47632.2019.9035260.

15. Alaparthy V., Morgera S. A multi-level intrusion detection system for wireless sensor networks based on immune theory. *IEEE Access.* 2018;6:47364–47373. DOI: 10.1109/ACCESS.2018.2866962.
16. Xiao X., Zhang R. A danger theory inspired protection approach for hierarchical wireless sensor networks. *KSII Transactions on Internet and Information Systems.* 2019;5(13):2732-2753.
17. Aldhaheri S., Alghazzawi D., Cheng L., Alzahrani B., Al-Barakat A., DeepDCA: novel network-based detection of IoT attacks using artificial immune system. *Applied Sciences.* 2020;10:1909–1932.
18. Powers S.T., He J. A hybrid artificial immune system and Self Organising Map for network intrusion detection. *Information Sciences.* 2008;178(15):3024–3042. DOI: 10.1016/j.ins.2007.11.028.
19. Nguyen V.T., Dung L.H., Le T.D. A combination of artificial immune system and deep learning for virus detection. *International Journal of Applied Engineering Research*. 2018;13(22):15622–15628.
20. Mahboubian M., Hamid N.A.W.A. A machine learning based AIS IDS. *International Journal of Machine Learning and Computing.* 2013;3(3):259–262.
21. Vaitsekhovich L. Intrusion detection in TCP/IP networks using immune systems paradigm and neural network detectors. *XI International PhD Workshop OWD.* 2009:219–224. Доступно по: https://www.researchgate.net/publication/306194779_Intrusion_detection_in_TCPIP_networks_using_immune_systems_paradigm_and_neural_network_detectors (дата обращения: 25.08.2021).
22. Komar M., Golovko V., Sachenko A., Bezobrazov S. Development of neural network immune detectors for computer attacks recognition and classification. *2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS).* 2013:665-668. DOI: 10.1109/IDAACS.2013.6663008.
23. Golovko V., Komar M., Sachenko A., Principles of neural network artificial immune system design to detect attacks on computers. *International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*. 2010:237–237. Доступно по: https://ieeexplore.ieee.org/document/5446089 (дата обращения: 12.08.2021).
24. Сухов В.Е. Система обнаружения аномалий сетевого трафика на основе искусственных иммунных систем и нейросетевых детекторов. *Вестник Рязанского государственного радиотехнического университета*. 2015;54-1:84–90.
25. Khang M.T., Nguyen V.T., Le T.D. A combination of artificial neural network and artificial immune system for virus detection. *Journal on Electronics and Communications.* 2015;(5)3-4:52–57. DOI: 10.21553/rev-jec.133.
26. Estlund D.M. Opinion leaders, independence, and Condorcet's Jury Theorem. *Theory and Decision.* 1994;36:131–162. DOI: 10.1007/BF01079210.
27. Combining multiple learners, Lecture Notes for E Alpaydın 2004 Introduction to Machine Learning, *The MIT Press (V1.1).* Доступно по: http://people.sabanciuniv.edu/berrin/cs512/lectures/9-i2ml-chap15-classifier-combination-short.pdf (дата обращения: 24.09.2021).
28. Le T.-T.-H., Park T., Cho D., Kim H. An effective classification for DoS attacks in wireless sensor networks. *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN).* 2018:689–692. DOI: 10.1109/ICUFN.2018.8436999.
29. Alsulaimanand L., Al-Ahmadi S. Performance evaluation of machine learning techniques for DoS detection in wireless sensor network. *International Journal of Network Security & Its Applications (IJNSA).* 2021;13(2):21–29.

30. NSL-KDD. *University of New Brunswick.* Доступно по: https://www.unb.ca/cic/datasets/nsl.html (дата обращения: 25.09.2022).
31. Васильев В.И. Шамсутдинов Р.Р. Интеллектуальная система обнаружения сетевых атак на основе механизмов искусственной имунной системы. Моделирование, оптимизация и информационные технологии. 2019;7(1). Доступно по: https://moit.vivt.ru/wp-content/uploads/2019/01/VasilyevShamsutdinov_1_19_1.pdf. DOI: 10.26102/2310-6018/2019.24.1.010 (дата обращения: 23.09.2021).
32. Han H., Wang W.Y., Mao B.H. Borderline-SMOTE: a new over-sampling method in imbalanced data sets learning. *International conference on intelligent computing, Springer, Berlin, Heidelberg*. 2005:878-887.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Васильев Владимир Иванович, доктор технических наук, профессор Уфимского университета науки и технологий, Уфа, Российская Федерация.
e-mail: vas0015@yandex.ru

Vladimir Ivanovich Vasilyev, Doctor of Technical Science, Professor at Ufa University of Science and Technology, Ufa, Russian Federation.

Вульфин Алексей Михайлович, кандидат технических наук, доцент Уфимского университета науки и технологий, Уфа, Российская Федерация.
e-mail: vulfin.alexey@gmail.com
ORCID: 0000-0001-5857-2413

Alexey Mikhailovich Vulfin, Doctor of Technical Sciences, Associate Professor at Ufa University of Science and Technology, Ufa, Russian Federation.

Гвоздев Владимир Ефимович, доктор технических наук, профессор Уфимского университета науки и технологий, Уфа, Российская Федерация.
e-mail: wega55@mail.ru

Vladimir Efimovich Gvozdev, Doctor of Technical Sciences, Professor at Ufa University of Science and Technology, Ufa, Russian Federation.

Шамсутдинов Ринат Рустемович, аспирант Уфимского университета науки и технологий, Уфа, Российская Федерация.
e-mail: shrr2019@yandex.ru
ORCID: 0000-0002-4178-5284

Rinat Rustemovich Shamsutdinov, Postgraduate Student, Ufa University of Science and Technology, Ufa, Russian Federation.

Статья поступила в редакцию 07.11.2022; одобрена после рецензирования 13.12.2022; принята к публикации 28.12.2022.

The article was submitted 07.11.2022; approved after reviewing 13.12.2022; accepted for publication 28.12.2022.