ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INFLUENCE OF DIGITAL TECHNOLOGIES ON INFORMATION SECURITY IN THE PUBLIC ADMINISTRATION SYSTEM

MYKOLA DURMAN[1], OLENA DURMAN[2], DMYTRO DROZHZHYN[3], IRYNA KRYLOVA[4] YURIY GAVRYLECHKO[5],

[1]Doctor of Science in Public Administration, Research Professor, The National School of Public Administration, Canada

[2] Ph.D. in Public Administration, Associate Professor of the Department of Public Management, Administration and Economics, University of Future Transformation, Ukraine

[3]Candidate of Science in Public Administration, Head of the Department of Luhansk Taras Shevchenko National University, Ukraine

[4] Doctor of Science in Public Administration, Candidate of Juridical Sciences (Ph. D.), Associate Professor of the Department of Public Management, Administration and Economics, University of Future Transformation, Ukraine

[5]Doctor of Philosophy in Public Administration, Associate Professor, Chernihiv Institute of Information, Business and Law of the ZVO "MNTU named after Academician Yuriy Bugaya", Ukraine

E-mail: [1]myk.durman@gmail.com, [2]helen.hrytsanchuk@gmail.com, [3]drozhzhyn.d@gmail.com, [4]irina.krilova7@gmail.com, [5]awaken8899@gmail.com

ABSTRACT

The use of digital technologies in public administration is a relevant issue in the face of the rising number of cyberattacks and threats to information security. The current trend demands operative substantiated decisions for the protection of state authorities. The primary aim of this article is to analyse the influence of digital technologies on information security in public administration systems. The research methodology involved the use of synthesis, generalisation, monitoring, and comparison methods for the evaluation of the current state of cybersecurity in public administration. The work has identified the main directions and means to prevent cyberattacks such as the introduction of cloud solutions, data encryption and the creation of national cybersecurity centres. The study results showed that integration of modern technologies ensures a reduction in the number of successful cyberattacks, enhances the level of information security and facilitates the development of international cooperation. The article deals with the limitations, which governments face while implementing the latest solutions, in particular insufficient financing and staff shortage. The practical significance of the work is in the provision of recommendations for the development of state programs for data protection and enhancing cybersecurity levels in public administration systems. Future studies shall be directed at the implementation of new instruments for threat monitoring and analysis of the effectiveness of international cybersecurity protocols.

Keywords: *Digital Technologies, Information Security, Public Administration, Blockchain, Cybersecurity, Cloud Technologies, International Cooperation*

1. INTRODUCTION

Information security is the key element of modern digital infrastructure, which ensures maintaining confidentiality, integrity, and accessibility of data in state and private structures. The concept of information security underwent significant transformation in the last decades. It is not limited to the security of physical information carriers but covers a wide range of digital technologies, including network security, protection of databases and cybersecurity. The digitalisation of state management caused the necessity to review approaches to ensuring information security due to the latest digital threats. They arise under conditions of implementation of modern technologies for maintaining infrastructure, containing vulnerabilities to cyberattacks. In the modern world, information security provides an active counteraction to cyberattacks, which are constantly evolving.

Modern digital threats with the use of encryption, ransomware, as well as manipulations through blockchain technologies, became a powerful instrument for the defeat of state systems. Criminals more often use complex encryption methods to block access to information resources of governmental institutions, demanding a ransom for data recovery. In 2021 a cyberattack on the infrastructure of the USA with the use of the Colonial Pipeline program demonstrated the scale and complexity of threats: hackers paralysed the energy supply system, using ransomware. They demanded payment of millions of dollars in cryptocurrency to restore the work of the system. Similar incidents were also documented in Europe. In 2022 governmental websites of Ukraine and Germany became objects of attacks with the use of complex encryption technologies. These technologies are directed at the destabilisation of the work of state structures and obtaining confidential information. Attacks on governmental organisations are becoming increasingly common, which requires the development of new strategies and technological solutions for their neutralisation.

Public administration uses variative approaches to the protection of digital infrastructure, combining different methods of cybersecurity to counteract increasing threats. Such an approach involves the implementation of cloud solutions for data storage and processing, the creation of data encryption systems, the use of multi-level authentication protocols and the development of national centres for cyber threat monitoring. Regardless of numerous security methods, the pace of cyberattack evolution demands constant improvement of security systems and optimisation of expenses on information security. Further improvement of cybersecurity systems should focus on the integration of the latest technologies and the development of international protocols for joint counteraction to threats.

The research aims to analyse the influence of digital technologies on information security in the public administration system in the face of the rising number of cyberattacks on state institutions. To achieve the aim, the following tasks were set:

– to analyse the dynamics of spending on information security in the selected countries with developed digital administration systems;

– to explore the most influential cases of cyberattacks on state authorities and evaluate their influence on the work of governmental systems;

– to determine the key measures and directions for counteracting cyberattacks, including the implementation of the latest security technologies and the creation of national cybersecurity centres.

– to evaluate the effectiveness of international cooperation in the areas of cybersecurity data exchange and the development of joint protocols to prevent threats.

2. LITERATURE REVIEW

Informational security in the public administration system is an important topic in modern studies, as it covers different aspects of state data protection and counteraction to cyber-attacks. Akinbowale, Klingelhofer and Zerihun [1] analysed the level of information security in the banking sector in South Africa, emphasising the importance of implementation of security standards for public administration. Barnes and Daim [2] studied information security in the healthcare field in the U.S.A and developed a security maturity model, which may be also used in state institutions. Butt et al. [3] explored cloud technologies threats and offered solutions for the protection of state systems, which use cloud services. Diener and Bolz [4] presented a Cloud Inspector instrument, oriented toward the implementation of information security processes in public clouds. Glybovets et al. [5] studied the restoration of urban architectural complexes, which is relevant for the development of the plan of information security of public administration of the object data.

Golebiowska [6] elucidated the Europeanisation of the legislation in Poland in information security, underlining the role of public administration in ensuring cybersecurity. Dryga [7] explored legal mechanisms for ensuring information security in the public administration of Ukraine, focusing on the role of legislative initiatives for the protection of state structures. Edegbeme-Beláz and Kerti [8] offered a new approach to the audit of information security in the public sector, which may be applied in European states. Szczepaniuk et al. [9] conducted an assessment of information security in public administration systems by identification of weak places in protection systems.

Panchenko [10] studied factors of information security of social development in public administration, underlining the role of state programs in enhancing the information security of society. Kindynis and Fleetwood [11] studied the issue of information security for criminological ethnographers, emphasising the importance of information systems protection in the public sector. Hermann [12] explored the instability of information systems and security risks in state structures of Burkina Faso, focusing on the necessity of investing in cybersecurity. Garayová [13] studied awareness of information security on the international level in public administration, underlining differences in approaches between the states.

Dryha [14] explored the understanding of the phenomenon of information security in state management in Ukraine, with a focus on the change of approaches to ensuring data protection. Nagy-Takács and Berényi [15] studied standards of information security management in the public sector in Hungary, indicating their role in effective state data protection. Ubowska and Królikowski [16] underlined the importance of creating a cybersecurity culture in public administration in Poland, demonstrating the relationship between the effectiveness of protection and awareness level. Moses and Sandkuhl [17] offered an approach to information security management for small state organisations, with consideration of their specific needs and restricted resources.

Tenzin, McGill and Dixon [18] studied factors influencing information security culture in government organisations in Bhutan, focusing on the importance of internal policies and standards. Pizam et al. [19] studied information security within the context of the hotel business, underlining the role of security risks, which can be transferred to the public sector. Ukeje, Gutierrez and Petrova [20] analysed cybersecurity and confidentiality challenges in governmental cloud services, emphasising the need for unification of security approaches. Banciu, Rădoi and Belloiu [21] studied awareness of information security in Romanian public administration, underlining the necessity for increasing the level of security culture. Based on the analysis of various views on information security in public administration, the common is the issue of integration of different technologies with administrative processes and effective protection.

Compared to the studies presented in the literature, this research expands on existing knowledge by offering a comprehensive analysis of digital technology integration and its dual role in enhancing and compromising information security in public administration systems. While previous works such as those by Szczepaniuk et al. [9] and Edegbeme-Beláz and Kerti [8] focused on identifying vulnerabilities and auditing mechanisms, this study delves deeper into the interplay between advanced technologies like AI, cloud services, and legislative frameworks. Additionally, unlike studies emphasizing regional perspectives, such as Dryga [7] in Ukraine or Nagy-Takács and Berényi [15] in Hungary, this research provides a global comparative analysis covering diverse regions with varying levels of digital infrastructure. By incorporating real-case monitoring from 2017–2024 and applying innovative visualization tools, this study contributes up-to-date insights and actionable recommendations for strengthening cybersecurity in public administration.

3. MATERIALS AND METHODS

3.1. Study procedure

The study procedure consisted of several stages, each of which was devoted to a specific aspect of the analysis of the influence of digital technologies on information security in the public administration system. In the first stage, an evaluation of total spending on information security: expenses on cybersecurity infrastructure, personnel, and technical support in selected countries was conducted. The second stage provided identification and analysis of the most significant cyberattacks, which took place in public administration in 2017–2024. In the third stage, the main means and directions to counteract these attacks, including technological solutions and policy initiatives aimed at the improvement of information security, were defined. The final stage included limitations of the study and presenting recommendations for ensuring further information protection of public administration systems with consideration of the latest technologies and specifics of the selected states.

3.2. Sample formation

The sample was formed on the basis of two main constituents. The first constituent covered public institutions in states with a high level of public administration development or those actively implementing it. These states were: Costa Rica, Ukraine, United States, Great Britain, Germany, Poland, Australia, Japan, France, and Canada. The mentioned sample is quite sufficient because of the presence of states with developed digital infrastructure, as well as those developing it. These states were selected due to their significant digital infrastructure and implementation of the latest technologies in administration systems, which makes them vulnerable to cyberattacks. The second constituent was related to the period of 2017–2024, as at that time the number of cyberattacks on public administration significantly increased, and they became more complex and destructive. The offered sample focused on the most actual and relevant information security data in public administration.

3.3. Methods

The study is based on the use of the following methods:

– synthesis and generalisation were used to consolidate heterogeneous information on cyberattacks and detect the main patterns observed in the selected states;

– statistical data processing enabled determining spending index and their dynamics;

– processing of secondary data received from SSL Insights, as well as official websites of governmental institutions in the selected states.

– monitoring of real cases of cyberattacks on public institutions to collect data on typical vulnerabilities and the effectiveness of protective mechanisms.

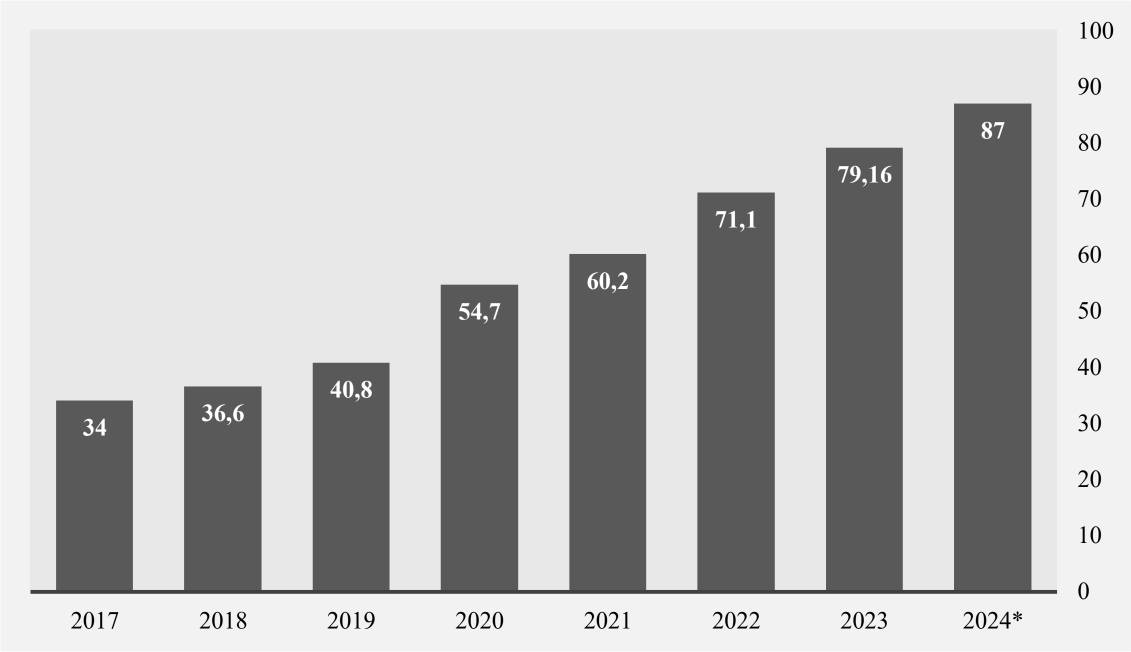
The set of the used methods ensured the reliability of the received results and their relevance to modern trends in the cybersecurity field.

3.4. Instruments

We used Microsoft Excel for data processing, which enabled systematisation and analysis of large information volumes. Tableau tools were used to make visualisation. We also used online platforms to collect secondary data from open government sources and analytical reports, which increased the accuracy and validity of the study. The study acknowledges potential threats to validity, including the reliance on secondary data from open sources, which may introduce bias or omit critical information. The selection of countries was based on their level of digital infrastructure and vulnerability to cyberattacks, ensuring a balanced representation but limiting generalizability to less developed nations. The chosen timeframe (2017–2024) captures relevant trends but may not fully account for evolving cybersecurity challenges beyond this period.

4. RESULTS

The analysis of global spending on cybersecurity in 2017–2024 demonstrates a significant increase, which indicates an increase in the importance of information systems protection on the international level. In 2017 the expenditures amounted to 34 billion US dollars, and in 2019 this value reached 48.8 billion, which reflects gradual consideration of the necessity to enhance cybersecurity. However, the largest spike was in 2020, when spending reached 54.7 billion. This trend may be explained by the COVID-19 pandemic, which changed global life pace, forcing many organisations and state structures to switch to the remote mode of work. Such a change created new vulnerabilities in security systems, which led to an increase in investments in information network protection. The main cause for it was the rapid adaptation of intruders to new conditions and their active use of cyberattacks for blackmailing and data extortion. Data on spending on digital security is presented in detail in Figure 1.



▨ Spending on cybersecurity, in billion U.S. dollars
** First 3 quarters of 2024*

Figure 1: Spending on Cybersecurity Worldwide from 2017 to 2024 (in Billions, U.S. Dollars)
Source: construed on the basis of data of Statista [22].

Further analysis shows that global spending for cybersecurity raised to 60.2 billion USD in 2021, and to 71.1 billion in 2022. Dynamic growth reflects the escalation of conflicts in different regions of the world, in particular, cyber campaigns related to geopolitical tensions and cyberattacks on critical infrastructure. During the Russian Federation's full-scale invasion of Ukraine in 2022, an increasing number of attacks on governmental servers and databases was fixed. Such actions prompted state governments to increase investments in protection technologies. According to the forecast for 2024, this sum will be 87 billion USD, which indicates the global tendency to enhance cybersecurity in the public sector.

Modern technologies in public administration cover a wide range of solutions aimed at enhancing the security and effectiveness of state services. One of the main instruments is electronic government systems (e-Government), which ensure public access to administrative services via the Internet. The most known among them are “Diia” in Ukraine and “Gov.uk” in Great Britain. The mentioned systems use digital identification cards, electronic signatures and multifactor authentication for secure access to personal data. Systems of monitoring and analytic of cybersecurity, using artificial intelligence for automatic detection and response to threats, are developed.

Technologies of separate monitoring (SIEM-security information and event management) for the collection of data from different sources and analysis of cyberattacks in real time are used in the USA. The important component is platforms for the protection of critical infrastructure such as energy networks and transport systems, which use machine learning systems for predicting potential attacks. Other innovations include blockchain technologies for ensuring transparency and security of financial operations in the public sector and backup systems for data recovery in case of successful attacks. Regardless of the latest means of ensuring data security, numerous cyberattacks on public administration institutions took place in 2022–2024, which is presented in detail in Table 1.

Table 1: Incidents of Cyberattacks on Public Administration in Different States

Date	State	Incident
2022-05-04	Costa Rica	Large-scale ransomware attack by Conti group on several state institutions, including the Ministry of Labor and Social Security. Service provision was significantly interrupted, which led to the issue of a national state of emergency
2022-11-14	Ukraine	Series of DDoS attacks on the energy sector and public administration sector in Ukraine, aimed at destabilisation of critical infrastructure under conditions of martial law
2023-03-22	United States	Hacking into the system of the New York Department of Education, which led to unauthorised access to sensitive data of students and teachers
2023-07-10	Great Britain	Cyberattack on the NHS Digital system, which led to the violation of the work of medical services and the leakage of patients' personal data
2023-09-15	Germany	Complex DDoS attack on the Federal Office for Information Security (BIS), which led to temporary inaccessibility to key state services and websites
2023-12-01	Australia	Attack on the Department of Home Affairs, which led to the leakage of sensitive data on immigration and visa applications
2024-02-05	Japan	Targeted cyberattack on the tax portal of the Ministry of Finance, which made it inaccessible for several hours
2024-05-21	France	The hacking of databases of the Municipal Administration of Paris, that led to the compromise of the personal data of thousands of people and significant interruptions in the work of local services
2024-07-15	Canada	Ransomware attack on servers of Canadian Tax Service, which led to the temporary suspension of online services related to tax declaration submission and leakage of information on taxpayers

Source: construed by the author.

After analysing incidents of cyberattacks on public administration in different states, it is possible to conclude that they have serious consequences for governmental structures. Firstly, they cause suspension in the work of important state services and confidential information leakage. In 2022, hacking of the servers of Pawlowice Administration led to database encryption, which factually paralysed the work of the institution and disrupted the performance of administrative functions. The other example is the attack on eZamowienia portal in Poland, caused by a DDoS attack on the infrastructure, causing significant delays in state contracts performance. The mentioned episodes underline the presence of vulnerabilities in the cybersecurity of state institutions, which require further improvement in the form of increasing spending and improvement of security systems.

Cyberattack geography covers different continents: from Europe and Asia to North America, and every country faces similar threats in the public sector. In 2023 a large-scale attack on ePUAP portal was fixed in Poland. It led to long-term disruption in the work of governmental services. In the USA, hackers use phishing attacks on state agencies, causing data leakage and vulnerability in critical infrastructure. In Ukraine, intruders' attacks on state portals have intensified after 2022, which led to mass disruption in services, including tax and energy resources. These examples underline the relevance and necessity of enhancing cybersecurity on the global level through investments in advanced protection technologies. Expansion of international cooperation and experience exchange between the states for the creation of effective mechanisms to counteract cyber threats should be the other important direction.

The war in Ukraine and other regional conflicts in the Middle East significantly influence the state of information security in the public administration sector. Cyberattacks are becoming a strategic tool to destabilise state institutions and interrupt the work of critical infrastructure and public data theft. Governments of states in a war zone or having interests in conflict regions invest in the improvement of cybersecurity systems. Such measures are taken to prevent information leakage, hacking of governmental websites and manipulations of administration systems, which can cause irreparable harm. Numerous DDoS attacks were made on governmental portals and information systems of critical infrastructure at the beginning of the full-scale Russian invasion of Ukraine in 2022. In particular, the servers of the largest banking systems Privatbank and Monobank were attacked in 2022–2023. Powerful attacks partially paralysed the work of state authorities and caused difficulties in service provision to the public. Similar incidents were observed in other conflict areas as well. Cyberattacks were used for disinformation, database hacking and influence on governmental decisions.

Prerogatives of the UN and G7 states are the issues of intensifying protection of public administration by the introduction of the latest technologies and cooperation between the states for the exchange of experience in the cybersecurity field. The creation of joint cybersecurity centres and the organisation of international exercises in repelling cyberattacks are already demonstrating their effectiveness. Still, the issue of insufficient financing and lack of qualified specialists remains, especially in the states with less developed infrastructure. Under conditions of war, cyber threats continue to grow, which makes strengthening defence capabilities in the area of information security critical at the state level. Table 2 presents the main trends, which can determine the further policy of global organisations and developed countries regarding public administration protection, based on the analysed SSL Insights data.

Table 2: Information Security in the Public Administration Sector

Trend	Content	Statistics
Increase in the cost of cyber incidents	The average cost of data leakage in the public sector reached a record high of 4.88 million USD in 2024	Recovery after ransomware attacks cost on average 2.73 million USD in 2024
Human factor	88% of cyber incidents in state authorities were caused by human errors, in particular in information management and employee negligence	68% of data leakage in the public sector involved human factors in 2024
Ransomware attacks	Increase in the number of ransomware attacks in 2023, related to critical infrastructure, in particular databases and accounting systems	The average payout for ransomware attacks in the public sector increased to 1.54 million USD
Phishing and social engineering	Phishing attacks are the main method of intruders to obtain access to confidential information in public administration bodies	The public sector loses 17,700 USD every minute due to phishing attacks
Increasing attacks on IoT	The high number of attacks on the Internet of Things (IoT) in the public sector, in particular video surveillance and automated control systems	About 10.54 million attacks on IoT devices, in particular urban security systems, were fixed in 2022
Cyberthreats in military conflicts	Public institutions underwent a significant increase in cyber threats during the period of military conflicts, which affected the stability of state systems	In 2022, about 6,000 DDoS attacks were aimed at state institutions within the context of military conflict
Personal data leakage	Large-scale data leakage in the public sector causes compromising the confidential information of millions of citizens	The leakage of personal data of about 37 million state service users was documented in 2023

Source: construed on the basis of data of SSL Insigh [23].

Analysis of modern trends and cyber incidents in the public sector shows that adaptation to new challenges in the cybersecurity sphere is pressing. The number of attacks on state institutions increased by more than 50% in Ukraine, Poland and Germany, which became the objects of targeted cyberattacks from 2020 to 2023. During the war in Ukraine in 2022–2023, cyberattacks on critical infrastructure – the energy sector and governmental servers, caused significant losses and complicated provision of state services. The government passed several legislative acts to counteract these threats. One of the main ones is the Law of Ukraine "On Critical Infrastructure", which introduced a complex of measures for the protection of strategically important facilities. Technologically, states actively implement systems based on the latest technologies – SIEM (Security Information and Event Management), to operatively respond to threats. They also use IDS/IPS (Intrusion Detection System/Intrusion Prevention System) to detect attacks in real-time.

The present situation with information security in the world emphasises the importance of developments of new technologies, with consideration of modern threats and the dynamic of their changes. The passing of Directive NIS2 by the European Union in 2022 significantly increased cybersecurity standards for public institutions. They obliged state bodies to implement modern protection means: multifactor authentication and regular infrastructure security checks. During 2022–2024, the number of DDoS attacks and ransomware campaigns significantly increased, which emphasised the importance of international cooperation for strengthening cybersecurity. In 2023 Poland and Lithuania signed a data exchange agreement for joint protection from cyberthreats in the public sector, using solutions based on cloud technologies Microsoft Azure and Google Cloud Security. In 2021 the US government passed the "Cybersecurity Improvement Act" which provides compulsory use of the EDR (Endpoint Detection and Response) system for governmental structures. AI-driven Threat Intelligence, ensuring constant monitoring and analysis of cyber threats in real-time, is implemented in the European Union states. In 2023 Germany approved the Cyber Security Strategy, which provides the creation of centralised cyber centres to coordinate defence actions and operatively respond to incidents. Strategic measures of the developed states underline the necessity of investing in the latest technologies and implementation of multifactor infrastructure of cybersecurity. Governments should regularly update their legislative acts and integrate blockchain-based systems for the protection of personal data and the prevention of their leakage in the public sector.

5. DISCUSSION

The results of the study of the influence of digital technologies on information security in the public administration system confirm that active implementation of modern technologies is essential for enhancing cybersecurity levels. Jumalieva [24] emphasises the importance of digital transformation in public administration for ensuring effective information protection, which is in line with our study. Yusupjanovich et al. [25] offered to use SECUBE to enhance information security in the public sector, which corresponds to the findings of our study.

Onopriienko [26] underlined the role of information security under conditions of armed aggression, emphasising the importance of the creation of institutional mechanisms and national centres for threat monitoring. This thesis is consistent with the findings of the study, which indicate the effectiveness of cybersecurity centres in the reduction of the number of successful attacks. The study by Myeong and Jung [27] explores the use of blockchain technologies for administrative reforms, which confirms the conclusion on the necessity of integration of the latest technologies for ensuring the stability of digital systems.

The study by Zahorskyi et al. [28] analysed the experience of the EU in ensuring information security in the public administration field. Their conclusions emphasise the importance of international cooperation and correlate with this article, which underlines the role of coordination of international-level efforts for effective data protection. Mikuletič et al. [29] studied information security culture in the medical sector, in particular, the issue of unauthorised access. The mentioned study confirms the necessity of strengthening internal security and data protection culture.

Li et al. [30] explored the use of deep neural networks to ensure the security of computer networks in hospitals, underlining that innovative technologies enable the enhancement of cybersecurity level. The author's statement is consistent with our findings, which demonstrated the effectiveness of such technologies' implementation in the public sector. Zhu [31] studied the use of blockchain technologies in public administration, which confirms conclusions on the importance of the latest technologies for information systems protection and risk reduction in state structures.

Henman [32] highlighted the possibilities and challenges of artificial intelligence use in the public sector, emphasising its potential for information security improvement. The hypothesis is consistent with the results, which indicate the necessity of technological development in public administration for effective detection and neutralisation of cyber threats. Wang et al. [33] studied the influence of breaches in information security on the management system using methods of cryptography and new algorithmic systems.

Li [34] analyzed the design of digital media systems and highlighted their role in enhancing information security, providing insights into how visual tools can support secure communication in public administration. Mikuletič et al. [35] explored information security culture in the healthcare sector, offering valuable parallels for addressing unauthorized access in public sector data management. Shaikh et al. [36] reviewed cryptographic trends, emphasizing their potential for safeguarding sensitive information in digital public administration systems, particularly in the context of Industry 5.0. Wang et al. [37] studied the deterrence effect of policy enforcement in information security, which aligns with the need for compliance frameworks in governmental digital infrastructures. Pizam et al. [38] examined customer perceptions of security in service-oriented environments, providing a basis for understanding public trust in secure digital platforms. Akinbowale et al. [39] investigated the challenges of maintaining information security in financial systems, offering comparative insights into protecting data in public administration.

Most authors confirm the importance of the integration of modern technologies and international cooperation in the information security field, which corresponds to the main conclusions of our study. The received results may be practically used for international public instances to protect critically important information.

5.1. Limitations

This study is limited to the period of 2017-2024, thus, it cannot fully reflect long-term trends in the information security field. The sample covers only states with developed digital administration systems and does not consider the experience of the less developed states.

5.2. Recommendations

Based on the conducted study, the following measures for enhancing information security in the public administration system are offered.

1. To develop national cybersecurity strategies, which integrate modern digital technologies and ensure operative information exchange between state institutions and international partners.
2. To invest in the modernisation of digital infrastructure and increase financing for the development of cloud technologies.
3. To implement programs of exercises and qualification advancing for specialists of state structures in the information security field.

6. CONCLUSIONS

The study found that digital technologies have a significant influence on information security in public administration systems. Analysis of the received data showed that investments in information security significantly increased during 2017–2024, but despite financing increase, complexity, and number of attacks continue to increase. This indicates the necessity of improvement of available protection systems and the development of new counteracting strategies. The use of cloud technologies, multilevel encryption, national centres of monitoring and rapid response demonstrated effectiveness in reducing the number of successful attacks. Still, these measures are not always able to follow the evolution of threats, which is observed in the increased number of ransomware and other harmful software attacks, oriented at governmental structures. The study found that cybersecurity infrastructure requires adaptability to new technological models and specialised infrastructure from 2023–2024.

The states with developed digital administration: the USA, Germany, Canada, and Ukraine demonstrate higher protection levels compared to the states, where the level of management digitalisation is less developed. However, even these states face issues related to personnel shortages and insufficient financing of separate aspects of cybersecurity. The complexity of coordination of international efforts in information exchange in the event of cyberattacks creates additional challenges. States in zones of active conflicts or political instability have more difficulties in complex protection realisation. The trends indicate the necessity of technological and managerial decisions, including the development of policy on the support of international cooperation and joint measures to counteract cyber threats. Such synergy will enable the formation of an integral information security system on the state level and improve resistance of the society to the latest cyber threats. Information security is of critical value for the protection of state data about national security and the stability of digital processes in public administration on the local levels. Therefore, further perspectives should be assessment of the quality of the use of the latest technologies and their integration with available systems for the detection of potential threats.

The study effectively addresses current and emerging threats in digital security within public administration, offering timely and relevant insights. It provides a structured framework for understanding risks and strategies for mitigation, making it a valuable resource for policymakers.

The findings have practical utility, extending beyond public administration to other sectors such as healthcare and education. The study's regional focus limits its global applicability, as it does not account for diverse legal and cultural contexts. Its emphasis on technological challenges over policy solutions leaves gaps in exploring governance measures. Reliance on publicly available data may exclude confidential insights, potentially affecting the comprehensiveness of the findings.

Future research should expand to include diverse regions, allowing for a global comparative analysis that considers varying legal and cultural environments. Advanced technologies, such as AI and quantum computing, should be examined to understand their potential in enhancing or threatening information security. Additionally, there is a need to explore human factors, focusing on insider threats and the role of training in mitigating security risks. Research into policy frameworks and legislative measures will help address evolving digital threats more effectively.

REFERENCES:

[1] O.E. Akinbowale, H.E. Klingelhofer, and M.F. Zerihun, "Exploring the Level of Information Security in the South African Banking Industry," *International Journal of Management and Sustainability*, Vol. 13, No. 1, 2024, pp. 40–59. https://doi.org/10.18488/11.v13i1.3594

[2] B. Barnes, and T. Daim, "Information Security Maturity Model for Healthcare Organizations in the United States," *IEEE Transactions on Engineering Management*, Vol. 71, 2024, pp. 928–939. https://doi.org/10.1109/TEM.2021.3139836

[3] U.A. Butt, R. Amin, M. Mehmood, H. Aldabbas, M.T. Alharbi, and N. Albaqami, "Cloud Security Threats and Solutions: A Survey," *Wireless Personal Communications*, Vol. 128, 2023, pp. 387–413. https://doi.org/10.1007/s11277-022-09960-z

[4] M. Diener, and T. Bolz, "Cloud Inspector: A Tool-Based Approach for Public Administrations to Establish Information Security Processes Towards Public Clouds," *Proceedings of the 9th International Conference on Information Systems Security and Privacy*, Vol. 1, 2023, pp. 543–551. https://doi.org/10.5220/0011694900003405

[5] V. Glybovets, M. Wei, T. Jing, V. Samchuk, S. Mosiiuk, M. Filipova, "Restoration of Urban Architectural Complexes: Dynamics of Visual Images, Urban Marketing, and Tourism Development," *Reice-revista Electronica de Investigacion en Ciencias Economicas*, Vol. 11, No. 21, 2023, pp. 63–80. http://dx.doi.org/10.5377/reice.v11i21.16545

[6] A. Golebiowska, "Europeanization of Law in Poland and Ensuring Information Security as a Task of Public Administration," *European Research Studies Journal*, Vol. XXV, No. 1, 2022, pp. 538–548. https://doi.org/10.35808/ersj/2868

[7] D.A. Dryga, "The Legal Mechanism of Information Security as a Category of Public Administration," *State and Regions. Series: Public Administration*, No. 2, pp. 93–97, 2023. https://doi.org/10.32782/1813-3401.2023.2.17

[8] A. Edegbeme-Beláz, and A. Kerti, "A New Approach to Information Security Auditing in Public Administration," *Hadmérnök*, Vol. 17, No. 3, 2022, pp. 109–131. https://doi.org/10.32567/hm.2022.3.8

[9] E.K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, and B. Klepacki, "Information Security Assessment in Public Administration," *Computers and Security*, Vol. 90, 2020, 101709. https://doi.org/10.1016/j.cose.2019.101709

[10] O.A. Panchenko, "Factors of Information Security of Social Development in Public Administration," *Klinical Informatics and Telemedicine*, Vol. 15, No. 16, 2020, pp. 121–128. https://doi.org/10.31071/kit2020.16.08

[11] T. Kindynis, and J. Fleetwood, "Information Cecurity for Criminological Ethnographers," *Crime, Media, Culture*, Vol. 20, No. 4, 2024, pp. 349–453. https://doi.org/10.1177/17416590231219746

[12] Y.K.J. Hermann, "Study on the Instability of Information Systems and Security Risks in the Public Administration: Case of Burkina Faso Public Administration," *Journal of Information Security*, Vol. 13, No. 02, 2022, pp. 76–84. https://doi.org/10.4236/jis.2022.132005

[13] L. Garayová, "Information Security Awareness in Public Administrations at an International Level," *Public Governance, Administration and Finances Law Review*, Vol. 4, No. 2, 2019, pp. 30–51. https://doi.org/10.53116/pgaflr.2019.2.3

[14] D.A. Dryha, "Features of Understanding the Phenomenon of Information Security in the Sphere of Public Administration," *Public Management and Administration in Ukraine*, Vol. 34, 2023, pp. 108–111. https://doi.org/10.32782/pma2663-5240-2023.34.21

[15] V. Nagy-Takács, and L. Berényi, "Information Security Management System Standards in Hungarian Public Administration," In: *CEEeGov '22: Central and Eastern European eDem and eGov Days*, September 22–23, 2022 Budapest. New York, NY: Association for Computing Machinery, 2022, pp. 112–117. https://doi.org/10.1145/3551504.3551554

[16] A. Ubowska, and T. Królikowski, "Building a Cybersecurity Culture of Public Administration System in Poland," *Procedia Computer Science*, Vol. 207, 2022, pp. 1242–1250. https://doi.org/10.1016/j.procs.2022.09.180

[17] F. Moses, and K. Sandkuhl, "Information Security Management in Small Public Sector Organizations: Requirements and Design of a Procedural Approach," *Complex Systems Informatics and Modeling Quarterly*, No. 37(2023), pp. 54–68. 2023https://doi.org/10.7250/csimq.2023-37.03

[18] S. Tenzin, T. McGill, and M. Dixon, "An Investigation of the Factors That Influence Information Security Culture in Government Organizations in Bhutan," *Journal of Global Information Technology Management*, Vol. 27, No. 1, 2024, pp. 37–62. https://doi.org/10.1080/1097198X.2023.2297634

[19] A. Pizam, A.B. Ozturk, A. Hacikara, T. Zhang, A. Balderas-Cejudo, D. Buhalis, and O. State, "The Role of Perceived Risk and Information Security on Customers' Acceptance of Service Robots in the Hotel Industry," *International Journal of Hospitality Management*, Vol. 117, 2024, 103641. https://doi.org/10.1016/j.ijhm.2023.103641

[20] N. Ukeje, J. Gutierrez, and K. Petrova, "Information Security and Privacy Challenges of Cloud Computing for Government Adoption: A Systematic Review," *International Journal of Information Security*, Vol. 23, No. 2, 2024, pp. 1459–1475. https://doi.org/10.1007/s10207-023-00797-6

[21] D. Banciu, M. Rădoi, and S. Belloiu, "Information Security Awareness in Romanian Public Administration: An Exploratory Case Study". *Studies in Informatics and Control*, Vol. 29, No. 1, 2020, pp. 121–129. https://doi.org/10.24846/v29i1y202012

[22] A. Borgeaud, "Global cybersecurity spending 2017–2024," [online] *Statista*, 2024 [Accessed 7 November 2008]. Available from: https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/

[23] Phishing Statistics for 2024: Latest Figures and Trends [online] *SSL Insights*, 2024 [Accessed 7 November 2008]. Available from: https://sslinsights.com/phishing-statistics/

[24] C. Jumalieva, "Improving the Digital Transformation in the Sphere of Public Administration and Ensuring Information Security," *Alatoo Academic Studies*, Vol. 23, No. 3, 2023, pp. 391–402. https://doi.org/10.17015/aas.2023.233.40

[25] S.N. Yusupjanovich, D.S. Sobirjonovich, and P.D. Xabibullayevich, "The Advantages of Using Secube in Public Administration to Ensure Information Security," *The American Journal of Social Science and Education Innovations*, Vol. 5, No. 12, 2023, pp. 77–79. https://doi.org/10.37547/tajssei/volume05issue12-10

[26] S. Onopriienko, "Functions of Ensuring Information Security of Public Administration in Ukraine in the Face of Full-Scale Armed Aggression of the Russian Federation," *Visnyk Taras Shevchenko National University of Kyiv. Military-Special Sciences*, 2022, pp. 95–98. https://doi.org/10.17721/1728-2217.2022.50.95-98

[27] S. Myeong, and Y. Jung, "Administrative Reforms in the Fourth Industrial Revolution: The Case of Blockchain Use," *Sustainability*, Vol. 11, No. 14, 2019, 3971. https://doi.org/10.3390/su11143971

[28] V. Zahorskyi, O. Bobrovskyi, D. Bondarenko, M. Karpa, O. Akimov, and L. Akimova, "Ensuring Information Security in the System of Public Management of Sustainable Development of the Region: EU Experience," *IJCSNS International Journal of Computer Science and Network Security*, Vol. 22, No. 8, 2022, pp. 163–168. https://doi.org/10.22937/IJCSNS.2022.22.8.21

[29] S. Mikuletič, S. Vrhovec, B. Skela-Savič, and B. Žvanut, "Security and Privacy Oriented

Information Security Culture (ISC): Explaining Unauthorized Access to Healthcare Data by Nursing Employees," *Computers and Security*, Vol. 136, 2024, 103489. https://doi.org/10.1016/j.cose.2023.103489

[30] G. Li, Z. Dong, and Y. Wang, "Information Security of Hospital Computer Network Based on SAE Deep Neural Network," *Applied Mathematics and Nonlinear Sciences*. Vol. 9, No. 1, 2024. https://doi.org/10.2478/amns.2023.1.00466

[31] Q. Zhu, "Research on Public Administration and Resource Allocation Based on Blockchain and Structured Occupational Therapy". *Occupational Therapy International*, No. 1, 2022. https://doi.org/10.1155/2022/2623656

[32] P. Henman, "Improving Public Services Using Artificial Intelligence: Possibilities, Pitfalls, Governance". *Asia Pacific Journal of Public Administration*, Vol. 42, No. 4, 2020, pp. 209–221. https://doi.org/10.1080/23276665.2020.1816188

[33] J. Wang, Z. Wu, X. Yuan, and Z. Song, "Peer Governance Effects of Information Security Breaches," *Energy Economics*, Vol. 129, 2024, 107264. https://doi.org/10.1016/j.eneco.2023.107264

[34] K. Li, "Digital Media System Design and Visual Art Analysis Based on Information Security," Measurement: Sensors, Vol. 31, 2024. https://doi.org/10.1016/j.measen.2023.100978

[35] S. Mikuletič, S. Vrhovec, B. Skela-Savič, and B. Žvanut, "Security and Privacy Oriented Information Security Culture (ISC): Explaining Unauthorized Access to Healthcare Data by Nursing Employees," Computers and Security, Vol. 136, 2024. https://doi.org/10.1016/j.cose.2023.103489

[36] Z. A. Shaikh, F. Hajjej, Y. D. Uslu, S. Yuksel, H. Dincer, R. Alroobaea, et al., "A New Trend in Cryptographic Information Security for Industry 5.0: A Systematic Review," IEEE Access, Vol. 12, 2024, pp. 7156–7169. https://doi.org/10.1109/ACCESS.2024.3351485

[37] X. Wang, C. Wang, T. Yi, and W. Li, "Understanding the Deterrence Effect of Punishment for Marine Information Security Policies Non-Compliance," Journal of Ocean Engineering and Science, Vol. 9, No. 1, 2024, pp. 9–12. https://doi.org/10.1016/j.joes.2022.06.001

[38] A. Pizam, A. B. Ozturk, A. Hacikara, T. Zhang, A. Balderas-Cejudo, D. Buhalis, et al., "The Role of Perceived Risk and Information Security on Customers' Acceptance of Service Robots in the Hotel Industry," International Journal of Hospitality Management, Vol. 117, 2024. https://doi.org/10.1016/j.ijhm.2023.103641

[39] O. E. Akinbowale, H. E. Klingelhofer, and M. F. Zerihun, "Exploring the Level of Information Security in the South African Banking Industry," International Journal of Management and Sustainability, Vol. 13, No. 1, 2024, pp. 40–59. https://doi.org/10.18488/11.v13i1.3594