УДК 351.72
JEL H5
DOI: https://doi.org/10.53920/ES-2024-1-2

Maryna KUTOVA,
PhD student of Department
of Management and Administration,
Chernihiv Polytechnic National University
ORCID ID: 0009-0007-1693-7278

THE FRAMEWORK OF INFORMATION SECURITY IN E-GOVERNANCE SYSTEM

The digital transformation of governance has underscored the critical importance of information security within e-governance systems, juxtaposed against an ever-evolving landscape of cyber threats. This article explores the framework of information security in e-governance, focusing on the multifaceted challenges and strategies pivotal for safeguarding digital government services. It emphasizes the dual-edged nature of digital technologies, which, while driving progress and innovation, also spawn sophisticated threats such as cybercrime, spyware, data breaches, and information warfare. A comprehensive approach, integrating legislative, organizational, technical, and educational tools, is advocated to fortify the information space against these threats. The paper provides analysis of existing and potential cyber threats, underscoring the necessity for a dynamic, responsive information security policy that encompasses continuous development and international cooperation. By delving into the Ukrainian context, the article highlights the efforts and challenges in aligning national e-governance information security measures with international standards, illustrating the critical roles played by various governmental bodies in implementing these strategies. This scholarly narrative contributes to the academic and practical discourse on enhancing e-governance information security, offering insights into effective measures for protecting information assets and ensuring the resilience of digital governance systems against global cyber challenges.

Keywords: *e-governance, information security, cyber threats, digital government, cybersecurity strategies.*

Марина Анатоліївна КУТОВА,
аспірантка кафедри менеджменту та адміністрування,
Національний університет «Чернігівська політехніка»

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ЕЛЕКТРОННОГО УРЯДУВАННЯ

В епоху цифровізації управління та адміністрування захист інформації в системах електронного урядування стає пріоритетним завданням для забезпечення національної безпеки та захисту громадянських прав. Ця стаття аналізує ключові аспекти інформаційної безпеки в контексті е-врядування, визначаючи основні виклики та розробляючи стратегії підвищення ефективності захисту цифрових державних сервісів від кіберзагроз. Вона висвітлює, як швидкий розвиток цифрових технологій сприяє прогресу, водночас породжуючи нові ризики, такі як кіберзлочини, витоки даних, інформаційні війни та інші форми кібератак. Автор наголошує на важливості формування комплексного підходу до захисту інформаційного простору, що містить застосування законодавчих, організаційних, технічних та освітніх заходів. Стаття проводить аналіз існуючих і потенційних кіберзагроз та підкреслює необхідність розробки динамічної політики інформаційної безпеки, здатної адаптуватися до постійно змінюваних умов кіберпростору. Це передбачає неперервний розвиток та вдосконалення національних систем інформаційної безпеки, активне залучення міжнародного досвіду та поглиблену співпрацю з міжнародними організаціями. Зокрема, на прикладі України демонструються зусилля та виклики в гармонізації національних заходів безпеки електронного урядування з міжнародними стандартами, а також розкривається ключова роль різних державних органів щодо впровадження стратегій кібербезпеки. У статті акцентується на важливості комплексного розуміння інформаційної безпеки, що охоплює не лише технічні аспекти захисту даних, а й організаційні, правові та освітні ініціативи. Автор пропонує низку конкретних рекомендацій, спрямованих на підвищення рівня захищення інформаційних систем в умовах електронного урядування, включаючи регулярну оцінку ризиків, розробку та впровадження відповідних заходів безпеки, законодавче забезпечення, підвищення обізнаності та підготовку до ефективного реагування на інциденти.

Також наголошується на значенні міжнародної співпраці в обміні знаннями та стратегіями протидії кіберзагрозам.

Ключові слова: *електронне урядування, інформаційна безпека, кіберзагрози, цифровий уряд, стратегії кібербезпеки.*

Problem Statement. In today's globalized world, where information flows span the entire globe, information has transformed into an exceptionally valuable resource, the worth and significance of which often surpass the traditional understanding of material and financial assets. Its strategic role in shaping international relations, economic development, and ensuring national security grants it the status of a critical asset within the global information ecosystem. Consequently, the issue of ensuring information security becomes particularly relevant, attracting meticulous attention at the national level.

The accelerated development of digital technologies, on one hand, fosters progress and innovation, but on the other, it spawns new types of threats to information security, such as cybercrime, spyware, data leaks, information warfare, and other forms of cyberattacks. In response to these challenges, the state must develop a comprehensive approach to protecting its information space, which entails creating an effective information security system. This system should be based on the integration of legislative, organizational, technical, and educational tools.

The formulation and implementation of a national information security policy require a thorough analysis of existing and potential threats, a balanced approach to choosing protection methods, and the ability to quickly adapt to the dynamic conditions of the information space. This implies continuous development and improvement of national information security systems, active incorporation of international experience, and deepened cooperation with international organizations in this sphere.

Goal of article. To explore the critical aspects of information security within the e-government framework, identifying key challenges, and outlining strategies to enhance the protection of digital government services against cyber threats.

Analysis of Recent Research and Publications. In modern times, information has become the most valuable asset at the global level, with its significance and value challenging to quantify. There-

fore, ensuring information security is considered a key task of management at the national level [1]. In such conditions, it is crucial for the state to develop and implement legislative, organizational, technical, and other measures and methodologies that are effective against existing threats to the information space and critical information, reflecting the state's policy in the sphere of information security.

The interpretation of information security within the context of national security involves the comprehensive protection of information and information systems from a wide range of threats. According to definitions provided by authoritative sources such as the National Institute of Standards and Technology (NIST), information security is fundamentally about safeguarding information and systems by preventing unauthorized access, use, disclosure, disruption, modification, or destruction [4]. This ensures the confidentiality, integrity, and availability of information, which are crucial components of information security. These principles apply not only to digital information but also to all forms of communication and data storage, making information security a critical aspect of national security efforts.

National security strategies increasingly recognize the importance of protecting information infrastructure as part of safeguarding a nation's security. This includes measures to defend against cyber threats, espionage, and other forms of information warfare that could compromise national security. Given the interconnected nature of global information systems, the protection of information security extends beyond national borders, requiring international cooperation and adherence to global standards and best practices.

Main Research Findings. Information security, in the context of directly protecting information, encompasses a comprehensive set of measures aimed at safeguarding information from unauthorized access, use, disclosure, destruction, modification, viewing, inspection, recording, or extraction. The application of information security can be considered within the context of state-level security, organizational security, and individual personal security. State information security ensures the protection of vital interests of individuals, society, and the state from potential harm that could arise from deficiencies in the completeness, timeliness, or accuracy of the information used, negative information influence, adverse consequences of using information technologies, as well as illegal dissemination and breaches of integrity, confidentiality, and availability of information. Orga-

nizational information security requires targeted actions from their management to ensure the safety of the information environment, which contributes to their stable functioning and development. Personal information security implies protection from negative information impacts and guarantees the possibility of unhindered searching, collecting, processing, and using information, as well as ensuring the protection of social groups to which the individual belongs [2].

In the realm of digital governance, the assurance of information security is a cornerstone in safeguarding the interests of individuals, society, and the state within the information domain. This multifaceted issue has given rise to various classifications of threats, each bearing potential negative consequences. A scholarly dissection of these threats offers a granular understanding essential for developing robust protection strategies. Herein, we delve into a refined categorization of such threats (figure 1).

THREATS TO INFORMATION SECURITY		
Arising from the Dissemination of Substandard Information	***Stemming from Unauthorized and Illegitimate Access***	***Informational Rights and Freedoms***
This category encapsulates the spread of misinformation, disinformation, and fake news capable of distorting reality and manipulating public perception. These threats undermine societal trust, distort public discourse, and can significantly impact state governance and societal harmony by fostering misinformation campaigns and undermining the democratic process.	Involving unauthorized entities seeking to infiltrate information systems, this group encompasses cyber-attacks, data breaches, and other forms of illicit access. Such activities aim to compromise the confidentiality, integrity, and availability of information, posing a direct threat to national security and individual privacy.	This group concerns violations of individual rights in the information sphere, including breaches of privacy, intellectual property rights, freedom of expression, and access to information. It highlights the conflict between the need for security measures and the protection of fundamental human rights, underscoring the importance of legal and ethical frameworks in information security.

Figure 1. Threats to information security

Source: Developed by the author based on [1, 2]

The overarching threat to information security can thus be viewed as any potential event, action, process, or phenomenon capable of adversely affecting the information security system. This includes risks to system components that could lead to information loss, destruction, or compromises in functionality. Implementing countermeasures to these threats is crucial for maintaining the stability and security of the information space.

To aid in understanding and addressing these risks, a detailed classification of threats is invaluable. It encompasses the nature of threats, including natural disasters and human-made actions, whether accidental or deliberate, and distinguishes between external and internal sources. This classification extends to the impact level on systems – distinguishing passive from active threats – and differentiates the methods of access to information system resources, highlighting standard and non-standard access routes. Such a granular approach not only facilitates a comprehensive risk assessment but also guides the formulation of effective information security strategies, ensuring a balanced approach that protects against threats while upholding democratic values and rights [2].

The objective and tasks of ensuring information security within the e-governance system are pivotal to maintaining the integrity, confidentiality, and availability of digital government services. This section for a scholarly article delineates the overarching goal and the specific tasks required to achieve a robust information security framework in e-governance.

The primary objective of information security in the e-governance system is to protect and secure the government's digital assets from various cyber threats and risks. This includes safeguarding sensitive data pertaining to the nation's citizens, ensuring the reliability and availability of e-government services, and preserving the public's trust in digital government initiatives. Achieving this objective is essential for the smooth functioning of e-governance platforms, facilitating efficient public service delivery, and enhancing the democratic process through digital means.

To accomplish the stated objective, several specific tasks must be undertaken, each contributing to the overall information security framework:

1. Risk Assessment. Regularly evaluate the e-governance infrastructure to identify potential vulnerabilities and threats. This

involves conducting comprehensive risk analyses to understand the landscape of possible cyber threats and their impact on e-governance services.

2. Implementation of Security Measures. Develop and deploy appropriate technological and procedural security measures to mitigate identified risks. This includes the use of encryption, firewalls, intrusion detection systems, and secure software development practices to protect data and systems.

3. Legislation and Policy Formation. Establish robust legal and regulatory frameworks that define standards, protocols, and guidelines for information security in e-governance. This task involves crafting policies that align with international best practices and ensuring compliance with these policies across all digital government platforms.

4. Awareness and Training. Educate government employees, as well as the public, on the importance of information security and promote best practices for safe online behavior. This includes regular training sessions and the dissemination of information on potential cyber threats and how to avoid them.

5. Incident Response and Recovery. Develop a comprehensive incident response plan to quickly address security breaches or data loss incidents. This task is critical for minimizing the impact of cyber-attacks and ensuring a swift recovery of e-governance services.

6. Collaboration and Sharing. Foster collaboration among government agencies, private sector, and international bodies to share knowledge, intelligence, and strategies for dealing with cyber threats. This collaborative approach enhances the ability to anticipate, prevent, and respond to cyber incidents effectively.

Ensuring information security within the e-governance system is a multifaceted goal that requires coordinated efforts across various tasks. By addressing these tasks diligently, governments can protect their digital infrastructure from cyber threats, thereby ensuring the confidentiality, integrity, and availability of e-governance services. This not only enhances public service delivery but also bolsters citizens' confidence in digital government initiatives.

In crafting a scholarly narrative on information security threats within the e-governance framework, it is paramount to leverage relevant legal frameworks and scholarly discourse to offer a nuanced analysis that contributes to the academic and practical understanding of information security challenges.

Under Ukrainian law, overcoming information security problems at the national level entails the execution of a series of measures, which include:

- Creating an effective information infrastructure of the country and ensuring the protection of its key components;
- Enhancing coordination between government institutions for the identification, assessment, and prediction of information threats, as well as preventing these threats and mitigating their consequences, including international cooperation in this field;
- Updating and improving the legislative framework to ensure information security, particularly concerning the protection of information resources, combating cybercrime, protecting personal data, and conducting law enforcement activities in this domain;
- Implementing and developing the National Confidential Communication System as a modern secure network for the integration of geographically dispersed information systems that process confidential information [2].

In the context of ensuring information security in the Ukrainian e-governance system, several key state organs play a critical role. An examination of their functions allows for a deeper understanding of the structure and mechanisms of the e-governance system [2].

The central executive body responsible for the formation and implementation of state policy in the sphere of e-governance in Ukraine is the State Agency for E-Governance of Ukraine. Its main tasks include the development of electronic services for citizens and businesses, enhancing the transparency and accessibility of public information, and the adoption of cutting-edge technologies to optimize administrative processes. The agency coordinates the development of the national electronic data infrastructure, establishes conditions for the integration of electronic services, and ensures information security within the realm of e-governance.

The State Service of Special Communication and Information Protection of Ukraine specializes in safeguarding the country's information space and critical information infrastructure components [3]. Its key responsibilities include protecting state information, overseeing the dissemination of confidential information, and developing and implementing information security standards. This service plays

a crucial role in combating cyber threats and attacks, ensuring the uninterrupted operation of state information systems.

Within the context of e-governance, the Ministry of Justice is responsible for managing electronic digital signatures, a fundamental element in ensuring information security and user authentication in state electronic services. Electronic signatures guarantee the integrity and confidentiality of services and the accountability for executive orders and decisions.

Furthermore, public administration bodies contain specialized information support units. These units develop and implement information security policies and procedures, responsible for creating, operating, and maintaining information security management systems. They also protect information from unauthorized access, use, disclosure, alteration, or destruction. The work of these units includes regular audits and monitoring of information systems, risk and vulnerability assessments, and the development and implementation of measures to prevent and respond to information security incidents.

The activities of these bodies are supported by two main legislative acts, namely the Law of Ukraine "On Electronic Trust Services" regulating the use of electronic digital signatures, which is a critical aspect of ensuring information security in e-governance; and the Law of Ukraine «On Protection of Information in Information and Telecommunication Systems» which establishes the legal and organizational foundations for information protection. For Ukraine, aiming to integrate into the European community, it is critically important to align national legislation with European standards. This process involves both the adoption of new legislative acts and the modernization and supplementing of the existing legal framework. One of the key tasks is to create an effective national standardization system in the field of information security that would take into account international requirements for information exchange and protection.

Summary. The proliferation of digital technologies, while propelling progress and innovation, has simultaneously introduced sophisticated threats to information security, such as cybercrime, spyware, and data breaches. Central to the discussion is the imperative for nations to develop a comprehensive and coherent approach towards protecting their information spaces. This entails the adoption

of a multifaceted strategy that integrates legislative frameworks, organizational measures, technological defenses, and educational initiatives aimed at both government employees and the public. It is important, a national information security policy that is responsive to the dynamic cyber threat landscape, advocating for continuous adaptation and enhancement of information security systems.

Focusing specifically on the e-government domain, the piece outlines the objectives of ensuring the confidentiality, integrity, and availability of government digital services. This includes conducting thorough risk assessments, implementing state-of-the-art security measures, establishing legal and regulatory frameworks, promoting cybersecurity awareness, and preparing for effective incident response. Moreover, the article emphasizes the necessity of international collaboration in sharing knowledge and strategies to combat cyber threats more effectively.

The Ukrainian experience in enhancing e-government information security provides a practical case study, illustrating the efforts made to align national legislation with international standards, the roles of key governmental bodies in implementing cybersecurity measures, and the challenges faced in protecting digital government infrastructure.

ЛІТЕРАТУРА

1. Карпенко О.В., Денисюк Ж.З., Наместнік В.В. Цифрове врядування. Київ. 2020. 336 с.

2. Електронне урядування та електронна демократія : навч. посіб. : у 15 ч. / за заг. ред. А. І. Семенченка, В. М. Дрешпака. Захист інформації в системах електронного урядування. Ч. 13/ О. М. Хошаба. Київ : ФОП Москаленко О. М. 2017. 72 с.

3. Про Стратегію національної безпеки України. Указ Президента України про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020/print.

4. Kissel, R. (2013), Glossary of Key Information Security Terms, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology. Gaithersburg. MD [online]. URL: https://doi.org/10.6028/NIST.IR.7298r2 (Accessed February 18. 2024).

REFERENCES

1. Karpenko O.V., Denysiuk Zh.Z., Namestnik V.V. Tsyfrove vriaduvannia. Kyiv. 2020. 336 p.

2. Elektronne uriaduvannia ta elektronna demokratiia : navch. posib. : u 15 ch. / za zah. red. A. I. Semenchenka, V. M. Dreshpaka. Zakhyst informatsii v systemakh elektronnoho uriaduvannia. Chastyna 13/ O. M. Khoshaba. Kyiv : FOP Moskalenko O. M. 2017. 72 p.

3. Pro Stratehiiu natsionalnoi bezpeky Ukrainy. Ukaz Prezydenta Ukrainy pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020/print.

4. Kissel, R. (2013), Glossary of Key Information Security Terms, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology. Gaithersburg. MD [online]. URL: https://doi.org/10.6028/NIST.IR.7298r2 (Accessed February 18. 2024).

СТАТТЯ НАДІЙШЛА ДО РЕДАКЦІЇ 05.02.2024