UDC: 004.8+004.056/.57:005.334
DOI: https://doi.org/10.17721/ISTS.2024.8.42-48

Serhii DAKOV, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0001-9413-3709
e-mail: serhii.dakov@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Dmytro MANKOVSKYI, Student
ORCID ID: 0009-0004-5053-2432
e-mail: dimamankovskyi@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Ivan BILOKON, PhD (Engin.), Assoc. Prof.
ORCID ID: 0009-0008-3074-7064
e-mail: ivan.bilokon@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ARTIFICIAL INTELLIGENCE SYSTEMS IN CYBER SECURITY AND THEIR CAPABILITIESFRONT MODERN CYBER THREATS

Background. ***In recent years, the level of cybercrime has grown rapidly. The complexity and diversity of these threats has forced organizations to prioritize advanced cybersecurity solutions, including the use of artificial intelligence technologies that can quickly analyze data to identify potential threats and anomalies. By 2027, the AI-based cybersecurity market is expected to exceed $46 billion. However, as AI strengthens and refines defenses, cybercriminals are adapting by exploiting vulnerabilities and even using AI to enhance attacks. This dual use of AI underscores the need for balanced and intelligent strategies that combine the predictable capabilities of AI with human knowledge and talent.***

Methods. ***My Research highlights effective risk prevention strategies, including promoting a security-aware culture, implementing strong passwords and two-factor authentication, regularly assessing and updating systems, enhancing firewalls, and adhering to cybersecurity regulations. AI proves valuable in threat detection and response, giving companies a competitive edge, though it raises concerns about reducing human roles in security tasks.***

Results. ***The research indicates that AI positively impacts cybersecurity by enabling faster detection and response to threats, allowing organizations to proactively identify and address vulnerabilities. Companies that integrate AI into their cybersecurity strategies gain an advantage in managing complex cyber threats. However, concerns persist about AI's dual-use nature, as it could also be leveraged by cybercriminals for advanced attacks. This potential for AI to operate independently raises questions about the diminishing role of human oversight. Ultimately, the findings stress the need for a balanced approach: while AI is essential for modern cybersecurity, human involvement remains crucial. Continuous adaptation and a blend of technological and human expertise are necessary to protect critical infrastructure and data.***

Conclusions. ***To summarise, the rapid growth of cybercrime underscores the necessity for robust cybersecurity measures to protect sensitive information and ensure operational integrity. Artificial Intelligence is becoming crucial in enhancing cybersecurity through advanced threat detection, pattern recognition, and predictive analysis. While AI offers significant benefits, it can also be exploited by cybercriminals, highlighting the importance of vigilance and innovation in security strategies. Despite advancements in AI, human expertise remains vital for interpreting insights, making informed decisions, and adapting to new threats. A multi-faceted approach, including employee training, regular audits, and strong data protection, is essential for effective cybersecurity. Enhanced cooperation among organizations, governments, and international partners is crucial for developing effective strategies to combat cybercrime. Continued research into AI capabilities and ethical considerations is necessary to address the evolving landscape of cybersecurity threats.***

Keywords: ***artificial intelligence, measures, strategy, cybersecurity, threats, analysis.***

Background

In recent years, artificial intelligence (AI) has had a significant impact on cybercrime and other industries. It is projected that the cost of the cybercrime industry will reach $8 trillion in 2023 and $10.5 trillion by 2025. It is clear that this figure will continue to grow. A robust cybersecurity system is more important than ever, especially now, as cyber professionals and criminals alike strive to stay ahead of the curve in a rapidly changing environment. Researching and preventing potential cybercrimes and their consequences should be a strategic goal for humanity, in which the role of digital technologies is growing every year. As in many other areas, the role of artificial intelligence in cyber security is likely to become more significant (https://www.village.com.ua/village/business/news/305021-tse-reytingkrayin-za-rivnem-kiberbezpeki-/ukrayina-na-25-mu-mistsi, 2024). Companies that implement AI technologies offer significant advantages, providing essential tools for navigating cybersecurity challenges and adapting flexibly to ever-evolving cyber threats. Moreover, some cyber threats are evolving faster than cybersecurity systems. Cyber threats are inherently complex and constantly adapt to the demands of time and technological progress. It is estimated that in 2024, cybercrime will cost the global economy more than a trillion dollars. Many organizations are investing heavily in modern cybersecurity to avoid financial and reputational damage from cyber threats. However, cybercriminals–often professionals in their field–always find new ways to infiltrate secure cybersecurity structures, exploiting vulnerabilities and even the latest technologies. AI is expected to play an increasingly important role in cybersecurity systems, potentially identifying threats autonomously and adjusting security infrastructure accordingly. AI technologies will also analyze security risks using analytical tools and data, providing companies' employees and regular internet users with advice on how to fine-tune security systems. Yet, there is a significant concern that AI may eventually surpass humans and perform all security-related tasks independently. This presents a challenge for humanity, which must maintain its role in IT security. However, technology is developing rapidly, and its impact on security architecture is already apparent today–especially in Ukraine (Impact of AI on

Cybersecurity, 2024). Artificial Intelligence Plays a Crucial Role in the science, where AI stimulates the optimization and development of research in new ways. It also facilitates enhanced collaboration with international partners. In cyber security, in addition to the fact that artificial intelligence accelerates the development of modern systems for countering cyber threats, it is also involved in the prevention of risks and threats, as well as helping to develop methods to protect important information. In cyberspace, the risks associated with cyberattacks are constantly rising–new risks are being invented all the time, with each one more dangerous than the last. New attackers emerge with increasingly sophisticated and unconventional ideas. Therefore, it is essential to leverage our knowledge to develop strategies for countering these ever-growing risks to the information space. It is also necessary to harness all the capabilities of artificial intelligence (AI) to achieve a high level of security (https://robotdreams.cc/uk/blog/352-shtuchniy-intelekt-/ne-zahistit-yakshcho-nevikoristovuvati-intelekt-prirodniy-/yak-rozvitok-shi-vplivaye-na-kiberbezpeku, 2024). Risk prevention methods are highly diverse and depend on the specific situation. Figure 2 illustrates the most commonly used methods for ensuring information security. These include employee vigilance, securing data through passwords and two-factor authentication, conducting regular information security audits, updating software, improving security control, training employees to address new challenges, and complying with all relevant laws. AI plays a supporting role in this critical issue by offering advice on how to act in different scenarios. However, it is quite possible that, in the near future, AI technologies will autonomously manage cybersecurity systems, diminishing the role of humans. The influence of AI technologies on the number of cyber incidents is generally considered positive. However, the limitless potential of AI means that it can also be exploited by malicious actors to increase the scale and intensity of cyberattacks. Below are examples of both the positive and negative impacts of AI technologies on cybersecurity systems (https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/the-role-of-ai-in-cybersecurity-/anticipating-and-preventing-attacks, 2024).

Positive Impact:

Advanced Response Systems: Modern AI-powered response systems can reduce the number of cyber incidents and mitigate their financial impact.

Improved Cybersecurity: AI systems enhance cybersecurity, increasing resilience against vulnerabilities.

Threat Forecasting and Network Modeling: AI can predict various cyber threats and simulate network behavior, enabling the development of new countermeasures.

Vulnerability Analysis: AI helps analyze existing cyber threats and identify weaknesses in computer systems.

Support for Human Decision-Making: AI can offer advice to humans on how to respond to emerging threats.

Data Analysis: AI aids in analyzing large datasets and interpreting information that humans might not be able to process, potentially uncovering critical insights about cyber threats.

Minimizing Damage: AI technologies can help minimize losses from cyber threats by implementing systems for threat prevention and prediction.

Negative Impact:

Facilitating Malicious Software: AI can assist attackers in generating more malware and launching cyberattacks at a scale far beyond human capabilities.

Identifying Vulnerabilities: AI can help attackers discover new vulnerabilities and weaknesses in enterprises and software systems that might otherwise go unnoticed.

Autonomous Attacks: AI could autonomously conduct attacks on computer systems without human intervention.

Strategic Advice for Attackers: AI might provide malicious actors with recommendations on how to act more effectively in specific situations to maximize their gains.

Privacy Issues: AI can cause user privacy problems, thereby increasing security risks.

Errors Leading to Cyberattacks: AI systems are not immune to errors, and these mistakes can also lead to cyberattacks.

Actuality. The cybercrime industry is projected to escalate to $10.5 trillion by 2025, highlighting the urgent need for effective cybersecurity measures as financial losses mount. Cyber threats are increasingly sophisticated, with new methods emerging constantly. This dynamic environment demands that organizations stay ahead through adaptive security measures. The integration of AI in cybersecurity is not just a trend but a necessity, as its capabilities enable organizations to analyze threats more efficiently and respond more rapidly. Nations and organizations are recognizing cybersecurity as a critical area of focus, with significant investments in modern technologies to protect against evolving threats. The ongoing importance of human oversight in cybersecurity strategies is gaining recognition, as the combination of AI tools and human expertise proves to be the most effective defense. There is an increasing emphasis on collaboration across industries and borders to share intelligence and resources, creating a united front against cybercriminal activities. As AI technologies advance, ethical considerations regarding their use and potential misuse are becoming a vital part of the conversation in cybersecurity.

Analysis of the sources. The analysis of sources reveals a comprehensive understanding of the current landscape of cybersecurity in Ukraine, particularly in relation to the integration of artificial intelligence (AI). The article detailing Ukraine's cybersecurity ranking provides insights into the country's position globally, indicating the significance of ongoing efforts to combat cyber threats. Furthermore, the discussion on AI applications across various sectors highlights the increasing interest in utilizing AI technologies, not just in cybersecurity but across the entire economy. Artificial intelligence in cyber security has potential in predicting and preventing cyber attacks (https://www.technologyreview.com/2023/05/24/1073395/ai-in-cybersecurity-yesterdays-promise-todays-reality, 2024). This is confirmed by the Security Service of Ukraine, which emphasizes the preventive measures taken to neutralize a significant number of cyber attacks, reflecting the constant threat that the country faces. The impact of artificial intelligence on cyber security requires further research, its advantages in detecting threats and reducing risks are analyzed. In this case, the National Cyber Security Index is indicative, as it provides quantitative data that help assess Ukraine's achievements and capabilities in the field of cyber security and identify areas for improvement and improvement. An important aspect is the distinction between artificial and natural intelligence in cybersecurity, emphasizing the limited capabilities of AI when operating independently of human control. This emphasizes the need and role of human intelligence and knowledge to develop effective information security strategies. In addition, various strategies that can be applied to use AI to predict and prevent cyber threats are explored. The connection between artificial intelligence and cybersecurity is becoming increasingly close, and this is leading to significant growth in the artificial intelligence cybersecurity sector, emphasizing opportunities for development. Scientific article materials containing research findings on contemporary cybersecurity issues contribute to academic discourse, while analysis of the current state of artificial intelligence in cybersecurity reveals expectations and today's realities.

Methods

My research investigates a variety of risk prevention methods that organizations can adopt to enhance their cybersecurity posture. These methods include promoting a culture of awareness, where employees are trained to recognize potential threats and suspicious activities. Implementing robust measures, such as strong passwords and two-factor authentication, is crucial for securing sensitive information. Additionally, conducting frequent assessments of security practices and systems helps identify and rectify vulnerabilities effectively. Regular software updates are essential to patch known vulnerabilities and protect against new threats. Moreover, improving existing security measures–such as firewalls and intrusion detection systems–can significantly strengthen defenses. Ongoing education and training for employees ensure they stay informed about the latest security challenges and response strategies. Adherence to relevant cybersecurity laws and regulations is vital to mitigate legal risks and maintain trust with stakeholders. The effectiveness of a cybersecurity strategy involving artificial intelligence highlights the importance of adapting approaches to meet specific organizational needs and contexts. This roadmap can significantly improve an organization's overall information security resilience. The effectiveness of specific solutions using artificial intelligence technologies also differs from each other (table 1).

Table 1

The effectiveness and ineffectiveness of ai technologies in cyber security

Effective	Ineffective
Faster, more coordinated, and stronger response to cyber threats	Displacement of humans by AI programs, diminishing the role of individuals in cybersecurity
Forecasting, modeling cyberattacks, and their evolution to develop appropriate response strategies. Analysis of existing cyberattacks	AI misuse by malicious actors could have severe consequences, as malware may autonomously adapt to the latest security systems
Assistance to humans in organizing defenses against cyberattacks. Ability to analyze vast data sets and scan the cyberspace for threats	AI aiding attackers by identifying vulnerabilities in computer systems
Providing qualified assistance to people through AI technologies	AI may also offer qualified assistance to attackers, thereby strengthening them
AI can potentially reduce the number of cyber incidents by improving security protocols and minimizing losses from cyberattacks to zero	On the contrary, AI could autonomously generate cyberattacks, increasing their frequency and making them more damaging

Impact of Artificial Intelligence Technologies on Information Security

Positive Impact:

AI helps people manage security systems more efficiently by automating processes and streamlining operations.

AI's analytical capabilities enable it to forecast potential threats and incidents, helping prevent cyberattacks.

AI allows cybersecurity systems to quickly adapt to new types of threats and changes in infrastructure.

AI takes over routine tasks, allowing humans to focus on more complex and critical activities.

AI provides suggestions for modernizing security architectures and identifying vulnerabilities.

Negative Impact:

Cybercriminals can leverage AI to discover vulnerabilities within security systems.

AI can autonomously generate sophisticated malware capable of bypassing traditional security measures.

In some cases, AI can fully automate cybersecurity processes, minimizing human control and oversight.

AI may sometimes offer incorrect advice on improving security systems, potentially leading to weaker defenses and increased vulnerabilities (https://ela.kpi.ua/items/bf50435a-bfc2-48ef-a400-d31ca2e99b06, 2022) and (Ilchenko, 2024; Mankovskyi, 2024), table 2 & table 3.

Formulas, shown in Table 4 allow us to analyze mathematical and analytical processes in the work of artificial intelligence systems. Making such calculations can improve our cybersecurity strategy.

Table 2

In cyber security, the use of AI technologies is very broad and diverse

Area of Application	Description	Area of Application	Description
Threat Detection and Prevention		AI can analyze malware, phishing attacks, and other cyber threats in real time by analyzing superb datasets and scanning fo anomalies in network traffic	
Intrusion Detection Systems (IDS)		AI enhances IDS by identifying unauthorized access attempts, suspicious behavior, and unknown attack vectors faster than traditional methods	
User Behavior Analytics (UBA)		AI monitors and learns normal user behaviors, helping detect unusual activities that might indicate insider threats or compromised accounts	
Fraud Detection		AI systems analyze transaction patterns to identify fraudulent activities in banking, e-commerce, and other sectors	

End of the tabl. 2

Area of Application	Description	Area of Application	Description
Incident Response Automation		AI can automate responses to threats, such as isolating infected systems or blocking malicious IP addresses, reducing response time	
Vulnerability Management		AI tools scan systems and applications for vulnerabilities, helping organizations prioritize patches and mitigate risks effectively	
Predictive Threat Intelligence		AI analyzes historical data to predict future attacks, enabling proactive defense strategies	
Security Operations Center (SOC) Support		AI assists SOC teams by filtering false positives, providing insights, and offering recommendations for threat mitigation	
Endpoint Protection		AI-based endpoint protection platforms prevent malicious files and activities on individual devices, even before known malware signatures are developed	
Phishing Detection and Email Security		AI filters emails and flags phishing attempts by identifying suspicious language patterns, links, or attachments	

Table 3

Examples of AI cyber security solutions

Solution	Description
Darktrace	A platform that uses AI to identify various cyber threats in real-time. It employs the "Enterprise Immune System," modeling network behavior and learning from it to identify new attacks and anomalies. Darktrace also provides tools for tracking, responding to, and analyzing the consequences of security incidents
CylancePROTECT	A program leveraging AI to detect and prevent cyberattacks and risks. Known for its "holistic protection" approach, it identifies and analyzes both known and unknown malware and cyber threats. It supports defense against various cyber threats proactively
IBM QRadar	A Security Information and Event Management (SIEM) platform that uses AI to detect abnormal activities, counter threats, and analyze security events. It combines network monitoring, log analysis, intrusion detection, incident classification, and response mechanisms to mitigate or prevent cybercrime losses
FireEye Helix	A cybersecurity platform offering a wide range of monitoring, analysis, and response functions. It uses AI to detect and analyze attacks from multiple angles and assists in managing incidents, tracking their impacts, and predicting future risks
Splunk Enterprise Security	An extension for the Splunk platform that analyzes security events and detects cyber threats in real-time. It provides continuous monitoring, threat detection, and response protocols. AI technologies are employed to improve the identification and mitigation of risks
Cisco Stealthwatch	A network security monitoring tool that uses traffic analytics and AI to detect and respond to cyber threats in real-time. It enables organizations to analyze network traffic, identify abnormal activities and vulnerabilities, and take appropriate actions to mitigate potential threats
ChatGPT and Other Chatbots	Advanced chatbot technology assists in developing cybersecurity strategies, providing advice on the best approaches, and solving various tasks and issues. These chatbots help identify network vulnerabilities and suggest solutions. However, caution is needed to avoid misuse of such technologies

Table 4

Math Formulas

Formula	Usage
$P(y=1\mid x)=\frac{1}{1+e^{-(\beta_0+\beta_{1x1}+\ldots+\beta_{nxn})}}$ (1) Logistic Regression for Binary Classification (Phishing vs. Safe Email)	Used to classify emails or files as malicious or safe. It also outputs a probability between 0 and 1, indicating the likelihood of a given instance being malicious.
$p(y_i)=\frac{e^{z_i}}{\sum_{j=1}^{n} e^{z_i}}$ (2) Softmax Function for Multi-Class Classification	Assigns probabilities to multiple classes (e.g., different types of attacks).It ensures that the output is a valid probability distribution over multiple classes
$P(X_{n+1}=j\mid X_n=i)=p_{ij}$ (3) Markov Chains for Predicting Attack Patterns	It is used in modeling sequential events, such as user behavior over time, to detect abnormal actions (e.g., lateral movement in cybersecurity)
$EMA_t=\alpha\cdot x_t+(1-\alpha)\cdot EMA_{t-1}$ (4) Exponential Moving Average (EMA) for Real-Time Threat Detection	This formula smooths time-series data for anomaly detection in network traffic

End of the tabl. 4

Formula	Usage
$$Q(s,a) = r + \gamma \max_{a^I} Q(s^I, a^I) \qquad (5)$$ Bellman Equation for Reinforcement Learning in Automated Responses	Helps optimize automated threat responses by learning the best action to take in each state. It is used in SOAR (Security Orchestration, Automation, and Response) systems

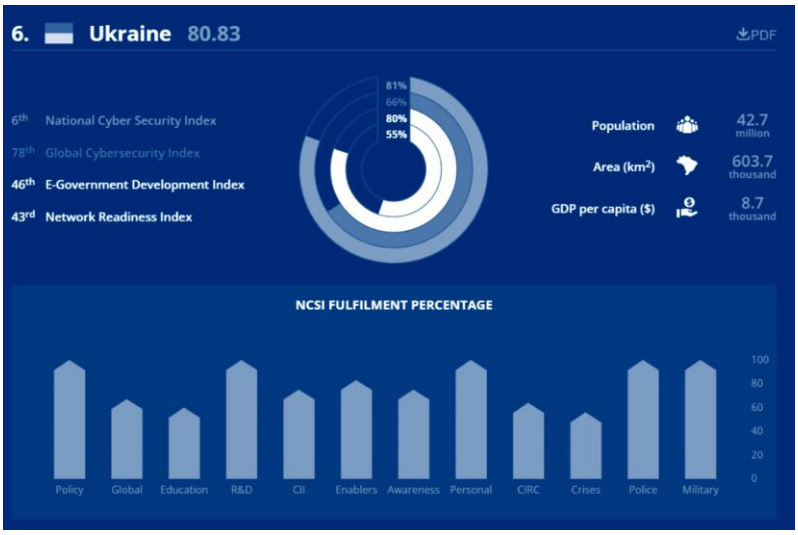
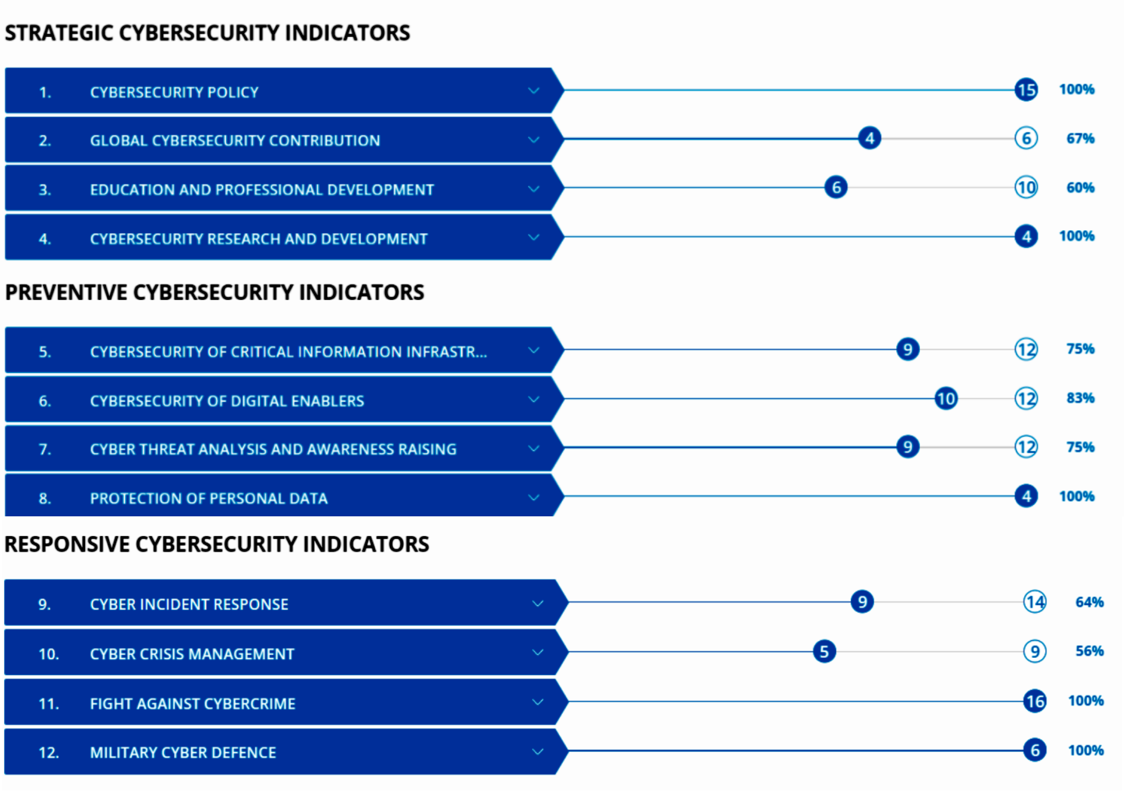


Fig. 1. Ukraine is 6th in NCSI Ranking (Cybersecurity rankings)



STRATEGIC CYBERSECURITY INDICATORS

1.	CYBERSECURITY POLICY	15		100%
2.	GLOBAL CYBERSECURITY CONTRIBUTION	4	6	67%
3.	EDUCATION AND PROFESSIONAL DEVELOPMENT	6	10	60%
4.	CYBERSECURITY RESEARCH AND DEVELOPMENT	4		100%

PREVENTIVE CYBERSECURITY INDICATORS

5.	CYBERSECURITY OF CRITICAL INFORMATION INFRASTR...	9	12	75%
6.	CYBERSECURITY OF DIGITAL ENABLERS	10	12	83%
7.	CYBER THREAT ANALYSIS AND AWARENESS RAISING	9	12	75%
8.	PROTECTION OF PERSONAL DATA	4		100%

RESPONSIVE CYBERSECURITY INDICATORS

9.	CYBER INCIDENT RESPONSE	9	14	64%
10.	CYBER CRISIS MANAGEMENT	5	9	56%
11.	FIGHT AGAINST CYBERCRIME	16		100%
12.	MILITARY CYBER DEFENCE	6		100%

Fig. 2. How experts value Ukraine`s cybersecurity level

As illustrated in Fig. 1, 2, several areas of cybersecurity receive top ratings, emphasizing the importance of personal data protection, military cybersecurity, and well-structured security policies, along with continuous research in the field. AI plays a significant role in enhancing these efforts, contributing to effective strategies across different domains.

Key insights from the figure include:

High Ratings in Critical Areas: Personal data protection, military cybersecurity, properly structured cybersecurity policies, ongoing research and innovation

Critical Infrastructure and Anti-Cybercrime Efforts: Cybersecurity in critical infrastructure and personal data protection is rated positively, as is the fight against cybercrime.

Threats to Ukraine's cyber security have been known and identified for a long time, which indicates opportunities for creating an effective strategy for countering threats.

There are areas that need improvement, in particular: risk management and prevention, anti-crisis management, regulation of the role of AI in cyber security at the legislative level.

This analysis highlights the current situation in Ukrainian cyber security and highlights the need for an AI implementation strategy that will help ensure effective operation while leveraging its potential for protection.

Results

The role of artificial intelligence in various sectors of the economy and human life is becoming more and more important, especially in IT, which is changing rapidly. Cyber security requires modern strategies to counter security threats. With the advent of new technologies, more and more dangerous vulnerabilities, viruses and other cyber threats appear. Organizations are trying to adapt their security protocols to new requirements. AI has the potential to ease some of this work by making security systems more productive, allowing people to focus on strategic planning and other important tasks. However, cyber threats are also evolving and intensifying. Cybercriminals can also use artificial intelligence to design and adapt malware, find system vulnerabilities, and execute more sophisticated attacks. There is a possibility and a risk that the rapid progress of AI may reduce, or even nullify, the human role in the cybersecurity architecture. This is a challenge and a problem that should be taken seriously. In cybersecurity, AI can analyze threat data, make far-sighted and far-reaching predictions, process large volumes of information, and create decoy networks to divert would-be cybercriminals away from mission-critical systems. Timely detection, modeling and forecasting of cyber threats, along with real-time response and accurate analysis of malicious software, as well as the human role in these processes are important aspects of the development of cyber security systems in combination with AI technologies. To effectively address the surge in cyberattacks and the challenges posed by artificial intelligence (AI), the following solutions are proposed:

Create sophisticated software that minimizes the impact of cyberattacks, enhancing overall resilience against threats.

Improve the quality of cyber incident prevention by adapting systems to better anticipate and respond to emerging threats.

Urge both governments and private companies to significantly invest in cybersecurity measures. For example, an investment of $300 million in cybersecurity and AI can help protect $10 billion in critical state assets.

Implement AI systems and leverage cutting-edge software technologies. While initial costs may be high, this investment can lead to substantial long-term savings and more efficient security architectures.

Ensure effective collaboration between humans and AI systems, preventing any reduction in human roles within cybersecurity frameworks.

Tighten access to AI technologies for malicious actors and increase penalties and countermeasures against cybercrime.

By combining strategic efforts and utilizing AI purposefully, it is possible to build a resilient cybersecurity system that effectively predicts and prevents various threats, adapting to contemporary demands.

This strategic approach highlights the dual nature of AI as both a powerful tool for enhancing cybersecurity and a challenge that necessitates careful management and oversight. By implementing these solutions, organizations can better protect their assets and respond to the evolving landscape of cyber threats.

Table 5

Measures to improve cybersecurity

Measure	How it works	Results
Network anomaly detection	AI analyzes network traffic and behavioral patterns to detect unusual activities (e.g., DDoS attacks or intrusions).	**30–50%** reduction in undetected threats through real-time anomaly detection
Malware detection and prevention	AI analyzes the code of programs and files to detect potential malware, including zero-day attacks, without relying on known signatures.	**40–60%** increase in detecting new types of malware
Automated incident response via SOAR platforms	AI triggers automated actions to mitigate threats (e.g., blocking IP addresses or isolating infected devices).	**30–40%** reduction in response time, minimizing potential damage
Phishing attack detection	AI scans emails and messages to identify phishing attempts based on textual, metadata, and behavioral patterns.	**25–40%** decrease in successful phishing attacks
Enhanced authentication using biometrics and behavioral factors	AI leverages user behavior (like typing patterns) or biometric data for additional access control.	**20–30%** decrease in account compromises
Threat prediction and prevention (threat intelligence)	AI analyzes data from multiple sources to predict and prepare for future attacks or vulnerabilities.	**30–50%** improvement in readiness for new threats
Log Analysis for anomaly detection	AI reviews logs and events to detect patterns that may indicate intrusions or policy violations.	**20–40%** reduction in undetected incidents
User education and defense against social engineering	AI personalizes phishing awareness training and educates users about social engineering threats.	**10–25%** reduction in the risk of social engineering attacks

To summarise the information given in Table 5, implementing AI-powered measures can **improve cybersecurity by 50–70%**, depending on the environment (network complexity, user behavior, and current defenses). However, **100% security is unattainable** as threats evolve continuously, and new malware samples appear and improve daily.

Discussion and conclusions

During the research, the following conclusions were drawn: Artificial intelligence is a highly valuable and rapidly evolving technology, with applications across diverse fields such as weather forecasting and complex software development. AI technologies have already made significant strides in cybersecurity and information protection, creating new opportunities for enhancing data security. With a thoughtful and cautious approach, it is possible to develop robust information systems that provide a high level of cybersecurity. There has been an analysis of the rising number of cyberattacks in recent years and the impact of AI technologies on these trends. While AI offers numerous benefits, it also poses challenges, as malicious actors can exploit these technologies to further their agendas. The study examined the various ways offenders utilize AI technologies. As AI increasingly takes over roles traditionally held by humans, the risks within the cybersecurity domain remain significant. Humanity must adapt to effectively collaborate with AI to preserve its role in this rapidly evolving field. Proper utilization of AI for its intended purposes can lead to the development of a dependable system for preventing cyber threats. This will help reduce the adverse effects of cyberattacks on the economy, businesses, and the lives of ordinary individuals, potentially safeguarding substantial financial and human resources from cybercrime.

Authors' contribution: Serhiy Dakov – conceptualization, methodology; Dmytro Mankovsky – analysis of sources, preparation of literature review, theoretical foundations of the study, preparation of the laboratory for the study, conducting the study.

References

Ilchenko, V. (2024). Cybersecurity Issues in Information and Telecommunication Systems. *VII International Scientific and Practical Conference "Problems of Cybersecurity of Information and Telecommunications Systems" (PCSITS)* (pp. 122–124) Taras Shevchenko National University of Kyiv [in Ukrainian]. [Ільченко В. (2024). Питання кібербезпеки в інформаційно-телекомунікаційних системах. *VII Міжнародна науково-практична конференція "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS)* (с. 122–124). Київський національний університет імені Тараса Шевченка].

Mankovskyi, D. (2024). Study on AI Systems Adaptation to New Threats: Analytical research. *VII International Scientific and Practical Conference "Problems of Cybersecurity of Information and Telecommunications Systems"* (223–225). Taras Shevchenko National University of Kyiv.

Отримано редакцією журналу / Received: 30.10.24
Прорецензовано / Revised: 27.11.24
Схвалено до друку / Accepted: 30.11.24

Сергій ДАКОВ, канд. техн. наук, доц.
ORCID ID: 0000-0001-9413-3709
e-mail: serhii.dakov@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Дмитро МАНЬКОВСЬКИЙ, студ.
ORCID ID: 0009-0004-5053-2432
e-mail: dimamankovskyi@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Іван БІЛОКОНЬ, канд. техн. наук, доц.
ORCID ID: 0009-0008-3074-7064
e-mail: ivan@bilokon@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ ТА ЇХНІ МОЖЛИВОСТІ ПРОТИСТОЯТИ СУЧАСНИМ КІБЕРЗАГРОЗАМ

Вступ. ***Останніми роками рівень кіберзлочинності стрімко зріс. Складність і різноманітність цих загроз змусили організації віддавати пріоритет передовим рішенням із кібербезпеки, включаючи використання технологій штучного інтелекту, які можуть швидко аналізувати дані для виявлення потенційних загроз і аномалій. Очікують, що до 2027 р. ринок кібербезпеки на основі ШІ перевищить 46 млрд дол. Однак, оскільки штучний інтелект зміцнює та покращує захист, кіберзлочинці адаптуються, використовуючи вразливості та навіть застосовуючи штучний інтелект для посилення атак. Таке подвійне використання ШІ підкреслює необхідність збалансованих і розумних стратегій, які поєднують передбачувані можливості ШІ з людськими знаннями та талантом.***

Методи. ***Наведене дослідження зазначає ефективні стратегії запобігання ризикам, зокрема і сприяння культурі безпеки, впровадження надійних паролів і двофакторної автентифікації, регулярне оцінювання й оновлення систем, удосконалення брандмауерів і дотримання правил кібербезпеки. Штучний інтелект доводить свою цінність у виявленні загроз і реагуванні на них, надаючи компаніям конкурентну перевагу, хоча викликає занепокоєння зменшення ролі людини в задачах безпеки.***

Результати. ***Дослідження показує, що штучний інтелект позитивно впливає на кібербезпеку, забезпечуючи швидке виявлення загроз і реагування на них, дозволяючи організаціям завчасно виявляти й усувати вразливості. Компанії, які інтегрують штучний інтелект у свої стратегії кібербезпеки, отримують перевагу в керуванні складними кіберзагрозами. Проте все ще викликає занепокоєння подвійне використання штучного інтелекту, оскільки його також можуть використовувати кіберзлочинці для розширених атак. Потенціал штучного інтелекту працювати незалежно ставить питання про зменшення ролі людського нагляду. Зрештою, результати підкреслюють необхідність збалансованого підходу: хоча ШІ є важливим для розв'язання задач сучасної кібербезпеки, участь людини у цьому процесі залишається вирішальною. Для захисту критичної інфраструктури та даних необхідні постійна адаптація і поєднання технологічного та людського досвіду.***

Висновки. ***Швидке зростання кіберзлочинності свідчить про необхідність розроблення надійних заходів кібербезпеки для захисту конфіденційної інформації та забезпечення операційної цілісності. Штучний інтелект стає вирішальним у підвищенні кібербезпеки за допомогою розширеного виявлення загроз, розпізнавання образів і прогнозного аналізу. Хоча штучний інтелект пропонує значні переваги, ним також можуть скористатися кіберзлочинці, що підкреслює важливість пильності й інновацій у стратегіях безпеки. Незважаючи на прогрес ШІ, людські знання залишаються життєво важливими для інтерпретації інформації, прийняття обґрунтованих рішень і адаптації до нових загроз. Для ефективної кібербезпеки важливий багатогранний підхід, включаючи навчання співробітників, регулярні аудити та надійний захист даних. Розширена співпраця між організаціями, урядами та міжнародними партнерами має вирішальне значення для розроблення ефективних стратегій боротьби з кіберзлочинністю. Необхідно продовжувати дослідження можливостей штучного інтелекту й етичних міркувань, щоб подолати мінливий ландшафт загроз кібербезпеці.***

Ключові слова: ***штучний інтелект, заходи, стратегія, кібербезпека, загрози, аналіз.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.