UDC 004.738.5:004.056:351.74:351.746
DOI https://doi.org/10.32782/cuj-2026-2-7

Honcharuk Vladyslav Leonidovych
Lawyer, Doctor of Philosophy in Law, Associate Professor,
Associate Professor at the Department
of National Security of the Prince Volodymyr the Great
Scientific and Educational Institute of Law and Security,
Private Joint-Stock Company "Higher Educational Institution "Interregional
Academy of Personnel Management"
ORCID: 0000-0002-9627-9530

DIGITALIZATION OF MANAGEMENT IN THE SPHERE OF STATE SECURITY: DATA, CYBERPROTECTION OF PERSONAL INFORMATION IN PUBLIC ORDER PROTECTION PRACTICES

Modern problems of digitalization are changing approaches to ensuring state security and protecting public order. The article examines how the use of digital data, analytical systems and technologies in the field of cyber protection affects the work of bodies responsible for security and public order. In addition, attention is paid to the issues of personal information security, data leakage risks and the need to comply with information security standards. An analysis of the use of practical tools to increase the effectiveness of control, response and management decision-making is carried out. The foundations of the use of practical tools necessary to increase the effectiveness of control, response and management decision-making are determined. It is noted that the harmonization of digital technologies and their protection contribute to strengthening trust in society, have a positive effect on improving the quality of management and the level of public safety.

It is established that digital transformation requires comprehensive coordination mechanisms between various state institutions, because effective information exchange and integration of surveillance systems significantly increase the ability of authorities to respond to violations in a timely and comprehensive manner. The development and implementation of digitalization affects the emergence of new ethical and legal challenges related to control over the use of algorithms, minimizing the risks of excessive interference in the personal lives of citizens, ensuring the transparency of data processing.

It is emphasized that effective security management requires not only innovative implementation, but also the formation of a culture of information responsibility, increasing the digital competence of employees and creating a reliable regulatory and legal framework. The combination of these aspects affects the development of a holistic digitally-oriented security system capable of resisting external threats and ensuring a high level of protection of citizens.

Key words: *digitalization, public administration, national security, personal data, cyber security, digital technologies, electronic services, smart technologies.*

Гончарук В. Л. Цифровізація управління у сфері державної безпеки: дані, кіберзахист і захист персональної інформації в практиках охорони громадського порядку

Сучасні проблеми цифровізації змінюють підходи у забезпеченні державної безпеки та охорони громадського порядку. У статті розглянуто як використання цифрових даних, аналітичних систем та технологій у сфері кіберзахисту впливає на роботу органів, відповідальних за безпеку та громадський порядок. Окрім того, увагу приділено питанням безпеки персональної інформації, ризикам витоку даних та необхідності дотримання стандартів інформаційної безпеки. Проведено аналіз застосування практичних інструментів з метою підвищення ефективності контролю, реагування та прийняття управлінських рішень. Визначено основи застосування практичних інструментів, необхідних для підвищення ефективності контролю, реагування та прийняття управлінських рішень. Зазначено, що гармонізація цифрових технологій та їх захист сприяють зміцненню довіри в суспільстві, позитивно впливають на покращення якості управління та рівня громадської безпеки.

Встановлено, що цифрова трансформація потребує комплексних механізмів координації між різними державними інституціями, адже ефективний обмін інформацією та інтеграція систем спостереження значно підвищують здатність органів влади своєчасно та в повному обсязі реагувати на порушення. Розвиток

і впровадження цифровізації впливає на появу нових етичних та правових викликів, пов'язаних із контролем за використанням алгоритмів, мінімізацією ризиків надмірного втручання в особисте життя громадян, забезпеченням прозорості обробки даних.

Наголошено, що ефективне управління у сфері безпеки потребує не лише інноваційного впровадження, а й формування культури інформаційної відповідальності, підвищення цифрової компетентності працівників та створенню надійної нормативно-правової основи. Сукупність зазначених аспектів впливає на розвиток цілісної цифроорієнтованої системи безпеки, здатної протистояти зовнішнім загрозам та забезпечувати високий рівень захисту громадян.

Ключові слова: *цифровізація, державне управління, національна безпека, персональні дані, кіберзахист, цифрові технології, електронні сервіси, смарт-технології.*

Introduction. The digitization of public administration reinforces the need to make changes to ensure security and public order. The use of innovative technologies for data collection, processing, and analysis contributes to more effective control, timely response to threats, and sound management decisions. For law enforcement agencies, the introduction of digital technologies in the field of public security is a necessary but complex process. This is primarily due to the insufficient level of technical equipment and staff qualifications, which complicates the effective use of modern analytical systems, automated registries, and video surveillance. The rapid growth in data volumes creates new problems related to data leaks or the unauthorized use of citizens' personal information. This leads to an increase in cyber threats and affects public trust in state institutions that ensure public safety.

In the context of the Russian-Ukrainian war, there is a lack of uniform standards for information protection, and the integration of most digital platforms is fragmented. This undoubtedly reduces the timeliness of responses to emergencies and complicates coordination between central and local authorities. Therefore, the problem lies not only in ensuring a comprehensive approach that combines technical, organizational, and legal aspects, but also in guaranteeing the protection of personal data while promoting more effective public safety management.

Research methods and methodology. The methodological basis of the study is a systematic approach that allows us to consider the digitization of state security as a set of interrelated technological, legal, and organizational processes. The scientific article uses a number of methods, in particular:

– comparative analysis method – used to compare national and international practices of personal data protection in the field of public security;

– system analysis – to assess the interaction of digital platforms, information systems, and security mechanisms.

The application of these methods will ensure a comprehensive study of digitalization processes and their impact on the protection of personal information.

Disscussion. The stability of national security depends on external and internal threats, the effectiveness of institutions, and the ability to act transparently and responsibly. Throughout the entire period of independence, the structured work of state bodies, strict adherence to the law, and accountability have ensured the creation of conditions for economic development, public trust, and state stability. Now, as social processes are changing, there is a need to find not only traditional security management mechanisms, but also to introduce digital technologies that would ensure rapid data collection, processing, and analysis. The growth in the volume of digital data contributes to an increase in the risks arising from unauthorised access associated with cyberattacks, misuse of confidential information, and the introduction of mechanisms for the use of intelligent systems in real time.

Scientists N. Novikova and L. Boiko define digitalization as a rapid process capable of influencing various spheres of society. In the context of the rapid development of innovative technologies, various digital solutions are emerging that can modernize public administration and, thereby, influence the protection of national security as a whole. Digital transformation is an important means of strengthening national security. Modern digital technologies ensure the growth of public administration efficiency and contribute

to political stability and the democratization of social processes [1, p. 74].

The history of digitalization in the field of national security is a long process of structural changes associated with the gradual introduction of innovative technologies to counter new forms of threats. This trend began to take shape in the mid-20th century, when defense systems discovered computer technology. This event became the impetus for the growth of digital security. More than a decade has passed since the first attempts to use basic computing systems to the modern implementation of artificial intelligence. Given this, the development of analytical platforms and the formation of comprehensive cyber security solutions have changed the approaches of states to responding to challenges related to cyber incidents [2, p. 178].

Modern models of public administration define digitalization as a key element of strategic and operational processes. Traditional hierarchical mechanisms based on centralized decision-making are gradually being transformed or combined with more flexible and adaptive approaches focused on speed of response and efficiency. As a result of such structural changes, digital platforms are being used to enable real-time information exchange, support interagency interaction, and facilitate decision-making based on reliable data [3, p. 110].

Researchers O.O. Sobko and O.P. Makarova emphasize that modern technological developments and the digitization of society affect all areas of life, including public safety. At the same time, the introduction of innovative technologies contributes to more effective crime control, reduces risks associated with threats to citizens, and promotes the proper maintenance of national security as a whole. The growth in citizen mobility and active use of social networks is changing traditional approaches, modernizing them through the introduction of digital technologies that are capable of ensuring timely monitoring and response to offenses at the appropriate level, as well as increasing the transparency of law enforcement activities. Undoubtedly, the role of digital services is significant: from reviewing appeals and providing information on the progress of investigations to implementing basic security measures. This process strengthens citizens' trust in law enforcement agencies and their structures, enabling the latter to work towards results. Digital platforms facilitate the unhindered submission of complaints and the receipt of information about offences affecting public safety, while mobile applications help to report new incidents in a timely manner, improving the response of law enforcement agencies and coordinating their actions [4, p. 40].

Digital technologies currently available in the country are one of the main tools for ensuring national security. For Ukraine, which is at war and constantly exposed to various types of threats, the use of innovative digital solutions opens up opportunities to strengthen the country's security, including in the area of public order. The use of digital systems in the military and civilian spheres increases the level of protection of critical infrastructure, the information environment, and communication networks [5, p. 66].

Currently, digitalization is one of the main elements of state modernization, increasing the transparency of state mechanisms, timeliness, and impartiality in decision-making. The gradual growth of digital services strengthens citizens' trust in law enforcement agencies, provides access to information, and facilitates rapid feedback.

Scientists V.O. Kostenko, I.P. Krynychna, and D.A. Zhurbinsky say that cybersecurity, as one of the key areas of Ukraine's national security, requires a review of the regulatory framework in order to enhance the capacity of the state cyber system to effectively counter threats in the current environment. During the war with Russia, cybersecurity plays a particularly important role, and successful repulsion of cyberattacks is only possible with close coordination and teamwork among all parties involved in the fight. Effective cybersecurity is based on the comprehensive and systematic application of administrative and legal mechanisms in combination with professional resources. Their successful combination will ensure the success of state policy in this area.

Modern digital technologies include video surveillance systems, automated devices, mobile applications, facial recognition technologies, and tools for analyzing large data sets. They influence the formation of a data-centric management model in which management decisions are based on timely, accurate, and structured information.

Thus, data is a key resource that requires adequate protection, confidentiality, and lawful use.

In wartime, special attention must be paid to the protection of digital data. Server rooms, data centers, and other locations where data is stored require enhanced security and protection measures, and the use of access control systems, compliance with fire safety standards, and the implementation of innovative technologies must become key resources necessary for their reliable storage.

Technical support for comprehensive information protection is also of great importance for public safety. This includes the use of specialized software to counter cyberattacks, means of preventing confidential data leaks, and other cyber protection tools. During wartime, a comprehensive approach to the security of critical infrastructure facilities – technical, technological, and organizational – becomes a priority. This includes personnel security, the development of clear rules for interaction between departments, and ensuring the continuous operation of key security systems [6, p. 75].

It is important for Ukraine to take into account international experience in building cyber defense systems. It is international best practices that serve as the basis for improving national regulatory and organizational approaches, especially in the context of hybrid warfare. The effectiveness of administrative and legal support for cybersecurity is determined by the simultaneous development of cooperation with international professional institutions and the formation of national legislation focused on daily challenges related to cyber defense and public safety [7, p. 228].

Let us consider the effectiveness of using innovative technologies in the field of cyber protection using the example of the world's leading countries – Estonia, the United States, and Singapore – identifying their secrets and how the experience of these countries can influence Ukraine. Estonia is an example of the successful implementation of digital technologies in the fight against cybercrime. Large-scale attacks that hit the country in 2007 forced it to look for new and improved ways to modernize its digital infrastructure. As a result, an effective e-government system based on blockchain technologies was created. This technology ensured data integrity and decentralized information processing centers, minimizing the risk of service interruptions during direct attacks. The introduction of the X-Road system, which was new at the time, helped ensure the continuous exchange of data between public and private organizations, guaranteeing the provision of necessary services even when unforeseen situations arose that threatened national security.

Without exaggeration, Estonia's experience has shown that by establishing a system of protection against cyber threats and creating a specialized state agency – the Estonian Information System Authority (RIA) – the state has secured its position as a leader in the fight against cyber threats, demonstrating its cyber resilience to the world. Today, Estonia's experience has been adopted by a number of other European countries for which cyberattacks have become not just a problem, but a threat to their financial, economic, and political systems. The security and stability of a state depends on the integrated functioning of all sectors of protection.

In the United States, a comprehensive approach to cyberattack protection is established at the national level. Founded in 2018, the Cybersecurity and Infrastructure Security Agency (CISA) acts as the central coordinator for the protection of critical infrastructure and digital services of government agencies. is responsible for monitoring cyber threats, developing security standards, responding to cyber incidents in a timely manner, and providing support to government agencies by providing technical assistance. Close cooperation between government agencies and private entities facilitates the rapid exchange of information based on recommendations and tools to improve security.

Singapore's experience in creating a safe and technologically advanced society has been developed and implemented and has become one of the most successful projects operating in the country. Developed as part of the national strategy, the Smart Nation program, which began in 2014, continues to actively implement data analytics, AI, and digital Internet of Things technologies to improve the quality of life of citizens, increase economic efficiency, and optimize management ideas. A key component of this process is the Singapore Cybersecurity Agency, created to protect important confidential information and develop educational programs in the field of cyber security.

The implementation of the National Cybersecurity Master Plan and the adoption of the Cybersecurity Act have formed an effective regulatory framework for preventing and responding to digital threats.

These examples illustrate different ways of integrating digital technologies into national security while responding to the specific challenges posed by geopolitical and technological changes in each country. Through proactive governance models, investments in cutting-edge technologies, and the development of cross-sectoral cooperation, these countries have demonstrated how digitalization can strengthen national resilience, protect critical assets, and ensure effective governance in the face of future risks. The lessons learned are a valuable guide for other countries seeking to leverage their capabilities while minimizing the risks of digital technologies [8, p. 177].

An analysis of the experiences of Estonia, the United States, and Singapore suggests that the digitization of national security is an important element for any country, including Ukraine, which is already gradually introducing innovative protection technologies into the field of digitization. These countries have successfully combined legislative norms, modern technologies, and effective organizational models, allowing them to respond in a timely manner to new challenges related to cybersecurity breaches. An important element of their strategies is the creation of national digital identification systems, which would ensure secure access to government services for citizens and businesses. The introduction of decentralized data centers and blockchain technologies can minimize the risks associated with disruptions in critical infrastructure and public safety. Data analytics, artificial intelligence, and the Internet of Things can be used to monitor situations and improve the effectiveness of management decisions.

It is worth noting that interaction between state bodies and the private sector increases the chances of a rapid response to cyber threats. As a result, such cooperation will contribute to the pooling of resources, specialist knowledge, and technological capabilities, facilitating more effective prevention of cyberattacks and minimizing their consequences. In general, the experience of leading countries in the field of digital security demonstrates, first and foremost, the importance of financing innovative technologies and developing national risk management mechanisms, which is one of the main conditions for ensuring digital resilience.

For Ukraine, these developments are primarily of practical value in terms of documenting war crimes and protecting human rights violations in wartime. Thanks to the use of mobile technologies, satellite monitoring, and open source intelligence methods, such digital evidence can play an important role in investigations and court proceedings both in Ukraine and in international judicial institutions, in particular the International Criminal Court or the International Court of Justice. In order for these materials to be legally valid and usable as evidence, their collection, storage, processing, and presentation must be carried out in accordance with internationally recognized rules and standards, such as the Berkeley Protocol on Working with Open Source Digital Information in Investigations [9, p. 315].

Currently, the State Center for Cyber Protection SSSCZI is successfully operating in Ukraine. This center is a state institution that is part of the State Service for Special Communications and Information Protection of Ukraine. The main tasks of the center include:

– development and practical implementation of an organizational and technical model of cyber protection, which is part of the national cybersecurity system;

– ensuring the creation and functioning of key components of the Secure Internet Access System for government agencies;

– development and support of the National Antivirus Protection System for Information Resources;

– conducting information security and cyber defense audits of critical information infrastructure facilities;

– creating and ensuring the operation of a system for identifying vulnerabilities and responding to cyber incidents and cyber attacks;

– organizing coordination between computer emergency response teams;

– developing new scenarios for responding to cyberattacks, searching for tools and approaches to combat cyber incidents, and developing educational programs and training courses in the field of cybersecurity;

– creating and supporting a National Center for Backing Up Public Information Resources [10].

An important step in strengthening cyber protection and cyber security was the improvement of the legal framework in the country. In March 2025, the President of Ukraine signed the Law of Ukraine "On Amendments to Certain Laws of Ukraine on the Protection of Information and Cyber Security of State Information Resources and Critical Information Infrastructure Objects". The adopted law provides for a number of changes and innovations, in particular:

– the formation of a new national system for responding to cyber threats and cyber incidents, preventing cyber attacks, etc.;

– the establishment of principles for the use of response mechanisms in crisis situations in the field of cybersecurity;

– establishing a clear framework for the system of information exchange on cyber incidents, cyber attacks, and potential cyber threats, reporting such incidents to special entities;

– abandoning CCSSI and defining the process of implementing risk management measures with support for such measures throughout the entire life cycle of systems based on security profiles;

– introduction of a cybersecurity assessment system – audit methods;

– establishment of full-time positions for cybersecurity managers and specialists in government agencies and critical infrastructure facilities [11].

Cooperation with international partners in the field of cyber defense remains important. One of the leading partners providing assistance in this area is the United States. The State Center for Cyber Protection of the State Special Communications Service received equipment and software from the US Agency for International Development (USAID) through the USAID Project "Cybersecurity of Ukraine's Critical Infrastructure". This assistance has had a positive impact on the work of the State Special Communications Service. This assistance includes several key components that contribute to strengthening cyber defense in Ukraine (Table 1):

In addition, the capabilities of Ukraine's Governmental Computer Emergency Response Team (CERT-UA) have been expanded through the introduction of specialized software. This allows for faster detection of new cyber threats, more effective analysis of cyber incidents, and prompt notification of government agencies and critical infrastructure facilities about potential risks. Thanks to the support of the USAID Project "Cybersecurity of Ukraine's Critical Infrastructure", the state has gained the ability to more effectively counter cyberattacks and ensure the rapid recovery of information systems after adverse incidents [12].

The digitization of the public safety system is a strategic factor in the development of the state, not just a technical tool for modernization. It affects the effectiveness of public administration, the transparency of government activities, and the level of public trust in state institutions. The use of digital platforms helps to automate accounting, analysis, and forecasting of events, reduce the risk of errors, and improve the soundness of management decisions.

The use of artificial intelligence is one of the major innovations in cybersecurity. Network and endpoint security are already showing significant growth, making them the largest segments in the AI cybersecurity market. Among the key advantages of AI is the automation of routine tasks that

Table 1

Key components of international assistance in the field of cybersecurity in Ukraine

No	Components of assistance	Content of assistance	Results
1	Upgrading the server equipment of the State Cyber Security Center	Modernization of the technical infrastructure of vulnerability detection and cyberattack response systems	Rapid detection of potential threats, improved response efficiency
2.	Strengthening the information and communication systems of the National Center for State Information Resources Reservation	Strengthening ICT systems for data storage and processing	Preservation of important information, stable operation of critical infrastructure facilities.

Source: concluded by the author.

can automatically detect and respond to violations or anomalies without human intervention. Another advantage is cost-effectiveness, which helps minimize human error as one of the main causes of cybersecurity breaches. These aspects are designed to speed up the process of eliminating threats. Although there is currently no specific legislation on AI in Ukraine, there are a number of recommendations that provide general guidelines for the implementation of these technologies. In particular, pilot projects are being implemented, such as the Declaration on the Responsible Use of AI, approved by the Ministry of Digital Transformation. As part of the European integration process, it is important to take into account Ukraine's interests and capabilities so that it remains competitive and can withstand external challenges.

Results. The relentless development of digital technologies in the field of public administration and security is creating new opportunities for effectively countering modern threats. Digital platforms, analytical systems, and mobile applications are tools for collecting, processing, and analyzing information from external sources, ensuring a rapid response by law enforcement agencies. The reliability of cyber security determines citizens' trust in state institutions, as well as the stability of critical infrastructure and public safety sectors.

An analysis of the experience of leading countries around the world suggests that a comprehensive approach that supports legislative, organizational, and technological measures increases the effectiveness of national security. Modernizing software and server infrastructure will help ensure the rapid detection and recovery of digital systems after cyberattacks. The professional development of IT specialists will contribute to the continuous functioning of digital services and effective interaction between cyber security entities. The integration of AI, blockchain, and big data technologies will contribute to the creation of more adaptive and resilient management systems, which are currently undergoing continuous modernization.

Further scientific research into the effectiveness of digital platforms and the assessment of risks to critical infrastructure and public order should focus on developing optimal models of interagency cooperation, assessing potential threats in real time, and improving regulatory and legal frameworks to ensure the stability and security of state systems in the context of modern societal development.

Bibliography

1. Новікова Н., Бойко Л. Цифровізація та національна безпека: тенденції та виклики. *Національна безпека: право та економіка.* 2024. Вип. 1(1). С. 72-77. DOI: http://doi.org/10.51369/3083-5917-2024-1-8

2. Яровой Т.С. Ретроспектива цифровізації в системі національної безпеки крізь призму публічного управління. *Вчені записки ТНУ імені В.І. Вернадського.* 2025. Вип. 1. 2025. С. 175-180. DOI https://doi.org/10.32782/TNU-2663-6468/2025.1/29

3. Бігняк П.І., Михальчук В.М. Реформування державного управління: цифровізація. *Інвестиції: практика та досвід.* 2021. № 15. С. 107–113. DOI: 10.32702/2306-6814.2021.15.107

4. Собко О.О., Макарова О.П. Вплив цифровізації та технологічних інновацій на забезпечення громадсько безпеки. ГО МОПЛ, 2024. С. 39-43. URL:https://dspace.univd.edu.ua/entities/publication/d9c99d55-f315-4558-a4c7-55c5b2267dd1

5. Руденко Є., Шапран О., Махно Є. Цифрова трансформація як фактор покращення національної безпеки України. *Публічне управління та місцеве самоврядування.* 2024. Вип. 2. С. 65-69. DOI: https://doi.org/10.32782/2414-4436/2024-2-9

6. Світличний В.С. Захист персональних даних в умовах воєнного стану в Україні. *Право і безпека.* 2023. Вип. 3(90). С. 226-236. DOI: https://doi.org/10.32631/pb.2023.3.19

7. Костенко В.О., Кринична І.П., Журбинський Д.А. Актуальність посилення кібербезпеки України в умовах воєнного стану в контексті Європейської інтеграції. *Публічне управління і адміністрування в Україні.* 2023. Вип. 34. С. 74-77. DOI https://doi.org/10.32782/ pma2663-5240-2023.34.14

8. Яровой Т.С. Ретроспектива цифровізації в системі національної безпеки крізь призму публічного управління. *Вчені записки ТНУ імені В.І. Вернадського.* 2025. Вип. 1. С. 175-180. DOI https://doi.org/10.32782/TNU-2663-6468/2025.1/29

9. Степаненко Н. Забезпечення прав людини в умовах цифрових технологій під час воєнного конфлікту. *Вісник Національного університету «Львівська політехніка».* 2025. Вип. 2(46). С. 312-320. DOI https://doi.org/10.23939/law2025.46.312

10. Офіційний сайт State Service for Special Communications and Information Protection of Ukraine (Держспецзв'язку). URL: https://scpc.gov.ua/en/main-functions-and-tasks

11. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури: Закон України від 27.03.2025. № 4336IX URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text

12. ДЦКЗ Держспецзв'язку посилює кіберзахист України за підтримки Агентства США з міжнародного розвитку. 2024. URL:https://scpc.gov.ua/uk/articles/377

References

1. Novikova, N., Boyko, L. (2024). Tsyfrovizatsiya ta natsional'na bezpeka: tendentsiyi ta vyklyky [Digitalization and national security: trends and challenges] *Natsional'na bezpeka: pravo ta ekonomika – National security: law and economics*. 1(1). 72–77. DOI: http://doi.org/10.51369/3083-5917-2024-1-8 [in Ukrainian].

2. Yarovoy, T.S. (2025). Retrospektyva tsyfrovizatsiyi v systemi natsional′noyi bezpeky kriz' pryzmu publichnoho upravlinnya [Retrospective of digitalization in the national security system through the prism of public administration]. *Vcheni zapysky TNU imeni V.I. Vernads'koho – Scientific notes of V.I. Vernadsky TNU.* 1. 175–180. DOI: https://doi.org/10.32782/TNU-2663-6468/2025.1/29 [in Ukrainian].

3. Bignyak, P. I., Mykhalchuk, V. M. (2021) Reformuvannya derzhavnoho upravlinnya: tsyfrovizatsiya [Reforming public administration: digitalization] Investytsiyi: praktyka ta dosvid – Investments: practice and experience. 15. 107–113. DOI: 10.32702/2306-6814.2021.15.107 [in Ukrainian].

4. Sobko, O.O., Makarova, O.P. (2024). Vplyv tsyfrovizatsiyi ta tekhnolohichnykh innovatsiy na zabezpechennya hromads′ko bezpeky [The impact of digitalization and technological innovations on ensuring public safety] HO MOPL – NGO MOPL. 39-43. Retrieved from: https://dspace.univd.edu.ua/entities/publication/d9c99d55-f315-4558-a4c7-55c5b2267dd1 [in Ukrainian].

5. Rudenko, E., Shapran, O., Makhno, E. (2024). Tsyfrova transformatsiya yak faktor pokrashchennya natsional′noyi bezpeky Ukrayiny [Digital transformation as a factor in improving the national security of Ukraine]. *Publichne upravlinnya ta mistseve samovryaduvannya – Public administration and local self-government*. 2. 65–69. DOI: https://doi.org/10.32782/2414-4436/2024-2-9 [in Ukrainian].

6. Svitlychny, V.S. (2023). Zakhyst personal'nykh danykh v umovakh voyennoho stanu v Ukrayini [Protection of personal data under martial law in Ukraine*]. Pravo i bezpeka – Law and Security.* 3(90). 226–236. DOI: https://doi.org/10.32631/pb.2023.3.19 [in Ukrainian].

7. Kostenko, V.O., Krynychna, I.P., Zhurbinsky, D.A. (2023). Aktual'nist' posylennya kiberbezpeky Ukrayiny v umovakh voyennoho stanu v konteksti Yevropeys′koyi intehratsiyi [The relevance of strengthening Ukraine's cybersecurity under martial law in the context of European integration] *Publichne upravlinnya i administruvannya v Ukrayini – Public administration and administration in Ukraine.* 34. 74–77. DOI https://doi.org/10.32782/ pma2663-5240-2023.34.14 [in Ukrainian].

8. Yarovoy, T.S. (2025). Retrospektyva tsyfrovizatsiyi v systemi natsional'noyi bezpeky kriz′ pryzmu publichnoho upravlinnya [Retrospective of digitalization in the national security system through the prism of public administration]. *Vcheni zapysky TNU imeni V.I. Vernads'koho – Scientific notes of V.I. Vernadsky TNU*. 1. 175–180. DOI https://doi.org/10.32782/TNU-2663-6468/2025.1/29 [in Ukrainian].

9. Stepanenko, N. (2025). Zabezpechennya prav lyudyny v umovakh tsyfrovykh tekhnolohiy pid chas voyennoho konfliktu [Ensuring human rights in the context of digital technologies during military conflict]. *Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika". – Bulletin of the National University "Lviv Polytechnic".* 2(46). 312–320. DOI https://doi.org/10.23939/law2025.46.312 [in Ukrainian].

10. Ofitsiynyy sayt State Service for Special Communications and Information Protection of Ukraine (Derzhspetszv'yazku) [Official website of the State Service for Special Communications and Information Protection of Ukraine (Dershpetszvyazku)]. Retrieved from: https://scpc.gov.ua/en/main-functions-and-tasks [in Ukrainian].

11. Pro vnesennya zmin do deyakykh zakoniv Ukrayiny shchodo zakhystu informatsiyi ta kiberzakhystu derzhavnykh informatsiynykh resursiv, ob'yektiv krytychnoyi informatsiynoyi infrastruktury: [On Amendments to Certain Laws of Ukraine on Information Protection and Cybersecurity of State Information Resources and Critical Information Infrastructure Facilities] Law of Ukraine dated 03.27.2025. No. 4336 IX Retrieved from: https://zakon.rada.gov.ua/laws/show/4336-20#Text [in Ukrainian].

12. DTSKZ Derzhspetszv'yazku posylyuye kiberzakhyst Ukrayiny za pidtrymky Ahent·stva SSHA z mizhnarodnoho rozvytku. [The State Central Communications Service of the State Special Communications Service Strengthens Ukraine's Cybersecurity with the Support of the United States Agency for International Development]. 2024. Retrieved from: https://scpc.gov.ua/uk/articles/377 [in Ukrainian].

Дата першого надходження статті до видання: 16.03.2026
Дата прийняття статті до друку після рецензування: 04.05.2026
Дата публікації (оприлюднення) статті: 29.05.2026