BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en

Vol. 29 No. 4. 2024

UDC 004.056.5:004.8
DOI: 10.62660/bcstu/4.2024.53

Improving cybersecurity with artificial intelligence

Nazar Zaplatynskyi*
Master
Lviv National University of Nature Management
80831, 1 Volodymyr Velykyi Str., Dubliany, Ukraine
https://orcid.org/0009-0002-7767-8795

Pavlo Lub
PhD in Technical Sciences, Associate Professor
Lviv National University of Nature Management
80831, 1 Volodymyr Velykyi Str., Dubliany, Ukraine
https://orcid.org/0000-0001-9600-0969

Serhiy Zaporozhtsev
PhD in Technical Sciences, Associate Professor
Lviv National University of Nature Management
80831, 1 Volodymyr Velykyi Str., Dubliany, Ukraine
https://orcid.org/0000-0002-8250-2834

Abstract. The study aimed to explore the possibilities of using artificial intelligence to improve cybersecurity systems in the context of increasing complexity and frequency of cyber threats. Analysis of the effectiveness of integrating machine and deep learning methods into the processes of detecting, assessing and neutralisation threats, as well as identification of the strengths and weaknesses of such approaches, were emphasised. The study substantiated the need to combine the technological capabilities of artificial intelligence with expert human experience to ensure comprehensive and adaptive protection of information systems. The study examined the potential application of artificial intelligence to improve cybersecurity systems, given the growing threats and complexity of modern cybercrime. The impact of machine learning and deep learning technologies on improving the effectiveness of traditional methods of protecting information systems was analysed. The study noted that despite the unchanged basic motivations of cybercriminals, their methods were becoming more sophisticated, which required new approaches to detecting and neutralising threats. The use of artificial intelligence was defined as one of the most promising areas of cybersecurity development, as it allows for the automation of risk assessment and incident response processes, reducing response times and increasing overall security efficiency. Particular attention was devoted to an analysis of the strengths and weaknesses of artificial intelligence in the context of cybersecurity. The necessity of integrating artificial intelligence with human intuition and experience was substantiated, as the combination of these components proved to be the most effective approach to ensuring comprehensive security. In addition, the potential risks and concerns associated with the use of artificial intelligence in cybersecurity were explored. The study concluded that a holistic approach that considers both technical and social aspects is needed to increase the maturity of cybersecurity systems. The importance of socially responsible use of artificial intelligence was emphasised to minimise potential threats and ensure the resilience of cyber systems to new challenges. The practical value of the study is to develop recommendations for

Article's History: Received: 13.08.2024; Revised: 21.11.2024; Accepted: 16.12.2024

Suggested Citation:
Zaplatynskyi, N., Lub, P., & Zaporozhtsev, S. (2024). Improving cybersecurity with artificial intelligence. *Bulletin of Cherkasy State Technological University*, 29(4), 53-61. doi: 10.62660/bcstu/4.2024.53.

*Corresponding author

the introduction of artificial intelligence into existing cybersecurity systems, which allows them to increase their resilience to new and complex cyber threats, as well as to identify potential risks and shortcomings in existing approaches to information security

Keywords: machine learning; neural networks; network traffic analysis; threat detection; automatic recognition; adaptive response

INTRODUCTION

Cybersecurity is becoming increasingly relevant in the modern digital world due to the growing complexity and frequency of cyber threats. Traditional defence methods are becoming insufficiently effective in the face of new, more sophisticated attacks, which requires the development of new approaches and technologies. Artificial intelligence (AI) technologies offer significant potential to improve cybersecurity systems by providing faster and more accurate threat detection and adaptive response to new challenges. However, despite considerable academic interest in this topic, there are still gaps in understanding the full potential of AI for cybersecurity, as well as how it can be effectively integrated into existing security systems.

Research in the field of cybersecurity using AI has been going on for several years, and many scientists have been focusing their efforts on studying various aspects of this topic. For example, the study by S.P. Samyuktha *et al*. (2022) discusses the use of AI to improve cybersecurity practices, emphasising the need to protect the huge amounts of data generated by modern technologies such as the Internet of Things and cloud computing. The authors explain that AI and machine learning technologies, such as big data analytics and deep learning, are being actively used to protect against cyber threats, including intrusion and malware detection. The article also discusses various methodologies and datasets that can be used to create effective AI-enabled cybersecurity solutions.

R. Das & R. Sandhane (2021) discuss the importance of automation to effectively manage the complexity of operations, and the scale of information used to protect cyberspace. The researcher notes that traditional technologies with fixed implementations are difficult to apply to successfully combat cyber threats, but the problem can be solved using machine learning methods. The article also assesses the modern applications of AI in cybersecurity, for edge protection and strategic decisions, and emphasises that certain cybersecurity problems can only be effectively addressed by implementing AI approaches. Artificial intelligence provides instant access to information, helping to cope with the data flow in cybersecurity, which is causing significant structural changes in the industry. The study by N.N. Abbas *et al*. (2019) visualised the hotspots, trends, and emerging applications of AI, providing businesses and governments with useful information for strategic planning. For the first time, the study offers a holistic view of the global distribution of AI research in cybersecurity, including the use of heat maps to analyse geographic areas of activity.

A.M. Shamiulla (2019) explored the impact of artificial intelligence on various areas of human life, including language processing, speech recognition, finance, and robotics. The author also examines the threats associated with the use of AI, including cybercrime and security vulnerabilities. The main focus is on the need for research to ensure control over AI and its safe use. L. Lazic (2019) explores the role of artificial intelligence in enhancing cybersecurity, in particular, the ability of machine learning to identify anomalies and improve threat detection strategies. Particular attention is devoted to obfuscation and de-obfuscation methods for Android applications, including a Low-Level Virtual Machine (LLVM) based platform to improve these processes. It also analyses the AndrODet system, which uses online training to identify the three main obfuscation methods in mobile applications.

X. Feng *et al*. (2020) analysed the role of artificial intelligence in forecasting and modelling, emphasising its importance for strategic planning in crises such as the COVID-19 pandemic. The authors highlight the cybersecurity issues that are necessary to ensure the accuracy of AI models and prevent their distortion. X. Feng *et al*. (2020)propose integrating security measures at every stage of AI development, focusing on the balance between technological, social, and political aspects. The study by A. Anandita Iyer & K.S. Umadevi (2023) analysed the impact of AI on current approaches to cybersecurity, with a focus on the speed of alert processing and filtering of critical information. The author also highlights the lack of visual interfaces for more efficient data analysis, which is an important component for improving results. The article examines the structural changes that have emerged in the field of cybersecurity due to the use of AI, as well as current trends and research in a geographical context.

The study by L. Chan *et al*. (2019) reviewed the current state of AI development in cybersecurity, presenting case studies and applied solutions to help a wider range of stakeholders, including executives, engineers, researchers, educators, innovators, entrepreneurs, and students, better understand the field. Particular attention is paid to existing problems and unresolved issues in the use of AI in cybersecurity. In addition, the paper provides practical conclusions and recommendations for businesses and government agencies on management policies in this area.

Based on the analysis of existing scientific works, it is possible to conclude that although AI technologies have significant potential for improving cybersecurity,

there are still some unresolved issues and limitations that require further study. This concerns the adaptability and reliability of AI algorithms, as well as their ability to work effectively in conditions of limited computing resources. The study aimed to identify and analyse modern approaches to the use of artificial intelligence technologies to improve cybersecurity, as well as to develop recommendations for their effective integration into existing security systems. Particular attention was devoted to the exploration of the possibilities of machine learning and deep neural networks for analysing network traffic, detecting malware, and responding adaptively to new threats. The problematic issue of the study is to determine the optimal methods of using AI to improve the effectiveness of cybersecurity, in the context of their ability to adapt to new challenges and ensure high accuracy of threat detection.

MATERIALS AND METHODS

For the analysis, scientific publications, studies and articles describing modern technologies and methods used to detect cyber threats, such as malware, abnormal behaviour in networks, zero-day attacks, etc., were used. The reviewed materials were used to compare different approaches to threat detection using machine and deep learning algorithms, as well as assess their advantages and disadvantages. The main materials used in the research include scientific articles from journals, conferences and books covering the application of machine and deep learning methods in cybersecurity, including works on algorithms such as support vector machines (SVMs), decision trees, naive Bayesian classifiers and neural networks. These algorithms are widely used to process large amounts of data in real-time, allowing for early detection of anomalies and threats. The methods and materials used in this study were used to consider in detail the potential and limitations of machine and deep learning in the field of cybersecurity. The analysis of existing approaches and methodologies contributes to a deeper understanding of how these technologies can be applied to detect and neutralise cyber threats, as well as identify their strengths and weaknesses. As the study focuses on theoretical analysis, it also provides an opportunity to assess the effectiveness of integrating machine and deep learning algorithms into existing information security systems. This was used to build an understanding of how to optimise the use of these technologies in real-world conditions, considering the limitations and needs of modern security systems, as well as to predict the directions of their further development and adaptation to new types of cyber threats.

RESULTS

In the context of cybersecurity, machine learning and deep learning are key tools for detecting and neutralising cyber threats. Comparison of these methods assessed their capabilities and limitations, which is critical for the development of effective information resource protection systems. Machine learning, as a sub-branch of artificial intelligence, is based on the use of algorithms that learn from historical data to make decisions or predictions (Fig. 1).

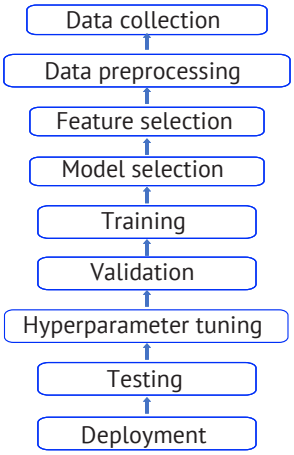

Figure 1. Machine learning algorithm
Source: compiled by the authors

In the field of cybersecurity, these methods are widely used to detect malware, analyse network traffic, and identify abnormal system behaviour (Chan *et al.*, 2019). Algorithms such as support vector machines, decision trees, naive Bayesian classifiers, and others allow efficient processing of large amounts of data with acceptable accuracy and speed. However, their effectiveness can be reduced when processing complex, non-linear dependencies that are typical of modern cyber threats. Deep learning, in turn, is a subset of machine learning that uses multi-layer neural networks to model complex patterns and relationships in data (Jain, 2021). Due to their ability to automatically extract relevant features from raw data, deep neural networks are highly effective in pattern recognition, natural language processing, and time series analysis. In the context of cybersecurity, deep learning is used to detect complex attacks, such as zero-day attacks, and analyse the behavioural characteristics of users and systems. Deep learning has been observed to outperform traditional machine learning methods in the face of large amounts of data and high pattern complexity. Due to the nonlinear nature of neural networks, deep learning can model complex relationships that may be invisible to simpler algorithms. This is relevant in cybersecurity, where threats are constantly evolving and taking on new forms (Macas *et al.*, 2022). However, deep models often require significant computational resources for training and operation, which can be a limiting factor in real-world settings.

Machine learning, despite its simplicity, has the advantages of faster learning and lower resource requirements. This makes it suitable for use in systems with limited computing capabilities or where fast, real-time data processing is required. However, these methods may

be less effective in detecting novel or complex attacks, as their performance is highly dependent on the quality and representativeness of the training data. In addition, deep learning is prone to the "black box" problem, where it is difficult to interpret how the model makes certain decisions (Sarker *et al.*, 2021). This can be critical in cybersecurity, where it is important to understand the reasons why a security system is triggered for further analysis and response. Machine learning, especially interpreted models such as decision trees or logistic regression, provides more transparent results, making them easier to interpret and more trustworthy for security professionals. The choice between machine learning and deep learning depends on the specific requirements and application. In cases where the speed and transparency of the model are important, machine learning may be more appropriate. Where complex, high-dimensional data needs to be analysed and hidden patterns discovered, deep learning offers powerful tools (Kant & Johannsen, 2022). The best approach may be to combine these methods, leveraging the strengths of each to build more effective and adaptive cybersecurity systems.

The development of models for integrating artificial intelligence algorithms with existing security systems is a key aspect of improving cybersecurity. This involves the creation of effective mechanisms that combine the capabilities of machine and deep learning algorithms with traditional security tools. The main goal is to increase the ability of systems to detect and neutralise complex and constantly evolving cyber threats. Integrating AI algorithms into existing security systems requires careful consideration of the architecture and interaction interfaces. AI algorithms must be adapted to the specific conditions and requirements of each system, considering their security protocols, standards, and policies (Mishra, 2023). This ensures smooth interaction between system components and minimises the risk of conflicts or malfunctions.

An important aspect is to ensure that AI algorithms are compatible with existing authentication, authorisation and access control mechanisms. This helps preserve data integrity and confidentiality, as well as comply with regulatory requirements and security standards, such as ISO/IEC No. 27001:2022 (2022). Models are being developed that take into account potential vulnerabilities and provide mechanisms to protect against the exploitation of algorithms by malicious actors. Optimising algorithm performance is another critical factor. AI algorithms need to efficiently process large amounts of data in real-time, which requires optimising computing resources and using high-performance computing platforms. This ensures rapid detection of threats and timely response to them, which is crucial in preventing potential security incidents. In addition, mechanisms are being developed to continuously update and train algorithms based on new threat data. This allows systems to adapt to new types of attacks and improve their effectiveness over time. The system is also scalable, enabling it to meet growing security requirements and handle increased data volumes without losing performance.

Artificial intelligence (AI) is increasingly important in cybersecurity (Trofymenko *et al.*, 2024). It opens new opportunities for detecting and neutralising cyber threats, but it also comes with certain challenges and limitations. A critical analysis of the strengths and weaknesses of AI in cybersecurity allows for a deeper understanding of the potential and risks associated with this technology. One of the main advantages of using AI in cybersecurity is its ability to process large amounts of data in real-time. Using machine learning and deep learning techniques, AI can analyse network traffic, user behavioural patterns, and system logs, identifying anomalies that may indicate the presence of cyber threats (Fig. 2). This can ensure quick response to attacks and minimisation of potential damage. In addition, AI can detect new, previously unknown threats, including zero-day attacks, which is a significant advantage over traditional signature-based security methods.

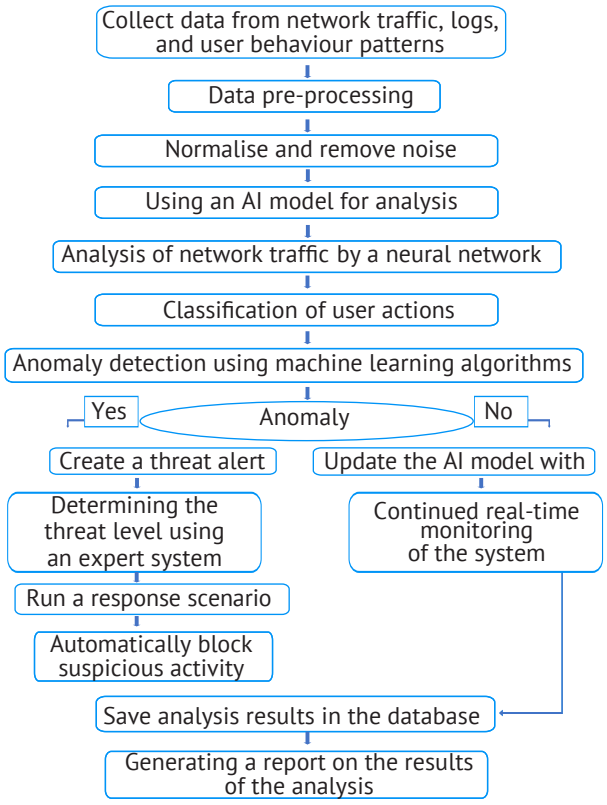

Figure 2. AI algorithm in cybersecurity
Source: compiled by the authors

Artificial intelligence also contributes to the automation of cybersecurity processes, which reduces the burden on human resources and increases the efficiency of security teams. Automated systems can continuously monitor the network, analyse threats, and even make decisions to block suspicious activity on their own (Goyal *et al.*, 2023). This is especially important in

the context of the growing complexity and frequency of cyber threats, when the human factor may not be able to keep up with the dynamics of events.

However, the use of AI in cybersecurity has its weaknesses. One of the key issues is the vulnerability of AI algorithms to attacks on the AI systems themselves. For instance, data poisoning techniques can be used by attackers to inject incorrect or manipulated data into training sets, leading to erroneous system decisions. Additionally, there are attacks based on spoofing or manipulating input data that can trick AI models into classifying malicious activity as safe. Another limitation is the problem of interpretability of AI models, especially deep neural networks. In cybersecurity, it is important not only to detect a threat but also to understand the causes and mechanisms of its occurrence to further eliminate vulnerabilities. The complexity of AI models can complicate this process, which can negatively impact the effectiveness of response and remediation. It can also create difficulties in the context of compliance with regulatory and security standards, which often require transparency and explanation of decisions.

Another important aspect is the dependence on high-quality and representative data to train AI models. If the training data does not reflect the full range of possible threats or contains biases, this can lead to poor system performance in real-world conditions (Dash *et al.*, 2022). Collecting and anonymising such data can be difficult due to privacy restrictions and legislation governing the processing of personal data. In addition, the use of AI can create a false sense of security and lead to a lack of vigilance on the part of cybersecurity professionals. Excessive trust in automated systems can lead to the missed detection of complex or atypical attacks that were not predicted by AI models (Nobles, 2024). This highlights the importance of combining automated solutions with expert human analysis. Ethical and privacy issues must also be considered. The use of AI in cybersecurity may involve the processing of large amounts of personal and confidential data, which requires compliance with strict data protection standards (ISO/IEC No. 27001:2022, 2022). Improper or unethical use of such data can lead to violations of users' rights and legal consequences for organisations.

Based on these aspects, the use of AI in cybersecurity has both significant potential and serious challenges. Maximising the benefits requires careful planning, proper design and implementation of systems, as well as continuous monitoring and improvement of models. It is important to ensure that algorithms are transparent and interpretable and that they are integrated with expert systems and human analysis. Cyber threats are becoming increasingly dynamic and complex, requiring the development of effective countermeasures. The development of theoretical scenarios can be used to model possible attacks and identify strategies to neutralise them using artificial intelligence. This involves analysing current trends in cybercrime, identifying new attack vectors, and forecasting their development.

The use of artificial intelligence in this process can be used to create models that can adapt to changing conditions. Machine learning and deep learning algorithms can analyse large amounts of data in real-time, identifying hidden patterns and anomalies that may indicate a potential threat. This is especially relevant in countering zero-day attacks that exploit unknown system vulnerabilities. One of the key aspects is modelling multi-vector attacks that combine different methods of penetration and exploitation of vulnerabilities. To do this, it is necessary to develop scenarios that consider the combined actions of attackers, including phishing, software exploits and social engineering. Artificial intelligence can help predict such complex threats by analysing the relationships between various events and compromise indicators.

It is also necessary to address the dynamics of changing tactics and techniques of cybercriminals. Continuously updating threat models using machine learning allows security systems to stay one step ahead of attackers. This includes the implementation of self-updating models that learn from new data and adjust their predictions to the current situation. In addition to technological solutions, counteraction scenarios should consider the human factor. The development of theoretical models that simulate user reactions to different types of attacks helps to identify possible vulnerabilities related to human behaviour. This may include analysing susceptibility to phishing attacks or the use of weak passwords. These aspects can be used to develop more comprehensive security strategies that combine technical tools with staff training.

DISCUSSION

The results of this study are consistent with the findings of other cybersecurity and artificial intelligence (AI) scholars, emphasising the importance of integrating modern technologies to improve the effectiveness of information resource protection systems. M.M. Yamin *et al.* (2021) analysed the use of AI as a weapon in cyber-attacks, demonstrating how AI can be used to create more sophisticated and complex threats. This underscores the need for continuous improvement of defence systems capable of withstanding new types of attacks that use AI to bypass traditional defence methods.

W.S. Admass *et al.* (2024) examined the current state of cybersecurity, identifying the main challenges and promising areas of development. The authors emphasised the need to integrate AI to provide adaptive defences in response to dynamic threats, which is in line with the findings of this study on the importance of using AI to automate risk assessment and incident response processes, increasing the efficiency and effectiveness of cybersecurity systems. N. Kaloudi & J. Li (2020) provide a comprehensive overview of the AI-driven cyber threat landscape, highlighting the

diversity and complexity of modern attacks. They note that AI can be used for both defence and attack, requiring defenders to adopt the latest techniques and technologies. This is consistent with the findings that defence systems need to be constantly evolving and adapting to new challenges.

R. Walters & M. Novak (2021) examine the interplay between cybersecurity, AI, data protection, and law. They emphasise the importance of compliance with legal norms and standards when using AI in cybersecurity, which is an important aspect of this study, which focuses on the socially responsible use of AI to minimise potential risks and ensure user confidence in security systems. M. Binhammad *et al*. (2024) explored the role of AI in digital identity protection, highlighting the potential of machine learning to detect and prevent fraudulent activity. They demonstrate how AI can be used to ensure the security of personal data and prevent identity theft, which correlates with the conclusion that AI needs to be integrated with human expertise to ensure comprehensive security.

S.K. Shandilya *et al*. (2022) developed an AI-supported test platform for adaptive defence inspired by natural processes. The results show that the use of AI in cybersecurity simulations can significantly improve the ability of systems to adapt and self-learn, supporting the study's recommendations to combine automated methods with expert human expertise to create more resilient defence systems. A. Ali *et al*. (2022) consider the use of AI as a horizon event in cybersecurity, analysing how AI can transform threat prediction and protection. They emphasise the potential of AI to create proactive defence systems that anticipate and respond to threats before they occur. This is in line with the conclusion that it is necessary to develop models capable of predicting and adapting to new threats. M. Tetaly & P. Kulkarni (2022) discuss whether AI is a threat or a cybersecurity solution, noting that while AI can significantly improve the effectiveness of defence systems, there are risks of misuse, which require careful regulation and ethical standards. This underscores the importance of the ethical use of AI, which is also considered in this study, which focuses on the socially responsible use of AI to minimise potential risks and ensure user confidence in security systems. S.A. Jawaid (2023) analyses the relationship between AI and cybersecurity, considering how AI can improve security methods and create new types of threats. The author emphasises the need to balance the use of AI for protection with the management of its potential risks, which correlates with the study's recommendations for a comprehensive approach to the use of AI in cybersecurity.

M.H.B.A. Alkareem *et al*. (2023) investigated the linguistic aspects of crime in the world with the help of AI-enabled cybersecurity. They show how AI can be used to analyse language patterns in criminal communications, which helps to detect and predict criminal activity. This underscores the importance of using AI in integrated security systems, where it is important to consider various aspects of cybersecurity, including technical, social, and linguistic. J. Ebenezer Taiwo Akinsola *et al*. (2022) consider the use of AI in the design of user interfaces for modelling cybersecurity threats. They demonstrate how AI can be used to create intuitive and adaptive interfaces that improve user interaction with security systems and contribute to the overall effectiveness of cybersecurity. A. Lakhani (2024) analyses the revolutionary impact of AI on cybersecurity, opening the future of digital defence. The author emphasises that AI can significantly improve the ability of systems to detect and respond to threats but also requires continuous improvement and adaptation to new challenges. This correlates with the conclusion that AI technologies in cybersecurity need to be continuously developed and adapted.

D. Aggarwal *et al*. (2023) examine the role of AI in cybersecurity through anomaly and predictive analysis. They demonstrate how machine learning techniques can be used to detect anomalies in network data and predict potential threats, allowing defence systems to be proactive and effective. This highlights the importance of using AI to predict and prevent threats, which is a key aspect of the research. However, despite significant progress, there are serious challenges, such as model interpretability, resource optimisation, and ethical aspects of AI use. This requires a comprehensive approach to the development and implementation of AI technologies in cybersecurity, where it is important not only to improve technical aspects but also to consider social and ethical factors.

Integrating AI with other security and analytical methods, as well as using AI to analyse different types of data, can significantly improve the ability of systems to detect and respond to complex and emerging threats. This underscores the importance of a multidisciplinary approach to cybersecurity, where AI acts as a powerful tool in the complex of measures to protect information systems. Further theoretical and practical research should be aimed at developing more effective, adaptive and interpretable protection models, as well as at integrating human expertise with automated protection systems. Thus, the study results confirm the importance of using modern AI methods to improve cybersecurity systems. The joint efforts of scientists, engineers, and cybersecurity professionals will help create a safer and more resilient digital environment that can effectively counter current and future cyber threats.

CONCLUSIONS

The study determined that the use of artificial intelligence methods, in particular machine and deep learning, significantly improves the efficiency of cybersecurity systems. An analysis of existing approaches has shown that deep neural networks are able to detect complex patterns and anomalies that are typical of modern cyber threats, providing a high level of

accuracy and speed of response. Auto-encoders and recurrent neural networks proved to be particularly effective, demonstrating the ability to self-learn and adapt to new types of attacks, which confirms their suitability for dynamic cybersecurity environments.

Research has also shown that generative adversarial networks (GANs) can be effectively used to create realistic attack patterns, allowing defence systems to better prepare for previously unknown threats. This confirms the need to integrate advanced artificial intelligence techniques to increase the adaptability and proactivity of cybersecurity systems. However, the study determined that deep models often require significant computing resources, which can limit their use in resource-limited environments. Critical analysis has shown that the interpretability of deep learning models remains a significant challenge. Despite their high accuracy in detecting threats, the difficulty of understanding the models' decision-making mechanisms poses risks to the trust of security professionals. This underscores the need to develop explainable artificial intelligence methods that would increase transparency and trust in automated security systems.

The analysis of the study results demonstrated that the use of artificial intelligence technologies in cybersecurity has significant potential to improve the efficiency of security systems. However, an important aspect is the optimisation of the resource consumption of artificial intelligence algorithms, which is critical for their effective use in real-world conditions. The study found that modern machine learning methods, including neural networks, can significantly improve the accuracy of detecting complex and emerging cyber threats. However, for their effective implementation, it is necessary to address the resources used to train and apply these algorithms, as high computing requirements may be a limitation in practical use. This highlights the need for further research and development of more efficient, less resource-intensive approaches to integrate AI into cybersecurity systems.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Abbas, N.N., Ahmed, T., Shah, S.H.U., Omar, M., & Park, H.W. (2019). Investigating the applications of artificial intelligence in cyber security. *Scientometrics*, 121(2), 1189-1211. doi: 10.1007/s11192-019-03222-9.

[2] Admass, W.S., Munaye, Y.Y., & Diro, A.A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2, article number 100031. doi: 10.1016/j.csa.2023.100031.

[3] Aggarwal, D., Sharma, D., & Saxena, A.B. (2023). Role of AI in cyber security through anomaly detection and predictive analysis. *Journal of Informatics Education and Research*, 3(2), 1846-1849. doi: 10.52783/jier.v3i2.314.

[4] Ali, A., Septyanto, A.W., Chaudhary, I., Hamadi, H.A., Alzoubi, H.M., & Khan, Z.F. (2022). Applied artificial intelligence as event horizon of cyber security. In *2022 international conference on business analytics for technology and security* (pp. 1-7). Dubai: IEEE. doi: 10.1109/icbats54253.2022.9759076.

[5] Alkareem, M.H.B.A., Nasif, F.Q., Ahmed, S.R., Miran, L.D., Algburi, S., & ALmashhadany, M.T. (2023). Linguistics for crimes in the world by AI-based cyber security. In *2023 7th international symposium on innovative approaches in smart technologies* (pp. 1-5). Istanbul: IEEE. doi: 10.1109/isas60782.2023.10391610.

[6] Anandita Iyer, A., & Umadevi, K.S. (2023). Role of AI and its impact on the development of cyber security applications. In V. Sarveshwaran, J.I.-Z. Chen & D. Pelusi (Eds.), *Artificial intelligence and cyber security in industry 4.0* (pp. 23-46). Singapore: Springer. doi: 10.1007/978-981-99-2115-7_2.

[7] Binhammad, M., Alqaydi, S., Othman, A., & Abuljadayel, L.H. (2024). The role of AI in cyber security: Safeguarding digital identity. *Journal of Information Security*, 15(2), 245-278. doi: 10.4236/jis.2024.152015.

[8] Chan, L., Morgan, I., Simon, H., Alshabana, F., Ober, D., Gentry, J., Min, D., & Cao, R. (2019). Survey of AI in cybersecurity for information technology management. In *2019 IEEE technology & engineering management conference* (pp. 1-8). Atlanta: IEEE. doi: 10.1109/temscon.2019.8813605.

[9] Das, R., & Sandhane, R. (2021). Artificial intelligence in cyber security. *Journal of Physics Conference Series*, 1964(4), article number 042072. doi: 10.1088/1742-6596/1964/4/042072.

[10] Dash, B., Ansari, M.F., Sharma, P., & Ali, A. (2022). Threats and opportunities with AI-based cyber security intrusion detection: A review. *International Journal of Software Engineering & Applications*, 13(5), 13-21. doi: 10.5121/ijsea.2022.13502.

[11] Ebenezer Taiwo Akinsola, J., Akinseinde, S., Kalesanwo, O., Adeagbo, M., Oladapo, K., Awoseyi, A., & Kasali, F. (2022). Application of artificial intelligence in user interfaces design for cyber security threat modeling. In *Software usability*. London: IntechOpen. doi: 10.5772/intechopen.96534.

[12] Feng, X., Feng, Y., & Dawam, E.S. (2020). Artificial intelligence cyber security strategy. In *2020 IEEE intl conf on dependable, autonomic and secure computing, intl conf on pervasive intelligence and computing, intl conf on cloud and big data computing, intl conf on cyber science and technology congress* (pp. 328-333). Calgary: IEEE. doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00064.

[13] Goyal, S.B., Rajawat, A.S., Solanki, R.K., Majmi Zaaba, M.A., & Long, Z.A. (2023). Integrating AI with cyber security for smart Industry 4.0 application. In *2023 international conference on inventive computation technologies* (pp. 1223-1232). Lalitpur: IEEE. doi: 10.1109/icict57646.2023.10134374.
[14] International Standard (ISO/IEC) No. 27001:2022 "Information Security, Cybersecurity and Privacy Protection". (2022, October). Retrieved from https://www.iso.org/standard/82875.html.
[15] Jain, J. (2021). Artificial intelligence in the cyber security environment. In *Artificial intelligence and data mining approaches in security frameworks* (pp. 101-117). Hoboken: Wiley. doi: 10.1002/9781119760429.ch6.
[16] Jawaid, S.A. (2023). Artificial intelligence with respect to cyber security. *Journal of Advances in Artificial Intelligence*, 1(2), 96-102. doi: 10.18178/jaai.2023.1.2.96-102.
[17] Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape: A survey. *ACM Computing Surveys*, 53(1), article number 20. doi: 10.1145/3372823.
[18] Kant, D., & Johannsen, A. (2022). Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs). *Electronic Imaging*, 34, article number MOBMU-387. doi: 10.2352/ei.2022.34.3.mobmu-387.
[19] Lakhani, A. (2024). *How AI is revolutionizing cybersecurity: Unlocking the future of digital protection*. Retrieved from https://cloud-computing.tmcnet.com/features/articles/459618-how-ai-revolutionizing-cybersecurity-unlocking-future-digital-protection.htm.
[20] Lazic, L. (2019). Benefit from AI in cybersecurity. In *11th international conference on business information security*. Belgrade: Belgrade Metropolitan University.
[21] Macas, M., Wu, C., & Fuertes, W. (2022). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. *Computer Networks*, 212, article number 109032. doi: 10.1016/j.comnet.2022.109032.
[22] Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences*, 13(10), article number 5875. doi: 10.3390/app13105875.
[23] Nobles, C. (2024). The weaponization of artificial intelligence in cybersecurity: A systematic review. *Procedia Computer Science*, 239, 547-555. doi: 10.1016/j.procs.2024.06.206.
[24] Samyuktha, S.P., Kavitha, P., Kshaya, V.A., Shalini, P., & Ramya, R. (2022). A survey on cyber security meets artificial intelligence: AI-driven cyber security. *Journal of Cognitive Human-Computer Interaction*, 2(2), 50-55. doi: 10.54216/JCHCI.020202.
[25] Sarker, I.H., Furhad, M.H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science*, 2(3), article number 173. doi: 10.1007/s42979-021-00557-0.
[26] Shamiulla, A.M. (2019). Role of artificial intelligence in cyber security. *International Journal of Innovative Technology and Exploring Engineering*, 9(1), 4628-4630. doi: 10.35940/ijitee.a6115.119119.
[27] Shandilya, S.K., Upadhyay, S., Kumar, A., & Nagar, A.K. (2022). AI-assisted computer network operations testbed for nature-inspired cyber security based adaptive defense simulation and analysis. *Future Generation Computer Systems*, 127, 297-308. doi: 10.1016/j.future.2021.09.018.
[28] Tetaly, M., & Kulkarni, P. (2022). Artificial intelligence in cyber security – a threat or a solution. *AIP Conference Proceedings*, 2519(1), article number 030036. doi: 10.1063/5.0109664.
[29] Trofymenko, O., Sokolov, A., Chykunov, P., Akhmametieva, H., & Manakov, S. (2024). AI in the military cyber domain. *Technologies and Engineering*, 25(4), 85-92. doi: 10.30857/2786-5371.2024.4.8.
[30] Walters, R., & Novak, M. (2021). *Cyber security, artificial intelligence, data protection & the law*. Singapore: Springer. doi: 10.1007/978-981-16-1665-5.
[31] Yamin, M.M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber attacks. *Journal of Information Security and Applications*, 57, article number 102722. doi: 10.1016/j.jisa.2020.102722.

Вдосконалення кібербезпеки за допомогою штучного інтелекту

Назар Заплатинський

Магістр
Львівський національний університет природокористування
80831, вул. Володимира Великого, 1, м. Дубляни, Україна
https://orcid.org/0009-0002-7767-8795

Павло Луб

Кандидат технічних наук, доцент
Львівський національний університет природокористування
80831, вул. Володимира Великого, 1, м. Дубляни, Україна
https://orcid.org/0000-0001-9600-0969

Сергій Запорожцев

Кандидат технічних наук, доцент
Львівський національний університет біоресурсів і природокористування
80831, вул. Володимира Великого, 1, м. Дубляни, Україна
https://orcid.org/0000-0002-8250-2834

Анотація. Метою дослідження було вивчення можливостей застосування штучного інтелекту для вдосконалення систем кібербезпеки в умовах зростання складності та частоти кіберзагроз. Особлива увага приділялася аналізу ефективності інтеграції методів машинного та глибинного навчання в процеси виявлення, оцінки та нейтралізації загроз, а також визначенню сильних та слабких сторін таких підходів. Дослідження було спрямоване на обґрунтування необхідності поєднання технологічних можливостей штучного інтелекту з експертним людським досвідом для забезпечення комплексного та адаптивного захисту інформаційних систем. У дослідженні розглядалися потенційні можливості застосування штучного інтелекту для вдосконалення систем кібербезпеки, враховуючи зростаючі загрози та складність сучасних кіберзлочинів. Аналізувався вплив технологій машинного навчання та глибинного навчання на підвищення ефективності традиційних методів захисту інформаційних систем. Відзначалося, що незважаючи на незмінність основних мотивів кіберзлочинців, їхні методи ставали дедалі витонченішими, що вимагало від захисників нових підходів до виявлення та нейтралізації загроз. Використання штучного інтелекту розглядалося як один з найперспективніших напрямків розвитку кібербезпеки, оскільки це дозволяє автоматизувати процеси оцінки ризиків та реагування на інциденти, знижуючи час реагування та підвищуючи загальну ефективність захисту. Особлива увага приділялася аналізу сильних і слабких сторін штучного інтелекту в контексті кібербезпеки. Обґрунтовувалася необхідність інтеграції штучного інтелекту з людською інтуїцією та досвідом, оскільки поєднання цих компонентів виявилося найефективнішим підходом для забезпечення комплексної безпеки. Окрім того, досліджувалися потенційні ризики та занепокоєння, пов'язані з використанням штучного інтелекту в кібербезпеці. Було зроблено висновок, що для підвищення зрілості систем кібербезпеки необхідний цілісний підхід, який враховує як технічні, так і соціальні аспекти. Наголошувалося на важливості соціально відповідального використання штучного інтелекту, щоб мінімізувати потенційні загрози та забезпечити стійкість кіберсистем до нових викликів. Практична цінність дослідження полягає в розробці рекомендацій щодо впровадження штучного інтелекту в існуючі системи кібербезпеки, що дозволяє підвищити їх стійкість до нових та складних кіберзагроз, а також виявляти потенційні ризики та недоліки в існуючих підходах до забезпечення інформаційної безпеки

Ключові слова: машинне навчання; нейронні мережі; аналіз мережевого трафіку; виявлення загроз; автоматичне розпізнавання; адаптивне реагування