Journal of Information Systems Engineering and Management
2025, 10(7s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Influence of Cutting-Edge Technologies on Cybersecurity in Contemporary Public Governance and Management

Oleksandr Yaremenko[1], Maryna Dzeveliuk[2], Andrii Dzeveliuk[3], Nataliia Chernyshchuk[4], Yelyzaveta Tymoshenko[5]

[1]Candidate of Sciences in Public Administration, Associate Professor, Department of Public Administration and Management, Dean of the Faculty of Law, Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, Ukraine.
[2]Candidate of Science of Law, Associate Professor, Department of Public Administration and Management, Faculty of Law, Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, Ukraine.
[3]Candidate of Science of Law, Associate Professor, Department of Fundamental and Private Law Disciplines, Faculty of Law, Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, Ukraine.
[4]Candidate of Historical Sciences, Associate Professor, Department of Public and Legal Disciplines, Faculty of Law, Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, Ukraine.
[5]Doctor of Philosophy, Asistant, Department of Fundamental and Private Law Disciplines, Faculty of Law, Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, Ukraine.

ARTICLE INFO

Received: 13 Oct 2024

Revised: 13 Dec 2024

Accepted: 26 Dec 2024

ABSTRACT

Introduction: This research is relevant because it needs to study the impact of innovative technologies on cybersecurity in modern public administration. With the constant development of the digital environment and the increase in cybersecurity threats, maintaining information security becomes a critical task for public institutions.

Objectives: The research aims to analyse and systematise data regarding the impact of innovative technologies on cybersecurity in modern public administration.

Methods: In the course of this research, the method of expert analysis was used to assess the impact of innovative technologies on cybersecurity in public administration. Based on the results of a survey of academic experts in the field of public administration (8 persons) and IT specialists (7 persons), a correlation analysis was conducted between the assessments of the level of cyber protection and the significance of innovative technologies for ensuring cybersecurity.

Results: According to the results of the correlation analysis, a significant degree of correlation with current cybersecurity challenges was found between blockchain technologies and the implementation of remote work ($r=0.77$ at $p<0.05$), biometric systems and the shortage of qualified specialists ($r=-0.86$ at $p<0.05$), as well as the Internet of Things and the transition to remote work ($r=0.93$ at $p<0.05$).

Conclusions: The expert survey results showed that academic experts in public administration (Group 1) focus on adapting national security policies, developing complex cyberattack methods, and needing a systematic approach to digital literacy. At the same time, IT experts (Group 2) emphasise the need to prevent the negative consequences of using cryptocurrencies in financial pyramids and the low level of users' knowledge of basic cybersecurity principles.

Keywords: cybersecurity, e-government, public services, state functioning, civil society.

INTRODUCTION

Innovative technologies are rapidly increasing their influence in various fields, including social, economic, public, and state governance sectors. In this context, cybersecurity becomes highly relevant due to the necessity of ensuring the protection of digital systems and information resources from the growing number of cyber threats and increasingly sophisticated cyberattacks.

This scientific article aims to study, analyse, and systematise information regarding the impact of innovative technologies on cybersecurity in modern public administration. This research must determine the correlation between digital development and the level of cybersecurity and identify the interrelationships between specific innovative technologies and the challenges associated with cybersecurity.

Thus, the relevance of the research lies in a thorough analysis of the impact of innovative technologies on cybersecurity in public administration, particularly in using mathematical analysis methods to identify complex interconnections between cybersecurity and innovative technologies. The research results can be used in developing specific strategies and measures to enhance cybersecurity to ensure high protection for state information and infrastructure amid the expanding use of information technologies in public administration.

LITERATURE REVIEW

In modern public administration, the role of innovative technologies is significantly increasing, becoming drivers of change in many areas of the country's activities. In this context, Predmestnikov and Bekhter [1] note that implementing modern technologies in public administration aims to enhance efficiency and relevance to global standards and address contemporary challenges and threats in cybersecurity. Additionally, Sporyshev [2] highlights that insufficient funding currently becomes a significant obstacle to ensuring the integrity of information security and the effective functioning of public administration bodies. A similar view is expressed by Vladyka and Prystupko [3] regarding implementing new technologies, considering the importance of adapting to a changing external environment. Meanwhile, Kushnarov [4] argues that information security is a crucial component of the national security of any state, making cybersecurity a priority for Ukraine, especially in the context of military aggression, and is being addressed by strengthening the national system's capacity to counter cyber threats and cybercrime.

In Kornaha's [5] study, it is noted that innovative technologies and digital platforms are becoming the basis for creating ecosystems that unite various entities—from businesses to civil society organisations – facilitating collaborative work and information exchange, positively impacting regional cybersecurity. Liapin [6] notes that the modern development and spread of information and communication technologies not only open new opportunities for improving interaction and cooperation between government agencies, citizens, and businesses but also create new challenges in cybersecurity.

In their scientific work, Bozhynskyi and Syniavskyi [7] note that modern technologies such as cloud computing, Big Data, crowdsourcing, cryptocurrency, and blockchain impact various economic sectors' cybersecurity. They emphasise the importance of digital tools such as monitoring systems, data analytics, and artificial intelligence in ensuring the security of substations. In this context, Hrabar et al. [8] mention that using new and innovative technologies provides various opportunities to enhance data privacy and security policies and strategies, explicitly highlighting blockchain's numerous possibilities for improving travel and expense management, thereby ensuring information security. Furthermore, Opirskyi et al. [9] noted the effectiveness of automation through machine learning and artificial intelligence. Thus, as Haiduk and Zvieriev [10] point out, rapid technological progress brings new opportunities for society and the economy. However, at the same time, it causes unpredictable challenges and threats from cyberspace, such as infrastructure, economy, politics, and individual privacy.

For the effective use of the opportunities provided by innovative technologies in public administration, attention should be paid to the research by Pokataiev and Arutiunian [11] on increasing the level of digital literacy among the population, as this will contribute to a better understanding of cybersecurity, learning to use modern information technologies, and the basics of cyber hygiene, which are vital to ensuring active citizen participation in e-government and the use of online services, reducing cybersecurity challenges. Stender et al. [12] indicate that there is currently an increase in new threats, and methods of identification and counteraction still need to be fully developed. These threats include cyberattacks, personal data breaches, spyware and virus impacts, phishing, and threats related to computer software updates. In turn, Mykhalchenko et al. [13] identify various methods and tools to protect against cyber threats, including cryptographic methods for protecting economic data and using artificial intelligence.

Additionally, as Kotukh [14] notes, developing e-government, focusing on empowering users and involving them in building civil society, is particularly important in the context of increasing cyberattacks. Bystrova [15] sees the effectiveness of proper professional training of cybersecurity specialists in reducing risks and enhancing the protection of public administration information systems. Modern cybersecurity challenges are primarily driven by the increasing activity in the darknet, the emergence of new cyberattack tactics, and the growing interest of criminals in cryptocurrency, in particular CaaS has democratized cybercrime, enabling even lowskilled attackers to launch powerful cyberattacks such as Distributed Denial of Service (DDoS), phishing campaigns, and ransomware attacks with ease [16].

METHODS

During the research, methods of literature analysis, statistical data analysis, comparative analysis, and methods of generalisation and systematisation were used to determine the current state, challenges, and problems related to cybersecurity and the development of innovative technologies.

Using the expert evaluation method contributed to precisely determining the interrelationships between innovative technologies and cybersecurity challenges in public administration. Two groups of experts conducted the evaluation: Group 1 consisted of academics researching various aspects of public administration (9 persons) – professors aged 50 to 60 years; and Group 2 consisted of qualified IT specialists (8 persons), specifically middle-level specialists (6 persons) aged 25 to 35 years and senior specialists (2 persons) aged 30 to 35 years. The experts assigned scores on a scale of 0 to 10, where 0–3 points corresponded to a low degree of impact, 4–7 points to a medium degree, and 8–10 points to a high degree. Based on the expert evaluations, an integral method was employed to calculate the weighted average indicator ($\text{Weighted Average} = \sqrt{K1^2 + K2^2 + K3^2 + K4^2 + K5^2 + K6^2 + K7^2 + K8^2}$) of the impact of innovative technologies on cybersecurity and to assess its significance. To identify the correlation between the determined factors, the functionality of the 'Excel' program was used, specifically the 'PEARSON' (or 'CORREL') function, which allows for calculating the degree of correlation between two measurement variables: cybersecurity challenges and the development of innovative technologies. The results of the correlation analysis revealed a significant degree of correlation between blockchain technologies and the implementation of remote work ($r = 0.77$ at $p < 0.05$), biometric systems and the shortage of qualified specialists ($r = -0.86$ at $p < 0.05$), and the Internet of Things and the transition to remote work ($r = 0.93$ at $p < 0.05$).

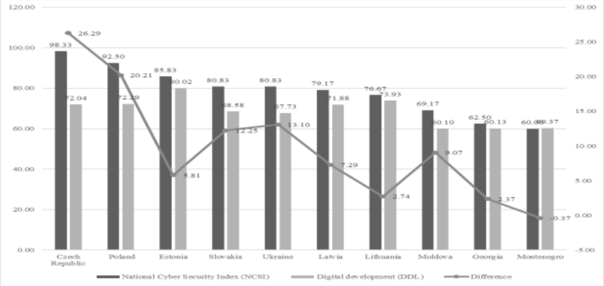
RESULTS

Over the past two decades, the world has undergone significant changes and innovative shifts, affecting government activities. Twenty years ago, only one in ten people used the internet; by 2022, this figure had risen to two out of three. In 2003, the UN Global E-Government Survey noted progress in the adoption of information and communication technologies (ICT) for e-government, manifested in the use of the internet and the presence of websites, while more ambitious governments created portals for providing integrated services. E-government has become one of the critical areas of development for public services, allowing for increased accessibility and transparency while reducing administrative costs [17]. In particular, in Ukraine, the Concept of E-Government Development was approved in 2017, featuring a modern approach and formulating principles for implementing e-Government [18]. In Poland, the first steps towards the realisation of the e-government idea were taken in 2001 with the adoption of the Law on Access to Public Information and the development of a comprehensive strategy for developing the information society in the country [19]. Overall, the e-government concept developed by the European Union (EU) aims to address the challenges associated with the technological revolution and cybersecurity issues. Its main goal is to create a unified, interoperable, and cross-border communication platform that ensures equal access to e-government services for all EU citizens [17].

In this context, integrating innovative technologies into all areas of modern life sets a new standard for social development. This process transforms how individuals and government bodies operate and affects corporate and civil society relationships. The transition to a digital environment, as an integral part of the modern global landscape, generates several technological challenges, primarily related to cybersecurity. Therefore, significant attention to the reliability and stability of information infrastructure becomes an essential aspect of ensuring the security and efficiency of society as a whole. Organising cyber protection at the state level involves various aspects that need to be systematically coordinated and improved, which can complicate this process [20].

The main target of cyberattacks is digital infrastructure, and such attacks lead to disruptions in telecommunications, transport, power grids, and other vital systems that ensure the functioning of the public and corporate sectors. These infrastructural assets include digital and physical components and structures supporting social and economic processes. The threat to the functioning of these elements can lead to service delivery issues, significant public safety disruptions, or other complication [26]. Therefore, it is essential to identify the means to avoid cyber threats, including the National Cyber Security Index (NCSI), which illustrates the capabilities of different countries to prevent and mitigate the consequences of cyber threats and manage cyber incidents [26]. In addition to the NCSI, it is necessary to consider the level of digital development (DDL), which will determine the level of development and monitor digital progress or shortcomings in cybersecurity. The correlation between digital development and cybersecurity in Ukraine and some other countries is shown in Figure 1.

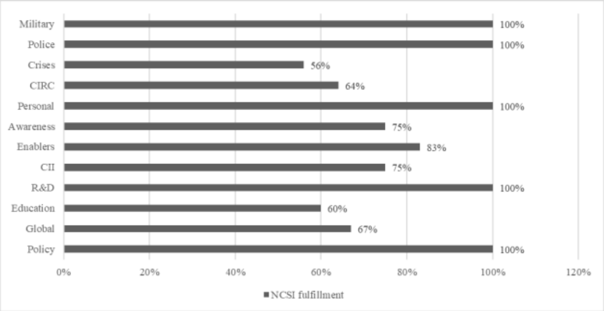
Figure 1: Correlation between Digital Development and Cybersecurity in Ukraine and Some Other Countries



Source: compiled by the author based on NCSI, [21]

In 2023, Ukraine ranked 8th with a cybersecurity index of 80.83 among 175 countries, according to the NCSI rating [25]. However, its level of digital development (DDL) is currently at 67.73, indicating certain areas for improvement in digital development that could affect its ability to defend against cyber threats effectively. The difference between the NCSI and DDL indicators for Ukraine is 13.1 units, pointing to a significant issue in the area of digital development that requires attention and improvement. In this context, it is essential to note the structure of the NCSI, which determines the country's cybersecurity level in various areas and its readiness to counter cyber threats (Figure 2).

Figure 2: Cyber Defence Level and Readiness to Counter Cyber Threats in Ukraine by Various Indicators



Source: compiled by the author based on NCSI,[22]

Thus, regarding cybersecurity policy, Ukraine has achieved 100% compliance with the requirements, indicating systematic and consistent legal acts regulating this area. Additionally, adequate public administration in Ukraine provides a solid foundation for combating cyber threats through developing and implementing cybersecurity strategies, regular risk monitoring and analysis, and providing the necessary resources and support for cyber defence.

Although Ukraine holds a leading position in cybersecurity, it is necessary to focus on preventing further risks associated with potential cyberattacks, considering Russia's armed aggression and associated factors that have a devastating impact on the overall security level in the country. In this context, to identify the main challenges in the field of cybersecurity, a large amount of professional literature was analysed, and the following factors were highlighted:

1. The threat of increasing complexity and scale of cyberattacks [8].

2. The need to increase the number of qualified cybersecurity specialists due to the development of new cyberattack methods [23].

3. The growing demand for stolen information and the associated risks due to increased activity in the darknet [8].

4. The necessity to adapt to new challenges associated with transitioning all areas of life to an online format [20].

5. The threat of increasing new schemes for using cryptocurrency for criminal purposes [24].

6. The insufficient level of cyber hygiene and low level of digital awareness and digital security threats [11].

An analysis was conducted to assess the importance of identified cybersecurity issues in modern public administration in Ukraine to assess the comprehensive impact of cybersecurity challenges and innovative technologies on ensuring cybersecurity. The assessment was conducted on a scale from 0 to 10, where 0–3 points correspond to a low degree of impact, 4–7 points to a medium degree, and 8–10 points to a high degree. Two groups of experts were selected for the assessment: Group 1 – academics focusing on various aspects of public administration (9 persons), who are professors aged 50 to 60 years; and Group 2 – representatives from the IT field (8 persons), among whom are middle-level specialists (6 persons) aged 25 to 35 years and senior specialists (2 persons) aged 30 to 35 years. The results of the analysis of expert evaluations of cybersecurity challenges in public administration are presented in Table 1 and Figure 3.

Table 1: Expert Assessments of Cybersecurity Challenges in Public Administration

Factors	Assessment areas	Weighting factor	Group 1	Group 2	Total Group 1	Total Group 2	Total Group 1	Total Group 2
Increase in the number of cyber attacks (K1)	Emergence of sophisticated attack methods (phishing, DDoS, zero-day exploits)	0,12	9	8	1,08	0,96	3,4	3,0
	A growing number of organised cybercrime groups	0,08	8	7	0,64	0,56		
Shortage of qualified cybersecurity professionals (K2)	The high demand for specialists exceeds the supply	0,07	6	9	0,42	0,63	2,2	3,2
	Insufficient number of cybersecurity education programmes	0,13	5	7	0,65	0,91		
Transition to remote and hybrid work (K3)	Use of unprotected home networks	0,05	8	6	0,4	0,3	3,4	2,8
	The need to adapt national security policy	0,15	9	8	1,35	1,2		
Increased activity in the darknet (K4)	Increased trade in stolen data	0,06	6	7	0,36	0,42	2,2	2,2
	Expansion of the cybercrime services market	0,14	5	4	0,7	0,56		
New ways to use cryptocurrency (K5)	Anonymous financing of cybercrime	0,07	7	5	0,49	0,35	2,6	2,2
	Use of cryptocurrencies in pyramid schemes	0,13	6	6	0,78	0,78		
Lack of digital awareness (K6)	Low level of user knowledge of basic cybersecurity principles	0,08	8	9	0,64	0,72	3,4	3,2
	Lack of a systematic approach to digital awareness	0,12	9	7	1,08	0,84		

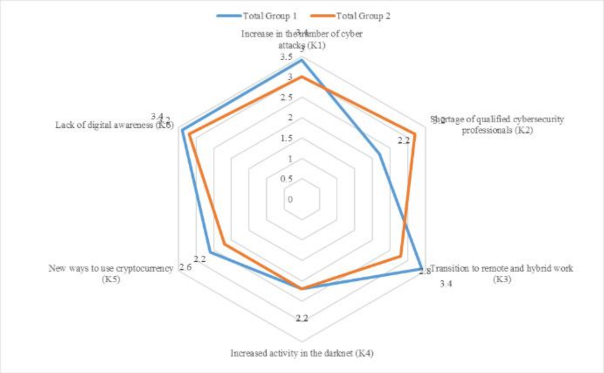


Figure 3: Relevance of Cybersecurity Challenges in Public Administration

The expert assessment of cybersecurity challenges in public administration identified several critical factors crucial for state systems' security. Academics in the field of public administration (Group 1) emphasise the development of sophisticated cyberattack methods (1.08), the need to adapt national security policy (1.35), and the lack of a systematic approach to digital awareness (1.08). IT specialists (Group 2) also rate these challenges highly but additionally highlight the negative consequences of using cryptocurrencies in financial pyramids (0.78) and the low level of user knowledge about basic cybersecurity principles (0.72).

To fully understand the significance of cybersecurity challenges in public administration, it is necessary to calculate the weighted average indicator for the groups of experts using the following formula:

$$\mathrm{WA} = \sqrt{\mathrm{K1}^2 + \mathrm{K2}^2 + \mathrm{K3}^2 + \mathrm{K4}^2 + \mathrm{K5}^2 + \mathrm{K6}^2 + \mathrm{K7}^2 + \mathrm{K8}^2} \quad (1)$$

where WA is the Weighted Average of the factors impacting the development of Euroregional cooperation.

Thus, WA Group 1 = 7.15, indicating a high level of influence of cybersecurity factors in modern public administration, reflecting the overall significance of problems and challenges in this area. In turn, WA Group 2 = 6.86, indicating that IT specialists also recognise a high degree of influence of cybersecurity factors, although they have a more critical view of the technical aspects of cybersecurity, resulting in slightly lower overall ratings compared to the assessments of academics in the field of public administration.

In this context, based on the analysis of current scientific literature, it is essential to determine the impact of the development of innovative technologies on ensuring cybersecurity in modern public administration. These technologies include blockchain technologies (I1), artificial intelligence and machine learning (I2), cloud computing (I3), the Internet of Things (I4), biometric technologies (I5), quantum cryptography (I6), identity and access management systems (I7), and Big Data analytics technologies (I8).

The identified directions have been grouped and presented in Table 2 and Figure 4 for further calculations. For this purpose, a survey was conducted among the existing group of experts, consisting of nine academics in public administration (Group 1) and eight specialists in information technology (Group 2). The obtained data allowed for the evaluation of the effectiveness of these directions in addressing current cybersecurity issues in public administration.

Table 2: Expert Assessments of the Impact of Innovative Technologies on Cybersecurity in Modern Public Administration

Factors	Weighting factor	Group 1	Group 2	Total Group 1	Total Group 2
Blockchain technologies (I1)	0,4	8	9	3,2	3,6
Artificial intelligence and machine learning (I2)	0,3	4	5	1,2	1,5
Cloud computing (I3)	0,4	5	6	2,0	2,4
Internet of Things (I4)	0,3	6	8	1,8	2,4
Biometric technologies (I5)	0,5	9	6	4,5	3,0
Quantum cryptography (I6)	0,2	8	8	1,6	1,6
Identity and access management systems (I7)	0,3	7	6	2,1	1,8
Big Data analytics technologies (I8)	0,4	9	8	3,6	3,2

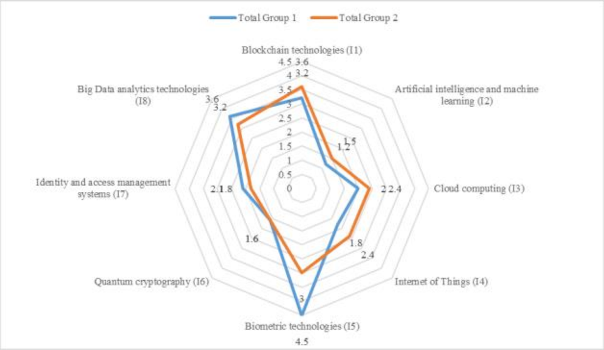


Figure 4: Relevance of Innovative Technologies for Cybersecurity in Public Administration

Thus, the use of blockchain technologies (I1) allows the creation of decentralised and immutable registers of state data. The high evaluation by experts (Group 1 = 3.2; Group 2 = 3.6) is because these registers provide high transparency and security, as the data is stored in a distributed network and protected by cryptographic methods. On the other hand, artificial intelligence and machine learning (I2) are rated low by all experts (Group 1 = 1.2; Group 2 = 1.5); even though these technologies are capable of working with large volumes of data to identify cyber threats, they are also tools for creating sophisticated attacks against state systems. Experts also emphasise the possibility of total dependence of the state on cloud service providers (I3) (Group 1 = 2.0; Group 2 = 2.4). Such dependence can create risks related to confidentiality and data control, and cloud service cyberattacks devastate state infrastructure.

Moreover, the effectiveness of using IoT (I4) from the perspective of public administration experts (Group 1 = 1.8) increases the security and efficiency of state infrastructure through real-time monitoring and management of systems, thus reducing the risks of failures and cyberattacks. However, IT experts (Group 2 = 2.4) believe that increasing connected devices creates more entry points for potential attacks. Regarding using biometric data at the state level (I5), public administration experts (Group 1 = 4.5) believe they provide reliable user authentication methods. On the other hand, IT experts (Group 2 = 3.0) consider that they also reduce the risks of unauthorised access to state systems.

In turn, all experts rated quantum cryptography (I6) highly (Group 1 = 1.6; Group 2 = 1.6) as this technology provides an ultra-high level of protection for transmitting state data, making it virtually impossible to intercept or hack. Expert opinions are divided on implementing an identity management system (I7). On the one hand, it automates granting access and monitoring user actions (Group 1 = 2.1). On the other hand, incorrect configuration or failures in such systems can lead to incorrect access granting and, consequently, increased risk of cyberattacks (Group 2 = 1.8). However, the evaluation of the capabilities of big data analytics technology (I8) is unequivocal (Group 1 = 3.6; Group 2 = 3.2), considering that it enhances the efficiency of identifying patterns and potential threats in data sets, thereby improving the prevention of cyber threats in the public sector.

Due to minor differences among academic experts in public administration (Group 1) and IT specialists (Group 2), there is a need to conduct a detailed correlation analysis using spreadsheet software such as Excel (Table 3). This analysis employs the 'PEARSON' (or 'CORREL') function, which allows calculating correlations between two measurement variables: cybersecurity challenges and the development of innovative technologies. This analysis aims to identify the interrelationships between these variables and determine the nature and extent of their impact on each other in the context of governance and state development.

Table 3: Correlation between Cybersecurity Challenges and Innovative Technologies in Modern Public Administration

	I1	**I2**	**I3**	**I4**	**I5**	**I6**	**I7**	**I8**
K1	-0,37725	-0,40436	-0,33349	-0,67288	0,676353	0,146786	0,259321	-0,22487
K2	0,617352	**0,769436**	0,651954	**0,933329**	**-0,85878**	0,235332	-0,46668	-0,07386
K3	-0,39196	-0,54593	-0,42887	**-0,67785**	**0,788386**	0	0,141773	-0,21793
K4	0,108	0,350371	-0,13992	0,299953	-0,31138	-0,07748	-0,54751	0,53782
K5	-0,052	-0,41979	-0,22977	-0,4482	0,620834	0,415175	0,29856	-0,22857
K6	-0,13301	-0,19975	-0,26442	-0,38621	0,647816	0,165056	0,205614	-0,18174

*Note: K1 – increase in the number of cyberattacks; K2 – shortage of qualified cybersecurity professionals; K3 – transition to remote and hybrid work; K4 – growth of activity in the darknet; K5 – new ways of using cryptocurrency; K6 – lack of digital awareness; I1 – blockchain technologies; I2 – artificial intelligence and machine learning; I3 – cloud computing; I4 – Internet of Things; I5 – biometric technologies; I6 – quantum cryptography; I7 – identity and access management systems; I8 – Big Data analysis technologies.

According to the data obtained through correlation analysis, it should be noted that the most significant degree of interrelationship is observed between the shortage of qualified cybersecurity specialists and the development of blockchain technologies (r= 0.77 at $p < 0.05$), indicating a need for specialists in this field for planning the development of decentralised state data registers.

A significant connection is also observed between the transition to remote work and biometric technologies ($r = 0.79$ at $p < 0.05$), meaning that implementing remote work increases interest in and using biometric technologies. The need to improve existing biometric technologies is related to ensuring the security and identification of employees in remote work environments, where conventional control methods can lead to the interception of personal data or confidential information.

Additionally, the following factors also show a significant degree of interrelationship: the shortage of qualified cybersecurity specialists and the Internet of Things ($r = 0.93$ at $p < 0.05$); the transition to remote work and the Internet of Things ($r = -0.68$ at $p < 0.05$); the shortage of qualified cybersecurity specialists and biometric technologies ($r = -0.86$ at $p < 0.05$).

Thus, considering the interrelationships identified by the correlation analysis, cybersecurity in modern public administration requires an integrated approach that combines technological solutions and the development of qualified personnel. Only such an approach can ensure the adequate protection of state information resources in the face of continuously increasing cybersecurity threats.

CONCLUSION

According to the results of the expert survey (Appendix A), it was determined that academic experts in the field of public administration (Group 1) particularly emphasise the necessity of adapting national security policy (1.35), as well as the development of sophisticated cyberattack methods (1.08) and the lack of a systematic approach to digital awareness (1.08). Conversely, IT experts (Group 2) also highly rate the challenges identified by the academics but additionally highlight the need to prevent the negative consequences of cryptocurrency use in financial pyramids (0.78) and the low level of user knowledge about basic cybersecurity principles (0.72).

The results of the correlation analysis indicate a significant impact of innovative technologies on cybersecurity in modern public administration. Specifically, innovative technologies are crucial in improving state resource management and ensuring cybersecurity. A significant degree of correlation with current cybersecurity challenges was identified in blockchain technologies and the implementation of remote work ($r = 0.77$ at $p < 0.05$), biometric systems and the shortage of qualified specialists ($r = -0.86$ at $p < 0.05$), and the Internet of Things and the transition to remote work ($r = 0.93$ at $p < 0.05$). Therefore, innovative technologies are tools for optimising and improving management processes in the public sector and essential elements of cybersecurity. Their implementation requires a comprehensive approach and continuous improvement to ensure the security and protection of state information resources in the modern digital environment.

REFRENCES

[1] Predmestnikov, O. H.; Bekhter, A. R. Use of innovative technologies in criminal procedure law: challenges and opportunities. *Scientific Bulletin of Uzhhorod National University*. Series: Law. 2024, 3(82), 117–122. https://doi.org/10.24144/2307-3322.2024.82.3.19.

[2] Sporyshev, K. Strategy of Development of Mechanisms of State Management of the System of Information and Analytical Support of the Security Forces of Ukraine. *Scientific Innovations and Advanced Technologies*. Series: Management and Administration. 2024, 4(32), 165–175. https://doi.org/10.52058/2786-5274-2024-4(32)-165-175.

[3] Vladyka, Yu. P.; Prystupko, A. O. Innovative Technologies in Banking as a Way of Increasing the Efficiency of Using the Resources of the Banking Institution. *Economy and Society*. 2023, 56, 1–5. https://doi.org/10.32782/2524-0072/2023-56-39.

[4] Kushnarov, V. V. National Cybersecurity System of Ukraine: challenges and cyber threats. In *Information, Communication and Knowledge Management in a Globalised World: Proceedings of the Fifth international scientific conference*. 2022, 29–33. KNUKiM Center. https://knukim.edu.ua/wp-content/uploads/2022/06/28.06.22-Zbirnyk-materialiv-2022-1.pdf#page=29.

[5] Kornaha, O. The Impact of Digital Transformation on the Mechanisms of Public Administration of Regional Development. Herald of Khmelnytskyi National University. *Economic Sciences*, 2024, 1(326), 189–193. https://doi.org/10.31891/2307-5740-2024-326-31.

[6] Liapin, K. E. Prospects of E-governance in Modern Cities. *Young scientist*. 2023, 7(119), 71–73. https://doi.org/10.32839/2304-5809/2023-7-119-13.

[7] Bozhynskyi, S. V.; Syniavskyi, O. Yu. Substations of the Future: Innovative Technologies and Development Prospects. *Young scientist*. 2023, 8(120), 1–4. https://doi.org/10.32839/2304-5809/2023-8-120-1.

[8] Hrabar, M. V.; Mashika, H. V.; Kashka, M. Yu. Conceptual bases of cybersecurity in the sphere of tourism and recreation. *Agrosvit*. 2023, 3–4, 43–49. https://dspace.uzhnu.edu.ua/jspui/handle/lib/48003.

[9] Opirskyi, I.; Susukailo, V.; Vasylyshyn, S. Investigating the Potential of Using AI Chatbots to Investigate Event Logs. *Ukrainian Information Security Research Journal*. 2023, 24(4), 177–183. https://doi.org/10.18372/2410-7840.24.17380.

[10] Haiduk, O. V.; Zvieriev, V. P. Analysis of Cyberthreats in the Conditions of Strong Development of Information Technologies. *Electronic Professional Scientific Publication "Cybersecurity: Education, Science, Technology"*. 2024, 3(23), 225–236. https://doi.org/10.28925/2663-4023.2024.23.225236.

[11] Pokataiev, P.; Arutiunian, V. Theories and Models of IT Efficiency in Public Administration. *Management and Entrepreneurship: Trends of Development*. 2024, 1(27), 119–125. https://doi.org/10.26661/2522-1566/2024-1/27-10.

[12] Stender, S. V.; Froter, O. S.; Snitko, Yu. M. Digital Integration and Cyber Protection of the Economy of Ukraine: Legal Aspects and Innovative Strategies. *Academic Visions*. 2023, 26, 1–13. https://doi.org/10.5281/zenodo.10389831.

[13] Mykhalchenko, H. H.; Snitko, Yu. M.; Ivanenko, V. O. Cyber Security in the Economy: Protecting Against Cyber Threats in a Digitized World. *Scientific Notes of Lviv University of Business and Law*. 2023, 38, 377–384. https://doi.org/10.5281/zenodo.10012434.

[14] Kotukh, Ye. V. Features of National and Regional Policy in the Field of Cybersecurity. *Theory and Practice of Public Administration*, 2019, 4(67), 40–47. https://doi.org/10.34213/tp.19.04.05.

[15] Bystrova, B. Basic Concepts of Research and Conceptual Foundations of Professional Training of Cybersecurity Specialists. *Pedagogical Sciences: Theory, History, Innovative Technologies*, 2017, 8(72), 58–70. http://nbuv.gov.ua/UJRN/pednauk_2017_8_8.

[16] Ganguli, P. The Rise of Cybercrime-as-a-Service: Implications and Countermeasures. *Heritage Group of Institutions*, 2024, September 15, pp. 1-46. https://doi.org/10.2139/ssrn.4959188.

[17] Kaska, K. Upgrading National Cyber Resilience: National Cybersecurity in Practice 2. *E-Governance Academy,* 2022, pp. 1–52. https://ega.ee/wp-content/uploads/2021/05/NCSI-Cyber-Resilience-Digi_F.pdf.

[18] Verkhovna Rada of Ukraine. On Approval of the Concept for the Development of E-Governance in Ukraine: Order of the Cabinet of Ministers of Ukraine of September 20, 2017, 649-p. *Legislation of Ukraine*. 2017. https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text.

[19] Konopka, M. N. The Concept of E-Government in the Light of Indicators of the European Commission. *Press Studies Notebooks,* 2017, 60(230), 329–349. https://doi.org/10.4467/22996362PZ.17.021.7301.

[20] Stolbovyi, V. M.; Kyslenko, D. P. Measures to Enhance Cyber Security at the State and Corporate Level in the Conditions of the Digitalisation of Society. *Scientific Notes of Lviv University of Business and Law*, 2023, 37, 175–183. https://doi.org/10.5281/zenodo.8019971.

[21] NCSI. National Cyber Security Index. E-Governance Academy, 2023a. https://ncsi.ega.ee/compare/

[22] NCSI. National Cyber Security Index: Ukraine. E-Governance Academy. 2023b. https://ncsi.ega.ee/country/ua/932/#details.

[23] Mullaliieva, D. S. Development of a Multimedia Course on Cybersecurity for Training Specialists. In *Problems of Informatization: The Eleventh International Scientific and Technical Conference*, 2023, pp. 10–11. Kharkiv: Impress. https://repository.kpi.kharkov.ua/handle/KhPI-Press/74849.

[24] Trozze, A.; Kamps, J.; Akartuna, E. A.; Hetzel, F. J.; Kleinberg, B.; Davies, T.; Johnson, S. D. Cryptocurrencies and Future Financial Crime. *Crime Science*. 2022, 11, 1–35. https://doi.org/10.1186/s40163-021-00163-8.

[25] NCSI. Methodology. E-Governance Academy, 2024. https://ncsi.ega.ee/methodology/.

[26] Rass, S.; Schauer, S.; König, S.; Zhu, Q. Cyber-Security in Critical Infrastructures. *Springer International Publishing*. 2020, 297 p. https://doi.org/10.1007/978-3-030-46908-5.

[27] Predmestnikov, O. H.; & Bekhter, A. R. Use of innovative technologies in criminal procedure law: challenges and opportunities. *Scientific Bulletin of Uzhhorod National University*, 2024, 3(82). 117–122. https://doi.org/10.24144/2307-3322.2024.82.3.19

APPENDIX A

Questionnaire for Collecting Expert Opinions on the Impact of Cybersecurity Challenges in Public Administration

Please write your answers to the questions in the form of a rating on a scale from 1 to 10, where 1 is not essential/not a threat at all, and 10 is very important/a threat.

1. How serious a threat does the emergence of sophisticated attack methods (e.g., phishing, DDoS, zero-day exploits) pose to cybersecurity?
2. Assess the growth of organised cybercrime groups as a factor affecting cybersecurity.
3. How significant is the lack of cybersecurity professionals?
4. Assess the problem of insufficient cybersecurity education programmes.
5. How high is the risk of using unsecured home networks for cybersecurity?
6. Assess the impact of the adaptation of national security policy in connection with the transition to remote and hybrid work on cybersecurity.
7. How serious is the threat of increased trade in stolen data on the darknet?
8. Assess the impact of the expansion of the darknet market for cybercrime services on cybersecurity.
9. Assess the problem of anonymous financing of cybercrime through cryptocurrency.
10. How significant is the threat of using cryptocurrencies in pyramid schemes?
11. Assess the risk that arises from users' limited knowledge of the basic principles of cybersecurity.
12. How vital is systematic work in raising digital awareness among users?