https://doi.org/10.31891/2307-5732-2026-363-2
УДК 004.8:004.056

АНТОНЕНКО АРТЕМ
Національний університет біоресурсів і природокористування України
https://orcid.org/0000-0001-9397-1209
e-mail: artem.v.antonenko@gmail.com
ВОСТРІКОВ СЕРГІЙ
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0008-8425-8872
e-mail: s.vostrikov@stud.duikt.edu.ua
ЧЕЧИК СЕРГІЙ
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0009-9293-5156
e-mail: kardinal5700@ukr.net
СОЛЬСЬКИЙ ДАНИЇЛ
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0005-0351-5987
e-mail: d.solskyi@stud.duikt.edu.ua

ПЕРСПЕКТИВИ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕКУ

У статті штучний інтелект (ШІ) визначається як система, що моделює аспекти людського інтелекту на базі комп'ютерних технологій, математики, інформатики та філософії, з метою імітації сприйняття, розуміння та взаємодії з середовищем. У контексті кібербезпеки ШІ інтегрується в системи виявлення вторгнень (IDS), де він підвищує ефективність за рахунок автоматизованого аналізу даних, прогнозування загроз та адаптивного реагування. Дослідження підкреслюють актуальність такої інтеграції, особливо в умовах зростання складності кібератак, включаючи AI-драйвені загрози, як автономне зловмисне ПЗ та соціальну інженерію. Ключові дослідження фокусуються на моделях, таких як IntruDTree – ML-базованій системі на основі дерев рішень, яка ранжує функції безпеки, мінімізує обчислювальну складність та досягає високої точності в виявленні вторгнень, перевершуючи традиційні методи (наївний Байєс, логістичну регресію тощо). Нейроморфний підхід поєднує глибоке навчання (DL) з нейроморфними процесорами, використовуючи автоенкодери (AE) для навчання без нагляду, дискретну факторизацію векторів (DVF) для перетворення ваг та симуляцію на чіпах як IBM True North, досягаючи 90,12% точності в виявленні шкідливих пакетів та 81,31% у класифікації атак. Це забезпечує енергоефективне, реального часу виявлення в високонавантажених мережах. Машинне навчання застосовується для аналізу зловмисного ПЗ, виявлення zero-day атак, аномалій та загроз трафіку, з акцентом на датасети як ADFA-LD, що відповідає сучасним технологіям для оцінки IDS. Ризики включають адверсарні атаки на ML-алгоритми, що вимагають превентивних заходів. Портал AZ Safe Hacker Assets Portal збирає дані з хакерських форумів для проактивного CTI, аналізуючи активи з ML для пошуку, навігації та порівняння коду. Запобігання атакам з ШІ охоплює соціальну інженерію, де вразливості залежать від людського фактора, але ШІ допомагає в освіті та зменшенні впливу. Байєсівські методи дозволяють кількісну оцінку ризиків, ситуаційну обізнаність та автоматизацію. За прогнозами досліджень (Gartner, Trend Micro), AI-агенти домінуватимуть в атаках та захисті, з фокусом на квантову безпеку, explainable AI та автономні системи, що вимагає балансу між інноваціями та ризиками.

Ключові слова: *штучний інтелект, кібербезпека, виявлення вторгнень, машинне навчання, нейроморфні обчислення, IntruDTree, ADFA-LD, адверсарні атаки, байєсівські методи, CTI.*

ANTONENKO ARTEM
National University of Life and Environmental Sciences of Ukraine
VOSTRIKOV SERGII, CHECHYK SERHII, SOLSKYI DANYIL
State University of Information and Communication Technologies

PROSPECTS FOR INTEGRATION OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

The article defines artificial intelligence (AI) as a system that models aspects of human intelligence based on computer technology, mathematics, computer science and philosophy, with the aim of imitating perception, understanding and interaction with the environment. In the context of cybersecurity, AI is integrated into intrusion detection systems (IDS), where it increases efficiency through automated data analysis, threat prediction and adaptive response. The materials emphasize the relevance of such integration, especially in the context of increasing complexity of cyberattacks, including AI-driven threats such as autonomous malware and social engineering. Key research focuses on models such as IntruDTree - an ML-based system based on decision trees, which ranks security features, minimizes computational complexity and achieves high accuracy in intrusion detection, outperforming traditional methods (naive Bayes, logistic regression, etc.). The neuromorphic approach combines deep learning (DL) with neuromorphic processors, using autoencoders (AE) for unsupervised learning, discrete vector factorization (DVF) for weight transformation, and simulation on chips like IBM True North, achieving 90.12% accuracy in detecting malicious packets and 81.31% in classifying attacks. This provides energy-efficient, real-time detection in high-traffic networks. Machine learning is applied to analyze malware, detect zero-day attacks, anomalies, and traffic threats, with a focus on datasets like ADFA-LD, which are in line with current technologies for evaluating IDS. Risks include adversarial attacks on ML algorithms, requiring preventive measures. The AZ Safe Hacker Assets Portal collects data from hacker forums for proactive CTI, analyzing ML assets for search, navigation, and code comparison. Preventing AI attacks involves social engineering, where vulnerabilities are human-driven, but AI helps with education and mitigation. Bayesian methods enable quantitative risk assessment, situational awareness, and automation. Research (Gartner, Trend Micro) predicts that AI agents will dominate attacks and defenses, with a focus on quantum security, explainable AI, and autonomous systems, requiring a balance between innovation and risk.

Keywords: *artificial intelligence, cybersecurity, intrusion detection, machine learning, neuromorphic computing, IntruDTree, ADFA-LD, adversarial attacks, Bayesian methods, CTI.*

Стаття надійшла до редакції / Received 29.01.2026
Прийнята до друку / Accepted
Опубліковано / Published

Statement of the problem in general form and its connection with important scientific or practical tasks

In today's digital environment, cybersecurity faces unprecedented challenges due to the rapid development of artificial intelligence (AI) technologies. The relevance of the problem of integrating AI into cybersecurity is confirmed by global trends: according to Gartner and Palo Alto Networks forecasts for 2026, AI-based preemptive cybersecurity will become dominant, with the transition to AI-native security platforms; mass implementation of agentic AI is expected, which will lead to an increase in risks, including shadow AI, autonomous threats and post-quantum challenges. At the same time, adversarial attacks on AI protection systems themselves make traditional approaches ineffective, and the shortage of specialists (estimated at 4.8 million vacancies globally) complicates management.

The main problem of the research is the paradox of AI integration: how to maximize the potential of artificial intelligence to improve cybersecurity effectiveness (detection of zero-day vulnerabilities, countering ransomware and APT attacks, SOC automation), while minimizing the risks associated with AI vulnerability to adversarial attacks, ethical aspects (according to the EU AI Act and NIST AI Risk Management Framework), loss of control over autonomous agents, and erosion of trust through deepfakes and AI-driven social engineering. The lack of understanding of the balance between "defense with AI" and "defense of AI itself" leads to the fact that many organizations are facing an increase in incidents (according to IBM and CrowdStrike reports 2025–2026) where attackers are ahead of defenders in using AI. Thus, the prospects for integrating AI into cybersecurity require a comprehensive analysis of benefits, challenges (adversarial robustness, explainable AI, governance), and development strategies (preemptive defenses, hybrid human-AI systems) to ensure sustainable defense in the era of AI-dominated cyberwarfare.

Analysis of recent research and publications

The integration of artificial intelligence (AI) into cybersecurity is currently a promising direction in the field of creating new protection systems by automating threat detection, attack prediction and adaptive response to incidents. AI-based cybersecurity systems should strengthen the protection of information resources of organizations with physiologically active algorithms, since the effectiveness of protection is determined precisely by the ability to analyze large volumes of data, detect anomalies, classify malicious software and make components available in real time [1-22]. Recent publications by Ukrainian scientists focus on the dual role of AI in hybrid warfare, critical infrastructure protection, risk assessment and legal regulation of technologies. The study by Skitska et al. analyzes the threats and risks of using AI, proposing approaches to creating a risk management system for state regulatory policy [3]. Gurzhiy S. V. considers the features of using AI to ensure cybersecurity, outlining the legal principles and threatening trends based on Europol reports [4]. Letychevsky O. O. highlights modern scientific problems of cybersecurity, in particular the role of neural networks and AI methods in addressing vulnerabilities [5]. Pantyushenko R. and Chaika Y. explore innovations, challenges and prospects for the development of AI in cybersecurity, with a focus on practical applications in the defense sector [6]. Foreign researchers provide systematic reviews of the effectiveness of AI, adversary attacks and future directions of development. Ferrag M. A. et al. offer a detailed literature review and taxonomy of the application of AI in cybersecurity, highlighting the prospects for automation [7]. Nievas J. et al. provide a comprehensive analysis of the application of AI in cybersecurity with an emphasis on future directions and challenges [8]. Truică C.-O. & Apostol E.-S. focus on advanced AI-driven threat detection techniques, including big data analysis [9]. Apruzzese G. et al. evaluate the effectiveness of machine and deep learning in cybersecurity compared to traditional methods [10].

Formulation of the purpose of the article

The purpose of the article is to study the prospects for integrating artificial intelligence into cybersecurity systems to improve the effectiveness of threat detection and countermeasures.

Object of research: application of artificial intelligence in cyberattack detection and prevention systems.

Subject of research: AI models and algorithms (IntruDTree, neuromorphic approaches, Bayesian methods), datasets (ADFA-LD), risks (adversarial attacks, social engineering) and tools (AZ Safe Hacker Assets Portal) for integration into cybersecurity.

Presenting main material

Artificial intelligence is a system created on the basis of computer technology that attempts to model certain aspects of human mentality and functioning. This system can interact with the environment, for example, recognize voice and convert it into different languages, imitating human abilities. It is based on various sciences such as mathematics, computer science and philosophy, and its main goal is to create systems that can demonstrate certain aspects of human intellectual activity. The term "artificial intelligence" is often used to describe systems that are able to emulate the basic functions of perception and understanding that are characteristic of human thinking Fig. 1.

The integration of artificial intelligence into intrusion detection systems (IDS) is gaining great relevance. X. A. Larriva-Novo et al. [12] propose algorithms to improve the effectiveness of IDS, particularly in the context of specific scenarios. To do this, cybersecurity datasets are categorized, which allows them to be grouped into specified categories. The paper considers different neural network models, such as multilayer and recurrent, uses various activation functions and training algorithms to achieve optimal accuracy depending on the characteristics of the database.

The results were used to determine which category of cybersecurity dataset is more important for intrusion detection and the most adequate configuration of the machine learning algorithm to minimize the computational load. There are also significant security risks in the interconnections required to exploit certain advantages of automated systems. The paper describes an intrusion detection system based on the concepts of unsupervised automated systems.

Fig. 1. Using artificial intelligence

A tree-based security machine learning model (IntruD Tree) is presented that evaluates a security feature based on its importance and builds a general intrusion detection model. This model not only has prediction accuracy for unattractive test cases, but also minimizes the computational complexity of the model by reducing the feature measurements. Finally, cybersecurity datasets and accuracy measurements are used to validate the performance of our IntruDTree model. The authors also compare the results of IntruDTree with various traditional, conventional machine learning approaches, such as naive classification system, logistic regression, support vector systems, and nearest neighbor, to evaluate the performance of the resulting security model.

In this paper, a neuromorphic cognitive computing approach was proposed for a deep learning (DL) cybersecurity network intrusion detection system (IDS). The algorithmic power of DL was combined with fast and high-performance neuromorphic cybersecurity processors. The data was numbered for training using a rigorous unsupervised learning technique called autoencoder during the training (AE) process. The AE weights generated for the supervised learning stage are used as initial weights for the neural networks. The final weights are converted into discrete weights, synaptic weights, and thresholds for nerve cells using discrete vector factorization (DVF). Finally, the generated cross-weights, synaptic weights, thresholds, and leakages were mapped into cross-stripes and neurons. During the checkpoint, the encoded samples are converted into a central shape using hybrid encoding methods. IBM Neurosynaptic Core Simulator (NSCS) and the new True North neurosynaptic chip were used for implementation and testing. For cybersecurity intrusion detection of the neuromorphic chip, the test results indicate an accuracy of approximately 90.12 percent. Furthermore, the authors have revised the proposed framework not only for detecting malicious packets but also for classifying these types of attacks and achieved an accuracy of 81.31%. The neuromorphic implementation provides amazing accuracy in detecting and classifying high-powered network intrusion detection. For cyber security intrusion detection of the neuromorphic chip, the test results indicate an accuracy of approximately 90.12 percent. Furthermore, the authors have revised the proposed framework not only for detecting malicious packets but also for classifying these types of attacks and achieved an accuracy of 81.31%.

Neuromorphic implementation provides amazing accuracy in detection and classification of high-powered network intrusion detection. For cyber security intrusion detection of neuromorphic chip, the test results indicate an accuracy of approximately 90.12 percent. In addition, the authors revised the proposed framework not only for detecting malicious packets, but also for classifying these types of attacks and achieved an accuracy of 81.31%. Neuromorphic implementation provides amazing accuracy in detection and classification of high-powered network intrusion detection.

Machine learning technology is popular in many fields, and machine learning technology has many applications in cybersecurity. Examples of malware include malware analysis, including zero-day malware detection, threat analysis, intrusion anomaly detection, and many others. In many cybersecurity products, researchers use machine learning detection due to the ineffectiveness of signature-based approaches in detecting new attacks or even minor variations of existing attacks. In this [14] study, in which machine learning is a method, the authors discuss various areas of cybersecurity. To manipulate learning and data classification research, the authors also have some experience with adverse attacks on machine learning algorithms, so these approaches do not work.

Preventing Cyberattacks and Threats with AI. Artificial intelligence was just a type of computerized version of human intelligence. The way AI functions is similar to learning, just like humans do, iteratively over and over again. The threat landscape is undoubtedly evolving in this century. Cybercriminals are driven solely by financial incentives. But the department has found a new way to prevent attacks before they happen, as it can no longer rely on old, conventional methods. This article [12] highlights the need to develop cybersecurity skills and how the use of artificial neural networks and machine learning algorithms can mean improved skills. Also included is an overview and definition of social engineering, the role it plays in online and cybercrime, and the causes and impact of cybercrime.

Preventive actions and potential solutions to threats and vulnerabilities in social engineering are recommended, based on the findings presented in the article [13], vulnerability depends on human behavior, mental impulses and psychological predispositions, although technology helps to reduce the impact of social engineering attacks. Although the literature confirms the investment risks in organizational training camps due to the sensitivity of social engineering, it can be optimistically said that social engineering attacks can be reduced.

Billions of dollars in losses are caused by cybercrime, operating system failures, destruction of classified information, network security and confidentiality violations. Computer system security has become essential to minimize the impact and, presumably, deter cybercrime in light of these crimes being committed every day. The article discusses recent advances in the use of cybersecurity datasets to evaluate machine learning intrusion detection systems and data mining. It has been found that current cybersecurity standards are no longer reliable because their databases no longer match modern computer technology developments. In 2013, a new ADFA Linux (ADFA-LD) cybersecurity benchmarking dataset was proposed to match the current world-class computer technology advances for machine learning analysis of data mining and intrusion detection systems. ADFA-LD includes better definitions of their attributes. The research community will use this research to move away from current cybersecurity benchmarking datasets and start using the newly implemented benchmarking dataset for efficient and systematic evaluation of computer and data mining intrusion detection systems. Social and Internet traffic analysis is essential for identifying and protecting against cyber threats. Advanced automated machine learning approaches are replacing traditional approaches that revert to manually defined rules. This revolution is being accelerated by massive data sets that provide machine learning models with higher performance. The paper [15] reviews recent analytical research on cyber traffic across social networks and the Internet, using a set of general principles of similarity, relationship, and collective indications in the context of a data-driven model. This is not an isolated desire, but the common use of various networks and social movements is explained by this. Streams also have a number of features, including fixed size and multiple messages between the source and the recipient. The paper presents a modern methodology for research and application in Internet security, data-driven social and Internet traffic (DDCS). The DDCS approach includes three elements: cybersecurity data collection, cybersecurity development, and cybersecurity modeling. Challenges and future paths are also discussed.

Cyberattacks pose a serious threat to national security. Today, the number of malicious tools that carry out numerous cyberattacks is increasing. Knowledge and tools to deter and mitigate attacks have been planned for Cyber Threat Intelligence (CTI) and Malware Analysis Portal. However, current CTI portals and malware analysis are accused of being too reactive because they depend on previous cyberattacks to collect data. Online hacker forums provide a new source of information for proactive CTI and malware portals. Research [15] shows AZ Safe Hacker Assets Portal. This website collects and analyzes malicious products from largely untapped and rich data sources of online hacker groups using state-of-the-art machine learning techniques. This paper discusses the creation and development of AZ Safe Hacker Assets Portal. The authors also provide basic portal features, including asset search, navigation and download, source code viewing and code comparison analytics, and an interactive CTI dashboard. Cybersecurity threats have increased over the past decade. Experts believe that existing security measures will soon be insufficient to prevent the spread of more sophisticated and dangerous cyberattacks. Recently, the complexity of cybersecurity has increasingly been dominated by approaches borrowed from artificial intelligence (AI) to facilitate automation. In this paper [11], researchers provide a brief overview and guidance on Bayesian cybersecurity programs to enable quantitative threat assessment for superior risk analysis and situational awareness.

Conclusions and prospects for further research

As cybercrime becomes more complex, cybersecurity approaches need to be more robust and intelligent. This will allow defense mechanisms to make real-time decisions to effectively respond to sophisticated attacks. However, AI approaches to combating cybercrime are still unclassified, which requires separate research. Therefore, to effectively combat cybercrime, researchers and practitioners need to be aware of existing cybersecurity methods and apply AI.

Artificial intelligence significantly enhances cybersecurity, in particular through models like IntruDTree, which optimizes intrusion detection with minimal computational complexity and higher accuracy compared to traditional methods. Neuromorphic computing with deep learning provides real-time analysis with up to 90.12% accuracy for detection and 81.31% for classification of attacks, making systems energy-efficient and adaptive. Datasets like ADFA-LD allow for the evaluation of IDS in modern conditions, and the AZ Safe Hacker Assets Portal provides proactive CTI from hacker sources. AI also carries risks, adversarial attacks manipulate ML algorithms, and social engineering exploits the human factor, requiring educational measures. Bayesian methods are effective for quantitative risk assessment and situational awareness. The outlook for 2025–2026 includes the dominance of AI agents in attacks and defense, integration with quantum technologies, and explainable AI to increase trust. Overall, the integration of AI transforms cybersecurity into an autonomous, preventive system, but requires a balance between innovation, ethics, and regulation to minimize vulnerabilities.

References

1. Natsionalnyi tekhnichnyi universytet Ukrainy «Kyivskyi politekhnichnyi instytut imeni Ihoria Sikorskoho». Metody shtuchnoho intelektu v kiberbezpetsi : navchalnyi posibnyk. – Kyiv, 2023.

2. Savchenko V. A. Osnovni napriamy zastosuvannia tekhnolohii shtuchnoho intelektu u kiberbezpetsi / V. A. Savchenko, O. D. Shapovalenko // Suchasnyi zakhyst informatsii. – 2020. – № 4. – S. 44.

3. Skitsko O. Zahrozy ta ryzyky vykorystannia shtuchnoho intelektu / O. Skitsko, P. Skladannyi, R. Shyrshov, M. Humeniuk, M. Vorokhob // Kiberbezpeka: osvita, nauka, tekhnika. – 2023. – № 2 (22). – S. 6–18.

4. Hurzhyi S. V. Osoblyvosti vykorystannia shtuchnoho intelektu u pytanniakh zabezpechennia kiberbezpeky / S. V. Hurzhyi // Informatsiia i pravo. – 2023. – № 4 (47).

5. Letychevskyi O. O. Suchasni naukovi problemy kiberbezpeky / O. O. Letychevskyi // Visnyk Natsionalnoi akademii nauk Ukrainy. – 2023. – № 2. – S. 12–20.

6. Pantiushenko R. Shtuchnyi intelekt u sferi kiberbezpeky: innovatsii, vyklyky ta perspektyvy rozvytku / R. Pantiushenko, Yu. Chaika // Mizhnarodnyi naukovyi zhurnal «Military Science». – 2024. – T. 2, № 1. – S. 200–206.

7. Ferrag M. A. Artificial intelligence for cybersecurity: Literature review and future research directions / M. A. Ferrag, L. Maglaras, S. Moschoyiannis, H. Janicke // Information Fusion. – 2023. – Vol. 97. – Article 101804.

8. Nievas J. Artificial intelligence in cybersecurity: A comprehensive review and future direction / J. Nievas, P. García-Teodoro, J. Díaz-Verdejo // Applied Artificial Intelligence. – 2024. – Vol. 38, № 1. – Article 2439609.

9. Truică C.-O. Advancing cybersecurity: A comprehensive review of AI-driven detection techniques / C.-O. Truică, E.-S. Apostol // Journal of Big Data. – 2024. – Vol. 11. – Article 129.

10. Apruzzese G. On the effectiveness of machine and deep learning for cyber security / G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, M. Marchetti // Information Fusion. – 2023. – Vol. 82. – P. 102–113.

11. Larriva-Novo X. A. Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies / X. A. Larriva-Novo, M. Vega-Barbas, V. A. Villagra, M. Sanz Rodrigo // IEEE Access. – 2020. – Vol. 8. – P. 9005–9014.

12. Straub J. CyberSecurity considerations for an interconnected self-driving car system of systems / J. Straub [et al.] // 2017 12th Syst. Syst. Eng. Conf. SoSE 2017. – 2017.

13. Shaukat K. Performance comparison and current challenges of using machine learning techniques in cybersecurity / K. Shaukat [et al.] // Energies. – 2020. – Vol. 13, № 10.

14. Coulter R. Data-Driven Cyber Security in Perspective – Intelligent Traffic Analysis / R. Coulter, Q. L. Han, L. Pan, J. Zhang, Y. Xiang // IEEE Trans. Cybern. – 2020. – Vol. 50, № 7. – P. 3081–3093.

15. Benedyko I. V. Klasyfikatsii modelei zastosuvannia mashynnoho navchannia u kiberbezpetsi / I. V. Benedyko, A. I. Vichkaruk, A. V. Antonenko, K. V. Lysenko, O. Yu. Syzhko // Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky. – 2023. – № 4. – S. 11–22.

16. Lemeshko A. V. Aktualni zasady stvorennia alhorytmiv obrobky informatsii dlia lohistychnykh tsentriv / A. V. Lemeshko, A. V. Antonenko, A. A. Balvak, Ye. O. Novichenko // Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky. – 2023. – № 1. – S. 25–32.

17. Lemeshko A. V. Neiromorfni systemy yak instrument realizatsii shtuchnoho intelektu / A. V. Lemeshko, A. V. Antonenko, A. V. Petryk // Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Tekhnichni nauky. – 2023. – T. 34 (73), № 3. – S. 175–183.

18. Lemeshko A. Doslidzhennia merezhevykh zahroz dlia zabezpechennia maksymalnoho zakhystu danykh ta infrastruktury / A. Lemeshko, N. Kuvik, A. Antonenko, V. Hnadyi // Herald of Khmelnytskyi National University. Technical sciences. – 2023. – T. 1, № 3 (321). – S. 64–68.

19. Pakhomov M. Vykorystannia shtuchnoho intelektu v avtomatyzovanykh systemakh / M. Pakhomov, A. V. Antonenko, T. Kalita, V. Haleta // Herald of Khmelnytskyi National University. Technical sciences. – 2023. – № 4 (323). – S. 11–20.

20. Solobaiev S. H. Vykorystannia neironnykh merezh u prohnozuvanni bezpeky merezhi / S. H. Solobaiev, S. O. Vostrikov, A. V. Antonenko, O. V. Tkachenko, A. O. Khodosov, O. S. Ostapenko // Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky. – 2025. – № 2. – S. 3–10.

21. Tverdokhlib A. O. Efektyvnist funktsionuvannia kompiuternykh system pry vykorystanni tekhnolohii blokchein i baz danykh / A. O. Tverdokhlib, D. S. Korotin, A. V. Antonenko // Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky. – 2023. – № 6. – S. 25–36.

22. Zaitsev I. Exploring advanced hypothesis generation in astronomy through the implementation of a mathematical model of linguistic neural networks / I. Zaitsev, O. Golubenko, O. Tkachenko, O. Pidmohylnyi, A. Antonenko // CEUR Workshop Proceedings. – 2023. – Vol. 3687. – P. 121–128.

Література

1. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського». Методи штучного інтелекту в кібербезпеці : навчальний посібник. – Київ, 2023.

2. Савченко В. А. Основні напрями застосування технологій штучного інтелекту у кібербезпеці / В. А. Савченко, О. Д. Шаповаленко // Сучасний захист інформації. – 2020. – № 4. – С. 44.

3. Скіцько О. Загрози та ризики використання штучного інтелекту / О. Скіцько, П. Складанний, Р. Ширшов, М. Гуменюк, М. Ворохоб // Кібербезпека: освіта, наука, техніка. – 2023. – № 2 (22). – С. 6–18.

4. Гуржій С. В. Особливості використання штучного інтелекту у питаннях забезпечення кібербезпеки / С. В. Гуржій // Інформація і право. – 2023. – № 4 (47).

5. Летичевський О. О. Сучасні наукові проблеми кібербезпеки / О. О. Летичевський // Вісник Національної академії наук України. – 2023. – № 2. – С. 12–20.

6. Пантюшенко Р. Штучний інтелект у сфері кібербезпеки: інновації, виклики та перспективи розвитку / Р. Пантюшенко, Ю. Чайка // Міжнародний науковий журнал «Military Science». – 2024. – Т. 2, № 1. – С. 200–206.

7. Ferrag M. A. Artificial intelligence for cybersecurity: Literature review and future research directions / M. A. Ferrag, L. Maglaras, S. Moschoyiannis, H. Janicke // Information Fusion. – 2023. – Vol. 97. – Article 101804.

8. Nievas J. Artificial intelligence in cybersecurity: A comprehensive review and future direction / J. Nievas, P. García-Teodoro, J. Díaz-Verdejo // Applied Artificial Intelligence. – 2024. – Vol. 38, № 1. – Article 2439609.

9. Truică C.-O. Advancing cybersecurity: A comprehensive review of AI-driven detection techniques / C.-O. Truică, E.-S. Apostol // Journal of Big Data. – 2024. – Vol. 11. – Article 129.

10. Apruzzese G. On the effectiveness of machine and deep learning for cyber security / G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, M. Marchetti // Information Fusion. – 2023. – Vol. 82. – P. 102–113.

11. Larriva-Novo X. A. Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies / X. A. Larriva-Novo, M. Vega-Barbas, V. A. Villagra, M. Sanz Rodrigo // IEEE Access. – 2020. – Vol. 8. – P. 9005–9014.

12. Straub J. CyberSecurity considerations for an interconnected self-driving car system of systems / J. Straub [et al.] // 2017 12th Syst. Syst. Eng. Conf. SoSE 2017. – 2017.

13. Shaukat K. Performance comparison and current challenges of using machine learning techniques in cybersecurity / K. Shaukat [et al.] // Energies. – 2020. – Vol. 13, № 10.

14. Coulter R. Data-Driven Cyber Security in Perspective – Intelligent Traffic Analysis / R. Coulter, Q. L. Han, L. Pan, J. Zhang, Y. Xiang // IEEE Trans. Cybern. – 2020. – Vol. 50, № 7. – P. 3081–3093.

15. Бенедіко І. В. Класифікації моделей застосування машинного навчання у кібербезпеці / І. В. Бенедіко, А. І. Вічкарук, А. В. Антоненко, К. В. Лисенко, О. Ю. Сижко // Таврійський науковий вісник. Серія: Технічні науки. – 2023. – № 4. – С. 11–22.

16. Лемешко А. В. Актуальні засади створення алгоритмів обробки інформації для логістичних центрів / А. В. Лемешко, А. В. Антоненко, А. А. Балвак, Є. О. Новіченко // Таврійський науковий вісник. Серія: Технічні науки. – 2023. – № 1. – С. 25–32.

17 Лемешко А. В. Нейроморфні системи як інструмент реалізації штучного інтелекту / А. В. Лемешко, А. В. Антоненко, А. В. Петрик // Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки. – 2023. – Т. 34 (73), № 3. – С. 175–183.

18. Лемешко А. Дослідження мережевих загроз для забезпечення максимального захисту даних та інфраструктури / А. Лемешко, Н. Кувік, А. Антоненко, В. Гнядий // Вісник Хмельницького національного університету. – 2023. – Т. 1, № 3 (321). – С. 64–68.

19. Пахомов М. Використання штучного інтелекту в автоматизованих системах / М. Пахомов, А. В. Антоненко, Т. Калита, В. Галета // Вісник Хмельницького національного університету. – 2023. – № 4 (323). – С. 11–20.

20. Солобаєв С. Г. Використання нейронних мереж у прогнозуванні безпеки мережі / С. Г. Солобаєв, С. О. Востріков, А. В. Антоненко, О. В. Ткаченко, А. О. Ходосов, О. С. Остапенко // Таврійський науковий вісник. Серія: Технічні науки. – 2025. – № 2. – С. 3–10.

21. Твердохліб А. О. Ефективність функціонування комп'ютерних систем при використанні технології блокчейн і баз даних / А. О. Твердохліб, Д. С. Коротін, А. В. Антоненко // Таврійський науковий вісник. Серія: Технічні науки. – 2023. – № 6. – С. 25–36.

22. Zaitsev I. Exploring advanced hypothesis generation in astronomy through the implementation of a mathematical model of linguistic neural networks / I. Zaitsev, O. Golubenko, O. Tkachenko, O. Pidmohylnyi, A. Antonenko // CEUR Workshop Proceedings. – 2023. – Vol. 3687. – P. 121–128.