# Building Digital Safety amid Technological Modernization and New Challenges for Management Strategy

**Serhii Lysenko [1*], Olha Verba [2], Viktor Kyrychenko [3], Vitaliy Gandziuk [4], Iryna Odobetska [5]**

[1] Institute of Security, Interregional Academy of Personal Management, Kyiv, Ukraine.
[2] Department of Civil Law Disciplines, Institute of Law, Lviv State University of Internal Affairs, Lviv, Ukraine.
[3] Department of Computer Science, Faculty of Information Technologies, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine.
[4] Department of Journalism, Advertising and Public Relations, Faculty of Philology and Journalism named after Mykhailo Stelmakh, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, Ukraine.
[5] Department of Journalism, Advertising and Public Relations, Faculty of Philology and Journalism named after Mykhailo Stelmakh, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, Ukraine.
* Corresponding author: crimeconsult@ukr.net


OIDA International Journal of Sustainable Development, Ontario International Development Agency, Canada.
ISSN 1923-6654 (print) ISSN 1923-6662 (online) www.oidaijsd.com
Also available at https://www.ssrn.com/index.cfm/en/oida-intl-journal-sustainable-dev/

**Abstract:** The information security system combines diverse strategies for interaction in today's digital society, which necessitates further research into the current risks associated with information protection. Increased risks of confidential information leaks and manipulation in the media space require a transformation of approaches to security guarantees. The purpose of this article is to analyze modern approaches to cybersecurity risk management. The study identifies current challenges in the field of cybersecurity and the most effective strategies for overcoming them, including through the use of artificial neural networks, blockchain, and monitoring systems. The features of the formation of comprehensive information protection systems are analyzed. The potential of cyber defense systems in a number of countries is compared using the National Cyber Security Index (NCSI). It is established that the potential consequences of cyberattacks exceed the predicted losses, especially in the case of threats to government websites, the financial sector, IT companies, media resources, and energy companies. The need for active interaction between the authorities, business, and the public in the field of information security risk management against the backdrop of the rapid digitalization of the information and communication field was substantiated. The significant role of the social context in shaping information security strategies has been noted, which involves combating information overload and digital stress, preventing cyberbullying and cyberaddiction, information manipulation, and confidential data leaks. It is argued that information security risk management requires the integration of effective educational strategies for developing resilience and psychological concepts of digital security.

**Keywords:** security, cyber threats, risk management, protection strategies, resilience, confidentiality, information.

## Introduction

Cyberattacks provoked by Russia in the Ukrainian information space are a striking example of the capabilities of modern cyber threats: sending emails with integrated malware from fake senders (Amazon, Microsoft); destruction of 40% of the digital infrastructure of the Kyivstar company [1]. At the same time, Russian hackers managed to carry out phishing attacks on German political parties [2]. It is clear that global crisis challenges to information security determine the need to improve risk prevention and resilience strategies, ensuring an active role for society in security strategies for interaction.

This issue has been reflected in numerous publications by contemporary researchers. In particular, the works of Roy [3], Dhillon et al. [4] examine the specifics of building society's resilience to new threats in the digital information and communication environment and explore the potential of modern strategies for preventive resilience of the

confidential information field. Some scholars [5, 6] focus on innovative methods of data protection in the digital environment.

Given the relevance of the issues under study and the importance of their effective resolution for strengthening personal and general information security, the development of risk management strategies will optimize existing information security concepts and ensure readiness for new cyber threats against the backdrop of geopolitical dynamics.

**Literature review**

A number of recent publications, including Alahmari and Duncan [7], are devoted to cases of innovative experience in the field of information security in the digital sphere. Researchers focus on innovative aspects of strategic management in the field of security and the development of digital inclusion in the public environment. The issue of the effectiveness of public-private interaction in the field of information security risk management is considered by Figueira et al. [8], who emphasize the importance of adhering to the principles of coordination of strategic industry documents, as well as control over the implementation of infrastructure projects in the digital information and communication space.

The issue of improving certain aspects of methodological support for information security in the public sector is considered in the publications by Singgalen et al. [9]. The authors emphasize the need to create guarantees for the information security of critical infrastructure. Continuing this theme, Nobles [10] analyzes modern security management strategies based on the relationship between digitalization and human resource management. The author considers IT technologies to be the main guarantors of information security in the context of increased risks of cyberattacks and justifies the need to develop the digital competence of the human capital of modern companies.

Ali et al. [11] update strategies for digitizing information and using blockchain and cloud solutions. The researchers conducted a critical review of developments in information system security and determined the specifics of strategies for ensuring confidentiality against the backdrop of integration and globalization processes.

Cartwright et al. [12] consider innovative IDS systems that are currently actively used for traffic analysis and cyberattack prevention. The researchers propose actively using the capabilities of artificial intelligence, equipping it with the functionality to develop the foundations of digital law for the purpose of comprehensive legislative regulation of information security. At the same time, there are a number of gaps that need to be filled in order to gain a more complete understanding of the nature of the impact of management processes on the formation of information security strategies in the context of digital development.

*Aims.* The aim of this article is to analyze modern approaches to cybersecurity risk management.

**Materials and methods**

*Design and scope of the study.* The research focuses on the peculiarities of forming complex information protection systems in the dynamic digital environment. Considerable attention is paid to the potential of risk management in the field of cyber security and the most effective strategies for overcoming them, including through the use of artificial neural networks, blockchain, monitoring systems, and increasing the resilience and awareness of human capital.

*Data collection and sources.* The study primarily involved a systematic and comprehensive analysis of scientific publications, research papers, and key global security trends based on industry statistics. Relevant primary sources from publications indexed in leading databases (Scopus, Web of Science) were used. The works taken into account were mostly published between 2020 and 2025. The criteria for inclusion and exclusion of publications were the spatial-temporal indicator and the level of reliability of information. The keywords “security, cyber threats, risk management, protection strategies, resilience, confidentiality, information” were used for the search.

*Evaluation criteria.* The limitations of the study are due to the complexity of experimental verification of theoretical conclusions.

*Analytical basis and methods.* The research methodology consists of a number of general scientific methods, including analysis and synthesis, comparison, systematization, generalization, and abstraction. These methods made it possible to trace the causal relationships between the influence of individual factors and the level of effectiveness of object and data protection strategies, determine the main criteria and definitions, and identify the most influential factors on the effectiveness of security strategies. In addition, scientific abstraction was used to detail the conceptual basis of security management mechanisms and strategies against the backdrop of innovative threats.

**Results**

The development of digital infrastructure requires active practical interaction between the public sector, business, the scientific community, and the general public. The transformation of social processes creates a need for adequate management to protect confidential data and digital infrastructure.

Against this backdrop, research into national cyber defense capabilities is becoming increasingly relevant, as reflected in the relevant rankings (Figure 1).

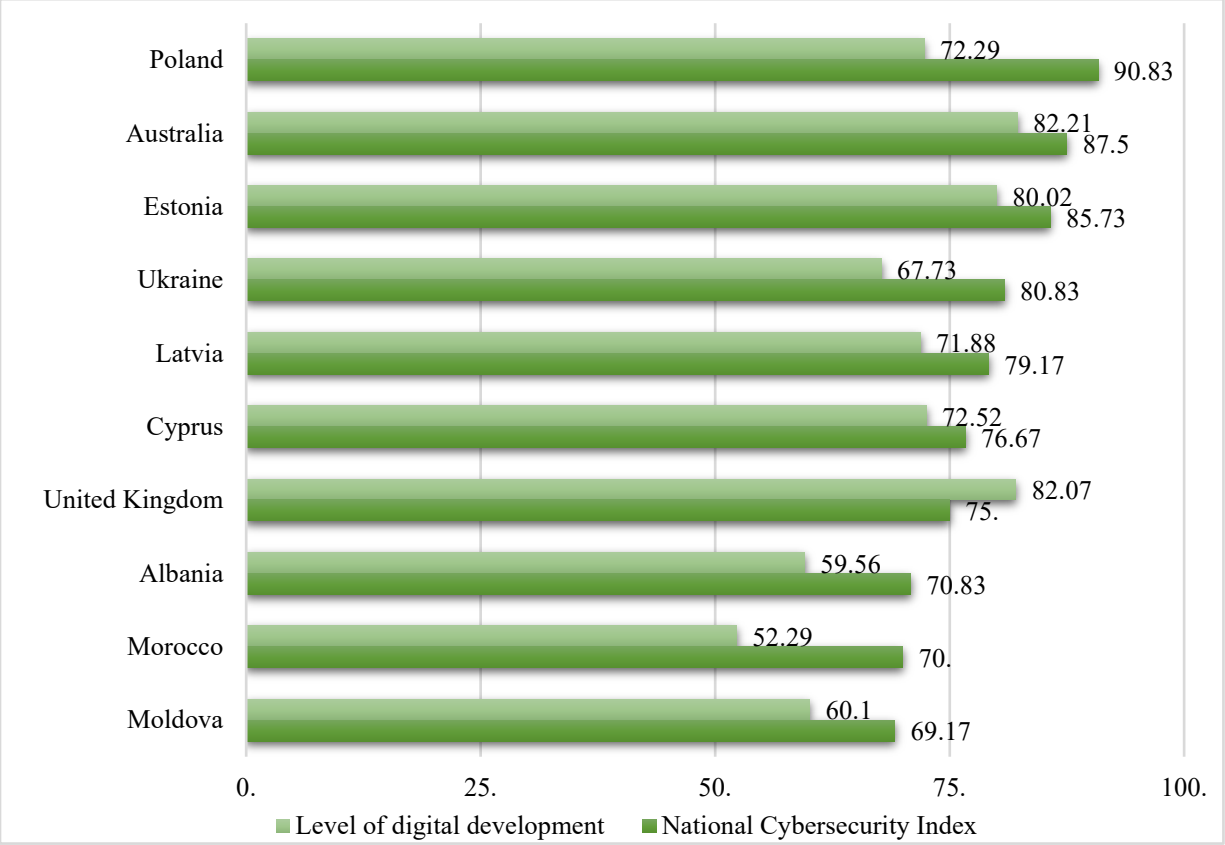


**Figure 1.** NCSI cybersecurity rating and digital development level, 2023
Source: NCSI [13]

An analysis of the areas most vulnerable to Russian cyberattacks in Ukraine (Figure 2) highlights the urgent need to introduce electronic identification and innovative protection methods.

Next Page

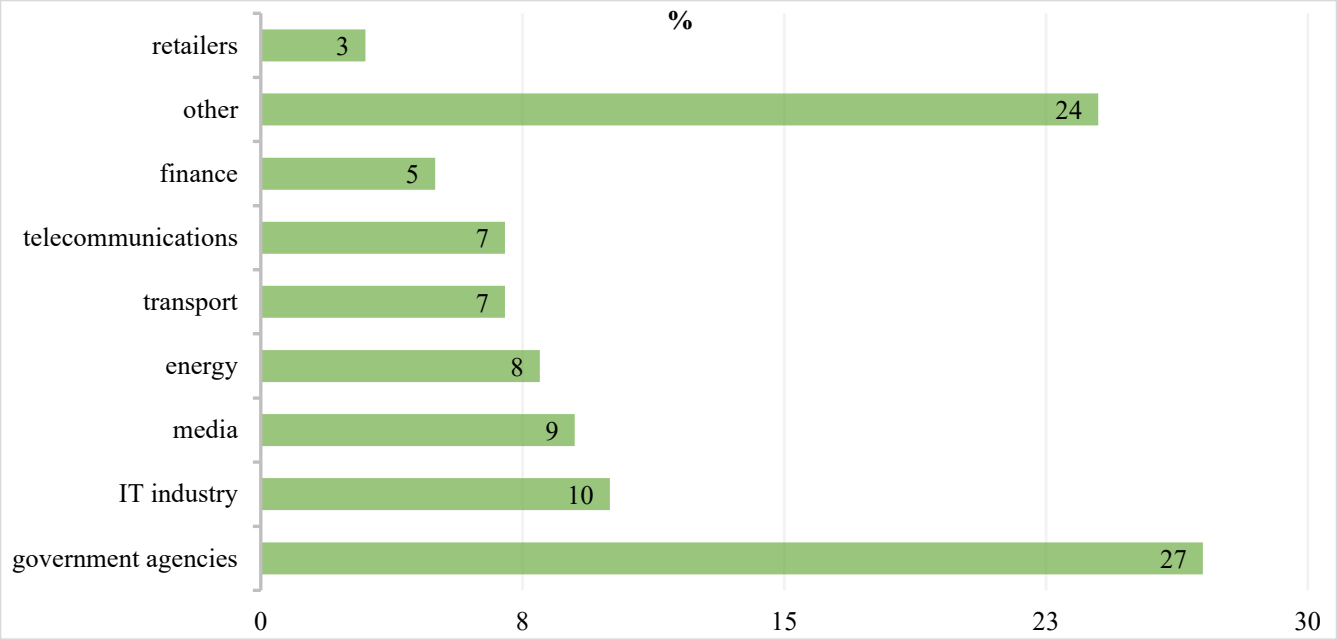


**Figure 2.** Differentiation of industries by number of cyber attacks in Ukraine, %
Source: Microsoft Digital Defense Report [1]

The situation requires a dynamic strategy to mitigate cyber threats based on coordinated communication and coordination of risk management efforts. Modern solutions must include the modernization of administrative, technical, and legal procedures. Priority management approaches include:

- introduction of state projects to enhance cyber resilience and implementation of international security standards;
- integration of effective monitoring systems;
- outsourcing of cyber security specialists for auditing and developing protective strategies;
- development of international cooperation;
- introduction of modern encryption systems, cyber incident identification, and multi-level authentication.

Modern integrated information security systems (IISS) currently have particular potential, as they provide for active interaction with international institutions, monitoring, and outsourcing. Organizational management measures within ISMS include the development and implementation of an effective cyber threat response plan, the integration of the concept of administration, use, and destruction of information carriers, and the development of digital competencies of human capital.

A systematic management approach to ensuring information security should include preventive risk assessment, multi-factor analysis of strategies to mitigate risks, consideration of economic feasibility, and determination of the possibility of adaptive strategy dynamics. At the same time, the main principles of ISMS are considered to be consistency, comprehensiveness, flexibility, and openness.

Against the backdrop of active digitalization, the risk management strategy in the public sector provides for regulating access to confidential data, guarantees of protection against unauthorized access, monitoring of system users' activities, ensuring the integrity of critical resources, and managing the resources of a comprehensive protection system. Among modern information protection methods, network protection tools are particularly important, including intrusion detection systems (IDS) and intrusion prevention systems; antivirus software and tools for protection against destructive programs; and systems for identifying and preventing intrusions by monitoring network traffic.

The human factor in cybersecurity focuses on the risks of human error. Human risks are concentrated on shadow IT practices, accidental data leaks or exchanges, disregard for authentication and secure communication protocols, unintentional disclosure of information on social networks, and insider threats. This requires the development of risk awareness among company personnel through targeted training and coaching.

Among the main aspects of information security risk psychology, the most common are personal data theft, information overload and digital stress, technology addiction, cyberbullying, and information manipulation.

Data theft is closely linked to phishing and other social engineering techniques that are often used to obtain confidential information from victims. Information overload is understood as the inability to process information in the volume in which it arrives. Digital stress is an abstract fear of missing information of any degree of importance.

Technological addiction refers to the compulsive and excessive use of digital devices and online platforms, leading to negative consequences for a person's physical, psychological, and social well-being. At the same time, cyberbullying is repeated behavior aimed at intimidating, provoking anger, or humiliating those against whom it is directed, using digital technologies. The key measures for managing the human factor in security strategies are: critical thinking; awareness of the impact of social networks and the development of social support; ensuring data privacy and security.

The potential of artificial neural networks in information security risk management (Figure 3) increases the speed and accuracy of threat identification.

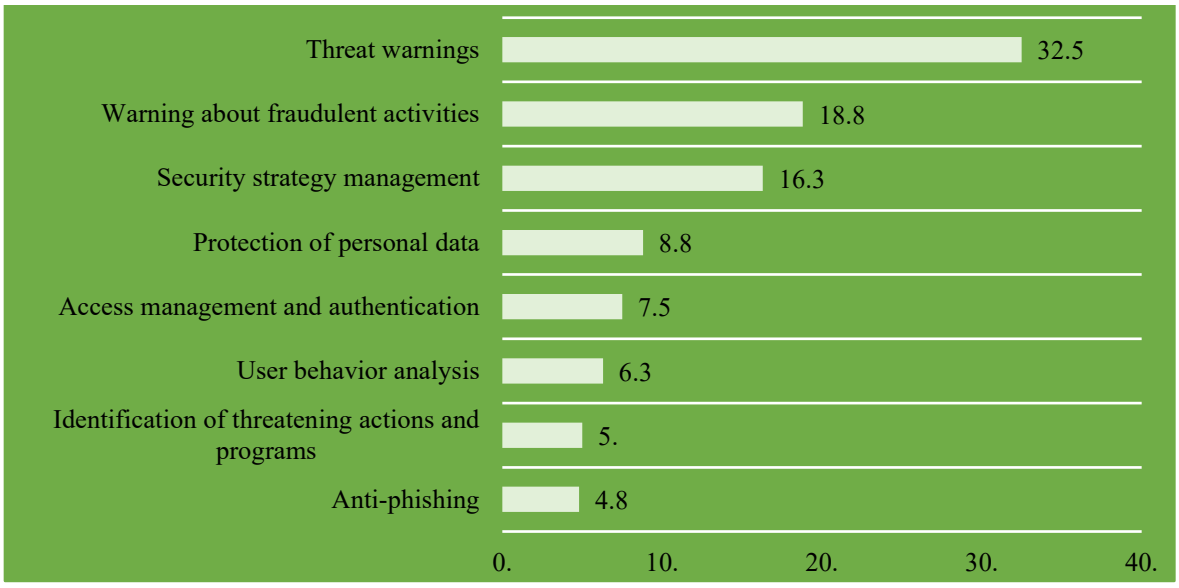


**Figure 3.** Use of artificial intelligence in information security risk management in European Union countries, % Source: Li et al. [14], Kunle-Lawanson [15]

In the context of the psychological aspects of information security risk management, it is necessary to promote the development of sustainable skills in human capital to recognize harmful and threatening types of interactions, develop practices of interaction and resilience through targeted training and coaching, improve digital literacy, and master practical skills in security process management.

**Discussion**

There are various conceptual visions of management strategies in the field of information security in the scientific field. In particular, Fonseca-Herrera et al. [16] highlight the need for an integrated approach to digital communication risk management that includes the potential of blockchain and artificial intelligence, as well as the development of relevant digital skills among employees. As Niu [17] continues, such a strategy should be consistent with the intentions of national cybersecurity policy development and have strong institutional support.

Landoll [18] and Li and Liu [19] study the functioning of international cybersecurity institutions and argue for the adoption and implementation of unified international standards. The authors see their advantages in the maximum representation of society's interests, guarantees of adaptability, transparency, and openness, and the implementation of high standards of information security. Kwateng et al. [20], researching the specifics of the geographical dimension of cyber threats, argue for

the need for public-private partnerships between the state sector, the public, and business. The scientists' proposals are particularly relevant in the context of threatening geopolitical dynamics.

Anu [21], Khosravi-Farmad and Ghaemi-Bafghi [22] have developed a taxonomy for preventing common types of attacks. The researchers emphasize the need to introduce a certification and regulation system in the field of cybersecurity and argue for the priority of investing in the information protection of critical infrastructure.

Kunle-Lawanson [15], Kilincer et al. [23] analyze the potential of artificial intelligence in cybersecurity in terms of security, reliability, maximum personalization of the user experience, and prevention of intrusions into confidential information systems. Scientists are improving the predictive management model, trying to raise awareness of this problem through vulnerability analysis of DMPC methods and the development of appropriate protection mechanisms. It should be noted that the researchers have overlooked the legal, social, and ethical implications, which creates a gap in the research.

The issue of the human factor in security management is a subject of active debate in the modern scientific community. Nobles [10] analyzes the possibilities of improving the security of companies' internal information fields through algorithmization and automation to ensure data confidentiality. It is necessary to agree with the researcher on the need to transform approaches to human capital management in companies against the backdrop of increased risks of information threats. The current study also proposes digitizing data processing to prevent unauthorized access to information.

According to Semenets-Orlova et al. [24], Popov et al. [25], Bakhov et al. [26], Bondarenko et al. [27], and Hren et al. [28], the key benefits of improving the digital skills of personnel are minimizing the risk of data loss. The authors' conclusions should be supplemented by offering targeted training and coaching on information security issues.

Davis et al. [29] highlight the need to develop unified approaches to the psychological basis of information security risk management. At the same time, it is this basis that creates the prerequisites for maintaining balance and resilience to threats in the digital information and communication field. The results of the current study and analysis of previous scientific developments confirm the relevance of comprehensive, person-oriented risk management strategies in information security. A modern cybersecurity management strategy should include several basic components:

- detailed risk assessment to identify potential threats and weaknesses in the management system;
- effective security policy;
- a system for improving the digital competencies of companies' human capital;
- a system for controlling access to confidential resources;
- an analytics and audit system;
- backup programs.

**Conclusion**

An analysis of current approaches to cybersecurity risk management has identified pressing challenges in the field of cyber defense and the most effective strategies for overcoming them, including through the use of artificial neural networks, blockchain, and monitoring systems. Key methods of information protection include cooperation with international institutions, regulatory and legal frameworks that are complementary to global requirements, and improving the digital security skills of human capital.

Against the backdrop of active digitalization, the risk management strategy provides for regulating access to confidential data, guarantees protection against unauthorized access, controlling the activities of system users, ensuring the integrity of critical resources, and managing the resources of a comprehensive protection system. Among modern information protection methods, network protection and intrusion detection tools, antivirus software, and network traffic identification and tracking systems are particularly important.

Human risks are concentrated in shadow IT practices, accidental data leakage or exchange, disregard for authentication and secure communication protocols, unintentional disclosure of information on social networks, and insider threats. This requires developing risk awareness among company personnel through targeted training and coaching. Further research in this area should focus on the impact of human capital's personal motivation on the level of information security in companies.

**References**


[1] Microsoft Digital Defense Report. (2022). https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022

[2] Significant Cyber Incidents. (2025). *CSIS.* https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[3] Roy, P. P. (2020). A high-level comparison between the nist cyber security framework and the iso 27001 information security standard. In *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*. (pp. 1–3). IEEE. https://doi.org/10.1109/NCETSTEA48365.2020.9119914

[4] Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. *The Journal of Strategic Information Systems, 30*(4), 101693. https://doi.org/10.1016/j.jsis.2021.101693

[5] Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. *Digital Communications and Networks, 8*(4), 422–435. https://doi.org/10.1016/j.dcan.2021.07.006

[6] Rass, S., Schauer, S., König, S., & Zhu, Q. (2020). *Cyber-Security in Critical Infrastructures.* Springer International Publishing. https://doi.org/10.1007/978-3-030-46908-5

[7] Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)* (pp. 1–5). IEEE. https://doi.org/10.1109/CyberSA49311.2020.9139638

[8] Figueira, P. T., Bravo, C. L., & López, J. L. R. (2020). Improving information security risk analysis by including threat-occurrence predictive models. *Computers & Security, 88*, 101609. https://doi.org/10.1016/j.cose.2019.101609

[9] Singgalen, Y. A., Purnomo, H. D., & Sembiring, I. (2021). Exploring MSMEs Cybersecurity Awareness and Risk Management: Information Security Awareness. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems), 15*(3), 233–244. https://doi.org/10.22146/ijccs.67010

[10] Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *Holistica Journal of Business and Public Administration, 13*(1), 49–72. https://doi.org/10.2478/hjbpa-2022-0003

[11] Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly, 37*(1), 101419. https://doi.org/10.1016/j.giq.2019.101419

[12] Cartwright, A., Cartwright, E., & Edun, E. S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. *Computers & Security, 131*, 103288. https://doi.org/10.1016/j.cose.2023.103288

[13] National Cyber Security Index. (2024). *NCSI.* https://ncsi.ega.ee/country/ua/

[14] Li, W., Su, Z., Li, R., Zhang, K., & Wang, Y. (2020). Blockchain-based data security for artificial intelligence applications in 6G networks. *IEEE Network, 34*(6), 31–37. https://doi.org/10.1109/MNET.021.1900629

[15] Kunle-Lawanson, N. O. (2022). The role of AI in information security risk management. *World Journal of Advanced Engineering Technology and Sciences, 7*(2), 308–319. https://doi.org/10.30574/wjaets.2022.7.2.0128

[16] Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG International Journal of Computer Science, 48*(2), 213–222. https://surl.li/nxccjn

[17] Niu, X. (2024). Exploration on human resource management and prediction model of data-driven information security in Internet of Things. *Heliyon, 10*(9). https://doi.org/10.1016/j.heliyon.2024.e29582

[18] Landoll, D. (2021). *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC press. https://doi.org/10.1201/9781003090441

[19] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7,* 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

[20] Kwateng, K. O., Amanor, C., & Tetteh, F. K. (2022). Enterprise risk management and information technology security in the financial sector. *Information & Computer Security, 30*(3), 422–451. https://doi.org/10.1108/ICS-11-2020-0185

[21] Anu, V. (2022). Information security governance metrics: a survey and taxonomy. *Information Security Journal: A Global Perspective, 31*(4), 466–478. https://doi.org/10.1080/19393555.2021.1922786
[22] Khosravi-Farmad, M., & Ghaemi-Bafghi, A. (2020). Bayesian decision network-based security risk management framework. *Journal of Network and Systems Management, 28*, 1794–1819. https://doi.org/10.1007/s10922-020-09558-5
[23] Kilincer, I. F., Ertam, F., & Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks, 188,* 107840. https://doi.org/10.1016/j.comnet.2021.107840
[24] Semenets-Orlova, I., Klochko, A., & Tereshchuk, O. (2022). Special Aspects of Educational Managers' Administrative Activity under Conditions of Distance Learning. *Journal of Curriculum and Teaching, 11*(1), 286–297. https://doi.org/10.5430/jct.v11n1p286
[25] Popov, O. O., Kyrylenko, Y. O., & Kameneva, I. P. (2022). The use of specialized software for liquid radioactive material spills simulation to teach students and postgraduate students. *CEUR Workshop Proceedings, 3085,* 306–322. https://doi.org/10.55056/cte.122
[26] Bakhov, I., Rudenko, Y., & Dudnik, A. (2021). Problems of Teaching Future Teachers of Humanities the Basics of Fuzzy Logic and Ways to Overcome Them. *International Journal of Early Childhood Special Education, 13*(2), 844–854. https://doi.org/10.9756/INT-JECSE/V13I2.211127
[27] Bondarenko, S., Makeieva, O., Usachenko, O., Veklych, V., Arifkhodzhaieva, T., & Lernyk, S. (2022). The legal mechanisms for information security in the context of digitalization. *Journal of Information Technology Management*, *14*(Special Issue: Digitalization of Socio-Economic Processes), 25–58. https://doi.org/10.22059/jitm.2022.88868
[28] Hren, L., Karpeko, N., Kopanchuk, O., Strelbitsky, M., & Tohobytska, V. (2023). Substantive Essence and Components of the Societal Phenomenon "Information Security" in the Age of Information Society. In *National Security Drivers of Ukraine: Information Technology, Strategic Communication, and Legitimacy* (pp. 75-91). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-33724-6_5
[29] Davis, J., Agrawal, D., & Guo, X. (2023). Enhancing users' security engagement through cultivating commitment: the role of psychological needs fulfilment. *European Journal of Information Systems, 32*(2), 195–206. https://doi.org/10.1080/0960085X.2021.1927866