EMERGING TECHNOLOGIES AND INNOVATIONS IN CYBERSECURITY

CYBER FRAUD AND ARTIFICIAL INTELLIGENCE

UDC: [004.056.5+004.8]:[343.72:004.6](477)
DOI: https://doi.org/10.53486/tids2025.01

LUDMILA RYBALCHENKO
Ph.D, Associate Professor
Department of Cyber Security and Information Technologies
University of Customs and Finance
Dnipro, Ukraine
luda_r@ukr.net
ORCID ID: 0000-0003-0413-8296

Abstract. The role of artificial intelligence in the life of every citizen is becoming even more important in the modern world, especially with the ever-increasing number of cyberattacks. In various spheres of life, attention is focused on the application of effective methods to ensure effective protection against cyber fraudsters. The variety of methods used by cybercriminals is growing, which makes them more difficult to detect. Decision-making to ensure the protection of personal data is based on compliance with regulatory requirements and standards in the field of information security.

The development of innovative technologies in the field of cybersecurity also affects the use of new, unusual methods of attacks used by cybercriminals. Therefore, it is important to use the latest technologies to create and ensure information security at all levels of citizens' life. The latest technologies and artificial intelligence are used to protect the modern digital environment from cybersecurity. Artificial intelligence in the field of cybersecurity plays an important role in identifying risks and protecting confidential information.

Initially, artificial intelligence was used to monitor network traffic for suspicious activity. Subsequently, it was the application of deep learning algorithms that made it possible to effectively detect active threats to ensure reliable cybersecurity.

The purpose of this paper is to study the current state of cybersecurity in Ukraine and to identify the features associated with the use of effective mechanisms to combat cyber fraud using artificial intelligence. The use of artificial intelligence in the field of cybersecurity opens up new opportunities for detecting, predicting and preventing cyber threats.

Keywords: cyber fraudsters, artificial intelligence, information security, digital environment, innovative technologies.

JEL Classification: H56, D80.

INTRODUCTION

Cybersecurity is one of the most important issues affecting the security of the modern digital environment. The number of cyber threats and their complexity are constantly growing, so effective methods and approaches to protecting information systems must be more reliable and efficient. Cybersecurity incidents involving the theft of personal data, banking secrets, and various types of cyberattacks, including attacks on critical infrastructure, pose a threat to economic stability and national security.

The use of artificial intelligence (AI) to ensure cybersecurity and protect against cyber fraud is a promising area in the modern information environment. AI technologies offer special opportunities for cyber defence.

Identifying potential threats, responding to cyber incidents, detecting malware, assessing system vulnerabilities, and predicting potential cyber attacks is possible with the use of artificial intelligence.

The introduction of digital technologies has caused a number of risks that lead to a high level of cyber threats. The pervasiveness of risks in all areas of activity threatens the normal operation of businesses, entrepreneurial activities, and government organisations. Modern cyber threats are constantly changing, making them harder to detect.

Global cyberattacks exploit software vulnerabilities, data leaks, and hackers create various cases of cybercrime that cause large financial losses for industrial enterprises and institutions. To stay a few steps ahead of fraudsters, it is necessary to apply reliable cybersecurity measures, innovative technologies to protect confidential data and prevent financial consequences from cyber fraud.

MAIN CONTENT

Malicious attacks are becoming a serious threat, so the use of artificial intelligence methods to ensure cybersecurity of organisations and enterprises is a promising area of research. AI systems based on machine learning algorithms and linguistic neural networks are widely used to protect data in modern tools [2]. One of the main areas of application of artificial intelligence is the detection of unauthorised research of an information resource. Systems automatically detect malicious code or unusual Internet traffic and respond to unusual user behaviour.

Machine learning algorithms help filter spam messages and use email filters to reduce phishing emails. Alerting employees to suspicious email activity helps reduce the risk of receiving and opening unwanted fraudulent messages. Therefore, the use of artificial intelligence is effective in combating cyber threats and ensures a high level of security in the digital environment.

The introduction of artificial intelligence in cybersecurity allows for the improvement of models designed to detect, identify, eliminate and mitigate potential threats and hazards in businesses and organisations. Artificial intelligence is able to recognise patterns that humans may not be able to detect. Detecting threats through malware, malicious attacks, analysing large amounts of data and unwanted activity, preventing possible threats, blocking malicious threats, and more, all of this is done through artificial intelligence. It is important and relevant to increase the level of prediction of future events using artificial intelligence and the effectiveness of regulatory compliance to increase the fight against cyber threats.

With the development of information technology and the use of artificial intelligence to create reliable cybersecurity tools, it is important to remember that cybercriminals can also use artificial intelligence to commit crimes and cyber threats. Therefore, the confidentiality and integration of artificial intelligence systems into critical situations is a prospect for further opportunities to increase the level of national cyber defence and reduce dangerous threats.

The availability of the object of protection is an important component of information security. The creation of a monitoring system for information security in information systems is a mandatory tool. Monitoring systems are used for the efficient management of possible risks and events. The main purpose of the monitoring system is to track the status of network services and information security subsystems using various criteria.

Improving the detection of possible threats and dangers, real-time response to the behaviour of information systems, and the ability to detect and avoid cyber threats at the stage of their manifestation are among the important issues in applying artificial intelligence capabilities to digital security strategies.

1. Materials and Methods

Cybersecurity requires improving existing cybersecurity methods, creating reliable protection against possible new threats, updating existing protection measures, monitoring cyber threats and developing protection strategies that meet the current conditions of life.

The main methods of controlling the operation and ensuring reliable protection against cyber threats are collecting and combining various data and indicators to establish control, analysing and correlating the collected data to prevent possible attacks, and automated verification of event monitoring parameters. Testing scenarios of various events allows you to analyse and confirm the availability of services at different levels. The use of automated system response in case of significant deviations from the normalised values makes it possible to make effective decisions on identifying anomalies and preventing cyber threats.

The collected anomaly detection databases help to further identify and predict events and mechanisms for further activities to create effective strategies to protect against cyber incidents.

2. Results and Discussion

In today's world of digitalised information environment, artificial intelligence has become not only an innovation but also an integral part of everyday life. It is continuously transforming various areas, helping to automate boring and routine tasks, effectively solve complex problems, and significantly improve productivity. But one of the most important areas of AI application is cybersecurity. AI is gaining critical importance as machine learning algorithms, analysing large amounts of data, detecting anomalies in network traffic, and identifying potentially dangerous vulnerabilities. AI uses technologies that can be applied in various industries, economics, finance, banking, military, education, and healthcare [1].

Artificial intelligence makes it possible to analyse large amounts of data and identify unusual situations or suspicious activity. Such actions make it possible to recognise cyber threats and attacks that may occur faster. Important priorities in the use of artificial intelligence in cybersecurity include automating threat detection, minimising errors, processing large amounts of data, predicting undesirable events and preventing them.

The use of machine learning algorithms to analyse and identify fraudster activity and respond to new types of attacks and dangers indicates that it is possible to provide reliable protection against cyber threats. The latest intelligent systems are able to respond to cyber threats in a timely manner and provide timely protection against network access. Processing large volumes of information in a minimum amount of time helps to timely anticipate and prevent possible threats or cyber attacks. The speed of decision-making on threat detection is an effective component in the use of artificial intelligence to reduce cyber threats.

CONCLUSIONS

The problems of information security and protection of society from the negative impact of cybercrime can be countered by artificial intelligence. The main issues are malfunctioning of hardware and software, proliferation of information weapons, use of malware, leakage of confidential

information, industrial espionage, technological influences, etc. Artificial intelligence technologies are one of the most effective tools in the field of cybersecurity. Fraud detection, unwanted intrusions, malware, risk assessment, network threats and other threats can be prevented and neutralised using artificial intelligence to improve the state of protection against cyber threats.

Artificial intelligence increases the ability of organisations to anticipate, prevent, defend against threats and control system access passwords, creating a strong defence against cybercrime. It is artificial intelligence that will expand the ability to protect the digital environment using the latest information technologies.

REFERENCES

1. The role of artificial intelligence in cybersecurity: predicting and preventing attacks. 2024. Available at: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/ [Accessde 05.06.2025]
2. Rybalchenko L. V. (2022). Cybercrime in the global space. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs,* special Issue № 2 (121). pp. 524-530. https://doi.org/10.31733/2078-3566-2022-6-524-530
3. Rybalchenko L. V., Haborets O. A. & Prokopovych-Tkachenko D. I. (2024). Cyber Resilience: Global Threats And National Cyber Defense Strategies. *Systems and Technologies*, *68*(2), 95-101. https://doi.org/10.32782/2521-6643-2024-2-68.11
4. Carvalho, J.-P. (2025). The political-economic risks of AI. SSRN. https://doi.org/10.2139/ssrn.5137622