АНОТАЦІЯ

Лазарів В.О. Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 281 Публічне управління та адміністрування. – Карпатський національний університет імені Василя Стефаника, Міністерство освіти і науки України. Івано-Франківськ, 2025.

У роботі здійснено комплексне дослідження теоретичних засад та світового досвіду щодо механізмів публічного управління інформаційною безпекою надання електронних послуг; обґрунтовано пропозиції щодо удосконалення цих механізмів з урахуванням світового досвіду.

Проаналізовано понятійно-категоріальний апарат дослідження механізмів публічного управління інформаційною безпекою надання електронних послуг. Зазначено, що «механізми публічного управління інформаційною безпекою надання електронних послуг» – це сукупність взаємопов'язаних нормативно-правових, організаційно-інституційних, технологічних та соціально-комунікативних інструментів, за допомогою яких органи публічної влади формують, реалізують і контролюють політику захисту електронних послуг від інформаційних загроз, забезпечуючи конфіденційність, цілісність, доступність і довіру до цифрових сервісів.

Систематизовано проблеми публічного управління інформаційною безпекою надання електронних послуг. В умовах воєнного стану проблеми публічного управління інформаційною безпекою надання електронних послуг виявилися комплексними та багатовимірними, поєднуючи технічні, організаційно-адміністративні, правові й соціальні чинники. Технічний вимір стосується вразливості державних ІТ-систем, які здебільшого проєктувалися у мирний час без урахування масштабних кризових сценаріїв, що зумовлює залежність від зовнішніх постачальників і підвищує ризик комбінованих атак. Організаційно-

адміністративні бар’єри проявляються у фрагментації відповідальності між різними суб’єктами, нестачі фахівців у державному секторі та необхідності інтеграції приватних і волонтерських структур у систему реагування, що створює ризики управлінської неузгодженості. Правове поле перебуває у стані постійної напруги, оскільки держава змушена балансувати між обмежувальними заходами задля захисту національної безпеки та зобов’язаннями щодо дотримання прав людини і прозорих процедур оскарження. Особливу гостроту мають проблеми доступу та цифрової рівності, адже перебої в електро- й телекомунікаційних мережах ставлять під загрозу реалізацію базових прав громадян через неможливість отримання електронних послуг.

Здійснено аналіз публічного управління інформаційною безпекою надання електронних послуг в Німеччині, Естонії, Данії, Литві, Сінгапурі, Південній Кореї, Тайвані, США. Зазначено, що досвід провідних країн світу у сфері публічного управління інформаційною безпекою електронних послуг демонструє широкий спектр підходів, які поєднують технологічні інновації, інституційні механізми та нормативно-правове забезпечення. Німеччина робить акцент на комплексному законодавчому регулюванні, інтегруючи стандарти кіберзахисту до державного управління та діяльності приватних постачальників послуг. Особливе значення приділяється обов’язковості виконання вимог до критичної інфраструктури, що забезпечує високий рівень стійкості та передбачуваності управлінських рішень. Естонія є прикладом формування цифрової держави, де побудова національної системи кіберзахисту спирається на принципи взаємодії держави й суспільства, інтегровану платформу обміну даними та розвиток спеціалізованих кіберструктур. Важливо, що естонська модель демонструє ефективність саме завдяки прозорості й довірі до державних інституцій.

Данія виділяється поєднанням децентралізованого управління з високим рівнем координації та контролю, що дозволяє створити гнучку систему реагування на кіберзагрози. Пріоритетом є розробка загальнодержавних стратегій і планів дій, які спрямовані на підвищення цифрової грамотності, формування культури кібербезпеки та довіри громадян до цифрових послуг. Литва, враховуючи

геополітичні ризики, вибудувала модель, зорієнтовану на захист державних інформаційних ресурсів і підвищення стійкості електронних послуг до зовнішніх кібератак. Основна увага зосереджується на міжвідомчій координації, партнерстві з НАТО та ЄС, а також на розвитку власних центрів реагування на інциденти.

Сінгапур демонструє стратегічний підхід, де інформаційна безпека є невід'ємним компонентом національної цифрової економіки. Тут застосовується принцип «безпека за замовчуванням», що означає інтеграцію механізмів кіберзахисту в усі етапи надання електронних послуг. Важливу роль відіграють спеціалізовані національні агентства, які координують діяльність у сфері кібербезпеки, а також системна підтримка інновацій, інвестиції у штучний інтелект та аналітику даних для передбачення і запобігання загрозам. Південна Корея демонструє ефективність завдяки глибокій інтеграції кібербезпеки в державну цифрову інфраструктуру, активному використанню публічно-приватного партнерства та масовій цифровій освіті населення. Тут пріоритетом є не лише технічні механізми захисту, а й розвиток культури інформаційної безпеки на всіх рівнях.

Тайвань у своїй практиці робить акцент на мобілізації національних ресурсів для захисту від кіберзагроз, що мають переважно геополітичний характер. Система управління ґрунтується на принципах швидкого реагування, постійного моніторингу та міжвідомчої координації. Важливим є також акцент на співпраці з громадянським суспільством і залученні IT-спільноти до гарантування безпеки електронних послуг. США представляють одну з найбільш комплексних і розгалужених моделей, яка поєднує багаторівневе регулювання, стратегічне планування, впровадження сучасних стандартів та активну роль спеціалізованих федеральних структур. Значна увага приділяється створенню єдиних підходів до управління ризиками, розвитку інструментів взаємодії міждержавних, приватних і міжнародних партнерів.

Ефективне публічне управління інформаційною безпекою електронних послуг ґрунтується на таких універсальних принципах: стратегічна інтеграція кіберзахисту в систему державного управління; постійний розвиток нормативно-

правового поля відповідно до динаміки загроз; високий рівень міжвідомчої та міжнародної координації; партнерство держави, бізнесу та громадянського суспільства; інвестиції в інновації, цифрову освіту та формування культури кібербезпеки. Водночас кожна країна адаптує ці принципи до власних політичних, економічних та безпекових умов, що забезпечує стійкість і довіру громадян до цифрової держави.

Визначено сучасні механізми публічного управління інформаційною безпекою електронних послуг в Україні. Сформовано концептуальні засади побудови функціонально-ієрархічної моделі механізмів публічного управління інформаційною безпекою електронних послуг, що враховують як сучасні виклики кіберсередовища, так і потреби стратегічного розвитку цифрового врядування. Здійснено класифікацію основних проблемних зон сучасної системи управління ІБ в Україні, серед яких: відсутність цілісної координаційної моделі, фрагментарність нормативно-правового регулювання, недостатня технічна готовність, обмеженість ресурсного забезпечення та низький рівень цифрової грамотності на всіх рівнях публічного управління.

Запропоновано запровадження інноваційного управління в систему інформаційною безпекою надання електронних послуг в умовах цифрової трансформації. Зазначено, що запровадження інноваційного управління в систему інформаційної безпеки електронних послуг в умовах цифрової трансформації постає як стратегічний пріоритет, що виходить за рамки суто технічного захисту та охоплює цілісну управлінську парадигму. Аналіз сучасних міжнародних практик свідчить, що ключовим викликом є поєднання високої швидкості впровадження інновацій та гнучкості цифрових сервісів із необхідністю забезпечення стійкості, надійності й довіри громадян та бізнесу до державних послуг. На відміну від традиційних підходів, що будуються на реактивних механізмах, інноваційне управління орієнтується на принципи «безпеки за дизайном» (security-by-design) та «приватності за дизайном» (privacy-by-design), які інтегрують вимоги безпеки у життєвий цикл електронних сервісів від моменту їхнього проєктування. Це забезпечує не лише зменшення ризиків, а й ефективніше використання ресурсів.

Обґрунтована модель механізмів публічного управління інформаційною безпекою електронних послуг в умовах цифрової трансформації. Модель механізмів публічного управління інформаційною безпекою електронних послуг в умовах цифрової трансформації має цілісний, багаторівневий і стратегічно орієнтований характер, який відображає як національні потреби України, так і кращі міжнародні практики у сфері кіберзахисту. Передусім ключовим досягненням є інтеграція інституційного механізму у вигляді Національної ради з питань інформаційної безпеки електронних послуг, яка виступає центральним координатором у системі управління. Нормативно-правовий механізм у моделі ґрунтується на гармонізації українського законодавства з міжнародними стандартами ISO/IEC 27001, ISO 27005, NIST Cybersecurity Framework та практиками GDPR. Важливим є закріплення принципів «безпека за дизайном» і «приватність за дизайном», що дозволяє враховувати аспекти захищеності ще на етапі створення нових електронних сервісів. Фінансовий механізм формує довгострокову та багатоканальну модель фінансування заходів кіберзахисту, яка передбачає державне бюджетування, створення цільових фондів кіберстійкості, залучення міжнародних грантів та розвиток державно-приватних партнерств. Кадровий механізм моделі передбачає створення професійного кадрового резерву шляхом формування стандартів компетенцій для ключових посад (CISO, адміністраторів реєстрів, аналітиків інцидентів), обов’язкових програм навчання для всіх державних службовців та спеціалізованої підготовки для фахівців. У цьому контексті важливим є впровадження системи сертифікації та безперервного підвищення кваліфікації, що відповідає міжнародним підходам, а також створення механізмів мотивації та утримання кадрів. Контрольний механізм передбачає системну багаторівневу перевірку ефективності заходів із захисту інформації через внутрішні й зовнішні аудити, регулярний моніторинг, індикатори ефективності та механізми санкцій. Інформаційно-комунікативний механізм орієнтований на створення довіри до державних електронних сервісів та формування культури кібербезпеки в суспільстві. Важливо, що модель містить механізм управління

ризиками, заснований на міжнародних стандартах ISO 27005 і NIST SP 800-30, а також передбачає визначення RTO і RPO для критичних сервісів.

Запропоновано розробити та прийняти Концепцію розвитку публічного управління інформаційною безпекою електронних послуг на 2026-2036 роки, в основі якої має бути зазначена вище модель.

Ключові слова: публічне управління, механізми публічного управління, інформація, інформаційна безпека, електронні послуги, адміністративні послуги, публічні послуги, принципи надання адміністративних послуг, публічне управління інформаційною безпекою, публічне управління наданням електронних послуг, цифрові технології, цифровізація, цифровізація публічних послуг, цифрова трансформація, європейська інтеграція

SUMMARY

Lazariv V.O. Mechanisms of public management of information security of electronic services: world experience. – Qualifying scientific work on manuscript rights.

Dissertation for obtaining the scientific degree of Doctor of Philosophy in specialty 281 Public Management and Administration. – Vasyl Stefanyk Carpathian National University, Ministry of Education and Science of Ukraine. – Ivano-Frankivsk, 2025.

The work carries out a comprehensive study of the theoretical foundations of the world experience of public management mechanisms for information security of electronic services, the identification of proposals for improving these mechanisms, taking into account world experience.

The author analyzes the conceptual and categorical apparatus of the study of public management mechanisms for information security of electronic services. "Mechanisms of public management of information security of electronic services" is a set of interrelated regulatory, organizational, institutional, technological and socio-communicative tools, with the help of which public authorities form, implement and control the policy of protecting electronic services from information threats, ensuring confidentiality, integrity, accessibility and trust in digital services.

The work systematizes the problems of public management of information security of electronic services. Under martial law, the problems of public management of information security in the provision of electronic services turned out to be complex and multidimensional, combining technical, organizational-administrative, legal and social factors. The technical dimension concerns the vulnerability of state IT systems, which were mostly designed in peacetime without taking into account large-scale crisis scenarios, which leads to dependence on external suppliers and increases the risk of combined attacks. Organizational-administrative barriers are manifested in the fragmentation of responsibility between different entities, the lack of specialists in the public sector and the need to integrate private and volunteer structures into the response system, which creates risks of managerial incoherence. The legal field is in a state of constant tension, as the state is forced to balance between restrictive measures to protect national security and obligations to respect human rights and transparent appeal procedures. The problems of access and digital equality are particularly acute, as disruptions in electricity and telecommunications networks jeopardize the realization of citizens' basic rights due to the inability to receive electronic services.

The section analyzes public management of information security of electronic services in Germany, Estonia, Denmark, Lithuania, Singapore, South Korea, Taiwan, and the USA. It is noted that the experience of leading countries in the world in the field of public management of information security of electronic services demonstrates a wide range of approaches that combine technological innovations, institutional mechanisms, and regulatory support. Germany emphasizes comprehensive legislative regulation, integrating cybersecurity standards into public administration and the activities of private service providers. Particular importance is placed on the mandatory fulfillment of requirements for critical infrastructure, which ensures a high level of stability and predictability of management decisions. Estonia is an example of the formation of a digital state, where the construction of a national cybersecurity system is based on the principles of state-society interaction, an integrated data exchange platform, and the development of specialized cyber structures. It is important that the Estonian model demonstrates effectiveness precisely due to transparency and trust in state institutions.

Denmark stands out for its combination of decentralized management with a high level of coordination and control, which allows for a flexible system of responding to cyber threats. The priority is the development of nationwide strategies and action plans aimed at increasing digital literacy, forming a culture of cybersecurity and ensuring citizens' trust in digital services. Lithuania, taking into account geopolitical risks, has built a model focused on protecting state information resources and increasing the resilience of electronic services to external cyberattacks. The main focus is on interagency coordination, partnership with NATO and the EU, as well as the development of its own incident response centers.

Singapore demonstrates a strategic approach where information security is an integral component of the national digital economy. The principle of "security by default" is applied here, which means integrating cyber protection mechanisms into all stages of the provision of electronic services. Specialized national agencies that coordinate cybersecurity activities play an important role, as well as systemic support for innovation, investments in artificial intelligence and data analytics to predict and prevent threats. South Korea demonstrates effectiveness through deep integration of cybersecurity into the state digital infrastructure, active use of public-private partnerships and mass digital education of the population. Here, the priority is not only technical protection mechanisms, but also the development of an information security culture at all levels.

Taiwan in its practice emphasizes the mobilization of national resources to protect against cyber threats, which are predominantly geopolitical in nature. The management system is based on the principles of rapid response, constant monitoring and interagency coordination. An emphasis on cooperation with civil society and the involvement of the IT community in ensuring the security of electronic services is also important. The USA represents one of the most complex and extensive models, combining multi-level regulation, strategic planning, implementation of modern standards and the active role of specialized federal structures. Considerable attention is paid to the creation of unified approaches to risk management, the development of tools for interaction between intergovernmental, private and international partners.

Effective public management of information security of electronic services is based on the following universal principles: strategic integration of cyber protection into the public administration system; constant development of the regulatory and legal field in accordance with the dynamics of threats; high level of interagency and international coordination; partnership of the state, business and civil society; investments in innovation, digital education and formation of a culture of cybersecurity. At the same time, each country adapts these principles to its own political, economic and security conditions, which ensures the stability and trust of citizens in the digital state.

The author identifies modern mechanisms of public management of information security of electronic services in Ukraine. Conceptual principles for building a functional-hierarchical model of mechanisms of public management of information security of electronic services, which take into account both modern challenges of the cyber environment and the needs of strategic development of digital governance, have been formed. The main problem areas of the modern information security management system in Ukraine are classified, including: the lack of a holistic coordination model, fragmentation of regulatory and legal regulation, insufficient technical readiness, limited resource provision and a low level of digital literacy at all levels of public administration.

The paper proposes the introduction of innovative management into the information security system of electronic services in the context of digital transformation. It is noted that the introduction of innovative management into the information security system of electronic services in the context of digital transformation appears as a strategic priority that goes beyond purely technical protection and encompasses a holistic management paradigm. An analysis of modern international practices shows that the key challenge is to combine the high speed of innovation implementation and flexibility of digital services with the need to ensure stability, reliability and trust of citizens and businesses in public services. Unlike traditional approaches based on reactive mechanisms, innovation management is guided by the principles of “security-by-design” and “privacy-by-design,” which integrate security requirements into the life cycle of electronic services from the moment they are designed. This not only reduces risks, but also makes more efficient use of resources.

The author substantiates the model of mechanisms for public management of information security of electronic services in the context of digital transformation. The model of mechanisms for public management of information security of electronic services in the context of digital transformation has a holistic, multi-level and strategically oriented nature, which reflects both the national needs of Ukraine and the best international practices in the field of cyber protection. First of all, the key achievement is the integration of an institutional mechanism in the form of the National Council for Information Security of Electronic Services, which acts as a central coordinator in the management system. The regulatory and legal mechanism in the model is based on the harmonization of Ukrainian legislation with international standards ISO/IEC 27001, ISO 27005, NIST Cybersecurity Framework and GDPR practices. It is important to consolidate the principles of "security by design" and "privacy by design", which allows taking into account security aspects even at the stage of creating new electronic services. The financial mechanism forms a long-term and multi-channel model of financing cyber protection measures, which involves state budgeting, the creation of cyber resilience trust funds, attracting international grants and the development of public-private partnerships. The personnel mechanism of the model involves the creation of a professional personnel reserve by forming competency standards for key positions (CISO, registry administrators, incident analysts), mandatory training programs for all civil servants and specialized training for specialists. In this context, it is important to implement a certification system and continuous professional development that meets international approaches, as well as create mechanisms for motivating and retaining personnel. The control mechanism involves a systematic multi-level verification of the effectiveness of information protection measures through internal and external audits, regular monitoring, performance indicators and sanction mechanisms. The information and communication mechanism is focused on creating trust in state electronic services and forming a culture of cybersecurity in society. It is important that the model contains a risk management mechanism based on international standards ISO 27005 and NIST SP 800-30, and also provides for the definition of RTO and RPO for critical services.

The author proposes to develop and adopt the Concept of Development of Public Management of Information Security of Electronic Services for 2026-2036, which is intended to regulate the above model.

Keywords: public administration, mechanisms of public administration, information, information security, electronic services (e-services), administrative services, public services, principles of administrative service delivery, public administration of information security, public administration of electronic service delivery, digital technologies, digitalization, digitalization of public services, digital transformation, European integration

Список опублікованих праць за темою дисертації

Статті в наукових виданнях, включених до переліку наукових фахових видань України:

1. Лазарів В.О. Порівняльний аналіз моделей публічного управління інформаційною безпекою: світовий досвід. *Успіхи і досягнення у науці*. 2025. № 4 (14). С. 606 – 615.

DOI: https://doi.org/10.52058/3041-1254-2025-4(14)-606-615

URL: http://perspectives.pp.ua/index.php/sas/article/view/22944

2. Лазарів В.О. Кібербезпека та публічне управління: виклики та можливості для електронних послуг. *Актуальні питання у сучасній науці*. 2025. № 1(31). С. 281 – 291.

DOI: https://doi.org/10.52058/2786-6300-2025-1(31)-281-291

URL: http://perspectives.pp.ua/index.php/sn/article/view/18787

3. Лазарів В.О. Моделювання процесів публічного управління інформаційними технологіями надання електронних послуг на публічному рівні. *Актуальні питання у сучасній науці*. 2024. № 1(29). С. 378 – 388.

DOI: https://doi.org/10.52058/2786-6300-2024-11(29)-378-388

URL: http://perspectives.pp.ua/index.php/sn/article/view/16517

4. Лазарів В.О. Концептуальні засади публічного управління інформаційною безпекою електронних послуг: теорія та виклики. *Наукові перспективи*. 2023. № 6(36). С. 149 – 150.

DOI: https://doi.org/10.52058/2708-7530-2023-6(36)-143-150

URL: http://perspectives.pp.ua/index.php/np/issue/view/156

Матеріали і тези міжнародних та всеукраїнських конференцій:

5. Лазарів В.О. Цифрова трансформація публічного управління: інституційні механізми захисту інформації при наданні електронних послуг. VII Міжнародна науково-практична конференція «Модернізація економіки: сучасні реалії, прогнозні сценарії та перспективи розвитку», (м. Херсон – м. Хмельницький, Україна, 17-18 квітня 2025 р.). Херсон – Хмельницький, 2025. С. 440-442.

URL: https://kntu.net.ua/ukr/content/download/127190/707962/file/Збірник_тез_доповідей_ХНТУ_2025.pdf

6. Лазарів В.О. Механізми забезпечення кіберстійкості в системі публічного управління електронними послугами: міжнародні практики та українські реалії. 1 Міжнародна науково-практична конференція. Modern Scientific Research: Theoretical and Practical Aspects. (Рига, Латвія, 14-16 квітня 2025 р.). Рига, 2025. С. 84-86.

URL: https://www.eoss-conf.com/arkhiv/modern-scientific-research-theoretical-and-practical-aspects/

7. Лазарів В.О. Політики захисту даних у публічному секторі: кращі світові практики для безпеки електронних послуг. International Scientific Internet Conference (Випуск 95). (Тернопіль – Ополе. 16-17 січня 2025 р.). Тернопіль – Ополе, 2025. С. 29-31.

URL: http://www.konferenciaonline.org.ua/data/downloads/file_1740428622.pdf

8. Лазарів В.О. Інформаційна безпека як складова цифрової трансформації публічних послуг: механізми інтеграції у практику публічного управління. 2

Міжнародна науково-практична конференція. From Ideas to Solutions: Innovations in Science and Technology. (Лондон, Велика Британія, 21-23 квітня 2024 р.). Лондон, 2024. С. 118-120.

URL: https://www.eoss-conf.com/arkhiv/from-ideas-to-solutions-innovations-in-science-and-technology-21-04-25/

9. Лазарів В.О. Цифрові технології як основа для побудови ефективних систем інформаційної безпеки в публічному управлінні. Collection of Scientific Papers with the Proceedings of the 2nd International Scientific and Practical Conference «Innovative Solutions in Science: Balancing Theory and Practice» (San Francisco, USA, December 23-25, 2024). San Francisco, 2024. P. 181-183.

URL: https://www.eoss-conf.com/wp-content/uploads/2024/12/San_Francisco_USA_23.12.2024.pdf

10. Лазарів В.О. Публічне управління інформаційною безпекою: сучасні виклики та перспективи розвитку. Наукова інтеграція в умовах глобальних викликів: збірник тез доповідей IV Міжнародної мультидисциплінарної науково-практичної конференції (Луцьк, 20 червня 2023 р.). Луцьк, 2023. С. 124-127.

URL: https://www.researchgate.net/publication/372438666_NAUKOVA_INTEGRACIA_V_UMOVAH_GLOBALNIH_VIKLIKIV_Zbirnik_tez_dopovidej_IV_MIZNARODNOI_MULTIDISCIPLINARNOI_NAUKOVO-PRAKTICNOI_KONFERENCII

11. Лазарів В.О. Публічне управління інформаційною безпекою: сучасні виклики та перспективи розвитку. Modern Aspects of Modernization of Science: Status, Problems, Development Trends. Materials of the 26th International Scientific and Practical Conference. (м.Загреб, Хорватія, дистанційно, 7 листопада 2022 р.). Загреб, 2022. С. 44-47.

URL: http://perspectives.pp.ua/public/site/conferency/conf-26.pdf