УДК 004.056 DOI: 10.26102/2310-6018/2021.34.3.019

Гибридная интеллектуальная система обнаружения атак на основе комбинации методов машинного обучения

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

Уфимский государственный авиационный технический университет,
Уфа, Российская Федерация

Резюме. Статья посвящена проблеме обнаружения сетевых атак в системах промышленного Интернета вещей. Анализируется актуальность рассматриваемой проблемы, обусловленная высоким уровнем рисков безопасности в подобных системах. Рассмотрены различные алгоритмы обнаружения сетевых атак, отмечен возрастающий интерес к применению методов искусственного интеллекта для решения данного рода задач. Подчеркиваются преимущества комплексирования для этих целей различных алгоритмов искусственного интеллекта и методов машинного обучения в составе гибридных систем обнаружения атак. Предложен подход к построению гибридной интеллектуальной системы обнаружения атак (СОА), включающей в себя на нижнем уровне искусственную иммунную систему, отвечающую за выявление аномалий и неизвестных сетевых атак, выполняющей таким образом функцию предварительной фильтрации сетевого трафика, а также многоклассовый классификатор на верхнем уровне, определяющий класс атаки, обнаруженной на нижнем уровне системы. В качестве способов построения классификатора верхнего уровня рассматриваются нейронная сеть и случайный лес. Для обучения и оценки эффективности предложенной системы использован набор данных о сетевых соединениях NSL-KDD. Как показали эксперименты, наилучшие результаты достигаются путем объединения в составе гибридной СОА алгоритмов искусственной иммунной системы со случайным лесом.

Ключевые слова: информационная безопасность, сетевая атака, машинное обучение, искусственная иммунная система, нейронная сеть, случайный лес, гибридная интеллектуальная система.

Для цитирования: Васильев В.И., Вульфин А.М., Гвоздев В.Е., Шамсутдинов Р.Р. Гибридная интеллектуальная система обнаружения атак на основе комбинации методов машинного обучения. *Моделирование, оптимизация и информационные технологии.* 2021;9(3). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1032 DOI: 10.26102/2310-6018/2021.34.3.019

Hybrid intelligent intrusion detection system based on combining machine learning methods

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

Ufa State Aviation Technical University,
Ufa, Russian Federation

Abstract: The article is devoted to the problem of detecting network attacks in Industrial Internet of Things systems. The topicality of the problem under consideration due to a high level of security risks in such systems is analyzed. Various algorithms of network attack detection are considered, and an increasing interest to applying methods of artificial intelligence for solving this kind of problems is noted. The advantages of combining various algorithms of artificial intelligence and methods of machine learning as a part of hybrid intrusion detection systems are underlined. The approach to design of hybrid intelligent intrusion detection system (IDS) is proposed, which includes at the lower level the artificial immune system, responsible for detection of anomalies and unknown network attacks, fulfilling so a function of preliminary network traffic filtration, and the multiclass classificator at the upper level, determining the class of the attack detected at the lower level of the system. The neural network and the

random forest algorithm are considered as methods of constructing the classifier of the upper level. The training and efficiency estimation of the system proposed were carried out with use of the NSL-KDD dataset. As experiments showed, the best results were achieved by combination in hybrid IDS of the algorithms of artificial immune system and random forest.

Keywords: information security, network attack, machine learning, artificial immune system, neural network, random forest, hybrid intelligent system.

For citation: Vasilyev V.I., Vulfin A.M., Gvozdev V.E., Shamsutdinov R.R. Hybrid intelligent intrusion detection system based on combining machine learning methods. *Modeling, Optimization and Information Technology*. 2021;9(3). Available from: https://moitvivt.ru/ru/journal/pdf?id=1032 DOI: 10.26102/2310-6018/2021.34.3.019 (In Russ).

Введение

Широкое применение промышленных систем Интернета вещей (Industrial Internet of Things, IIoT) сопровождается увеличением рисков нарушения их безопасности. Согласно отчета Nokia Threat Intelligence Lab 2020 года [1], 32,72% всех случаев заражения в мобильных сетях приходится на IIoT-устройства. В 2019 году этот показатель составлял 16,17%. По данным [2] Лаборатории Касперского, отмечается значительный рост новых образцов вредоносного программного обеспечения (ПО) для IIoT в 2015-2020 гг., как это представлено на Рисунке 1.

Рисунок 1 – Количество новых образцов вредоносного ПО для IIoT
Figure 1 – The Number of New IIoT Malware Samples

55% респондентов, опрошенных Лабораторией Касперского [3], выделили использование IIoT в качестве одного из главных факторов, влияющих на кибербезопасность АСУ ТП, но только 14% компаний внедрили инструменты детектирования сетевых аномалий и 19% – средства мониторинга сети и трафика.

Многообразие подходов к обнаружению сетевых атак на эти системы, включая поведенческие методы, методы на основе знаний, машинного обучения, вычислительного интеллекта и др. подробно описано в [4, 5]. Одно из перспективных направлений – разработка систем обнаружения атак (СОА) в классе гибридных интеллектуальных систем (ГИС), объединяющих в своем составе две или более технологии искусственного интеллекта (ИИ) с целью получения синергетического эффекта, нивелирования недостатков одной технологии преимуществами другой. К

примеру, системы нечеткой логики понятны и прозрачны для пользователя, но у них отсутствует способность к обучению. Искусственные нейронные сети (ИНС), наоборот, способны к обучению, но непрозрачны для пользователя. Их совместное использование в составе нечеткой нейронной сети позволяет получить адаптивную систему, способную к обучению и одновременно прозрачную для пользователя [6].

Как показано в [7], гибридное использование нечетких когнитивных карт и нейро-нечеткой сети ANFIS позволяет повысить точность прогнозирования многомерных временных рядов. В [8] рассмотрены другие комбинации методов ИИ, таких как ИНС и эволюционные алгоритмы, нечеткая логика и эволюционные алгоритмы, машинное обучение и нечеткая логика, машинное обучение и эволюционные алгоритмы и др.

Общая идея построения СОА в классе гибридных интеллектуальных систем обсуждается в ряде работ [9-14]. Как правило, в основе построения таких систем используется объединение ИНС, алгоритмов кластерного анализа, деревьев решений, машины опорных векторов (SVM) и других различных по своей идеологии методов ИИ. Отдельную перспективную группу СОА занимают СОА на базе искусственных иммунных систем (ИИС) в дополнении с другими технологиями ИИ.

Гибридные интеллектуальные СОА на основе ИИС

В [15] предложен конструктивный алгоритм обнаружения вирусов, основанный на объединении ИИС и глубокой сети доверия (Deep Belief Network, DBN):

– формирование векторов признаков;

– формирование 2-х датасетов: R_1 – «Норма» (Benign) и R_2 – «Вирус» (Virus);

– формирование случайным образом набора детекторов (той же длины, что и векторы в R_1 и R_2);

– отрицательный отбор и клональная селекция: удаление из набора детекторов R' векторов, имеющих максимальный показатель аффинности (сходства) по отношению к векторам из R_1, то есть построение набора R_2', состоящего из векторов "скорее всего, вирус";

– выделение из множества R_2' векторов, имеющих максимальную аффинность по отношению к векторам из R_2; полученное множество R_2'' используется в качестве обучающего множества для глубокой сети доверия;

– с помощью DBN в качестве классификатора решается задача распознавания конкретного вируса, то есть для каждого входного вектора признаков принимается решение: «Норма» или «Вирус».

Совместное использование ИИС и самоорганизующейся карты Кохонена в [16] позволило повысить эффективность обнаружения атак Denial-of-Service и User-to-Root при низком уровне ошибок первого рода. В данном случае работа СОА происходит в 2 этапа:

1) фильтрация признаков сетевых соединений с помощью иммунных детекторов, обученных по методу отрицательного отбора; тем самым отсеиваются те образцы, которые соответствуют нормальным соединениям;

2) аномальные экземпляры обрабатываются самоорганизующимися картами Кохонена и группируются в отдельные кластеры со схожими признаками.

В [17] рассматривается объединение теории отрицательного отбора (характерной для ИИС) с построением продукционных правил обработки знаний. Приводятся результаты экспериментов на наборе данных DARPA KDD-99. Предложенный подход позволяет обнаруживать различные типы атак, продукционные правила генерируются при этом с помощью пакета WEKA в виде деревьев решений).

В [18-20] в качестве иммунных детекторов выбраны многослойные ИНС, которые генерируются при помощи метода клональной селекции. В [21] в роли детекторов используются ИНС Кохонена, реагирующие на изменение статистики сетевого трафика. Блок формирования иммунной памяти реализует операции клонирования и мутации детекторов, мутация заключается в случайном изменении весов ИНС-детектора на малую величину, механизм клонирования детекторов заключается в создании 5 копий детектора, обнаружившего аномалию.

В [22] предлагается искусственная нейронная иммунная сеть (Artificial Neural Immune Network, ANIN), которая является комбинацией искусственной нейронной сети и искусственной иммунной сети (Artificial Immune Network, AiNet). В ANIN каждая ИНС представляет собой детектор и множество таких детекторов используется таким образом, что они могут кооперироваться для решения задачи. AiNet используется для обучения детекторов на основе ИНС как в плане корректировки весов, так и их структуры. Результаты экспериментов показывают, что точность обнаружения сетевых атак достигает 87,98% при низком уровне ложной тревоги.

Предлагаемый подход к построению гибридной интеллектуальной СОА

В основе предлагаемого подхода используется следующая процедура построения гибридной СОА:

1) получение исходных данных о сетевом трафике и их предобработка (формирование вектора признаков, сокращение его размерности);
2) разметка полученной обучающей выборки (датасета), разделение этой выборки на собственно обучающую и тестовую выборку;
3) генерация набора детекторов (шаблонов) для обучения ИИС;
4) алгоритм отрицательного отбора (удаление шаблонов, совпадающих с векторами из класса «Норма»);
5) фильтрация оставшихся детекторов путем сравнения с векторами, принадлежащих классам «Атака», выделение претендентов по критерию максимальной аффинности;
6) обучение классификатора на выделенной части датасета (распознавание нескольких классов «Атака»);
7) оценка качества распознавания атак (эффективности СОА).

В качестве датасета был выбран NSL-KDD [23]. Размерность пространства признаков при этом была уменьшена с 41 до 16 описанным в [24] способом. Далее количественные признаки были масштабированы путем приведения их к нулевому среднему значению и единичному отклонению, категориальные признаки были перекодированы к равномерной числовой шкале. Для оценки эффективности системы использовались следующие показатели:

– *True Positives* (*TP*) – количество верно выявленных аномалий;

– *True Negatives* (*TN*) – количество верно определенных образов нормальной активности;

– *False Positives* (*FP*) – количество образов нормальной активности, определенных как аномалии (ошибки первого рода);

– *False Negatives* (*FN*) – количество образов аномальной активности, определенных как норма (ошибки второго рода);

– *Precision* – доля верно выявленных аномалий среди всех образов, определенных как аномалии:

–

$$Precision = \frac{TP}{TP+FP}; \quad (1)$$

– *Recall* – доля верно выявленных аномалий среди всех аномалий:

$$Recall = \frac{TP}{TP+FN}; \quad (2)$$

– *Accuracy* – доля верно классифицированных образов среди всех образов:

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN}; \quad (3)$$

– F_1 *score* – среднее гармоническое точности (Precision) и полноты (Recall):

$$F_1 score = \frac{2 \times Precision \times Recall}{Precision+Recall}. \quad (4)$$

ИИС была обучена на основе данных о нормальной активности, затем протестирована на соответствующем наборе данных. Аномалии, выявленные ИИС, передавались двум различным по своей структуре классификаторам: ИНС и случайный лес (Random Forest). Не все виды атак в NSL-KDD представлены в достаточном для обучения количестве. ИНС и случайный лес (СЛ) были обучены распознаванию атак, для которых представлено по меньшей мере 500 образцов. Это такие атаки, как: neptune, satan, ipsweep, portsweep, smurf, nmap, back, teardrop, warezclient. Остальные атаки, выявленные ГИС, но не подходящие ни к одному из вышеуказанных видов атак, классифицируются как неизвестные, что позволяет гибридной системе потенциально выявлять не только атаки, не имеющие достаточно обучающих примеров в датасете, но и ранее неизвестные атаки. Результаты вычислительных экспериментов ИИС представлены в Таблице 1.

Таблица 1 – Показатели эффективности ИИС
Table 1 –Artificial Immune System efficiency

Показатели	$Precision$	$Recall$	$Accuracy$	$F_1 score$
Значения	0,997	0,993	0,995	0,995

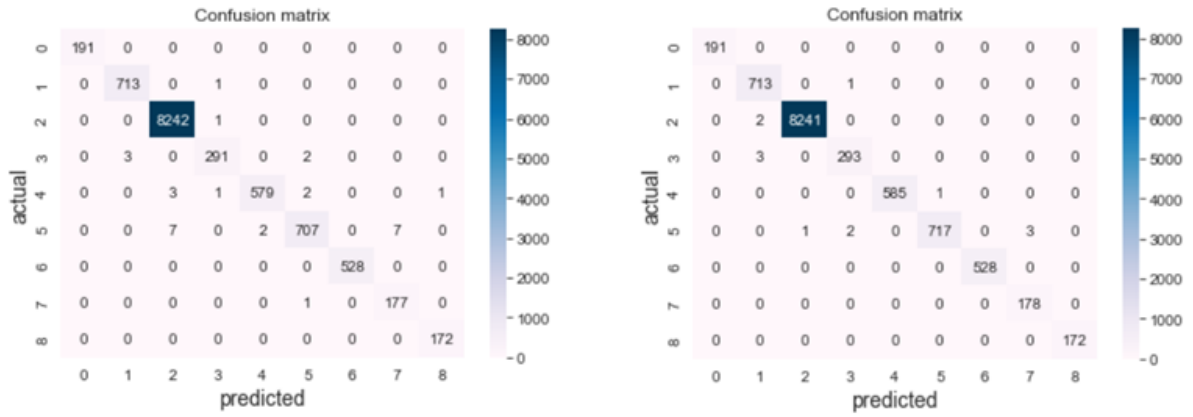
Как видно из Таблицы 1, ИИС обладает высокой точностью распознавания аномалий. Благодаря алгоритму отрицательного отбора, обеспечивается низкий уровень ошибок первого рода (False Positives) – менее 1%, а благодаря алгоритму клональной селекции – высокая адаптивность: система самостоятельно обучилась выявлению неизвестных для нее атак с точностью 99,5%.

Использованная в экспериментах в качестве классификатора ИНС представляет собой сеть прямого распространения, скрытый слой содержит 16 нейронов с сигмоидальной функцией активации, количество нейронов в выходном слое – 9 (по количеству распознаваемых классов, с функцией активации softmax). Коэффициент исключения (dropout) для регуляризации сети подобран экспериментально и равен 0,1. Множество используемых данных (датасет) из NSL-KDD было разделено на обучающую, тестовую и контрольную выборки в соотношении 80 – 15 – 5. Контрольная выборка использовалась для предотвращения переобучения ИНС с реализацией раннего останова.

Параметры классификатора на основе случайного леса подбирались с помощью процедуры поиска по сетке с перекрестной проверкой с тремя заходами – перебирались

конкретные значения: количество деревьев, количество признаков, максимальная глубина и минимальное количество примеров в листовом узле.

Матрицы ошибок ИНС и СЛ для тестовой выборки по каждому из 9-ти видов атак представлены на Рисунке 2.



а) искусственная нейронная сеть *б) случайный лес*

Рисунок 2 – Матрицы ошибок ИНС и СЛ
Figure 2 – Confusion Matrices of ANN and Random Forest

Значения показателей $Accuracy$ и F_1score для классификаторов на основе ИНС и СЛ приведены в Таблице 2.

Таблица 2 – Показатели эффективности ИНС и СЛ
Table 2 – Detection Efficiency of ANN and Random Forest

Классификатор	$Accuracy$	F_1score
ИНС	0,997	0,997
СЛ	0,999	0,999

Таким образом, предложенная гибридная интеллектуальная СОА обеспечивает высокий уровень эффективности обнаружения и распознавания сетевых атак. Как следует из Таблицы 2, использование СЛ в комбинации с ИИС является при этом более предпочтительным по сравнению с ИНС, поскольку значения показателей $Accuracy$ и F_1score для СЛ лучше, чем для ИНС.

Заключение

Широкое распространение промышленных систем Интернета вещей сопровождается возрастанием рисков нарушения их безопасности. Одним из перспективных направлений в области снижения рисков является разработка и внедрение систем обнаружения атак (СОА) в классе гибридных интеллектуальных систем, объединяющих в своем составе две или более взаимодополняющих технологии искусственного интеллекта.

Предложенная в статье СОА является двухуровневой, на нижнем уровне которой искусственная иммунная система (ИИС) анализирует показатели сетевого трафика, выделяет аномалии и передает сведения о них классификатору на верхнем уровне. В качестве классификаторов верхнего уровня рассмотрены искусственная нейронная сеть (ИНС) и случайный лес (СЛ), выполняющие функцию классификации аномалий,

обнаруженных с помощью ИИС, а при отсутствии такой возможности отнесения их к классу неизвестных. Проведенные вычислительные эксперименты подтвердили высокий уровень эффективности гибридной СОА. Сравнение двух вариантов построения СОА показало более высокую эффективность объединения ИИС с СЛ, обеспечивающего адаптивность системы, высокую точность классификации известных угроз, способность обнаруживать неизвестные атаки.

В качестве перспектив дальнейших исследований следует отметить возможность применения совместно с ИИС комитета классификаторов (ансамблей методов машинного обучения).

Благодарности

Работа выполнена при поддержке гранта РФФИ №20-37-90024

Acknowledgments

This work was supported by the RFBR grant No. 20-37-90024

ЛИТЕРАТУРА

1. Threat Intelligence Report 2020. *NOKIA*. Доступно по: https://pages.nokia.com/T005JU-Threat-Intelligence-Report-2020.html?_ga=2.216248470.1653315497.1608038999-829562352.1608038999. (дата обращения: 30.07.2021).
2. Лаборатория Касперского. Что угрожает промышленному интернету вещей и как от этого защититься. *Vc.ru*. Доступно по: https://vc.ru/kaspersky/265770-chto-ugrozhaet-promyshlennomu-internetu-veshchey-i-kak-ot-etogo-zashchititsya. (дата обращения: 30.07.2021)
3. Лаборатория Касперского: распространение умных устройств в промышленности повлечёт за собой смену подхода к киберзащите. *Лаборатория Касперского*. Доступно по: https://www.kaspersky.ru/about/press-releases/2020_laboratoriya-kasperskogo-rasprostranenie-umnih-ustroistv-v-promishlennosti-povlechyot-za-soboi-smenu-podhoda-k-kiberzaschite. (дата обращения: 30.07.2021).
4. 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.
5. Добкач Л.Я. Анализ методов распознавания компьютерных атак. *Правовая информатика*. 2020;1:67-75. DOI: 10.21681/1994-1404-2020-1-67-75.
6. 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: 30.07.2021).
7. Аверкин А.А., Ярушев С.А., Павлов В.Ю. 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.
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: 30.07.2021).
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 (дата обращения: 30.07.2021).

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 DOI: 10.1109/CyberPELS.2019.8925064 (дата обращения: 30.07.2021).
14. Alem S., Espes D., Martin E., Nana L., 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. Доступно по: https://hal.archives-ouvertes.fr/hal-02506109v2/document. DOI: 10.1109/AICCSA47632.2019.9035260. (дата обращения: 30.07.2021).
15. 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.
16. Powers S.T., He J. A hybrid artificial immune system and Self Organising Map for network intrusion detection. *Information Sciences*. 2008;15(178):3024-3042. DOI: 10.1016/j.ins.2007.11.028.
17. 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. DOI: 10.7763/IJMLC.2013.V3.315.
18. 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: 30.07.2021).
19. 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.
20. 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. Доступно по: https://ieeexplore.ieee.org/document/5446089. (дата обращения: 30.07.2021).
21. Сухов В.Е. Система обнаружения аномалий сетевого трафика на основе искусственных иммунных систем и нейросетевых детекторов, *Вестник РГРТУ*. 2015;54:84-90.
22. 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;3-4:52-57.
23. NSL-KDD // University of New Brunswick. Доступно по: https://www.unb.ca/cic/datasets/nsl.html. (дата обращения: 25.12.2020).

24. Васильев В.И., Шамсутдинов Р.Р. Интеллектуальная система обнаружения сетевых атак на основе механизмов искусственной иммунной системы. *Моделирование, оптимизация и информационные технологии*. 2019;1(7):521-535. Доступно по: https://moitvivt.ru/ru/journal/pdf?id=592. doi: 10.26102/2310-6018/2019.24.1.010.

REFERENCES

1. Threat Intelligence Report 2020. *NOKIA*. Available at: https://pages.nokia.com/T005JU-Threat-Intelligence-Report-2020.html?_ga=2.216248470.1653315497.1608038999-829562352.1608038999. (accessed 30.07.2021).
2. Laboratoriya Kasperskogo. Chto ugrozhaet promyshlennomu internetu veshchei i kak ot ehtogo zashchitit'sya. *Vc.ru*. Available at: https://vc.ru/kaspersky/265770-chto-ugrozhaet-promyshlennomu-internetu-veshchey-i-kak-ot-etogo-zashchititsya. (In Russ) (accessed 30.07.2021).
3. Laboratoriya Kasperskogo: rasprostranenie umnykh ustroistv v promyshlennosti povlechet za soboi smenu podkhoda k kiberzashchite. *Kaspersky*. Available at: https://www.kaspersky.ru/about/press-releases/2020_laboratoriya-kasperskogo-rasprostranenie-umnih-ustroistv-v-promishlennosti-povlechyot-za-soboi-smenu-podhoda-k-kiberzaschite. (accessed 30.07.2021).
4. Branitskiy A.A., Kotenko I.V. Analysis and Classification of Methods for Network Attack Detection. *SPIIRAS Proceedings*. 2016;2(45):207-244. (In Russ) DOI: 10.15622/sp.45.13.
5. Dobkach L. An Analysis of methods for identifying computer attacks. *Legal Informatics*. 2020;1:67-75. (In Russ) DOI: 10.21681/1994-1404-2020-1-67-75.
6. 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. (accessed 30.07.2021).
7. Averkin A.N. Yarushev S.A. Pavlov V.Yu. Cognitive hybrid systems for decision support and forecasting. *Software & Systems*. 2017;4(30):632-642. (In Russ) DOI:10.15827/0236-235X.120.632-642.
8. Dounias G. Hybrid Computational Intelligence in Medicine. Available at: http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=EE461823CC470C45FC8909C60AC93956?doi=10.1.1.71.6170&rep=rep1&type=pdf. (accessed 30.07.2021).
9. Panda M., Abraham A., Patra M.R., Hybrid intelligent systems for detecting network intrusions. *Security and Communication Networks*. 2012;8(16). Available at: https://www.researchgate.net/publication/260408971_Hybrid_intelligent_systems_for_detecting_network_intrusions. DOI: 10.1002/sec (accessed 30.07.2021).
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 at: https://ieeexplore.ieee.org/document/8925064 DOI: 10.1109/CyberPELS.2019.8925064 (accessed 30.07.2021).
14. Alem S., Espes D., Martin E., Nana L., 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. Available at: https://hal.archives-ouvertes.fr/hal-02506109v2/document. DOI: 10.1109/AICCSA47632.2019.9035260. (accessed 30.07.2021).
15. 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.
16. Powers S.T., He J. A hybrid artificial immune system and Self Organising Map for network intrusion detection. *Information Sciences*. 2008;15(178):3024-3042. DOI: 10.1016/j.ins.2007.11.028.
17. 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. DOI: 10.7763/IJMLC.2013.V3.315.
18. 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 at: https://www.researchgate.net/publication/306194779_Intrusion_detection_in_TCPIP_networks_using_immune_systems_paradigm_and_neural_network_detectors. (accessed 30.07.2021) .
19. 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.
20. 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. Available at: https://ieeexplore.ieee.org/document/5446089. (accessed 30.07.2021).
21. Sukhov V.E. Sistema obnaruzheniya anomalii setevogo trafika na osnove iskusstvennykh immunnykh sistem i neirosetevykh detektorov, *Vestnik of Ryazan State Radio Engineering University*. 2015;54:84-90. (In Russ).
22. 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;3-4:52-57.
23. NSL-KDD // University of New Brunswick. Available at: https://www.unb.ca/cic/datasets/nsl.html. (accessed 25.12.2020).
24. Vasilyev V.V., Shamsutdinov R.R. Intelligent network intrusion detection system based on artificial immune system mechanisms. *Modeling, Optimization and Information Technology*. 2019;1(7):521-535. Available at: https://moitvivt.ru/ru/journal/pdf?id=592. Doi: 10.26102/2310-6018/2019.24.1.010 (In Russ) (accessed 30.07.2021).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Васильев Владимир Иванович, доктор технических наук, профессор Уфимского государственного авиационного технического университета, Уфа, Российская Федерация
e-mail: *vasilyev@ugatu.ac.ru*

Vladimir Ivanovich Vasilyev, Doctor Of Technical Science, Professor Of Ufa State Aviation Technical University, Ufa, Russian Federation

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

Alexey Mikhailovich Vulfin, Ph.D. Of Technical Science, Associate Professor Of Ufa State Aviation Technical University, Ufa, Russian Federation

Гвоздев Владимир Ефимович, доктор технических наук, профессор Уфимского государственного авиационного технического университета, Уфа, Российская Федерация
e-mail: *wega55@mail.ru*

Vladimir Efimovich Gvozdev, Doctor Of Technical Science, Professor Of Ufa State Aviation Technical University, Ufa, Russian Federation

Шамсутдинов Ринат Рустемович, аспирант Уфимского государственного авиационного технического университета, Уфа, Российская Федерация
e-mail: *shrr2019@yandex.ru*

Rinat Rustemovich Shamsutdinov, Ph.D. Student Of Ufa State Aviation Technical University, Ufa, Russian Federation

Статья поступила в редакцию 10.08.2021; одобрена после рецензирования 14.09.2021; принята к публикации 15.09.2021.

The article was submitted 10.08.2021; approved after reviewing 14.09.2021; accepted for publication 15.09.2021.