CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

DOI 10.20535/2411-1031.2021.9.1.249821
UDC 004.056.53(045)

SERHII SERHEIEV,
ANDRII DAVYDIUK,
ALLA ONYSKOVA

DEVELOPMENT DETECTION CYBERATACS METHODS IN THE CRITICAL INFRASTRUCTURE OBJECTS INFORMATION SYSTEMS OVERVIEW AND PROSPECTS

With the rapid development of information technology and its implementation in our lives, the problem of information protection is becoming increasingly important. During the hybrid war, the large-scale transition of private and public organizations to remote work during the COVID-19 pandemic, the era of digital transformation of the state, this problem urgently requires a constant search for effective solutions. Critical infrastructure, public and private sector information systems suffer significant damage from cyberattacks. The magnitude of these losses directly depends on the timely detection of unauthorized interference in their work. The purpose of this article is to establish the advantages and disadvantages of known methods for their further effective implementation within the construction of information security systems. To achieve this goal, the most common methods of detecting cyberattacks are analyzed, their advantages and disadvantages are identified. In particular, systems based on signature analysis are more stable and have fewer false positives. However, they are ineffective in detecting new cyberattacks. Expert methods based on fuzzy logic are characterized by the subjectivity of the results and time spent in implementation. Based on the analysis, the prospects for the development of methods for detecting cyberattacks using artificial intelligence technologies are identified, in particular, the use of grid networks to increase computing power when working with large amounts of data and implementation of in-depth information analysis algorithms is proposed. The results obtained can be used in the construction of integrated information security systems and/or information security management systems. In addition, they can contribute to the indexing (rating) of objects for assessing the level of cybersecurity, the development of cyber insurance as an alternative approach to information protection and increase Ukraine's potential in the field of cybersecurity and cyber defence. Building active cyber defence systems using artificial intelligence technologies will provide a safer environment for the further development of new technologies and the sustainable existence of society in it. In addition, it can have a positive economic effect by minimizing anticipated losses and centralized implementation of technical means of protection using dynamic allocation of resources.

Keywords: cybersecurity, cyberattack, intrusion detection systems, anomaly detection, artificial intelligence, grid network.

Problem statement. In Ukraine, the processes of digital transformation are rapidly developing [1], radical changes are being made to provide public services to citizens. The private sector is also trying to attract customers through simplified procedures for obtaining goods and services. However, on the other hand, all this carries risks of information security, in particular cyberattacks can cause significant damage to both the state and its citizens [2]. It is important in the implementation of measures to counter the attacks of an attacker is the timely detection of cyberattacks and taking immediate measures to locate and neutralize them. Normative documents in Ukraine define two approaches to information protection, including the creation of integrated information security systems in information and telecommunications systems and the construction of information security management systems [3]. As part of the implementation of both approaches, an integral part is the implementation of organizational and technical means of monitoring and the

ensuring the monitoring of information and telecommunications systems. Thus, one of the priorities of cybersecurity in Ukraine is the creation and implementation of systems for rapid detection, prevention and neutralization of cyber attacks.

Analysis of recent research and publications. The most commonly used methods of detecting cyberattacks include such as the use of anomaly and intrusion detection systems, expert methods based on mathematical models and fuzzy logic methods [4]. It should be noted that unauthorized actions on the resources of the information system have an impact on the environment that surrounds them, thus creating certain anomalies. For such systems, the concept of normal behavior is quite vague, as to predict user behavior is not an easy task. As a result, the disadvantage of this approach is the large number of false positives. However, such systems, in contrast to systems based on signature methods, can detect new attacks on certain grounds. Anomaly detection systems have the ability to generate data that can be used to create intrusion detection system signatures. In [5], [6], [7] the efficiency of application of the mathematical apparatus of fuzzy sets for the decision of such problems is investigated, and possibilities of its use for increase of efficiency of the developed systems of detection of cyberattacks are outlined. In [8], an analysis is carried out and a conclusion is made on expediency of application anomaly identification models that simultaneously operate with qualitative and quantitative data and are based on the mathematical apparatus of fuzzy set theory and fuzzy inference. In particular, an improved model for detecting anomalies in the operation of information and telecommunications systems and networks is presented. The essence of the improvement is to introduce weights for fuzzy rules that describe anomalies that may occur during the operation of information and telecommunications systems and networks as a result of unauthorized cyber interference and after the introduction of which, the problem of fuzzy identification of anomalies in the information and telecommunications system is to find a solution of the analytical expression, which connects the set of parameters of the state of the system on the basis of which its anomalous behavior is determined and the expert decision which corresponds to them taking into account the entered weights for rules. In [9] the method of detecting one of the most common cyberattacks – JS (HTML) / ScrInject based on the application of the mathematical apparatus of fuzzy set theory and fuzzy inference is presented. The development of the methodology is based on an algorithm of actions, which includes the stages of preparation of input data, fassification of the values of the studied parameters and the implementation of the fuzzy inference procedure. In [10], a model for detecting anomalies in information networks of military authorities is proposed, which is based on the theory of fuzzy sets and fuzzy inference. As part of the analysis [11] a generalized study of software intrusion detection systems on a certain basic set of characteristics (“Class of cyberattacks”, “Adaptability”, “Detection methods”, “System management”, “Scalability”, “Level of observation”, “Reaction on cyber attack”, “Security” and “Operating system support”). In [12], methods for identifying signs of system compromise that can lead to cyberattacks are considered. In [13] the main methods of detecting cyber attacks were analyzed, namely signature analysis (method of detecting abuses) and the method of detecting anomalies. Based on the analysis of these methods, it is concluded that to increase the level of security of information resources in information and telecommunications systems, it is advisable to use methods based on the detection of anomalies, because they are characterized by the detection 0-day cyberattacks. The paper reviews the main means of detecting (counteracting) cyber attacks, including Intrusion Detection System / Intrusion Prevention System, Firewall, antivirus programs and Security information and event management technologies. On the basis of the considered means the typical scheme of application of means of protection against cyber attacks was presented and analyzed. In [14] the most dangerous modern cyberattacks, in particular, groups “ransomware”, and the phases of their passage are considered. Enterprise security systems have been found to be unreliable in resisting “ransomware” attacks. One reason is that the detection of passive bots by anti-virus scanning systems is becoming increasingly difficult due to software code variability, bot behavior, and their diversity, while existing cyberattack detection systems are largely based on macro descriptions (signatures, etc.) that present pre-identified known security threats. In [15] is proposed a method of network-centric monitoring of cyber incidents,

which is implemented in 8 stages: classification of cyberattacks, detection of cyberattacks, categorization of cyber incidents, formation of a set of rules for extrapolation of cyber incidents, definition of objects of protection, determining the impact of cyber incidents on the components of information and telecommunications systems, determining the most critical components of information and telecommunications systems, ranking the degree of danger of cyber incidents.

Based on the analysis of the above publications, it can be concluded that systems based on signature analysis are more stable and have fewer false positives, but are completely ineffective in detecting new attacks. Expert methods based on mathematical models and methods of fuzzy logic have a subjective factor and are quite time consuming to implement.

The aim of this paper is the question arises of the optimal use of existing approaches to detecting cyberattacks. The solution to this problem is based on finding a system model in which the number of false positives will be less than the number of detected incidents, and the set of states of normal operation of the system will be greater than the set of states of its incorrect operation.

The main material research. Given the development of information technology and ways of cyberattacks to achieve such a ratio is quite a difficult task that requires a large amount of data, automatic mechanisms for analysis and retrieval, knowledge and experience of the expert.

These tools can be provided using artificial intelligence technologies, as cybersecurity analysts rely on vast amounts of security event data to predict, detect, characterize, and address security threats. These analysts need to understand vast amounts of data to identify patterns that lead to sensible decision-making and warning of potential threats, and this process requires automation. Big data analytics and artificial intelligence can improve cybersecurity. Big data analysis methods are applied to large data sets containing different types of data. The aim is to identify patterns, correlations, trends and other useful information. Artificial intelligence provides algorithms that can reason and learn to improve their behavior, and also includes semantic technologies. Currently, a large number of automated systems are based on syntactic rules, which are usually not complex enough to deal with the level of complexity in this area [16]. Thus, artificial intelligence in combination with the methods of multifactor data analysis can form a synergetic system for analyzing events in the information and telecommunications system that can affect the state of such a system.

Of course, the process of creating such an artificial intelligence system is quite long, but almost the only way to meet new challenges in cybersecurity.

Artificial intelligence systems based on neural networks have the opportunity to learn both independently and with a teacher. Such a combined approach to their development may be the most effective at present. The basis for the construction of such systems should be algorithms for working with big data and in-depth analysis. The paper [17] presents an analysis of recent publications on the construction of neural network models for detecting cyberattacks.

These technologies require significant computing power, which is currently lacking in our state. However, in our opinion, the creation of a grid network (white botnet) is promising [18]. That is, every conscious citizen, having established a client application, can sacrifice part of the capacity of his device, both during downtime and during active use of his device for the general cyber security of the state. Everyone’s interest will be based not only on the importance of solving cybersecurity problems, but also on the security of their own data. Thus, a certain security ecosystem is formed [19], see Fig 1.

Rational for the implementation of such a system is the creation of the state's own free-to-distribute antivirus or modification of existing antivirus products in the country with the consent and support of developers, part of which will be the software module client grid. As a result, it will be possible to obtain a large amount of data for analysis, increase the level of cybersecurity of citizens, and obtain large computing power.

Successful examples of using grid networks to solve extremely complex problems in the field of medicine, economics, production of new materials, nanotechnologies, etc. are already known in the world [20].

On the other hand, there is the issue of protecting this data, preventing compromise of such grid client software. The introduction of such technologies in the international space and the establishment of data exchange will make it possible to define the boundaries of Ukrainian cyberspace. In turn, D.V. Dubov in his own monograph defines cyberspace as a new dimension of geopolitical rivalry [21].

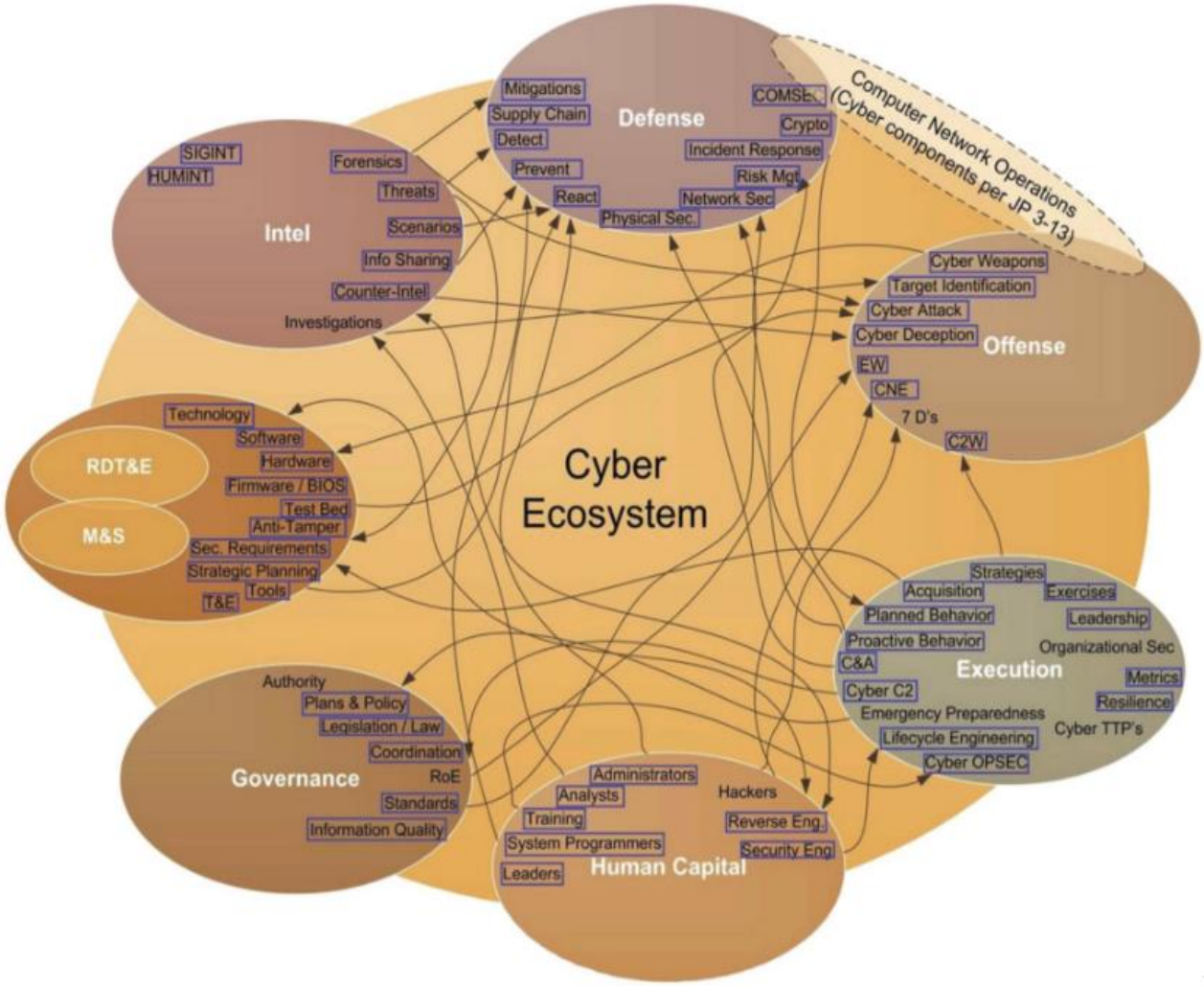

Figure – Cybersecurity ecosystem [19]

Further research in this area should relate to the setting of multi-criteria problems in order to reduce the number of false positives and increase the adequacy of decisions. The development of new interfaces for interaction with such a system will improve data collection and analysis processes.

Some of the advantages of this approach include the ability to predict cyberattacks and support the decisions of a specialist to neutralize the effects of negative influences. Such data can also be used to index (rating) organizations, critical infrastructure objects, information and communication technology service providers to monitor the development of cybersecurity in the country [22].

In addition, it will contribute to the development of threat and attack classification [23], which in turn can significantly affect the evolution of protection, through the development of new modules and more specialized settings.

It is also possible to use such technologies to introduce the cyber insurance market [24] as an alternative approach to information security. In which the organization, having assessed the possible risks of information security can transfer them to the insurance company, reducing its own costs of

information security. The main task of cyber insurance is to protect against attackers. This type of insurance provides a financial mechanism for recovery after large losses, helping companies to return to normal operation, maintain stability, solvency and reduce losses due to production interruptions. Cyber insurance has gained its popularity in developed countries due to the understanding that, implementing the latest solutions in the field of cybersecurity and conducting constant work with staff, there is always the 1% risk of compromising the system, which is impossible to predict and assess. That is why the procedure of cyber insurance is appropriate here, which is characterized by a wide range of coverage and protects companies from financial losses as a result of various attacks. And last but not least – the coverage is a break in production, loss of profits as a result of cyber incidents. In addition, insurance companies offer the following additional conditions: reimbursement of cybercrime investigation costs, anti-crisis PR to restore reputation, the cost of legal protection and the restoration of IT systems.

One of the possible problems in the implementation of such an organizational and technical solution is the need to develop regulations that will regulate the use of artificial intelligence technologies. Although, the beginning of work in this direction is already there [25]. This document defines the purpose, principles and objectives of the development of artificial intelligence technologies in Ukraine as one of the priority areas in the field of scientific and technological research. Additionally, it is noted that the introduction of information technology, part of which is artificial intelligence technology, is an integral part of the development of socio-economic, scientific and technical, defense, legal and other activities in areas of national importance. The lack of conceptual foundations of state policy in the field of artificial intelligence does not allow to create and develop a competitive environment in these areas.

However, it should be understood that artificial intelligence can be used for cyberattacks [26]. At present, such technologies are quite limited due to their cost, but given the trend towards the development of technologies and their cheapening due to widespread use, it is necessary to respond in advance to future threats.

Undoubtedly, no less important is the development of cyberattacks using artificial intelligence in the framework of cyber defense of the state, the construction of active cyber defense systems. Such systems can be used as a deterrent for other countries, which is extremely relevant in the context of hybrid wars and the use of special information influences.

Conclusions. Thus, in our opinion, it is rational to simultaneously develop both cyber defense and cyber defense elements using artificial intelligence. These areas can complement each other, contributing to the continued development of such systems.

Of course, the possible risks of such technologies falling into the hands of criminals and / or intelligence services of other states should not be underestimated. The development of approaches to the protection of such systems can be the subject of a separate scientific study.

REFERENCES

[1] Digital Transformation of Communities: How It Happens in Ukraine, Decentralization, 2021. [Online]. Available: https://decentralization.gov.ua/news/13294. Accessed on: Mah 02, 2021.

[2] Analysis of the regulatory impact of the draft resolution of the Cabinet of Ministers of Ukraine “On Amendments to the Rules for Ensuring Information Protection in Information, Telecommunication and Information-Telecommunication Systems”. [Online]. Available: http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=288142. Accessed on: Jan 11, 2021.

[3] Verkhovna Rada of Ukraine. VI convocation, 11th session. (1994, Jul. 05). *Zakon № 31, On Information Protection in Information and Telecommunication Systems*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text. Accessed on: Jan 11, 2021.

[4] A. I. Stasiuk, and A. A. Korchenko, “The method of abnormality detection caused by cyber attacks in computer networks”, *Ukrainian Information Security Research Journal*, vol. 14, no. 4 (57), pp. 127-132, 2012, doi: https://doi.org/10.18372/2410-7840.14.3503.

[5] A. H. Korchenko, *Construction of information protection systems on fuzzy sets*. Moscow, Russia: MK-Press, 2006.
[6] V. V. Volianska, O. O. Korchenko, and E. V. Patsira, "Anomaly detection system based on fuzzy models", *Collection of scientific works of the Pukhov Institute for Modeling in Energy Engineering of the National Academy of Sciences of Ukraine*, vol. 2, Kyiv, pp. 56-60, 2007.
[7] O. H. Korchenko, *Information protection systems*. Kyiv, Ukraine: NAU, 2004.
[8] I. Yu. Subach, and V. V. Fesokha, "Analysis of existing intrusion prevention solutions in information and telecommunication networks, opened on the basis of public licenses", *Information Technology and Security*, vol. 5, iss. 2 (9), pp. 145-152, July – December 2017, doi: https://doi.org/10.20535/2411-1031.2017.5.2.136984.
[9] I. Yu. Subach, Yu. M. Zdorenko, and V. V. Fesokha, "Method of detecting cyberattacks of the type js (html)/scrinject based on the application of the mathematical apparatus of fuzzy set theory", *Collection of scientific works of VITI*, no. 4, pp. 125-131, 2018.
[10] I. Yu. Subach, and V. V. Fesokha, "Model of detection of anomalies in information and telecommunication networks of military administration bodies on the basis of fuzzy sets and fuzzy inference", *Collection of scientific works of VITI*, no. 3, pp. 158-164, 2017.
[11] S. V. Kazmirchuk, A. O. Korchenko, and T. I. Paraschuk, "Analysis of intrusion detection systems", *Ukrainian Information Security Research Journal*, vol. 20, no. 4, pp. 259-276, 2018. doi: https://doi.org/10.18372/2410-7840.20.13425.
[12] N. S. Kozak, P. V. Tsymbal, and Ya. L. Varshavets, "Some aspects of detecting and preventing cybersecurity incidents", in *Proc. Scientific and Practical Conference Cybersecurity in Ukraine: legal and organizational issues*, Odessa, 2017, p. 98-99.
[13] O. Yu. Cherednychenko, Yu. O. Protsyuk, O. V. Shemendyuk, and I. R. Maltseva, "Ways to improve protection schemes against cyberattacks in information and telecommunication systems", *Collection of scientific works of VITI*, no. 3, pp. 103-109, 2019.
[14] V. Yu. Zubok, O. I. Zakharchenko, and Yu. O. Bielanov, "Recognition of anomalous states in information and telecommunication systems with a vague description of events", in *Proc. XVII International Scientific and Practical Conference on Information Technologies and Security*, Kyiv, 2017, pp. 41-45.
[15] O. Korchenko, V. Hnatiuk, E. Ivanchenko, S. Hnatiuk, and N. Seilova, "Method of network-centric monitoring of cyber incidents in modern information and telecommunication systems", *Ukrainian Information Security Research Journal*, vol. 18, no. 3, pp. 229-247, 2016, doi: https://doi.org/10.18372/2410-7840.18.10852.
[16] L. Leenen, and T. Meyer, "Artificial Intelligence and Big Data Analytics in Support of Cyber Defense", in *Proc. Research Anthology on Artificial Intelligence Applications in Security,* 2021, doi: https://doi.org/10.4018/978-1-7998-7705-9.ch076.
[17] A. A. Babkin, and O. V. Kudin, "Review of Neural Network Models of Intrusion Detection Systems", *Informatics, Computing and Automation*, vol. 31 (70), no. 3, pp. 77-82, 2020, doi: https://doi.org/10.32838/TNU-2663-5941/2020.3-1/12.
[18] J. DamianSegrelles Quilis, G. Moltó, I. Blanquer, "A cloud framework for problem-based learning on grid computing", *Journal of Parallel and Distributed Computing* , vol. 155, pp. 24-37, 2021, doi: https://doi.org/10.1016/j.jpdc.2021.04.012.
[19] Cybersecurity ecosystem, 2014. [Online]. Available: https://www.sentar.com/cybersecurity-ecosystem/. Accessed on: Jan 11, 2021.
[20] A. V. Strizhkova, "Historical development of Grid-technologies on the Internet", *Information and law*, no. 1 (16), pp.151-159, 2016.
[21] D. V. Dubov, *Cyberspace as a New Dimension of Geopolitical Rivalry*, Kyiv, Ukraine: National Institute for Strategic Studies, 2014.
[22] O. H. Trofymenko, Yu. V. Prokop, N. I. Loginova, and O. V. Zadereiko, "Monitoring the level of cybersecurity of Ukraine in world ratings". [Online]. Available: http://www.academy.ssu.gov.ua/ua/page/page_1581429315.htm. Accessed on: Jan 11, 2021.

[23] M. Komarov, A. Davydiuk, A. Onyskova, V. Tkachenko, and S. Honchar, "Requirements for a taxonomy of cyber threats of critical infrastructure facilities and an analysis of existing approaches", *Studies in Systems, Decision and Control*, pp. 189-205, 2021, doi: https://doi.org/ 10.1007/978-3-030-69189-9_11.

[24] L. S. Seliverstova, and D. A. Trukhan, "Approaches to the development of cyber insurance as a segment of the global insurance market", *Economics and state*, no. 1, pp. 23-26, 2020, doi: https://doi.org/10.32702/2306-6806.2020.1.23.

[25] Cabinet of Ministers of Ukraine (2020, Dec. 02). *Order № 1556-r, On approval of the Concept of development of artificial intelligence in Ukraine*. [Online]. Available: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220. Accessed on: Jan 11, 2021.

[26] AI-powered Cyber Attacks. [Online]. https://www.f5.com/labs/articles/cisotociso/ai-powered-cyber-attacks. Accessed on: Jan 11, 2021.

The article was received 19.03.2021.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Цифрова трансформація громад: як це відбувається в Україні, Децентралізація, 2021. [Електронний ресурс]. Доступно: https://decentralization.gov.ua/news/13294. Дата звернення: Бер. 02, 2021.

[2] Аналіз регуляторного впливу проекту постанови Кабінету Міністрів України "Про внесення змін до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах". [Електронний ресурс]. Доступно: http://195.78.68.84/ dsszzi/control/uk/publish/article?showHidden=1& art_id=288142. Дата звернення: Січ. 11, 2021.

[3] Верховна рада України (1994, Лип. 05). *Закон № 31, Про захист інформації в інформаційно-телекомунікаційних системах*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text. Дата звернення: Січ. 11, 2021.

[4] А. І. Стасюк, та О. О. Корченко, "Метод выявления аномалий порожденных кибератаками в компьютерных сетях", Захист інформації, том 14, № 4 (57), с. 127-132, 2012. doi: https://doi.org/ 10.18372/2410-7840.14.3503.

[5] О. Г. Корченко, *Построение систем защиты информации на нечетких множествах.* Москва, Росія: МК-Пресс, 2006.

[6] В. В. Волянська, О. О. Корченко, та Є. В. Паціра, "Система виявлення аномалій на основі нечітких моделей", *Збірник наукових праць Інституту проблем моделювання в енергетиці НАН України ім. Г.Є. Пухова*, Том 2, с. 56-60, 2007.

[7] О. Г. Корченко, *Системи захисту інформації.* Київ, Україна: НАУ, 2004.

[8] І. Ю. Субач, та В. В. Фесьоха, "Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі, відкритих на основі загальнодоступних ліцензій", Information Technology and Security, vol. 5, iss. 2 (9), pp. 145-152, July – December 2017, doi: https://doi.org/10.20535/2411-1031.2017.5.2.136984.

[9] І. Ю. Субач, Ю. М. Здоренко, та В. В. Фесьоха, "Методика виявлення кібератак типу js(html)/scrinject на основі застосування математичного апарату теорії нечітких множин", *Збірник наукових праць ВІТІ*, № 4, с. 125-131, 2018.

[10] І. Ю. Субач, та В. В. Фесьоха, "Модель виявлення аномалій в інформаційно – телекомунікаційних мережах органів військового управління на основі нечітких множин та нечіткого логічного виводу", *Збірник наукових праць ВІТІ,* № 3, с. 158-164, 2017.

[11] С. В. Казмірчук, А. О. Корченко, та Т. І. Паращук, “Аналіз систем виявлення вторгнень”, *Захист інформації*, том 20, № 4, с. 259-276, 2018, doi: https://doi.org/10.18372/2410-7840. 20.13425.

[12] Н. С. Козак, П. В. Цимбал, Я. Л. Варшавець, “Деякі аспекти виявлення і попередження інцидентів кібербезпеки”, на *Всеукраїнської науково-практичної конференції Кібербезпека в Україні: правові та організаційні питання,* Одеса, 2017, с. 98-99.

[13] О. Ю. Чередниченко, Ю. О. Процюк, О. В. Шемендюк, та І. Р. Мальцева “Способи вдосконалення схем захисту від кібернетичних атак в інформаційно-телекомунікаційних системах”*, Збірник наукових праць ВІТІ,* № 3, с. 103-109, 2019.

[14] В. Ю. Зубок, О. І. Захарченко, та Ю. О. Бєланов, “Розпізнавання аномальних станів в інформаційно-телекомунікаційних системах при нечіткому описі подій”, на *XVII International Scientific and Practical Conference on Information Technologies and Security,* Київ, 2017, с. 41-45.

[15] О. Корченко, В. Гнатюк, Є. Іванченко, С. Гнатюк, та Н. Сейлова, “Метод мережево-центричного моніторингу кіберінцидентів в сучасних інформаційно-телекомунікаційних системах”, *Захист інформації*, Том. 18, № 3, с. 229-247, 2016, doi: https://doi.org/10.18372/2410-7840.18.10852.

[16] L. Leenen, and T. Meyer, “Artificial Intelligence and Big Data Analytics in Support of Cyber Defense”, in *Proc. Research Anthology on Artificial Intelligence Applications in Security,* 2021. doi: https://doi.org/10.4018/978-1-7998-7705-9.ch076.

[17] А. А. Бабкін, та О.В. Кудін, “Огляд нейромережевих моделей систем виявлення вторгнень”, *Інформатика, обчислювальна техніка та автоматизація*, Том 31 (70), № 3, с.77-82, 2020. doi: https://doi.org/10.32838/TNU-2663-5941/2020.3-1/12.

[18] J. DamianSegrelles Quilis, G. Moltó, I. Blanquer, “A cloud framework for problem-based learning on grid computing”, *Journal of Parallel and Distributed Computing* , vol. 155, pp. 24-37, 2021, doi: https://doi.org/10.1016/j.jpdc.2021.04.012.

[19] Cybersecurity ecosystem, 2014. [Електронний ресурс]. Доступно: https://www.sentar.com/ cybersecurity-ecosystem/. Дата звернення: Січ. 11, 2021.

[20] А. В. Стріжкова, “Історичний розвиток Grid-технологій у мережі Інтернет”, *Інформація і право*, № 1(16), с. 151-159, 2016.

[21] Д. В. Дубов, *Кіберпростір як новий вимір геополітичного суперництва*, Київ, Україна: Національний інститут стратегічних досліджень, 2014.

[22] О. Г. Трофименко, Ю. В. Прокоп, Н. І. Логінова, та О. В. Задерейко, “Моніторинг рівня кібербезпеки України у світових рейтингах”. [Електронний ресурс]. Доступно: http://www.academy.ssu.gov.ua/ua/page/page_1581429315.htm. Дата звернення: Січ. 11, 2021.

[23] M. Komarov, A. Davydiuk, A. Onyskova, V. Tkachenko, and S. Honchar, “Requirements for a taxonomy of cyber threats of critical infrastructure facilities and an analysis of existing approaches”, *Studies in Systems, Decision and Control*, с. 189-205, 2021, doi: https://doi.org/ 10.1007/978-3-030-69189-9_11.

[24] Л. С. Селіверстова, та Д. А. Трухан, “Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку”, *Економіка та держава*, № 1, с. 23-26. 2020. doi: https://doi.org/10.32702/2306-6806.2020.1.23

[25] Кабінет Міністрів України. (2020, Груд. 02). *Розпорядження № 1556-р, Про схвалення Концепції розвитку штучного інтелекту в Україні*. [Електронний ресурс]. Доступно: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220. Дата звернення: Січ. 11, 2021.

[26] Кібер-атаки на основі штучного інтелекту. 2020 [Електронний ресурс]. Доступно: https://www.f5.com/labs/articles/cisotociso/ai-powered-cyber-attacks. Дата звернення: Січ. 11, 2021.

СЕРГІЙ СЕРГЕЄВ,
АНДРІЙ ДАВИДЮК,
АЛЛА ОНИСЬКОВА

ОГЛЯД ТА ПЕРСПЕКТИВИ РОЗВИТКУ МЕТОДІВ ВИЯВЛЕННЯ КІБЕРАТАК НА ІНФОРМАЦІЙНІ СИСТЕМИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

В умовах стрімкого розвитку інформаційних технологій та впровадження їх у наше життя все актуальнішою стає проблема захисту інформації. У період гібридної війни, масштабного переходу приватних та державних організацій на віддалену роботу під час пандемії COVID-19, епохи цифрової трансформації держави дана проблема невідкладно потребує постійного пошуку ефективних рішень. Інформаційні системи об'єктів критичної інфраструктури, державного та приватного секторів зазнають значних збитків від кібератак. Величина цих втрат напряму залежить від своєчасного виявлення несанкціонованого втручання в їхню роботу. Метою цієї статті є встановлення переваг і недоліків відомих методів для подальшого ефективного їх впровадження у межах побудови систем захисту інформації. Для досягнення поставленої мети проаналізовано найбільш розповсюджені методи виявлення кібератак, визначені їх переваги і недоліки. Зокрема, системи на основі сигнатурного аналізу є більш стабільними та мають меншу кількість помилкових спрацьовувань. Однак, вони неефективні для виявлення нових кібератак. Експертні методи на основі нечіткої логіки характеризуються суб'єктивністю отриманих результатів та часовими затратами у реалізації. На основі аналізу визначено перспективи розвитку методів виявлення кібератак з використанням технологій штучного інтелекту, зокрема, запропоновано використання грідмереж для збільшення обчислювальних потужностей при роботі з великими обсягами даних та реалізації алгоритмів глибинного аналізу інформації. Отримані при цьому результати можуть використовуватися при побудові комплексних систем захисту інформації та/або систем управління інформаційною безпекою. Крім цього можуть сприяти індексуванню (рейтингуванню) об'єктів оцінювання рівня кіберзахисту, розвитку впровадження ринку кіберстрахування як альтернативного підходу до захисту інформації та збільшення потенціалу України в галузі кібербезпеки та кібероборони. Побудова систем активного кіберзахисту з використанням технологій штучного інтелекту забезпечить більш безпечне середовище для подальшого розвитку новітніх технологій і сталого існування суспільства в ньому. Додатково це може мати позитивний економічний ефект завдяки мінімізації передбачуваних збитків та централізованого впровадження технічних засобів захисту з використанням динамічного розподілу ресурсів.

Ключові слова: кібербезпека, кібератака, системи виявлення вторгнень, виявлення аномалій, штучний інтелект, грідмережа.

Serheiev Serhii, postgraduate student, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine, ORCID 0000-0001-7454-0024, ssn@dsszzi.gov.ua.

Davydiuk Andrii, postgraduate student, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine, ORCID 0000-0003-1238-2598, andrey19941904@gmail.com.

Onyskova Alla, junior researcher, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine, ORCID 0000-0003-2833-5569, alla.oniskova@ukr.net.

Сергеєв Сергій Миколайович, аспірант, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

Давидюк Андрій Вікторович, аспірант, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

Ониськова Алла Вікторівна, молодший науковий співробітник, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.