Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Матеріали
II наукової онлайн-конференції

(Суми, 02 липня 2024)

Суми
Сумський державний університет
2024

004.056.5:336(082)
В43

Головний редактор
доц., к.е.н., ***Койбічук Віталія***, завідувачка кафедри економічної кібернетики, Сумський державний університет
.

Затверджено Вченою Радою Сумського державного університету (протокол № 1, 29.08.2024)

S62 Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми, 02 липня 2024. Збірник матеріалів тез наукової онлайн-конференції / за загальною редакцією доц. Койбічук В.В. – Суми : Сумський державний університет, 2024. – 72 с.

Матеріали наукової онлайн-конференції "Виклики кібербезпеки індустрії фінансових послуг" присвячені пошуку системного вирішення проблем у сфері протидії кібеззагрозам у сфері фінансових послуг, підвищенню рівня кіберзахисту об'єктів критичної інфраструктури.

Видання розраховане на науковців, викладачів, студентів вищих навчальних закладів, аспірантів, докторантів та інших зацікавлених осіб.

004.056.5:336(082)

© Сумський державний університет, 2024

ЗМІСТ

СЕКЦІЯ 1	***ЦИФРОВІ ТРАНСФОРМАЦІЇ В ЕКОНОМІЦІ***	**5**
Іван Нестеренко	ДОСЛІДЖЕННЯ ЦИФРОВИХ ТРАНСФОРМАЦІЙ В ЕКОНОМІЦІ	5
Катерина Дідоренко	ЦИФРОВІЗАЦІЯ ЯК ФАКТОР ПОСИЛЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ КРАЇНИ	9
Володимир Науменко	МОДЕЛЮВАННЯ ТА ПРОГНОЗУВАННЯ ВПЛИВУ РІВНЯ ЦИФРОВІЗАЦІЇ НА ЕКОНОМІЧНИЙ РОЗВИТОК	12
Дмитро Харченко	РОЛЬ ЦИФРОВІЗАЦІЇ В ПРОТИДІЇ КОРУПЦІЇ	16
Захарченко Андрій	ЦИФРОВІ НАВИЧКИ: ВИКЛИКИ ТА МОЖЛИВОСТІ	19
Даніїл Савченко, Тетяна Доценк	ТЕОРЕТИЧНІ АСПЕКТИ ВЗАЄМОЗВ'ЯЗКІВ КІБЕРБЕЗПЕКИ ТА БЕЗПЕКИ ОХОРОНИ ЗДОРОВ'Я	24
СЕКЦІЯ 2	***КІБЕРЗАГРОЗИ У СФЕРІ ФІНАНСОВИХ ПОСЛУГ***	***27***
Віталія Койбічук	ІДЕНТИФІКАЦІЯ ТА УПЕРЕДЖЕННЯ КІБЕРШАХРАЙСТВ В ЕЛЕКТРОННОМУ БАНКІНГУ: ДОСВІД ЄС	27
Роєнко Олександр	КОНВЕРГЕНЦІЙНІ ПРОЦЕСИ МІЖ КІБЕРЗЛОЧИННІСТЮ ТА ТІНЬОВОЮ ЕКОНОМІКОЮ	31
Ксенія Могильна	АНАЛІЗ ОСНОВНИХ ТРЕНДІВ НА СВІТОВОМУ РИНКУ КІБЕРСТРАХУВАННЯ	34
Ольга Горбачова	ТЕНДЕНЦІЇ РОЗВИТКУ РИНКУ КІБЕРСТРАХУВАННЯ У СВІТІ	39
Валерія Кочнєва	РОЛЬ КІБЕРСТРАХУВАННЯ У ПІДВИЩЕННІ РІВНЯ КІБЕРСТІЙКОСТІ КОМПАНІЙ	41
Іван Гончарук	КОРУПЦІЯ ЯК ІНСТРУМЕНТ ПРОНИКНЕННЯ ТА ВИКРАДАННЯ ІНСАЙДЕРСЬКИХ ДАНИХ	45
СЕКЦІЯ 3	***ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПРОТИДІЇ КІБЕРЗАГРОЗАМ***	92

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Avhusta Hrytsenko	*THE ROLE OF ARTIFICIAL INTELLIGENCE IN COUNTERING CYBER THREATS*	*48*
Вікторія Біловодська	*РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОТИДІЇ КІБЕРЗАГРОЗАМ*	*53*
Оголь Дмитро	*МЕТОДИ ПІДВИЩЕННЯ ЦИФРОВОЇ ОБІЗНАНОСТІ СПОЖИВАЧІВ ФІНАНСОВИХ ПОСЛУГ: УСПІШНІ ВІТЧИЗНЯНІ ТА ЗАКОРДОННІ КЕЙСИ*	*57*
Анна Шаповалова	*ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ*	*61*
Еліна Шрамко	*ШТУЧНИЙ ІНТЕЛЕКТ У БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ: ЕФЕКТИВНІ СТРАТЕГІЇ ТА ІНСТРУМЕНТИ*	*64*
Єлизавета Литюга	*ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ*	*69*

СЕКЦІЯ 3 ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПРОТИДІЇ КІБЕРЗАГРОЗАМ

THE ROLE OF ARTIFICIAL INTELLIGENCE IN COUNTERING CYBER THREATS

Avhusta Hrytsenko, student,
Sumy State University, Ukraine

Scientific adviser:
Olena Pahnenko, PhD, Associate Professor
Sumy State University, Ukraine

In the digital age, the proliferation of interconnected devices and reliance on technology has transformed the way we live, work, and interact. However, alongside the benefits of connectivity and innovation come unprecedented cybersecurity challenges. The increasing frequency and sophistication of cyber threats, ranging from malware and phishing attacks to data breaches and ransomware incidents, pose significant risks to individuals, organizations, and societies at large. In response to these evolving threats, there has been a growing recognition of the need for advanced cybersecurity measures capable of effectively detecting, mitigating, and preventing cyber-attacks in real time. In this context, the role of artificial intelligence (AI) has emerged as a game-changer in the field of cyber security.

Cybersecurity is a specific practice of protecting systems, networks, and programs from digital attacks. This term is often used interchangeably with “information security” and means a set of security measures and policies aiming to prevent data from disruptions or unauthorized access, use, disclosure, or modification (Ghelani, 2022). Cyber threats have a profound impact on various areas from individuals and organizations to governments and critical infrastructures. Thus, there is a huge need for proactive measures to enhance resilience, safeguard critical infrastructure, and protect individuals' rights and freedoms in cyberspace. Additionally, this problem is complicated by the spreading use of AI. Cyberattackers are developing AI-enabled malware that is adaptive, has the ability to understand the target environment, evade detection, continue to learn, and make advanced decisions. In this regard, malware is getting smarter and cyberthreats are evolving and becoming more sophisticated and complex. Hence, human intervention and capacity are not enough to sufficiently deal with advanced threats, the speed of processes, the amount of data, and the vulnerability of intrusion.

Thus, the countering of advanced adversaries requires an active approach to security that will place an emphasis on proactive measures, real-time detection, active monitoring, and mitigation of key threats. Therefore, innovative approaches such as the application of AI tools that have a learning capacity, are adaptable, analysis-driven, and able to detect user behavior and make intelligent and real-time decisions become a new powerful weapon in fighting cyber threats (Kadel et al., 2023).

Artificial Intelligence is the development of complex computer systems with the aid of human mentality which is able to perform its function like a human being. AI is a comprehensive scientific system with varying branches in math, computer science, and philosophy whose purpose is to develop another system that shows intelligence properties.

The integration of AI offers a promising avenue for countering the ever-evolving landscape of cyber threats. AI systems possess the capability to process vast amounts of data at incredible speeds, enabling them to detect patterns, anomalies, and potential threats more effectively than traditional methods (Agrawal et al., 2023). Moreover, AI-driven algorithms can adapt and learn from new data, continuously improving their ability to identify and mitigate risks. By automating threat detection, response, and remediation processes, AI not only enhances the efficiency of cyber security operations but also minimizes human error and response times (Tao et al., 2021). Additionally, AI facilitates predictive analytics (Kadet et al., 2023), allowing organizations to anticipate and proactively address emerging threats before they materialize. However, while AI holds immense potential in bolstering cyber defenses, it is not without challenges. Ethical considerations, biases in AI algorithms, and the potential for adversaries to exploit AI systems are among the concerns that must be carefully navigated (Dash et al., 2022). Nonetheless, with vigilant oversight, collaborative efforts, and ongoing innovation, the strategic deployment of AI can serve as a powerful tool in the fight against cyber threats, contributing to a more secure digital landscape for individuals, businesses, and governments alike.

The use of AI in cybersecurity has been instrumental in enhancing protection across various critical areas, including the following (Li & Liu, 2021).

AI is widely employed in protecting corporate networks by continuously monitoring network traffic for anomalies and potential threats. AI-driven intrusion detection systems (IDS) and intrusion prevention systems (IPS) analyze network behavior in real time, enabling rapid identification and mitigation of suspicious activities. AI-powered endpoint security solutions utilize machine learning algorithms to detect and respond to malware, ransomware, and other cyber threats targeting corporate devices.

Financial institutions face significant cybersecurity threats due to the sensitive nature of the data they handle. AI plays a crucial role in safeguarding

financial systems by detecting fraudulent transactions, identity theft, and unauthorized access. Furthermore, AI-driven risk assessment models help financial institutions evaluate and mitigate potential risks associated with lending, investments, and other financial activities.

Governments and state institutions rely on robust cybersecurity measures to protect sensitive information and critical infrastructure from cyber threats. AI is utilized in state information systems to bolster defenses against cyber-attacks, espionage, and other malicious activities. AI-driven threat intelligence platforms collect, analyze, and disseminate information about emerging cyber threats, enabling governments to proactively respond to potential risks. Additionally, AI-powered security analytics tools assist in identifying and mitigating vulnerabilities within state IT infrastructure, enhancing overall resilience against cyber threats.

AI technologies are employed to safeguard user data from unauthorized access, data breaches, and privacy violations. AI-driven identity and access management (IAM) systems utilize biometric authentication, behavioral analysis, and anomaly detection to verify user identities and prevent unauthorized access to sensitive data. Furthermore, AI-powered data loss prevention (DLP) solutions monitor and control the movement of confidential information across networks, ensuring compliance with data protection regulations such as GDPR and CCPA.

However, the application of AI in cybersecurity also presents several challenges that must be carefully addressed. Among these challenges are the following ethical issues and potential for abuse, dependence on accuracy and timeliness of data, and presence and possibility of development of countermeasures by attackers(Bhatnagar et al., 2018). Additionally, the growing use of AI in this field undoubtedly leads to the growth and changes in cyber-attacks. For instance, expansion of existing threats due to the lowered costs of attacks or change to the typical character of threats due to the AI features itself. The possible changes in the cyber threats because of the use of AI can be illustrated through three main security domains, such as digital, physical, and political (Bhatnagar et al., 2018).

1. Digital security. The current trade-off between attack effectiveness and scalability will be reduced by using AI to automate cyberattack-related chores. This could increase the risk of labor-intensive cyberattacks (like spear phishing). It is also reasonable to anticipate new attacks that take advantage of software flaws (automated hacking), human weaknesses (speech synthesis used for impersonation), or AI system vulnerabilities (data poisoning and adversarial examples).

2. Physical security. The hazards connected to drone attacks could increase if artificial intelligence (AI) is used to automate processes related to carrying out attacks using drones and other physical systems (e.g., through the deployment of autonomous weapons systems). It is also reasonable to anticipate fresh attacks that utilize physical systems that would be impossible to control remotely, such as a

swarm of thousands of micro-drones, or manipulate cyber-physical systems, like crashing autonomous cars.

3. Political security. The possibilities of privacy invasion and social manipulation may increase if AI is used to automate operations related to surveillance (e.g., analyzing mass-collected data), persuasion (e.g., developing targeted propaganda), and deception (e.g., editing films). Furthermore, it is reasonable to anticipate new attacks that capitalize on the enhanced ability to examine human emotions, behaviors, and beliefs using the data at hand. While these issues are particularly important in the setting of authoritarian nations, they may also make it more difficult for democracies to continue having honest public discussions.

Concluding, the role of AI in countering cyber threats is pivotal in addressing the ever-evolving landscape of digital risks and vulnerabilities. AI-powered technologies offer unprecedented capabilities in detecting, mitigating, and responding to cyber-attacks with speed and accuracy. From automated threat detection to adaptive defense mechanisms, AI strengthens cybersecurity across various domains, including corporate networks, financial institutions, state information systems, and the personal privacy of users. However, the widespread adoption of AI in cybersecurity also presents challenges and threats, such as ethical considerations, dependence on data accuracy, and the possibility of adversarial exploitation.

References

1. Agrawal, J., Kalra, S. S., & Gidwani, H. (2023). AI in cyber security. *International Journal of Communication and Information Technology*, *4*(1). https://doi.org/10.33545/2707661x.2023.v4.i1a.59

2. Bhatnagar, S., Cotton, T., Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Carrick, J. S., Seán, F., Héigeartaigh, Ó., Beard, S., … Amodei, D. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation Authors are listed in order of contribution Design Direction. *ArXiv Preprint ArXiv:1802.07228*, *February 2018*.

3. 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). https://doi.org/10.5121/ijsea.2022.13502

4. Kadel et al., (2023). Emergence of AI in cyber security. *International Research Journal of Modernization in Engineering Technology and Science*. https://doi.org/10.56726/irjmets32643

5. Ghelani, D. (2022). X(X): XX-XX Diptiben Ghelani. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal*

of Science, Engineering and Technology, *3*(6), 12–19. https://doi.org/10.11648/j.XXXX.2022XXXX.XX

6. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*. https://doi.org/10.1016/j.egyr.2021.08.126

7. Tao, F., Akhtar, M., & Jiayuan, Z. (2021). The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey. *EAI Endorsed Transactions on Creative Technologies*, *8*(28). https://doi.org/10.4108/eai.7-7-2021.170285