The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.16

Artificial intelligence in the sphere of cybersecurity: innovations, challenges, and development prospects

Roman Pantiushenko
Leading Researcher of the Research and Testing Section
Central Research Institute of the Armed Forces of Ukraine
03049, Povitroflotskyi Ave., 28 B, Kyiv, Ukraine
e-mail: prvm79@gmail.com
ORCID: 0000-0002-9301-9389

Yuliia Chaika
Head of Research Section
Central Research Institute of the Armed Forces of Ukraine
03049, Povitroflotskyi Ave., 28 B, Kyiv, Ukraine
e-mail: jul.seagull@gmail.com
ORCID: 0009-0002-4342-3313

Abstract. The relevance of the study is due to the need for effective protection of information systems in the face of ever-growing cyber threats. In the modern digital world, where cyberattacks are becoming increasingly complex and widespread, the use of artificial intelligence in cybersecurity is extremely relevant. The problem of cybersecurity is becoming increasingly important and conducting relevant research is becoming a necessary aspect of ensuring security in the digital space.

In this context, we propose an article that examines the role of artificial intelligence, innovations, challenges, and prospects of its development in the sphere of cybersecurity. Additionally, it explores the utilization of artificial intelligence for automating processes of detecting, analysing, and responding to cyber threats, and its practical significance for enhancing security levels in the digital space and the effectiveness of cyber threat protection.

The main approaches for this study are trend analysis and expert assessments, which allow for a comprehensive review of the directions of artificial intelligence development in the field of cybersecurity, the benefits and challenges of its implementation, as well as potential opportunities and threats to information security.

The article discusses advanced security information and event management systems designed to collect, analyse and respond to cyber threats and other systems aimed at specific aspects of protection and expanding automation capabilities to improve the security level of information systems.

The materials of the article are of theoretical value for further scientific research on the use of artificial intelligence in the sphere of cybersecurity and reflect important features of its influence on this area. This research can contribute not only to deepening the understanding of the theoretical aspects of the use of artificial intelligence in cybersecurity but also to identifying specific practical applications and innovations that will help improve protection against cyber threats in the future.

Keywords: artificial intelligence, cyberspace, big data, Security Information and Event Management.

Introduction

The rapid and unrestrained development of digital technologies has led to cybersecurity becoming one of our time's most pressing and urgent issues (Hryshchuk, Zhovnovatiuk, Nosova,

2019). In a world where cybercrime is spreading faster than ever (Kogut, 2022), protecting against cyberattacks is a priority for all organisations and individuals operating in cyberspace. In this context, artificial intelligence (AI) is becoming increasingly important and relevant (Onyshchenko, Kalancha, Geldt, 2023) as a tool for detecting, countering and preventing cyber threats.

This article discusses the role and benefits of using AI in cybersecurity (Gurzhiy, 2023) and the challenges and prospects for further development.

Focusing on innovative methods and technologies, the research was conducted on the impact of AI on the efficiency and reliability of cybersecurity and the possibilities for further improvement (Ustymenko, Olishevskyi, 2022) in this area to ensure security in the digital space were considered.

Methodological Framework

The study examined Security Information and Event Management (SIEM) systems intended to collect, analyse and respond to cyber threats (Yushko and Shevchuk, 2020). These technologies provide real-time monitoring and analysis of events occurring in networks and other components of information systems. The obtained data was used to identify the main trends, challenges, and prospects for the development of AI in cybersecurity.

Modern SIEM systems are actively using AI to improve the efficiency of cyber threat detection. The use of AI helps to automate the collection, and analysis of big data (BD) and detection of anomalies, significantly increasing the efficiency of responding to potential threats. The AI-based approach allows us to effectively identify unusual patterns in system and user behaviour that may indicate potential threats.

Consequently, the use of AI in SIEM systems helps to increase the efficiency and speed of cyber threat detection, as well as reduce incident response time, which in turn increases the overall level of cybersecurity.

Results and Discussions

In the modern world, where cyber threats are becoming increasingly complex and sophisticated, the use of AI in the sphere of cybersecurity is extremely important and necessary. Innovative methods and technologies based on the use of AI play a key role in the continuous improvement of cyber security.

AI is widely used in cybersecurity to automate the process of detecting and analysing potential cyber threats, analysing information from event logs, detecting anomalies in user behaviour, recognising new and unknown threats, and developing predictive models to help predict possible attacks. According to research, the use of AI in cybersecurity can reduce the time for detection and recovery from an incident by up to 25% and reduce the number of false alarms by up to 50%. These capabilities can significantly improve the efficiency and speed of response to cyber threats, ensuring a higher level of security in the digital space.

An example of the use of AI in cybersecurity can be SIEM systems that integrate it into their structure to automate the analysis of BD and identify potential threats and anomalies in the network, ensuring effective response to cyber incidents and reducing response time.

A SIEM system is a comprehensive information and analytical infrastructure that combines software and hardware, network solutions, management methods and processes aimed at ensuring the security of information systems and is designed to collect, analyse, detect and respond to security events that occur in computer systems, networks and software applications.

SIEM systems widely use AI to solve cybersecurity management tasks, including detecting, analysing and responding to cyber threats. This helps to reduce false alarms and increase the effectiveness of information system protection in the current environment of ever-growing cyber threats.

As a result of the research conducted by the world's leading research and consulting company

Gartner, Inc., the Magic Quadrant for SIEM systems was created, which is the result of an analysis of the information technology security market. This quadrant (Figure 1) provides an objective view of the leaders in this field (Inci, 2023) and helps to select the best technological solutions.

Figure 1. The magic quadrant for SIEM

Based on this, a number of leading companies in this area are identified that should be considered when choosing SIEM systems, namely:

1. Splunk Enterprise Security
2. IBM Security QRadar
3. LogRhythm
4. Securonix
5. Micro Focus ArcSight
6. RSA NetWitness Platform
7. Exabeam
8. Elastic
9. SolarWinds Security Event Manager
10. AT&T Cybersecurity (AlienVault)

Figure 2 shows the interface of the IBM Security QRadar SIEM system, which includes an intuitive user interface for monitoring and analysing security events.

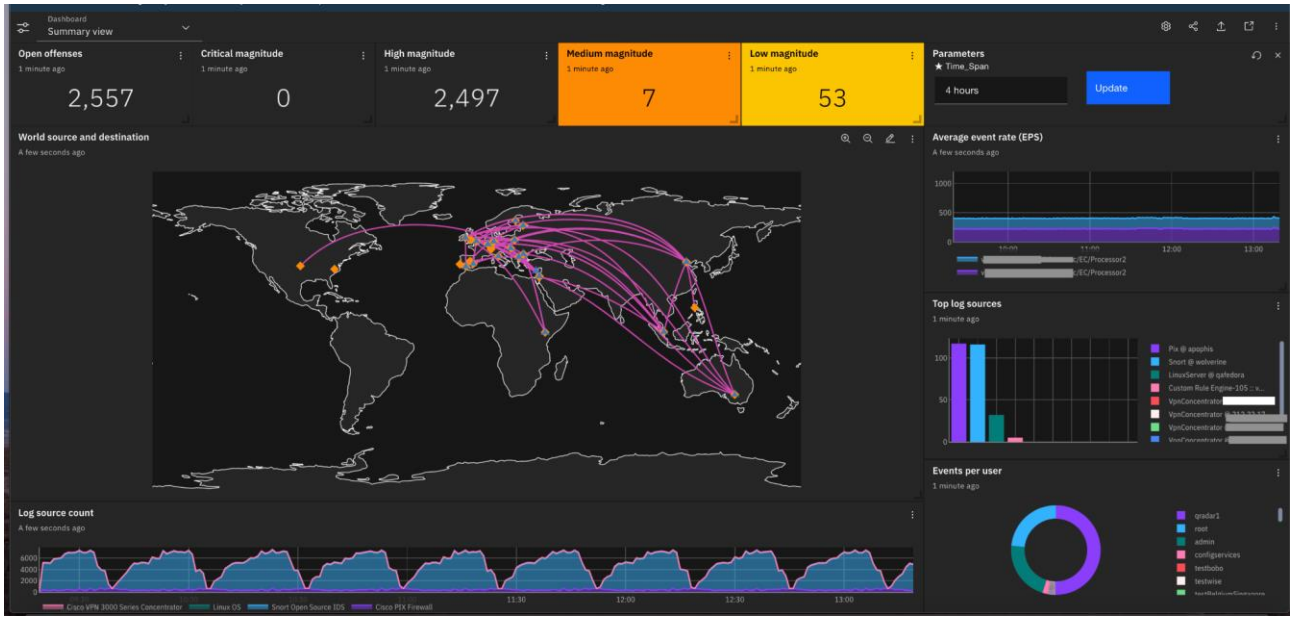

Figure 2. Interface of the IBM Security QRadar SIEM system

This interface provides operators with the ability to monitor data flows, detect anomalous activity, analyse vulnerabilities, and respond to potential threats in real-time. In addition, it can display reports and statistics on security measures, helping administrators make informed decisions about measures to improve the security of the information infrastructure.

Figure 3 shows the current and projected spending on SIEM systems by companies worldwide, illustrating the stable trend of increasing financial investments in this segment of cybersecurity, as well as the constant demand for such technological solutions.

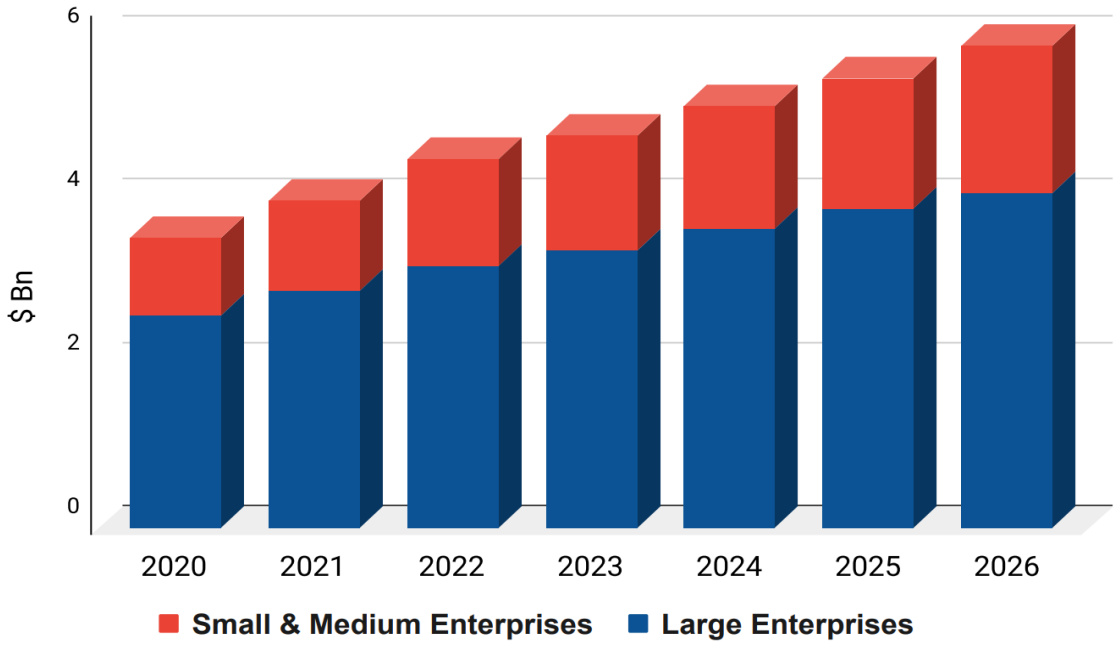

Figure 3. Existing and projected enterprise spending on SIEM from 2020 to 2026

Beyond these SIEM systems, there are other important cybersecurity tools that extend this approach to protection and use AI to improve the security of information systems. Their main difference is a focus on specific aspects of protection and advanced automation capabilities to improve the security of information systems. Among them are:

Security Orchestration, Automation, and Response (SOAR). This is a system that combines coordination, automation and response to events in the sphere of cybersecurity, which helps to increase the efficiency of threat response and optimise security processes.

Endpoint Detection and Response (EDR). This is a security system aimed at detecting and responding to threats at the level of endpoints in the network, such as computers, laptops, servers and other devices, by detecting and analysing anomalous activity.

User and Entity Behaviour Analytics (UEBA). This is a system used to analyse the behaviour of users and entities in information systems to detect anomalies in their activity to identify potential cyber threats.

These systems complement SIEM capabilities by expanding the range of tools for detecting, analysing and responding to cyber threats in various aspects of information security. They extend security management capabilities by providing additional functionality such as detecting anomalous network activity, automating routine processes, and using AI to detect complex threats. This combination of tools creates an effective and advanced security architecture that provides a high level of protection against cyberattacks in the modern cyberspace.

Having considered these systems, we can conclude that the use of AI is widely used and is a necessary component of modern technological solutions in the sphere of cybersecurity.

Despite the advantages of using AI in cybersecurity, its development is accompanied by a number of challenges and difficulties that we may potentially face in this area. Let us consider some of them.

Lack of accuracy can lead to underestimation or overestimation of threats, as well as an increase in false alarms, which affects the work of analysts and threatens the effectiveness of the system.

Uncertainty in threat behaviour makes it difficult to detect and counter cybercriminals, who are constantly developing new methods and techniques to circumvent defences.

The lack of access to relevant data can complicate training and reduce its effectiveness, while the increasing use of AI may lead to system dependence on its operation, thereby increasing their vulnerability to attacks.

Ethical and privacy issues, in particular in relation to the collection and processing of users' personal data, also need to be addressed and resolved.

When considering the role of AI in cybersecurity, it is important to note that it plays a dual role in the future of the industry. On the one hand, it undoubtedly contributes to the improvement of defence systems by providing more effective detection and prevention of attacks. On the other hand, the growing number of attacks using AI and issues related to confidentiality also pose serious challenges for cybersecurity. In this regard, all these aspects require careful analysis and development of appropriate strategies to address them in order to ensure effective and reliable security in cyberspace.

The prospects for development in the sphere of cybersecurity using AI are promising. With the development of technology and continuous improvement of its level, we can expect further development of more accurate and faster methods of detecting cyber threats, which will help increase the effectiveness of security systems.

One of the main prospects is the development of autonomous intelligent protection systems that can adapt to new types of threats and attacks without direct intervention from operators. Such systems will be able to respond faster and more effectively to changes in cyberspace and prevent

potential attacks.

Another perspective is to increase the integration of AI with other cybersecurity technologies, such as quantum computing and blockchain. This will create more comprehensive and reliable security systems that can effectively respond to current and future cybersecurity challenges.

In addition, the development of cybersecurity standards and regulations is an important prospect, which will stimulate innovation and ensure a high level of security in the Internet of Things (IoT), cloud services and other modern technological spheres.

The introduction of AI into the activities of the Armed Forces of Ukraine opens up prospects for increasing their readiness and efficiency in modern military conflicts. This innovative technology makes it possible to optimise the planning and conduct of military operations, ensuring the accuracy in making relevant decisions and instant response to sudden changes in the operational situation. Also, the use of AI contributes to strengthening the cybersecurity of the Armed Forces of Ukraine, protecting their critical information resources from cyberattacks and ensuring the stability of military communication systems. In addition, efficiency can be increased through the use of AI of cyber exercises and simulations to prepare the military for various crisis situations and cyber threats. Thus, the use of AI in the Armed Forces of Ukraine has the potential to increase their readiness and effectiveness in the modern military environment.

All in all, AI has the potential to transform the way we approach cybersecurity, providing more adaptive, intelligent and effective defence systems that can cope with the growing threats in the digital world.

Conclusion

The development of AI in the sphere of cybersecurity opens up significant potential for increasing the effectiveness of information protection in both the civilian and military sectors. Through the application of AI, cyber threats can be detected, analysed, and responded more quickly and effectively, ensuring a high level of protection against modern cyber attacks. The integration of AI into cybersecurity also increases the security and ability to respond to the challenges of the modern digital environment.

Therefore, the integration of AI in the sphere of cybersecurity opens up new opportunities to provide effective and comprehensive protection against cyber threats in the modern digital world, which is becoming a key factor in ensuring cybersecurity in the future.

Recommendations

Further research should be focused on enhancing the effectiveness of AI into cybersecurity for accurate detection and analysing of cyber threats, development of adaptive security systems, and exploration of forecasting capabilities for future threats and the development of prevention strategies.

Acknowledgments

The authors declare that they have no competing interests in the subject matter of the article.

References

1. Hryshchuk, R., Zhovnovatiuk, R., & Nosova, H. (2019). Hybrid threats in cyberspace: factors influencing the nature of emergence. *Modern Information Technologies in the Sphere of Security and Defence, 36(3)*, 53–58.
2. Kohut, Y. I. (2022). *Cyberwarfare, cyberterrorism, cybercrime (concepts, strategies, technologies)*. Sidcon Consulting Company.
3. Barabash, O. V., Hryshchuk, R. V., Molodetska-Grynchuk, K. V., & Molodetska-Grynchuk, K. V. (2018). *Identification of threats to the information security of the state in the content of*

textual content of social Internet services.
4. Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). The role of artificial intelligence in cyber security. In *Countering cyber attacks and preserving the integrity and availability of critical systems* (pp. 170-192). IGI Global.
5. Onishchenko, Y. M., Kalancha, A. A., & Geldt, S. V. (2023). Application of artificial intelligence in the field of cybersecurity. In *The 8th International scientific and practical conference "Trends, theories and ways of improving science" (February 28–March 03, 2023) Madrid, Spain. International Science Group. 2023*. 565 p. (p. 544).
6. Gurzhiy, S. (2023). Features of the use of artificial intelligence in cybersecurity issues. *Information and Law*, 4 (47), 207–216.
7. Golubenko, O. I., Lemeshko, A. V., Polischuk, A. R., Kuzmenko, M. V. & Degtyarev, E. O. (2023). Research of the application of artificial intelligence in cybersecurity. *ITSynergy, (2)*, 71–81.
8. Ustymenko, V. O., & Olishevskyi, I. G. (2022). *Prospects for the application of artificial intelligence technologies in the field of cybersecurity*.
9. Opirskyi, I., Susukailo, V., & Vasylyshyn, S. (2023). Investigation of the possibilities of using artificial intelligence chatbots for the study of event logs. *Information Protection*, 24(4), 177–183.
10. Soldatova, M. O., Vityuk, A. E., Martyniuk, A. S., & Chernoborodyuk, V. D. (2022). In *The 9th International scientific and practical conference "Innovations and prospects of world science"* (April 28-30, 2022) Perfect Publishing, Vancouver, Canada. *2022*. April. P. 256.
11. Inci, S. (2023). The Best 10 SIEM Tools for 2023. *Medium*. 5 May. https://medium.com/@sedatinci1001/the-most-popular-10-siem-tools-b36f86d9fc7a
12. Yushko, A. V., & Shevchuk, R. P. (2020). *Analysis of information security event management systems*.