ТЕХНОЛОГІЇ ЯК ФАКТОР ЕКОНОМІЧНОГО ЗРОСТАННЯ

UDC 004.89
JEL Classification: O33, M21
DOI: https://doi.org/10.20535/2307-5651.30.2024.313042

Zavrazhnyi Kostiantyn
PhD in Economics, Junior Researcher of the Department of Economics,
Entrepreneurship and Business Administration
(corresponding author)
ORCID ID: 0000-0002-0408-0269
Kulyk Anzhelika
PhD Student of the Department of Financial Technologies and Entrepreneurship
Sumy State University
ORCID ID: 0009-0009-0743-8973

Завражний К. Ю.
кандидат економічних наук, молодший науковий співробітник
кафедри економіки, підприємництва та бізнес-адміністрування
Кулик А. К.
аспірантка кафедри фінансових технологій і підприємництва
Сумський державний університет

MODERN BUSINESS CYBERSECURITY CHALLENGES AND THE ROLE OF ARTIFICIAL INTELLIGENCE IN COUNTERING THREATS[1]

СУЧАСНІ ВИКЛИКИ КІБЕРБЕЗПЕКИ БІЗНЕСУ ТА РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОТИСТОЯННІ ЗАГРОЗАМ

Business cybersecurity involves the protection of its important interests when using cyberspace, as well as timely detection, prevention and neutralization of real and potential threats. Digital transformation has led to an increase in cyberattacks on enterprises with an unprecedented number of attack routes. Lack of scalability, slow response time, and inability to detect modern and insider threats are some of the problems of traditional approaches to network security. These shortcomings highlight the need for research to create more effective protection methods and develop recommendations for improving cyber hygiene among employees. Artificial intelligence is one of the best technologies for detecting and preventing unexpected risks that can engulf a business. This study provides detailed information on the implementing of cyber threat protection systems to help companies minimize the risks of cyberattacks, identity theft and other online fraud. The research findings show that artificial intelligence is able not only to automatically identify anomalies in the behavior of users and systems, but also to provide a timely response to threats. By identifying and addressing security gaps in time, businesses will be able to increase the cyber resilience of their automated systems.

Keywords: *cybersecurity, cyberattack, business, artificial intelligence, cyber resilience.*

Кібербезпека бізнесу передбачає захист його важливих інтересів при використанні кіберпростору, а також своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз. Цифрова трансформація призвела до збільшення кількості кібератак на підприємства з безпрецедентною кількістю маршрутів атак. Відсутність масштабованості, повільний час реагування, нездатність виявляти сучасні та інсайдерські загрози – це деякі з проблем традиційних підходів до мережевої безпеки. Ці недоліки підкреслюють необхідність проведення досліджень для створення більш ефективних методів захисту та розробки рекомендацій щодо покращення кібергігієни серед співробітників. Штучний інтелект є однією з найкращих технологій для виявлення та запобігання неочікуваних ризиків, які можуть охопити бізнес. Це дослідження надає детальну інформацію про впровадження систем захисту від кіберзагроз, які допоможуть компаніям мінімізувати ризики кібератак, крадіжок персональних даних та інших видів онлайн-шахрайства. Результати дослідження показують, що штучний інтелект здатний не тільки автоматично виявляти аномалії в поведінці користувачів і систем, але й забезпечувати своєчасну реакцію на загрози. Вчасно виявляючи та усуваючи прогалини в безпеці, підприємства зможуть підвищити кіберстійкість своїх автоматизованих систем.

Ключові слова: *кібербезпека, кібератака, бізнес, штучний інтелект, кіберстійкість.*

[1] The paper is prepared within the scientific research project "Fulfillment of tasks of the perspective plan of development of a scientific direction "Social sciences" Sumy State University" (№ 0121U112685).

Formulation of the problem. Digital transformation provides new opportunities and benefits for businesses, reducing costs and increasing labour efficiency, but at the same time increases vulnerability due to cyber challenges. Cyberthreats are consistently ranked among the biggest global security risks by the World Economic Forum [1]. Cybercrime is rapidly growing in scope and scale against the backdrop of geopolitical conflicts, causing serious financial losses to businesses and violating the privacy of individuals.

According to research, since 2022, Ukraine has become the most attacked country in the world, in 2023 the number of hacks increased by 62.5%, Ukrainian business suffers about 148,000 registered cyberattacks annually, which significantly increases the risks for all companies [2]. In this context, cybersecurity, which responds to threats with all possible tools: from risk assessment, implementation of appropriate protection measures, proper configuration of IT infrastructure, to correct instructions to employees, becomes an integral part of business processes.

Artificial intelligence is a key technology of our time that can protect businesses from cyberattacks, including detecting network intrusions, malware, spam, and analyze network traffic. AI-based cybersecurity systems remain stable during hostile attacks, are adaptive, and can learn from each attack to autonomously improve defensive capabilities. The technology helps cybersecurity systems withstand an attack. One of the most important elements of sustainable cybersecurity systems is the identification of cyberthreats, which can be done with the help of AI-based anomaly detection algorithms [3].

This paper is devoted to the analysis of modern cyberthreats and increasing the resilience of companies' cybersecurity systems using artificial intelligence.

Analysis of the recent research and publications. The conducted analysis shows that the regulatory and legislative acts of Ukraine define cybersecurity as the protection of the vital interests of a person and citizen, society and the state during the use of cyberspace, ensuring the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential cyberthreats to the national security of Ukraine [4]. Research on the problems of protecting business from cyber threats is carried out by such scholars as Biliavska Yu. [5], Shestak Ya. [5], Shostak L. [6], Fedoniuk A. [6], Pomazun O. [6], Jain V. [7], Chouhan S. [7], Kate V. [7], Nigam N. [7], Bhalerao S. [7].

For the analysis of the latest research and publications, 106 English-language publications in periodical scientific journals indexed by the scientometric database Scopus [8] were selected for 2018-2024. Relevant articles were found by combining the keywords «cyberthreat» – «business» – «artificial intelligence» – «cybersecurity». Using the method of relationship density, the VOSviewer software structured the 49 keywords and grouped them into five clusters.

The first cluster (highlighted in red) includes 16 items with the main keyword «big data». The group covers research on the technical characteristics of systems that become targets of cyberattacks, their vulnerabilities, as well as the measures used to protect them. The second cluster (highlighted in green) contains 12 items with the main keyword «artificial intelligence». This cluster focuses on the implementation of artificial intelligence and the ethical issues of cyber security. The third cluster (highlighted in blue) unites 9 elements, with the main keyword «network security». The set is focused on methods for detecting and protecting against cyber attacks. The fourth cluster (high-

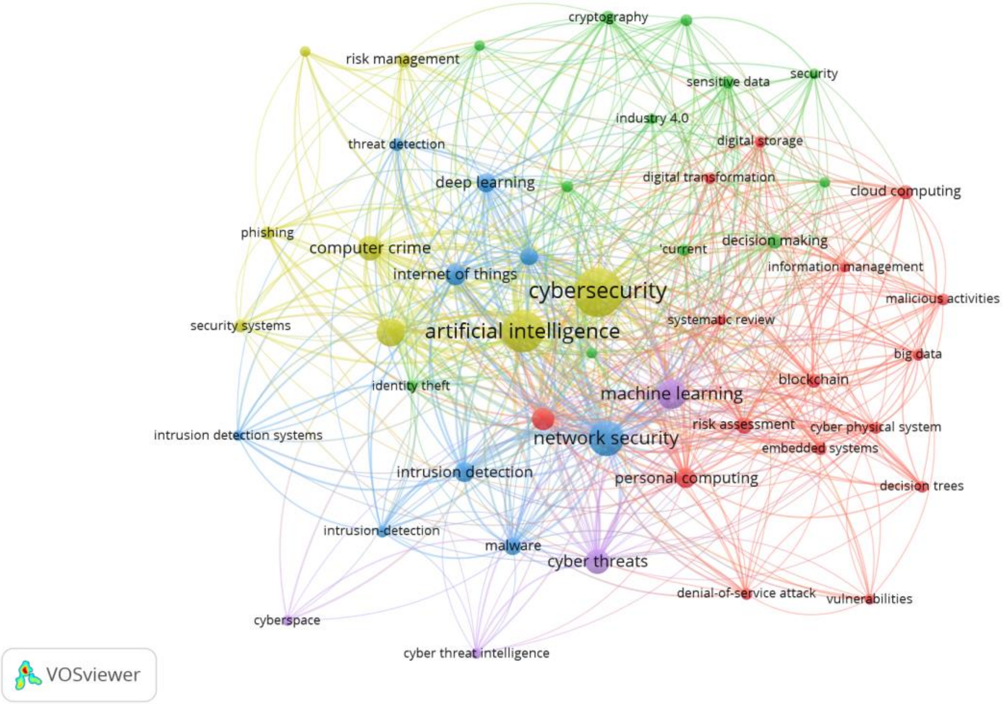

Figure 1. Co-occurrence network «cyberthreat – business – artificial intelligence – cybersecurity»

Source: compiled by the authors using VOSviewer based on Scopus publications lighted in yellow) includes 8 items with the main keyword «cybersecurity». This group covers general cybersecurity and risk management issues. The fifth cluster (highlighted in purple) contains 4 items with the main keyword «machine learning». This cluster focuses on intelligent systems for detecting and analyzing cyber threats.

The co-occurrence analysis identifies the key concepts in research related to business, artificial intelligence and digital transformation. Artificial intelligence and machine learning are becoming important tools for improving cybersecurity, while cyberattacks and cybercrime remain serious threats.

The keywords from the analyzed array of publications that were mentioned most often, their belonging to the cluster, the number of mentions and the indicator of the overall strength of the connection are shown in Table 1.

The results of the bibliometric analysis show a significant increase in the number of publications over the past four years, which indicates the relevance of the problem for the scientific community.

Highlighting previously unresolved parts of the general problem and formulating the goals of the article. Despite the big amount of research in the field of cybersecurity, there are a number of unsolved problems in protecting the digital ecosystems of modern businesses. One such challenge is the lack of effectiveness of traditional security methods in detecting and responding to complex attacks such as Advanced Persistent Threats (APT), phishing and malware. The goal of this research is to analyze modern cyberthreats, evaluate existing methods for protecting information systems, networks and data, and develop recommendations for increasing enterprise protection using artificial intelligence (AI)-powered cybersecurity models.

Presentation of the primary research material. In today's digital world, most companies process important information in cyberspace, the leakage or theft of which has serious consequences, such as complete or partial failure of the system, financial losses, and loss of customer and partner trust. The most common types of cyberthreats include malware, phishing, hacker attacks, data leakage, denial of service (DoS), account or system compromise. The aim of attackers is reconnaissance operations, long-term espionage, destruction of data and information systems. A cyberattack can exploit any organization's resources, including software, hardware, networks, data, personnel, physical security, and more. For example, a cyberattack on a power grid could lead to massive power outages, and an attack on a bank could leave customers unable to access their accounts. Criminals can steal or destroy personal information, financial data, intellectual property or other critical data of their victims, use infected systems to send spam, spread malware, track user activity.

Table 2 shows common methods cybercriminals use to initially contact victims and gain access to their systems, data, or resources.

One of the most complex types of cyberattacks is the Advanced Persistent Threat (APT). This form is characterized by the high level of professionalism and expertise of the attackers, the long time during which the criminals penetrate the system, explore it and collect confidential information, and use various methods and tools to avoid detection and the implementation of protective mechanisms. These attacks include several steps, which are described in Table 3.

The digital transformation of business has increased the popularity of remote work and the need for cloud technologies to keep companies and their employees connected. The transition to cloud services and remote work has led to an increase in the number of cyberattacks that use easily accessible malware. In addition, the growth of computing power available for scaling and automating cyberattacks has opened an unprecedented number of avenues for attacks to hackers [9].

According to statistics, in 2023, 48% of small and medium-sized enterprises (SMEs) became the objects of cyberattacks, 25% experienced more than one such incident during the year. Most violations are system intrusions, social engineering, and attacks on basic web applications. Figure 2 presents the most common consequences of intervention in the information systems of small enterprises [10].

Statistics show that SMEs are more vulnerable to cyberattacks than large corporations. Data vulnerability: 87% of these businesses collect or process customer data that can be hacked, 46% do not use firewalls, and 42% do not back up important data. Insufficient access control and monitoring: only 57% of small and medium-sized enterprises control the security of remote work, and 24% of small business owners send phishing test emails to their employees. 56% of small business owners conduct cybersecurity training for their employees once a year, and only 8% of businesses with less than 50 employees have a dedicated cybersecurity budget [10].

To protect against and respond effectively to cyberattacks, every business must develop comprehensive cybersecurity strategies. The aim of the cyber protection system is to ensure the confidentiality, integrity and availability of data, the normal operation of digital infrastructures: data protection from unauthorized access, unauthorized modification or destruction, ensuring access to data for authorized users, protecting systems from failures and ensuring their continuous operation, restoring systems after cyber-

Table 1

Analysis of the ten most mentioned keywords of the co-occurrence network «cyberthreat – business – artificial intelligence – cybersecurity»

Keyword	Cluster	The overall strength of the connection	The number of mentions of the term
Cybersecurity	4	851	137
Artificial intelligence	2	349	59
Network security	3	298	41
Machine learning	5	299	43
Cyberattacks	4	195	26
Computer crime	4	151	20
Cyberthreats	5	121	20

Source: compiled by the authors

Table 2

Methods of initial interaction between criminals and victims

Method	Description	Prevention of risks
Exploitation of vulnerabilities	Criminals look for and exploit vulnerabilities in a victim's software, systems, or networks to gain access, install malware, or steal data.	Regularly update software, conduct security audits, use reliable firewalls.
Phishing	Criminals send fraudulent emails, messages, or create fake websites to trick a victim into revealing personal information or downloading malware.	Educating and training employees to detect phishing attacks, filtering spam and phishing.
Using stolen accounts	Criminals gain access to a victim's accounts using stolen passwords or other data, allowing them to access the victim's systems or data.	Using strong and unique passwords, using multi-factor authentication (MFA), changing passwords regularly.
Returns	Criminals use already infected systems to further infiltrate the network or attack other systems.	Network segmentation, network traffic monitoring implementation, user behavior analysis.
Website compromise	Criminals attack websites to infect them with malware or steal user data.	Web application protection with firewalls (WAF) and intrusion prevention systems (WIPS), regular website and software updates.
Attacks through contractors	Criminals attack third-party contractors who have access to the victim's systems or data.	Inclusion of cybersecurity requirements in contracts with contractors, monitoring of contractors' activities.
Brute force selection	Criminals use software to go through all possible password combinations to gain access to a victim's account.	Using complex passwords and limiting the number of login attempts.

Source: compiled by the authors

Table 3

Stages of an APT attack

Stage	Description
Preparation	The criminal gathers information about the target, researches its security systems, and develops an attack plan. This can include network scanning, vulnerability scanning, credential theft, or even physical surveillance of an object.
Penetration	The criminal uses various methods such as social engineering, exploiting vulnerabilities or phishing to penetrate the victim's systems.
Capturing	The criminal takes control of the infected systems, configures backdoors, hides presence. This can include obtaining administrative rights in the system, creating hidden communication channels, encrypting the victim's data, installing malware.
Culmination	The criminal achieves the goal, which may include data theft, espionage, sabotage of critical infrastructures.

Source: compiled by the authors

attacks or other emergency situations. An effective cyber defense system must be built with three main components: people, processes and technology. All employees should be involved in ensuring the security of the enterprise.

Protecting data from unauthorized access, loss, damage, or disclosure plays a significant role in building an enterprise's cyber defences. Implementation of technical security measures (firewalls, anti-virus software, data encryption), use of security policies and procedures (password policy, cybersecurity training, incident response plan), employee training reduces the risks of information leakage and other incidents. Data encryption is an important tool for protecting confidential information. Encrypted files on computers, mobile devices, or external storage devices provide protection in case of device loss or theft. Only authorized users will be able to decrypt and read these files. Establishing a multi-level data access system helps reduce the risk of internal threats and user errors, allows to effectively control and manage access to confidential information, providing an additional level of protection. Backup allows to restore lost or damaged information with minimal effort. Backups can be stored on external media, such as external hard drives or USB drives, or in cloud storage, providing an additional layer of protection against physical threats such as fire or theft.

Anti-virus software protects systems from various types of threats, helping to detect and block malware that can damage or steal data. An important element in the overall cybersecurity strategy is users who can apply their knowledge and skills to detect and prevent threats. Increasing user awareness and skills is a key step in strengthening cyber hygiene and cyber resilience. Also, a necessary component of a business protection strategy is cybersecurity analysis, which consists of collecting information about systems, vulnerability testing, risk assessment and social engineering.

The implementation of artificial intelligence provides an opportunity for enterprises to improve cybersecurity measures, to ensure the reliability and stability of the digital environment. An intrusion detection system (IDS) plays an important role in the resilience of business protection against cyberattacks. Traditional IDS have limitations: inability to identify new attacks, low accuracy, high number of false alarms.

Criminals have created sophisticated malware that uses stealth techniques, often making it difficult to iden-

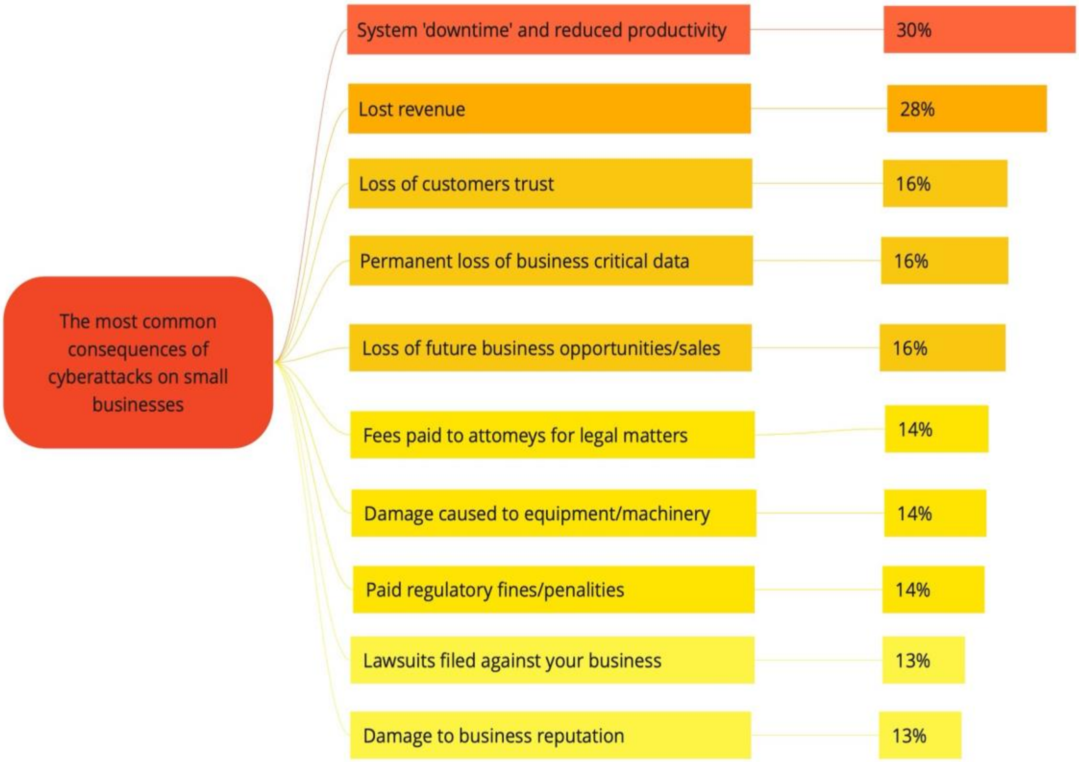

Figure 2. The most common consequences of cyberattacks

Source: compiled by the authors

Table 4

Describes a comprehensive cybersecurity strategy that will help businesses protect data and systems from cyberattacks

Stage	Action	Description
Cybersecurity campaigning	Developing and distributing desktop materials.	Creation of informative booklets, posters and other materials that familiarize employees with the main cyberthreats, security rules and data protection recommendations.
	Internal information campaigns.	Organization of information campaigns using email, corporate website, internal chats and other communication channels to constantly remind about the importance of cybersecurity.
Formalizing cybersecurity	Development of information security policy.	Defining clear rules and procedures that govern access to data, use of computer systems, information sharing, and other elements of cybersecurity.
	Implementation of technical standards.	Setting standards for the use of software, passwords, and network connections.
Review processes and tools	Risk assessment.	Conducting a comprehensive cyber security risk assessment to identify potential threats, vulnerabilities and potential consequences of cyberattacks.
	Implementation of security measures.	Installing reliable anti-virus software, firewalls, intrusion detection systems (IDS) and other security tools.
	Data encryption.	Use encryption to protect sensitive data both at rest and in transit.
	Backup and restore.	Regular creation of backup copies of data and ensuring the possibility of their quick recovery in the event of a cyberattack.
Implementation of trainings and simulations	Training sessions.	Regular training for staff on cybersecurity, covering topics such as identifying cyber threats, using safe online practices, and recognizing phishing attacks.
	Conducting simulations.	Development of cyberattack simulations to test employee readiness to respond to real cybersecurity incidents.
	Staff training.	Providing training on recognizing and avoiding social engineering techniques used by fraudsters to gain access to confidential information.
Continuous monitoring support	Involvement of experts.	Getting advice on implementing an effective cybersecurity strategy, engaging external experts to constantly monitor cyberthreats, identify vulnerabilities and provide recommendations for their elimination.
	Creation of a cybersecurity committee.	Providing leadership and coordination of efforts to improve enterprise cyber resilience.

Source: compiled by the authors

tify changes to the system. AI-based detection algorithms can identify all forms of malicious activity and have higher detection accuracy than traditional IDS. The use of AI makes it possible to automatically respond to cyberincidents, such as blocking suspicious IP addresses or removing malware. To increase the overall stability of the security system, we recommend that enterprises use IDS based on AI algorithms.

Modern AI-based intrusion detection systems offer reliable protection against cyberattacks by detecting anomalies and malicious behaviour. The ability to collect and analyze information about previous attacks, propose solutions based on this data, constantly monitor the network, adapt to new and changing cyberthreats, predict future attacks and propose solutions to combat threats gives them an advantage over traditional protection methods [11]. AI-powered solutions help identify similarities between multiple attacks that have occurred in the past and instantly warn about detection of such an attack. AI can continuously decipher user behaviour, changing usage patterns, and all types of breaches. This systems can automate the process of scanning networks for vulnerabilities, identify potential threats, and initiate risk mitigation measures such as automatic software updates or blocking malicious IP-addresses. This level of automation not only increases the efficiency of cybersecurity processes, but also ensures their consistency and unification

In addition, the automation of tasks with the help of artificial intelligence will allow enterprises to reduce the costs of cybersecurity experts and physical resources for 24/7 network monitoring. Thus, the implementation of AI has a positive effect on the stability and reliability of the cyberspace security system of modern business.

Conclusions. Enterprise cybersecurity is a topical issue. Criminals are constantly improving their techniques, so defences against cyberthreats must be constantly updated. Cybersecurity requires a comprehensive approach that includes the use of the latest technologies, such as artificial intelligence, to improve system efficiency, and the implementation of well-defined awareness and employee training programmes to reduce costs and incidents.

Businesses can use AI to improve their cyber resilience, protect sensitive data and ensure the long-term stability of digital operations. By implementing AI-powered cybersecurity measures, companies can better defend against complex and evolving cyberthreats, including advanced persistent threats (APT), phishing, and malware attacks.

Timely detection of threats and attacks, before they cause damage to the system, is the main task of enterprise cybersecurity. The AI-based approach not only responds to threats, but also conducts analysis to prevent future attacks, making it superior to traditional security methods.

Future research will explore the possibilities of using hybrid systems that combine the advantages of traditional cybersecurity methods with the capabilities of artificial intelligence. It should also focus on the use of AI to detect and neutralize new types of cyberthreats, such as attacks on artificial intelligence.

References:

1. The Global Risks Report 2022. World Economic Forum. Available at: https://www.weforum.org/reports/global-risks-report-2022/ (accessed: 19.07.2024)

2. Interfax-Ukraine. Available at: https://interfax.com.ua/news/interview/911979. html (accessed: 19.07.2024)

3. Schmitt, M. (2023). Securing the digital world: protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration,* vol. 36. DOI: https://doi.org/10.1016/j.jii.2023.100520 (accessed: 19.07.2024)

4. On the basic principles of cybersecurity in Ukraine. (2017). Law of Ukraine, № 2163-VIII. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text (accessed: 19.07.2024)

5. Biliavska, Ju. & Shestak, Ja. (2022). Cyber security and cyber hygiene: the new era of digital technologies. *International scientific and practical journal «Commodities and Markets»*, vol. 3(43). DOI: https://doi.org/10.31617/2.2022(43)04 (accessed: 19.07.2024)

6. Shostak, L., Fedoniuk, A. & Pomazun O. (2024). Features of business cyber security in wartime conditions. *Digital economy and economic security*, vol. 3 (12). DOI: https://doi.org/10.32782/dees.12-22 (accessed: 19.07.2024)

7. Jain, V., Chouhan, S., Kate, V., Nigam, N. & Bhalerao, S. (2023). Enhancing data security and data sensitivity: leveraging the synergy of blockchain artificial intelligence. *IEEE International Conference on ICT in Business Industry & Government (ICTBIG).* DOI: https://doi.org/10.1109/ICTBIG59752.2023.10456105 (accessed: 19.07.2024)

8. Scopus. Available at: https://www.scopus.com/search/form.uri?display=basic&zone=header&origin=searchbasic#basic

9. Stone, B. (2024). Cyberattacks on SMBs are increasing, will your business be ready? *TechRepublic.* URL: https://www.techrepublic.com/article/cyberattacks-on-smbs-are increasing-will-your-business-be-ready/ (accessed: 20.07.2024)

10. Smith, G. (2024). +50 cyberattacks on small businesses statistics. *StationX.* Available at: https://www.stationx.net/cyber-attacks-on-small-businesses-statistics/

11. Al-garadi, M., Mohamed, A., Al-ali, A., Du, X., Guizani, M. (2019). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Xplore,* vol. 22 (3). DOI: https://doi.org/10.1109/COMST.2020.2988293 (accessed: 19.07.2024)

Стаття надійшла до редакції 10.09.2024
Стаття опублікована 09.10.2024