




Evaluating Information Security Strategies in the Public Sector: Efficiency and Cybersecurity Risks

Serhii Shtantsel ^{1,*}, Zoriana Buryk ², Dymytrii Grytsyshen ³, Oleksii Yevenok ⁴, Larysa Sergiienko ⁵

¹Candidate of Technical Sciences, Department of Public Administration, Interregional Academy of Personnel Management, Kyiv, Ukraine

² Doctor of science of Public Administration, Professor, Department of Public Administration Hryhorii Skovoroda University in Pereiaslav, Pereiaslav, Ukraine, z.burik@ukr.net

³Doctor of Sciences in Public Administration, Doctor of Economic Sciences, Professor, Vice-Rector for Scientific and Pedagogical Work and Innovative Development, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine

⁴Postgraduate Student of the Department of National Security, Public Management and Administration, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine

⁵Doctor of Science in Public Administration, Associate Professor, Department of National Security, Public Management and Administration, Dean of the Faculty of National Security, Law and International Relations, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine

* Corresponding Author: sht@ntsel.net

ARTICLE INFO

Received: 12 Oct 2024

Revised: 09 Dec 2024

Accepted: 19 Dec 2024

ABSTRACT

Introduction: Given the steady growth of the importance of information and communication technologies in developing socio-economic and managerial activities, the issue of cybersecurity is becoming particularly relevant. The problem is exacerbated by the military aggression of the Russian Federation in Ukraine, where cybersecurity is positioned as an integral part of national security.

Objectives: The purpose of the article is to analyse modern methods of information protection in the public sector.

Methods: The research methodology is based on several modern scientific methods, including the following: a systemic method, a method of retrospective analysis, comparative analysis.

Results: The author examines the NCSI (National Cyber Security Index) cybersecurity rating and the correspondence of the level of digital development of several countries, particularly Ukraine. Current risks and challenges in the cybersecurity sector are identified. The most effective approaches to the information security strategy, mainly using artificial intelligence and innovative technologies, cooperation with international institutions and monitoring, are studied. The specifics of creating modern integrated information protection systems (IPS), which use artificial intelligence and innovative technologies today, are investigated. It is substantiated that cybersecurity in the public sector should be based on the principle of effective implementation of the functionality of the relevant public authorities.

Conclusions: Thus, it is established that in the cyber defence system, the priority role of protecting information resources and the state's digital infrastructure is assigned to public authorities. It is substantiated that against the background of active digitalisation of all spheres of public life, active interaction between government agencies, the business sector, research institutions and the public in the context of effective prevention of cyber threats and mitigation of their consequences is becoming a priority.

Keywords: public sector, cyber threats, digitalisation, society, cybersecurity, information.

INTRODUCTION

In today's digitalised reality, cybersecurity is positioned as an essential condition for the successful functioning of the public sector. The diversity of threats and challenges related to the active digitalisation of society requires reliable means of protecting information and personal data, which is seen as the basis for socio-economic and political stability.

Developed countries are actively funding projects to expand the capabilities of digital technologies in the context of increasing the productivity and efficiency of economic development and improving public administration. At the same time, the integrity and confidentiality of the information infrastructure are at risk from dynamic cyber threats. Implementing innovative technologies requires alignment of the economic vector of state policy with national security priorities.

With the rapid scaling of cloud services and the increasing number of connected digital devices, traditional methods of information protection are becoming unable to ensure resilience amid the growing number and strength of cyber threats. Today, the challenge is to find an optimal balance between the effectiveness and complexity of security systems and to develop adaptive methods of mitigating threats in the public sector, which are characterised by constant dynamics. This task requires integrating innovative security systems with a high level of digital information security.

LITERATURE REVIEW

Issues related to improving cybersecurity in the public sector are gaining considerable popularity in the works of modern scholars. The analysis of the implementation of contemporary cybersecurity strategies in government bodies is being addressed by scholars Skybun [1], Sopilko [2], Revak and Gren [3].

In particular, the peculiarities of modernising systems integrated into the Digital State project are presented in the study by Skybun [1]. Researcher Sopilko [2] examines the regulatory and legal support for the information security system and highlights the need to harmonise the sectoral legislative framework in Ukraine in line with the requirements and norms of international standards. Scholars Revak and Gren [3] study modern methods of practical combating cybercrime in the context of the state and corporate levels.

Bondarenko et al. [4], Sytnyk et al. [5] study the specifics of improving the national concept of strategic planning for the development of the national security sector in the context of society's informatisation. At the same time, Dovgyi et al. [6] analyse the impact of the "legitimacy crisis" on the information security of the state's system of public authorities.

The issues of public-private partnership in cybersecurity are paid attention to by Krukhlov et al. [7]. The researchers focus on the need for mutual coordination of strategic documents, monitoring the implementation of infrastructure projects in the digital sector, and strengthening institutional capacity.

The problems of the public sector information protection methodology are addressed in the scientific works and publications of foreign scientists Rass et al. [8] and Albahar [9]. Scientists emphasise the importance of ensuring cyber defence in the context of critical public infrastructure.

Despite the significant developments of scientists in the field of the studied problem, the issue of cybersecurity guarantees for the public sector in the context of active digitalisation of society requires expanded scientific research.

The article aims to analyse modern methods of information protection in the public sector.

METHODS

The research methodology is based on several modern scientific methods, including the following:

- a systemic method that allows the study of the phenomenon of cybersecurity as a systemic formation, and the methodology of information protection as its integral subsystem, which functions based on approved theoretical views and effective practices;
- a method of retrospective analysis based on the concepts of the theory and practice of information systems protection in the process of formation and modern development;

comparative analysis allows the study of the specifics of cyber defence strategies in Ukraine and other countries, considering practical experience and existing challenges.

RESULTS

Information and communication technologies require a reliable and resilient digital infrastructure, which has become the new normal for the public sector. The country's cybersecurity is generally considered the responsibility of the state and national governments. The development of cyber resilience in today's environment requires active, practical

cooperation both in the interstate format and within the framework of regional interaction between the state, corporate sector, academia and the public.

The active digitalisation of social processes is actualising the role of cyberspace, which requires adequate provision of coordinated actions in the context of implementing the functionality of the cybersecurity system [10]. Developed countries in the international community use modern, innovative tools for data protection and digital infrastructure. Therefore, the potential for avoiding cyber threats is actively studied in the scientific and practical space [11].

In particular, the National Cybersecurity Index (NCSI) demonstrates the ability of states to implement a strategy for practical cyber incident management and effectively counter cyber threats. The dynamics of this index allow us to track a country's progress in digital development. The corresponding ranking (Figure 1) in 2023 shows the top ten leaders, and Ukraine is ranked fourth among them, which indicates the rapid development of the country's digital sector.

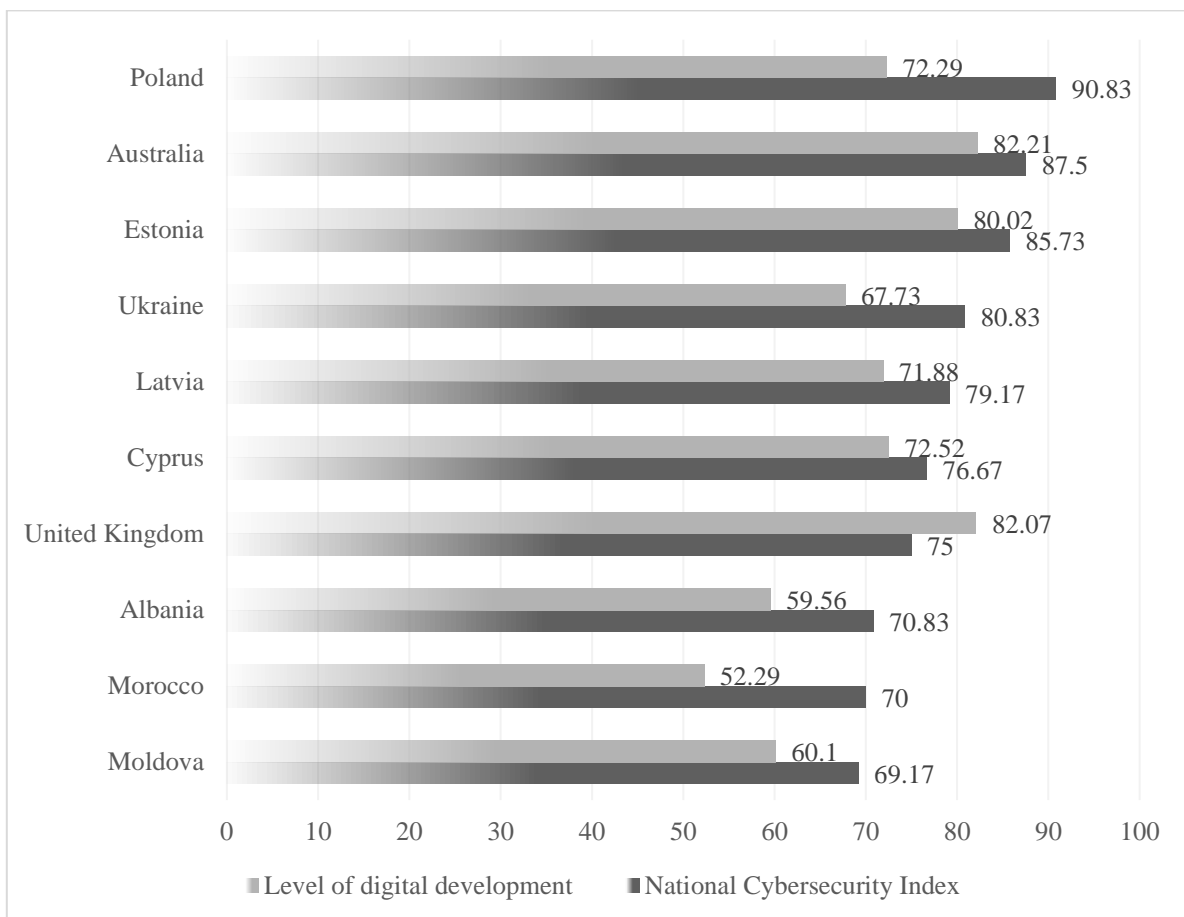


Figure 1. National Cyber Security Index for 2023

Source: NCSI [12]

Since the beginning of the full-scale war, Russia has been conducting between 102 and 293 cyberattacks per month, according to the State Special Communications Service at the request of Forbes (2024). The dynamics are shown in Figure 2.

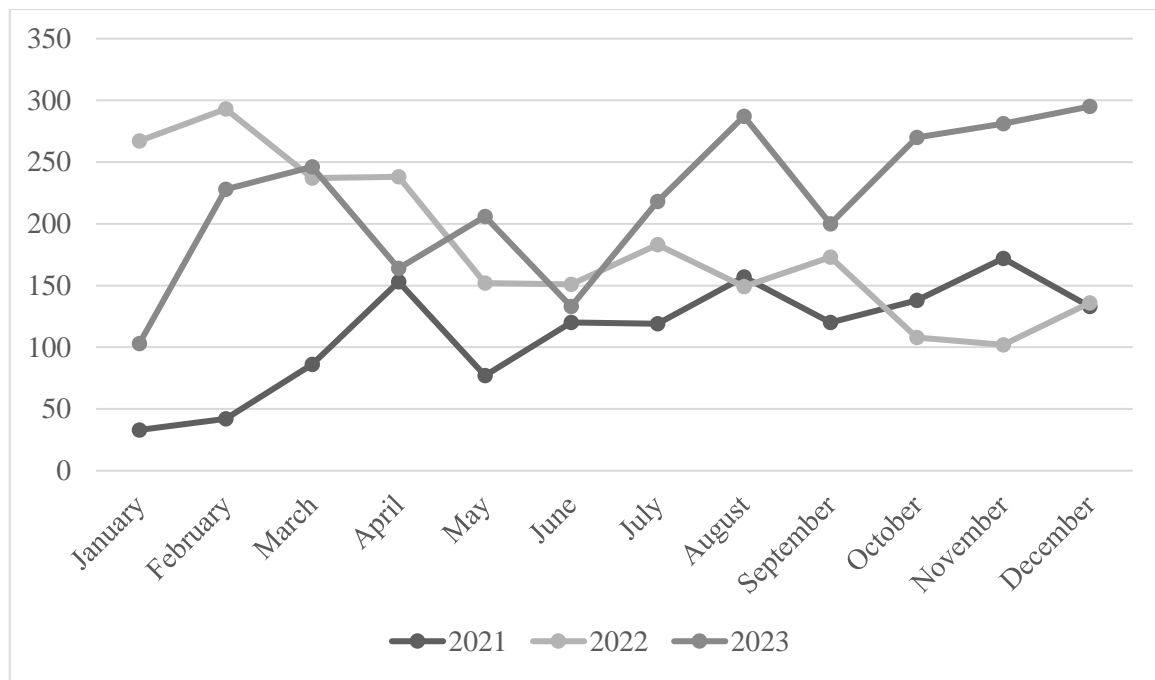


Figure 2. Dynamics of Cyberattacks, number/month, 2021-2023

Source: State Service for Special Communications and Information Protection of Ukraine [13]

The consequences of such attacks exceed all predicted losses. The websites of government agencies that handle large amounts of data suffer the most. The financial sector, as well as the media, IT companies and the energy sector, are also subject to significant attacks.

Kyivstar, for example, suffered billions of hryvnias in losses due to a large-scale cyberattack. Forty per cent of the company's infrastructure, including servers and data, was destroyed, causing a network outage.

Qualified experts from partner countries significantly assist Ukraine in cyber defence. Some companies freely share their experience or provide industry-specific training and competence development courses.

An extended analysis of the directions of cyberattacks in Ukraine since the beginning of the full-scale invasion (Figure 3) shows that government agencies are exposed to the highest risks in the context of information leakage and cybercrime. In this regard, a high level of electronic identification and the implementation of innovative methods of information data protection are becoming an urgent requirement of the present [4]. The state's efforts in military cyber operations also require further improvement.

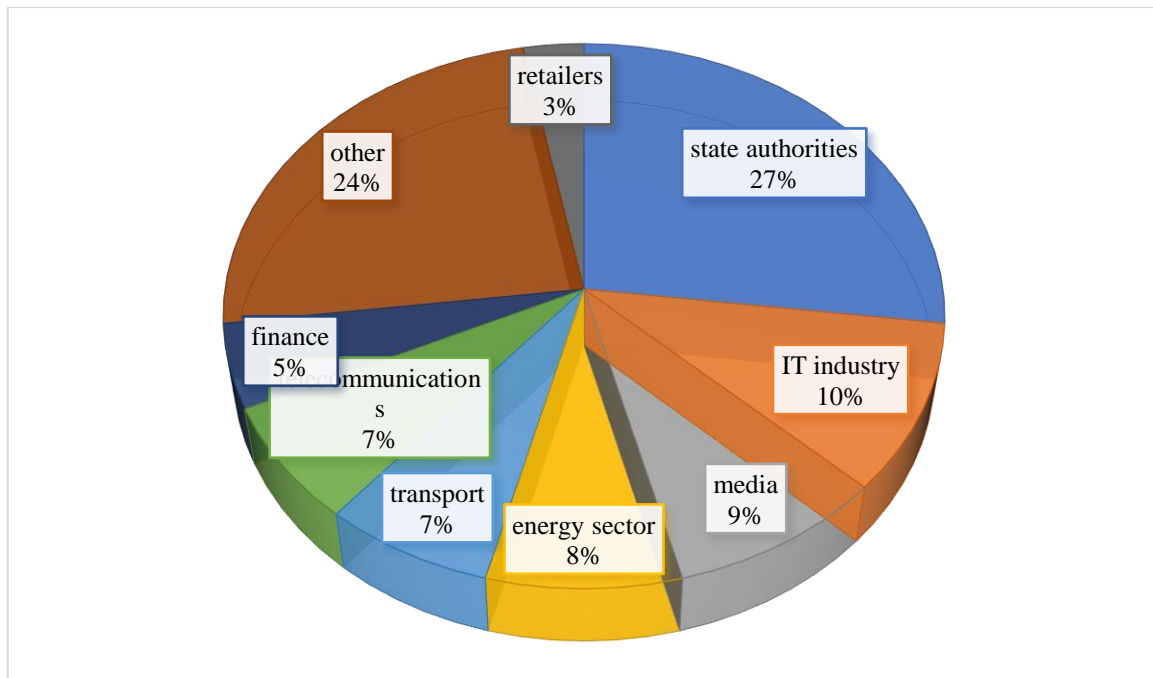


Figure 3. Industries affected by Cyberattacks in Ukraine since the beginning of the Full-scale Invasion

Source: Microsoft digital defence report [14]

The European Policy Strategy Centre (EPSC) presented the concept of digital sovereignty, representing the reliability of communication infrastructure, the provision of digital needs, and the possibility of regulatory influence in this area. In addition, the European community pays considerable attention to the activities of institutional bodies that combat crimes in cyberspace.

In this context, legal and regulatory support is critical, especially in translating general strategies into specific principles and responsibilities [4]. The legislation's functionality should include the introduction of accountability mechanisms and political commitments to increase cybersecurity's priority in public administration [15].

The dynamics of the strategy for mitigating cyber threats are being updated in the format of long-term planning and investment, which requires coordinated communication and efforts to overcome risks in the cyber environment. Modern cybersecurity strategy implementation approaches should be based on government programmes and strategic documents on modernising administrative, technical and legal procedures. In the context of Ukraine, "On the Cybersecurity Strategy of Ukraine" [16] and "On the Implementation Plan of the Cybersecurity Strategy of Ukraine" [17] are essential documents in this area. The documents determine the strategic framework for implementing and developing the cyber defence concept. In addition, the intensification of legal mechanisms for the functioning of the cybersecurity system is represented by the Resolution of the Cabinet of Ministers of Ukraine: "Some issues of response by cybersecurity entities to various types of events in cyberspace" [18]. Ukrainian legislation protects information in the format defined by the Law of Ukraine (Law) "On Protection of Information in Information and Communication Systems" [19], as well as the Laws of Ukraine "On Access to Public Information" [20], "On Electronic Documents and Electronic Document Management" [21], "On the Protection of Personal Data" [22], "On the State Service for Special Communications and Information Protection of Ukraine" [23], the Resolution of the Cabinet of Ministers of Ukraine "On Approval of the Rules for Ensuring Information Protection in Information, Electronic Communication and Information and Communication Systems" [24] and several others.

Promising areas for the development of the regulatory framework for the information security system in the public sector should include the implementation of international norms on combating cybercrime and the integration of innovative means of protecting digital infrastructure [4, 5]. Among the priority strategies, the following approaches are worth highlighting:

- monitoring of cyberattack tools through systematic analysis of innovative methods and technologies, and identification of threats;
- outsourcing of functions by integrating the efforts of cyber defence specialists to perform security audits, implement technologies, and develop defence strategies;
- state projects and strategic programmes to intensify cyber resilience and implementation of international security standards;
- expanding the boundaries and directions of international cooperation through active exchange of experience, information, and joint training projects;
- technical support involves introducing innovative security technologies, cyber incident identification systems, encryption and multi-factor authentication [7, 8, 9].

Creating modern integrated information security systems (IIS) today involves using artificial intelligence and innovative technologies, active interaction with international institutions, outsourcing and monitoring [1, 2, 3]. Organisational measures include:

- formulating and approving rules for the administration, accounting, accumulation, use and destruction of data storage media;
- developing an effective plan for responding to unauthorised access to information;
- ensuring the competence of public sector participants in users' information security rules.

A systematic approach to the methodology of information protection in the public sector involves operational threat assessment; research of the specifics of the object; multifactorial analysis of strategies for building a cyber defence system; study of the system itself, its operating principles, properties and the existing potential to increase its resistance to cyber threats; assessment of economic feasibility; correlation of the entire set of exogenous and endogenous factors; possibility of additional adaptive changes [8, 9].

The basic principles of the IPSC organisation are complexity, systematicity, flexibility of management and application, continuity of protection, openness of algorithms and protection mechanisms, reasonable sufficiency, and simplicity of application of protective measures and means.

The main tasks that a comprehensive information security system in the public sector should address are outlined below:

- effective management of access to information resources and confidential data, guarantees of protection against interference and unauthorised access by third parties, including limiting the powers of specific users in this regard;
- protection of information data transmitted via communication channels in order to maximise the integrity and confidentiality of information;
- monitoring of the system users' activities by the administration, with prompt notification of the security administrator of unauthorised access attempts;
- collecting, accumulating, storing, processing and using information about all events related to system security for operational control and analysis of potential threats;
- ensuring the integrity of critical system resources;
- creating a closed environment for trusted software to protect against malware, viruses and security system damage effectively;
- management of the means of the integrated protection system, including their configuration, monitoring and analysis of effectiveness [1, 2, 3].

In general, cybersecurity in the public sector should rely on implementing the functions of state bodies, forming strategies and sectoral policies, practical legal support, and international cooperation.

The methodology of information protection in the public sector requires the formation of a stable data security posture, which involves the development of a risk management plan. This programme should include information about the threat level of risks. Information protection methods include network security tools, which involve the use of modern firewalls; antivirus software and protection against malicious software; and access control systems:

- intrusion detection systems (IDS) and intrusion prevention systems: to prevent the penetration of malicious information data, hardware and software firewalls create a barrier between internal networks and external traffic, while security rules are formed to effectively filter incoming data;
- antivirus and anti-malware tools that provide vector-based protection by scanning data and extracting identified threats;
- implementing intrusion detection and prevention systems by monitoring network traffic allows for real-time alerts and active blocking of existing threats.

The human factor in cybersecurity focuses on the risks of human error. The current level of digital development in all areas of life requires timely and complete employee awareness, personal security tools, and digital security training. Among the security measures in this context, access control and research into the specifics of employees' behavioural responses are necessary to identify potential insiders.

The methodology for protecting information in the public sector in the context of executives is based on the awareness of the manager's priority of the profitability factor. In a challenging financial environment, managers ignore investments in critical cybersecurity needs in favour of cost savings, which is a negative trend. In general, top managers should be integrated into the cybersecurity system. Their involvement will optimise change management processes while driving the success of cybersecurity investments.

A modern cybersecurity strategy includes several essential components:

- risk assessment to identify weaknesses and potential threats;
- security policy, which provides for the implementation of a system of rules and standards for adequate information protection;
- staff training, including the acquisition of competencies in proactive prevention and rapid response to security incidents;
- physical protection system: access control systems to critical resources and their protection;
- technical protection, which involves the use of security tools to prevent intrusions;
- incident management provides rapid response and analysis of threatening events;
- audit and monitoring;
- backup;
- access control.

We are positioning ourselves in the cybersecurity product classes:

- infrastructure security, which ensures the security of physical and virtual resources by combining control and monitoring systems, access control solutions, and external threat identification tools;
- network security guarantees the security of network traffic and resources (firewalls, virtual private networks, intrusion detection and prevention systems);
- application security;
- data security: encryption, key management, data masking, data leakage prevention systems;
- user security: raising user awareness and authentication;
- workstation and endpoint security ensures individual devices' security: anti-malware solutions, antiviruses, and mobile device management systems;

- modern information security technologies are constantly evolving.

Among the innovative areas:

- machine learning and artificial intelligence, which can identify threats or anomalies that are invisible to human experts at a high speed;
- a blockchain used for integrity and inviolability of information data;
- behavioural Biometrics security;
- automated and integrated security testing;
- cloud security;
- Zero Trust Architecture, which sets strict requirements for all resource requests to pass verification.

These technologies provide multi-level protection to minimise the risk of cyber attacks. They continue to evolve rapidly in line with the constant dynamics of cyber threats.

DISCUSSION

Many contemporary authors explore the possibilities of mitigating cyber threats related to the functioning and development of the public administration sector. In particular, Miroshnychenko and Chernova [25] position the interconnection of politics and administration in the context of regulatory and empirical approaches to forming a cyber defence strategy in modern conditions as important. The authors identify the similarities between the methodology of information protection in the public sector and private business structures and pay attention to the latest approaches, such as blockchain technologies and machine learning in cybersecurity.

Researcher Arutiunian [26] proposes an integrated approach using blockchain and artificial intelligence to ensure transparency, efficiency, and accessibility of public services while ensuring information security. The researcher pays special attention to the need to develop digital skills among civil servants and the priority of optimising the institutional framework that will facilitate the integration of IT into public administration.

As Dombrovska et al. [27] continue, such an approach contributes to the formation of innovative intentions for designing Ukraine's cybersecurity policy. One of the priorities is developing and adopting the Concept of Information Security of Ukraine. The latter should include practical experience in European security strategy development.

At the same time, Marchenko [28] examines the activities of international cyber defence institutions. The author pays special attention to the search for effective antivirus software solutions for digital cyberspace security systems. According to the scientists, implementing international standards for cybersecurity management systems in developing countries should be accompanied by effectively monitoring the dynamics throughout all cybersecurity strategy implementation processes: modelling, analysis, planning, development, construction and operation.

Several modern scholars as Rosenbloom et al. [29] emphasise the need to raise public awareness of cybercrime, including among public sector employees. This will help to maximise the representation of public interests, guarantee openness and transparency in implementing democratic social principles, and maintain high standards of information security and confidentiality.

In continuation, Li and Liu [30] examine the specifics of the disappearance of the geographical dimension of cyber threats and the vulnerabilities created by cyber threats. The researchers argue for practical bilateral cooperation between the public sector and private entities, as well as the public, in the context of common interests in combating cyber threats.

Kilincer et al. [31] examine innovative IDS systems developed to detect attack traffic. According to the authors, artificial intelligence technologies can be used to achieve preventive cyber defence strategies.

Instead, Zuiderwijk et al. [32], studying the potential of artificial intelligence in cybersecurity, emphasise developing the foundations of digital law to ensure the integrity of legislative regulation of information security. The researchers analyse exploratory, conceptual, qualitative and practice-oriented studies, focusing on the consequences of using artificial intelligence for public administration in the context of cybersecurity, including negative ones.

Several modern foreign researchers pay special attention to innovative ways to protect against cyber threats. In particular, Husák et al. [33], Zhang and Thing [34] study the possibilities of predictive analysis to provide proactive next-generation cyber defence in the context of intrusion detection and propose new means of preventive attack identification.

Contemporary researchers Yurekten and Demirci [35], Broeders [36] develop a taxonomy for SDN-based solutions for common types of attacks, emphasising the need to form a legitimate market for effective cyber defence tied to the state through certification and regulation. In continuation, Zheng et al. [37] analyse the open challenges, related risks, and potential opportunities for dynamic defence in cybersecurity.

Lau et al. [38] propose several methods for modelling threats in cybersecurity. The authors argue that the ability to resist intrusions can be much higher if more protection resources are invested in critical infrastructure. Instead, Potteiger et al. [39] have developed an approach that protects against attackers acquiring the intelligence necessary to carry out attacks.

Researchers Huang and Zhu [40] and Gupta et al. [41] analyse the impact of generative artificial intelligence on cybersecurity and privacy and its social, legal, and ethical implications. The researchers highlight promising areas for improving artificial intelligence tools in the context of security, reliability and ethics. In addition, Arauz et al. [42], Bondarenko et al. [43] improve the predictive management model, trying to raise awareness of this problem by analysing the vulnerabilities of DMPC methods and developing appropriate protection mechanisms.

Despite significant scientific developments, rethinking the methodology of information protection in the public sector against the backdrop of rapid digitalisation requires extensive scientific research.

CONCLUSION

Considering the rapid digitalisation of all spheres of public life, ensuring cybersecurity in the public sector is positioned as one of the priority issues determining the reliability of critical infrastructure and the security of government agencies.

The growing number of cyber threats, both in the national space and in the context of the world community, requires an understanding of the essence of cyber risks and effective cyber defence management to ensure the security of the States. The author substantiates a strategy based on a systematic approach and active interaction of government agencies, businesses, and the public to improve cybersecurity measures continuously.

It is established that the main methods of information protection in the public sector today are technical and digital innovations, in particular, artificial intelligence tools and blockchain technologies, analysis and monitoring of cyberattack technologies, cooperation with international institutions, as well as adequate regulatory and legal support complementary to the requirements of the present, and raising public and civil servants' awareness of digital security. It is proved that cybersecurity in the public sector should be based on the principle of effective implementation of the functionality of the relevant public authorities, as well as on developing and implementing an effective strategy for developing the cybersecurity system and integrating modern tools for its implementation.

REFERENCES

- [1] Skybun, O. Zh. Cybersecurity of electronic communications systems of public authorities of Ukraine. *Visnyk of the National Academy of Public Administration. Series "Public Administration"*, 2021, 1(100), 30-39. http://nbuv.gov.ua/UJRN/vnaddy_2021_1_6
- [2] Sopilko, I. Information security and cybersecurity: a comparative legal aspect. *Scientific works of the National Aviation University. Series: Legal Bulletin "Air and Space Law"*, 2021, 2(59), 110-115. <https://er.nau.edu.ua/handle/NAU/53733>
- [3] Revak, I. O.; Gren, R. T. Features of the formation of secure cyberspace in the context of the development of the digital economy. *Innovative economy*, 2021, 3-4, 164-169. <https://doi.org/10.37332/2309-1533.2021.3-4.23>
- [4] Bondarenko, S.; Bratko, A.; Antonov, V. Improving the State system of strategic planning of national security in the context of informatisation of society. *Journal of Information Technology Management*, 2022, 14, 141-124. https://jitm.ut.ac.ir/article_88861.html

- [5] Sytnyk, H. P.; Zubchuk, O. A.; Orel, M. H. Conceptual understanding of the peculiarities of managing innovation-driven development of the state in the current conditions. *Science and Innovation*, 2022, 18(2), 3-15. <https://doi.org/10.15407/scine18.02.003>
- [6] Dovgyi, S.; Radchenko, O.; Radchenko, O. "Legitimacy Crisis" and its Impact on the Stability and Security of the System of Public Authorities of the State during the Formation of the Global Information Space. In: *Contributions to Political Science*. pp. 237–256. Springer, Cham, 2023. https://doi.org/10.1007/978-3-031-33724-6_14
- [7] Krukhlov, V.; Latynin, M.; Horban, A.; Petrov, A. *Public-Private Partnership in Cybersecurity*. CEUR Workshop Proceedings, 2020.
- [8] Rass, S.; Schauer, S.; König, S.; Zhu, Q. *Cyber-Security in Critical Infrastructures*. Springer International Publishing, 2020. <https://doi.org/10.1007/978-3-030-46908-5>
- [9] Albahar, M. Cyber attacks and terrorism: A twenty-first-century conundrum. *Science and engineering ethics*, 2019, 25(4), 993-1006. <https://doi.org/10.1007/s11948-016-9864-0>
- [10] Chmyr, Y.; Nekryach, A.; Kochybei, L. Postindustrial Society and Global Informational Space as Infrastructure Medium and Factor for Actualisation of the State Informational Security. *Contributions to Political Science*, 2023, 1367, 61-73. https://doi.org/10.1007/978-3-031-33724-6_4
- [11] Radchenko, O.; Bielai, S.; Kovach, V. Formation of Information Security Systems of the State: Current Status, Trends, and Problems. *Contributions to Political Science*, 2023, 1367, 93-112. https://doi.org/10.1007/978-3-031-33724-6_6
- [12] NCSI (National Cyber Security Index) cybersecurity rating for 2023. NCSI, 2024. <https://ncsi.ega.ee/country/ua/>
- [13] State Service for Special Communications and Information Protection of Ukraine, 2024. <https://cip.gov.ua/ua/news/25-travnya-den-derzhavnoyi-sluzhbi-specialnogo-zv-yazku-ta-zakhistu-informaciyi-ua>
- [14] Microsoft digital defence report, 2022. <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022>
- [15] Global Cybersecurity Outlook, 2023. *World Economic Forum*. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf
- [16] Decree of the President of Ukraine of 26 August 2021 No. 447/2021 On the Decision of the National Security and Defence Council of Ukraine of 14 May 2021 "On the Cybersecurity Strategy of Ukraine". <https://www.president.gov.ua/documents/4472021-40013>
- [17] Decree of the President of Ukraine of 1 February 2022 No. 37/2022 On the Decision of the National Security and Defence Council of Ukraine of 30 December 2021 "On the Implementation Plan of the Cybersecurity Strategy of Ukraine". <https://www.president.gov.ua/documents/372022-41289>
- [18] Resolution of the Cabinet of Ministers of Ukraine of 04 April 2023 No. 299 "Some issues of response by cybersecurity entities to various types of events in cyberspace". <https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text>
- [19] Law of Ukraine as of 28.06.2024 No. 80/94-BP "On Protection of Information in Information and Communication Systems". <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
- [20] Law of Ukraine of 08.10.2023 No. 2939-VI "On Access to Public Information". <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
- [21] Law of Ukraine No. 851-IV of 31.12.2023 "On Electronic Documents and Electronic Document Management". <https://zakon.rada.gov.ua/laws/show/851-15#Text>
- [22] Law of Ukraine as of 27.04.2024 No. 2297-VI "On the Protection of Personal Data". <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
- [23] Law of Ukraine of 28.06.2024 No. 3475-IV "On the State Service for Special Communications and Information Protection of Ukraine". <https://zakon.rada.gov.ua/laws/show/3475-15#Text>
- [24] Resolution of the Cabinet of Ministers of Ukraine of 21.10.2022 No. 373-2006-p "On Approval of the Rules for Ensuring Information Protection in Information, Electronic Communication and Information and Communication Systems". <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text>
- [25] Miroshnychenko, M. Yu.; Chernova, H. V. *Modern information security technologies: analysis of efficiency and development prospects. Improving the educational process in a higher education institution: a collection of scientific and methodological works*. Tavria State Agrotechnological University named after Dmytro

- Motornyi, 2024. 478 p. <http://www.tsatu.edu.ua/nmc/wp-content/uploads/sites/52/zbirnyk-tdatu-280624-pravka.pdf#page=256>
- [26] Arutiunian, V. Modern trends in the use of IT in public administration. *Aspects of Public Administration*, 2024, 12(1), 49-56. <https://doi.org/10.15421/152407>
- [27] Dombrovska, S. M.; Pomaza-Ponomarenko, A. L.; Kriukov, O. I.; Poroka, S. H. *Information threats and communication infrastructure in the public sector: a monograph*. Kharkiv: NUCSU, 2024. 244 p. http://repositsc.nuczu.edu.ua/bitstream/123456789/19990/1/%D0%9C%D0%BE%D0%BD%D0%BE_%D0%86%D0%BD%D1%84%D0%BE%20%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B8_2024%20%282%29.pdf
- [28] Marchenko, O. Cybersecurity and information protection: analysis of the impact of risks and threats using modern effective strategies for protecting cyberspace. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2023, 3, 50-59. <https://doi.org/10.32782/IT/2023-3-6>
- [29] Rosenbloom, D. H.; Kravchuk, R. S.; Clerkin, R. M. *Public administration: Understanding management, politics, and law in the public sector*. London: Routledge, 2022. <https://doi.org/10.4324/9781003198116>
- [30] Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 2021, 7, 8176-8186. <https://doi.org/10.1016/j.egy.2021.08.126>
- [31] Kilincer, I. F.; Ertam, F.; Sengur, A. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks*, 2021, 188, 107840. <https://doi.org/10.1016/j.comnet.2021.107840>
- [32] Zuiderwijk, A.; Chen, Y. C.; Salem, F. Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*, 2021, 38(3), 101577. <https://doi.org/10.1016/j.giq.2021.101577>
- [33] Husák, M.; Bartoš, V.; Sokol, P.; Gajdoš, A. Predictive methods in cyber defence: Current experience and research challenges. *Future Generation Computer Systems*, 2021, 115, 517-530. <https://doi.org/10.1016/j.future.2020.10.006>
- [34] Zhang, L.; Thing, V. L. Three decades of deception techniques in active cyber defence-retrospect and outlook. *Computers & Security*, 2021, 106, 102288. <https://doi.org/10.1016/j.cose.2021.102288>
- [35] Yurekten, O.; Demirci, M. SDN-based cyber defence: A survey. *Future Generation Computer Systems*, 2021, 115, 126-149. <https://doi.org/10.1016/j.future.2020.09.006>
- [36] Broeders, D. Private active cyber defence and (international) cyber security-pushing the line? *Journal of Cybersecurity*, 2021, 7(1). <https://doi.org/10.1093/cybsec/tyab010>
- [37] Zheng, Y.; Li, Z.; Xu, X.; Zhao, Q. Dynamic defences in cyber security: Techniques, methods and challenges. *Digital Communications and Networks*, 2022, 8(4), 422-435. <https://doi.org/10.1016/j.dcan.2021.07.006>
- [38] Lau, P.; Wei, W.; Wang, L.; Liu, Z.; Ten, C. W. A cybersecurity insurance model for power system reliability considering optimal defence resource allocation. *IEEE Transactions on Smart Grid*, 2020, 11(5), 4403-4414. <https://doi.org/10.1109/TSG.2020.2992782>
- [39] Potteiger, B.; Zhang, Z.; Koutsoukos, X. Integrated moving target defence and control reconfiguration for securing cyber-physical systems. *Microprocessors and microsystems*, 2020, 73, 102954. <https://doi.org/10.1016/j.micpro.2019.102954>
- [40] Huang, L.; Zhu, Q. A dynamic games approach to proactive defence strategies against advanced persistent threats in cyber-physical systems. *Computers & Security*, 2020, 89, 101660. <https://doi.org/10.1016/j.cose.2019.101660>
- [41] Gupta, M.; Akiri, C.; Aryal, K.; Parker, E.; Praharaj, L. From chatgpt to threatgpt: Impact of generative AI in cybersecurity and privacy. *IEEE Access*, July 2023. <https://doi.org/10.1109/ACCESS.2023.3300381>
- [42] Arauz, T.; Chanfreut, P.; Maestre, J. M. Cyber-security in networked and distributed model predictive control. *Annual Reviews in Control*, 2022, 53, 338-355. <https://doi.org/10.1016/j.arcontrol.2021.10.005>
- [43] Bondarenko, S.; Makeieva, O.; Usachenko, O.; Veklych, V.; Arifkhodzhaieva, T.; LERNYK, S. The legal mechanisms for information security in the context of digitalisation. *Journal of Information Technology Management*, 2022, 14, 25-58. <https://doi.org/10.22059/jitm.2022.88868>