КАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

ЛАЗАРІВ ВЛАДИСЛАВ ОЛЕГОВИЧ

УДК 35.078.3; 004.056.5

ДИСЕРТАЦІЯ

МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НАДАННЯ ЕЛЕКТРОННИХ ПОСЛУГ: СВІТОВИЙ ДОСВІД

Спеціальність: 281 Публічне управління та адміністрування
Галузь знань: 28 Публічне управління та адміністрування

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ Лазарів В.О.

Науковий керівник – Нагорняк Михайло Миколайович, доктор політичних наук, професор

Івано-Франківськ – 2025

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

ЗМІСТ:

Перелік умовних скорочень

ІБ – інформаційна безпека;

GDPR – Загальний регламент захисту даних;

NIS2 – Директива ЄС Network and Information Security Directive;

SO/IEC – міжнародний стандарт в галузі ІТ;

Мінцифри – Міністерство цифрової трансформації України;

МОЗ – Міністерство охорони здоров’я України;

МОН – Міністерство освіти і науки України;

Мінсоцполітики – Міністерство соціальної політики України;

ЦНАП – Центр надання адміністративних послуг;

РНБО – Рада національної безпеки і оборони України;

НКЦК – Національний координаційний центр кібербезпеки;

СБУ – Служба безпеки України;

ДССЗЗІ – Державна служба спеціального зв'язку та захисту інформації України;

ОМС – органи місцевого самоврядування;

ЄС – Європейський Союз.

ВСТУП

Розвиток інформаційного суспільства та цифрових технологій формує нову архітектоніку сучасної цивілізації, у якій інформація набуває статусу ключового стратегічного ресурсу для всіх секторів, зокрема і для публічного управління. Трансформація від аграрної до індустріальної, далі до постіндустріальної моделі та, зрештою, до інформаційного суспільства зумовлює зростання ролі обробки, збереження, передачі та захисту інформації як основної цінності соціально-економічного розвитку.

У розвинутих країнах цифрова трансформація охоплює економічну, соціальну сфери та систему надання електронних публічних послуг. У цьому контексті формування та впровадження ефективних механізмів публічного управління інформаційною безпекою стає визначальним чинником стабільності цифрового розвитку держави. Саме механізми публічного управління забезпечують скоординовану дію інституцій, регламентацію процесів, моніторинг ризиків та реалізацію адаптивних управлінських рішень для гарантування безпеки в інформаційному просторі.

Здатність держави розробляти, впроваджувати та оновлювати механізми публічного управління інформаційною безпекою надання електронних послуг визначає рівень її цифрової спроможності, легітимності та довіри з боку громадян. У сучасних умовах ці механізми охоплюють нормативно-правові, організаційно-інституційні, технологічні, кадрові та комунікаційні складові, які взаємодіють у рамках єдиної управлінської системи, спрямованої на протидію загрозам та зміцнення цифрової стійкості.

Інформаційна безпека електронних публічних сервісів є невід’ємною частиною внутрішньої та зовнішньої політики держави, що зумовлює необхідність створення дієвих та адаптивних механізмів публічного управління, здатних ефективно реагувати на комплекс загроз: від цілеспрямованих кібератак до витоку персональних даних, від дезінформації до зниження довіри до державних цифрових сервісів.

Для України, яка декларує інтеграцію до Європейського Союзу та орієнтується на принципи прозорості, відкритості, підзвітності та безпеки в публічному управлінні, формування надійних механізмів публічного управління інформаційною безпекою є технологічним, правовим завданням та виявом інституційної відповідальності, елементом демократичного врядування в цифрову епоху.

Особливої актуальності проблематика забезпечення інформаційної безпеки набула в умовах повномасштабної військової агресії російської федерації проти України. На передній план вийшли ризики, пов’язані з деструктивними впливами на інформаційний простір: поширенням дезінформації та фейків, хакерськими атаками на державні ресурси, маніпуляцією громадською думкою, незаконним збором та використанням персональних даних. У таких умовах захист інформаційної інфраструктури, що забезпечує функціонування електронних публічних послуг, стає критичним завданням публічного управління.

Вирішення цього завдання потребує системного розгортання ефективних механізмів публічного управління інформаційною безпекою, які ґрунтуються на принципах кіберстійкості, правової визначеності, технологічної спроможності та інституційної взаємодії між органами влади, приватним сектором і громадянським суспільством. Такі механізми мають забезпечувати безперервність управлінських процесів, оперативне реагування на загрози, прозорість і підзвітність дій органів публічного управління у сфері інформаційної безпеки.

Отже, необхідність формування, впровадження та постійного вдосконалення механізмів публічного управління інформаційною безпекою у сфері електронних послуг в умовах цифрової трансформації та постійних безпекових викликів обумовлює теоретичну цінність та високу практичну значущість обраної теми дисертаційного дослідження. Системне дослідження зазначених механізмів дозволить сформувати науково обґрунтовані підходи до побудови ефективної моделі механізмів публічного управління в умовах гібридних загроз і нестабільності.

Теоретичні, методичні та практичні аспекти дослідження цифровізації електронних послуг, формування інформаційної безпеки розглядають вітчизняні та зарубіжні вчені, зокрема: А. Алієв [1], І. Андріянов [2], Є. Архіпова [3], Г. Бондар [4], В. Бондаренко [5], В. Борисенко [6], О. Бурдяк [7], З. Бурик [8], Л. Буряк [9], О. Вальчук [10], Д. Гарфінкель [11], Р. Гасимов [12], Г. Гнатієнко [13], К. Гончаренко [14], Н. Грабар [15], П. Гриценко [16], М. Гупта [17], Д. Дєгтяр [18], В. Дзюндзюк [19], І. Динник [20], І. Доронін [21], О. Євтушенко [22], С. Єсімов [23], К. Єфремова [24], М. Засуха [25], М. Ільницький [26], С. Карасаєв [27], П. Клімушин [28], Н. Пасенко [29-30], І. Ковбас [31], М. Ковтун [32], О. Кожушко [33], Ю. Котельникова [34], В. Котляров [35], О. Красногор [36], І. Криворучко [37], Т. Кужда [38], Г. Куспляк [39], В. Лонська [51], К. Майстренко [52], Т. Маматова [53-54], І. Матюшенко [55], А. Мгалоблішвілі [56], М. Нагорняк [57-58], Е. Наджафлі [59], Г. Нестеренко [60], Р. Новосад [61], О. Оболенський [62], Н. Опар [63], Н. Орлова [64], О. Панченко [65], О. Пархоменко-Куцевіл [66], П. Покатаєв [67], О. Пучков [69], І. П'ятничук [70-71], І. Риженко [72], В. Саприкін [75], І. Сердюк [76], Н. Сидоренко [77], Ж. Сільва [78], І. Скляр [79-80], Л. Спицька [81], О. Соловйова [82], А. Соломаха [83], А. Сурай [84], І. Тищенкова [85], М. Тюхтій [86], О. Угоднікова [87], А. Чечель [88], Г. Чміль [89], Я. Чмир [90], С. Чукут [91], С. Шандрук [92], С. Шийович [93], І. Шопіна [94], Є. Щербина [95] та ін.

Проведений аналіз літературних джерел підтверджує наукову і практичну актуальність дослідження механізмів публічного управління інформаційною безпекою у сфері надання електронних послуг. Водночас можна констатувати, що на сьогодні відсутні системні дослідження механізмів публічного управління інформаційною безпекою надання електронних послуг в умовах цифрової трансформації.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертація виконана відповідно до плану науково-дослідних робіт Карпатського національного університету імені Василя Стефаника за темою: «Теоретико-методологічні та прикладні засади розроблення і функціонування інноваційних механізмів публічного управління та адміністрування» (номер

державної реєстрації 0120U100494). У межах теми автором проведені дослідження, пов'язані з розробкою механізмів публічного управління забезпечення кібербезпеки надання електронних послуг.

Метою дисертаційного дослідження є обґрунтування та розробка концептуальних теоретико-методичних і науково-практичних підходів до формування, впровадження та вдосконалення механізмів публічного управління інформаційною безпекою надання електронних послуг в умовах цифрової трансформації, гібридних загроз і глобальних безпекових викликів.

Для досягнення поставленої мети в дисертаційному дослідженні визначено такі *завдання*:

– визначити наукові підходи до механізмів публічного управління інформаційною безпекою надання електронних послуг;

– проаналізувати понятійно-категоріальний апарат дослідження механізмів публічного управління інформаційною безпекою надання електронних послуг;

– систематизувати проблеми публічного управління інформаційною безпекою надання електронних послуг;

– здійснити аналіз стану публічного управління інформаційною безпекою електронних послуг у країнах ЄС;

– дослідити розвиток публічного управління інформаційною безпекою електронних послуг в азійських країнах;

– охарактеризувати модернізацію публічного управління інформаційною безпекою електронних послуг у США;

– оцінити сучасні механізми публічного управління інформаційною безпекою електронних послуг в Україні;

– аргументувати запровадження інноваційного управління в систему інформаційної безпеки електронних послуг в умовах цифрової трансформації;

– обґрунтувати модель механізмів публічного управління інформаційною безпекою електронних послуг в умовах цифрової трансформації.

Об’єкт дослідження – суспільні відносини, що виникають при забезпеченні інформаційної безпеки надання електронних послуг в умовах цифрової трансформації та сучасних безпекових викликів.

Предмет дослідження – світовий досвід формування та реалізації механізмів публічного управління інформаційною безпекою надання електронних послуг.

Методи дослідження. Для вирішення поставлених у дослідженні завдань застосовано комплекс загальнонаукових і спеціалізованих методів, які забезпечують цілісне та системне осмислення сутності, структури та функціонування механізмів публічного управління інформаційною безпекою у системі надання електронних послуг. На етапі формування теоретико-методичних засад дослідження використано методи аналізу, синтезу, індукції, дедукції, узагальнення, систематизації та логічного структурування. Застосування цих методів дало змогу здійснити критичне переосмислення наукових підходів, нормативно-правового регулювання та практики впровадження механізмів публічного управління у сфері забезпечення інформаційної безпеки. Для уточнення понятійно-категоріального апарату дослідження, структури, ознак і функціонального змісту механізмів публічного управління інформаційною безпекою застосовано методи класифікації, типологізації, функціонального аналізу, а також методи гносеологічного пізнання з метою виявлення внутрішніх взаємозв’язків і причинно-наслідкових залежностей між елементами досліджуваного управлінського явища. Під час аналізу світового досвіду реалізації механізмів публічного управління в галузі інформаційної безпеки електронних сервісів використовувалися методи компаративного аналізу, узагальнення міжнародних статистичних, нормативних і практичних матеріалів, що дозволило ідентифікувати ефективні моделі управлінських механізмів, релевантні до сучасних викликів цифрової безпеки та до умов функціонування електронного врядування. У третьому розділі, присвяченому розробці напрямів підвищення ефективності впровадження механізмів публічного управління інформаційною безпекою електронних послуг, застосовано методи моделювання, прогнозування, сценарного аналізу та стратегічного планування. Їх використання ґрунтується на оцінці

актуальних тенденцій у сфері інформаційної безпеки, адаптації провідних світових практик до національного контексту, а також на узагальненні результатів попереднього емпіричного дослідження.

Зазначені методи дозволили сформувати концептуальну модель механізмів публічного управління, здатну забезпечити стійкість, адаптивність та ефективність функціонування системи надання електронних публічних послуг в умовах цифрової трансформації, воєнних загроз і потреб післявоєнного відновлення.

Наукова новизна дисертаційного дослідження полягає в комплексному теоретико-методичному обґрунтуванні та розробці концептуальних засад механізмів публічного управління інформаційною безпекою надання електронних послуг в умовах цифрової трансформації, зростаючих безпекових викликів та необхідності адаптації міжнародного досвіду до національного контексту.

Уперше:

– обґрунтована модель механізмів публічного управління інформаційною безпекою надання електронних послуг в умовах цифрової трансформації, яка має цілісний, багаторівневий і стратегічно орієнтований характер та відображає як національні потреби України, так і кращі міжнародні практики у сфері кіберзахисту, до основних елементів якої віднесені: *інституційний механізм* представлений Національною радою з питань інформаційної безпеки електронних послуг; *нормативно-правовий механізм* ґрунтується на гармонізації українського законодавства з міжнародними стандартами; *фінансовий механізм* формує довгострокову та багатоканальну модель фінансування заходів кіберзахисту; *кадровий механізм* передбачає створення професійного корпусу державних службовців; *контрольний механізм* передбачає системну багаторівневу перевірку ефективності заходів із захисту інформації; *інформаційно-комунікативний* механізм орієнтований на створення довіри до державних електронних сервісів та формування культури кібербезпеки в суспільстві;

удосконалено:

– поняття «механізми публічного управління інформаційною безпекою надання електронних послуг» як 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;

– систематизація проблем публічного управління інформаційною безпекою надання електронних послуг через виокремлення наступних кластерів: вразливість державних ІТ-систем, які здебільшого проєктувалися у мирний час без урахування масштабних кризових сценаріїв; фрагментація відповідальності між різними суб'єктами; нестача фахівців у державному секторі; запровадження обмежувальних заходів задля захисту національної безпеки та зобов'язання щодо дотримання прав людини і прозорих процедур оскарження; проблема доступу та цифрової рівності, адже перебої в електро- й телекомунікаційних мережах ставлять під загрозу реалізацію базових прав громадян через неможливість отримання електронних послуг; потреба у розробці національної стратегії кіберстійкості та створення багаторівневих резервних механізмів; потреба в удосконаленні нормативного регулювання з гарантіями прав людини, формалізацію публічно-приватного партнерства та посилення координації між організаційними підрозділами або спеціалізованими командами реагування на комп'ютерні надзвичайні події, операторами критичної інфраструктури та правоохоронними органами;

– закономірності публічного управління інформаційною безпекою електронних послуг в Німеччині, Естонії, Данії, Литві, Сінгапурі, Південній Кореї, Тайвані, США, зокрема виокремлені: системність у формуванні інформаційної безпеки; чіткі нормативно-правові засади формування інформаційної безпеки; прозорість процедур; розвиток державно-приватного партнерства; обов'язковість виконання вимог до критичної інфраструктури; стійкість та передбачуваність управлінських рішень; побудова національної системи кіберзахисту; координація та контроль у діяльності інституцій; формування культури кібербезпеки та забезпечення довіри громадян до цифрових послуг;

– сучасні механізми публічного управління інформаційною безпекою електронних послуг в Україні та сформовані 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;

– механізми запровадження інноваційного управління в систему інформаційної безпеки електронних послуг в умовах цифрової трансформації, які орієнтуються на принципах «безпеки за дизайном» та «приватності за дизайном» та інтегрують вимоги безпеки у життєвий цикл електронних сервісів від моменту їхнього проєктування;

набули подальшого розвитку:

– наукові підходи до механізмів публічного управління інформаційною безпекою надання електронних послуг;

– понятійно-категоріальний апарат дослідження, зокрема: поняття «інформаційна безпека електронних послуг» визначено як структурно інтегрований стан забезпечення конфіденційності, цілісності, доступності та стійкості інформації у процесі надання публічних цифрових сервісів;

– пропозиції щодо імплементації світового досвіду публічного управління інформаційною безпекою надання електронних послуг до національної системи механізмів публічного управління, яка дозволяє адаптувати міжнародні стандарти інформаційної безпеки до українського контексту шляхом інтеграції організаційних, нормативних і цифрових компонентів у цілісну систему публічного управління.

Практичне значення отриманих результатів полягає в тому, що теоретичні положення, висновки, практичні рекомендації дисертації можуть бути використані в діяльності центральних органів державної влади для удосконалення механізмів публічного управління інформаційною безпекою надання електронних послуг з урахуванням світового досвіду.

Результати дисертаційного дослідження були використані в діяльності асоціацій, підрозділів органів місцевого самоврядування, ІТ-компаній, закладів

вищої освіти, а саме: Івано-Франківського регіонального відділення ВАОМС “Асоціація міст України” (акт впровадження № 131/2025 від 18.09.2025 р.), Департаменту інфраструктури, житлової та комунальної політики Івано-Франківської міської ради (акт впровадження), ТОВ «Н-ІКС ДЕЛІВЕРІ» (довідка № 1-1/19-09/2025 від 19.09.2025 р.), Карпатського національного університету імені Василя Стефаника на кафедрі публічного управління та адміністрування (довідка № 03.04-29/22 від 30.10.2025 р.).

Особистий внесок здобувача. Дисертація є самостійно виконаним науковим дослідженням. Наукові розробки, висновки та пропозиції, що містяться в роботі, належать особисто автору. Наукові праці, опубліковані у співавторстві, відсутні.

Апробація результатів дисертації. Основні положення дисертаційного дослідження доповідалися, обговорювалися та отримали позитивну оцінку на 7 міжнародних науково-практичних конференціях: 2 Міжнародній науково-практичній конференції. From Ideas to Solutions: Innovations in Science and Technology. Лондон. Великобританія; VII Міжнародній науково-практичній конференції «Модернізація економіки: сучасні реалії, прогнозні сценарії та перспективи розвитку», (м. Херсон – м. Хмельницький, Україна) 17-18 квітня 2025 року; 1 Міжнародній науково-практичній конференції. Modern Scientific Research: Theoretical and Practical Aspects. Рига. Латвія; International Scientific Internet Conference (Випуск 95). Тернопіль – Ополе. 16-17 січня 2025 року; Collection of Scientific Papers with the Proceedings of the 2nd International Scientific and Practical Conference «Innovative Solutions in Science: Balancing Theory and Practice» (December 23-25, 2024. San Francisco, USA). European Open Science Space, 2024; IV Міжнародній мультидисциплінарній науково-практичній конференції (Луцьк, 20 червня 2023 р.) 2023; Modern Aspects of Modernization of Science: Status, Problems, Development Trends. Materials of the 26th International Scientific and Practical Conference. November 7, 2022, Zagreb (Croatia) remotely.

Публікації. За результатами дослідження опубліковано 11 наукових праць, що належать особисто автору, з яких: 4 статті у виданнях України, які входять до

фахових періодичних видань категорії Б, 7 тез доповідей та матеріалів міжнародних науково-практичних конференцій.

Структура роботи. Дисертаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 233 сторінки, із них 177 сторінка основного тексту. Список використаних джерел налічує 242 найменувань.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ МЕХАНІЗМІВ ПУБЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НАДАННЯ ЕЛЕКТРОННИХ ПОСЛУГ

1.1. Систематизація наукових підходів до механізмів публічного управління інформаційною безпекою надання електронних послуг

Публічне управління інформаційною безпекою на рівні надання електронних послуг слід розглядати як багаторівневу суспільно-технічну проблему, що поєднує нормативно-правові, організаційно-адміністративні, технічні та поведінкові елементи. У міру розгортання електронного уряду та масового використання державних онлайн-сервісів питання забезпечення конфіденційності, цілісності та доступності інформації перестає бути тільки технічною задачею й перетворюється на суспільний ресурс, що потребує системного регулювання, гарантій відповідальності й механізмів довіри між державою й громадянином. Нормативні ініціативи на рівні ЄС (NIS2) та національні рамкові закони про кібербезпеку формують базовий контекст для розробки механізмів управління, визначаючи обов’язки, механізми звітності й мінімальні вимоги до управління ризиками в критичних секторах, до яких належать і е-сервіси публічної адміністрації [126].

Слід зазначити, що в науковій літературі лише фрагментарно аналізується питання механізмів публічного управління інформаційною безпекою надання електронних послуг, частіше розглядаються питання інформаційної безпеки та питання надання електронних послуг.

Тому на початку дослідження проаналізуємо основні підходи до питання механізмів публічного управління інформаційною безпекою надання електронних послуг, які врегульовані у міжнародних нормативних документах.

Питання організації інформаційної безпеки в публічному секторі зазвичай розглядають через призму управлінських систем, де центральним поняттям є інформаційна система управління безпекою (ISMS – система управління інформаційною безпекою). Найпоширенішим і найвпливовішим міжнародним

нормативним стандартом у цій сфері є ISO/IEC 27001:2022 – документ, який формалізує вимоги до побудови, впровадження, підтримки та безперервного вдосконалення ISMS. Офіційний стандарт підкреслює управління ризиками як основу вибору та застосування технічних і організаційних контролів і визначає циклічну логіку поліпшення процесів через цикл PDCA (Plan – плануй, Do – впроваджуй, Check – перевіряй, Act – коригуй) [153].

У науковій літературі ISO/IEC 27001 [153] розглядається не лише як суто технічний набір контролів, але й як соціотехнічна управлінська парадигма, що вимагає інтеграції політик, процедур, ролей і відповідальності, системи внутрішнього й зовнішнього аудиту та стандартизованих механізмів сертифікації. Огляди літератури вказують, що дослідження стандарту фокусуються на трьох взаємопов'язаних рівнях: 1) конфігурація та технічна реалізація контролів (шифрування, автентифікація, контроль доступу, безпека мережі); 2) організаційні процеси (політики, управління ризиками, процедури інцидент-менеджменту, навчання персоналу); 3) інституційні механізми (сертифікація, зовнішній нагляд, вимоги замовників і постачальників). Джованна Кулот і співавтори в огляді літератури підкреслюють, що ISO/IEC 27001 найчастіше вивчають не як статичний набір процедур, а як соціальну практику впровадження стандартизованих управлінських систем, яка має різний вплив залежно від контексту організації та її ресурсів [111].

Циклічний підхід PDCA у вимогах ISO/IEC 27001 задає операційну послідовність: від визначення контексту та цілей (Plan) до застосування контролів (Do), моніторингу і внутрішнього аудиту (Check) і впровадження коригувальних заходів (Act). PDCA підкреслює, що ISMS – це не одноразовий проєкт, а постійний процес, орієнтований на адаптивність до змін у загрозовому ландшафті й у внутрішніх умовах організації. Управління ризиками у стандарті є центральним механізмом для прийняття рішень щодо того, які контролі застосувати та як пріоритезувати ресурси. Практичні гіди й коментарі до стандарту деталізують інструменти ризик-аналізу, критерії прийнятного ризику та вимоги до документування рішень [238].

Сертифікація за ISO/IEC 27001 виконує кілька взаємопов'язаних функцій у державних органах, що надають е-послуги:

1) формалізує процеси й політики, створюючи документовану доказову базу відповідності;

2) служить інструментом зовнішнього довіроутворення перед громадянами і бізнесом;

3) є елементом контрактних вимог у взаємодії з постачальниками (supply-chain);

4) створює рамки для проведення регулярних аудитів і перевірок.

Разом із тим огляди вказують на те, що сертифікація сама по собі не гарантує високої стійкості – її ефективність посилюється за умови наявності компетентного персоналу, підтримки керівництва та ресурсного забезпечення для підтримки і розвитку ISMS. Матео Подрекка та співавтори знаходять кореляцію між впровадженням ISO/IEC 27001 і поліпшеннями у продуктивності та управлінні, але наголошують на залежності ефекту від масштабу і контексту організації [167].

Для державних е-послуг характерною є використання зовнішніх постачальників (хмарні провайдери, інтегратори, розробники). ISO/IEC 27001 містить вимоги до управління відносинами з постачальниками, але практичні дослідження показують, що саме постачальницькі ланцюги часто стають джерелом вразливостей. Отже, у межах ISMS державні органи повинні вбудовувати в контрактні процедури положення щодо безпеки, вимоги до аудиту постачальників та процеси приймання/перевірки оновлень компонентів. Це також вимагає координації між юридичними, закупівельними та IT-підрозділами органів влади [111].

Огляд літератури та кейс-дослідження питання організації інформаційної безпеки в публічному секторі зазвичай розглядають через призму управлінських систем, виявляють низку типових перешкод: обмежені фінансові та людські ресурси, наявність застарілих IT-систем, фрагментованість управлінської структури, недостатня культура безпеки та брак спеціалізованих компетенцій. Ці чинники знижують ефективність від стандартизації, якщо не супроводжуються

програмами навчання, централізованою методичною підтримкою і політиками стимулювання дотримання (наприклад, вимоги у держзакупівлях, центри підтримки для місцевих органів влади).

Поряд із інформаційною системою управління безпекою у публічному секторі набули поширення рамкові підходи до управління кібербезпекою, зокрема рамка Рамка кібербезпеки NIST – Структура кібербезпеки (CSF) та його оновлення (CSF 2.0), які пропонують функціональну модель (ідентифікувати – виявити – реагувати – відновити) і сприяють інтеграції технічних та організаційних заходів у місцеві політики й практики урядових агентств. Рамки Національного інституту стандартів і технологій США корисні для державної політики тим, що вони придатні для адаптації (добровільні, масштабовані) й орієнтують на управління ризиками, постачальницьку безпеку та ідентифікацію ключових функцій життєзабезпечення е-послуг [220].

Наукові підходи до механізмів публічного управління інформаційною безпекою умовно групуються за двома великими вимірами: техніко-адміністративним та соціально-технічним. Перший вимір (техніко-адміністративний) охоплює формування нормативно-правової бази, стандарти та технічні контрзаходи (шифрування, автентифікація, контроль доступу, безпека мережі), аудит і сертифікацію, а також організацію формального нагляду й відповідальності. У сучасній науковій літературі та нормативних документах перший вимір техніко-адміністративного забезпечення інформаційної безпеки електронних послуг розглядається через поєднання правових, стандартних і технічних механізмів.

Одним із ключових джерел є стандарт ISO/IEC 27001:2022 [153], який у міжнародній практиці використовується як основа для впровадження систем управління інформаційною безпекою. Він задає структуровану рамку на основі циклу – цикл безперервного вдосконалення – PDCA, що включає політики, розподіл ролей, управління ризиками та технічні контрзаходи, зокрема шифрування, автентифікацію, контроль доступу й аудит. Цей стандарт є також базою для процедур сертифікації, які в публічному секторі відіграють роль

формалізованого нагляду й відповідальності. Подібну роль виконує й Рамка кібербезпеки NIST CSF 2.0, яка структурує управління ризиками за функціями «визначати – захищати – виявляти – реагувати – відновлювати» та включає вимоги до криптографії, ідентифікації, сегментації мережі й процедур моніторингу. Документ Національного інституту стандартів і технологій США наголошує на інтеграції технічних та адміністративних заходів у єдиний процес управління безпекою, що є визначальним для електронних сервісів державного сектору [220].

У правовому полі Європейського Союзу важливу роль відіграє Загальний регламент про захист даних, що накладає обов'язок на постачальників послуг упроваджувати як організаційні, так і технічні заходи захисту, включаючи шифрування, псевдонімізацію та процедури повідомлення про порушення. Нормативна логіка Загального регламенту про захист даних базується на принципах «конфіденційність за принципом проєктування» та «конфіденційність за замовчуванням», які фактично перетворюють технічні вимоги у зобов'язання для публічних органів [192]. Своєю чергою, Директива NIS2 [126] спрямована на підвищення рівня безпеки мереж і інформаційних систем у критичних секторах, включаючи публічне управління. Вона визначає обов'язкові заходи для управління ризиками, інцидент-репортингу, забезпечує формальний нагляд на національному рівні та передбачає санкції за недотримання. Таким чином, директива інституалізує контрольні функції держави та зміцнює техніко-адміністративну основу для захисту електронних послуг.

Вагомий внесок у деталізацію практичних аспектів зробили також звіти та аналітичні документи Агентства ЄС із кібербезпеки (ENISA). Вони містять методичні вказівки щодо впровадження рамки NIS2, рекомендації для взаємодії командам фахівців, що займаються реагуванням на інциденти комп'ютерної безпеки, судових і правоохоронних органів, а також технічні настанови щодо застосування сертифікатів, криптографічного протоколу і моніторингу. Ці документи перетворюють вимоги директив у конкретні технічні й адміністративні процедури, що можуть бути використані у публічному секторі для забезпечення відповідності та контролю [133].

Серед академічних досліджень варто відзначити статтю Рібейро та співавторів (2025), у якій здійснено масштабну оцінку захищеності понад трьох тисяч платформ електронних послуг. Використовуючи неінвазивні методи автоматизованого аналізу, автори показали системні вади в конфігурації безпеки (застарілі сертифікати криптографічного протоколу, слабкі політики автентифікації, відсутність оновлень). Їхні висновки підтверджують необхідність централізованого аудиту та технічного нагляду, оскільки значна частина ризиків може бути усунута своєчасними технічними заходами [199]. Схожі результати продемонстрували Аволе та колеги, які оцінили уразливості веб-застосунків урядових сайтів методом тестування безпеки й класифікували їх за «Відкритим проєктом безпеки веб-застосунків» (OWASP). Вони виявили високу частоту атак типу SQL-ін’єкцій (атака, під час якої зловмисник впроваджує шкідливий SQL-код у запит до бази даних, щоб отримати несанкціонований доступ, змінити або видалити дані чи навіть отримати контроль над сервером) та XSS (міжсайтовий скриптинг), а також слабкі конфігурації сесій. Рекомендації авторів зводилися до інтеграції вимог безпеки у державні закупівлі та регулярного обов’язкового аудитного тестування [103; 198].

Огляд літератури, проведений Кюло, Насімбені, Подрекка та Сартор, узагальнює наукові дослідження, що аналізують впровадження стандарту ISO/IEC 27001. Автори виявили, що сертифікація підвищує формалізованість процедур аудиту, але її ефективність значною мірою залежить від рівня організаційної готовності й ресурсного забезпечення. У публічному секторі особливо важливим є поєднання сертифікації з додатковими механізмами нагляду та підготовки кадрів [111;167].

Значно більше на поведінкові та організаційні аспекти звернено увагу в дослідженнях Сохрабі Сафа, фон Сольмс і Фернелл та Іфінедо. Перша робота пропонує модель відповідності політикам безпеки, засновану на опитуваннях співробітників, і показує, що ключовими факторами є навчання, підтримка керівництва та культура обміну знаннями. Автор робить висновок, що технічні контрзаходи мають сенс лише тоді, коли вони інтегровані у формальні

адміністративні процеси [213]. Іфінедо ж інтегрує теорію запланованої поведінки та теорію мотивації захисту, доводячи, що сприйняття ризику й самоефективність визначають ступінь дотримання політик безпеки, а тому формальний нагляд, санкції й аудит мають поєднуватися з психологічними і мотиваційними механізмами [190].

Таким чином, проаналізовані джерела – від міжнародних стандартів та директив ЄС до емпіричних і поведінкових досліджень – одностайно підтверджують, що техніко-адміністративний вимір управління інформаційною безпекою електронних послуг має ґрунтуватися на інтеграції трьох груп механізмів: нормативно-правових (GDPR, NIS2), стандартизованих технічних (ISO/IEC 27001, NIST CSF) і організаційно-контрольних (аудит, сертифікація, відповідність), при цьому ефективність забезпечується лише за умов поєднання формального нагляду з реальними технічними контрзаходами та освітньо-мотиваційними програмами для персоналу.

Другий вимір – соціально-технічний – розглядає інформаційну безпеку як властивість соціально-технічної системи: технологічні механізми взаємодіють із соціальними практиками, організаційними культурами, моделями поведінки користувачів та міжвідомчою координацією. Соціально-технічний підхід підкреслює, що технологічних рішень без відповідного управлінського дизайну процесів, навчання персоналу та участі зацікавлених сторін недостатньо; він пропонує методології для моделювання людського фактора, сценаріїв неправомірного використання й симуляцій для прогнозування вразливостей.

Ерік Тріст і колеги – класичні засновники соціально-технічної теорії. Ранні емпіричні спостереження Тріста і Мюррея сформолювали архітектоніку соціально-технічних систем як сукупність технічних підсистем і соціальних практик, що співконструюють результативність роботи. Методологія – польові дослідження і кейс-аналізи промислових робочих систем; результати показують, що технічні зміни, не підкріплені реорганізацією соціальних ролей і культурою, часто призводять до неочікуваних негативних наслідків. Імплікація для е-послуг: без інтеграції організаційного дизайну, навчання персоналу й механізмів координації

технічні контрзаходи щодо шифрування чи автентифікації не забезпечать стійкої інформаційної безпеки [224].

Гордон Бакстер і Сем Соммервілл показують, що системи, побудовані лише на технічних параметрах, виявляються вразливими, якщо ігноруються поведінкові й організаційні фактори. Їхній висновок – необхідно одночасно оптимізувати як технічні, так і соціальні елементи систем для досягнення стійкої безпеки [142].

Кетрін Парсонс зі співавторами доводять, що інформаційна безпека значною мірою залежить від знань, ставлень і поведінки користувачів. Їхній опитувальник HAIS-Q виявляє прямий зв’язок між рівнем обізнаності та реальною здатністю протидіяти фішинговим атакам. Висновок – навчання та формування культури безпеки є таким самим важливим, як і технологічні засоби [158].

Алісія Полліні та колеги наголошують, що людський фактор слід розглядати комплексно: через призму індивідуальних навичок, організаційних практик та технологічних інтерфейсів. Висновок їхнього дослідження – тільки системні інтегровані рішення дозволяють зменшити ризики, пов’язані з людськими помилками, і підвищити рівень безпеки, особливо у сферах критичної інфраструктури на кшталт охорони здоров’я [189].

Каур, ван Ітен та інші здійснюють наукометричний огляд і доходять висновку, що наукове поле досліджень людського фактора в безпеці є нерівномірним: переважають роботи про поведінку кінцевих користувачів, тоді як роль організацій та експертів вивчена недостатньо. Це свідчить про потребу більш збалансованих і теоретично обґрунтованих підходів [165].

Едвард Чжан у своєму аналізі китайського «Закону про кібербезпеку» показує, що правове регулювання само по собі не гарантує стійкості систем: воно змінює соціальні практики та інституційні відносини, що вимагає паралельної адаптації організаційної культури, міжвідомчої координації та навчання персоналу [149].

Ані У.Д. та співавтори пропонують нове покоління методів моделювання – симуляції соціально-технічних систем, які дозволяють у віртуальному середовищі тестувати реакції організацій на кіберзагрози. Їхній висновок – такі інструменти є

перспективними для державного управління, адже дозволяють оцінювати не лише технічні, а й організаційні ризики [227].

Андреа Франделл і колеги, досліджуючи місцеве самоврядування, показують, що рівень кіберстійкості органів влади напряму залежить від культури управління, кадрових ресурсів та фінансування. Технологічні засоби виявляються неефективними без відповідної політичної підтримки і системного навчання персоналу [141].

П. Ківімаа демонструє, що трансформації на кшталт цифровізації чи переходу до сталого розвитку створюють нові ризики, які потребують одночасного врахування технічних і соціальних вимірів. Висновок – безпека має бути вбудованою у стратегії трансформацій, а не додаватися як вторинний елемент [187].

Ноел Ворфорд і його колеги звертають увагу на особливості «ризикових користувачів» – груп, які через соціальний або економічний контекст більш вразливі до кіберзагроз. Їхній висновок – політика у сфері е-послуг має враховувати нерівність і проєктувати сервіси так, щоб мінімізувати додаткові бар’єри для вразливих категорій населення [235].

Аналіз зазначених досліджень дає підстави зазначити, що інформаційна безпека є результатом спільної дії технічних, організаційних і соціальних факторів. Жоден із вимірів не може забезпечити стійкість самостійно. Для публічного управління це означає: впровадження електронних послуг вимагає не лише технічних стандартів і регуляцій, а й формування культури безпеки серед персоналу та користувачів, інституційної координації, інвестицій у людські ресурси та врахування соціальних особливостей різних груп громадян.

Соціально-технічний підхід консистентно доводить, що інформаційна безпека е-послуг – це властивість системи, котра виникає тільки за умови узгодженості технічних засобів (шифрування, автентифікація, контроль доступу, моніторинг) із соціальними практиками (навчання, культура безпеки, організаційні ролі) й інституційними механізмами (координація, нормативи, інцидент-плани). Методологічно джерела пропонують поєднання:

а) наукометричних/оглядових аналізів для виявлення трендів;

б) кількісних опитувань і інструментів (HAIS-Q) для оцінки поведінки;

в) симуляцій-моделювань для тестування політик;

г) кейс-досліджень для інституційного контексту.

На рівні політики це транслюється у рекомендації: інтегровані навчальні програми, моделі «спільної оптимізації» технічних та організаційних рішень, інструменти для ідентифікації й підтримки вразливих користувачів, а також практика регулярних соціально-технічних симуляцій інцидентів.

У багатьох недавніх бібліометричних дослідженнях простежується явне зростання тематичної ваги понять «кіберстійкість» і «безперервність надання послуг» як окремої лінії досліджень, що виходить за рамки традиційної вузькотехнічної орієнтації на захист периметра. Історичний і тематичний аналіз розвитку дисципліни демонструє, що від початкових досліджень у сфері захисту інфраструктур на передньому плані опинилися дослідження, які поєднують стратегії превенції з моделями відновлення та адаптації (resilience-by-design). Це гіпотеза підтверджує огляд, який простежує еволюцію терміна «кіберстійкість» і виділяє кластери публікацій, що присвячені сценарному тестуванню, резервуванню сервісів і міжсекторальній кооперації [226].

Паралельно з цим число публікацій на перетині штучного інтелекту (ШІ) і безпеки стрімко зростає: бібліометричні карти показують великі «кластерні» групи статей, присвячені методам на основі машинного навчання та глибинного навчання для виявлення атак, а також роботі з великими журналами логів і потоків подій. Огляди, що ґрунтуються на базах Scopus і Web of Science, ідентифікують прискорений ріст публікацій між 2015 і 2024 роками та концентрують увагу на двох основних напрямах – розпізнавання аномалій і автоматизація інцидент-респонсу. Це має прямі наслідки для публічного сектора: інструменти ШІ потенційно підвищують здатність державних платформ швидко виявляти та локалізувати інциденти, але одночасно породжують запитання щодо верифікації моделей, прозорості рішень і аудиту алгоритмів [146].

Ще один усталений тренд – посилення міждисциплінарності: огляди тематичних мереж вказують на зростання кількості робіт, які об’єднують експертів із публічної політики, права, соціальних наук та комп’ютерних/інформаційних технологій. Такі наукові «мости» проявляються у публікаціях, що поєднують нормативно-правовий аналіз, політичну економію кібербезпеки й технічні методи аналізу ризиків. Графічні карти співпраці показують, що успішні міждисциплінарні проєкти частіше виходять із мереж університетів, які мають одночасний доступ до технічних лабораторій і факультетів суспільних наук. Це означає, що формування політик безпеки для е-послуг має базуватися на знаннях, що інкорпорують і технічну досконалість, і соціально-політичні контексти [235].

Аналізи структури наукового поля (включно з оцінкою «вкладу країн/інституцій», показниками цитованості та мережею співавторства) регулярно демонструють високий ступінь концентрації: велика частина продуктивних і цитованих публікацій походить від вузького кола наукових центрів і університетів у розвинених країнах, тоді як низка регіонів залишається слабо представленою. Це виявлено у кількох наукометричних дослідженнях, які аналізували бази Web of Science і Scopus: вони показують, що лідерство в публікаціях з кібербезпеки та цифрового урядування сконцентроване в США, країнах Західної Європи та кількох університетах Азії, тоді як країни з меншим науковим капіталом виробляють одиничні публікації або локальні технічні звіти. Наслідок для політики – ризик того, що стандарти і практики, що формуються в академічному середовищі, можуть бути непридатні або непропорційні для контекстів країн з іншими інституційними реаліями [206].

Бібліометричні роботи також виявляють чітку тенденцію до «зростання платформних досліджень» – тобто досліджень, які аналізують не окремі технічні заходи, а системні екосистеми цифрових сервісів: взаємозв’язки постачальників, залежності від ланцюжків постачання (supply-chain), роль третіх сторін і вразливість, що виникає через інтеграцію зовнішніх компонентів. Це важливо для державних е-послуг, де використання сторонніх хмарних сервісів і відкритих

компонентів робить необхідним координацію політик постачальницької безпеки та контрактні механізми в держзакупівлях [121].

З методологічної точки зору значна частина наукових робіт пропонує комбіновані методи оцінки ефективності механізмів: кількісні оцінки безпеки (метрики, індикатори, сканування вразливостей), які доповнюються якісними дослідженнями (інтерв'ю, кейс-дослідженнями, аналізом політик). На рівні національних досліджень застосовуються великомасштабні непроникні інструменти оцінки (методики оцінки, які дозволяють виявляти та моніторити дефекти обладнання, без необхідності його розбирання чи проникнення всередину) для аналізу відкритих е-платформ, що дає можливість порівнювати стан захищеності між країнами та визначати пріоритети для політик.

Проведений аналіз дає підстави зазначити, що багато бібліометричних аналізів підкреслюють «екранування» тем – надмірну концентрацію тем у технічній площині і відносну бідність робіт, орієнтованих на політико-організаційні аспекти або прикладні кейси в країнах із низьким ресурсним забезпеченням. Крім того, існує ризик «метричного зміщення»: важливі практичні звіти урядів або агентств часто ігноруються, хоча вони критично важливі для розробки політик у реальному середовищі. Водночас спостерігається слабка регіональна інтероперабельність у науковому діалозі – мало транснаціональних мереж, які би щільно поєднували академічних дослідників із практиками та регуляторами у країнах, що розвиваються.

Існуючі наукові підходи до механізмів публічного управління інформаційною безпекою при наданні електронних послуг формують скоординовану, багаторівневу картину, в якій технічні, організаційні, нормативні та соціальні елементи утворюють взаємодоповнювальні підсистеми. Центральним «ядерним» підходом у цій парадигмі виступає концепція управлінських систем – передусім система управління інформаційною безпекою (ISMS), формалізована в стандарті ISO/IEC 27001:2022; ця рамка задає обов'язкову логіку управління ризиками, документування політик і процедур та циклічне вдосконалення через цикл «плануй – впроваджуй – перевіряй – коригуй (PDCA)», що робить її

природним орієнтиром для державних органів, які прагнуть уніфікувати підходи до конфіденційності, цілісності й доступності даних.

Поряд із цим у науковій і практичній літературі виокремлюють рамкові, ризик-орієнтовані підходи, зокрема Рамку кібербезпеки Національного інституту стандартів і технологій (NIST CSF), яка структурує функції «визначати – захищати – виявляти – реагувати – відновлювати» і служить операційною картою для інтеграції технічних контролів (шифрування, автентифікація, контроль доступу, моніторинг) з адміністративними процесами і механізмами звітності; наукові праці підкреслюють роль таких рамок у перетворенні технічних практик у керовані державними політиками процедури.

Роль нормативно-правового поля як механізму управління підкреслена низкою робіт і практичних документів: загальноєвропейський регуляторний пакет – зокрема Регламент (ЄС) 2016/679 (GDPR) – формалізує вимоги щодо проєктування послуг із вбудованою приватністю та обов’язки щодо технічних і організаційних заходів захисту; директива NIS2 уніфікує обов’язкові вимоги щодо управління ризиками, повідомлення про інциденти і механізмів нагляду для широкого кола суб’єктів, що істотно посилює адміністративну складову захисту електронних послуг у публічному секторі. Таким чином, нормативна логіка диктує не лише «що» має бути захищено, а й «хто» несе відповідальність і які процедури контролю мають існувати.

Емпіричні наукові дослідження і великомасштабні технічні аудити є практичними індикаторами слабких місць, які має адресувати публічне управління. Наприклад, нещодавнє глобальне дослідження, що охопило тисячі державних платформ, виявило системні дефекти в налаштуванні безпечних протоколів, у ланцюгах сертифікації та політиках автентифікації – висновок, який підкреслює, що багато загроз є усуненими через прості технічні й процедурні втручання, якщо існують централізовані механізми аудиту і координації. Наукові статті цього типу дають вагомі емпіричні підстави для політик «швидкого усунення» базових вразливостей у державних е-послугах.

Друга велика група наукових підходів акцентує увагу на людському і соціальному вимірі – на соціально-технічних моделях і поведінкових факторах. Інструменти оцінки людського фактора (наприклад, опитувальник «Людські аспекти інформаційної безпеки», HAIS-Q) показують, що знання, ставлення і поведінка співробітників прямо корелюють із ризиком фішингу та іншими інцидентами; отже, технічні контрзаходи (наприклад, багатофакторна автентифікація) мають поєднуватися з навчанням, симуляціями інцидентів і процедурними стимулами для забезпечення реального комплаєнсу. Наукові підходи також демонструють необхідність адаптації інтерфейсів і робочих процесів для зниження когнітивного навантаження та людських помилок у державних службах.

У зростаючому числі публікацій підкреслюють значення кіберстійкості – здатності систем до швидкого відновлення критичних функцій – що зміщує фокус із лише превентивних заходів до поєднання превенції, виявлення й відновлення. Наукові й практичні огляди радять включати сценарні вправи, резервування сервісів та інтегровані плани безперервності як обов’язкові елементи механізмів публічного управління.

Інтеграція штучного інтелекту й автоматизації у виявленні загроз і реакції є іншим помітним напрямом; одночасно це породжує виклики верифікації моделей, прозорості та алгоритмічної підзвітності. Сучасні рамки управління ризиком для систем ШІ (наприклад, NIST AI RMF) і технічні керівництва ENISA пропонують підходи до оцінки безпеки інструментів ШІ, але політики публічного сектору повинні вимагати процедур аудиту алгоритмів, моніторингу даних і заходів щодо зниження упереджень і непрозорості при використанні ШІ у держсервісах.

Щодо ланцюгів постачання наукові й практичні дослідження підкреслюють вразливість е-послуг через залежність від зовнішніх постачальників, відкритих компонентів і хмарних сервісів; отже, контракти, сертифікація постачальників, вимоги до перевірок та належна перевірка ланцюга поставок мають стати стандартною частиною системи управління інформаційною безпекою у

публічному секторі. ENISA і NIST дають практичні настанови з картографування залежностей і організації взаємодії з CSIRT/компетентними органами.

Бібліометричні дослідження й огляди підтверджують, що поле досліджень цифрового управління є швидкоростучим і дедалі більш міждисциплінарним (поєднання права, публічної політики, соціальних наук і комп'ютерних технологій), але в той же час фіксують кислотні точки: висока концентрація продуктивності в обмеженій кількості інституцій і недоотримана присутність досліджень у тих юрисдикціях, де політика впровадження е-послуг найбільш уразлива. Це породжує необхідність розширення транснаціональної наукової співпраці і інкорпорації практичних звітів у мета-аналізи для формулювання релевантної політики.

З методологічної та оперативної точки зору з цих підходів випливають такі інтегровані висновки для публічного управління: поєднання стандартів ISMS (ISO/IEC 27001) й оперативних рамок (NIST CSF) з юридичними вимогами (GDPR, NIS2) створює нормативно-керовану основу; але ця основа має бути підсилена централізованими технічними аудитами і координаційними механізмами, програмами навчання і поведінкових інтервенцій, планами кіберстійкості та чіткими політиками щодо постачальницької безпеки; також необхідні правила та процедури для безпечного й підзвітного застосування ШІ. Цілісна політика повинна відображати: техніко-адміністративну строгість, соціально-поведінкову роботу з персоналом і користувачами та адаптивність до контексту й ресурсів конкретної юрисдикції.

Таким чином, наукові підходи до механізмів публічного управління інформаційною безпекою е-послуг консолідуються навколо принципу багаторівневої інтеграції: стандарти й рамки дають архітектуру, правове поле – легітимність і обов'язковість, соціально-технічні дослідження – механізми впровадження й адаптації, емпіричні аудити – індикатори пріоритетних технічних втручань, а наративи кіберстійкості і регулювання ШІ визначають майбутні вимоги до стійкості й прозорості. На цьому підґрунті політика публічного сектора має транслювати наукові висновки у практичні інструменти (шаблони ризик-аналізу,

централізовані програми аудиту, вимоги до контрактів і модулі навчання) з урахуванням локального контексту й ресурсних обмежень.

1.2. Понятійно-категоріальний апарат дослідження механізмів публічного управління інформаційною безпекою надання електронних послуг

Розвиток суспільства визначив формування та розвиток підходів до сприйняття, використання та захисту інформації в залежності від викликів та форматів використання інформаційних ресурсів. Інформація впливає на прийняття рішень, якість послуг, ефективність та прозорість управління в усіх галузях суспільства. Сучасні технології та цифрова трансформація ще більше підкреслюють значення інформаційної безпеки у публічному секторі. Отже, важливо дослідити концептуальні підходи до визначення ролі та місця інформації в системі публічного управління. Сфера публічного управління стикається з різними загрозами та викликами інформаційної безпеки, такими як кібератаки, розповсюдження дезінформації та зловживання з інформацією. Дослідження має на меті розглянути ці загрози та визначити способи їхнього подолання. Важливо вивчити, як використання інформації може покращити якість публічних послуг, підвищити ефективність прийняття рішень та забезпечити більшу прозорість і відкритість у сфері публічного управління.

Інтенсифікація процесів цифровізації та глобальні трансформації, пов’язані зі зростанням обсягів оброблюваної інформації, зумовили суттєве переосмислення ролі інформації як стратегічного ресурсу публічного управління. Якщо раніше інформація виконувала переважно комунікаційну або допоміжну функцію, то в умовах цифрової економіки вона перетворилася на ключову детермінанту якості, результативності та прозорості управлінських процесів. Така трансформація змінила не лише зміст управлінських практик, а й парадигму управлінського впливу, в межах якої інформаційна безпека стала критично важливою категорією для збереження функціональної цілісності публічної влади.

У зв’язку з цим інформаційна безпека в системі публічного управління більше не може розглядатися як суто технічне чи відомче завдання. Вона набуває статусу одного з центральних об’єктів управлінського впливу, що потребує формалізованого підходу до регулювання, координації та контролю. Зростання складності загроз від масових кіберінцидентів до системних атак на інститути демократії через дезінформацію вимагає не лише наявності технологічних засобів захисту, а й розбудови цілісних управлінських механізмів, здатних забезпечити системне реагування та стійкість публічних інституцій.

Саме в такому контексті виникає необхідність наукового осмислення категорії «механізми публічного управління». Вона стає ключовою для розуміння того, яким чином інституційно, процедурно та нормативно реалізується вплив публічної влади на об’єкти управління, у тому числі у сфері інформаційної безпеки. Механізми виступають не просто інструментами реалізації політики, а структурованими системами, що забезпечують ефективну координацію дій суб’єктів, дотримання процедур, використання ресурсів і досягнення цільових показників безпеки в цифровому середовищі.

Для подальшого теоретико-методологічного конструювання механізмів публічного управління важливо визначити їхню природу, відмежувавши від суміжних понять методів, інструментів, засобів, важелів. У науковій літературі спостерігається розмитість меж між цими категоріями, що ускладнює формування єдиного підходу до їх дослідження та впровадження. Саме тому необхідною передумовою будь-якої аналітичної або прикладної моделі управління є теоретичне окреслення сутності механізмів як цілісних, впорядкованих систем публічного впливу.

У цьому контексті подальше дослідження зосереджується на теоретичному осмисленні поняття «механізми публічного управління» з метою його концептуалізації як ключової категорії дослідження. Такий підхід дозволяє не лише сформувати методологічне підґрунтя для аналізу практик інформаційної безпеки в системі електронних послуг, а й забезпечити наукову узгодженість при

моделюванні механізмів, адаптованих до умов цифрової трансформації, ризиків гібридного характеру та євроінтеграційного напряму розвитку України.

Поняття «механізми» в управлінській науці зазнало суттєвої еволюції від суто технократичного розуміння до складної багаторівневої управлінської категорії, що використовується для опису системної організації управлінського впливу. На ранніх етапах розвитку науки поняття механізмів ототожнювалося переважно з сукупністю інструментів або технічних засобів реалізації політики та рішень. У такому розумінні механізм розглядався як технічний процес виконання волі суб'єкта управління, без глибокого аналізу його внутрішньої структури.

З розвитком системного, функціонального, інституційного та управлінсько-поведінкового підходів у сфері публічного управління поняття «механізм публічного управління» зазнало суттєвого методологічного переосмислення й наповнилося новими змістовими характеристиками. Якщо в попередні періоди це поняття розглядалося переважно через призму сукупності адміністративних процедур або технічних інструментів, то в умовах сучасного управлінського середовища воно трансформувалося у складну, багаторівневу систему, що виконує роль інтегратора управлінських дій, процесів і ресурсів. У науковому дискурсі сьогодення механізм публічного управління все частіше трактується як впорядкована, цілеспрямована, інституціоналізована та нормативно врегульована система взаємопов'язаних елементів, які спільно забезпечують реалізацію управлінських функцій та досягнення публічно значущих результатів у конкретній сфері суспільного розвитку.

Визначення передбачає, що механізм не лише є інструментом або методом впливу, а й охоплює ширший контекст від структурних інституцій, що здійснюють управлінську діяльність, до нормативних документів, інформаційно-аналітичної підтримки, процедур управлінського циклу, каналів комунікації та ресурсного забезпечення. Механізми функціонують у межах певної управлінської логіки, яка обумовлена не лише формальними регламентами, а й ціннісно-нормативними орієнтирами публічного управління, такими як ефективність, підзвітність, відкритість, інклюзивність і дотримання прав людини.

У контексті сучасних викликів, зокрема цифрової трансформації, кіберзагроз, гібридної війни та суспільного запиту на якісні публічні послуги, поняття «механізм публічного управління» набуває ще більшої релевантності. Воно слугує ключовим концептом для пояснення того, яким чином публічна влада організовує, координує, управляє й контролює процеси, що мають критичне значення для національної безпеки, зокрема у сфері захисту інформаційного середовища та забезпечення безпечного функціонування електронних сервісів.

Отже, вивчення структури, принципів побудови, складових елементів і логіки дії таких механізмів не лише є теоретично значущим, а й має безпосереднє прикладне значення для розбудови стійкої системи публічного управління в Україні [55].

При цьому механізми не зводяться лише до інструментів впливу. Вони включають [19]:

– інституційний компонент (учасники управлінського процесу, їхні повноваження та відповідальність);

– нормативно-правову основу (регламентуючі документи, стандарти, положення);

– організаційно-процедурний рівень (моделі, процедури, регламенти прийняття рішень);

– ресурсне забезпечення (фінанси, кадри, IT-рішення, цифрова інфраструктура);

– комунікаційні канали та зворотний зв’язок.

Таким чином, змістовна трансформація поняття «механізмів» в науці публічного управління полягає у переході від вузького, інструментального трактування до системного, комплексного та адаптивного розуміння, що дозволяє аналізувати не лише засоби впливу, але і процеси, структури та умови досягнення управлінських результатів [21].

Особливого значення ця трансформація набуває в контексті цифровізації та інформаційної безпеки, де механізми публічного управління мають бути не лише

ефективними, а й гнучкими, стійкими до ризиків і здатними до адаптації в умовах динамічних загроз і технологічних змін.

Для чіткого розмежування наукових підходів і забезпечення термінологічної визначеності доцільно відокремити поняття «механізм публічного управління» від суміжних категорій «інструмент», «метод» і «важіль», які часто використовуються у дослідницькому дискурсі як синоніми.

Однак між ними існують суттєві змістовні та функціональні відмінності, що мають бути враховані при формуванні концептуального апарату дослідження, що наведено в табл. 1.1.

Таблиця 1.1

Відмінність механізмів від інструментів, методів, важелів

Категорія	Визначення	Характерні ознаки	Функціональне призначення
1	2	3	4
Механізм публічного управління	Сукупність взаємопов'язаних інституційних, нормативних, організаційних, технологічних та комунікаційних елементів, що забезпечують цілеспрямовану реалізацію функцій публічного управління наданням електронних послуг у системі забезпечення інформаційної безпеки	Комплексність, структурованість, ієрархічність, наявність зворотного зв'язку, стратегічна спрямованість.	Забезпечення узгодженої реалізації політики у певній сфері через систему органів, процедур та ресурсів.
Інструмент	Окремий засіб або прийом впливу, що	Однофункціональність, прикладний характер,	Виконання конкретного управлінського завдання

	використовується в межах механізму для досягнення конкретної управлінської мети.	обмеженість сферою застосування.	в рамках ширшого механізму.
Метод	Спосіб або процедура здійснення управлінського впливу відповідно до певних принципів і логіки дій.	Процесуальність, раціональність, залежність від типу завдання.	Регламентація процесу управління, вибір оптимального способу досягнення цілі.
Важіль	Фактор або умова, що дозволяє впливати на об’єкт управління з метою його зміни чи спрямування.	Мотиваційність, точковість впливу, гнучкість.	Стимулювання або обмеження поведінки об’єкта управління.

Джерело: розроблено автором на основі аналізу [19; 21-22; 55]

Таким чином, порівняльний аналіз понять «механізм», «інструмент», «метод» і «важіль» дає підстави стверджувати, що механізм публічного управління є найбільш комплексною, системною і багаторівневою категорією. Він містить в собі інструменти, методи і важелі як складові елементи, проте не зводиться до них. Механізм охоплює не лише засоби впливу, а й інституційну структуру, нормативне регулювання, управлінські процедури та ресурсне забезпечення [28].

Під механізмом публічного управління інформаційною безпекою електронних послуг доцільно розуміти інтегровану систему взаємодіючих інституцій, нормативно-правових норм, організаційно-функціональних процедур, управлінських інструментів, цифрових ресурсів і комунікаційних каналів, які забезпечують цілеспрямоване виконання функцій публічного управління у сфері забезпечення захищеного надання електронних послуг [58].

Таке розуміння створює методологічне підґрунтя для подальшого конструювання ефективних, адаптивних та стійких механізмів публічного управління, що відповідають викликам цифрової трансформації та сучасної безпекової ситуації.

Дослідження механізмів публічного управління вимагає цілісного, міждисциплінарного підходу до їх концептуалізації, що передбачає інтеграцію філософсько-методологічних, системно-аналітичних і прикладних основ сучасної управлінської науки. Упродовж останніх десятиліть у науковому дискурсі сформувався ряд теоретико-методологічних підходів, які по-різному трактують сутність і структуру механізмів публічного управління, акцентуючи увагу на певних аспектах їх функціонування та організації.

З позицій функціонального підходу механізми публічного управління розглядаються як упорядковані управлінські дії, спрямовані на реалізацію основних функцій публічного адміністрування планування, організації, мотивації, координації, моніторингу та контролю. У цьому контексті механізм постає як системна сукупність засобів, процедур і рішень, які забезпечують досягнення управлінських цілей у конкретній галузі, включаючи сферу забезпечення інформаційної безпеки.

Інституційний підхід зосереджується на аналізі організаційно-структурного аспекту механізмів, які забезпечують реалізацію владних повноважень у публічному секторі. Механізм у цьому розумінні трактується як інституціоналізована форма взаємодії органів публічної влади, яка функціонує відповідно до визначених правових норм, регламентів і стандартів. Важливим елементом інституційного підходу є вивчення розподілу компетенцій, взаємодії між суб’єктами управління та рівнем їхньої відповідальності за досягнення результатів у сфері цифрової безпеки [18].

Процесний підхід пропонує розглядати механізм як динамічну послідовність взаємопов’язаних етапів управлінського впливу від формування проблемного поля до ухвалення рішень, їх реалізації, моніторингу та коригування. Такий підхід дозволяє виявити часову логіку та циклічність функціонування механізмів публічного управління, що є особливо важливим у контексті змінного цифрового середовища та необхідності гнучкого реагування на нові загрози інформаційній безпеці [70].

З огляду на складність сучасного управлінського середовища системний підхід є найбільш адекватним для комплексного аналізу механізмів публічного управління. Він передбачає розгляд механізму як цілісної багаторівневої системи, що включає взаємодіючі підсистеми: нормативно-правову, інституційну, процедурну, інформаційно-аналітичну, ресурсну та комунікаційну. У рамках цього підходу механізм виконує роль зв'язувального елементу між ціннісно-цільовими орієнтирами публічної політики та практикою її реалізації [71].

У процесі наукового осмислення природи та змісту механізмів публічного управління в сучасній управлінській науці сформувалося кілька методичних підходів, кожен з яких висвітлює окремі аспекти функціонування, побудови та цільового призначення цих механізмів. Їх розгляд у межах функціонального, інституційного, процесного та системного підходів дозволяє комплексно оцінити механізми як складні управлінські утворення, що мають як структурну завершеність, так і динамічну здатність до трансформації. Порівняння зазначених підходів на основі ключових характеристик і дослідницьких пріоритетів дозволяє забезпечити цілісне теоретико-методологічне підґрунтя для подальшого аналізу, моделювання та вдосконалення механізмів публічного управління, зокрема у сфері забезпечення інформаційної безпеки під час надання електронних послуг. Узагальнені характеристики зазначених підходів наведено в табл. 1.2.

Узагальнюючи зазначені підходи, можна стверджувати, що механізми публічного управління – це не просто набір засобів чи інструментів реалізації політики, а складна організована система, яка функціонує на перетині управлінських функцій, інституційних структур, процедур і ресурсів, забезпечуючи реалізацію публічного інтересу в умовах багатофакторного та ризиконасиченого середовища.

У цьому контексті доцільно окреслити основні ознаки механізмів публічного управління, що визначають їх концептуальні межі [66]:

– цілеспрямованість: орієнтація на досягнення конкретного публічного результату;

Таблиця 1.2

Порівняльний аналіз підходів до визначення механізмів публічного управління

Підхід	Сутність	Ключові характеристики	Значення
1	2	3	4
Функціональний	Розглядає механізм як систему дій і засобів, що забезпечують реалізацію основних функцій публічного управління.	Орієнтація на управлінські функції: планування, організація, координація, контроль, моніторинг.	Дозволяє ідентифікувати механізми як інструменти досягнення управлінських цілей.
Інституційний	Трактує механізм як взаємодію інституцій з чітко визначеними повноваженнями в межах правового поля.	Фокус на суб'єктах управління, їх компетенціях, ролях, відповідальності.	Забезпечує аналіз формалізованої взаємодії публічних інституцій у сфері ІБ.
Процесний	Розглядає механізм як динамічну послідовність управлінських дій, що реалізуються в часі.	Циклічність, стадійність, гнучкість, наявність логіки управлінського процесу.	Дозволяє структурувати механізми за етапами та оптимізувати їх послідовність.
Системний	Трактує механізм як комплексну систему взаємодіючих елементів у межах цілісного управлінського середовища.	Складність, багаторівневість, взаємозв'язки, інтеграція компонентів.	Сприяє формуванню узагальненого бачення механізмів як цілісного управлінського явища.

Джерело: акумульовано автором на основі аналізу [18; 58; 70-71]

– інституціоналізованість: наявність визначених суб'єктів управління із закріпленими повноваженнями;

– нормативна визначеність: функціонування в межах чинного правового поля;

– системність: взаємодія елементів в єдиному управлінському контурі;

– адаптивність: здатність до змін залежно від зовнішніх викликів;

– результативність: досягнення цільових індикаторів ефективності.

Відповідно, класифікація механізмів публічного управління може здійснюватися за низкою критеріїв: за рівнем управління (національний, регіональний, локальний), за функціональним навантаженням (нормативно-правові, організаційно-адміністративні, інформаційно-аналітичні, технологічні), за напрямом впливу (превентивні, реактивні, стабілізаційні).

Особливу увагу при аналізі механізмів публічного управління варто звернути на їх відповідність принципам концепції «належного управління», яка утвердилася як базова парадигма сучасного публічного управління в глобальному вимірі. Згідно з положеннями Організації Об’єднаних Націй та Європейського Союзу, належне врядування включає такі принципи, як прозорість, підзвітність, ефективність, інклюзивність, правова визначеність і орієнтація на результат. Механізми, які не відповідають цим критеріям, не можуть вважатися дієвими з точки зору демократичного врядування та публічної довіри [85].

Таким чином, методичне осмислення сутності та структури механізмів публічного управління на основі функціонального, інституційного, процесного та системного підходів, у поєднанні з принципами «належного управління», дозволяє сформувати глибоке теоретичне підґрунтя для подальшого аналізу та моделювання ефективних механізмів забезпечення інформаційної безпеки у сфері електронних послуг.

Наступний етап дослідження – це визначення поняття «інформаційна безпека». Поняття «інформаційна безпека» вперше ввів у науковий обіг інженер та криптолог Клауд Шенон у своїй роботі «Математична теорія зв'язку», яка була опублікована в 1948 році. У цій роботі Шенон вперше сформулював математичну теорію передачі інформації та вводив поняття «ентропія» як міру невизначеності в повідомленні. Ця робота стала основою для розвитку теорії інформації і кібернетики [205]. На той момент поняття «інформаційна безпека» означало захист інформації від несанкціонованого доступу та змін, а також забезпечення конфіденційності та цілісності інформації в процесі її передачі та зберігання [205].

Згодом, з розвитком інформаційних технологій і зростанням кількості загроз кібербезпеці, поняття «інформаційна безпека» стало включати в себе також заходи щодо захисту від кібератак та забезпечення доступності інформації в умовах віртуального середовища. Концепція інформаційної безпеки Деніела Дефініса базується на управлінському підході до захисту інформації та інформаційних систем. Вона акцентує на необхідності ефективного управління інформаційною безпекою в організаціях і публічних установах. Основні риси та характеристики цієї концепції включають [205]:

– управлінський підхід: концепція визнає, що інформаційна безпека не обмежується лише технічними заходами, але потребує системного управління та координації на рівні організації;

– захист інформації: від несанкціонованого доступу, використання, розголошення, руйнування та відмови від обслуговування, що включає в себе фізичний, логічний та організаційний захист інформації;

– стратегічний підхід підкреслює важливість включення інформаційної безпеки в стратегічне управління організацією. Інформаційна безпека повинна підтримувати досягнення стратегічних цілей;

– участь керівництва в питаннях інформаційної безпеки і визначення стратегічного напрямку для захисту інформації;

– важливість дотримання законодавства та стандартів щодо інформаційної безпеки і регулярного аудиту для оцінки ступеня виконання вимог;

– залучення співробітників до питань інформаційної безпеки та активної участі у процесі захисту інформації.

Інститут національної стандартизації і технологій (NIST) визначає інформаційну безпеку як «захист інформації та інформаційних систем від несанкціонованого доступу, використання, змін, розголошення та руйнування». Інститут пропонує докладний стандартний підхід до управління інформаційною безпекою. Концепція інформаційної безпеки, розроблена Інститутом національної стандартизації і технологій (NIST), має свої особливості [179]. Основною метою концепції є забезпечення захисту інформації та інформаційних систем, що включає

в себе заходи для запобігання несанкціонованому доступу до інформації, контролю за її використанням, змінами, розголошенням та руйнуванням. NIST пропонує докладний стандартний підхід до управління інформаційною безпекою. Представники інституту розробляють і публікують документи та стандарти, які надають рекомендації та вказівки з питань інформаційної безпеки для різних організацій та галузей. Отже, особливість концепції полягає в її системності та стандартизації. NIST розробляє рекомендації та стандарти, які охоплюють всі аспекти інформаційної безпеки, включаючи політики, процедури, технології та практики. Систематичність дозволяє організаціям ефективно впроваджувати заходи інформаційної безпеки та забезпечувати відповідність стандартам і вимогам безпеки даних [179].

Міжнародна організація зі стандартизації (ISO) визначає інформаційну безпеку як «захист конфіденційності, цілісності та доступності інформації». Визначення використовується як основа для розробки міжнародних стандартів інформаційної безпеки, таких як ISO 27001 та ISO/IEC 27002. Відповідно до міжнародних стандартів, розроблених Міжнародною організацією зі стандартизації, підхід до теоретико-методичного обґрунтування поняття інформаційної безпеки має такі особливості [153; 154]:

1. Захист конфіденційності, цілісності та доступності інформації. Як основну мету, ISO визначає захист конфіденційності (забезпечення, щоб інформація не потрапляла в руки несанкціонованих осіб), цілісності (збереження цілісності та недоступність змін інформації) та доступності (забезпечення доступу до інформації тим, хто має на це право).

2. Міжнародний стандарт ISO встановлює міжнародні стандарти інформаційної безпеки, такі як ISO 27001, які стають основою для розробки і впровадження систем управління інформаційною безпекою. Ці стандарти допомагають організаціям створювати ефективні системи захисту інформації та відповідати міжнародним вимогам.

3. Теоретичне обґрунтування поняття інформаційної безпеки в концепції ISO базується на важливості забезпечення конфіденційності, цілісності та доступності інформації для забезпечення довіри в усіх аспектах діяльності.

4. Специфіка полягає в тому, що ISO розробляє та публікує міжнародні стандарти, які є загальновизнаними і використовуються в усьому світі.

5. Стандарти надають практичні вказівки та вимоги з питань інформаційної безпеки, які допомагають організаціям підвищити рівень захисту своєї інформації та відповідати стандартам та регуляторним вимогам.

Акумулюючи концепції до визначення поняття інформаційної безпеки, доцільно сформувати результати аналізу шляхом групування підходів до визначення поняття інформаційної безпеки – табл. 1.3

Таблиця 1.3

Аналіз теоретико-методичних підходів до визначення поняття інформаційної безпеки

Назва підходу	Представники	Особливості визначення поняття інформаційної безпеки	Переваги	Недоліки
Функціональ-ний підхід	Брюс Шнайер, Майкл Конрад і інші	Забезпечення конфіденційності, цілісності та доступності інформації.	Простота визначення.	Не завжди враховує ризики та загрози.
Ризик-орієнтований підхід	Дуглас Штолф, Джозеф Гроуберг, Пітер Нортхаус і інші	Зосереджений на управлінні ризиками для захисту інформації та систем.	Адаптований до конкретних потреб.	Складний аналіз ризиків та оцінка витрат.
Конфіденційно спрямований підхід	Дейвід Гарфінкель та інші	Захист інформації для забезпечення національних інтересів через контроль інформаційних потоків.	Важливість національної безпеки.	Може призвести до обмеження свободи інформації.
Системний підхід	Міжнародна організація зі стандартизації (ISO) та інші	Захист конфіденційності, цілісності та доступності інформації.	Міжнародний стандартний підхід.	Вимагає значних ресурсів для впровадження.

Джерело: розроблено автором на основі акумулювання результатів досліджень [83; 153; 179-205]

Отже, різні підходи відображають різні аспекти та акценти в сфері інформаційної безпеки, і вони можуть використовуватися в залежності від конкретних потреб та контексту організації чи держави. У дослідженні автором пропонується використовувати системний підхід, який передбачає таке визначення поняття інформаційної безпеки – це комплекс заходів, організаційних, технічних та людських ресурсів, спрямований на забезпечення конфіденційності, цілісності та доступності інформації в усіх аспектах її збереження, передачі та обробки, що сприяє захисту інформації від несанкціонованого доступу, модифікації, руйнування та незаконного розголошення, а також забезпечує її надійність і доступність для авторизованих користувачів у контексті підтримки стратегічних цілей організації та створення довіри в електронному середовищі.

Акумулюючи результати аналізу підходів до теоретико-методичного обґрунтування інформаційної безпеки, автор розробив схему специфіки визначення інформаційної безпеки в системі публічного управління – рис. 1.1.

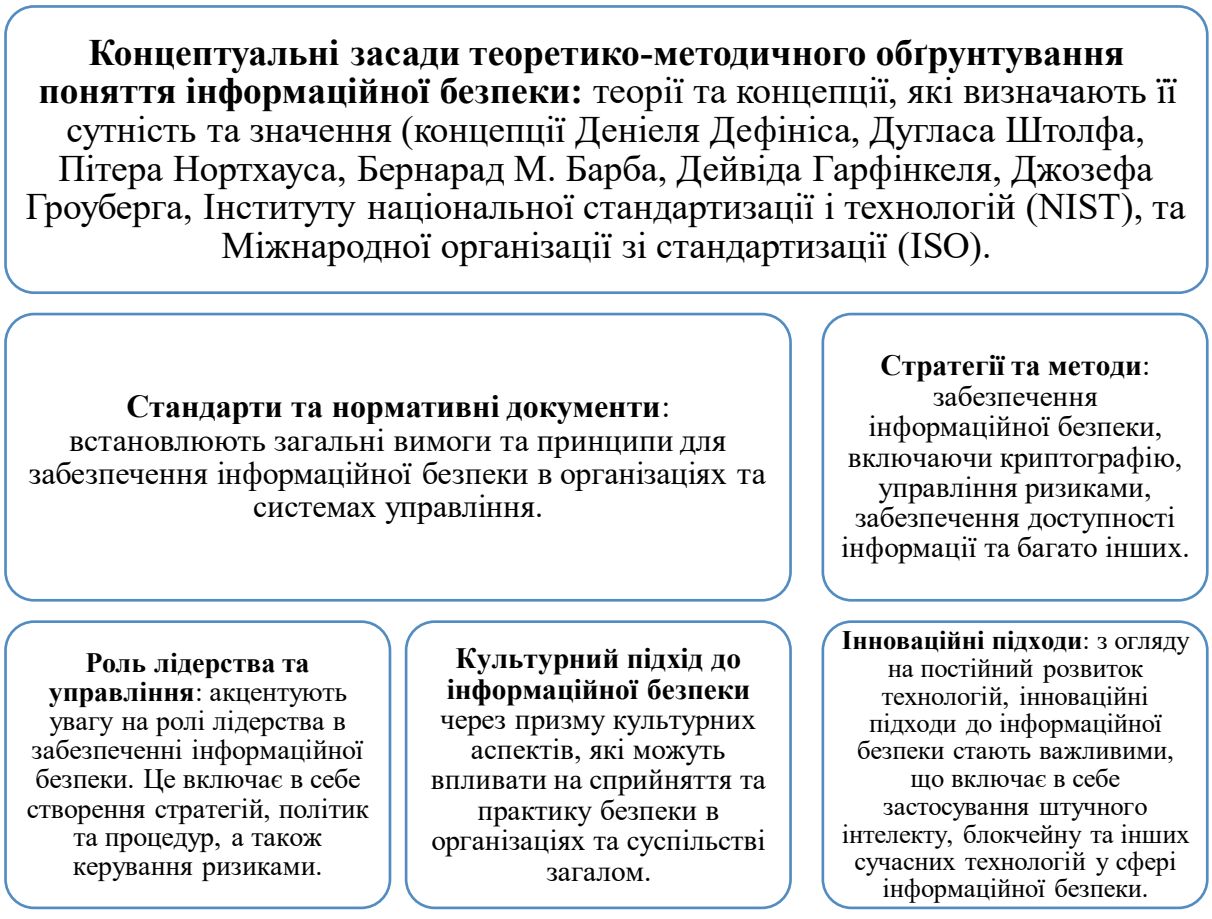

Рис. 1.1. – Специфіка визначення інформаційної безпеки у системі публічного управління

** Джерело: розроблено автором на основі аналізу джерел [15; 29; 59; 64; 78; 90]*

Отже, визначення інформаційної безпеки в системі публічного управління має свої особливості і відмінності від підходів у бізнесі та інших галузях. У сфері публічного управління інформаційна безпека завжди спрямована на захист інтересів суспільства та громадян. Відповідно, визначення інформаційної безпеки враховує не тільки комерційні аспекти, але й соціальні та політичні потреби. У системі публічного управління інформаційна безпека важлива для забезпечення демократичних процесів, зокрема забезпечення доступу до інформації для громадян та заборони цензури. Інформаційна безпека включає в себе підзвітність перед суспільством і громадянами, а також прозорість діяльності органів влади. Вона сприяє запобіганню корупції та забезпеченню відкритості. Поняття національної безпеки та інтересів держави є важливими у визначенні інформаційної безпеки в системі публічного управління, що може включати в себе заходи щодо захисту від зовнішніх загроз і кібератак на державні інформаційні ресурси. У публічному управлінні інформаційна безпека часто регулюється законодавством та політичними документами, які визначають правила обробки, збереження та розповсюдження інформації в державних органах. Одним з головних завдань органів публічного управління є забезпечення безпеки громадян. Тому інформаційна безпека в системі публічного управління спрямована на захист особистих даних, прав та свобод громадян. Публічне управління також стикається з глобальними викликами, такими як кібертероризм, кібершпигунство і кібератаки, які можуть мати міжнародний характер і вимагати співпраці з іншими країнами. Загалом, визначення інформаційної безпеки в системі публічного управління є більш комплексним та різноманітним порівняно з підходами у бізнесі. Воно орієнтоване на загальний інтерес, підзвітність, демократію та національну безпеку і враховує глобальні виклики, що виникають у світі сьогодні.

У науковій літературі пропонується розрізняти кілька ключових складових механізмів публічного управління інформаційною безпекою. По-перше, це нормативно-правові інструменти, що формують основу державної політики та визначають стандарти, регламенти, правила функціонування і відповідальність за порушення у сфері інформаційної безпеки. Без законодавчої бази та підзаконних актів будь-які технічні чи організаційні заходи залишаються фрагментарними. По-друге, організаційно-управлінські інструменти охоплюють створення спеціалізованих органів, визначення їх компетенцій, розподіл функцій і завдань між різними рівнями управління, формування механізмів координації та контролю. Вони забезпечують можливість системно реалізовувати політику інформаційної безпеки, перетворюючи її на практичні дії. По-третє, важливою складовою є технологічні інструменти – апаратні та програмні рішення, методи криптографічного захисту, системи виявлення вторгнень, засоби моніторингу, аналізу ризиків і управління інцидентами. Водночас технічні заходи ефективні лише за умови їх інтеграції з організаційними процесами та правовим забезпеченням. По-четверте, соціально-комунікаційні інструменти відображають культурні та освітні аспекти: формування культури інформаційної безпеки серед державних службовців, проведення навчання, інформування громадян про правила користування електронними послугами, забезпечення прозорості й довіри. Вони критично важливі, оскільки людський фактор традиційно визнається найбільш уразливим елементом інформаційних систем. Таким чином, механізми публічного управління інформаційною безпекою є комплексними, багаторівневими та соціотехнічними за своєю природою. Вони передбачають інтеграцію різних підсистем – інфраструктури, даних, людей та процесів – в єдину систему, здатну адаптуватися до змін середовища і протидіяти як зовнішнім, так і внутрішнім загрозам. У наукових дослідженнях підкреслюється, що саме системність і комплексність відрізняють механізми від окремих інструментів чи заходів. Вони виступають не лише засобом захисту, а й способом формування довіри громадян до держави, підвищення ефективності публічного управління та забезпечення

безперервності надання електронних послуг навіть в умовах кризових чи надзвичайних ситуацій.

На нашу думку, механізми публічного управління інформаційною безпекою доцільно розглядати як комплекс інституційних, організаційних, правових, технологічних та соціальних інструментів, за допомогою яких держава забезпечує захищеність інформаційних ресурсів, інформаційних систем та електронних сервісів у публічному секторі. Вони не є суто технічними або суто адміністративними діями, а формуються на перетині нормотворчості, управлінських процесів, координації діяльності різних суб'єктів і застосування спеціалізованих технологій. Таким чином, механізми виконують роль інтегрованих засобів, що, з одного боку, забезпечують стабільне функціонування державних електронних послуг, а з іншого – створюють умови для своєчасного виявлення, запобігання та нейтралізації загроз інформаційній безпеці.

Тепер перейдемо до аналізу поняття «електронні послуги».

Електронні послуги як поняття в науковій літературі розглядаються як інтердисциплінарний феномен, що поєднує технологічні, організаційні, соціальні та публічно-управлінські виміри. У вузькому технічному сенсі електронні послуги – це сервіси, надані через інформаційно-комунікаційні технології (ІКТ); у ширшому – це трансформація взаємодії громадян, бізнесу та держави завдяки цифровим каналам, яка включає зміни в процесах, інститутах і відносинах довіри. Цей міждисциплінарний підхід проявляється у кількох основних наукових напрямах, кожен з яких підкреслює власний набір теоретичних припущень, методів і практичних рекомендацій.

Технологічно-інфраструктурний підхід. Цей підхід акцентує на інструментах (портали, транзакційні системи, API, ідентифікація), стандартах і сумісності – тобто на «як працює» надання електронної послуги. Модель зрілості і стадій розвитку електронного урядування (каталогізація → транзакції → вертикальна інтеграція → горизонтальна інтеграція) показує, що технологічна складова є необхідною базою для повноцінних електронних послуг. «Етапна модель пояснює,

як сервіси еволюціонують від простого розміщення інформації до інтегрованих транзакційних систем».

Організаційно-процесуальний підхід (реінжиніринг процесів і управлінські зміни). Електронні послуги розглядають як інструмент трансформації публічної адміністрації: зміни бізнес-процесів, реорганізація компетенцій, нові ролі та відповідальність. Рамки, що поєднують технологію та організаційні мережі, підкреслюють необхідність синхронізації ІТ-інвестицій із процесними змінами. «Електронне урядування покликане поліпшити урядові процеси та зв'язки з громадянами шляхом ІКТ» [148].

Соціотехнічний підхід. Центральна ідея: електронні послуги – не лише технічні артефакти, а системи, де технологія та соціальні практики співеволюціонують. Аналіз публічних е-послуг має враховувати одночасно три характеристики: сервіс (функція), електронність (технологічна форма) та публічність (юридичний/інституційний контекст). Такий багатовимірний підхід дає змогу уникнути редукціонізму, коли «е-послуга» зводиться тільки до веб-форм. «Публічні електронні послуги мають три взаємопов'язані виміри: сервіс, електронність і публічність» [150; 162; 164].

Підхід довіри, ризику і прийняття користувачем. Дослідження прийняття е-послуг підкреслюють, що технічна наявність послуги ≠ її використання: ключові фактори – довіра до Інтернету і до держави, сприйнята корисність та простота використання, а також ризики (безпека даних, правова захищеність). Політики, що ігнорують ці фактори, отримують низьку користувацьку активність. «Довіра й сприйнятий ризик суттєво впливають на готовність використовувати електронні державні послуги» [140].

Модель публічної цінності і результативності. Заміщуючи вузькі індикатори (кількість форм), сучасні підходи роблять акцент на «публічній цінності» – наскільки е-послуги підвищують ефективність, прозорість, доступність, справедливість та підзвітність. Оцінка має комбінувати кількісні метрики (використання, час обслуговування) та якісні (довіра, інклюзивність). «Публічна цінність е-уряду – ключ до оцінки успіху електронних послуг» [156].

Підхід інтеграції й сумісності. Наукові дослідження вказують: реальна цінність електронних послуг досягається, коли системи різних владних рівнів й відомств можуть обмінюватися даними й процесами. Сумісність – це не лише технічні інтерфейси, а й політики, управління та стандарти. «Сумісність – багатовимірна здатність організацій ділитися інформацією та інтегрувати процеси» [186].

Підхід моделювання зрілості та вимірювання (індекси й метрики). Моделі зрілості/індекси (UN EGDI, OECD рекомендації) створюють стандартизовані рамки для порівнянь між країнами й моніторингу прогресу в наданні онлайн-послуг. Однак критики зауважують, що індекси часто фокусуються на «пропозиції» і менш – на «попиті» та реальному впливі. «EGDI оцінює надання онлайн-послуг як одну з трьох ключових складових цифрового уряду» [128].

Економіко-правовий та політико-адміністративний підходи. Ці напрями аналізують нормативно-правову базу (правила цифрового підпису, захист даних, доступність), політику відкритих даних і механізми забезпечення відповідальності. Вони показують, що без чіткої легітимації та правових гарантій електронні послуги залишаться фрагментованими. «Електронне управління визначається через правові та політичні рамки, що регулюють електронну взаємодію між владою та громадянами» [184; 185].

Бізнес-орієнтований підхід – модель спільних послуг. Деякі дослідники розглядають електронні послуги як результат упровадження спільних сервіс-центрів і бізнес-моделей, що зменшують дублювання і підвищують ефективність управлінських ресурсів. «Моделі спільних сервісів дозволяють оптимізувати витрати і покращити доступ до цифрових сервісів» [166].

Когнітивно-поведінкові та інклюзивні підходи. Окремий напрям зосереджений на бар'єрах у користувачів: цифрова грамотність, мовні й функціональні бар'єри, а також на методах дизайну для підвищення інклюзивності. Практики дизайну послуг і принципи «орієнтації на користувача» є ключовими для реальної доступності. «Дизайн публічних послуг має бути орієнтований на потреби користувача, а не на зручність організацій» [236].

Таким чином, електронні послуги – це форма надання адміністративних, комерційних чи соціальних сервісів за допомогою сучасних інформаційно-комунікаційних технологій (насамперед Інтернету), яка дозволяє здійснювати взаємодію між державою, бізнесом і громадянами дистанційно, у зручному цифровому форматі. Вони включають як надання інформації, так і виконання транзакційних дій (подання заяв, отримання довідок, здійснення платежів, реєстрація бізнесу тощо).

Проведений аналіз наукових підходів до поняття «механізми», «механізми публічного управління», «інформаційна безпека», «електронні послуги» дає підстави визначити поняття «механізми публічного управління інформаційною безпекою надання електронних послуг».

Поняття «механізми публічного управління інформаційною безпекою надання електронних послуг» слід розглядати як багатовимірну категорію, що поєднує інституційно-правові, організаційно-адміністративні, технологічні та соціально-комунікативні інструменти, спрямовані на гарантування захищеності процесів цифрової взаємодії громадян, бізнесу та держави. Наукова логіка цього визначення полягає в тому, що будь-яка електронна послуга є не лише сервісною функцією публічної влади, а й об’єктом ризиків і загроз, пов’язаних із несанкціонованим доступом, кібератаками, витоком чи маніпуляцією даними. Відтак, механізми управління інформаційною безпекою в цій сфері мають формувати цілісну систему, в якій правові норми забезпечують легітимність і підзвітність, організаційні процедури – безперервність та ефективність, технологічні засоби – стійкість та захищеність, а комунікаційні практики – довіру та прозорість.

З наукового погляду, це поняття передбачає синтез превентивних, захисних та адаптаційних заходів, що реалізуються через державну політику у сфері кібербезпеки, стандартизацію процесів електронного урядування, багаторівневу аутентифікацію користувачів, криптографічний захист інформації, а також розвиток цифрової культури суспільства. Таким чином, механізми публічного управління інформаційною безпекою електронних послуг виступають фундаментом довіри до

державних інституцій у цифровому середовищі, визначають якість взаємодії «держава – громадянин – бізнес» та забезпечують стійкий розвиток електронного урядування.

Системний аналіз наявних наукових підходів до визначення механізмів публічного управління дозволяє зробити висновок про необхідність інтегративного підходу до їх осмислення, який передбачає об’єднання функціонального, інституційного, процесного та системного вимірів у межах єдиного управлінського контуру [10]. Такий підхід відкриває можливість не лише до типологізації або класифікації управлінських механізмів, а й до формування авторського бачення їх структури, наповнення та логіки функціонування в конкретному предметному полі у сфері забезпечення інформаційної безпеки під час надання електронних публічних послуг [12].

З урахуванням специфіки цифрового середовища, яке характеризується високим рівнем технологічної складності, підвищеними ризиками інформаційних загроз, потребою в оперативному реагуванні та високими очікуваннями громадян щодо доступності й надійності послуг, механізми публічного управління мають бути не лише формально організованими, а й структурно адаптивними [87]. У цьому зв’язку доцільно визначити базовий склад компонентів механізмів публічного управління інформаційною безпекою електронних послуг, які мають бути наявними у будь-якій повноцінній моделі.

Нормативно-правовий компонент механізмів публічного управління інформаційною безпекою відіграє фундаментальну роль у забезпеченні легітимності, регламентованості та передбачуваності управлінських рішень і дій суб’єктів публічного управління. Він формує основу для упорядкованого функціонування системи захисту інформаційного простору, забезпечуючи правову визначеність меж повноважень, процедур реагування на загрози, вимог до технологічних рішень, прав та обов’язків суб’єктів і користувачів електронних публічних послуг. Цей компонент включає комплекс законодавчих, підзаконних, інституційних і міжвідомчих актів, які регулюють сферу інформаційної безпеки в контексті цифрового врядування. До його складу належать нормативні документи,

що визначають стандарти кіберзахисту, політику з обробки персональних даних, режим конфіденційної інформації, регламент функціонування електронних інформаційних систем, вимоги до безпеки цифрової ідентифікації та електронного документообігу. Особливе значення має узгодженість національного нормативно-правового поля із міжнародними стандартами, такими як ISO/IEC 27001, Загальний регламент ЄС про захист даних (GDPR), Директива NIS2 тощо. Нормативно-правовий компонент виконує низку функцій: забезпечує формальну легітимацію управлінських повноважень у сфері інформаційної безпеки; створює правові умови для функціонування механізмів міжвідомчої взаємодії; виступає основою для адміністративного і кримінального переслідування за порушення режиму безпеки; встановлює вимоги до відкритості, звітності та прозорості діяльності органів публічного управління. Важливо, що нормативно-правова основа не є сталою системою, що потребує постійного оновлення з урахуванням змін у технологічному середовищі, зростання складності загроз і трансформації міжнародних зобов'язань України. Таким чином, нормативно-правовий компонент є не лише формальним підґрунтям для реалізації механізмів публічного управління, а й запобіжником від зловживань, інструментом забезпечення довіри користувачів до публічних сервісів і гарантом збереження стабільності в умовах цифрових викликів та гібридних загроз [91].

Інституційно-організаційний компонент механізмів публічного управління інформаційною безпекою визначає структурну побудову системи суб'єктів, їхню компетенцію, функціональні зв'язки та взаємодію, а також формати координації та підпорядкування в межах реалізації управлінських функцій. Саме через цей компонент формується суб'єктно-інституційне поле публічного управління, в якому визначаються головні учасники процесу забезпечення інформаційної безпеки, розподіляються ролі та відповідальність за реалізацію стратегічних і тактичних управлінських завдань. Інституційно-організаційний вимір охоплює сукупність органів державної влади, органів місцевого самоврядування, спеціалізованих установ, координаційних рад, центрів кібербезпеки, технічних агентств та цифрових регуляторів, діяльність яких пов'язана з формуванням і

реалізацією політики в сфері інформаційної безпеки електронних публічних послуг. Особливу роль у цій системі відіграють такі інституції, як Міністерство цифрової трансформації, Державна служба спеціального зв'язку та захисту інформації, Національний координаційний центр кібербезпеки при РНБО, а також відповідні структурні підрозділи в обласних та місцевих адміністраціях. Змістом інституційно-організаційного компонента є не лише визначення суб'єктів, але й чітке окреслення меж їхніх повноважень, рівня автономності, механізмів підзвітності та взаємодії. У межах ефективної моделі механізму публічного управління має бути забезпечений баланс між централізованим стратегічним управлінням та децентралізованим виконанням управлінських функцій на регіональному та локальному рівнях. Важливим елементом є встановлення процедур комунікації, обміну інформацією, спільного реагування на інциденти, а також оперативної координації дій у разі загроз інформаційній інфраструктурі. Інституційно-організаційний компонент також передбачає наявність чітких регламентів, посадових інструкцій, організаційних структур та процедур делегування відповідальності, що дозволяє забезпечити передбачуваність і ефективність управлінських процесів. Його функціонування ґрунтується на принципах субсидіарності, прозорості, координації, ієрархічності та компетентності. За своєю суттю цей компонент виступає каркасом усього механізму, формуючи управлінське середовище, в межах якого реалізуються інші складові: технологічна, правова, ресурсна тощо [38].

Функціонально-процесуальний компонент механізмів публічного управління інформаційною безпекою електронних послуг виконує системоутворюючу роль, оскільки забезпечує логічну послідовність, структурованість та узгодженість реалізації управлінських функцій у динамічному цифровому середовищі. Його сутність полягає у формалізації циклу управлінських дій, спрямованих на досягнення цілей безпеки, мінімізацію ризиків і підвищення стійкості електронних сервісів до внутрішніх та зовнішніх загроз. Цей компонент охоплює повний цикл управління від ідентифікації та аналізу ризиків, до планування, реалізації заходів реагування, моніторингу, оцінювання ефективності та коригування політик і

процедур. Кожен з етапів є необхідною ланкою у забезпеченні системної дії механізму публічного управління. Зокрема, виявлення загроз передбачає постійний моніторинг інформаційного середовища, оцінку вразливостей та аналіз індикаторів безпеки; планування, організацію та координацію відповідних технічних, нормативних і адміністративних кроків; моніторинг, збір та аналіз зворотної інформації про стан безпеки. Особливістю функціонально-процесуального компонента є його орієнтація на безперервність і циклічність, що забезпечує гнучкість та адаптивність системи публічного управління. У сучасних умовах цифрової трансформації цей компонент має бути здатним до швидкого реагування на нетипові або нові загрози, що вимагає застосування сучасних інструментів аналізу даних, ситуаційного прогнозування, сценарного моделювання та управління інцидентами в режимі реального часу. Крім того, функціонально-процесуальний компонент передбачає встановлення чітких регламентів, інструкцій, процедур управління подіями, що становлять ризик для інформаційної безпеки. Важливою складовою є механізми звітності, контролю й аудитів, які дозволяють оцінити ефективність реалізованих заходів, виявити слабкі місця в системі та ініціювати відповідні управлінські рішення щодо її вдосконалення. Таким чином, реалізація управлінських функцій в рамках цього компонента повинна бути не лише формалізованою, але й гнучкою до змін, щоб залишатися ефективною в умовах високої невизначеності [3]. Загалом функціонально-процесуальний компонент виступає не просто технічною основою механізму, а його динамічною логікою дії, що забезпечує узгодженість між стратегічним баченням інформаційної безпеки, інституційними можливостями та ресурсним забезпеченням. Його якісна реалізація є критичним фактором результативності публічного управління в цифрову епоху, коли ризики мають комплексний характер, а управлінські рішення мають прийматися в умовах обмеженого часу та зростаючих очікувань з боку громадськості.

Технологічний компонент механізмів публічного управління інформаційною безпекою електронних послуг є критично важливою складовою, що забезпечує практичну реалізацію управлінських рішень у цифровому середовищі. Він включає

широкий спектр інструментів, рішень та інфраструктурних елементів, які спрямовані на гарантування конфіденційності, цілісності, доступності та стійкості інформації, що циркулює в системах електронного врядування. У межах цього компонента здійснюється безпосередня інтеграція інформаційно-комунікаційних технологій в управлінську діяльність публічного сектора з метою забезпечення захищеного функціонування електронних сервісів. Технологічна складова не лише забезпечує технічну реалізацію стандартів інформаційної безпеки, а й формує базу для автоматизованої підтримки прийняття управлінських рішень. Використання алгоритмів машинного навчання, систем штучного інтелекту та автоматизованих протоколів дозволяє здійснювати проактивне виявлення аномалій у роботі систем, моделювання поведінки загроз, а також розробку сценаріїв реагування. Застосування таких технологій значно підвищує ефективність публічного управління в умовах зростання обсягів і складності даних. Ключовим завданням цього компонента є забезпечення неперервного захисту інформаційного простору публічного сектора на всіх рівнях – від інфраструктурного (фізичні сервери, дата-центри, хмарні рішення) до прикладного (платформи е-сервісів, мобільні застосунки, вебпортали). Технологічні рішення повинні інтегруватися в загальну архітектуру механізму публічного управління, відповідати національним стандартам та міжнародним вимогам, а також бути придатними до масштабування, модернізації та адаптації до нових типів загроз [59]. Отже, технологічний компонент є не просто технічним елементом системи, а стратегічною основою для формування кіберстійкої моделі механізмів публічного управління. Він забезпечує функціонування електронних послуг на засадах безпеки, надійності та доступності, сприяючи водночас підвищенню рівня довіри громадян до цифрових сервісів держави та зміцненню її інформаційного суверенітету.

Комунікаційний компонент механізмів публічного управління інформаційною безпекою електронних послуг є ключовим елементом, що забезпечує ефективну інформаційну взаємодію між усіма учасниками управлінського процесу: суб’єктами публічного управління, громадськістю, постачальниками цифрових сервісів, технічними операторами та безпосередніми

користувачами електронних публічних послуг. Він реалізує функцію двостороннього обміну інформацією, зворотного зв’язку, оперативного інформування про ризики, інциденти, заходи реагування, а також забезпечує прозорість і відкритість дій публічної влади в сфері інформаційної безпеки. Компонент охоплює мережу каналів, платформ і механізмів комунікації, які використовуються для узгодження дій, передачі управлінських рішень, роз’яснення нормативних вимог, інформування про нові цифрові сервіси, збору зворотної інформації щодо роботи електронних послуг, а також підвищення обізнаності громадян про ризики в інформаційному середовищі. До складу комунікаційного блоку входять урядові інформаційні портали, електронні системи публічних консультацій, мобільні застосунки, платформи е-демократії, офіційні канали в соціальних мережах, а також системи раннього попередження про кіберінциденти [28].

Ресурсний компонент механізмів публічного управління інформаційною безпекою електронних послуг є базовим елементом, що забезпечує практичну реалізацію усіх інших складових механізму та визначає його спроможність до сталого функціонування, адаптації до змін і підвищення ефективності в умовах динамічного цифрового середовища. У найширшому розумінні ресурсний компонент охоплює кадрове, фінансове, матеріально-технічне, організаційне та інфраструктурне забезпечення, необхідне для стабільної дії механізмів управління інформаційною безпекою. На кадровому рівні цей компонент передбачає наявність кваліфікованих фахівців з інформаційної безпеки, цифрового управління, права, кіберзахисту, а також управлінців, здатних координувати міжвідомчу взаємодію та приймати стратегічні рішення в умовах високої невизначеності. Питання людського капіталу є особливо актуальним у контексті цифрової трансформації, що вимагає від публічного сектора не лише технічної компетентності, а й постійного оновлення знань, розвитку «м'яких» навичок, адаптивності та критичного мислення, що зумовлює потребу в системній політиці держави щодо підготовки, сертифікації та підвищення кваліфікації кадрів у сфері інформаційної безпеки, з урахуванням міжнародних стандартів і технологічних трендів. Фінансове забезпечення

функціонування механізмів публічного управління у сфері інформаційної безпеки охоплює бюджетне фінансування, цільові програми, грантову підтримку, проєктно-орієнтовані інструменти та державно-приватне партнерство. Ефективність фінансового ресурсу полягає не лише в обсягах виділених коштів, а й у прозорості їх розподілу, підзвітності за їх використання, пріоритетності інвестування в найбільш вразливі ділянки цифрової інфраструктури. Зважаючи на вартість сучасних технологічних рішень у сфері ІБ, зокрема захищених платформ, систем шифрування, інструментів виявлення та реагування на кіберінциденти, достатній і стабільний фінансовий ресурс є необхідною умовою безперервного функціонування механізму. Матеріально-технічне та інфраструктурне забезпечення включає в себе обладнання (сервери, захищені канали зв'язку, дата-центри), засоби резервного копіювання, автономні джерела живлення, а також розвинену ІТ-інфраструктуру, яка дозволяє здійснювати захищену обробку, збереження та передачу даних. Особливе значення має відповідність цієї інфраструктури сучасним вимогам безпеки, її захищеність від фізичного доступу сторонніх осіб, стійкість до форс-мажорних ситуацій та здатність до швидкого відновлення після інцидентів. Загалом ресурсний компонент виступає основою для інституційної стійкості та операційної спроможності механізмів публічного управління інформаційною безпекою. Без належного ресурсного забезпечення будь-які нормативні, організаційні чи технологічні рішення залишаються декларативними. Саме тому системне планування, прозоре управління ресурсами, а також стратегічне інвестування в розвиток кадрового, технологічного й фінансового потенціалу є критично важливими умовами для реалізації ефективної політики публічного управління.

Ураховуючи складність цифрового середовища, динаміку ризиків, а також міжсекторну природу процесів надання електронних публічних сервісів, доцільним є системне групування елементів механізму за функціональними ознаками. Наведена нижче схема (рис. 1.2) відображає базову логіку побудови механізмів публічного управління інформаційною безпекою.

Рис. 1.2. Компоненти механізмів публічного управління інформаційною безпекою надання електронних послуг

** Джерело: розроблено автором на основі аналізу [4; 32; 34; 85;]*

Визначення саме таких компонентів базується на глибокому осмисленні потреб електронного врядування в умовах цифрової трансформації, а також на узагальненні практичного досвіду держав-членів ЄС, що реалізують високі стандарти цифрової безпеки у публічному секторі.

1.3. Проблеми публічного управління інформаційною безпекою надання електронних послуг

Публічне управління інформаційною безпекою під час надання електронних послуг в Україні зазнало суттєвих викликів, які загострились у зв'язку з воєнним станом. Масштабні кібератаки на держреєстри та критичну інфраструктуру, ампліфіковані фізичними ударами по енергетичних і телекомунікаційних об'єктах, створили комбінований ризик одночасного порушення доступності, цілісності й конфіденційності державних електронних сервісів; виявлені атаки мали достатньо високий ступінь координації та спрямовані на дезорганізацію надання публічних послуг (тимчасове припинення роботи реєстрів, масове зниження доступності порталів і сервісів). Це вимагало швидкої реакції від операторів сектора й державних органів, але також виявило системні слабкості управління ризиками й координації.

Технічні проблеми, що ускладнюють забезпечення інформаційної безпеки державних електронних послуг у воєнний час, мають кілька взаємопов'язаних вимірів. По-перше, значна частина державних ІТ-систем була спроєктована й впроваджена у мирний період з акцентом на функціональність і централізацію, а не на сценарії масштабних криз і бойових дій; через це виявляються системні вразливості – відсутність географічно розподілених резервів, обмежена кількість розподілених копій реєстрів, слабка фізична та логічна ізоляція критичних компонентів і мінімальна підготовка до відмов у разі втрати енергопостачання або каналів зв'язку. Наслідком такої архітектури є висока кореляція між фізичними ударами по інфраструктурі й цифровими збоями, що підвищує ймовірність одночасної втрати доступності багатьох служб. Цей факт підтверджується як

аналітичними оглядами, зосередженими на досвіді України під час широкомасштабних кібератак, так і дослідженнями, які показують швидкий перехід від реактивного режиму відповіді до нагальної потреби в проактивному плануванні стійкості [231; 234].

По-друге, сучасний ландшафт атак дедалі частіше має мультивекторний характер: DDoS-удари використовуються не лише для виведення сервісів з доступу, але і як прикриття або компонент ширшої кампанії, що включає витоки або модифікацію даних, а також цілеспрямоване ураження механізмів логування й моніторингу. Комбінація DDoS та операцій, спрямованих на цілі дані, значно ускладнює стандартні процедури реагування: під час DDoS-атаки відсутня оперативна видимість, що сповільнює ідентифікацію витоку; одночасна компрометація резервних копій або шляхів реплікації може унеможливити швидке повернення до консистентного стану. Сучасні наукові огляди й практичні звіти підкреслюють, що захист від окремих типів атак (тільки відмовостійкість або тільки контроль доступу) перестає бути достатнім; потрібні інтегровані механізми виявлення багатокомпонентних інцидентів і автоматизовані системи реагування [106; 237].

По-третє, питання ланцюгів постачання програмних продуктів і залежності від іноземних хмарних провайдерів створюють додаткові ризики під час воєнного часу. Атаки на програмні залежності, маніпуляції з відкритим кодом або зберіганням пакунків, а також залежність від сервісів техпідтримки й оновлень з-за кордону роблять державні сервіси вразливими до саботажу чи втрати підтримки в умовах обмежень логістики або санкцій. Практичні розслідування і державні огляди показують, що компрометація одного компонента ланцюга розробки може мати масовий каскадний ефект на всі системи, які його використовують, а відсутність у державних замовників прозорих процедур управління залежностями підсилює ризики.

Ці технічні проблеми мають кілька практичних наслідків для забезпечення безперервності електронних послуг. По-перше, архітектурна централізація посилює ймовірність одночасної втрати доступу для великої кількості користувачів

(зростає радіус розповсюдження інциденту). По-друге, мультивекторні атаки вимагають від оператора не лише реагування на симптоми (відновлення доступу), а й одночасного проведення ретельного аналізу цілісності даних і ланцюгів довіри, що уповільнює повернення до попереднього стану. По-третє, проблеми з постачанням і оновленням можуть призвести до того, що вразливості залишаються незаґейтованими тривалий час або що державні органи будуть змушені використовувати неконтрольовані тимчасові рішення, що підриває загальну безпеку. Оцінка економічних і функціональних наслідків таких сценаріїв підкреслює необхідність інвестицій у кіберстійкість як ключовий елемент національної безпеки [203].

Технічні контрзаходи та практики пом’якшення повинні бути багаторівневими й практично орієнтованими. Перше – це архітектурні практики – геодиверсифікація дата-центрів, мультихостинг і дзеркалювання сервісів, ізоляція критичних реєстрів у «повітряних зазорах» або в логічно відокремлених зонах з обмеженим експортуванням даних – знижують ризик кореляції відмов. Друге – оперативні практики – автоматизовані інструменти для детекції аномалій, скоординовані сценарії реагування, використання «червоних команд» і регулярні імітаційні навчання – підвищують швидкість і якість реагування на мультивекторні інциденти. По-третє, безпека ланцюга постачання потребує політик управління залежностями, впровадження специфікації матеріалів програмного забезпечення, підписування артефактів і застосування практик безпечного DevSecOps (методологія та культура, що інтегрує безпеку в кожен етап життєвого циклу розробки програмного забезпечення, перетворюючи безпеку на спільну відповідальність команд розробки, безпеки та експлуатації), а також пріоритезації локалізації критичних компонентів або доступу до альтернативних джерел оновлень у кризових умовах. На технічному рівні також необхідно впроваджувати криптографічні механізми забезпечення консистентності (наприклад, підписи та хешування резервних копій) й автоматизовані процедури валідації резервів перед відновленням [203; 210; 222].

Важливо підкреслити, що технічні заходи не можуть бути ефективними без підтримки на рівні політики й кадрового потенціалу. Інвестиції в підготовку фахівців, стандартизація процедур обміну індикаторами компрометації, нормативне визначення вимог до стійкості провайдерів і механізмів аудиту – усе це необхідні елементи комплексної стратегії кіберстійкості. Дослідження в ряді країн демонструють, що здатність системи адаптуватися і швидко відновлюватися значною мірою визначається наявністю попередньо відпрацьованих процедур і кадрової спроможності, а отже, підтримка масштабних інвестицій у нарощування потенціалу має прямий практичний ефект [231; 240].

Таким чином, технічні проблеми – це не лише питання окремих вразливостей, а комплексна взаємодія архітектурних рішень, модальностей атак і глобальних ланцюгів постачання, загострена контекстом воєнного часу. Ефективна відповідь вимагає одночасного посилення архітектурної стійкості, оперативної детекції і реагування на мультивекторні інциденти, а також системного управління ланцюгами постачання програмного забезпечення з урахуванням можливих логістичних і політичних обмежень.

Організаційно-адміністративні проблеми публічного управління інформаційною безпеки під час надання електронних послуг в умовах воєнного стану мають системний характер і формуються на перетині інституційної структури, нормативного поля та людських ресурсів. Так, характерною проблемою є фрагментація відповідальності між різними державними органами – міністерствами, відомствами, спеціалізованими службами (наприклад, Службою безпеки України, Держспецзв'язком, Національним банком, Національною поліцією) та операторами критичної інфраструктури – що створює множинні «перехідні зони» відповідальності, в яких рішення про пріоритезацію ресурсів, доступ до реєстрів або ініціацію заходів реагування можуть затримуватися або дублюватися. Така інституційна роздрібненість підсилює ризики повільної координації у кризі і ускладнює реалізацію єдиного оперативного підходу до захисту та відновлення електронних послуг. Аналіз національних моделей кібербезпеки свідчить, що без чіткого визначення мандатів і механізмів

міжвідомчої взаємодії країни стикаються з відставанням у швидкості реакції та уніфікації процедур (прикладні оцінки структури української системи кібербезпеки) [171; 229].

Крім того, відсутність єдиного, оперативного механізму обміну інформацією про кіберінциденти та індикаторами компрометації між державними установами, приватними операторами та суміжними структурами підриває колективну здатність виявляти, локалізувати та нейтралізувати загрози. Коли обмін інформацією здійснюється фрагментарно або з великими часовими лагами, локальні інциденти ризикують ескалувати в масштабніші кампанії; крім того, неповна картина подій ускладнює проведення аналізу цілісності даних і коректного відновлення сервісів. Державні практики, де працюють централізовані CERT/CSIRT-структури з протоколами швидкого обміну даними та стандартизованими форматами звітування, показують вищу ефективність у зниженні «часу виявлення – часу реагування» [105; 228].

Водночас дефіцит кваліфікованих кадрів у державному секторі загострює проблему: державні органи часто не мають достатніх резервів IT-безпекових фахівців, здатних працювати 24/7 під час масованих атак, одночасно здійснювати аналіз інцидентів, координувати відновлення сервісів і вести комунікацію з громадянами. У воєнний час частина висококваліфікованих спеціалістів може бути мобілізована або залучена до інших пріоритетних завдань, що ще більше обмежує кадровий потенціал. Брак штатних ресурсів змушує державу звертатися до зовнішніх джерел компетенцій, проте без формалізованих процедур залучення такі дії створюють додаткові ризики у сфері контролю доступу, збереження державної таємниці й юридичної відповідальності [97; 229].

Вимушене й широке залучення волонтерських кіберспільнот та приватних IT-компаній породжує гібридну модель реагування, котра має як переваги, так і суттєві недоліки. З одного боку, волонтерські ініціативи (у тому числі так звані «IT Army» та інші неформальні групи) прискорюють технічне покриття інцидентів, забезпечують додаткові людські ресурси і мобілізують суспільну підтримку в кіберзахисті. З іншого – відсутність чітких процедур інтеграції волонтерів у

державні плани, стандартизованих вимог до доказовості дій, механізмів контролю і підзвітності може ускладнити координацію великих операцій, привести до перешкоджання офіційним операціям або до порушення міжнародних і національних правових норм. Емпіричні та аналітичні дослідження показують, що добровольчі ініціативи іноді виконують тактичні функції, але їх діяльність може конфліктувати з довгостроковими стратегічними операціями та створювати ризики для правового статусу доказів і дипломатичної відповідальності [163].

Також відсутність прозорих процедур публічно-приватного партнерства у сфері кібербезпеки ускладнює формалізацію ролей приватних операторів та постачальників при реагуванні на інциденти. Хоча приватний сектор часто має передові технології й оперативні рішення, їхня інтеграція в державні механізми потребує узгоджених контрактних умов, стандартів обміну інформацією, правил доступу до критичних систем і вимог щодо аудитів та сертифікації. Публікації про успішні приклади публічно-приватного партнерства підкреслюють необхідність формалізованих платформ для обміну знаннями, регулярних сумісних навчань і чітких правил щодо розподілу відповідальності під час кризи [207].

Підсумовуючи, організаційно-адміністративні проблеми в публічному управлінні інформаційною безпекою під час воєнного стану виникають із поєднання фрагментації інституцій, дефіциту кадрів, неформальної участі волонтерів і недостатньо впорядкованих механізмів публічно-приватного партнерства. Розв’язання цих проблем вимагає не лише технічних інвестицій, але й глибинних реформ у сфері управління: нормативного закріплення мандатів, стандартів обміну й підзвітності, систем підготовки людських ресурсів та формалізованих процедур інтеграції усіх зацікавлених сторін у єдину систему національного реагування.

У правовому та регуляторному вимірі публічного управління інформаційною безпекою в умовах воєнного стану спостерігається багатовимірна напруга, пов’язана з одночасною необхідністю оперативного реагування на загрози національній безпеці та дотриманням фундаментальних прав людини – права на доступ до інформації, приватності та доступу до ефективних судових засобів.

Законодавче запровадження воєнного стану відкриває державі можливість вживати спеціальних обмежень, проте такі обмеження повинні відповідати критеріям суворої необхідності, пропорційності та тимчасовості, закріпленим у міжнародних стандартах про дерогації у надзвичайних ситуаціях; зокрема, загальні коментарі Комітету ООН з прав людини та практика Європейського суду з прав людини підкреслюють, що дерогації від прав мають бути «строго необхідними» і не повинні суперечити іншим міжнародним зобов'язанням держави [232].

Практика застосування обмежень у воєнний час часто включає заборони або обмеження використання певних цифрових сервісів у службовому середовищі (як-от рішення щодо блокування або недопущення офіційного використання певних месенджерів), які аргументуються ризиками контррозвідки, кібератак чи витоку даних. Такі заходи можуть бути виправданими як тактичні кроки для зниження ризиків оперативної компрометації, але їх правомірність залежить від чітко визначених юридичних підстав, прозорих процедур запровадження та механізмів контролю (наприклад, строків дії, критеріїв оцінки ризику, процедур перегляду рішень). Інакше кажучи, технічна обґрунтованість заходу не звільняє від необхідності забезпечити юридичні гарантії і процесуальні механізми для захисту прав осіб. Окремі приклади державних обмежень свідчать про тенденцію до оперативного прийняття рішень адміністративного характеру, що потребує нормативного підсилення та прозорої комунікації з суспільством.

Вплив таких обмежень на доступ до інформації і приватність є багатогранним. По-перше, заборони в офіційних середовищах можуть ускладнювати внутрішню комунікацію й доступ працівників до довідкових ресурсів, якщо альтернативи не забезпечені або не відповідають необхідним рівням функціональності. По-друге, заходи, які передбачають посилену перевірку пристроїв, централізований моніторинг або вилучення даних з мобільних пристроїв, створюють ризики непропорційного втручання у приватне життя і зменшують довіру громадян до державних сервісів; міжнародні керівні принципи закликають до збереження балансу між національною безпекою та правами людини шляхом запровадження чітких меж і процедур доступу до персональних даних. У

національному контексті це означає, що будь-які операції з обробки даних у воєнний час мають бути здійснені відповідно до принципів необхідності та пропорційності, а також із встановленням механізмів контролю й аудиту [96].

Проблема процедур адміністративного оскарження і підзвітності набуває важливого значення саме у кризовому режимі: оперативні рішення органів влади щодо обмеження доступу до сервісів, блокування ресурсів чи доступу до даних повинні супроводжуватися доступними та ефективними формами оскарження, можливістю незалежного перегляду і прозорою публічною звітністю. Відсутність таких механізмів підвищує ризик зловживань, створює підґрунтя для перманентного розширення надзвичайних практик і підриває верховенство права. Практика міжнародних організацій та рекомендації з прав людини наголошують, що навіть у стані війни держава не втрачає всіх своїх зобов'язань: дерогації застосовні лише в межах, суворо необхідних для подолання загрози, а деякі права (наприклад, право на життя, заборона катувань) є недоторканними.

Реформаторські виклики у національному регуляторному полі стосуються як оновлення законодавства про захист персональних даних, так і розробки спеціальних процедур та стандартів для застосування екстрених повноважень. Процеси адаптації національного правового поля (зокрема кроки щодо імплементації сучасних стандартів захисту персональних даних та їхнього поєднання з нормами воєнного часу) мають забезпечити сумісність із європейськими практиками і міжнародними зобов'язаннями, водночас дозволяючи оперативну гнучкість у відповідь на кіберзагрози. Така інтеграція вимагає як нормативних змін (чітке визначення підстав для втручання, процедур видачі дозволів, строків дії), так і технічних та організаційних гарантій (аудит, логування дій, незалежні наглядові органи).

Нарешті, існує ризик «функціональної інерції» – коли тимчасові екстрені норми та практики, запроваджені під час війни, можуть закріпитися в адміністративній практиці після завершення надзвичайної ситуації. Щоб запобігти такому розвитку подій, правове регулювання має містити чіткі механізми автоматичного перегляду та скасування надзвичайних заходів, строки дії, вимоги

до звітування про їх застосування та критерії для оцінки їхньої доцільності після припинення воєнного стану. Міжнародні стандарти й практика ЄСПЛ вимагають, щоб дерогації не ставали звичкою й щоб відновлення прав і процедур здійснювалося невідкладно після зникнення загрози [144].

Отже, правовий і регуляторний вимір інформаційної безпеки в умовах війни – це поле напруженого балансування між оперативною потребою захищати критичну інформацію й обов'язком держави забезпечувати права і свободи громадян. Ефективна регуляторна відповідь повинна поєднувати: чітко виписані правові підстави для експедитивних обмежень із вимогами пропорційності й тимчасовості; прозорі процедури контролю й оскарження, які зберігають доступ до правосуддя; технічні гарантії мінімізації втручань у приватність; механізми повернення до звичайного режиму з детальним аудиторським звітом про використані повноваження. Такий підхід дозволить поєднати необхідність оборони під час війни із захистом фундаментальних прав у довгостроковій перспективі.

Проблеми доступу та цифрової рівності в умовах воєнного часу мають багатошаровий характер і прямо впливають на реалізацію базових прав громадян. Зокрема, війна спричинила як пряму фізичну деградацію інфраструктури (удари по енергетичних та телекомунікаційних об'єктах), так і непряму – через масове переміщення населення та тимчасову втрату послуг. Це призвело до зниження загальної доступності Інтернету та падіння числа активних користувачів у порівнянні з мирним часом, що фіксують міжнародні огляди; відповідно, частина населення опинилася поза цифровим простором у найкритичніший момент потреби в електронних сервісах.

Крім того, відключення електропостачання та руйнування мережевих вузлів створюють прямий бар'єр для користування електронними послугами, оскільки навіть мобільні пристрої і меседжери залежать від енергії та Інтернет-покриття. Ураження енергетичної інфраструктури має мультисекторний ефект: воно одночасно обмежує доступ до онлайн-платформ, унеможливлює роботу банківських терміналів і регіональних відділень соціальних установ, а також

ускладнює логістику доставки допомоги – ситуацію, яку відзначають ООН і гуманітарні агентства при оцінці ризиків перед настанням зимового періоду [102].

Водночас вразливі групи постраждали непропорційно: громадяни з інвалідністю, багатодітні родини, літні люди, внутрішньо переміщені особи та ті, хто втратив джерела доходів, стикаються з подвійним бар'єром – фізичним (відсутність інфраструктури, енергії, пристроїв) і цифровим (низька цифрова грамотність, відсутність реєстраційних даних або цифрової ідентичності). Оцінки міжнародних організацій вказують, що численні групи, які раніше не були серед бідних, опинилися в зоні вразливості; одночасно старші верстви населення та люди з низьким рівнем доходу користуються електронними послугами значно рідше, що посилює нерівність у доступі до соціальних виплат і адміністративних довідок [195].

На додачу, технічна залежність від окремих провайдерів зв'язку та супутникових рішень (наприклад, широко використовуваного в країні Starlink) створює системний ризик: глобальні збої чи локалізовані проблеми у зовнішнього провайдера миттєво відбиваються на спроможності органів влади та населення отримувати критичні послуги. Нещодавні випадки масових перебоїв у роботі таких сервісів показали вразливість операцій, що спираються на одну технологічну опору, та підкреслили необхідність диверсифікації каналів зв'язку й планів запасних рішень.

Інформаційна доступність електронних послуг під час інфраструктурних збоїв також ускладнюється недоліками процедур «резервного обслуговування»: відсутність офлайн-альтернатив, недостатнє розгортання мобільних пунктів надання послуг, слабка мережа локальних центрів допомоги й поширеність централізованих цифрових реєстрів без належних дзеркал або механізмів офлайн-верифікації. У підсумку це призводить до реальних порушень прав – невиплат соціальної допомоги, неможливості оформити документи, складнощів у доступі до медичних і соціальних сервісів – особливо у віддалених регіонах або зонах, що зазнали ударів. Громадські організації та правозахисні групи давно звертають увагу

на ризик перетворення цифрового виключення на додатковий фактор гуманітарної кризи [230].

Ці проблеми мають системні наслідки для довіри до державних електронних сервісів і для ефективності політик соціального захисту. Якщо електронні канали не гарантують доступності у критичні моменти, урядові програми ризикують втратити оперативність і справедливість у наданні допомоги. Міжнародні та національні оцінки закликають поєднувати технічні інвестиції (диверсифікація мереж, резервні енергетичні джерела, дзеркальні реєстри) з організаційними заходами (мобільні центри, офлайн-процедури, грошові ваучери, альтернативні канали реєстрації) та соціально-орієнтованими інтервенціями, які надають пріоритет уразливим групам.

Управлінські наслідки для політики цифрової безпеки вимагають системної, багаторівневої відповіді, що поєднує стратегічне планування, нормативно-правову реформу, міжсекторальну координацію та технічні інструменти реалізації. Необхідність національної стратегії кіберстійкості витікає як із практики реагування на інциденти, так і з принципів управління критичною інфраструктурою: стратегія має змістити фокус із суто реактивного захисту на забезпечення безперервності послуг і відновленості, встановивши цілі, індикатори й відповідальні інституції для реалізації заходів з диверсифікації каналів зв’язку, географічно розподілених дата-центрів, та резервування критичних сервісів. Така стратегія повинна містити чіткі вимоги до архітектури державних ІТ-систем (наприклад, мультихостинг, дзеркалювання даних, ізольовані «бастіони» для критичних реєстрів), а також механізми ресурсного забезпечення (фонди на модернізацію, пільги, програми кредитування інвестпроєктів з підвищення стійкості). Емпіричні та політик-орієнтовані керівні документи підкреслюють, що національні стратегії повинні поєднувати технічні стандарти з управлінськими механізмами моніторингу й оцінки впровадження [174].

Крім того, забезпечення безперервності послуг потребує конкретних технічних і процедурних вимог, що мають бути закладені в державні політики: мультиканальне резервування (фіксована мережа + мобільні мережі + супутникові

рішення), геодиверсифікація дата-центрів із відокремленим енергозабезпеченням, автономні канали зв'язку для критичних служб (резервні посилання, супутниковий резервний канал), автоматизовані процедури відновлення (підручники з організованого аварійного відновлення) і регулярне тестування планів аварійного відновлення (настільні вправи, повномасштабні тренування). При цьому важливим елементом є стандартизація вимог до постачальників послуг та контрактів з урахуванням сценаріїв криз – щоб забезпечення резервних потужностей і терміни відновлення були формально закріплені. Відомі практики національних програм та технічні стандарти (NIST, ENISA) детально описують підходи до проєктування кіберстійких систем і методів тестування [134].

Водночас реформування нормативного поля є критично необхідним для балансування між оперативною гнучкістю у кризі й захистом прав громадян. Законодавчі ініціативи повинні уніфікувати критерії для застосування надзвичайних заходів (строго визначені підстави, часові межі, механізми перегляду і прозорі процедури повідомлення громадськості), встановити процедури контролю й оскарження адміністративних рішень у сфері інформаційної безпеки, а також забезпечити гарантії захисту персональних даних під час кризових операцій (мінімізація збору, логування доступу, аудит, незалежний нагляд). Міжнародні настанови з дерогацій і захисту даних під час надзвичайних ситуацій (EDPB, ЄК, OECP) вказують, що дерогації від стандартних правил мають бути тимчасовими, пропорційними й супроводжуватись механізмами відновлення звичайного режиму після завершення кризи.

Формалізація механізмів публічно-приватного партнерства і інтеграція волонтерських ІТ-груп у державні плани реагування є практичною необхідністю, але вимагає чітких правил. Це означає розробку стандартів сертифікації і допуску зовнішніх фахівців, шаблонів договорів із визначенням відповідальності й SLA, процедур обміну інформацією (формати IOC, часові вимоги, канали передачі) і протоколів для залучення волонтерів із визначенням правового статусу їхніх дій, вимог до збереження доказів і захисту державної інформації. Публічно-приватні платформи обміну інформацією й секторальні ISAC/ISAO показали свою

ефективність у підвищенні ситуаційної обізнаності; однак інтеграція має супроводжуватися правовими гарантіями (конфіденційністю, незастосуванням санкцій проти інформаторів, чіткими межами доступу до критичних систем) [152].

Посилення правозастосування й технічної координації на рівні організаційних підрозділів або спеціалізованих команд реагування на комп'ютерні надзвичайні події та інциденти інформаційної безпеки та операторів критичної інфраструктури вимагає єдиних директив щодо обміну індикаторами компрометації, стандартів реагування та процедур координації між операторами і державою. Практично це означає впровадження стандартизованих форматів обміну, обов'язкових процедур сповіщення про інциденти з визначеними строками і формою звітування, а також створення міжвідомчих оперативних центрів, здатних оркеструвати одночасні заходи реагування і приймати стратегічні рішення щодо пріоритезації відновлення послуг. Міжнародні рекомендації щодо кіберкризового менеджменту підкреслюють необхідність регулярних спільних навчань команд реагування на кіберінциденти, правоохоронних органів і операторів критичної інфраструктури/телекомунікацій для підвищення оперативної сумісності [134].

Крім того, ефективність політики цифрової безпеки значною мірою залежить від інвестицій у кадровий потенціал і процедури управління знаннями: створення резервних команд, програми підготовки й ротації персоналу, сертифікаційні програми для фахівців держсектора, а також механізми залучення академічних і науково-дослідних інститутів до розробки методів моніторингу загроз і проведення аналізу інцидентів. Довгостроково це також означає розробку національних стандартів DevSecOps (інтеграція безпеки в життєвий цикл розробки та експлуатації програмного забезпечення), SBOM (програмна відомість компонентів) і політик управління ланцюгами постачання для зменшення ризиків від залежностей.

Реалізація цих чотирьох блоків заходів має супроводжуватись системою моніторингу і звітності (ключові показники ефективності, періодичні аудит-огляди, механізми незалежного нагляду) та планом фінансування, який забезпечить сталість ініціатив навіть поза межами кризових періодів. Відсутність таких

інструментів може призвести до фрагментарного впровадження змін і втрати колективних вигод від побудови кіберстійкої державної архітектури. Міжнародні аналітичні та політичні документи рекомендують «цілісні» підходи до управління кіберстійкістю, які поєднують технічні, організаційні й правові елементи в єдину систему політики.

На прикладній площині пріоритетні заходи включають: розгортання адаптивних процедур і алгоритмів, які дозволяють переводити частину адміністративних процесів у офлайн-режим або в дзеркальні точки доступу при втраті головних цифрових каналів; підвищення кібергігієни серед персоналу держустанов через регулярні тренінги та «червоні команди» для тестування вразливостей; запровадження прозорих комунікацій із громадянами під час інцидентів (щоб мінімізувати паніку й дезінформацію); а також інвестування в локальні центри підтримки вразливих груп (щоб гарантувати доступ у разі відсутності приватних гаджетів або Інтернету). Не менш важливою є міжнародна кооперація: обмін досвідом, технологічна допомога, спільні проєкти з відновлення й підвищення стійкості електронних послуг.

Проведений аналіз дає підстави зазначити, що війна значно підвищила як кількість, так і складність загроз для інформаційної безпеки електронних публічних послуг, виявивши технічні, організаційні та правові вразливості системи публічного управління. Відповідь має бути комплексною і заснованою на принципах стійкості, мінімізації шкоди правам людини та прозорості. Це означає не лише модернізацію технічної інфраструктури, а й реформу управлінських практик – від координації між відомствами до юридичних гарантій і залучення громадянського суспільства – аби електронні послуги залишалися доступними, безпечними й підзвітними навіть у найскладніших кризових умовах.

Систематизовані наукові підходи до механізмів публічного управління інформаційною безпекою надання електронних послуг. Виокремлено п’ять підходів, зокрема:

- техніко-адміністративний підхід орієнтований на формалізацію регулятивної бази, застосування міжнародних і національних стандартів (ISO/IEC

27001, NIST Рамки кібербезпеки), розвиток систем управління інформаційною безпекою (ISMS), а також впровадження інструментів контролю, аудиту, сертифікації та процедур комплаєнсу. Він забезпечує уніфікацію практик захисту даних, закріплення ролей і відповідальностей, а також підвищує підзвітність органів влади у сфері надання е-послуг;

– соціально-технічний підхід зосереджує увагу на тому, що інформаційна безпека є властивістю не лише технологій, а й соціально організованих практик. Тут наголос робиться на взаємодії користувачів і технологій, ролі організаційних культур, поведінкових моделей, міжвідомчої координації. Саме цей підхід підкреслює значення «людського фактора» та необхідність розвитку цифрової грамотності, довіри та прозорості у відносинах між державою й громадянами;

– управлінсько-організаційний підхід інтерпретує механізми інформаційної безпеки через призму управлінських систем, процедур стратегічного планування, ризик-менеджменту та циклічного вдосконалення (модель PDCA). Він демонструє, що ефективність публічного управління визначається не лише наявністю технологічних засобів, а й здатністю органів влади забезпечувати узгодженість політик, стратегічне прогнозування та координацію дій на різних рівнях;

– міжнародно-порівняльний підхід базується на аналізі практик різних країн і міжнародних організацій, що дозволяє адаптувати та трансформувати перевірені інструменти до національних умов. У цьому контексті особливого значення набувають питання кіберстійкості, стандартизації, транснаціональної співпраці та розбудови дослідницьких мереж, які забезпечують сталість політик у глобальному цифровому середовищі;

– бібліометричний та наукометричний підхід забезпечує виявлення ключових трендів розвитку науки: інтеграцію штучного інтелекту для моніторингу загроз, міждисциплінарність досліджень, зростання ролі питань довіри та соціальної легітимності. Цей підхід допомагає зрозуміти, які напрями є домінуючими у світовій науковій думці, а які – залишаються недостатньо дослідженими.

Систематизація підходів показує, що механізми публічного управління інформаційною безпекою електронних послуг слід розглядати як інтегровану систему, що поєднує правові, технічні, організаційні та соціальні виміри. Висновком є те, що жоден із підходів не може вичерпно забезпечити ефективність управління окремо: лише їх поєднання формує умови для комплексного захисту, підвищення довіри громадян, сталості цифрової інфраструктури та посилення легітимності держави в умовах цифрової трансформації.

Проаналізований понятійно-категоріальний апарат дослідження механізмів публічного управління інформаційною безпекою надання електронних послуг. Зазначено, що понятійно-категоріальний апарат дослідження механізмів публічного управління інформаційною безпекою надання електронних послуг формується на перетині кількох наукових площин – адміністративно-правової, інформаційно-технологічної, соціально-технічної та управлінсько-організаційної. У науковому дискурсі чітко простежується тенденція до інтеграції технічних категорій, що описують засоби захисту (криптографію, автентифікацію, контроль доступу, моніторинг), з управлінськими та правовими категоріями (політикою безпеки, регулюванням, підзвітністю, відповідальністю, інституційною координацією). Саме ця інтеграція створює змістовне поле для аналізу механізмів публічного управління.

Ключове поняття «механізми публічного управління» у цьому контексті відображає сукупність інструментів, процедур і практик, які забезпечують вплив держави на процеси гарантування безпеки в електронних послугах. До таких механізмів належать: нормативно-правові (закони, регламенти, стандарти), організаційні (централізовані агентства, центри реагування на інциденти – CSIRT/CERT, служби внутрішнього контролю), інструментально-технологічні (системи управління інформаційною безпекою, автоматизовані засоби виявлення загроз, аудиторські платформи) та соціально-комунікативні (програми навчання, підвищення обізнаності, поведінкові інтервенції).

У понятійному апараті центральним є термін «інформаційна безпека», який у сучасних дослідженнях розглядається не лише як технічна категорія (захист

конфіденційності, цілісності та доступності даних), але і як соціально-технічне явище, що включає взаємодію технологій із поведінкою користувачів, організаційними культурами, управлінськими моделями та нормативними регуляціями. Це дозволяє виокремлювати соціально-технічний підхід, у якому інформаційна безпека є властивістю системи, що виникає через баланс між технологічними механізмами, управлінськими рішеннями та соціальними практиками.

Категорія «електронні послуги» у межах дослідження має подвійний зміст: з одного боку, це інструмент цифрової трансформації публічного сектора, а з іншого – вразлива інфраструктура, що потребує особливих заходів управління ризиками, захисту персональних даних та забезпечення довіри користувачів. Це означає, що понятійний апарат неможливо будувати без урахування категорій «довіра», «надійність», «стійкість» і «сталість», що набувають особливого значення в умовах цифровізації державного управління.

Понятійно-категоріальний апарат дослідження включає базові категорії («публічне управління», «інформаційна безпека», «електронні послуги») та похідні, що описують механізми їх взаємодії («система управління інформаційною безпекою», «механізми регуляторного впливу», «соціально-технічні практики», «кіберстійкість», «постачальницька безпека»). Його особливість полягає в міждисциплінарності: він поєднує правові, організаційні, технічні та соціальні концепти, створюючи цілісну методологічну основу для аналізу та вдосконалення механізмів публічного управління.

Обґрунтоване авторське трактування поняття «механізми публічного управління інформаційною безпекою надання електронних послуг». Механізми публічного управління інформаційною безпекою надання електронних послуг доцільно визначити як 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. Таке авторське визначення акцентує увагу на кількох ключових аспектах: нормативно-правовий компонент – закони, стандарти та регламенти, що створюють обов'язкові правила гри для суб'єктів, які надають або користуються е-послугами; організаційно-інституційний компонент – система органів, установ і підрозділів (центри реагування на інциденти, служби захисту інформації, контролюючі інститути), які забезпечують координацію та підзвітність; технологічний компонент – застосування інформаційно-комунікаційних технологій і методів (системи управління інформаційною безпекою, криптографія, аудит, автоматизовані засоби моніторингу та виявлення загроз); соціально-комунікативний компонент – підвищення обізнаності користувачів, формування культури безпеки, розвиток довіри до державних цифрових сервісів. Узгодженість цих складових відображає комплексність управління: воно не обмежується технічними чи правовими заходами, а передбачає інтегровану взаємодію різних рівнів управління і суспільних практик. Саме така багатовимірність дозволяє говорити про механізми як про системоутворюючий чинник, що забезпечує не лише функціональну безпеку електронних послуг, але й стабільність цифрової взаємодії між державою та громадянами.

Здійснена систематизація проблем 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.

Матеріали цього розділу оприлюднені в таких публікаціях автора: [43; 44; 49].

РОЗДІЛ 2. КРАЩІ СВІТОВІ ПРАКТИКИ ПУБЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НАДАННЯ ЕЛЕКТРОННИХ ПОСЛУГ

2.1. Аналітична оцінка стану публічного управління інформаційною безпекою електронних послуг у країнах ЄС

За останні десятиліття інформаційні технології стали невід'ємною частиною багатьох аспектів соціально-економічного та суспільно-політичного життя держави, зокрема набули суттєвого розвитку інформаційні системи та цифрові процеси у сфері надання електронних послуг, як базові запити населення при реалізації функції публічного управління. Зростання обсягів використання електронних сервісів населенням призвело до необхідності забезпечення високого рівня захисту інформації, що передається та зберігається в цифровому форматі. Інформаційний захист процесів надання електронних послуг став однією з найбільш актуальних проблем у контексті надання електронних послуг, систем Е-урядування.

За останнє десятиліття цифрова трансформація публічного управління перейшла від класичного «електронного урядування», орієнтованого на онлайн-послуги, до сучасного «цифрового уряду» із глибокими змінами інституцій, процесів і взаємодії держави з суспільством. Міжнародні рейтинги свідчать про постійний прогрес: за даними ООН за 2024 рік, показники розвитку цифрового уряду стабільно зростають. Світовими лідерами залишаються Данія, Естонія та Сінгапур, які впроваджують підхід «digital-by-default», системно орієнтуються на потреби користувачів та інвестують у довіру до цифрової інфраструктури.

«Індекс цифрового урядування ОЕСР» (DGI, 2023) переконливо свідчить: найуспішніші країни забезпечують прорив у цифровому урядуванні завдяки синхронному розвитку шести взаємозалежних напрямів — від «цифрового проєктування» й «керування на основі даних» до «уряду як платформи», «відкритості за замовчуванням», «орієнтації на користувача» та «проактивного підходу». Ця стратегія змінює логіку розвитку: замість окремих ІТ-інструментів

формуються цілісні екосистеми та платформи, де держава виступає координатором спільних цифрових сервісів і ключової інфраструктури для всієї системи публічного управління.

Ключовими структурними «несучими балками» цифрових послуг у світі стали інтероперабельність і цифрова ідентичність. В ЄС у 2024 році набули чинності два системоутворюючі акти: Акт про взаємосумісну Європу, що створює «мережу мереж» взаємопов'язаних адміністрацій для безперервних транскордонних сервісів, та оновлений Регламент eIDAS 2024/1183, який започаткував Європейський цифровий гаманець ідентичності з обов'язком держав забезпечити доступність гаманця та взаємне визнання електронної ідентифікації [129]. Це формує єдину інфраструктуру довіри для електронних послуг на європейському просторі.

Розглянемо досвід зарубіжних країн більш детально.

Питання інформаційної безпеки електронних публічних послуг у Німеччині має складний і багатовимірний характер, поєднуючи технічні, організаційні та правові аспекти. Ефективне публічне управління у цій сфері визначається якістю нормативної бази, діяльністю компетентних органів, рівнем впровадження технічних стандартів, а також здатністю системи реагувати на інциденти за умов федеративного устрою та інтеграції з європейським правовим простором.

Законодавча основа захисту цифрових державних сервісів в Німеччині спирається на Закон про IT-безпеку (IT-Sicherheitsgesetz, зокрема редакцію 2.0), що значно посилив вимоги до операторів критичної інфраструктури, розширив сферу їх відповідальності та надав Федеральному відомству з безпеки інформаційних технологій (BSI) додаткові повноваження щодо контролю, нагляду та реагування [119]. Паралельно активно застосовуються стандарти «базового IT захисту», які є методологічною базою для побудови систем управління інформаційною безпекою в органах влади та відповідають вимогам міжнародних стандартів ISO/IEC 27001. Регулятивний вимір доповнюється впливом норм Європейського Союзу, зокрема директиви NIS/NIS2, Регламенту про кібербезпеку та eIDAS, що задають рамкові умови для кіберзахисту і сертифікації рішень [155].

Центральним органом у системі публічного управління інформаційною безпекою виступає Федеральне відомство з безпеки інформаційних технологій (BSI) [242], яке виконує функції розробки стандартів, реагування на інциденти через Команду реагування на комп'ютерні надзвичайні ситуації федерального рівня (CERT-Bund), консультування державних органів та бізнесу, а також реалізує контрольні функції. Водночас у федеративній системі важливу роль відіграють Рада з планування IT (IT-Planungsrat) і Федеральна IT-кооперація (FITKO), що забезпечують координацію цифровізації між федеральним і земельним рівнями. Проте саме федералізм створює ризик фрагментації: неоднорідність ресурсів і рівень цифрової зрілості між землями та муніципалітетами ускладнює уніфікацію стандартів безпеки.

Розвиток електронних адміністративних послуг у рамках Закону про онлайн-доступ (OZG) передбачає забезпечення цифрового доступу до всіх ключових державних сервісів, проте процес реалізації зустрів значні труднощі. Федеральна контрольна палата неодноразово критикувала повільні темпи, високі витрати та залежність від зовнішніх консультантів, а також відсутність системності у впровадженні. Масове розгортання електронних сервісів збільшило поверхню атаки, що підвищило значення уніфікованих процедур аутентифікації, шифрування, інтеграції з IT-Grundschutz та впровадження систем управління інформаційною безпекою [120; 145].

На європейському рівні ключовим викликом залишається транспозиція Директиви NIS2 (Директива Європейського Союзу про безпеку мереж та інформаційних систем 2-го покоління) [126], яка істотно розширює перелік організацій, зобов'язаних забезпечувати кіберзахист, та вводить більш жорсткі вимоги до звітності. У Німеччині процес адаптації цих норм відбувається повільно, що викликало критику і створює стан правової невизначеності для багатьох установ і підприємств.

Сильними сторонами німецької моделі є наявність технічного центру компетенцій у вигляді Федерального відомства з безпеки інформаційних технологій, стандартизована методологічна основа базової безпеки, розвиток

механізмів реагування (німецька державна команда реагування на комп'ютерні надзвичайні ситуації, Служба попередження та інформації) і тісна інтеграція з європейськими ініціативами у сфері кібербезпеки. Водночас слабкі місця проявляються у фрагментації системи через федералізм, затримках у впровадженні Директиви Європейського Союзу про безпеку мереж та інформаційних систем, неефективному адмініструванні проєктів цифровізації за Законом про онлайн-доступ та кадрових і фінансових обмеженнях на місцевому рівні.

Таким чином, стан публічного управління інформаційною безпекою цифрових послуг у Німеччині можна оцінити як відносно стабільний і заснований на потужній нормативно-технічній базі, проте з істотними операційними прогалинами. Подальше вдосконалення системи потребує централізації й обов’язкової уніфікації стандартів на всіх рівнях влади, розвитку спільних сервісних центрів кіберзахисту для муніципалітетів, прискореного та прозорого впровадження європейських норм, а також створення умов для зменшення залежності від зовнішніх постачальників і консультантів. Це дозволить посилити цілісність та стійкість системи та забезпечити належний рівень довіри громадян до цифрових публічних послуг.

Естонія є одним зі світових лідерів у сфері цифровізації державного управління, зокрема в аспекті забезпечення інформаційної безпеки електронних послуг. З моменту здобуття незалежності в 1991 році країна активно впроваджувала інноваційні технології для оптимізації публічних сервісів, забезпечення прозорості та підвищення довіри громадян до державних інституцій.

Естонська модель публічного управління інформаційною безпекою електронних послуг вирізняється високим рівнем інтеграції технічних рішень, нормативно-інституційної координації та орієнтацією на міжсекторну інтероперабельність; ключовим координуючим органом є Управління державних інформаційних систем, яке відповідає за адміністрування реєстрів державних інформаційних систем, організацію діяльності з інформаційної безпеки та координацію реагування на інциденти [197].

Законодавча та політико-адміністративна рамка має чітку базову структуру: основні правові вимоги щодо безпеки мереж і інформаційних систем закріплені в Законі про кібербезпеку [117], який встановлює обов'язки для власників і операторів критичних систем, механізми звітування про інциденти та визначає роль Управління державних інформаційних систем як координатора превентивних та реактивних заходів; паралельно застосовуються спеціальні регламенти і публічні акти щодо управління даними та прозорості (зокрема норми, пов'язані з адмініструванням реєстру RIHA) [117]. Така нормативна конструкція поєднує імперативні вимоги з гнучкими інструментами адміністрування, що дозволяє поєднувати централізований нагляд і децентралізовану реалізацію сервісів.

Технічний каркас естонського цифрового простору базується на декількох «опорних» рішеннях, з яких центральне місце займає шина обміну даними X-tee (X-Road / X-tee) [241] – захищений шар обміну даними між інформаційними системами, що забезпечує автентифікацію, підписи, шифрування й логування транзакцій, дозволяючи уникати централізованого накопичення даних і водночас забезпечувати їх доступність для легітимних запитів; X-tee реалізовано як відкритий проєкт і використовується як на національному, так і на міжнародному рівні. Одночасно держава підтримує централізований реєстр державних інформаційних систем RIHA, який є обов'язковим для органів влади та забезпечує прозорість відповідальностей, джерел даних та сумісних артефактів [241].

Система електронної ідентифікації та довіри є ще одним стрижнем: державний портал eesti.ee виступає єдиним «вікном» для користувача, а програми цифрової ідентифікації (електронні ID-картки, Mobile-ID, програма e-Residency) забезпечують юридично значущу аутентифікацію й електронні підписи, що дозволяє побудувати повноцінний юридично вагомий цифровий сервісний ланцюг. Водночас естонський досвід показує, що навіть у високотехнологічному середовищі ідентифікація потребує постійного аудиту: на прикладі вразливості ROCA (2017) стосовно криптографічних чіпів ID-карт держава оперативно запроваджувала заходи з оновлення сертифікатів та механізми відновлення довіри до системи. Така динаміка демонструє, що інноваційна ідентифікація підвищує

масштаб і швидкість послуг, але створює й додаткові вимоги до управління життєвим циклом криптографічних засобів та процедур реагування [199; 214].

Щодо гарантування цілісності даних і перевірки змін в Естонії практично впроваджено технологію KSI (Інфраструктура безключового підпису) – розподілену інфраструктуру підписів без ключа, яка дозволяє створювати недвозначні докази цілісності записів у державних реєстрах і тим самим знижує ризик невідворотних змін у масивах даних. Використання KSI підсилює довіру до державних реєстрів і дозволяє нівелювати частину ризиків, пов'язаних із компрометацією окремих компонентів [113].

Управлінська модель поєднує централізовану координацію (Управління державних інформаційних систем як національний координаційний центр кібербезпеки, який також виконує функції CSIRT / Національного центру кібербезпеки) і механізми розподіленого впровадження на рівні міністерств та місцевих органів; сучасна стратегія держави (стратегія кібербезпеки 2024–2030 «Кіберсвідома Естонія») підкреслює необхідність збереження високого рівня довіри до цифрових сервісів, стійкості до кризових сценаріїв та посилення нормативно-правової бази в умовах загроз зростаючого геополітичного тиску. Ця стратегія також акцентує увагу на міжвідомчій координації, розвитку людського капіталу та посиленому захисті критичних систем [197].

Практична імплементація демонструє сильні сторони, які роблять естонську модель релевантною для порівняльного дослідження: високий ступінь сумісності сервісної архітектури (X-tee, RIHA), розвинена інституційна координація (Управління державних інформаційних систем як центральний орган), технологічні інновації (KSI, e-ID, e-Residency) і прозорість адміністрування послуг через єдиний портал eesti.ee. У поєднанні це створює відносно високу швидкість цифрових трансакцій і корисну «економіку довіри», що спрощує як внутрішні, так і зовнішні (міжнародні) інтеграційні ініціативи [214; 241].

Водночас існують системні ризики й операційні обмеження. По-перше, концентрація функцій у невеликому технологічно інтегрованому просторі підвищує значення управління ланцюгом постачання програмного забезпечення і

апаратного компонента – уразливості апаратних чи криптографічних компонентів (як у випадку ROCA) можуть мати масовий ефект; по-друге, естонський цифровий простір є мішенню геополітичних і гібридних загроз, що вимагає поєднання технічних засобів і політико-адміністративних інструментів реагування; по-третє, швидке впровадження інновацій створює потребу в постійному оновленні норм і процедур, включно з підвищенням кваліфікації кадрів у сфері кібербезпеки. Аналіз щорічних звітів Управління державних інформаційних систем вказує на зростання кількості інцидентів і на те, що більшість із них мають соціально-інженерну або фішингову природу, що підкреслює значення превентивних заходів і цифрової гігієни громадян та бізнесу [197].

Отже, досвід Естонії переконливо демонструє, що ефективне публічне управління інформаційною безпекою електронних послуг можливе лише за умови поєднання інноваційних технічних рішень, чіткої правової бази та постійної інституційної адаптації. Системи на кшталт X-tee та RIHA, платформи електронної ідентифікації та програма e-Residency не лише забезпечили високу операційну ефективність, а й сформували унікальний «капітал довіри» громадян до держави, що є стратегічним ресурсом у цифрову добу. Проте ключовим чинником стійкості є не самі технології, а наявність циклічного управлінського процесу, який включає регулярне оновлення законодавства, стратегічні інвестиції у людський капітал, аудит криптографічних рішень і контроль за якістю постачань.

Для України, яка активно рухається шляхом цифровізації державного управління (зокрема через розвиток порталу «Дія» та законодавчі ініціативи у сфері кібербезпеки), естонський досвід є надзвичайно цінним. По-перше, адаптація моделі X-tee дозволила б знизити фрагментарність інформаційних систем і забезпечити прозорий та захищений обмін даними між відомствами, що є критично важливим в умовах воєнних загроз. По-друге, розвиток єдиної системи електронної ідентифікації з високим рівнем юридичної значущості підписів і транзакцій міг би суттєво зміцнити правову основу цифрових послуг. По-третє, створення спеціалізованих міжвідомчих центрів компетенцій з кібербезпеки сприяло б підвищенню здатності до оперативного реагування на загрози. По-четверте,

інституціоналізація програм кіберобізнаності населення та бізнесу могла б знизити вразливість до соціально-інженерних атак, які, за досвідом Естонії, залишаються найбільш поширеним каналом атак.

Таким чином, імплементація естонських практик в Україні є доцільною та можливою за умови їх адаптації до національного контексту: інтеграції в існуючу архітектуру цифрових послуг, врахування особливостей правової системи та воєнного стану, а також належного фінансування й інституційної підтримки. Використання цих підходів може не лише посилити інформаційну безпеку українських електронних сервісів, але й забезпечити підвищення довіри громадян до держави, що в умовах війни та відбудови матиме стратегічне значення.

Данська модель публічного управління інформаційною безпекою електронних послуг поєднує високий ступінь централізованої координації з розвиненими міжвідомчими та секторними механізмами відповідальності; ключовими інституціями виступають Центр кібербезпеки як національний орган з питань ІТ-безпеки та Урядова команда реагування на комп'ютерні інциденти, Агентство цифрового уряду, що адмініструє критичну цифрову інфраструктуру публічного сектора, а також Данський орган із захисту даних та поліцейські спеціалізовані підрозділи (зокрема, Національний центр боротьби з кіберзлочинністю – NC3); така інституційна архітектура забезпечує розподіл ролей між захисною аналітикою, операційним адмініструванням сервісів та наглядом за захистом персональних даних [104; 217; 218].

Нормативно-правова база формує мультисекторальний підхід: замість єдиного «кіберзаконодавства» у Данії діє сукупність спеціалізованих актів і регламентів, що охоплюють управління інформаційною безпекою, захист даних, логування телекомунікацій, а також спеціальні акти щодо функціонування Центру кібербезпеки; водночас національні стратегії з кібер- та інформаційної безпеки (напр., стратегія 2022–2024) встановлюють пріоритети щодо захисту критичних функцій, посилення міжвідомчої координації та підвищення кіберстійкості. Така закономірність – поєднання законодавчої «ширини» із стратегічним плануванням

– дозволяє гарантувати гнучкість регулювання, але водночас потребує ефективного механізму координації для уникнення розпорошення відповідальності [219].

Технічна інфраструктура державних сервісів витримана за принципами централізованих сервісів з розподіленою відповідальністю: національна система ідентифікації MitID (національне електронне посвідчення особи Данії) замінила NemID та встановила сучасні вимоги до аутентифікації та кваліфікованих електронних підписів [168]; Цифрова пошта [125] як обов'язкова національна цифрова поштова служба забезпечує захищену двосторонню комунікацію між державою й громадянами; інші сервіси (реєстри, NemKonto (Національний реєстр рахунків Данії) тощо) інтегровані в єдину екосистему публічних сервісів, адміністровану Агентством цифрового уряду [178]. Комбінація централізованих «спільних послуг» і єдиного набору операційних стандартів підвищує стійкість систем, скорочує поверхню атак для окремих департаментів і сприяє уніфікованому управлінню інцидентами.

Оперативні механізми реагування і ситуаційної обізнаності в Данії зорієнтовані на інтеграцію розвідки, оборони та правоохоронних інструментів: Центр кібербезпеки [104] здійснює нагляд за національним кібер-ландшафтом, координує діяльність Урядової команди реагування на комп'ютерні інциденти [110], підтримує 24/7 ситуаційну картину та координує обмін інформацією зі структурою ЄС; паралельно Національний центр з кіберзлочинності (NC3) та Національна спеціальна одиниця поліції відповідають за розслідування кіберзлочинів і кримінально-оперативні дії. Така розбудова дозволяє поєднати превентивний моніторинг і оперативне розслідування, але вимагає чіткої регламентації обміну розвідувальними даними та ролей у кризових сценаріях.

Підхід до регулювання критичних секторів спирається на принцип секторної відповідальності: держава формує загальні норми та забезпечує координацію, але секторні регулятори (енергетика, фінанси, телекомунікації) зберігають вертикальну відповідальність за виконання технічних вимог і нагляд; такий принцип сприяє адаптації вимог до галузевої специфіки, але ускладнює уніфікацію порядків у міжсекторних ланцюгах постачання та сервісної взаємодії [122].

У плані загроз і пріоритетів Центр кібербезпеки та національні стратегії фіксують ключові виклики: посилення кібершпигунства та розвідувальної активності іноземних держав, підвищений рівень соціально-інженерних атак і фішингу, а також ризики від постачальницьких ланцюгів і апаратно-програмних вразливостей; у зв'язку з цим держава акцентує інвестиції в ситуаційну обізнаність, освоєння можливостей обміну розвідувальними даними та підвищення стійкості критичних сервісів [219].

Практична реалізація цифрових послуг у Данії демонструє сильні сторони: високий рівень використання електронної ідентифікації серед населення, зрілість централізованих сервісів (MitID, Цифрова пошта, NemKonto), інтегровані моделі управління ризиками на рівні держави та секторів, а також розвинені можливості міжвідомчого співробітництва. Водночас наявні слабкі місця: потреба у постійному оновленні нормативної бази (особливо в контексті Директиви (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року про заходи щодо забезпечення високого загального рівня кібербезпеки в Союзі [126]), виклики у транссекторальному управлінні ланцюгами постачання програмного забезпечення й апаратури, а також необхідність підтримувати оперативну взаємодію між оборонними, правоохоронними та цивільними структурами при одночасному захисті прав і свобод громадян.

Щодо імплементації ЄС-ініціатив стан транспозиції Директиви (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року про заходи щодо забезпечення високого загального рівня кібербезпеки в Данії знаходився під пильним наглядом Європейської Комісії (стан на 2025 рік включав офіційні запити до держави щодо повноти повідомлення заходів транспозиції), що підкреслює важливість своєчасного правового приведення національних механізмів у відповідність до європейських стандартів та чіткої ролі національних регуляторів у виконанні нових вимог звітування й нагляду. Така динаміка покликана підвищити правову передбачуваність і уніфікувати мінімальні стандарти захисту в усіх державах-членах.

На основі наведеного можна зробити такі висновки. По-перше, успіх Данії обумовлений інтегрованою архітектурою: централізовані «спільні послуги» для публічних процесів (MitID, Цифрова пошта), національний центр кібербезпеки з функціями Урядової команди реагування на комп'ютерні інциденти Данії та чіткий секторний нагляд; саме поєднання технічних платформ і політико-адміністративної координації забезпечує високу операційну ефективність і стійкість. По-друге, для підтримки цієї моделі критично важливі постійне оновлення правових норм (включно з адаптацією до Директиви (ЄС) 2022/2555), інвестиції в кадри й технологічну оновлюваність, а також механізми контролю за ланцюгами постачання і системами третіх сторін. По-третє, секторний принцип регулювання вимагає розвинених інструментів міжсекторної координації та протоколів обміну даними, що мають бути формалізовані і технічно забезпечені.

Досвід Данії у сфері публічного управління інформаційною безпекою електронних послуг може бути цінним орієнтиром для України, зважаючи на схожі виклики у сфері цифровізації, необхідність протидії гібридним загрозам і потребу у зростанні довіри громадян до державних цифрових сервісів. В основі данської моделі лежить інтегрований підхід: поєднання централізованих органів координації, спеціалізованих команд реагування на кіберінциденти, а також тісна співпраця між державними структурами, приватним сектором і науковими установами. Для України, яка вже має певні напрацювання в цій сфері, доцільним є вибудовування подібної багаторівневої системи. По-перше, ключовим елементом імплементації є адаптація моделі Центру з кібербезпеки Данії, що діє при Службі оборонної розвідки, до українських реалій. Йдеться не про копіювання інституційної архітектури, а про створення координаційного центру з широкими аналітичними, технічними та превентивними повноваженнями, який би поєднував діяльність сектора оборони, правоохоронних органів та цивільних інституцій. Це дозволило б мінімізувати дублювання функцій між наявними органами в Україні (наприклад, Держспецзв'язку, СБУ, Міністерством цифрової трансформації) та підвищити рівень узгодженості дій.

По-друге, досвід GovCERT Данії як урядової команди реагування на комп'ютерні інциденти можна використати для вдосконалення української CERT-UA. Зокрема, мова йде про впровадження більш розгалуженої системи взаємодії з відомчими CSIRT-структурами та розробку інституційного механізму обміну інформацією у режимі реального часу між державою та приватними провайдерами критичної інфраструктури. Данська практика демонструє, що оперативність і прозорість у реагуванні значно підвищують рівень довіри бізнесу до держави, що критично важливо й для України.

По-третє, варто врахувати досвід роботи NC3 – Національного центру з кіберзлочинності Данії, який діє у складі Національної поліції. Для України актуальною є інтеграція підрозділів кіберполіції в ширший контекст національної політики кібербезпеки із застосуванням інноваційних інструментів аналітики, кіберфорензіки та міжнародного співробітництва. Це особливо важливо з огляду на транснаціональний характер кіберзлочинності та потребу у гармонізації з європейськими стандартами (наприклад, відповідно до директиви ЄС NIS2).

По-четверте, важливого значення набуває данська практика формування єдиних стратегій цифрової стійкості, що охоплюють не лише державний сектор, а й критичну інфраструктуру, муніципалітети, освітні установи та бізнес. Для України доцільним буде формування комплексної «дорожньої карти» цифрової стійкості, яка інтегрувала б регіональний і місцевий рівні управління з центральним. У цьому контексті важливим є створення платформ для обміну знаннями та найкращими практиками, подібних до данських міжсекторальних ініціатив із кіберобізнаності.

По-п'яте, необхідно врахувати значення освітніх і просвітницьких програм. У Данії значна увага приділяється формуванню кіберкультури серед громадян, бізнесу та держслужбовців. Для України актуально інтегрувати подібні програми у систему підготовки кадрів державної служби, а також у шкільну та університетську освіту, створюючи підґрунтя для довгострокової цифрової стійкості.

Таким чином, імплементація данського досвіду в Україні можлива у кількох напрямах: створення потужного координаційного центру з кібербезпеки з

функціями стратегічного аналізу та оперативного реагування; посилення інституційної спроможності CERT-UA за моделлю GovCERT; інтеграція кіберполіції в єдину національну систему протидії загрозам; формування комплексної стратегії цифрової стійкості з урахуванням багаторівневої взаємодії держави, бізнесу і громадян; розвиток освітніх та комунікаційних програм для підвищення кіберобізнаності. Ці кроки дозволили б Україні не лише посилити захист електронних послуг, а й закласти фундамент для довгострокової довіри громадян до цифрової держави, що є стратегічним чинником у контексті євроінтеграції та відбудови після війни.

Ефективність публічного управління інформаційною безпекою електронних послуг у Литві зумовлена поєднанням правової модернізації, чіткої інституційної ролі ключових органів, масштабної інфраструктури електронної ідентифікації та централізованих сервісів для надання е-послуг. Литва має розгалужену екосистему е-урядування – національний портал «Електронні державні ворота» [130] забезпечує доступ до сотень електронних послуг, а частка користувачів і рівень проникнення цих сервісів відображають високу цифрову активність населення й державного апарату [135].

Головним національним координатором кібербезпеки є Національний центр кібербезпеки (NKSC), який функціонує в системі Міністерства національної оборони і виконує функції моніторингу, координації реагування на інциденти та контролю виконання вимог інформаційної безпеки. У рамках Національного центру кібербезпеки працює національна команда реагування на комп’ютерні інциденти (CERT-LT), що виступає єдиною точкою контакту для міжнародних CSIRT/CERT-структур і забезпечує оперативну роботу з інцидентами кібербезпеки. Така організаційна побудова забезпечує єдність політики та оперативний зв’язок між оборонними, цивільними й приватними акторами [182; 183].

Нормативно-правова база пройшла суттєве оновлення у зв’язку з імплементацією вимог ЄС: Закон Литовської Республіки «Про кібербезпеку» було актуалізовано та приведено у відповідність із директивою NIS2; відповідні зміни

набрали чинності у 2024 році, що підсилює вимоги до управління ризиками, звітування про інциденти, захисту ланцюгів постачань та повноважень наглядових органів [181]. Ця юридична трансформація створює підґрунтя для підвищення відповідальності суб'єктів, що надають критичні та важливі цифрові послуги.

Технічна та операційна інфраструктура державних сервісів базується на кількох ключових компонентах. По-перше, існує розвинена система електронної ідентифікації: державна ID-картка, рішення Mobile-ID [169] та комерційний Smart-ID [208] дають змогу надійно аутентифікувати користувачів і ставити юридично значущі електронні підписи, причому деякі з цих рішень були визнані відповідними до рівнів довіри згідно з Регламентом ЄС про електронну ідентифікацію та довірчі послуги [126; 193]. По-друге, Державне підприємство «Центр реєстрів» адмініструє ключові державні реєстри й надає сертифікаційні та технічні сервіси для роботи реєстрових систем – це створює централізований корпус реєстрів, на базі якого будуються багато електронних послуг. У сукупності такі технічні платформи дозволяють поєднувати зручність для користувача з високими вимогами до автентичності, цілісності і невідмовності транзакцій.

Організаційно-правова імплементація та практична експлуатація електронних послуг супроводжується запровадженням механізмів моніторингу ситуації в кіберпросторі, міжвідомчої координації та превентивного аналізу загроз. Національний центр кібербезпеки у взаємодії з міністерствами, секторними регуляторами та правоохоронними органами формує ситуаційну обізнаність держави; одночасно CERT-LT забезпечує технічну координацію, інформування та обмін індикаторами компрометації. Офіційні звіти і огляди підкреслюють активну роль державних структур у створенні 24/7-режиму спостереження та уніфікованих процедур реагування [170].

Аналіз загрозного середовища показує, що Литва, як і інші країни регіону, стикається з поєднанням державної розвідувальної активності, цілеспрямованих атак на критичну інфраструктуру, фішингових і соціально-інженерних кампаній, а також значними ризиками в ланцюгах постачання програмного й апаратного забезпечення. У своїх офіційних оглядах Міністерство національної оборони і

Національний центр кібербезпеки акцентують на необхідності підвищувати стійкість ланцюгів постачання, контролювати сторонні компоненти та розвивати можливості місцевої кіберфорензіки і оперативного аналізу загроз [183].

Сильні сторони литовської моделі випливають із синергії правової модернізації, інституційної координації та технологічних рішень: висока проникність е-послуг і систем ідентифікації сприяє довірі користувачів; централізовані реєстри і сертифікаційні сервіси забезпечують стандартизовану основу для побудови сервісів; оновлений законодавчий пакет (транспозиція NIS2) підвищує мінімальні вимоги до суб'єктів. Ці чинники роблять Литву одним із показових прикладів успішної інтеграції електронних послуг і національної кібербезпеки.

Водночас існують очевидні обмеження та ризики. По-перше, зростання кількості інцидентів і складність атак вимагають постійного нарощення людського капіталу та експертної спроможності (кібероперативні підрозділи, аналітика, форензика). По-друге, залежність від сторонніх постачальників і міжнародних постачальницьких ланцюгів створює системні вразливості, що потребують стандартних вимог до контролю постачань (SBOM, аудит постачальників, сертифікація допоміжних компонентів). По-третє, законодавчі та технічні ініціативи мають супроводжуватися практичними механізмами імплементації на рівні муніципалітетів і окремих операторів, інакше ризик фрагментації та нерівномірності захищеності залишається високим. Міністерські огляди прямо зазначають потребу в цілісному підході до управління ризиками й міжсекторної взаємодії.

Ефективність литовської моделі публічного управління інформаційною безпекою електронних послуг базується на трьох взаємопов'язаних елементах: централізованій координації кібербезпеки через Національний центр кібербезпеки при Міністерстві національної оборони, централізованій інфраструктурі реєстрів і сервісів, яку адмініструє Державне підприємство «Центр реєстрів», а також розвинутій системі електронної ідентифікації (державні ID-картки, Mobile-ID, Smart-ID) та національному порталі електронних послуг e-paslaugos.lt як «єдиному

вікні» доступу до державних сервісів. Усі ці компоненти формують екосистему, де нормативне регулювання, технічні платформи й операційні процедури діють узгоджено, що суттєво підвищує рівень довіри до цифрової взаємодії громадян із державою.

З огляду на цей досвід, для України першочерговим є створення національного координаційного осередку кібербезпеки з чітко визначеними повноваженнями. Литовський Національний центр кібербезпеки виконує функції моніторингу загроз, реагування на інциденти та контролю за дотриманням вимог безпеки, що дозволяє уникати розпорошення відповідальності. Україна могла б удосконалити або трансформувати наявні структури, зокрема Держспецзв'язку та відповідні підрозділи Мінцифри й СБУ, у координаційний центр із визначеним статусом та єдиним оперативним органом реагування CERT-UA, закріпленим у правовому полі. Це зменшило б міжвідомчі конфлікти й пришвидшило реагування на загрози.

Централізоване адміністрування державних реєстрів і надання послуг через «єдине вікно» також є сильним аспектом литовської моделі. Українська система «Дія» вже рухається у цьому напрямку, але потребує розширення технічних модулів безпеки, зокрема централізованого логування, системи виявлення аномалій та оперативного відключення скомпрометованих сервісів. Для підвищення довіри необхідно встановити єдині стандарти API, формати даних і процедури обов'язкових аудитів при підключенні нових сервісів до центральних реєстрів. При цьому слід враховувати ризики концентрації даних і застосовувати багаторівневе шифрування, сегментацію доступу та резервні копії в розподілених дата-центрах.

Литовський досвід із поєднанням державних і комерційних інструментів електронної ідентифікації має особливе значення. В Україні слід зберегти державну ID-картку як базовий стандарт юридично значущої ідентифікації, але водночас інтегрувати безпечні мобільні рішення на кшталт Smart-ID, сертифіковані відповідно до європейського регламенту eIDAS. Це підвищить доступність сервісів для громадян і бізнесу. Додатково варто створити механізми акредитації приватних

постачальників таких рішень, розробити процедури відновлення криптосертифікатів і швидкого відкликання ключів у разі виявлення вразливостей, що вже довело свою важливість у європейській практиці.

Ще однією складовою є адаптація українського законодавства до вимог Директиви ЄС NIS2, яка визначає обов'язки операторів критичної та важливої інфраструктури щодо управління ризиками та звітування про інциденти. Україні доцільно встановити чіткі вимоги до суб'єктів цифрової інфраструктури, запровадити контроль ланцюгів постачання програмного й апаратного забезпечення, включно з обов'язковим наданням списків компонентів (SBOM) у державних закупівлях, а також визначити механізми акредитації постачальників. Для малих і середніх компаній, які можуть відчувати складності з виконанням вимог, варто запровадити перехідні періоди та програми підтримки.

Управління ризиками в ланцюгах постачання має стати окремим напрямком політики. Українські державні органи могли б вимагати від постачальників програмних рішень надання SBOM та підтвердження аудиту безпеки. Це підвищить прозорість використаних технологій і зменшить ймовірність критичних уразливостей у ключових системах. Паралельно доцільно створити реєстр постачальників, що не відповідають вимогам безпеки, та розробити політику підтримки локальних альтернатив.

Литовська практика акцентує на важливості людського капіталу й освіти в сфері кібербезпеки. Україна може запровадити національну програму підготовки кадрів із сертифікацією та курсами для держслужбовців, включити кібергігієну до освітніх програм у школах і університетах, а також створити кадровий резерв для залучення фахівців під час кризових ситуацій. Це дозволить забезпечити сталість функціонування системи навіть в умовах зростання кіберзагроз.

Міжнародна співпраця з країнами Балтії та ЄС має стати ще одним напрямом імплементації досвіду Литви. Вона може забезпечити Україні оперативний обмін індикаторами загроз, участь у спільних навчаннях та поступову інтеграцію до стандартів eIDAS і NIS2. Двосторонні угоди та партнерство з НАТО дозволять посилити координацію й отримати додаткову технічну підтримку.

Запровадження цих заходів доцільно здійснювати поетапно. Спочатку слід провести правову діагностику та підписати меморандуми з балтійськими партнерами, далі реалізувати пілотні проєкти у сфері централізованих реєстрів, електронної ідентифікації та розширеного функціоналу CERT, а потім перейти до масштабування на рівні всієї країни. Для оцінки ефективності необхідно визначити ключові показники, зокрема час виявлення та реагування на інциденти, частку сервісів під централізованим аудитом, рівень поширеності електронної ідентифікації серед громадян, кількість проведених навчань та сертифікованих фахівців.

Очевидно, що впровадження литовських практик в Україні може дати значний ефект у сфері цифрової трансформації та кіберстійкості, однак потребує політичної волі, достатнього фінансування й узгодженості міжвідомчих дій. Головним викликом залишаються ризики концентрації даних та міжвідомчі суперечності, які можливо мінімізувати за рахунок чіткої законодавчої бази, прозорих правил координації та зовнішнього аудиту. Таким чином, поступове імплементування литовської моделі в Україні здатне суттєво підвищити рівень інформаційної безпеки електронних послуг, зміцнити довіру громадян до цифрових сервісів і забезпечити їхню стабільність навіть в умовах високих зовнішніх загроз.

Порівняльний аналіз досвіду публічного управління інформаційною безпекою електронних послуг в Німечині, Естонії, Данії та Литві (табл. 2.1).

Таблиця 2.1.

Узагальнення досвіду публічного управління інформаційною безпекою електронних послуг в Німечині, Естонії, Данії та Литві

Країна	*Ключові інституції*	*Нормативна база*	*Технічна інфраструктура*	*Сильні сторони*	*Виклики / обмеження*
Німе-ччина	Федеральне відомство з безпеки інформаційних технологій (BSI),	Закон про IT-безпеку (IT-Sicherheitsgesetz), імплементація	Централізовані стандарти кіберзахисту, система раннього	Системність регулювання, високий технічний рівень BSI,	Складність через федеративну структуру, бюрократичність процедур

	Федеральна команда реагування на інциденти (CERT-Bund), IT-Planungsrat, FITKO	NIS2, стандарти BSI	попередження, міжвідомча координація	інтеграція федеративного рівня	
Естонія	Міністерство економіки та комунікацій, Департамент інформаційних систем (RIA), X-tee, CERT-EE	Закон про кібербезпеку (оновлений), імплементація NIS2	X-tee (рівень обміну даними), RIHA (реєстр інформаційних систем), e-ID, e-Residency	Висока цифрова довіра, операційна ефективність, міжнародна інтеграція (NATO CCDCOE)	Залежність від сталого оновлення законодавства, потреба у контролі ланцюгів постачань
Данія	Центр з кібербезпеки (CFCS) при Службі оборонної розвідки (DDIS), урядова команда реагування (GovCERT), Національний центр з кіберзлочинності (NC3)	Національна стратегія кібербезпеки, імплементація NIS2, GDPR	GovCERT (національний CSIRT), інтеграція з військовою та поліційною розвідкою, платформи безпеки для держсектора	Високий рівень міжвідомчої координації, орієнтація на оперативне реагування, інтеграція кібер- та кримінальної безпеки	Ризик «мілітаризації» кіберполітики, залежність від оборонної структури
Литва	Національний центр кібербезпеки (NKSC) при Міноборони, CERT-LT, Державне підприємство «Центр реєстрів»	Закон про кібербезпеку, імплементація NIS2, GDPR	Електронна ідентифікація (ID-картка, Mobile-ID, Smart-ID), портал e-paslaugos.lt, централізовані державні реєстри	Єдине «вікно» е-послуг, поєднання державних і приватних рішень e-ID, сильна правова основа	Єдине «вікно» е-послуг, поєднання державних і приватних рішень e-ID, сильна правова основа

Ця таблиця демонструє, що всі чотири країни поєднують правові інструменти ЄС (імплементація Директиви NIS2, GDPR) із власними інституційними моделями, але акценти різні: Німеччина робить ставку на стандартизацію і федеративну координацію, Естонія – на технологічну інновацію та відкритість, Данія – на інтеграцію кіберзахисту з оборонною й поліцейською сферою, Литва – на централізацію е-сервісів та практичну імплементацію електронної ідентифікації.

2.2. Розвиток публічного управління інформаційною безпекою електронних послуг в азійських країнах

Розвиток публічного управління інформаційною безпекою електронних послуг у Сінгапурі представлений як цілісна державна політика, яка поєднує нормативно-правову базу, інституційний сегмент відповідальності, технічні платформи та операційну практику реагування на інциденти. У Сінгапурі цей комплекс формувався поступово впродовж останнього десятиліття в контексті національної ініціативи «Розумна нація» та цифрової трансформації уряду: водночас нарощувалися заходи захисту критичної інфраструктури, впроваджувалися механізми захисту персональних даних і створювалася інституційна спроможність до управління кіберризиками на національному рівні [209].

Ключовим законом, що задає рамки державного нагляду за кібербезпекою, є Закон про кібербезпеку, який встановлює правові підстави для ідентифікації та регулювання власників і операторів критичної інформаційної інфраструктури, запроваджує вимоги до повідомлення про інциденти та дає повноваження Агентству кібербезпеки Сінгапуру щодо контролю та нагляду. Закон та його поправки спрямовані на підвищення стійкості критичної інформаційної інфраструктури і забезпечення механізмів адміністративного реагування на загрози; останні оновлення відображали спроби адаптувати регуляцію до швидких технологічних змін (зокрема впливу ШІ і розподілених обчислень) [116; 118].

Паралельно з кіберзаконодавством Сінгапур має розвинуту систему захисту персональних даних – Закон про захист персональних даних, яку адмініструє Комісія з захисту персональних даних. Закон про захист персональних даних встановлює базові обов’язки організацій щодо збору, використання, зберігання та розкриття персональних даних, а Комісія з захисту персональних даних видає роз’яснювальні настанови та супроводжує практичну імплементацію принципів приватності у державному й приватному секторах. Для державних електронних

послуг це означає суміщення вимог інформаційної безпеки й захисту приватності на рівні проєктування послуг [100].

Координаційною віссю кібербезпеки є Агентство кібербезпеки Сінгапуру (CSA), яке поєднує функції нагляду, координації секторного захисту критичної інформаційної інфраструктури і операційного реагування через SingCERT – Службу реагування на кіберінциденти Сінгапуру. Агентство кібербезпеки Сінгапуру реалізує державні стратегії (зокрема «Стратегію кібербезпеки Сінгапуру 2021») [223], координує секторальні «секторні лідерства» для забезпечення безперервності критичних послуг і розвиває програму підвищення кіберстійкості організацій через нормативні вимоги та підтримку спроможностей. Одночасно Урядове технологічне агентство (GovTech) і Група «Розумна нація та цифровий уряд» відповідають за побудову й експлуатацію спільних цифрових платформ (наприклад, SingPass – національна система електронної ідентифікації) з вбудованими механізмами безпеки та управління доступом. Така функціональна розбивка – на національний регулятор (Агентство кібербезпеки Сінгапуру), оператора платформ (Урядове технологічне агентство та Група «Розумна нація та цифровий уряд») та орган державного нагляду за приватністю (Комісія з захисту персональних даних) – є однією з ознак системного підходу Сінгапуру [159].

У межах Плану цифрового уряду і ініціатив «Розумна Нація» уряд впроваджує спільні технічні стандарти, архітектури і платформи, які дозволяють уніфікувати механізми аутентифікації, керування ідентифікацією, логи й моніторинг безпеки. Централізовані сервіси (апі-шлюзи, сховища логів, послуги ідентифікації) спрощують управління ризиками й дозволяють застосовувати єдині засоби захисту та моніторингу для багатьох електронних послуг, водночас створюючи концентровані точки відповідальності за їхню безпеку (і, відповідно, потенційні вразливості, якщо захист не посилений) [123; 139].

У Сінгапурі поєднуються превентивні заходи (оцінка ризиків, аудит безпеки, вимоги до власників критичної інформаційної інфраструктури), навчальні програми й інвестиції у людський капітал, а також операційні механізми реагування: Службу реагування на кіберінциденти Сінгапуру координує збір й

аналіз індикаторів компрометації, оприлюднює попередження та вказівки для організацій, а Агентство кібербезпеки Сінгапуру веде моніторинг загроз і здійснює інспекційні заходи для визначених категорій критичної інформаційної інфраструктури. Учасники ринку і державні структури також працюють над створенням ринкової екосистеми кібербезпеки (стартапи, дослідження, програми сертифікації) [211; 212].

Сінгапурський підхід демонструє інтеграцію принципів «вбудована безпека у процесі проєктування» і «вбудована приватність у процесі проєктування»: при проєктуванні національної системи електронної ідентифікації та інших цифрових платформ одночасно застосовано технічні засоби захисту доступу, шифрування й журналювання, а також організаційні правила мінімізації даних та контролю доступу згідно з Законом про захист персональних даних [209]. Такий комплекс гарантує не лише технічну стійкість, а й правову відповідність обробки персональних даних.

Проведений аналіз дає підстави визначити такі основні виклики та обмеження публічного управління інформаційною безпекою електронних послуг в Сінгапурі:

– централізація платформ створює «одну точку відмови», тому вимоги до захищеності таких платформ є надзвичайно високими;

– швидкий розвиток технологій (ШІ, Інтернет речей, великі дані тощо) генерує нові загрози та породжує складні питання нормативного охоплення;

– баланс між ефективністю надання послуг і захистом приватності є динамічним і вимагає постійного перегляду політик та практик. Амбітність проєкту «Розумна Нація» також ставить завдання соціальної довіри – для збереження якої потрібна прозорість імплементації заходів безпеки та активна комунікація з громадянами.

Таким чином, Сінгапур демонструє системний, багаторівневий підхід до публічного управління інформаційною безпекою електронних послуг, що поєднує нормативні інструменти (Закон про кібербезпеку, Закон про захист персональних даних), інституційну координацію (Агентство кібербезпеки Сінгапуру, Службу

реагування на кіберінциденти Сінгапуру, Комісія з захисту персональних даних, Урядове технологічне агентство і Група «Розумна нація та цифровий уряд»), централізовані технічні платформи (національна система електронної ідентифікації та інші) і практики підвищення спроможності. Такий підхід забезпечує високу оперативну готовність і регуляторну ясність, але потребує постійного оновлення стандартів і механізмів контролю в умовах швидких технологічних змін. Для інших країн, що прагнуть підвищити кіберстійкість публічних електронних послуг, досвід Сінгапуру корисний як приклад інтеграції права, інституцій та платформи – однак його запозичення вимагає адаптації до національних інституційних особливостей, рівня довіри громадян і правових стандартів захисту приватності.

Імплементація досвіду Сінгапуру у сфері публічного управління інформаційною безпекою електронних послуг в Україні потребує поєднання правових, інституційних та технологічних рішень, адаптованих до національних умов. Передусім варто розглянути створення комплексної нормативно-правової бази, яка б системно регулювала як питання захисту критичної інформаційної інфраструктури, так і аспекти захисту персональних даних у межах надання електронних послуг. Прикладом може стати інтеграція положень Закону України «Про основні засади забезпечення кібербезпеки України» із спеціальним законом, що визначатиме категорії критичної інформаційної інфраструктури, встановлюватиме механізми обов’язкового повідомлення про кіберінциденти та закріплюватиме функції державного органу з нагляду та реагування. Такий підхід є аналогом моделі відповідно до Закону про кібербезпеку у Сінгапурі, яка забезпечила правову визначеність для операторів послуг і державних інституцій.

Окремо важливою є гармонізація регулювання приватності. Досвід Сінгапуру показує, що незалежний орган із захисту персональних даних може виступати каталізатором довіри до цифрових послуг. Для України доцільно посилити інституційну роль Уповноваженого Верховної Ради з прав людини у сфері захисту персональних даних або створити спеціалізовану комісію, яка б забезпечувала методичний супровід впровадження принципу «приватність за

задумом» у державних цифрових платформах. Це особливо актуально в умовах розвитку «Дії» та подальшого розширення функціоналу державних сервісів.

З інституційної точки зору Україна потребує централізованого координатора кібербезпеки електронних послуг. Агентство кібербезпеки Сінгапуру об'єднує функції політичного регулятора, наглядового органу і центру реагування. В Україні ці функції розподілені між Держспецзв'язку, Міністерством цифрової трансформації, Службою безпеки України та іншими суб'єктами. Доцільно було б розробити єдину модель координації, яка б включала операційний центр реагування на інциденти (аналог SingCERT), а також механізми взаємодії з приватним сектором та органами місцевого самоврядування.

На рівні технічної інфраструктури пропонується створення уніфікованих платформних сервісів для управління ідентифікацією та доступом, що відповідали б найвищим вимогам безпеки. Прикладом є сінгапурська система SingPass, яка забезпечує багатофакторну автентифікацію, централізований контроль доступу й інтеграцію до різних електронних послуг. В Україні розвиток «Дія.ID» може бути підсилений обов'язковими вимогами до криптографічного захисту, централізованим моніторингом аномалій доступу та інтеграцією з національними реєстрами за принципом «безпека за задумом».

Особливу увагу необхідно приділити розвитку людського капіталу та підвищенню обізнаності. У Сінгапурі кіберстійкість підкріплюється широкими програмами навчання та сертифікації кадрів, що працюють у сфері інформаційної безпеки. Для України потрібне масштабування освітніх програм у співпраці з університетами, ІТ-компаніями та державними органами з урахуванням стандартів НАТО та ЄС, що дозволить сформувати кадровий резерв для публічного сектора.

Ще одним важливим напрямом є стимулювання інновацій у сфері кібербезпеки через підтримку стартапів, проведення конкурсів рішень для захисту електронних послуг і формування національної екосистеми кіберпродуктів. Це дозволить поєднати державний попит на безпеку з приватною пропозицією новітніх технологій, як це зроблено у Сінгапурі в рамках державних програм «Розумна нація».

Водночас імплементація цього досвіду має враховувати українські реалії – зокрема воєнний контекст, високий рівень кібератак з боку держав-агресорів та обмеженість фінансових ресурсів. Тому доцільно запровадити поетапну модель: спершу посилення нормативної бази та інституційної координації, далі – впровадження централізованих технічних сервісів і, нарешті, розвиток ринку кібербезпеки та інноваційної екосистеми.

Загалом, використання досвіду Сінгапуру в Україні може суттєво підвищити довіру громадян до державних електронних послуг, зміцнити стійкість критичної інформаційної інфраструктури та закласти основи для інтеграції української системи кібербезпеки у європейський та глобальний безпековий простір.

Розвиток публічного управління інформаційною безпекою електронних послуг у Південній Кореї формувався як багатошарова державна політика, яка інтегрує всеосяжне законодавство з питань захисту персональних даних і безпеки мереж, інституційний поділ функцій регулювання та реагування, централізовані технічні платформи для автентифікації й обміну даними та активну взаємодію з приватним сектором і міжнародними партнерами. Цей підхід задекларований у національній стратегії кібербезпеки та матеріалізується через операційні підрозділи державних агентств і програмні ініціативи цифрового уряду [160; 173].

Нормативно-правова база в Південній Кореї складається з кількох взаємодоповнюючих елементів. Основним актом у сфері захисту персональних даних є Закон про захист персональної інформації (PIPA) [188], який створює загальні правила обробки персональних даних, принципи законності, мінімізації даних, вимоги до згоди та жорсткі санкції за порушення; великий пакет поправок до Закону про захист персональної інформації набув чинності в 2023 році і посилив регуляторні вимоги. Паралельно діє Закон про сприяння використанню інформаційно-комунікаційних мереж та захист інформації [98], який регулює використання мереж зв’язку й забезпечення інформаційної безпеки при наданні послуг через телекомунікаційні мережі. Разом ці акти створюють правову архітектуру, в якій поєднуються вимоги до технічного захисту мереж, зобов’язання

щодо повідомлення про інциденти і гарантії приватності для користувачів електронних послуг.

Інституційна архітектура зорієнтована на чіткий поділ ролей між регулятором приватності, національним координатором кібербезпеки та операційними центрами реагування. Ключовим гравцем є Корейське агентство інтернету та безпеки (KISA) [160; 161], яке виконує широкий спектр функцій: технічний нагляд, розроблення стандартів, операційне реагування через Координаційний центр реагування на комп'ютерні інциденти (KrCERT/CC), підтримку сертифікацій і міжнародну координацію. Регулятор із питань персональних даних представлений Комісією з питань захисту персональної інформації (PIPC), а політику в галузі науки і цифрових технологій формує Міністерство науки та інформаційно-комунікаційних технологій (MSIT) [172]. Одночасно у сфері внутрішньої безпеки та аварійного управління залучене Міністерство внутрішніх справ і безпеки (MOIS). Така багатовимірна модель дозволяє поєднати нормативний контроль, технічну експертизу і оперативні можливості.

Технічні платформи та практики проєктування цифрових сервісів у Республіці Корея спрямовані на поєднання зручності для користувачів і високих стандартів безпеки. Уряд реалізував масштабні програми мобільної цифрової ідентифікації, що надають громадянам еквівалентні фізичній ідентифікаційній картці цифрові документи, прийняті як юридично значущі для доступу до державних та банківських послуг; водночас уряд впроваджує політику мульти-автентифікації («Any-ID»), яка дозволяє користувачам використовувати різні способи аутентифікації (включно з приватними мобільними сервісами, наприклад PASS) для доступу до урядових сервісів, що підвищує інтероперабельність платформи та зручність користування. Крім того, уряд розвиває єдині портали (наприклад, gov.kr) і плани цифрового уряду (Генеральний план цифрового урядування), де принципи «безпека за задумом» та «захист приватності за задумом» інтегровані в архітектуру сервісів [124; 143; 204].

Операційні практики включають обов’язкові механізми повідомлення про інциденти, роботу національного Координаційного центру реагування на комп'ютерні інциденти (KrCERT/CC) у складі Корейського агентства Інтернету та безпеки, програмні ініціативи з підвищення кіберстійкості критичної інформаційної інфраструктури та секторальні заходи захисту. Корейське агентство Інтернету та безпеки також реалізує програми сертифікації безпеки пристроїв Інтернету речей та інші стандарти, які покликані зменшити ризики в екосистемі підключених пристроїв, що має прямий вплив на безпеку електронних послуг. Секторні гравці (банківський сектор, енергетика, телекомунікація) координують з Корейським агентством Інтернету та безпеки і відповідними органами спільні заходи з аналізу загроз, навчання та кібервправи [161; 173].

У політично-стратегічному вимірі останні редакції національної стратегії кібербезпеки демонструють посилення акценту на превентивному та проактивному контролі, включно з підвищенням співпраці на міжнародному рівні та визнанням ризику державно-спонсорованих кібератак. Аналітичні матеріали, що супроводжували оновлення стратегії, вказують на перехід до більш активної позиції у сфері кіберзахисту та посилення здатності реагування на складні загрози. Це впливає й на управління електронними послугами: посилюються вимоги до стійкості платформ, контролю постачальницьких ланцюгів та координації між органами.

Незважаючи на сильні сторони, корейська модель має низку структурних і операційних викликів. По-перше, високий рівень регуляторної жорсткості у сфері захисту даних (PIPA) створює складні процедури для обробки персональних даних, що вимагає від розробників електронних послуг ретельної юридичної та технічної проєктної роботи; по-друге, централізовані цифрові сервіси й масове впровадження мобільних ID підвищують вимоги до захисту «точок концентрації» даних і служать привабливою мішенню для атак, якщо захисні бар’єри неповноцінні; по-третє, динамічний розвиток Інтернету речей, штучного інтелекту і хмарних сервісів породжує нормативні розриви, які доводиться оперативно закривати через технічні стандарти і сертифікацію. На додачу, перехід до більш проактивної оборонної

стратегії ставить питання правового й етичного регулювання дій державних кіберструктур у контексті міжнародного права.

Загалом Південна Корея є прикладом інтегрованого державного підходу до інформаційної безпеки електронних послуг: сильне законодавство з охорони персональних даних, централізовані технічні платформи для ідентифікації й доступу, операційна спроможність реагування та активна політика у сфері стандартів і сертифікації. Одночасно розвиток цієї моделі вимагає балансування між безпекою й правами індивіда, постійного оновлення нормативів під впливом технологічних змін і міжнародної співпраці для протистояння еволюціонуючим загрозам.

Розвиток публічного управління інформаційною безпекою електронних послуг в Україні може бути суттєво посилений за рахунок адаптації досвіду Південної Кореї. Передусім варто звернути увагу на уніфікацію правового поля та адаптацію сучасних стандартів захисту персональних даних. Українське законодавство потребує комплексної ревізії для узгодження норм, що регламентують обробку персональних даних, інцидент-репортинг і захист критичної інформаційної інфраструктури. Південнокорейський Закон про захист персональної інформації (PIPA) може бути використаний як зразок, зокрема щодо мінімізації даних, розширення прав суб’єктів і вимог до обробників. Необхідно закріпити право на портативність даних, чіткі правила стосовно автоматизованих рішень і впровадження обов’язкових оцінок впливу на захист даних у великих проєктах. Це підвищить правову передбачуваність і довіру користувачів, хоча може зустріти опір бізнесу, який сприйматиме зміни як додаткові витрати, тому слід передбачити перехідні періоди і технічну підтримку.

Важливим кроком є створення централізованого координатора кібербезпеки з операційною складовою за аналогією з Корейським агентством Інтернету та безпеки та інтегрованою підсистемою – Координаційним центром реагування на комп'ютерні інциденти. В Україні функції розподілені між різними установами, що ускладнює координацію. Необхідно визначити єдиний «центр тяжіння», який виконував би роль національного Координаційного центру реагування на

комп'ютерні інциденти, координував приватні й державні центри реагування на комп'ютерні інциденти, вів реєстри критичної інфраструктури, збирав інцидент-репорти та надавав технічну допомогу. Це дозволить швидше виявляти та реагувати на інциденти, хоча потребуватиме значних інвестицій у людський ресурс і технології, що частково можуть покриватися міжнародною технічною допомогою.

Ще одним пріоритетом є розвиток систем цифрової ідентифікації. Південна Корея впровадила політику «Any-ID», що дозволяє громадянам користуватися різними методами автентифікації, зберігаючи безпеку та інтероперабельність. В Україні потрібно розвивати «Дія.ID», але одночасно відкрити ринок для сертифікованих приватних провайдерів автентифікації. Це передбачає встановлення технічних вимог до багаторівневої автентифікації, запровадження механізмів сертифікації провайдерів та юридичне закріплення мобільних ID. Такий підхід підвищить зручність і охоплення послуг, хоча створює ризик концентрації вразливостей, які необхідно мінімізувати завдяки розподіленим архітектурам і незалежним аудитам.

Не менш значущим є створення системи сертифікації та стандартів безпеки для пристроїв і послуг, зокрема Інтернету речей, хмарних рішень та мобільних сервісів. За прикладом Південної Кореї в Україні варто встановити мінімальні стандарти безпеки, створити акредитовані лабораторії тестування й запровадити поступовий перехід на обов’язкову сертифікацію для постачальників у держсектор. Це знизить ризик використання вразливих пристроїв і рішень, хоча може збільшити витрати виробників, що слід компенсувати грантами або державною підтримкою.

Для підвищення ефективності реагування слід розвинути механізми обміну інформацією про загрози, впровадити централізовані платформи для аналізу загроз і регулярно проводити кібервправи за участю критичних секторів. Це забезпечить швидше виявлення загроз і зміцнить координацію між державою та бізнесом, але потребуватиме гарантій правового захисту обміну даними, щоб подолати недовіру.

Важливим чинником є міжнародна співпраця. Україна має розширювати участь у програмах ЄС, НАТО та співпрацювати з Південною Кореєю, залучаючи

технічну допомогу й міжнародні гранти. Це дозволить швидше впровадити стандарти та знизити фінансове навантаження.

Необхідно забезпечити прозору комунікацію з громадянами, публікувати звіти про кіберстійкість і заходи захисту. Це підвищить довіру до державних електронних сервісів і зменшить ризики соціальної напруги у випадку збоїв. Водночас має бути розроблена чітка модель фінансування, що поєднує бюджетні кошти, приватні інвестиції та міжнародну допомогу, із розрахунком економічних вигод від зниження кіберризиків та розширення цифрової участі громадян.

Узагальнюючи, можна стверджувати, що адаптація південнокорейського досвіду має базуватися на оновленому законодавстві, створенні потужного національного координатора, розвитку сучасної цифрової ідентифікації, впровадженні системи сертифікації та стандартів, підготовці людських ресурсів, прозорості комунікації та міжнародній співпраці. Такий підхід дозволить посилити інформаційну безпеку електронних послуг в Україні, забезпечити стійкість державної інфраструктури та підвищити довіру громадян до цифрової держави.

Розвиток публічного управління інформаційною безпекою електронних послуг у Тайвані представлений як інтегрована політика, що поєднує спеціалізоване законодавство, централізовану координацію кібербезпеки на урядовому рівні, національні операційні структури реагування, практики «вбудованої безпеки» та цифрової ідентифікації, а також активну міжнародну і міжгалузеву співпрацю. Уряд Тайваню підкреслює, що кібербезпека є елементом національної безпеки й економічної стійкості, що особливо актуально в умовах інтенсифікації гібридних загроз у регіоні; на стратегічному рівні це відображено в останніх національних програмах та документах, які координуються Виконавчою Юань (Executive Yuan) і реалізуються через Міністерство цифрових справ (MODA) [175].

Нормативно-правова основа Тайваню будується на кількох комплементарних актах. Центром регулювання є Закон про управління кібербезпекою, який встановлює обов’язки для операторів критичної інформаційної інфраструктури, порядок повідомлення про інциденти та механізми нагляду й інспекцій; для

реалізації окремих положень ухвалено також виконавчі правила [114]. Паралельно діє Закон про захист персональних даних – із суттєвими поправками останніх років, що посилили вимоги щодо повідомлення про витоки, визначення посадових обов'язків відповідальних осіб і підвищили санкційні механізми [131]. Така правова архітектура дозволяє сумістити вимоги щодо технічної стійкості інфраструктури й гарантій приватності при наданні електронних послуг.

Інституційна архітектура Тайваню спрямована на централізацію політики з одночасним розподілом операційних функцій. У межах Міністерства цифрових справ діє Адміністрація з питань кібербезпеки, яка відповідає за імплементацію національних програм кіберстійкості, розроблення базових стандартів для секторів критичної інфраструктури та координацію між відомствами [99]. На оперативному рівні функціонує Координаційний центр реагування на комп'ютерні інциденти Тайваню [225], що забезпечує збір і поширення індикаторів компрометації, технічну допомогу при інцидентах і міжнародну взаємодію в рамках Команди реагування на комп'ютерні надзвичайні події (CERT). Така модель поєднує політичну координацію, встановлення стандартів і оперативне реагування як єдину екосистему управління кіберризиками.

На національно стратегічному рівні Тайвань систематично розвиває послідовні «фази» національної програми кібербезпеки (Національна програма розвитку кібербезпеки / Національна стратегія кібербезпеки), що охоплюють підвищення кіберстійкості держсектору, нарощення людського капіталу, секторальні заходи для енергетики, охорони здоров'я та телекомунікацій, а також міжнародну кооперацію. У 2020-х роках уряд акцентував увагу на «цивільно-військовому» вимірі кіберзахисту, оперативній готовності та інтеграції заходів захисту ланцюгів постачання, що відображено в офіційних стратегічних документах і планах дій до 2025 року [115; 175].

Технічна інфраструктура електронних послуг у Тайвані поєднує державні платформи аутентифікації, сертифікаційні механізми і програми підвищення стійкості Інтернету та хмарних сервісів. Традиційно значну роль відіграє «Сертифікат цифрового громадянина», який видається через сертифікаційну

інфраструктуру, підпорядковану Міністерству внутрішніх справ; останні роки уряд просуває також мобільний варіант сертифіката (Мобільний цифровий сертифікат громадянина) для легітимного доступу до е-послуг. Такі рішення реалізують принципи «безпека за задумом» і «захист приватності за задумом», інтегруючи криптографічні механізми, багатофакторну автентифікацію і мінімізацію наборів персональних даних, що обробляються при взаємодії громадянина з сервісом [132; 239].

Операційні практики включають обов'язкові процедури інцидент-репортингу, міжвідомчі симуляції та навчання, створення галузевих базових стандартів безпеки та акредитаційні програми для продуктів Інтернету речей і постачальницьких ланцюгів. Координаційний центр реагування на комп'ютерні інциденти Тайваню як національний координатор, забезпечує технічні консультації, збір аналітики загроз і координацію зі світовими партнерами, що підсилює здатність країни швидко реагувати на масові кампанії та цілеспрямовані атаки. Регулярні кібервправи й навчання державних ІТ-підрозділів підвищують операційну готовність і апробують процедури взаємодії між секторами [225].

Контекст загроз робить Тайвань вразливим до складних, довготривалих і гібридних атак, зокрема акторів державного рівня. Це визначає пріоритети – захист критичних секторів (наприклад, напівпровідникова промисловість і ланцюги поставок), активна розвідка загроз та міжнародна кооперація у сфері кібербезпеки. Тайвань також працює над зміцненням партнерств із приватним сектором і міжнародними компаніями для нарощення талантів у галузі кібербезпеки (приклад – ініціативи міжнародних ІТ-гравців щодо навчання та створення центрів кібербезпеки на острові). Ці зусилля підсилюють країну в умовах постійного тиску й ескалації операційної інтенсивності з боку супротивних акторів [108].

Водночас у тайванській моделі існують виклики, котрі мають навчальне значення для дослідників і практиків. Централізація повноважень і значущість декількох «точок концентрації» даних підвищують наслідки потенційних компрометацій, отже, потрібні значні інвестиції в захищені архітектури, аудит та розподілені резервні механізми. Також нормативний тиск на відповідність

(особливо після посилення PDPA) створює додаткові операційні навантаження для державних і приватних розробників сервісів; це вимагає практичних настанов, шаблонів DPIA та технічної допомоги для впровадження вимог у проєктній практиці. Крім того, стратегічна орієнтація на кібербезпеку як елемент національної оборони піднімає питання балансу між оперативними заходами та прозорістю перед суспільством [215].

Таким чином, тайванський підхід до публічного управління інформаційною безпекою електронних послуг поєднує формалізоване законодавство (Закон про управління кібербезпекою), централізовану політико-організаційну модель (Міністерство цифрових справ; Адміністрація з питань кібербезпеки), високодоступні сервіси цифрової ідентифікації (Сертифікат цифрового громадянина і мобільні сертифікати), операційну спроможність на рівні Координаційного центру реагування на комп'ютерні інциденти Тайваню та активну міжнародну співпрацю. Це створює високу оперативну готовність і нормативну передбачуваність для провайдерів державних послуг, але вимагає постійних інвестицій у технічні резерви, кадровий потенціал і прозорість політик задля збереження суспільної довіри.

Імплементація досвіду Тайваню у сфері публічного управління інформаційною безпекою електронних послуг в Україні потребує врахування кількох взаємопов'язаних напрямів, що відображають особливості тайванської моделі. Передусім доцільно звернути увагу на нормативно-правову основу. Тайвань створив комплексну архітектуру, що складається із Закону про управління кібербезпекою та Закону про захист персональних даних. Україна може посилити власну правову базу через ухвалення спеціалізованого закону, який би чітко регламентував обов'язки органів влади та операторів критичної інфраструктури щодо управління інцидентами, встановлював вимоги до звітності, технічної перевірки та регулярного аудиту. Важливим елементом може стати й оновлення законодавства про захист персональних даних із урахуванням вимог «захист приватності за задумом» і «безпека за задумом», що дозволить забезпечити баланс між розвитком цифрових сервісів та гарантіями прав людини.

Організаційна модель Тайваню передбачає створення єдиного центру політичної координації у сфері цифрових справ – Міністерства цифрових справ, якому підпорядковується Адміністрація з питань кібербезпеки. Україна може розглянути можливість посилення інституційної ролі спеціалізованого органу, здатного централізувати стратегічне планування, але водночас делегувати операційні завдання технічним підрозділам на зразок CERT-UA та галузевим центрам реагування. Це дозволить уникнути дублювання функцій між міністерствами, підвищити ефективність взаємодії та створити єдині стандарти для всіх секторів.

Особливу увагу слід приділити розвитку електронної ідентифікації. Тайванський досвід із «Сертифікатом цифрового громадянина» та його мобільним варіантом показує, що поєднання централізованої системи сертифікації з багатофакторною автентифікацією забезпечує безпечний і зручний доступ громадян до послуг. В Україні це можна реалізувати через розвиток інтегрованої системи електронної ідентифікації з акцентом на мобільні додатки та криптографічні сертифікати, що зменшить ризики підробки та підвищить довіру до сервісів.

Досвід Тайваню свідчить про ефективність функціонування національного центру реагування на інциденти, який виконує роль координатора між відомствами і приватним сектором, а також забезпечує міжнародну кооперацію. Для України варто посилити можливості CERT-UA, розширивши його функції щодо аналітики загроз, індикаторів компрометації та проведення національних кібервправ. Це дозволить швидко і комплексно реагувати на атаки, у тому числі цілеспрямовані кампанії проти державних інформаційних ресурсів.

Окремий напрям стосується кадрового потенціалу. Тайвань систематично інвестує у підготовку фахівців, розвиваючи програми підвищення кваліфікації та співпрацюючи з університетами і приватними компаніями. Україна може адаптувати цю практику, запровадивши міжвідомчі програми навчання державних службовців у сфері кібербезпеки, а також створивши національні грантові програми для підтримки досліджень у цій сфері.

Таким чином, імплементація досвіду Тайваню в Україні повинна відбуватися через поєднання правових реформ, інституційного зміцнення, розвитку систем електронної ідентифікації, модернізації CERT-UA, інвестицій у людський капітал, інтеграцію принципів безпеки та приватності «за задумом» і розширення міжнародної співпраці. Це дозволить підвищити кіберстійкість держави, забезпечити надійність електронних послуг та зміцнити довіру громадян до цифрових трансформацій.

Таблиця 2.2.

Узагальнення досвіду публічного управління інформаційною безпекою електронних послуг в Сінгапурі, Південній Кореї та Тайвані

Критерій	*Сінгапур*	*Південна Корея*	*Тайвань*
Нормативно-правова база	Закон про кібербезпеку (Cybersecurity Act, 2018), Акт про захист персональних даних (PDPA). Суворі правила для операторів критичної інфраструктури.	Закон «Про сприяння використанню інформаційних мереж» та інші закони щодо захисту персональних даних (PIPA). Вимоги до звітності про інциденти, ліцензування провайдерів послуг.	Закон про управління кібербезпекою (CSMA), Закон про захист персональних даних (PDPA) із посиленими санкціями. Обов'язковий аудит та звітність для держсектора і критичних галузей.
Інституційна архітектура	Агентство з кібербезпеки Сінгапуру (CSA) – центральний координатор; урядові програми «Розумна нація» і GovTech.	Агентство Інтернет-безпеки Кореї (KISA), підпорядковане Міністерству науки та ІКТ. Централізоване управління, координація з місцевими CERT.	Міністерство цифрових справ (MODA) як стратегічний координатор; Адміністрація з питань кібербезпеки (ACS) і TWCERT/CC як операційні структури.
Електронна ідентифікація	SingPass (єдина державна система аутентифікації) з багатофакторною перевіркою, інтеграція з усіма держпослугами.	Національна система e-ID, розширена мобільними додатками (Mobile ID), інтеграція з фінансовими й державними послугами.	Сертифікат цифрового громадянина та мобільний сертифікат; криптографічна інфраструктура для доступу до е-послуг.
CERT/CSIRT-структури	GovTech-CSC (Центр кібербезпеки), співпраця з CSA; активна участь у міжнародних об'єднаннях.	KISA-CERT і галузеві CERT, інтегровані у національну систему реагування.	TWCERT/CC – національний координатор, співпраця з міжнародною мережею FIRST.
Принципи «за задумом»	Security-by-design та Privacy-by-design,	Вимога «захисту приватності за задумом»	Безпека та приватність «за задумом»

	інтегровані у проєктування «Розумної нації».	(privacy-by-design), закріплена у PIPA, кібербезпека – базова умова цифрових сервісів.	впроваджуються через сертифікаційні механізми, аудит і обов'язкову оцінку впливу на дані (DPIA).
Міжнародна співпраця	Членство у глобальних кіберініціативах, активна регіональна кооперація (ASEAN).	Співпраця з міжнародними організаціями (OECD, ITU), активна роль у кібервправах НАТО і Азії.	Співпраця з міжнародними CERT, партнерство з IT-компаніями, обмін досвідом у межах FIRST.
Особливості та сильні сторони	Високий рівень централізації, інтеграція кібербезпеки в національну стратегію «Розумна нація».	Системність, розвиток інновацій у кіберзахисті, багаторівнева структура реагування.	Баланс між централізованим управлінням і технічними підрозділами, поєднання безпеки й приватності, гнучка реакція на гібридні загрози.
Виклики	Ризик надмірної централізації та вразливість при атаках на єдину систему.	Необхідність постійної модернізації через швидкий розвиток технологій та масштаб атак.	Значний тиск на інфраструктуру з боку державних акторів, потреба у прозорості та захисті від концентрації даних.

Порівняльний аналіз розвитку публічного управління інформаційною безпекою електронних послуг у Сінгапурі, Південній Кореї та Тайвані демонструє, що ці країни реалізують схожі підходи, але кожна з них формує власну модель з урахуванням національних потреб та геополітичного контексту. Спільними рисами є наявність спеціалізованого законодавства, яке регламентує кібербезпеку та захист персональних даних, створення централізованих інституцій-координаторів, розбудова національних структур реагування на комп'ютерні інциденти та впровадження принципів «безпека за задумом» і «захист приватності за задумом» у проєктуванні електронних послуг. Усі три країни приділяють значну увагу міжнародній співпраці та інтеграції у глобальні кіберініціативи, що підвищує їхню стійкість до транскордонних загроз.

Водночас наявні й відмінності. Сінгапур робить акцент на повній централізації політики через Агентство з кібербезпеки та інтеграцію безпеки у стратегію «Розумна нація», що є ефективним, але водночас створює ризик концентрації вразливостей. Південна Корея застосовує багаторівневу модель із

широкою мережею CERT і фокусом на інноваціях у кіберзахисті, що дозволяє їй оперативно реагувати на технологічні виклики. Тайвань, перебуваючи в умовах постійного зовнішнього тиску, поєднує централізоване стратегічне управління та гнучкі технічні структури, забезпечуючи баланс між захистом критичної інфраструктури і правами громадян.

2.3. Модернізація публічного управління інформаційною безпекою електронних послуг у США

Сполучені Штати Америки відомі своїми передовими практиками у сфері інформаційної безпеки, які стали невід'ємною складовою розвитку системи електронних послуг у публічному управлінні. Враховуючи масштабність цифрової інфраструктури, високий рівень технологічної інноваційності та стратегічне значення кіберпростору для національної безпеки, США сформували комплексну багаторівневу систему гарантування інформаційної безпеки, що поєднує правові, організаційні, технологічні та комунікаційні інструменти.

У сучасних умовах електронні послуги федерального уряду США функціонують у контексті багаторівневої системи публічного управління, що поєднує законодавчі вимоги, адміністративні інструменти, технічні стандарти та міжвідомчу координацію. Центром координації національної кібербезпеки та захисту критичної інфраструктури виступає Агентство з кібербезпеки та безпеки інфраструктури (CISA), яке виконує роль національного координатора безпеки цифрових і фізичних інфраструктур, надає практичні рекомендації для державних органів і допомагає у реагуванні на інциденти кібербезпеки. Завдання Агентства з кібербезпеки та безпеки інфраструктури включають управління ризиками, забезпечення спроможності реагувати на загрози та сприяння побудові захищеного екосистемного середовища для електронних послуг [107].

Сполучені Штати Америки розробляють та впроваджують широкий спектр стратегій та механізмів для захисту конфіденційної інформації та забезпечення цілісності даних під час надання електронних послуг громадянам та бізнесу.

Однією з ключових проблем є постійно зростаючі загрози кібербезпеці, включаючи кібератаки, витоки даних та інші форми кіберзлочинності. Крім того, великі обсяги конфіденційної інформації, які обробляються в системі публічного управління, створюють складнощі в гарантії її безпеки та конфіденційності. Іншою проблемою є нестача ресурсів та фахівців у галузі кібербезпеки, що ускладнює ефективне впровадження заходів захисту. Аналіз літературних джерел дозволив виокремити сукупність механізмів захисту інформації при наданні електронних послуг, що широко використовуються в США – рис 2.1.

Рис. 2.1. Сукупність механізмів захисту інформації при наданні електронних послуг у США

** Джерело: розроблено автором на основі аналізу [107]*

Описані механізми спільно сприяють ефективному захисту інформації та гарантії безпеки в електронному середовищі в рамках системи публічного управління США. З метою створення інформаційної безпеки в електронних послугах у публічному управлінні США існують ряд нормативних документів та стандартів.

Базовим нормативним документом, що регламентує процеси інформаційної безпеки надання електронних послуг у системі публічного управління, є Закон про свободу інформації. Закон, що був прийнятий у 2002 році, встановлює практики забезпечення інформаційної безпеки для федеральних комп'ютерних систем штатів. Сутність положень Закону передбачає розробку вимог проведення періодичних оцінок ризиків та визначення можливих збитків від несанкціонованого доступу, використання, розкриття, руйнування або модифікації інформації та інформаційних систем публічного управління.

Закон про електронний уряд [240] спрямований на модернізацію публічного управління та поліпшення доступу до публічних послуг через використання інформаційних технологій. Він передбачає створення електронних систем та порталів для надання різноманітних послуг громадянам і бізнесу. Закон також містить положення про захист інформації та конфіденційність даних, що обмінюються та зберігаються в електронній формі.

Закон про модернізацію федеральної інформаційної безпеки встановлює обов’язок для федеральних виконавчих органів розробляти, документувати та впроваджувати програми інформаційної безпеки, здійснювати оцінку ризиків та звітувати про значні інциденти. Закон про модернізацію федеральної інформаційної безпеки також делегує ролі та відповідальність таким органам, як Міністерство внутрішньої безпеки (DHS) та Адміністративно-бюджетне управління США (OMB), для моніторингу дотримання стандартів і підтримки заходів щодо захисту інформаційних активів.

Департамент оборони США також має свою систему управління інформаційною безпекою – Програму інформаційної безпеки Міністерства оборони США (DoDM 5200.01 Vol 1), що визначає загальний огляд програми

інформаційної безпеки, включаючи класифікацію та декласифікацію ризиків, визначає загальні принципи, процедури та вимоги щодо забезпечення конфіденційності, цілісності та доступності інформації в рамках Програми інформаційної безпеки Міністерства оборони США. Законодавчо встановлюються процедури та критерії для класифікації інформації за рівнями конфіденційності та ризиків, процеси декласифікації ризиків та умови, за яких процеси можуть бути реалізовані. Програма інформаційної безпеки Міністерства оборони США встановлює стандарти та вимоги щодо захисту інформації, включаючи контроль доступу, шифрування даних, моніторинг та аудит. Особливості системи управління інформаційною безпекою передбачають, що [240]:

1. DoD використовує систему класифікації інформації, яка визначає рівні конфіденційності та заходи захисту для кожного рівня.

2. Кожен працівник, що працює в межах DoD, несе відповідальність за збереження конфіденційності та цілісності інформації, з якою він працює.

3. DoD співпрацює з іншими урядовими агентствами та міжнародними партнерами з метою обміну інформацією та координації заходів захисту.

Загалом цей закон встановлює ряд механізмів та стандартів для забезпечення ефективного управління інформаційною безпекою в рамках Департаменту оборони США, що допомагає зберегти конфіденційність та цілісність важливої інформації [127].

Технічний стандартний каркас для ідентифікації, автентифікації та управління доступом до електронних послуг формується Національним інститутом стандартів і технологій (NIST). NIST оприлюднює серію спеціальних публікацій, зокрема NIST SP 800-63 «Рекомендації з цифрової ідентичності», що визначають вимоги до ідентифікації користувачів, процесів верифікації та автентифікації для використання у федеральних IT-системах; ці настанови широко застосовуються при проєктуванні механізмів входу до урядових сервісів, систем управління ідентичностями та процедур підтвердження особи. Використання NIST-стандартів забезпечує єдність підходів до верифікації індивідів, знижує шахрайські ризики та підвищує довіру громадян до електронних послуг. Важливим є те, що рекомендації

NIST ґрунтуються на принципі ризик-орієнтованого підходу: кожен рівень автентифікації чи верифікації визначається відповідно до категорії ризиків, пов’язаних з конкретною електронною послугою. Наприклад, для доступу до сервісів, що передбачають обмін чутливою інформацією (податкові дані, медичні записи), встановлюються вищі вимоги до автентифікації, включно з багатофакторною перевіркою, тоді як для сервісів загального користування можуть застосовуватися менш складні процедури.

У серії SP 800-63 виділяються кілька рівнів впевненості (Identity Assurance Level, IAL), рівнів автентифікації (Authentication Assurance Level, AAL) та рівнів управління федерацією ідентичності (Federation Assurance Level, FAL). Кожен із цих рівнів визначає, наскільки суворо має здійснюватися перевірка особи користувача, які механізми автентифікації застосовуються та як здійснюється передача атрибутів ідентичності між різними органами чи системами. Завдяки цьому створюється уніфікована структура, яка дозволяє органам влади взаємно визнавати результати автентифікації користувачів без дублювання процедур, що значно підвищує зручність використання електронних послуг для громадян і водночас гарантує дотримання високих стандартів безпеки [179].

Особливе значення мають підходи NIST до багатофакторної автентифікації, які стали обов’язковим компонентом більшості федеральних систем після ухвалення Виконавчого указу Президента США 14028 про підвищення національної кібербезпеки. Ці підходи передбачають використання комбінації щонайменше двох факторів – наприклад, знання (пароль чи PIN-код), володіння (смартфон, сертифікат безпеки, смарт-карта) та біометричні характеристики (відбиток пальця, розпізнавання обличчя). Таким чином зменшується ймовірність несанкціонованого доступу навіть у разі компрометації одного з факторів. Крім того, рекомендації NIST активно інтегрують концепцію «нульової довіри», що передбачає постійну перевірку користувачів і пристроїв, а не одноразову автентифікацію при вході [180].

Важливим є і те, що NIST визначає стандарти сумісності для інтеграції різних систем управління ідентичностями через федеративні рішення. Це дозволяє

агентствам використовувати загальні платформи доступу, як-от Login.gov, що пропонують єдиний обліковий запис для доступу до багатьох урядових послуг. Такі підходи знижують витрати, спрощують обслуговування користувачів та одночасно посилюють контроль за доступом і відстеженням інцидентів [180].

Отже, публікації NIST у сфері цифрової ідентичності стали основою побудови єдиного нормативно-технічного поля для управління доступом до електронних послуг у США. Вони забезпечують баланс між безпекою та зручністю користувачів, створюючи передумови для масштабного розвитку цифрових сервісів. Крім того, їхня універсальність і модульність дозволяють постійно адаптувати стандарти до нових технологічних викликів, зокрема біометричних технологій, мобільних пристроїв і хмарних платформ.

Пакет законодавчих ініціатив, що відображений у проєкті Закону про посилення американської кібербезпеки від 2022 (S.3600), був спрямований на системне посилення кібербезпеки федеративного уряду США через комплекс змін у правовій, інституційній та процедурній площинах; у тексті проєкту визначалися оновлення до Федерального закону про інформаційну безпеку, запровадження вимог щодо прозорості інцидентів, установлення мобільних стандартів безпеки, а також створення механізмів для оцінювання ризиків і бюджетного планування, пов’язаних із кіберзагрозами. Проєкт S.3600 пройшов Палату сенаторів та містив кілька тематичних заголовків (зокрема «Федеральний закон про модернізацію інформаційної безпеки 2022 року», «Закон про звітування про кіберінциденти для критичної інфраструктури 2022 року» та «Федеральний закон про покращення безпечної хмари та створення робочих місць 2022 року»), що ілюструє комплексність підходу – від оперативної звітності про інциденти до нормативного регулювання хмарних рішень [201].

Законодавчий шлях положень, запропонованих у S.3600, був частково реалізований через інші законодавчі процедури: зокрема положення про обов’язкове звітування про кіберінциденти для операторів критичної інфраструктури були включені як окрема дивізія (Division Y) до Зведеного закону про асигнування (Consolidated Appropriations Act, 2022, Public Law 117–103) і

підписані Президентом у березні 2022 року; ця частина, відома як Закон про звітування про кіберінциденти для критичної інфраструктури 2022 (CIRCIA), поклала на Агентство з кібербезпеки та безпеки інфраструктури обов'язок розробити правила та процедури для повідомлення про «висвітлення кіберінцидентів» і платежі щодо викупів, визначивши часові рамки та механізми обміну інформацією між державою і приватними операторами. У практичному вимірі це означало легалізацію обов'язку повідомляти про інциденти і створення підґрунтя для подальшого регламентування операційного реагування та обміну інформацією [101].

Положення, що стосуються хмарної інфраструктури та уніфікації оцінки її безпеки, реалізуються через Федеральну програму управління ризиками та авторизації хмарних сервісів – FedRAMP. Федеральна програма управління ризиками та авторизації хмарних сервісів як урядова програма існувала раніше в рамках Адміністрації загальних служб США і визначала стандарти для оцінки безпеки, авторизації та безперервного моніторингу хмарних послуг, які використовуються федеральними агентствами; офіційний сайт програми містить технічні описи процесів авторизації, вимог до безперервного моніторингу та механізмів повторного використання пакета авторизації між агентствами. Паралельно у Конгресі обговорювалися та вносилися законодавчі ініціативи (зокрема Закон про покращення та робочі місця в безпечній хмарі Федерального уряду, S.3099 та суміжні проєкти), спрямовані на надання Федеральній програмі управління ризиками та авторизації хмарних сервісів більш чіткої статутної основи і вдосконалення процесів авторизації. В подальшому положення, що формалізують Федеральну програму управління ризиками та авторизації хмарних сервісів, були кодифіковані в межах актів, прийнятих наприкінці 2022 – початку 2023 року, що посилило роль програми як урядового стандарту для хмари [138; 202].

У текстах, що отримали статус закону або були включені до ухвалених актів, закріплено кілька типових інструментів державного регулювання кібербезпеки, які мають пряме відношення до надання електронних послуг: 1) вимоги щодо повідомлення про значні інциденти і встановлення правил обміну інформацією між

державою та приватним сектором (приписи CIRCIA); 2) делегування регуляторної та виконавчої ролі Агентства з кібербезпеки та безпеки інфраструктури з метою здійснення безперервних оцінок державного ризик-профілю; 3) встановлення підстав для формалізації процесів оцінки безпеки хмарних сервісів через Федеральну програму управління ризиками та авторизації хмарних сервісів та створення дорадчих структур і рад для забезпечення прозорості і взаємодії з індустрією; 4) вимоги щодо управління ризиками у вигляді оновлених процедур оцінки, моніторингу та бюджетного планування кіберзаходів в агентствах. Ці елементи не лише визначають адміністративні обов'язки, але й створюють нормативний каркас, у межах якого проєктуються технічні рішення для електронних послуг (захищені канали, автентифікація, шифрування, моніторинг доступу та логування) [112; 201].

Паралельно з регуляцією безпеки розвивається і правова інфраструктура, спрямована на сприяння інноваціям і трансферу технологій з державних наукових установ у комерційні та прикладні продукти. Історично такими «хребтовими» актами є Закон Стівенсона-Вайдлера про технологічні інновації (1980), який уперше визначив роль технологічного трансферу в діяльності федеральних лабораторій, а також Федеральний закон про передачу технологій (1986), що формально дозволив лабораторіям укладати договори про спільні дослідження та розробки (CRADA) та надавати ліцензії на винаходи, створені за державного фінансування. Додатково Закон про національну передачу та розвиток технологій (1995) (NTTAA) зобов'язав федеральні агентства використовувати технічні стандарти, розроблені добровільними організаціями зі стандартизації, коли це можливо, що сприяло комерціалізації розробок і уніфікації вимог до продуктів і послуг. Ці норми створюють законодавче підґрунтя для переходу від академічно-лабораторних розробок до практичних рішень, що можуть бути застосовані в галузі кібербезпеки та для захисту електронних послуг [147; 200].

Конкретний операційний інструментарій технологічного трансферу – зокрема механізм-договори про спільні дослідження та розробки – детально регламентований і використовується для забезпечення співпраці між

федеральними лабораторіями й промисловістю без прямих державних виплат лабораторіями приватним партнерам; через такі угоди забезпечується доступ комерційних суб'єктів до державних наукових ресурсів при збереженні прав і процедур щодо інтелектуальної власності. У сукупності з вимогою Закону про національну передачу та розвиток технологій щодо використання добровільних стандартів це створює сприятливі умови для швидшої адаптації інновацій у практиці захисту електронних сервісів (наприклад, модернізації засобів автентифікації, криптографічних практик, забезпечення походження програмного забезпечення) [109; 176].

Адміністративні ініціативи та виконавчі рішення Президента США теж безпосередньо впливають на політику інформаційної безпеки. Виконавчий указ «Покращення національної кібербезпеки», виданий 12 травня 2021 року, зобов`язує федеральні агентства посилити заходи кіберзахисту, впроваджувати принципи «нульової довіри», покращувати безпеку ланцюгів постачання програмного забезпечення та активізувати співпрацю між урядом і приватним сектором для запобігання й реагування на складні кібератаки. Цей указ ініціював комплексну координацію між Національним інститутом стандартів і технологій, Агентством з кібербезпеки та безпеки інфраструктури, Адміністративно-бюджетним управлінням США та іншими структурами задля уніфікації підходів і прискорення реалізації захисних заходів [136; 137; 151].

Таким чином, у системі публічного управління США спостерігається двоплощинний підхід: нормативно-регуляторні заходи, спрямовані на підвищення стійкості інформаційних систем державного сектора (звітність про інциденти, стандарти для хмарних сервісів, моніторинг, делегування повноважень Агентства з кібербезпеки та безпеки інфраструктури), які закріплені у комплектах законодавчих ініціатив і їхніх реалізаційних механізмах; інструменти, що стимулюють інновації і технологічний трансфер (Закон Стівенсона-Вайдлера про технологічні інновації, Федеральний закон про передачу технологій, Закон про національну передачу та розвиток технологій і механізми договорів про спільні дослідження та розробки), які забезпечують входження передових технічних

рішень у комерційний оборот і, відповідно, їхню доступність для державних і приватних операторів електронних послуг. У сукупності ці підходи зменшують бар'єри для впровадження сучасних засобів кіберзахисту, проте потребують ефективної координації між законодавчим рівнем, регулятором (Агентство з кібербезпеки та безпеки інфраструктури, Адміністрація загальних служб США / Федеральна програма управління ризиками та авторизації) і виконавчою практикою на рівні агентств.

Організаційно-функціональні механізми управління інформаційною безпекою електронних послуг включають безпосередню відповідальність кожного агентства за свої інформаційні системи, централізоване технічне та методологічне лідерство з боку таких органів як Агентство з кібербезпеки та безпеки інфраструктури і Національний інститут стандартів і технологій, а також інструменти міжвідомчого контролю і стандартизації (наприклад, Федеральна програма управління ризиками та авторизації хмарних сервісів, Адміністративно-бюджетне управління США). Крім того, існують практичні ініціативи з модернізації цифрових сервісів – зокрема Цифрова служба США (U.S. Digital Service) та платформи на кшталт Login.gov, які забезпечують централізовані механізми доступу, уніфіковане управління ідентичностями та підвищення зручності використання, водночас інтегруючи сучасні підходи до безпеки і захисту приватності користувачів [221; 233].

Аналіз еволюції політики демонструє декілька ключових трендів:

1) посилення ролі ризик-орієнтованого підходу до безпеки, коли рішення про заходи захисту ґрунтуються на оцінці й управлінні ризиками, а не на формальному виконанні правил;

2) зростання значущості стандартів цифрової ідентичності й автентифікації для створення безпечного доступу до державних сервісів;

3) централізація процедур оцінки безпеки хмарних сервісів через Федеральну програму управління ризиками та авторизації хмарних сервісів;

4) посилена увага до захищеності ланцюгів постачання програмного забезпечення та впровадження принципів «нульової довіри» у мережевій архітектурі урядових систем.

Ці зміни підсилюються як технічними документами (Національний інститут стандартів і технологій), так і політико-адміністративними рішеннями (Виконавчий указ Президента США, Адміністративно-бюджетне управління США), що створює конвергентну модель управління інформаційною безпекою.

Проведений аналіз дає підстави зазначити, що публічне управління інформаційною безпекою електронних послуг у США базується на багатовимірній архітектурі, що поєднує законодавчі акти (Закон про модернізацію федеральної інформаційної безпеки), адміністративні вказівки (Циркуляр № А-130 «Управління інформацією як стратегічним ресурсом»), технічні настанови (серію спеціальних публікацій Національного інституту стандартів і технологій), програми сертифікації (Федеральну програму управління ризиками та авторизації хмарних сервісів) та практичну координацію через агентства на кшталт Агентства з кібербезпеки та безпеки інфраструктури і ініціативи цифрової модернізації (U.S. Digital Service, Login.gov). Така модель забезпечує високу ступінь формалізації процедур і можливість централізованого реагування, але одночасно потребує постійного інвестиційного й політичного забезпечення для адаптації до нових загроз та збереження балансу між безпекою і доступністю державних електронних послуг [196].

Можливості імплементації досвіду США у сфері публічного управління інформаційною безпекою електронних послуг в Україні є надзвичайно значними, адже Сполучені Штати сформували комплексну нормативно-інституційну систему, що поєднує стандартизацію, управління ризиками, технічне регулювання та обов’язковість звітності про кіберінциденти. Передусім важливим є приклад Національного інституту стандартів і технологій США (NIST), який розробив серію спеціальних публікацій (SP NIST), зокрема рекомендації з цифрової ідентичності (NIST SP 800-63). Ці документи створюють цілісний каркас для ідентифікації, автентифікації та управління доступом до електронних послуг. Для

України доцільним є адаптація цих стандартів до національного законодавства, зокрема в частині вимог до електронної ідентифікації, процедур багатофакторної автентифікації та систем управління ідентичностями, що дозволило б зменшити ризики шахрайства, підвищити довіру громадян і забезпечити сумісність із міжнародними практиками.

Досвід США також показує важливість централізованої ролі органів, які визначають політику у сфері інформаційної безпеки. Адміністративно-бюджетне управління США (OMB) встановлює політики та зобов'язує федеральні відомства їх виконувати, забезпечуючи єдині стандарти у сфері кібербезпеки. В Україні подібну функцію може посилено виконувати Міністерство цифрової трансформації у співпраці з Державною службою спеціального зв'язку та захисту інформації. Варто запровадити єдину нормативну рамку, яка б об'єднувала технічні стандарти, вимоги до цифрових сервісів і процедури моніторингу ризиків у державному секторі.

Закон «Про зміцнення кібербезпеки Америки» 2022 року (Strengthening American Cybersecurity Act of 2022 [201]) передбачає обов'язковість звітування про кіберінциденти, формалізацію програми оцінки безпеки хмарних сервісів та вимоги до управління мобільними пристроями й ризиками. Для України важливо адаптувати цей досвід через створення національної програми оцінки безпеки цифрових платформ та хмарних сервісів, які використовуються державними установами, з одночасним зобов'язанням постачальників звітувати про кіберінциденти в центральний координаційний орган. Це дозволить не лише підвищити прозорість у сфері державних цифрових послуг, а й створити передумови для швидкого реагування на інциденти.

Додатково США створили гнучкі механізми взаємодії науки, бізнесу та держави через закони про технологічний трансфер – зокрема Закон про інновації у сфері технологій Стівенсона-Відлера (1980), Федеральний закон про трансфер технологій (1986) та Закон про національний технологічний трансфер і просування (1995). Ці акти дозволяють державним лабораторіям співпрацювати з приватним сектором, передавати технології та розробляти стандарти. Для України це означає

потребу активніше використовувати механізми публічно-приватного партнерства у сфері кібербезпеки, а також стимулювати університети та науково-дослідні установи до спільної розробки рішень із державними органами та ІТ-компаніями.

Значний досвід США пов'язаний також із використанням виконавчих указів Президента, які встановлюють обов’язкові до виконання стандарти для всієї системи державних органів. В Україні доцільно закріплювати ключові рішення у сфері кібербезпеки не лише підзаконними актами, а й указами Президента чи постановами Кабінету Міністрів, щоб забезпечити обов’язковість їх виконання для всіх установ.

Таким чином, імплементація досвіду США в Україні можлива шляхом поєднання кількох напрямів: гармонізації стандартів цифрової ідентичності й управління доступом із публікаціями NIST; створення національної програми оцінки безпеки хмарних сервісів за зразком FedRAMP; впровадження обов’язкової звітності про кіберінциденти; розвитку механізмів публічно-приватного партнерства у сфері кібербезпеки; закріплення стратегічних рішень через акти вищого рівня. Такий підхід не лише зміцнить національну систему інформаційної безпеки, але й сприятиме інтеграції України до єдиного міжнародного цифрового простору та підвищить довіру громадян до електронних державних сервісів.

Таблиця 2.3.

Порівняльна таблиця імплементації досвіду США у сфері публічного управління інформаційною безпекою електронних послуг в Україні

Інституція / механізм	США – короткий опис	Україна – нинішній/потен-ційний аналог	Рекомендації щодо адаптації для України	Пріоритет (кор., серед., довг.)
NIST – серія спеціальних публікацій (SP)	Національний інститут стандартів і технологій (NIST) формує технічні стандарти та рекомендації (наприклад, SP 800-63 для цифрової	В Україні відсутній прямий еквівалент рівня NIST із широким спектром спеціалізованих публікацій; частково функції виконують	Запровадити національний «пакет» технічних рекомендацій на основі NIST (переклад, локалізація, адаптація SP 800-63, RMF). Створити постійну міжвідомчу робочу	Коротк.

	ідентичності; RMF для управління ризиками).	профільні НДІ, робочі групи Мінцифри і Державна служба спеціального зв'язку та захисту інформації (ДССЗІ).	групу з підтримки стандартів і оновлення документації.	
FedRAMP (Федеральна програма управління ризиками та авторизацією)	Уніфікована програма оцінки ризиків і авторизації хмарних сервісів для федеральних агентств; авторизація, повторне використання пакетів, безперервний моніторинг.	В Україні відсутня формалізована національна програма оцінки безпеки хмари на рівні всієї держави; існують поодинокі внутрішні процедури в окремих органах.	Розробити національну програму авторизації хмар (аналог FedRAMP): класифікація ризиків для хмарних сервісів, процеси оцінки, перелік акредитованих аудиторів, механізм повторного використання сертифікацій.	Середн.
CISA (Агентство з кібербезпеки та безпеки інфраструктури)	Національний координаційний центр кібербезпеки і захисту інфраструктури, який координує реагування, інформування та стандартизацію.	В Україні – Державна служба спеціального зв'язку та захисту інформації (ДССЗІ) виконує координаційні функції; також Мінцифра відповідає за е-послуги.	Посилити координаційну роль ДССЗІ (ресурсне, правове підсилення), створити чіткі SLA/процедури взаємодії між ДССЗІ, Мінцифрою та сектором критичної інфраструктури; налагодити централізовані платформи обміну IOC (Ознаки компромісу).	Середн.
CIRCIA / обов'язкове повідомлення про кіберінциденти	Закон про звітування про кіберінциденти для критичної інфраструктури: зобов'язання повідомляти про інциденти, встановлення строків, обмін інформацією з CISA.	В Україні існують вимоги щодо повідомлення про інциденти, але механізми декларування, строки та юридичні гарантії для приватного сектора	Прийняти або уніфікувати норматив про обов'язкове повідомлення про інциденти, визначити точні часові рамки та формат звітності; забезпечити захист інформації, що передається (щоб не порушувати конфіденційність бізнесу).	Коротк.

		потребують уніфікації.		
OMB (Офіс з управління бюджетом) – політики для агентств	Координує бюджетні та регуляторні політики, встановлює вимоги (наприклад, OMB Circular A-130 для управління інформаційними ресурсами).	В Україні функцію політико-координаційного органу виконує Кабінет Міністрів, Мінцифра та Мінфін у частині бюджетних процедур.	Закріпити стандарти управління інформаційними ресурсами на національному рівні (аналог A-130), інтегрувати вимоги у бюджетні процедури для забезпечення фінансування безпекових ініціатив.	Середн.
Цифрова служба США / Login.gov	Агентство та сервіси для модернізації цифрових сервісів, централізований доступ (Login.gov) з уніфікованою ідентифікацією.	В Україні існує державна платформа «Дія», яка виконує функції єдиної точки доступу для е-послуг та цифрової ідентифікації.	Використати модель Цифрової служби США для формування команд «модернізації», застосувати принципи UX/UI і юзабіліті, інтегрувати багаторівневу автентифікацію відповідно до NIST SP 800-63.	Коротк.
RMF (Структура управління ризиками) / NIST RMF	Системний, поетапний підхід до управління ризиками (ідентифікація, оцінка, запровадження контролів, моніторинг).	В Україні застосовують окремі методики оцінки ризиків, але відсутня єдина національна RMF-схема, широко визнана усіма відомствами.	Адаптувати NIST RMF або розробити на його основі національний RMF; провести навчання та створити сертифікацію фахівців із RMF.	Середн.
Закони про технологічний трансфер (Stevenson–Wydler, FTTA, NTTAA)	Нормативна база для співпраці федеральних лабораторій та промисловості: CRADA, ліцензування, стимулювання R&D.	В Україні існують законодавчі положення щодо наукової діяльності, але механізми ефективного технологічного трансферу вимагають розбудови (університети, НДІ, державні лабораторії).	Розвивати механізми CRADA-подібних угод, стимулювати комерціалізацію R&D, створити стимули для державних лабораторій щодо передачі технологій та співпраці з IT-сектором.	Довг.

Механізми публічно-приват-ного партнерства (PPP)	Широко використовуються для обміну інформацією, досвідом, залучення індустріальних CERT/CSIRT і проектів R&D.	В Україні PPP існують, але у сфері кібербезпеки ще не на належному рівні координації та довіри.	Розробити стандартні договори, гарантії конфіденційності для обміну інформацією; створити промислові консорціуми та платформи обміну загрозами.	Середн.
Розвиток кадрів	Програми сертифікації, академічні програми, «ініціативи щодо кіберпрацівників», гранти на підготовку кадрів.	Навчальні програми в Україні з кібербезпеки розвиваються, але є дефіцит фахівців та практичних програм.	Інвестувати у спеціалізовану підготовку (університети, прикладні курси), створити програми обміну та стажувань із закордонними партнерами; впровадити національний план розвитку кіберкадрів.	Довг.
Придбання і вимоги до ПО	У США закупівлі IT та вимоги безпеки інтегровані у процедури закупівель; є вимоги щодо SBOM (Специфікація матеріалів програмного забезпечення) в контексті EO 14028.	В Україні процедури публічних закупівель регулюються окремими законами; вимоги до безпеки ПО і SBOM ще не є обов'язковими у всіх тендерах.	Інтегрувати вимоги до безпеки ПО у процедури держзакупівель (вимога SBOM, критерії безпеки при оцінці пропозицій), навчити закупівельні департаменти оцінювати кіберризики.	Середн.
Інцидент-репор-ти та CSIRT/CERT -структури	Існує мережева система CSIRT/CERT на федеральному і секторному рівнях; CISA координує загальнодержавні заходи.	В Україні діють CERT-UA (під ДССЗІ) та інші командні утворення, однак потребують ресурсного підсилення і інтеграції з приватним сектором.	Посилити можливості CERT-UA, створити секторні CSIRT у критичних галузях, формалізувати процедури взаємодії з приватними CSIRT.	Коротк.

Розроблено автором

У розділі здійснений аналіз публічного управління інформаційною безпекою 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 забезпечення 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 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 гарантії 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.

Узагальнюючи, можна стверджувати, що 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.

Матеріали цього розділу оприлюднені в таких публікаціях автора: [40; 41; 45; 46].

РОЗДІЛ 3. МОДЕЛЬ МЕХАНІЗМІВ ПУБЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЕЛЕКТРОННИХ ПОСЛУГ В УКРАЇНІ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

3.1. Сучасні механізми публічного управління інформаційною безпекою електронних послуг в Україні

В умовах динамічного розвитку цифрових технологій і трансформації системи надання електронних послуг проблема забезпечення інформаційної безпеки (ІБ) набуває особливої актуальності для системи публічного управління в Україні. Станом на сьогодні існує низка викликів і системних обмежень, що істотно ускладнюють побудову ефективної, цілісної та адаптивної системи захисту інформації у процесах цифрового урядування.

Однією з ключових проблемних зон є відсутність єдиного стратегічного підходу до управління інформаційною безпекою на всіх рівнях публічного управління. Незважаючи на існування базових нормативно-правових актів (зокрема Закону України «Про основні засади забезпечення кібербезпеки України» [68], Стратегії кібербезпеки України [74], Стратегії інформаційної безпеки [73] тощо), все ще не сформовано чіткого функціонального поділу відповідальності між суб’єктами ІБ, що породжує фрагментарність рішень, дублювання функцій або навпаки їхню відсутність на певних ділянках.

Другий виклик полягає в недостатньому рівні інтеграції інформаційної безпеки в стратегічне планування цифровізації публічних послуг. Часто системи електронного урядування розробляються без комплексної оцінки ризиків інформаційної безпеки, що зумовлює наявність недоліків на етапах впровадження і експлуатації електронних сервісів. Також спостерігається низький рівень цифрової грамотності персоналу органів державної влади та місцевого самоврядування, що істотно впливає на якість управлінських рішень у сфері захисту інформації. У контексті гібридних загроз і цифрової трансформації, критично важливою є підготовка кадрів, які здатні не лише реалізовувати технічні

рішення, але й формувати стратегії інформаційного управління на основі сучасних підходів до ризик-менеджменту.

Доцільно зазначити, що системною вразливістю є обмеженість фінансування та відсутність економічного обґрунтування інвестицій у сферу ІБ, внаслідок чого пріоритети безпеки відходять на другий план, поступаючись потребам операційного функціонування. Більшість ІТ-бюджетів спрямовуються на підтримку основної інфраструктури, залишаючи захисні компоненти недофінансованими.

Варто окремо виділити інституційну слабкість механізмів міжвідомчої координації. Відсутність стійких горизонтальних зв’язків між органами виконавчої влади, структурами секторальної спеціалізації (медичні, освітні, соціальні служби) та регіональними підрозділами публічного управління призводить до зниження загального рівня ситуаційної обізнаності та спроможності до реагування на кіберзагрози.

Нарешті, сучасний контекст публічного управління ІБ в Україні ускладняється зовнішніми викликами, зокрема:

– повномасштабним військовим вторгненням, що супроводжується гібридною агресією російської федерації, зокрема масованими кібератаками, спрямованими на публічні сервіси, бази даних та критичну інфраструктуру;

– активізацією дезінформаційних кампаній, які підривають довіру до електронного врядування, створюючи перешкоди для цифровізації державного сектора.

Зазначені виклики формують складне поле ризиків, у якому публічне управління має не просто реагувати на загрози, а діяти проактивно, стратегічно та системно. В умовах гібридної війни, посиленої цифровізації та постійної ескалації кіберзагроз постає об’єктивна потреба у формуванні багатофакторної цільової моделі забезпечення інформаційної безпеки (ІБ) у системі публічного управління. Така модель повинна враховувати як стратегічні цілі держави, так і операційні потреби різнорівневих органів влади, користувачів цифрових послуг і суб’єктів кіберпростору.

Функціонально-ієрархічна модель, яку пропонується розробити, повинна виконувати три основні цільові функції:

– превентивну (передбачення), виявлення та нейтралізація потенційних загроз інформаційній безпеці у процесі надання електронних послуг;

– управлінсько-координаційну – забезпечення узгодженості дій між суб'єктами публічного управління, визначення зон відповідальності та рівнів повноважень у сфері інформаційної безпеки;

– оцінювально-моніторингову – формування системи оцінки ризиків, індикаторів ефективності та зворотного зв'язку щодо впроваджених рішень у сфері ІБ.

Описані функції мають реалізовуватися на трьох рівнях управління, які відображають ієрархічну побудову публічного адміністрування:

– стратегічний рівень (національний) передбачає формування державної політики, національних стандартів та стратегій інформаційної безпеки. На цьому рівні діють центральні органи виконавчої влади (Кабінет Міністрів України, Рада Національної Безпеки та Оборони, Міністерство цифрової трансформації України, Державна служба спеціального зв'язку та захисту інформації України), що визначають пріоритети та забезпечують ресурсне підкріплення;

– тактичний рівень (секторальний / регіональний) відповідає за адаптацію державної політики до особливостей галузей та регіонів: працюють галузеві міністерства, обласні (військові) державні адміністрації, профільні агенції, що впроваджують політику ІБ в конкретних середовищах (освіта, охорона здоров'я, соціальний захист тощо);

– оперативний рівень (місцевий / інституційний) охоплює безпосередніх надавачів електронних послуг (ЦНАПи, органи місцевого самоврядування, державні портали, реєстри тощо), які забезпечують безпеку обробки, збереження, передачі та архівування даних. На цьому рівні функціонують служби інформаційної безпеки, адміністрації ІТ-систем та фахівці з кіберзахисту.

Ключовою логікою побудови моделі є функціональна взаємодія між рівнями, що забезпечується через реалізацію таких дій:

– створення єдиної системи нормативного регулювання;

– запровадження уніфікованих стандартів ІБ для всіх постачальників електронних послуг;

– забезпечення взаємного доступу до реєстрів подій та загроз через централізовані платформи (SOC, CERT, платформи аудиту);

– формування вертикальних ліній відповідальності з чітко визначеними зонами управлінської компетенції;

– розвиток інструментів горизонтальної взаємодії (консорціуми, галузеві альянси, міжвідомчі ради тощо).

Окрім ієрархічної структури, модель має бути адаптивною та динамічною, що передбачає можливість гнучкого реагування на нові типи загроз, технологічні зміни та суспільні запити. Для цього доцільно використовувати моделі ризик-орієнтованого управління, де пріоритетність заходів визначається на основі кількісного та якісного аналізу ризиків (Risk-Based Decision-Making). Також передбачається застосування індикаторної системи оцінки ефективності, яка має включати такі елементи:

– індикатори оперативності реагування на інциденти;

– рівень цифрової довіри громадян;

– ступінь захищеності персональних даних;

– частку інституцій, що відповідають вимогам національних стандартів.

Таким чином, запропонована функціонально-ієрархічна модель не лише забезпечує структурованість і цілісність управління інформаційною безпекою, але й дозволяє впровадити інноваційні підходи до проєктування політик, орієнтованих на сталий, безпечний і довірчий розвиток цифрового публічного управління в Україні.

Цільова функція моделі повинна бути зорієнтована на досягнення стійкої, адаптивної, інституційно узгодженої та проактивної системи управління інформаційною безпекою, тобто максимізація рівня кіберстійкості публічної адміністрації за умов обмежених ресурсів, постійної еволюції загроз та необхідності дотримання прав людини в інформаційному просторі. Для цього

доцільно структурувати модель за такими ключовими логіко-функціональними блоками:

1. Інституційно-координаційний блок, який охоплює: узгодження дій основних суб’єктів національної системи кібербезпеки (Національний координаційний центр кібербезпеки, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, Міністерство оборони України тощо); формалізацію механізмів міжвідомчої взаємодії (включно з військово-цивільним партнерством); координаційне управління кризовими ситуаціями в кіберпросторі.

2. Нормативно-правовий блок, що забезпечує: адаптацію українського законодавства до положень Конвенції про кіберзлочинність та права людини в цифровому середовищі; юридичне оформлення повноважень кібервійськ; впровадження принципів публічності, підзвітності та правової визначеності в практиці кіберзахисту.

3. Технологічний блок, який включає: розвиток національної системи моніторингу, раннього виявлення та автоматичного реагування на кіберінциденти; створення державного реєстру об'єктів критичної інформаційної інфраструктури (КІІ) з функцією оцінки їх захищеності; розвиток національної телекомунікаційної мережі та впровадження DNS-сервісу з елементами кіберстійкості.

4. Фінансово-ресурсний блок у системі забезпечення інформаційної безпеки відіграє ключову роль, оскільки без стабільного та цілеспрямованого фінансування неможливо створити ефективну, стійку та адаптивну інфраструктуру кіберзахисту. Передусім він передбачає виокремлення видатків на кібербезпеку як окрему бюджетну програму, що дозволяє уникнути їх розпорошення серед різних статей витрат і забезпечує системний підхід до планування й контролю за використанням коштів. Такий механізм сприяє прозорості державної політики у сфері кіберзахисту та дозволяє підвищити ефективність витрачання публічних ресурсів. Фінансово-ресурсний блок охоплює бюджетну, військову, страхову та партнерську складові, що в комплексі забезпечують сталість функціонування системи кібербезпеки.

5. Соціокомунікаційний блок, в якому акценти зосереджено на: розвитку кіберграмотності серед населення (через національну програму); реалізації механізмів інформаційної взаємодії з громадськістю у кризових ситуаціях; забезпеченні участі громадян у формуванні політики ІБ через опитування, консультації, залучення до оцінки публічної ефективності.

Описані вище блоки взаємопов'язані через систему індикаторів, що є одночасно елементами моніторингу та критеріями оцінки ефективності реалізації Стратегії кібербезпеки України. Зокрема, цільові функції системи управління ІБ мають включати [68]:

F1: Мінімізація ризику критичних кіберінцидентів щодо об'єктів КІІ;

F2: Максимізація оперативності реагування на загрози (час між виявленням і нейтралізацією);

F3: Зростання довіри до цифрових послуг серед населення (% користувачів, рівень задоволеності);

F4: Оптимізація витрат на інформаційну безпеку (ефективність на 1 млн грн);

F5: Спроможність забезпечити кіберстійкість в умовах масованих атак (% індикаторів виконання національного плану реагування).

Таким чином, побудова моделі управління ІБ у публічній сфері має базуватися на принципах системності, адаптивності, доказовості й орієнтації на результат. Її фундаментом виступають міжгалузева координація, проактивна політика, об'єктивна оцінка ризиків та стратегічне планування на основі індикаторного підходу, як закладено у Стратегії кібербезпеки України.

Отже, за результатами аналізу розроблено функціонально-ієрархічну модель механізмів публічного управління інформаційною безпекою електронних послуг – рис. 3.1.

У контексті побудови адаптивної системи публічного управління інформаційною безпекою електронних послуг надзвичайно важливим є встановлення чітких зв'язків між функціональними блоками управління та системою цільових індикаторів, що дозволяють здійснювати моніторинг ефективності реалізації стратегічних завдань. Кожен з блоків – інституційно-

координаційний, нормативно-правовий, технологічний, фінансово-ресурсний та соціокомунікаційний не лише виконує окрему функцію в межах управлінської моделі, але й безпосередньо впливає на досягнення певних результатів, що можуть бути виміряні за допомогою відповідних індикаторів.

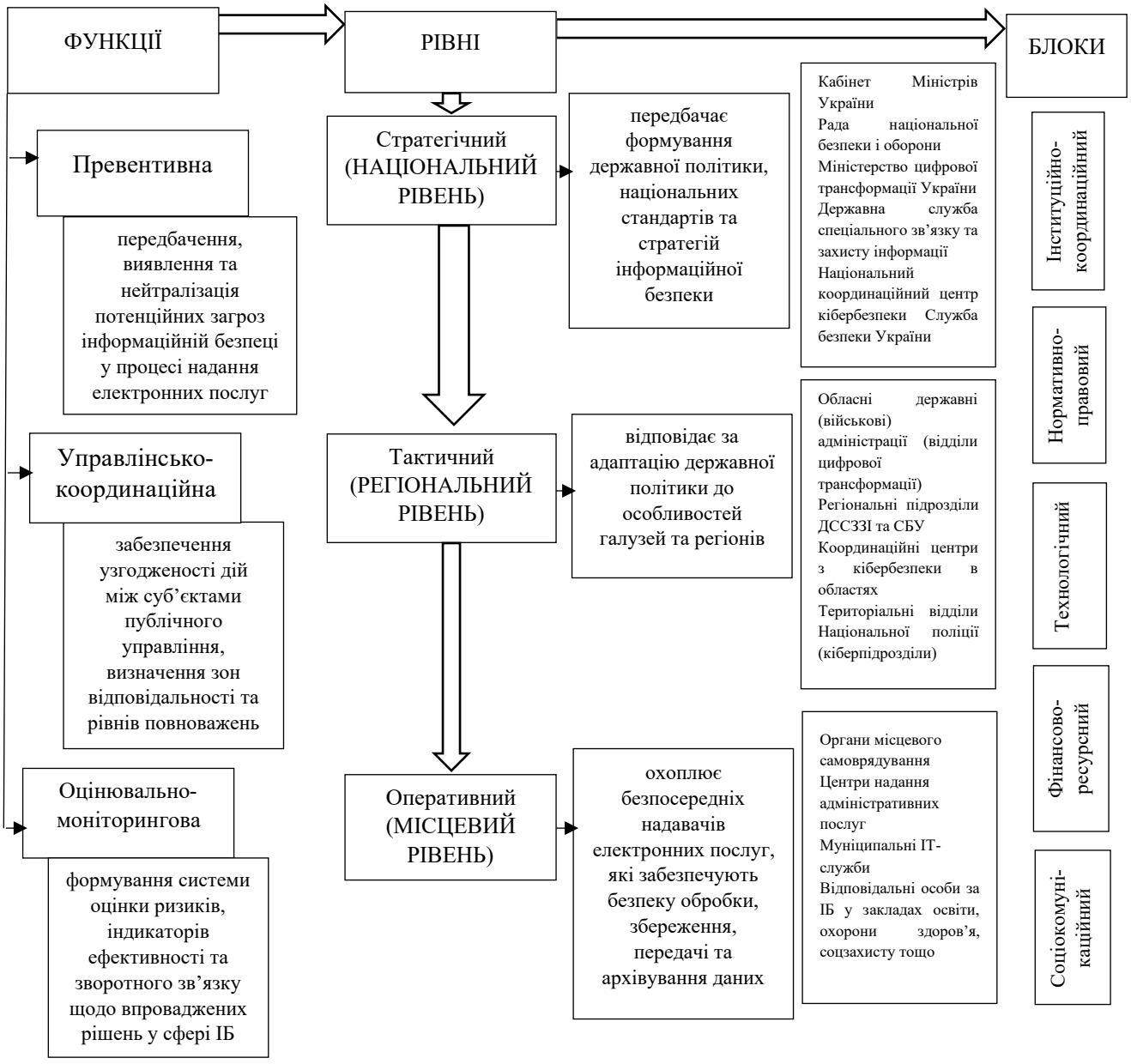

Рис. 3.1. Функціонально-ієрархічна модель механізмів публічного управління інформаційною безпекою електронних послуг (розроблено автором)

Визначення цих взаємозв'язків є ключовим для побудови системно орієнтованої, багатофакторної моделі управління, яка дозволяє забезпечити як

вертикальну інтеграцію рішень (від стратегічного до оперативного рівня), так і горизонтальну синергію між суб'єктами ІБ. Такий підхід дозволяє не лише оперативно реагувати на загрози, а й проактивно формувати середовище цифрової довіри, правової визначеності та кіберстійкості. У таблиці нижче представлено узагальнену матрицю взаємозв'язку між ключовими блоками управління та індикаторами ефективності інформаційної безпеки.

Таблиця 3.1

Взаємозв'язок блоків управління з індикаторами ефективності інформаційної безпеки

Функціональний блок	Суть функцій	Пов'язані індикатори (F)
Інституційно-координаційний	Координація дій між основними суб'єктами ІБ, формування механізмів міжвідомчої та військово-цивільної взаємодії, кризове реагування.	F1: Зниження ризику кіберінцидентів F2: Підвищення швидкості реагування F5: Стійкість до масованих атак
Нормативно-правовий	Гармонізація законодавства з міжнародними актами, визначення повноважень суб'єктів ІБ, забезпечення прозорості та правової визначеності.	F1: Мінімізація ризиків через стандартизацію F3: Довіра користувачів F5: Інституційна відповідність плану
Технологічний	Розбудова інфраструктури моніторингу, створення реєстрів КІІ, впровадження технічних інструментів кіберзахисту.	F1: Захист КІІ F2: Автоматизація реагування F5: Технічна готовність до атак
Фінансово-ресурсний	Формування окремих бюджетних програм, забезпечення фінансування кібервійськ, впровадження системи кіберстрахування та економічної мотивації.	F4: Ефективність витрат F1/F5: Посилення системної спроможності
Соціокомунікаційний	Розвиток цифрової та кіберграмотності, забезпечення комунікації з громадськістю, залучення населення до формування політики безпеки.	F3: Довіра до цифрових послуг F5: Спроможність до самостійного реагування населення

Таким чином, запропонована матриця зв'язків між функціональними блоками управління та відповідними індикаторами ефективності дозволяє не лише структурувати внутрішню архітектуру системи публічного управління інформаційною безпекою, але й забезпечує її практичну орієнтацію на досягнення

вимірюваних результатів. Такий підхід сприяє створенню адаптивної, прогнозованої та підзвітної моделі управління, яка відповідає сучасним викликам цифрової трансформації, євроінтеграційним зобов'язанням та вимогам національної безпеки. Поєднання інституційної узгодженості, технологічної стійкості, нормативно-правової визначеності, достатнього фінансування та високого рівня соціальної включеності формує цілісну основу для ефективного функціонування національної системи кібербезпеки. Використання індикаторного підходу в системі моніторингу дозволяє вчасно виявляти ризики, оцінювати ефективність реалізації політики та коригувати управлінські рішення на всіх рівнях.

Отже, 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.

Запропонована модель базується на ідеї взаємодії трьох рівнів управління – стратегічного, тактичного та оперативного – із чітким функціональним поділом відповідальностей і взаємозв'язком між ними. У межах моделі визначено п'ять ключових функціональних блоків (інституційно-координаційний, нормативно-правовий, технологічний, фінансово-ресурсний та соціокомунікаційний), кожен з яких виконує унікальну роль у формуванні кіберстійкої цифрової екосистеми публічного управління.

Узагальнено систему цільових індикаторів ефективності інформаційної безпеки, яка дає змогу кількісно оцінювати досягнення стратегічних цілей у цій сфері. Запропонована логіка взаємозв'язку між блоками управління та індикаторами забезпечує інтеграцію концептуальних засад у практичну площину,

створюючи умови для розробки проєктних рішень, інструментів реалізації та механізмів моніторингу ефективності політики публічного управління ІБ. Сформульовані положення є методологічною основою для подальших етапів дисертаційного дослідження, що дасть змогу верифікувати запропоновану модель, адаптувати її до реального управлінського середовища та розробити практичні механізми її впровадження.

3.2. Запровадження інноваційного управління в систему інформаційної безпеки електронних послуг в умовах цифрової трансформації

У сучасних умовах цифрової трансформації публічного управління особливої значущості набуває не лише теоретичне осмислення проблематики інформаційної безпеки, але і її практичне вимірювання. Точне розуміння реального стану системи управління інформаційною безпекою в Україні, ступеня готовності основних суб'єктів до реагування на кіберзагрози, а також рівень суспільної довіри до захищеності електронних сервісів можливе лише за умови застосування науково обґрунтованих емпіричних методів дослідження.

Інноваційне управління у системі інформаційної безпеки електронних послуг в умовах цифрової трансформації – це цілеспрямована діяльність державних органів, інституцій та організацій, спрямована на формування, реалізацію й постійне вдосконалення механізмів захисту інформації шляхом інтеграції сучасних технологій, управлінських методів та нових організаційних моделей. Його сутність полягає у відмові від суто реактивних заходів безпеки на користь проактивних і адаптивних рішень, що враховують високу динаміку цифрових загроз та вимоги до довіри громадян до електронних сервісів.

Основними принципами інноваційного управління в системі інформаційної безпеки електронних послуг є:

– пріоритет безпеки та довіри – будь-які цифрові сервіси повинні розроблятися з урахуванням безпеки як базового елемента, що гарантує стабільність та захист персональних даних;

– комплексність і багаторівневість – інформаційна безпека створюється завдяки поєднанню правових, організаційних, технологічних, кадрових та освітніх заходів;

– адаптивність і гнучкість – механізми безпеки повинні швидко змінюватися відповідно до нових типів кібератак та технологічних рішень;

– проактивність – акцент робиться не лише на реагуванні на інциденти, а й на їх запобіганні через прогнозування загроз, тестування вразливостей, сценарне планування;

– інтероперабельність і стандартизація – забезпечення узгодженості між різними інформаційними системами та відповідність міжнародним стандартам (ISO/IEC, рекомендації NIST, ENISA);

– прозорість і підзвітність – користувачі повинні мати доступ до інформації про рівень безпеки сервісів та механізми захисту своїх даних;

– інклюзивність та партнерство – залучення приватного сектора, громадськості та міжнародних організацій до побудови стійкої системи кіберзахисту.

Закономірності інноваційного управління у цій сфері проявляються в кількох вимірах. По-перше, спостерігається неперервна еволюція загроз і рішень, що означає постійну необхідність оновлення як технічних, так і управлінських інструментів. По-друге, має місце зростаюча інтеграція технологій і політик, оскільки цифрові послуги неможливо відокремити від інформаційної безпеки, а захист має бути складовою кожного етапу життєвого циклу сервісу. По-третє, діє закономірність зростання ролі міжнародних стандартів і колективної безпеки, адже цифрові загрози не знають кордонів, і ефективність протидії залежить від гармонізації підходів між країнами та інституціями. По-четверте, простежується посилення людського фактора, оскільки навіть найсучасніші технології не гарантують безпеки без належної підготовки кадрів і розвитку культури кібергігієни. Нарешті, закономірністю є збалансованість між інноваціями й ризиками: запровадження нових цифрових рішень потребує оцінки не лише

користі, а й потенційних загроз, що вимагає впровадження механізмів управління ризиками як основи системи (табл. 3.2.).

Таблиця 3.2.

Принципи та закономірності інноваційного управління в системі інформаційної безпеки електронних послуг в умовах цифрової трансформації

Принципи	Закономірності
Безпека за дизайном (security-by-design) – інтеграція захисту на всіх етапах життєвого циклу послуги	Чим раніше вбудовані механізми безпеки, тим нижчі ризики та витрати на усунення вразливостей
Приватність за дизайном (privacy-by-design) – захист персональних даних з моменту проєктування	Зростання довіри користувачів прямо пов’язане з дотриманням норм захисту даних
Адаптивність – здатність швидко реагувати на нові загрози та технологічні зміни	Середовище кіберзагроз динамічне: стійкість можлива лише за умови постійного оновлення політик та процедур
Прозорість і підзвітність – відкритість дій органів управління перед суспільством і бізнесом	Високий рівень прозорості сприяє формуванню довіри та ефективному громадському контролю
Гібридність управління ризиками – поєднання централізованих і децентралізованих механізмів	Централізація забезпечує узгодженість, а децентралізація – швидкість і гнучкість реагування
Партнерство «держава – приватний сектор» – спільна відповідальність за кіберзахист	Стійкість можлива лише через кооперацію всіх учасників екосистеми цифрових послуг
Безперервність і відновлюваність – забезпечення сталого функціонування навіть у кризових умовах	Впровадження резервних архітектур та планів відновлення знижує вірогідність повного виходу з ладу систем

Запровадження інноваційного управління в систему інформаційної безпеки електронних послуг в умовах цифрової трансформації вимагає комплексного поєднання правових, організаційних, технічних та культурних заходів, що мають на меті забезпечення довіри користувачів, стійкості інфраструктури та

адаптивності до швидкозмінного середовища загроз. Це передбачає формування такої моделі управління, яка здатна не лише реагувати на інциденти, а й проактивно запобігати новим ризикам, використовуючи передові технології та методології. На фундаментальному рівні інноваційне управління розглядається як управлінська парадигма, що поєднує кілька ключових компонентів. По-перше, це впровадження підходів «безпека за дизайном» (security-by-design) та «приватність за дизайном» (privacy-by-design), коли безпека і захист персональних даних інтегруються в усі етапи життєвого циклу електронних послуг – від проєктування й розробки до їх виведення з експлуатації. Такий підхід значно зменшує ризик уразливостей і підвищує довіру користувачів до цифрових сервісів, що підтверджується рекомендаціями Європейського агентства з кібербезпеки (ENISA), яке наголошує на необхідності інтеграції безпеки у саму архітектуру державних цифрових платформ.

По-друге, важливим є застосування гібридних моделей централізованого й децентралізованого управління ризиками, що дозволяє поєднати стратегічний контроль на національному рівні з гнучкістю та інноваційністю місцевих органів і приватних постачальників послуг. Такий підхід практикується, наприклад, в Естонії, де національна платформа X-Road забезпечує централізований і водночас децентралізований обмін даними між державними та приватними установами, гарантує інтероперабельність і базові вимоги безпеки для всіх учасників цифрової екосистеми.

По-третє, інноваційне управління передбачає створення механізмів швидкого оновлення політик і процедур у відповідь на інциденти чи нові технологічні виклики. В умовах зростання кібератак це означає необхідність застосування підходів DevSecOps – інтеграції процесів безпеки безпосередньо у цикл розробки та експлуатації програмного забезпечення. У США Національний інститут стандартів і технологій (NIST) у своїх рекомендаціях (серія SP 800) пропонує моделі управління ризиками, які передбачають динамічне оновлення заходів захисту та безперервний моніторинг середовища.

По-четверте, суттєвою умовою є формування прозорої системи підзвітності й комунікації з громадянами та бізнесом. Це не лише підвищує довіру до державних електронних послуг, але й формує культуру кібергігієни, що є необхідною складовою стійкості цифрової екосистеми. Організація економічного співробітництва та розвитку (ОЕСР) у своїх принципах управління цифровою безпекою наголошує, що прозорість, довіра та багатостороння участь стейкхолдерів є ключовими факторами ефективності державних цифрових стратегій.

Таким чином, інноваційне управління у сфері інформаційної безпеки електронних послуг виходить за межі суто технічних заходів і охоплює інституційні, правові та соціальні аспекти. Його стратегічною метою є створення стійкої, адаптивної та прозорої системи, у якій інформаційна безпека є не додатковим шаром захисту, а інтегрована в архітектуру і функціонування електронних сервісів. Це дозволяє забезпечити безперервність роботи критичних державних платформ, підвищити рівень довіри громадян і бізнесу та сформувати конкурентоспроможне цифрове середовище, що відповідає міжнародним стандартам і викликам сучасної цифрової трансформації.

Інституційна трансформація у сфері управління інформаційною безпекою електронних послуг передбачає не лише модернізацію технічних засобів захисту, а й формування нової архітектури державного управління, де ключову роль відіграють спеціалізовані органи та координаційні центри. Створення або підсилення органів, відповідальних за кібербезпеку державних сервісів, таких як національні центри кібербезпеки, урядові CSIRT (команди реагування на інциденти у сфері комп’ютерної безпеки) та інші координаційні структури, є критично необхідним кроком для забезпечення безперервності роботи та стійкості державних інформаційних систем. Практика провідних країн показує, що саме наявність таких інституцій забезпечує здатність держави не лише реагувати на атаки, але й здійснювати системний моніторинг, аналіз загроз і проактивну профілактику інцидентів.

Одним із центральних аспектів такої трансформації є розбудова партнерств між державним і приватним секторами. Це пов’язано з тим, що значна частина критичної цифрової інфраструктури знаходиться у приватній власності і держава не може ефективно протидіяти масштабним кібератакам без залучення бізнесу та провайдерів цифрових послуг. Модель «публічно-приватного партнерства» активно розвивається в Європейському Союзі, де Європейське агентство з кібербезпеки (ENISA) виступає координатором співпраці між державами-членами та ключовими учасниками ринку, зокрема у сфері обміну інформацією про вразливості та методи їх нейтралізації.

Важливим напрямом інституційної трансформації є створення механізмів оперативного обміну розвідувальною інформацією про кіберзагрози. Такі механізми дозволяють не лише швидко виявляти атаки, але й запобігати їх поширенню через координацію дій на національному та міжнародному рівнях. Прикладом є функціонування CSIRT-мережі в Європейському Союзі, створеної відповідно до Директиви NIS, яка об’єднує національні команди реагування для координації дій у разі масштабних інцидентів та обміну оперативною інформацією між країнами-членами.

Досвід Сінгапуру є показовим у контексті інституційного підходу до кібербезпеки. Cyber Security Agency (Агентство з кібербезпеки Сінгапуру, CSA) було створено як єдиний координаційний орган, який забезпечує не лише розробку політики у сфері кіберзахисту, але й практичне управління ключовими елементами національної цифрової безпеки. CSA відповідає за моніторинг інцидентів, створення стандартів безпеки для державних і приватних організацій, проведення навчання та тестування кіберстійкості інфраструктури. Завдяки такій централізації Сінгапур демонструє здатність швидко адаптуватися до нових типів загроз, забезпечуючи як політичне лідерство, так і технічну підтримку всіх секторів економіки.

Подібні моделі свідчать про важливість чіткого розподілу ролей, належного ресурсного забезпечення та прозорої підзвітності органів управління кібербезпекою. Країни, які запровадили інтегровані підходи, поєднуючи державні

структури, приватний сектор та міжнародне співробітництво, досягають вищого рівня кіберстійкості. У глобальному масштабі також спостерігається закономірність: чим краще налагоджена інституційна координація та співпраця на багаторівневому рівні, тим вищий рівень готовності держави до протидії масштабним кіберінцидентам (табл. 3.3.).

Таблиця 3.3.

Порівняльна таблиця інституційних моделей управління кібербезпекою державних сервісів

Країна / Регіон	Основні інституції	Функції та компетенції	Особливості моделі
Сінгапур	Cyber Security Agency (CSA) – Агентство з кібербезпеки	Розробка державної політики у сфері кібербезпеки; моніторинг загроз і реагування на інциденти; стандартизація вимог до державних і приватних структур; підготовка кадрів; тестування кіберстійкості	Централізована модель, поєднання політичного лідерства і технічної експертизи в одному органі; високий рівень інтеграції держави й бізнесу
Європейський Союз	ENISA – Європейське агентство з кібербезпеки; мережа CSIRT; Кооперaційна група з кібербезпеки	Координація співпраці між державами-членами; технічні настанови; обмін інформацією про інциденти; розробка рекомендацій з управління ризиками; аудит і сертифікація	Наднаціональна модель, що поєднує координацію на рівні ЄС і відповідальність національних органів; акцент на публічно-приватне партнерство
США	Cybersecurity and Infrastructure Security Agency (CISA) – Агенція з кібербезпеки та безпеки інфраструктури; NIST – Національний інститут стандартів і технологій	Моніторинг та реагування на інциденти (CISA); розробка стандартів і керівництв з кібербезпеки (NIST); партнерства з приватним сектором; підтримка критичної інфраструктури	Децентралізована модель із чітким розподілом функцій між органами; акцент на стандартизацію, ризик-менеджмент і широке залучення бізнесу
Україна	Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ); Національний координаційний центр кібербезпеки при РНБО; урядовий CERT-UA	Захист державних інформаційних ресурсів; реагування на кіберінциденти (CERT-UA); координація політики (НКЦК при РНБО); взаємодія з міжнародними партнерами	Модель у процесі розвитку, активна інституційна трансформація в умовах гібридної війни; високий рівень міжнародного партнерства й залежність від зовнішньої підтримки

Впроваджуючи інновації, необхідно також враховувати людський фактор: системне підвищення кібергігієни, професійної підготовки персоналу держслужб і стандартні процедури для розробників (DevSecOps, обов'язкові SBOM – «список компонентів програмного забезпечення») мають стати обов'язковими елементами життєвого циклу проєкту. Орієнтація на принципи безпечної розробки та автоматизованого тестування безпеки скорочує час виявлення вразливостей і знижує довгострокові витрати на підтримку. Паралельно потрібні політики, що стимулюють прозорість та аудити, зокрема з обов'язковими процедурами публічного звітування про інциденти і регулярними незалежними перевірками [216].

Інституційна та технічна специфіка впровадження заходів інформаційної безпеки в умовах воєнного або гібридного протистояння визначається принципом оперативної адаптації і багаторівневої стійкості – тобто здатності державних електронних сервісів зберігати критичну функціональність під дією як прямого фізичного тиску, так і масованих кібероперацій. Практичні елементи цієї специфіки включають запровадження резервних архітектур, сегментацію критичних реєстрів і сервісів, формування планів безперервності бізнесу та відновлення після інцидентів, а також активне міжнародне партнерство для оперативного обміну розвідувальною інформацією, технологічною допомогою й інструментами протидії. Досвід України під час воєнних дій свідчить, що поєднання цих заходів суттєво підвищує стійкість національних цифрових сервісів – зокрема, завдяки переведенню критичних даних до хмарних сервісів і швидкій міграції частини інфраструктури державні сервіси уникли повного паралічу під час початкових фаз вторгнення. Цей кейс чітко ілюструє роль резервних рішень і планування для забезпечення безперервності послуг [234].

Резервні архітектури слід проєктувати за принципом розподіленої надлишковості, яка виключає одиночні точки відмови: дублювання даних і сервісів у географічно рознесених дата-центрах або на ізольованих хмарних майданчиках, застосування змішаних стратегій, а також готові механізми швидкого перемикання і відновлення. Такі архітектури мають передбачати чіткі процедури синхронізації

даних, шифрування резервних копій та тестування процедур відновлення в реальних сценаріях. Рекомендації з планування безперервності та відновлення IT-систем від Національного інституту стандартів і технологій США (NIST SP 800-34 та суміжні документи) створюють методологічну основу для побудови таких процесів, включно з класифікацією сервісів за критичністю, визначенням RTO (цільового часу відновлення) і RPO (допустимого обсягу втрати даних) [179].

Сегментація критичних реєстрів і мереж виступає ключовим механізмом обмеження потенційного розповсюдження компрометації. Практично це означає виділення окремих мережевих зон для держреєстрів, інтегрованих платформ обміну даними та адміністративних систем з застосуванням принципу найменших привілеїв, багаторівневої автентифікації та криптографічного захисту каналів передачі. У контексті війни важливо також передбачити «повітряні зазори» для надчутливих систем або застосування апаратних модулів апаратної безпеки для зберігання ключів, що мінімізує ризики віддаленого доступу в умовах компрометації периферійних систем. Міжнародні аналізи кіберінцидентів під час війни в Україні підкреслюють, що сегментація істотно ускладнює ескалацію атак і скорочує потенційні збитки [231].

Плани безперервності бізнесу й сценарії відновлення повинні бути інтегровані у національні цифрові стратегії та базуватися на регулярних тестуваннях і незалежних аудитах. Вони мають охоплювати не лише технічні заходи, але й організаційні процеси: розподіл ролей і відповідальностей між міністерствами та операторами, процедури взаємозамінності кадрів, політики комунікації з громадянами під час перебоїв, механізми правового забезпечення операцій у надзвичайному стані та планування ресурсного резерву (енергія, доступ до міжнародних каналів зв’язку, фінансування на екстрене відновлення). Документація NIST щодо контингентного планування і міжнародні настанови (включно з матеріалами НАТО з кіберзахисту) можуть бути адаптовані як стандартна методологічна база для державних агентств, що здійснюють планування безперервності бізнесу або планування забезпечення безперервності

діяльності, а також планування відновлення після аварій/катастроф або планування аварійного відновлення [177; 179].

Міжнародне партнерство та оперативний обмін розвідувальною інформацією про загрози є критичними компонентами протидії у гібридних конфліктах. Співпраця з міжнародними командами реагування на інциденти, з європейськими та трансатлантичними структурами дозволяє прискорити ідентифікацію атак, отримати інструменти для їх нейтралізації, обмінюватись індикаторами компрометації і методиками реагування. Українські структури активно співпрацювали з партнерами, що включало обмін тактичною та технічною інформацією, координацію реагування і постачання спеціалізованих інструментів – це значно підвищило здатність країни витримувати складні кібероперації. Аналіз міжнародних звітів та оглядів досвіду війни підкреслює, що скоординована допомога й оперативний обмін інформацією зменшують час виявлення й реагування, що є критично важливим під час масованих кібератак [194; 234].

Український досвід також ілюструє організаційні висновки: по-перше, сильна міжвідомча координація (синхронізація дій між міністерствами, національними центрами кібербезпеки, силовими структурами й операторами критичної інфраструктури) підвищує оперативність і ефективність реакції; по-друге, публічно-приватне партнерство є рушійною силою при захисті інфраструктури, що перебуває у приватній власності; по-третє, відсутність єдиних, чітко задокументованих стандартів і процедур ускладнює масштабне й скоординоване реагування, отже, потребує систематизації й уніфікації правил і технічних вимог. Саме поєднання цих факторів визначає, наскільки успішно держава може забезпечити стійкість сервісів у кризових умовах.

Практичні рекомендації для підвищення стійкості у воєнному контексті мають включати: 1) оперативне впровадження та регулярне тестування резервних архітектур і механізмів резервного перемикання; 2) жорстку сегментацію мереж і доступів до державних реєстрів із застосуванням багатофакторної автентифікації та апаратних модулів захисту ключів; 3) обов’язкові плани безперервності й сценарії відновлення для всіх критичних державних сервісів з визначеними

нормами цільового часу відновлення і допустимого обсягу втрати даних і регулярними вправами; 4) інтеграцію національних команд реагування на інциденти у міжнародні мережі обміну розвідданими і створення формальних каналів для координації допомоги в разі масових інцидентів; 5) посилення нормативно-правової рамки щодо обміну інформацією, відповідальності операторів та процедур надзвичайного управління у цифровому просторі; 6) інвестиції в людський капітал – навчання, ротацію кадрів та програми підвищення кібергігієни для держслужб і операторів. Ці заходи базуються як на міжнародних методологіях (NIST, рекомендації НАТО), так і на практичних висновках, здобутих під час війни в Україні.

Практична дорожня карта запровадження інноваційного управління у сфері інформаційної безпеки електронних послуг у державному секторі має базуватися на системному й поетапному підході, що дозволяє поєднувати швидкість цифрових інновацій із контрольованим управлінням ризиками. Першим кроком є аудит поточного стану, який передбачає ідентифікацію активів та класифікацію електронних сервісів за критичністю. Для цього використовуються методики оцінки ризиків, розроблені Національним інститутом стандартів і технологій США (NIST SP 800-30), та стандарти серії ISO/IEC 27005, які дозволяють визначати рівні загроз і потенційний вплив на користувачів і державу. Класифікація створює основу для пріоритезації ресурсів і формування базового профілю захищеності.

Наступний етап полягає у визначенні мінімальних вимог до безпеки та стандартизації процесів на основі міжнародних настанов. У практиці ЄС широко застосовуються рекомендації Європейського агентства з кібербезпеки, яке надає орієнтири для публічних адміністрацій щодо управління цифровими ризиками та забезпечення стійкості критичних послуг. Такі вимоги включають політику управління доступом, процедури автентифікації, сегментацію мереж, застосування шифрування та управління вразливостями. На рівні ISO важливим є застосування ISO/IEC 27001 для формалізації системи управління інформаційною безпекою та ISO/IEC 27701 для інтеграції захисту персональних даних.

Третім етапом виступає створення або оновлення координаційної структури, що забезпечує комплексне управління ризиками. Це може бути національний центр кібербезпеки або урядова команда реагування на комп'ютерні інциденти, що виконує завдання моніторингу, реагування та стратегічного планування. Приклади ефективних моделей спостерігаються в Сінгапурі, де Агентство з кібербезпеки (CSA) об'єднує функції технічного реагування та політичного керівництва, або в країнах ЄС, де діють урядові CERT-структури з розвиненою мережею партнерств.

Четвертий етап передбачає імплементацію технічних рішень: систем ідентифікації користувачів (зокрема багатофакторної автентифікації), забезпечення міжсистемного обміну даними з дотриманням стандартів сумісності (наприклад, eIDAS у ЄС), журналювання дій користувачів і адміністраторів, а також моніторингу через системи виявлення і реагування на інциденти. Ці рішення формують технологічний фундамент для запобігання та своєчасного виявлення атак.

П'ятий етап полягає у перекладі організаційних і технічних процедур у модель інтегрованої розробки, безпеки та експлуатації – DevSecOps. Цей підхід дозволяє вбудовувати механізми кіберзахисту в усі фази життєвого циклу електронних послуг: від проєктування та програмування до супроводу та виведення з експлуатації. Міжнародні практики підтверджують, що модель інтегрованої розробки, безпеки та експлуатації знижує час реагування на вразливості та мінімізує витрати на їх усунення.

Шостий етап включає систематичне навчання персоналу і кампанії з підвищення обізнаності користувачів. За даними ENISA, людський фактор залишається ключовою вразливістю, тому програми підвищення кібергігієни мають бути регулярними й адаптованими до різних груп працівників – від державних службовців до технічних адміністраторів.

Сьомий етап – регулярне тестування безпеки, включно з внутрішніми і зовнішніми аудитами, вправами з реагування на інциденти, симуляціями кібератак. Стандарти NIST SP 800-61 рекомендують чіткі процедури для підготовки,

виявлення, аналізу й усунення інцидентів, що підвищує рівень готовності органів управління.

Останнім етапом є впровадження механізмів зворотного зв'язку та постійної еволюції політик на основі зібраних даних. Це означає використання аналітики журналів, звітів про інциденти, показників продуктивності систем безпеки для вдосконалення процедур і політик у режимі безперервного циклу PDCA (плануй, роби, перевіряй, впливай), який закладений в основу стандартів ISO/IEC 27001.

Поетапна реалізація такої дорожньої карти дозволяє державним органам уникати фрагментарності, поєднувати інноваційність із належним контролем ризиків, а також підвищувати довіру суспільства й бізнесу до цифрових сервісів як стійкої та захищеної інфраструктури.

Таким чином, інноваційне управління інформаційною безпекою електронних послуг – це комплексна трансформація, що поєднує технічні стандарти (наприклад, у сфері цифрової ідентичності й управління ризиками), інтегровану інституційну координацію, інженерні практики сучасної розробки програмного забезпечення і постійну роботу з людським капіталом. Виконання цієї трансформації потребує адаптації міжнародних настанов до національного контексту, ресурсного забезпечення відповідних органів, прозорих механізмів підзвітності та сталого міжнародного співробітництва. Інвестування в такі заходи підвищує довіру громадян, зменшує ймовірність серйозних збоїв у наданні послуг та сприяє стійкості держави в умовах цифрових викликів.

3.3. Обґрунтування моделі механізмів публічного управління інформаційною безпекою електронних послуг в умовах цифрової трансформації

Побудова ефективної моделі механізмів публічного управління інформаційною безпекою в умовах цифрової трансформації державного сектора передбачає не лише ієрархічну координацію інституцій, а й розгортання комплексу стратегічних механізмів, які формують фундамент довгострокового розвитку.

Стратегічні механізми реалізації моделі є відповіддю на структурні виклики, виявлені в процесі дослідження, і охоплюють такі системні елементи, як нормативно-правове середовище, координаційні інститути, архітектуру цифрової безпеки, кадровий резерв та міжнародну інтеграцію. Їхня ефективна реалізація забезпечує не лише функціонування управлінських процедур, а й гарантує стійкість цифрового середовища до внутрішніх і зовнішніх загроз.

Пропонуємо розробити та прийняти Концепцію розвитку публічного управління інформаційною безпекою електронних послуг на 2026-2036 роки, де передбачити такі розділи:

Загальні положення. Мета публічного управління інформаційною безпекою електронних послуг: забезпечення конфіденційності, цілісності та доступності державних електронних послуг.

Сфера застосування: усі інформаційні системи, реєстри, персональні дані та цифрові сервіси, що адмініструються державним органом.

Нормативна основа: міжнародні стандарти (ISO/IEC 27001, NIST Рамки кібербезпеки, рекомендації ENISA), національне законодавство України.

Розділ 1. Принципи управління інформаційною безпекою електронних послуг:

– «безпека за дизайном» та «приватність за дизайном»;

– принцип найменших привілеїв;

– розподіл повноважень та підзвітність;

– постійна адаптація до нових загроз;

– прозорість і довіра користувачів.

Розділ 2. Інституційний механізм – Національна рада з питань інформаційної безпеки електронних послуг.

2.1. Основні функції ради:

2.1.1. Забезпечення координації між центральними органами виконавчої влади, регіонами, операторами реєстрів, командами реагування на інциденти комп'ютерної безпеки та приватним сектором.

2.1.2. Формування стратегічних документів щодо інформаційної безпеки електронних послуг, національних стандартів та планів імплементації.

2.1.3. Прийняття рішень щодо критичних інвестицій, надзвичайних заходів при національних інцидентах.

2.1.4. Здійснення стратегічного планування і затвердження національних цілей (конфіденційність, цілісність, доступність).

2.1.5. Координація між механізмами (RACI-матриця для ключових процесів).

2.1.6. Оцінка національного ризикового профілю (щорічний національний звіт).

2.1.7. Реалізація механізму кризового реагування: скликання міжвідомчих штабів.

2.2. Склад і повноваження.

Голова (представник уряду), заступники від міністерств (цифрова трансформація, юстиція, фінанси, внутрішні справи, оборона), представники Нацбанку, НАЗК, державних реєстрів, представники команд реагування на інциденти комп'ютерної безпеки, парламентський представник, експерти з громадянського суспільства та приватного сектора.

Розділ 3. Управління ризиками.

3.1. Ідентифікація та оцінка ризиків (на основі ISO 27005 та NIST SP 800-30).

3.2. Категоризація інформаційних активів за критичністю.

3.3. Регулярний перегляд ризиків (не рідше 1 разу на рік).

Розділ 4. Захист даних і користувачів

4.1. Класифікація та маркування даних.

4.2. Захист персональних даних відповідно до GDPR/національного закону.

4.3. Використання криптографії для зберігання та передавання даних.

4.4. Механізми автентифікації: багатофакторна (MFA) для доступу до реєстрів.

Розділ 5. Технічні та організаційні заходи

5.1. Сегментація мереж і критичних систем.

5.2. Використання системи керування інформацією та подіями безпеки, системи виявлення вторгнень, системи запобігання вторгненням для моніторингу загроз.

5.3. Регулярне оновлення програмного забезпечення та патч-менеджмент.

5.4. Контроль доступу та журналювання дій користувачів.

Розділ 6. Управління інцидентами інформаційної безпеки електронних послуг

6.1. Визначення процесу реагування на інциденти (NIST SP 800-61).

6.2. Створення внутрішньої групи реагування (CSIRT).

6.3. Механізм оперативного обміну інформацією з ENISA, CERT-EU, міжнародними партнерами.

6.4. Звітність і документування кожного інциденту.

Розділ 7. Планування безперервності діяльності та відновлення інформаційної безпеки електронних послуг

7.1. Плани безперервності діяльності.

7.2. Плани відновлення після аварій/інцидентів.

7.3. Визначення допустимого часу відновлення та допустимої втрати даних у часі для кожної критичної послуги.

7.4. Регулярне тестування сценаріїв відмовостійкості.

Розділ 8. Навчання та підвищення обізнаності в сфері інформаційної безпеки електронних послуг

8.1. Обов’язкове навчання держслужбовців з питань кібергігієни.

8.2. Щорічні тренінги з реагування на інциденти.

8.3. Спільні навчання з приватним сектором та міжнародними партнерами.

Розділ 9. Моніторинг, аудит і вдосконалення інформаційної безпеки електронних послуг

9.1. Внутрішні та зовнішні аудити безпеки (ISO/IEC 27001).

9.2. Оцінка ефективності заходів.

9.3. Постійне вдосконалення відповідно до моделі PDCA (План–Виконання–Перевірка–Дія).

Зазначені етапи формують модель механізмів публічного управління інформаційною безпекою електронних послуг (рис. 3.2.)

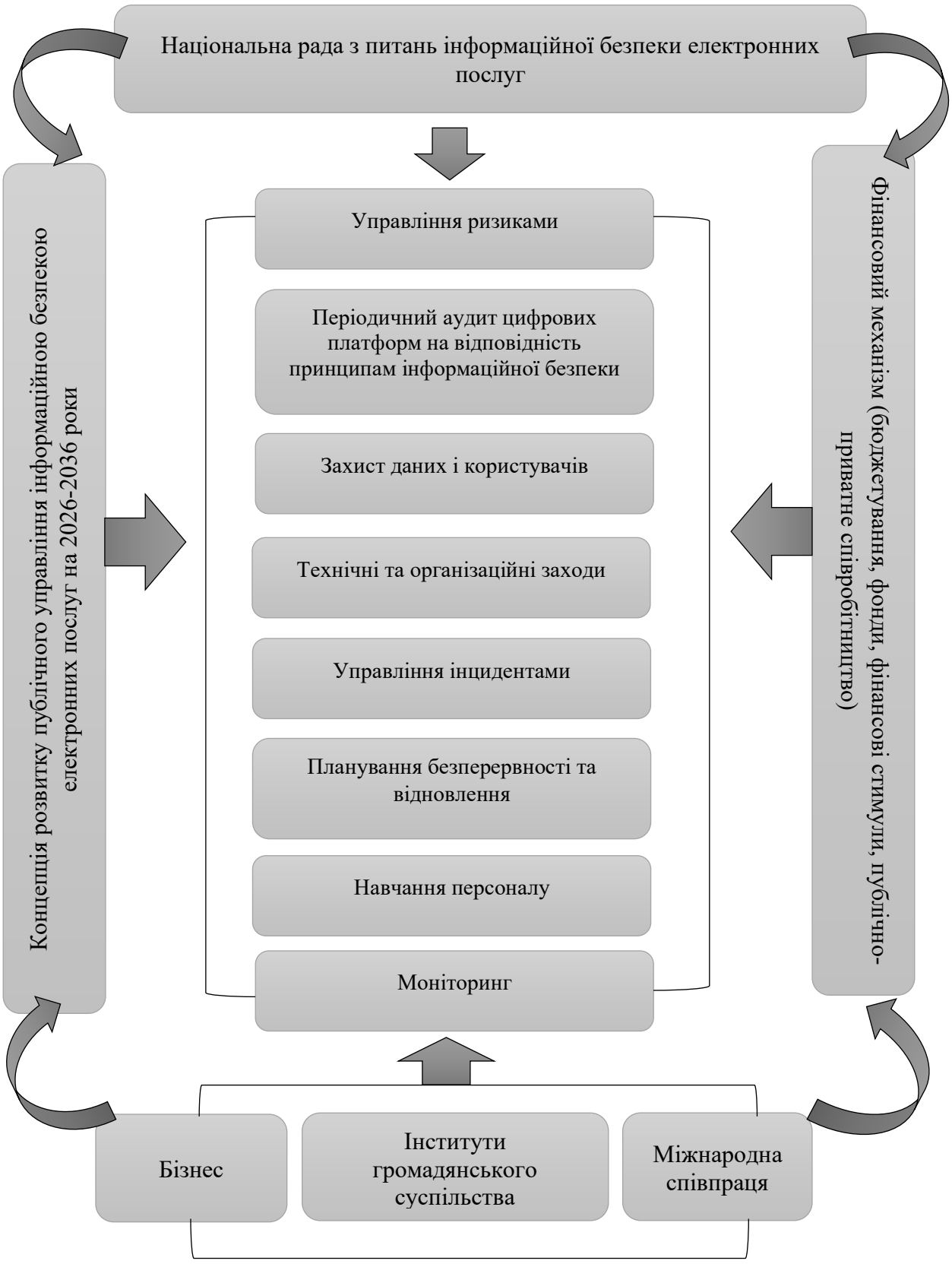

Рис. 3.2. Модель механізмів публічного управління інформаційною безпекою електронних послуг

Модель механізмів публічного управління інформаційною безпеки електронних послуг, представлена на рис. 3.2, має цілісний, багаторівневий характер і поєднує інституційну координацію, нормативно-правове регулювання, фінансове забезпечення, кадрове становлення, контрольні процедури та інформаційно-комунікаційні практики в єдину систему державного управління.

Ця модель виходить із передумови, що забезпечення конфіденційності, цілісності й доступності електронних державних послуг неможливе лише технічними заходами; воно вимагає стійкої інституційної архітектури, чіткої правової бази, планового та прозорого фінансування, професійного кадрового забезпечення та систематичного контролю й взаємодії зі стейкхолдерами.

Інституційний компонент моделі концентрує повноваження стратегічного керівництва та міжвідомчої координації в рамках Національної ради з питань інформаційної безпеки електронних послуг, яка виконує роль вищого орієнтирного органу щодо формування політик, затвердження національних стандартів і пріоритетів, мобілізації ресурсів та ініціювання нормативних змін. Така роль обґрунтовується принципами багаторівневого управління і теорією координації публічних благ: Рада забезпечує синхронізацію дій центральних органів виконавчої влади, національних CSIRT, операторів реєстрів, міжнародних партнерів та представників приватного сектора, задає вимоги щодо розподілу повноважень, систему підзвітності та механізми кризового реагування.

Нормативно-правовий механізм реалізує принципи «безпека за дизайном» і «приватність за дизайном» через прийняття законів, підзаконних актів, технічних регламентів та стандартів відповідності. В його межах формуються вимоги до класифікації даних, застосування криптографії, автентифікації (включно з багатофакторною), зберігання логів і вимог до постачальників IT-послуг. Нормативні інструменти повинні містити перехідні положення та чіткі терміни імплементації, відповідні до міжнародних підходів (ISO/IEC 27001, ISO 27005, NIST CSF та ін.), забезпечуючи баланс між технологічною досяжністю та безпековими вимогами. Законодавча база також має закласти механізми

сертифікації і акредитації, що сприятимуть підвищенню загального рівня заходів та уніфікації практик у державному секторі.

Фінансовий механізм моделі передбачає багатоканальне і прогнозоване фінансування заходів безпеки: виділення цільових бюджетних програм, створення резервних фондів кіберстійкості, залучення міжнародних грантів і впровадження публічно-приватного партнерства для співфінансування великих закупівель (наприклад, SIEM/EDR-платформи, системи резервного копіювання та відновлення). Управління фінансами має базуватися на принципах прозорості й оцінки ефективності витрат, з обов'язковим аудитом використання коштів і звітністю перед Національною радою та парламентом. Пріоритезація фінансування орієнтується на критичність послуг і ризиковий профіль інформаційних активів.

Кадровий механізм забезпечує формування професійного пулу фахівців через визначення стандартів компетенцій, обов'язкових профілів для ролей (CISO у кожному органі, адміністратори реєстрів, аналітики інцидентів, оператори SIEM), систему сертифікації, безперервного підвищення кваліфікації та програм утримання кадрів. На державному рівні доцільно впровадити національні програми підготовки спільно з університетами й приватним сектором, створити резервні кадрові ресурси для кризових ситуацій і систему мотивації (конкурентні умови оплати, професійний ріст, обмін стажуваннями). Цей механізм зменшує ризики людського фактора як джерела інцидентів і підвищує оперативні можливості реагування.

Контрольний механізм поєднує внутрішні та зовнішні аудити, постійний моніторинг стану (через централізовані SIEM, інструменти лог-менеджменту й індикатори вразливостей), регламент звітності щодо інцидентів і механізми застосування санкцій. Система контролю повинна опиратися на модель PDCA (планування – виконання – перевірка – дія), забезпечувати періодичні незалежні перевірки відповідно до ISO/IEC 27001, а також передбачати оперативний аудит цифрових платформ на предмет відповідності принципам інформаційної безпеки. Показники ефективності контролю включають частку органів, які пройшли

зовнішню сертифікацію, середній час виявлення і реагування на інциденти, а також рівень виконання планів безперервності.

Інформаційно-комунікаційний механізм спрямований на формування довіри користувачів та забезпечення прозорої взаємодії зі стейкхолдерами, що включає розробку та реалізацію протоколів публічного інформування під час інцидентів, навчальних кампаній для громадян і бізнесу з кібергігієни, а також налагодження каналів обміну інформацією з міжнародними партнерами (ENISA, CERT-EU, двосторонні CSIRT-канали). Ефективна комунікація покликана мінімізувати репутаційні та операційні ризики, забезпечити адекватне інформування користувачів про заходи захисту та надати механізми зворотного зв'язку для виявлення системних проблем.

Технічні та організаційні заходи інтегруються в усі вищеназвані механізми і містять сегментацію мереж, управління патчами, застосування криптографії для зберігання й передавання даних, журналювання й контроль доступу, резервування даних, тестування відмовостійкості та регулярні сценарні випробування BCP/DRP. Управління інцидентами організовується за міжнародними підходами (процеси виявлення, аналізу, стримування, відновлення та уроків з інцидентів), передбачає створення внутрішніх груп реагування (CSIRT) з чіткими SLA і каналами координації на національному рівні та з міжнародними акторами.

Ключовим елементом моделі є механізм управління ризиками, що забезпечує ідентифікацію, оцінку і категоризацію інформаційних активів за критичністю, регулярний перегляд ризиків і коригування заходів відповідно до змін у середовищі, де існують загрози. Управління ризиками має спиратися на стандартизовані методики (наприклад, ISO 27005, NIST SP 800-30) і містити чітку процедуру для визначення RTO/RPO для критичних сервісів.

Інтеграція всіх компонентів моделі забезпечується операційною матрицею відповідальностей (RACI), де Національна рада виступає як орган, що несе відповідальність за стратегічну координацію і затвердження політик, міністерства та уповноважені підрозділи – за імплементацію і щоденне управління, CSIRT – за реагування на інциденти, аудитори – за незалежну перевірку, а фінансові інституції

– за розподіл ресурсів. Така матриця дозволяє мінімізувати агентські конфлікти, підвищити підзвітність і зменшити розмивання відповідальності.

Впровадження моделі вимагає поетапного підходу: прийняття національної концепції та визначення пріоритетів, адаптація нормативної бази, створення фінансових механізмів і програм підготовки кадрів, технічна модернізація критичних платформ, формування та укріплення CSIRT, запровадження систем моніторингу й аудиту та запуск інформаційних кампаній. Ризики імплементації (недофінансування, кадровий дефіцит, опір змінам) пом’якшуються через створення захищених фондів, міжнародні партнерства, програми обміну та чіткі мотиваційні моделі для держслужбовців.

З огляду на це, запропонована модель виступає як практично орієнтована й науково обґрунтована архітектура публічного управління інформаційною безпекою електронних послуг, котра поєднує інституційну керованість, правову визначеність, фінансову стійкість, кадрову компетентність, контролювальні практики та прозору комунікацію, забезпечуючи тим самим стійкість і довіру до державних цифрових сервісів.

У представленій моделі механізмів публічного управління інформаційною безпекою електронних послуг чітко простежується інтеграція світового досвіду, яка дозволяє забезпечити її відповідність сучасним міжнародним стандартам і кращим практикам. Основою моделі насамперед є принципи «безпека за дизайном» та «приватність за дизайном», які активно розвиваються у країнах Європейського Союзу, зокрема в рамках Загального регламенту про захист даних (GDPR). Їхня імплементація гарантує врахування вимог безпеки ще на етапі проєктування електронних сервісів і повний захист персональних даних громадян. У частині управління ризиками модель спирається на напрацювання міжнародних організацій, передусім стандарти ISO/IEC 27005 та рекомендації NIST SP 800-30, які застосовуються у Сполучених Штатах Америки та країнах ЄС для систематичної ідентифікації та оцінки ризиків. Використання таких підходів сприяє уніфікації методів оцінювання загроз, визначенню критичності інформаційних активів і побудові ефективних стратегій реагування.

Механізм реагування на інциденти інформаційної безпеки відтворює світову практику, закріплену в документах NIST SP 800-61, та діяльність міжнародних команд CSIRT і CERT. Це дозволяє впроваджувати уніфіковані процеси виявлення, стримування та усунення наслідків інцидентів, а також забезпечувати обмін інформацією з такими структурами, як ENISA та CERT-EU. Подібні інструменти зарекомендували себе в Європейському Союзі та США, де міжвідомча координація і міжнародна співпраця є ключем до підвищення кіберстійкості.

Фінансовий механізм моделі також має міжнародні аналоги, оскільки в багатьох країнах створюються спеціалізовані фонди для реагування на кіберінциденти й фінансування проєктів у сфері кібербезпеки. Наприклад, у США реалізуються програми грантової підтримки в межах державних стратегій кіберзахисту, а в країнах ЄС діють механізми співфінансування національних проєктів через програми «Цифрова Європа» та «Горизонт Європа». Це дає змогу знизити фінансове навантаження на державні органи та стимулювати розвиток державно-приватного партнерства.

Кадровий механізм значною мірою спирається на досвід провідних країн, які активно формують системи професійної підготовки і сертифікації фахівців з кібербезпеки. Так, у США діє програма NICE (Національна ініціатива з освіти в галузі кібербезпеки), що визначає стандарти компетентностей для спеціалістів у сфері інформаційної безпеки, тоді як у країнах ЄС розробляються освітні програми на основі рекомендацій ENISA та ініціатив Європейської комісії. Включення таких підходів у модель дає змогу сформувати кадровий резерв і забезпечити сталий розвиток людського капіталу у сфері захисту електронних послуг.

Контрольний механізм відображає міжнародну практику аудиту і сертифікації інформаційних систем відповідно до ISO/IEC 27001, що є глобальним стандартом у сфері управління інформаційною безпекою. Його використання гарантує впровадження циклу постійного вдосконалення PDCA (План–Виконання–Перевірка–Дія), який широко застосовується в управлінських практиках у різних країнах світу для підвищення ефективності систем управління.

Інформаційно-комунікативний механізм також запозичує елементи зі світової практики, зокрема з досвіду держав ЄС, США, Південної Кореї та Сінгапуру, де велике значення надається прозорості, публічній звітності, інформуванню громадян про кіберзагрози та розбудові довіри до електронних сервісів. Просвітницькі кампанії, тренінги для громадян і бізнесу, а також платформи для швидкого інформування про інциденти довели свою ефективність у забезпеченні сталості цифрового суспільства.

Таким чином, модель є поєднанням національних потреб та світових напрацювань, що створює синергетичний ефект. Вона не копіює іноземні зразки, а адаптує їх до умов України, закладаючи фундамент для побудови стійкої системи інформаційної безпеки електронних послуг, що відповідає міжнародним стандартам і водночас враховує специфіку національного правового та інституційного середовища (табл. 3.4.).

Таблиця 3.4.

Імплементація світового досвіду в національну модель механізмів публічного управління інформаційною безпекою електронних послуг: реалізовані елементи

Механізм моделі	**Запозичені елементи зі світового досвіду**	**Країни-приклади**	**Обґрунтування доцільності застосування в Україні**
Інституційний	Міжвідомчі ради з кібербезпеки, стратегічні центри координації (National Cybersecurity Council, Cyber Command)	США, Велика Британія, Естонія	Координація на найвищому рівні дозволяє уникнути фрагментації відповідальності й забезпечити швидке ухвалення рішень при кризах.
Нормативно-правовий	Принципи «безпека за дизайном», «приватність за дизайном»; стандарти ISO/IEC 27001, ISO 27005, NIST CSF; імплементація GDPR	ЄС, США, Канада	Гармонізація з міжнародними стандартами забезпечує сумісність, довіру міжнародних партнерів і захист персональних даних.
Фінансовий	Створення спеціальних фондів для кіберстійкості; державно-приватні партнерства (PPP); міжнародні гранти (Цифрова Європа, Горизонт Європа)	США, ЄС, Сінгапур	Диверсифікація фінансування знижує ризик недофінансування й забезпечує сталі інвестиції у сферу безпеки.

Кадровий	Національні програми підготовки і сертифікації (NICE Framework, освітні ініціативи ENISA); формування кадрового резерву	США, країни ЄС, Південна Корея	Стандартизовані компетенції та підготовка фахівців підвищують якість людського капіталу і зменшують кадровий дефіцит.
Контрольний	Аудит і сертифікація за ISO/IEC 27001; використання моделі PDCA для постійного вдосконалення; незалежні зовнішні перевірки	ЄС, Японія, Канада	Регулярний аудит і аналіз підвищують довіру до державних сервісів і забезпечують системність розвитку.
Інформаційно-комунікативний	Публічні звіти про стан безпеки, протоколи інформування громадян, навчальні кампанії з кібергігієни	Естонія, Сінгапур, Південна Корея	Прозорість та просвітницька робота підвищують довіру до е-послуг і сприяють формуванню культури кібербезпеки.
Управління ризиками	Ідентифікація ризиків за ISO 27005 і NIST SP 800-30; категоризація інформаційних активів; щорічний перегляд ризиків	США, Німеччина, Нідерланди	Систематичний ризик-менеджмент дозволяє ефективно розподіляти ресурси і концентрувати захист на критичних об’єктах.
Управління інцидентами	Методологія реагування NIST SP 800-61; створення CSIRT/CERT; міжнародний обмін інформацією (ENISA, CERT-EU)	США, ЄС, Естонія	Єдина методологія реагування забезпечує оперативність, а міжнародна кооперація посилює захист від глобальних загроз.

Таким чином, модель механізмів публічного управління інформаційною безпекою електронних послуг базується на інтеграції кращих міжнародних практик, які довели свою ефективність у провідних країнах світу. Запозичення інституційного підходу у вигляді створення координаційної ради відповідає досвіду США, Великої Британії та Естонії, де міжвідомчі структури дозволяють забезпечити узгодженість рішень і швидке реагування на кризові ситуації. Нормативно-правове підґрунтя моделі орієнтоване на міжнародні стандарти ISO/IEC, рекомендації NIST та вимоги GDPR, що забезпечує гармонізацію української системи з глобальними правилами кіберзахисту й гарантує довіру міжнародних партнерів.

Визначені 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.

Запропонована модель базується на ідеї взаємодії трьох рівнів управління – стратегічного, тактичного та оперативного – із чітким функціональним поділом відповідальностей і взаємозв'язком між ними. У межах моделі визначено п'ять ключових функціональних блоків (інституційно-координаційний, нормативно-правовий, технологічний, фінансово-ресурсний та соціокомунікаційний), кожен з яких виконує унікальну роль у формуванні кіберстійкої цифрової екосистеми публічного управління.

Узагальнено систему цільових індикаторів ефективності інформаційної безпеки, яка дає змогу кількісно оцінювати досягнення стратегічних цілей у цій сфері. Запропонована логіка взаємозв'язку між блоками управління та індикаторами забезпечує інтеграцію концептуальних засад у практичну площину, створюючи умови для розробки проєктних рішень, інструментів реалізації та механізмів моніторингу ефективності політики публічного управління ІБ. Сформульовані положення є методологічною основою для подальших етапів дисертаційного дослідження, що дасть змогу верифікувати запропоновану модель, адаптувати її до реального управлінського середовища та розробити практичні механізми її впровадження.

Запропоновано запровадження інноваційного управління в систему інформаційної безпеки електронних послуг в умовах цифрової трансформації. Зазначено, що запровадження інноваційного управління у 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» та «приватності за дизайном», які інтегрують вимоги безпеки у життєвий цикл електронних сервісів від моменту їхнього проєктування. Це забезпечує не лише зменшення ризиків, а й ефективніше використання ресурсів.

Управлінські закономірності вказують на те, що ефективність інформаційної безпеки залежить від балансу між централізованими й децентралізованими моделями управління ризиками, що дозволяє одночасно забезпечувати стратегічну координацію та оперативну гнучкість. Важливим є також швидке оновлення політик і процедур у відповідь на нові загрози, що відображає динаміку сучасного кіберпростору. Прозора система підзвітності, комунікації з громадянами і бізнесом, а також інтеграція публічно-приватних партнерств створюють передумови для зростання рівня довіри та ефективного колективного реагування.

В умовах воєнного й гібридного протистояння, як демонструє досвід України, інноваційне управління неможливе без резервних архітектур, сегментації критичних реєстрів, планів безперервності та сценаріїв відновлення. Активна міжнародна співпраця, зокрема в межах ЄС, НАТО та через спеціалізовані платформи кіберобміну, підсилює стійкість до атак та забезпечує доступ до найкращих практик. Водночас систематизація стандартів та узгоджене інституційне зміцнення органів кібербезпеки залишається необхідною умовою для підвищення ефективності захисту державних електронних послуг.

Отже, інноваційне управління інформаційною безпекою електронних послуг в умовах цифрової трансформації варто розглядати як динамічну систему, що поєднує технологічні рішення, організаційні структури, нормативно-правові механізми та культуру безпеки. Це управління повинно бути не лише інструментом зниження ризиків, а й фактором забезпечення довіри суспільства до цифрової держави, підвищення її конкурентоспроможності у глобальному середовищі та

стійкості в умовах кризових ситуацій. Вибудова такої моделі є тривалим процесом, проте саме вона відповідає викликам цифрової епохи і здатна забезпечити сталий розвиток електронних сервісів як основи сучасного публічного управління.

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. Її діяльність забезпечує взаємодію між центральними органами виконавчої влади, регуляторами, адміністраторами реєстрів, національними командами CSIRT та міжнародними партнерами. Такий підхід запобігає дублюванню функцій і фрагментації відповідальності, створюючи єдиний центр прийняття рішень на стратегічному рівні.

Нормативно-правовий механізм у моделі ґрунтується на гармонізації українського законодавства з міжнародними стандартами ISO/IEC 27001, ISO 27005, NIST Рамки кібербезпеки та практиками GDPR. Це дає можливість забезпечити відповідність національної системи управління інформаційною безпекою міжнародним вимогам, спростити інтеграцію до європейського кіберпростору та водночас гарантувати захист персональних даних громадян. 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. Такий підхід забезпечує стабільність і прогнозованість фінансових потоків, дозволяє здійснювати великі інфраструктурні

проєкти (наприклад, впровадження SIEM, EDR, резервного копіювання) та стимулює приватний сектор до співпраці з державою у сфері кібербезпеки.

Кадровий механізм моделі передбачає створення професійного кадрового резерву шляхом формування стандартів компетенцій для ключових посад (CISO, адміністратори реєстрів, аналітики 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. Це дозволить знизити кадровий дефіцит та мінімізувати ризики людського фактора.

Контрольний механізм передбачає системну багаторівневу перевірку ефективності заходів із захисту інформації через внутрішні й зовнішні аудити, регулярний моніторинг, індикатори ефективності та механізми санкцій. Використання міжнародного стандарту ISO/IEC 27001 та моделі PDCA дає змогу забезпечити постійне вдосконалення системи, оперативне виявлення відхилень і підвищення рівня довіри до державних електронних послуг. Окреме значення має прозорість у звітуванні, що дозволяє громадянам і міжнародним партнерам оцінювати ефективність публічної політики.

Інформаційно-комунікативний механізм орієнтований на створення довіри до державних електронних сервісів та формування культури кібербезпеки в суспільстві. Він передбачає обов'язкову публічну звітність, інформування користувачів у випадку інцидентів, проведення освітніх та просвітницьких кампаній, а також активний обмін інформацією з міжнародними структурами, зокрема ENISA та CERT-EU. Це забезпечує прозорість, підзвітність і сприяє підвищенню стійкості до загроз.

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. Це дозволяє систематизувати процеси оцінки й мінімізації ризиків, визначати пріоритети у фінансуванні та концентрувати ресурси на найбільш вразливих сегментах. Доповненням виступає

механізм управління інцидентами, який ґрунтується на NIST SP 800-61 і передбачає створення CSIRT-структур, уніфіковані протоколи реагування та міжнародний обмін даними про загрози.

Узагальнюючи, можна зробити висновок, що модель механізмів публічного управління інформаційною безпекою електронних послуг формують науково обґрунтовану, практично орієнтовану й комплексну систему управління, яка враховує національні особливості України та водночас інтегрує кращий світовий досвід. Вона створює інституційну, нормативну, фінансову, кадрову, контрольну та комунікаційну основу для підвищення кіберстійкості держави, захисту прав громадян і забезпечення довіри до електронних послуг, закладаючи фундамент для інтеграції України у глобальний простір кібербезпеки.

Запропоновано розробити та прийняти Концепцію розвитку публічного управління інформаційною безпекою електронних послуг на 2026-2036 роки, де передбачається врегулювати зазначену вище модель.

Матеріали цього розділу оприлюднені в таких публікаціях автора: [42; 47; 48; 50].

ВИСНОВКИ

У дисертаційній роботі здійснено теоретичне узагальнення та запропоновано нове вирішення важливої наукової проблеми щодо удосконалення механізмів публічного управління інформаційною безпекою надання електронних послуг. За результатами дослідження сформульовано висновки й пропозиції, що мають теоретичне та практичне значення, зокрема:

1. Визначено наукові підходи до механізмів публічного управління інформаційною безпекою надання електронних послуг та виокремлено п’ять підходів:

– техніко-адміністративний підхід, який орієнтований на формалізацію регулятивної бази, застосування міжнародних і національних стандартів (ISO/IEC 27001, NIST Рамки кібербезпеки), розвиток систем управління інформаційною безпекою (ISMS), а також на впровадження інструментів контролю, аудиту, сертифікації та процедур аналізу. Він забезпечує уніфікацію практик захисту даних, закріплення ролей і відповідальностей, а також підвищує підзвітність органів влади у сфері надання е-послуг;

– соціально-технічний підхід зосереджує увагу на тому, що інформаційна безпека є властивістю не лише технологій, а й соціально організованих практик. Тут наголос робиться на взаємодії користувачів і технологій, ролі організаційних культур, поведінкових моделей, міжвідомчої координації. Саме цей підхід підкреслює значення «людського фактора» та необхідність розвитку цифрової грамотності, довіри та прозорості у відносинах між державою й громадянами;

– управлінсько-організаційний підхід інтерпретує механізми інформаційної безпеки через призму управлінських систем, процедур стратегічного планування, ризик-менеджменту та циклічного вдосконалення (модель PDCA). Він демонструє, що ефективність публічного управління визначається не лише наявністю технологічних засобів, а й здатністю органів влади забезпечувати узгодженість політик, стратегічне прогнозування та координацію дій на різних рівнях;

– міжнародно-порівняльний підхід базується на аналізі практик різних країн і міжнародних організацій, що дозволяє адаптувати та трансформувати перевірені інструменти до національних умов. У цьому контексті особливого значення набувають питання кіберстійкості, стандартизації, транснаціональної співпраці та розбудови дослідницьких мереж, які забезпечують сталість політик у глобальному цифровому середовищі;

– бібліометричний та наукометричний підхід забезпечує виявлення ключових трендів розвитку науки: інтеграцію штучного інтелекту для моніторингу загроз, міждисциплінарність досліджень, зростання ролі питань довіри та соціальної легітимності. Цей підхід допомагає зрозуміти, які напрями є домінуючими у світовій науковій думці, а які – залишаються недостатньо дослідженими.

Систематизація підходів показує, що механізми публічного управління інформаційною безпекою електронних послуг слід розглядати як інтегровану систему, що поєднує правові, технічні, організаційні та соціальні виміри. Таким чином, жоден із підходів не може вичерпно забезпечити ефективність управління окремо: лише їх поєднання формує умови для комплексного захисту, підвищення довіри громадян, сталості цифрової інфраструктури та посилення легітимності держави в умовах цифрової трансформації.

2. Проаналізовано понятійно-категоріальний апарат дослідження механізмів публічного управління інформаційною безпекою надання електронних послуг. Зазначено, що понятійно-категоріальний апарат дослідження механізмів публічного управління інформаційною безпекою надання електронних послуг формується на перетині кількох наукових площин – адміністративно-правової, інформаційно-технологічної, соціально-технічної та управлінсько-організаційної. У науковому дискурсі чітко простежується тенденція до інтеграції технічних категорій, що описують засоби захисту (криптографія, автентифікація, контроль доступу, моніторинг), з управлінськими та правовими категоріями (політика безпеки, регулювання, підзвітність, відповідальність, інституційна координація).

Саме ця інтеграція створює змістовне поле для аналізу механізмів публічного управління.

Ключове поняття «механізми публічного управління» в цьому контексті відображає сукупність інструментів, процедур і практик, які забезпечують вплив держави на процеси гарантування безпеки в електронних послугах. До таких механізмів належать: нормативно-правові (закони, регламенти, стандарти), організаційні (централізовані агентства, центри реагування на інциденти, служби внутрішнього контролю), інструментально-технологічні (системи управління інформаційною безпекою, автоматизовані засоби виявлення загроз, аудиторські платформи) та соціально-комунікативні (програми навчання, підвищення обізнаності, поведінкові інтервенції).

У понятійно-категоріальному апараті центральним є термін «інформаційна безпека», який у сучасних дослідженнях розглядається не лише як технічна категорія (захист конфіденційності, цілісності та доступності даних), але й як соціально-технічне явище, що включає взаємодію технологій із поведінкою користувачів, організаційними культурами, управлінськими моделями та нормативними регуляціями. Це дозволяє виокремлювати соціально-технічний підхід, у якому інформаційна безпека є властивістю системи, що виникає через баланс між технологічними механізмами, управлінськими рішеннями та соціальними практиками.

Категорія «електронні послуги» у межах дослідження має подвійний зміст: з одного боку, це інструмент цифрової трансформації публічного сектора, а з іншого – вразлива інфраструктура, що потребує особливих заходів управління ризиками, захисту персональних даних та забезпечення довіри користувачів. Це означає, що понятійний апарат неможливо будувати без урахування категорій «довіра», «надійність», «стійкість» і «сталість», що набувають особливого значення в умовах цифровізації державного управління.

Понятійно-категоріальний апарат дослідження включає базові категорії («публічне управління», «інформаційна безпека», «електронні послуги») та похідні, що описують механізми їх взаємодії («система управління інформаційною

безпекою», «механізми регуляторного впливу», «соціально-технічні практики», «кіберстійкість», «постачальницька безпека»). Його особливість полягає в міждисциплінарності: він поєднує правові, організаційні, технічні та соціальні концепти, створюючи цілісну методологічну основу для аналізу та вдосконалення механізмів публічного управління.

Обґрунтовано авторське трактування поняття «механізми публічного управління інформаційною безпекою надання електронних послуг». Механізми публічного управління інформаційною безпекою надання електронних послуг доцільно визначити як 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. Таке авторське визначення акцентує увагу на кількох ключових аспектах: нормативно-правовий компонент – закони, стандарти та регламенти, що створюють обов'язкові правила гри для суб'єктів, які надають або користуються е-послугами; організаційно-інституційний компонент – система органів, установ і підрозділів (центри реагування на інциденти, служби захисту інформації, контролюючі інститути), які забезпечують координацію та підзвітність; технологічний компонент – застосування інформаційно-комунікаційних технологій і методів (системи управління інформаційною безпекою, криптографія, аудит, автоматизовані засоби моніторингу та виявлення загроз); соціально-комунікативний компонент – підвищення обізнаності користувачів, формування культури безпеки, розвиток довіри до державних цифрових сервісів. Узгодженість цих складових відображає комплексність управління: воно не обмежується технічними чи правовими заходами, а передбачає інтегровану взаємодію різних рівнів управління і суспільних практик. Саме така багатовимірність дозволяє говорити про механізми як про системоутворюючий чинник, що забезпечує не лише функціональну безпеку електронних послуг, але й стабільність цифрової взаємодії між державою та громадянами.

3. Систематизовані 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.

Управлінські наслідки цих викликів свідчать про потребу системної відповіді, яка включає розробку національної стратегії кіберстійкості, створення багаторівневих резервних механізмів, удосконалення нормативного регулювання з гарантіями прав людини, формалізацію публічно-приватного партнерства та посилення координації між організаційними підрозділами або спеціалізованими командами реагування на комп'ютерні надзвичайні події, операторами критичної інфраструктури та правоохоронними органами. Лише комплексний підхід, що поєднує технологічну модернізацію, адміністративну інтеграцію та правову збалансованість, здатний забезпечити стійкість та довіру до електронних послуг навіть в умовах тривалих криз і воєнних загроз.

4. Здійснений аналіз стану публічного управління інформаційною безпекою електронних послуг в країнах ЄС. Зазначено, що публічне управління

інформаційною безпекою електронних послуг у Німеччині, Естонії, Данії та Литві демонструє різні моделі організації, проте об’єднане спільною метою – гарантування кіберстійкості державних і суспільних цифрових систем. Німеччина спирається на інституційну силу Федерального відомства з інформаційної безпеки та комплексну законодавчу базу, де ключову роль відіграють директиви Європейського Союзу (зокрема NIS2) і власні нормативно-правові акти. Сильним боком німецької моделі є високий рівень стандартизації, проте головним викликом лишається складність координації між федеральними та земельними структурами, що може знижувати оперативність реагування.

Естонія є прикладом держави-лідера у сфері цифрової трансформації та кіберзахисту. Її модель базується на інтеграції технічних рішень (X-Road, RIHA), єдиної електронної ідентифікації та інноваційної програми e-Residency. Цей досвід доводить, що стійка кібербезпека досягається не лише завдяки технологіям, а й через постійне оновлення законодавства, підготовку фахівців і формування високого рівня довіри громадян до цифрових сервісів. Водночас викликами є збереження балансу між відкритістю системи та її захищеністю, а також масштабування рішень за межі країни.

Данія орієнтується на гнучку модель управління, де основний акцент робиться на співпраці держави, бізнесу та суспільства. Діяльність Національного центру з кібербезпеки та Данського центру з кібербезпеки (CSIRT) забезпечує швидке реагування на інциденти та постійний моніторинг ризиків. Особливістю є високий рівень інтеграції кібербезпеки у щоденне функціонування державних структур і приватного сектора. Водночас значним викликом є утримання належного рівня інвестицій у кіберзахист у довгостроковій перспективі та підвищення стійкості суспільства до гібридних загроз.

Литва має більш компактну, але ефективну систему управління інформаційною безпекою. Центральну роль тут відіграє Національний центр кібербезпеки при Міністерстві оборони, який поєднує як превентивні, так і оперативні функції. Перевагою є скоординованість між урядом, бізнесом і міжнародними партнерами, проте виклики полягають у дефіциті людських

ресурсів, потребі постійного оновлення інфраструктури та високій вразливості перед зовнішніми кібератаками.

5. Досліджено розвиток публічного управління інформаційною безпекою електронних послуг в азійських країнах. Публічне управління інформаційною безпекою електронних послуг у Сінгапурі, Південній Кореї та Тайвані характеризується високим рівнем комплексності, системності та стратегічної спрямованості. Ці країни розглядають кібербезпеку не лише як технічне завдання, а як невід'ємну складову національної безпеки, економічної стійкості та довіри громадян до держави.

Сінгапур вирізняється високим ступенем централізації та інтеграції безпеки в державні цифрові програми. Створення Агентства з кібербезпеки Сінгапуру та запуск єдиної системи електронної ідентифікації SingPass забезпечили зручність користування й одночасно контрольовану захищеність. Особливістю є принцип «кібербезпека як фундамент» для стратегії «Розумна нація», що дозволило інтегрувати захист у всі цифрові сервіси. Водночас концентрація інфраструктури створює ризики при масованих атаках.

Південна Корея застосовує багаторівневу модель управління кібербезпекою. Центральне агентство KISA забезпечує координацію, а розгалужена мережа галузевих CERT дозволяє оперативно реагувати на інциденти в різних секторах. Важливою рисою є акцент на інноваціях, залученні приватного сектора та міжнародній співпраці. Система електронної ідентифікації з мобільними рішеннями сприяє швидкому поширенню безпечних цифрових послуг. Водночас динамічний розвиток технологій змушує постійно модернізувати нормативну й технічну базу.

Тайвань демонструє баланс між централізованим стратегічним управлінням і технічними механізмами реагування. Міністерство цифрових справ і його Адміністрація з питань кібербезпеки забезпечують політичну координацію, тоді як TWCERT/CC виконує оперативні функції. Електронна ідентифікація через цифровий сертифікат громадянина і мобільні сертифікати поєднує зручність та безпеку. Значну увагу приділено принципам «безпека за задумом» і «захист

приватності за задумом», що реалізуються через сертифікаційні механізми, аудит і оцінку впливу на дані. Тайвань, перебуваючи в умовах постійного кібертиску, активно розвиває міжнародну співпрацю та кібернавчання, що зміцнює його стійкість.

6. Охарактеризована модернізація публічного управління інформаційною безпекою електронних послуг в США. Публічне управління інформаційною безпекою електронних послуг у США ґрунтується на поєднанні нормативно-правових, організаційних та технологічних механізмів, що дозволяють забезпечувати високу стійкість державних цифрових сервісів до сучасних кіберзагроз. У цій системі ключову роль відіграє поєднання стратегічних документів, законодавчих актів та стандартів, які формують єдиний простір регулювання й практичної реалізації політики безпеки. Президентські виконавчі укази визначають стратегічні пріоритети у сфері кіберзахисту та встановлюють обов’язкові вимоги для федеральних агентств, тоді як Адміністративно-бюджетне управління США координує політику управління інформаційними ресурсами та контролює інтеграцію вимог безпеки у бюджетний процес.

Важливим інструментом є діяльність Національного інституту стандартів і технологій, який розробляє серію спеціальних публікацій, що регламентують вимоги до цифрової ідентичності, управління ризиками, автентифікації та захисту даних. Саме стандарти NIST створюють уніфіковану методологію, яка використовується всіма федеральними структурами, а також приватними підрядниками, що надають послуги уряду. У сфері хмарних обчислень критичним елементом є Федеральна програма управління ризиками та авторизацією (FedRAMP), яка встановлює єдині правила оцінки ризиків та сертифікації хмарних сервісів, забезпечуючи стандартизований рівень захисту й можливість повторного використання результатів авторизації різними агентствами.

Координаційні та оперативні функції зосереджені в Агентстві з кібербезпеки та безпеки інфраструктури, яке відповідає за моніторинг інцидентів, підтримку діяльності національних команд реагування на комп’ютерні інциденти, обмін інформацією про загрози та реагування на масштабні атаки. Своєю чергою

законодавство, зокрема Закон про посилення американської кібербезпеки 2022 року, формалізує вимоги до звітування про інциденти, стандартизує правила роботи з мобільними пристроями й системами та закріплює FedRAMP як обов'язковий елемент політики.

Суттєве значення мають і закони про технологічний трансфер, які створюють умови для співпраці державних лабораторій із приватним сектором, стимулюючи розвиток інноваційних рішень у сфері кіберзахисту. Це забезпечує органічний зв'язок між науково-дослідним середовищем, державними органами та ринком технологій.

7. Визначені 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.

Запропонована модель базується на ідеї взаємодії трьох рівнів управління – стратегічного, тактичного та оперативного – із чітким функціональним поділом відповідальностей і взаємозв'язком між ними. У межах моделі визначено п'ять ключових функціональних блоків (інституційно-координаційний, нормативно-правовий, технологічний, фінансово-ресурсний та соціокомунікаційний), кожен з яких виконує унікальну роль у формуванні кіберстійкої цифрової екосистеми публічного управління.

Узагальнено систему цільових індикаторів ефективності інформаційної безпеки, яка дає змогу кількісно оцінювати досягнення стратегічних цілей у цій сфері. Запропонована логіка взаємозв'язку між блоками управління та індикаторами забезпечує інтеграцію концептуальних засад у практичну площину,

створюючи умови для розробки проєктних рішень, інструментів реалізації та механізмів моніторингу ефективності політики публічного управління ІБ. Сформульовані положення є методологічною основою для подальших етапів дисертаційного дослідження, що дасть змогу верифікувати запропоновану модель, адаптувати її до реального управлінського середовища та розробити практичні механізми її впровадження.

8. Запропоновано запровадження інноваційного управління в систему інформаційної безпеки 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» та «приватності за дизайном», які інтегрують вимоги безпеки у життєвий цикл електронних сервісів від моменту їхнього проєктування. Це забезпечує не лише зменшення ризиків, а й ефективніше використання ресурсів.

Управлінські закономірності вказують на те, що ефективність інформаційної безпеки залежить від балансу між централізованими й децентралізованими моделями управління ризиками, що дозволяє одночасно забезпечувати стратегічну координацію та оперативну гнучкість. Важливим є також швидке оновлення політик і процедур у відповідь на нові загрози, що відображає динаміку сучасного кіберпростору. Прозора система підзвітності, комунікації з громадянами і бізнесом, а також інтеграція публічно-приватних партнерств створюють передумови для зростання рівня довіри та ефективного колективного реагування.

В умовах воєнного й гібридного протистояння, як демонструє досвід України, інноваційне управління неможливе без резервних архітектур, сегментації

критичних реєстрів, планів безперервності та сценаріїв відновлення. Активна міжнародна співпраця, зокрема в межах ЄС, НАТО та через спеціалізовані платформи кіберобміну, підсилює стійкість до атак та забезпечує доступ до найкращих практик. Водночас систематизація стандартів та узгоджене інституційне зміцнення органів кібербезпеки залишається необхідною умовою для підвищення ефективності захисту державних електронних послуг.

Інноваційне управління інформаційною безпекою електронних послуг в умовах цифрової трансформації варто розглядати як динамічну систему, що поєднує технологічні рішення, організаційні структури, нормативно-правові механізми та культуру безпеки. Це управління повинно бути не лише інструментом зниження ризиків, а й фактором забезпечення довіри суспільства до цифрової держави, підвищення її конкурентоспроможності у глобальному середовищі та стійкості в умовах кризових ситуацій. Побудова такої моделі є тривалим процесом, проте саме вона відповідає викликам цифрової епохи і здатна забезпечити сталий розвиток електронних сервісів як основи сучасного публічного управління.

9. 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. Ключовим досягненням є передусім інтеграція інституційного механізму у вигляді Національної ради з питань інформаційної безпеки електронних послуг, яка є центральним координатором у системі управління. Її діяльність забезпечує взаємодію між центральними органами виконавчої влади, регуляторами, адміністраторами реєстрів, національними командами CSIRT та міжнародними партнерами. Такий підхід запобігає дублюванню функцій і фрагментації відповідальності, створюючи єдиний центр прийняття рішень на стратегічному рівні.

Нормативно-правовий механізм у моделі ґрунтується на гармонізації українського законодавства з міжнародними стандартами ISO/IEC 27001, ISO

27005, NIST Рамки кібербезпеки та практиками GDPR. Це дає можливість забезпечити відповідність національної системи управління інформаційною безпекою міжнародним вимогам, спростити інтеграцію до європейського кіберпростору та водночас гарантувати захист персональних даних громадян. 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. Такий підхід забезпечує стабільність і прогнозованість фінансових потоків, дозволяє здійснювати великі інфраструктурні проєкти (наприклад, впровадження SIEM, EDR, резервного копіювання) та стимулює приватний сектор до співпраці з державою у сфері кібербезпеки.

Кадровий механізм моделі передбачає створення професійного кадрового резерву шляхом формування стандартів компетенцій для ключових посад (CISO, адміністратори реєстрів, аналітики 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. Це дозволить знизити кадровий дефіцит та мінімізувати ризики людського фактора.

Контрольний механізм передбачає системну багаторівневу перевірку ефективності заходів із захисту інформації через внутрішні й зовнішні аудити, регулярний моніторинг, індикатори ефективності та механізми санкцій. Використання міжнародного стандарту ISO/IEC 27001 та моделі PDCA дає змогу забезпечити постійне вдосконалення системи, оперативне виявлення відхилень і підвищення рівня довіри до державних електронних послуг. Окреме значення має прозорість у звітуванні, що дозволяє громадянам і міжнародним партнерам оцінювати ефективність публічної політики.

Інформаційно-комунікативний механізм орієнтований на створення довіри до державних електронних сервісів та формування культури кібербезпеки в суспільстві. Він передбачає обов'язкову публічну звітність, інформування користувачів у випадку інцидентів, проведення освітніх та просвітницьких кампаній, а також активний обмін інформацією з міжнародними структурами, зокрема ENISA та CERT-EU. Це забезпечує прозорість, підзвітність і сприяє підвищенню стійкості до загроз.

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. Це дозволяє систематизувати процеси оцінки й мінімізації ризиків, визначати пріоритети у фінансуванні та концентрувати ресурси на найбільш вразливих сегментах. Доповненням виступає механізм управління інцидентами, який ґрунтується на NIST SP 800-61 і передбачає створення CSIRT-структур, уніфіковані протоколи реагування та міжнародний обмін даними про загрози.

Модель механізмів публічного управління інформаційною безпекою електронних послуг формують науково обґрунтовану, практично орієнтовану й комплексну систему управління, яка враховує національні особливості України та водночас інтегрує кращий світовий досвід. Вона створює інституційну, нормативну, фінансову, кадрову, контрольну та комунікаційну основу для підвищення кіберстійкості держави, захисту прав громадян і забезпечення довіри до електронних послуг, закладаючи фундамент для інтеграції України у глобальний простір кібербезпеки.

Запропоновано розробити та прийняти Концепцію розвитку публічного управління інформаційною безпекою електронних послуг на 2026-2036 роки, де передбачається врегулювати зазначену вище модель.

Список використаних джерел

1. Алієв А. А. Особливості цифровізації у сфері публічного управління. *Вчені записки Університету «КРОК»*. 2024. № 2(74). С. 237–243. DOI: https://doi.org/10.31732/2663-2209-2024-74-237-243

2. Андріянов І. О. Адміністративно-правове регулювання надання публічних послуг у рамках адміністративних процедур. *Інвестиції: практика та досвід*. 2024. № 5. С. 197–201. DOI: https://doi.org/10.32702/2306-6814.2024.5.197

3. Архіпова Є. О. Електронне урядування як форма організації публічного управління. *Public Administration and Regional Development.* 2015. August. [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/343399009.

4. Бондар Г. Л. Цифрова трансформація уряду України, відкриті дані (open data) та електронні послуги. *Public Administration and Regional Development*. 2021. № 11. С. 97–123. DOI: https://doi.org/10.34132/pard2021.11.05

5. Бондаренко В. О., Михальчук В. М. Інформаційна безпека держави. *Інвестиції: практика та досвід*. 2021. № 5. С. 95–101. DOI: https://doi.org/10.32702/2306-6814.2021.5.95

6. Борисенко В. Д. Електронне урядування в публічному адмініструванні. *Науковий вісник Ужгородського національного університету. Право*. 2023. Т. 2. Вип. 76. С. 36–40. DOI: https://doi.org/10.24144/2307-3322.2022.76.2.5

7. Бурдяк О., Помазан Л., Гаврилюк І. Роль інфлюенсерів соціальних мереж в забезпеченні ефективності реклами. *Економіка та суспільство*. 2024. № 60. DOI: https://doi.org/10.32782/2524-0072/2024-60-125

8. Бурик З., Івасютин І., Косоногов Д. Диджиталізація в системі публічного управління. *Публічне управління і політика*. 2025. № 2(6). С. 1–10. DOI: https://doi.org/10.70651/3041-2498/2025.2.04

9. Буряк Л. Ф., Ляшенко О. В. Інформаційна безпека в системі публічного управління: системний підхід. Київ: НАДУ, 2020. 212 с.

10. Вальчук О. І. Електронні сервіси в системі публічного управління соціальним страхуванням в Україні. *Публічне управління: удосконалення та розвиток*. 2020. № 5. DOI: https://doi.org/10.32702/2307-2156-2020.5.55

11. Гарфінкель Д. Проривний копірайтинг: як швидко заробити за допомогою написаного слова. [Електронний ресурс]. Режим доступу: https://pdfcoffee.com/garfinkel-david-breakthrough-copywriting-how-to-generate-quick-cash-with-the-written-word-2014-t-3-pdf-free.html.

12. Гасимов Р. А. Електронне урядування як механізм публічного управління та адміністрування: автореф. дис. ... канд. наук з держ. управління: 25.00.02. Київ, 2018. 22 с.

13. Гнатієнко Г. М., Снитюк В. Є. Експертні технології прийняття рішень : монографія. Київ : Маклаут, 2008. 444 с.

14. Гончаренко К. С. Бутафорність трендів та відсутність глобальних перспектив розгубленої сучасності. *Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Релігієзнавство. Культурологія. Філософія.* 2020. Вип. 42. С. 234–240. [Електронний ресурс]. Режим доступу: http://nbuv.gov.ua/UJRN/Nchnpu_7_2020_42_30

15. Грабар Н. С. Інформаційна безпека в умовах становлення глобального інформаційного суспільства. *Державне управління: удосконалення та розвиток.* 2019. № 7. DOI: https://doi.org/10.32702/2307-2156-2019.7.21

16. Гриценко П. І. Досягнення та перспективи цифровізації сфер публічного управління в Україні. *Збірник наукових праць*. 2023. № 4. С. 98–105.

17. Gupta M. P., Jana D. E-government evaluation: a framework and case study. *Government Information Quarterly*. 2003. Vol. 20, № 4. P. 365–387. DOI: https://doi.org/10.1016/j.giq.2003.08.002

18. Дєгтяр О. А. Використання технологій штучного інтелекту у публічному управлінні інформаційною безпекою. *Публічне адміністрування та національна безпека*. 2024. № 3. С. 75-80. DOI: https://doi.org/10.25313/2617-572X-2024-3-9785.

19. Дзюндзюк В. Б., Дзюндзюк Б. В. Публічне управління за допомогою блокчейн-технології та платформ: нові можливості. *Актуальні проблеми публічного*

управління. 2022. № 2(61). С. 104-115. DOI: https://doi.org/10.26565/1684-8489-2022-2-07.

20. Динник І. Законодавче регулювання адміністративних послуг в умовах воєнного стану. *Зовнішня торгівля: економіка, фінанси, право*. 2024. № 3. С. 26–36. DOI: https://doi.org/10.31617/3.2024(134)03

21. Доронін І. М. Національна безпека України в інформаційну епоху: правові аспекти : монографія. Київ : АртЕк, 2019. 434 с.

22. Євтушенко О. Цифровізація - інструмент модернізації публічного управління в Україні. *Публічне адміністрування і регіональний розвиток*. 2024. № 26. С. 1158–1176. DOI: https://doi.org/10.34132/pard2024.26.03

23. Єсімов С. С. Цифрові платформи у контексті надання публічних послуг. *Аналітичне-порівняльне правознавство.* 2024. №4. С. 352-357. [Електронний ресурс]. Режим доступу: http://journal-app.uzhnu.edu.ua/article/view/311011/302303

24. Базові аспекти цифровізації та їх правове забезпечення : монографія / [К. В. Єфремова, Д. І. Шматков, В. П. Кохан та ін.]; за ред. К. В. Єфремової. – Харків: НДІ прав. забезп. інновац. розвитку НАПрН України, 2021. – 180 с. [Електронний ресурс]. Режим доступу: https://ndipzir.org.ua/wp-content/uploads/2021/Tsyfrovizatsiya21/Tsyfrovizatsiya21.pdf

25. Засуха М. В. Сутність цифрової трансформації публічного управління. *Проблеми сучасних трансформацій*. 2024. № 12. DOI: https://doi.org/10.54929/2786-5746-2024-12-02-04

26. Ільницький М. П. Адміністративно-правове регулювання електронного урядування у сфері публічного управління в Україні : автореф. … дис. канд. юрид. наук 12.00.07. Ужгород, 2017. 20 с.

27. Карасаєв С. У., Лікарчук Н. В. Міжнародні аспекти використання інформаційних технологій у державному управлінні. *Міжнародні відносини: теоретико-практичні аспекти*. 2023. № 12. С. 151–163. DOI: https://doi.org/10.31866/2616-745X.12.2023.292411

28. Клімушин П. С. Стратегії та механізми електронного урядування в інформаційному суспільстві : монографія. Харків. Вид-во ХарРІ НАДУ “Магістр”, 2016. 524 с.

29. Пасенко Н.К. Реінжиніринг впливу на інвестиційний потенціал територій на основі реалізації принципів відкритості та прозорості органів влади [Електронний ресурс] // Публічне управління в Україні: історія державотворення, виклики та перспективи: матеріали XI наук. інтернет-конф. за міжнар. участю для аспірантів та докторантів (29 трав. 2020 р.) / ОРІДУ НАДУ при Президентові України. Одеса, 2020. С. 254–257. [Електронний ресурс]. Режим доступу: http://www.oridu.odessa.ua/9/buk/Internet_konf_DU-2020.pdf

30. Pasenko N. K. Current trends in digital transformation of public administration. *Scientific Bulletin of Mukachevo State University. Series «Economics»*. 2022. Vol. 9, № 2. P. 46–51. https://doi.org/10.52566/msu-econ.9(2).2022.46-51

31. Ковбас І. В., Коваль В. О. Поняття, ознаки та сутність адміністративних послуг в Україні. *Юридичний бюлетень*. 2023. № 29. С. 236–243. DOI: https://doi.org/10.32850/lb2414-4207.2023.29.27

32. Ковтун М. С., Моісеєва Є. О., Маркосян В. Г. Проблеми надання електронних послуг в Україні. *Аналітично-порівняльне правознавство*. 2022. № 2. С. 163–167. DOI: https://doi.org/10.24144/2788-6018.2022.02.31

33. Кожушко О. О. Щодо питання адміністративно-правового регулювання надання адміністративних послуг органами місцевого самоврядування. *Актуальні проблеми вітчизняної юриспруденції*. 2023. № 1. С. 125–129. DOI: https://doi.org/10.32782/39221441

34. Котельникова Ю. М. Особливості розвитку електронних послуг в цифровому суспільстві. *Український журнал прикладної економіки та техніки*. 2022. Т. 7, № 3. С. 107–113. DOI: https://doi.org/10.36887/2415-8453-2022-3-15

35. Котляров В. О. Теоретичні засади сутності та концепції інформаційної безпеки. *Наукові перспективи*. 2023. № 6(36). С. 131–142. DOI: https://doi.org/10.52058/2708-7530-2023-6(36)-131-142

36. Красногор О. Публічне управління та адміністрування надання адміністративних послуг населенню в умовах воєнного стану. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. № 9. С. 64–69. DOI: https://doi.org/10.31470/2786-6246-2024-9-64-69

37. Криворучко І. В. Ключові тренди цифровізації публічного управління в контексті євроінтеграції України. *Теорія та практика публічного управління*. 2024. № 2(79). С. 115–135. DOI: https://doi.org/10.26565/1727-6667-2024-2-06

38. Кужда Т., Луциків І., Гевко В. Теоретичні та правові засади організації надання публічних електронних послуг в Україні. *Соціально-економічні проблеми і держава.* 2021. Вип. 2(25). С. 374–384. DOI: https://doi.org/10.33108/sepd2022.02.374

39. Куспляк Г., Куспляк І., Серенок А. Напрями вдосконалення надання адміністративних та публічних електронних послуг в умовах воєнного стану. *Теоретичні та прикладні питання державотворення*. 2023. № 30. С. 103–114. DOI: https://doi.org/10.35432/tisb302023295150

40. Лазарів В.О. Порівняльний аналіз моделей публічного управління інформаційною безпекою: світовий досвід. *Успіхи і досягнення у науці.* 2025. № 4 (14). С. 606 – 615. URL: http://perspectives.pp.ua/index.php/sas/article/view/22944 DOI: https://doi.org/10.52058/3041-1254-2025-4(14)-606-615

41. Лазарів В.О. Кібербезпека та публічне управління: виклики та можливості для електронних послуг. *Актуальні питання у сучасній науці*. 2025. № 1(31). С. 281 – 291. URL: http://perspectives.pp.ua/index.php/sn/article/view/18787 DOI: https://doi.org/10.52058/2786-6300-2025-1(31)-281-291

42. 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. URL: http://perspectives.pp.ua/index.php/sn/article/view/16517 DOI: https://doi.org/10.52058/2786-6300-2024-11(29)-378-388

43. Лазарів В.О. Концептуальні засади публічного управління інформаційною безпекою електронних послуг: теорія та виклики. *Наукові*

перспективи. 2023. № 6(36). С. 149 – 150. URL: http://perspectives.pp.ua/index.php/np/issue/view/156 DOI: https://doi.org/10.52058/2708-7530-2023-6(36)-143-150

44. 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. [Електронний ресурс]. Режим доступу: https://www.eoss-conf.com/arkhiv/from-ideas-to-solutions-innovations-in-science-and-technology-21-04-25/

45. 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. [Електронний ресурс]. Режим доступу: https://kntu.net.ua/ukr/content/download/127190/707962/file/Збірник_тез_доповідей_ХНТУ_2025.pdf

46. 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. [Електронний ресурс]. Режим доступу: https://www.eoss-conf.com/arkhiv/modern-scientific-research-theoretical-and-practical-aspects/

47. 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. [Електронний ресурс]. Режим доступу: http://www.konferenciaonline.org.ua/data/downloads/file_1740428622.pdf

48. 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. [Електронний ресурс]. Режим доступу: https://www.eoss-conf.com/wp-content/uploads/2024/12/San_Francisco_USA_23.12.2024.pdf

49. 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. [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/372438666_NAUKOVA_INTEGRACIA_V_UMOVAH_GLOBALNIH_VIKLIKIV_Zbirnik_tez_dopovidej_IV_MIZNARODNOI_MULTIDISCIPLINARNOI_NAUKOVO-PRAKTICNOI_KONFERENCII

50. 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. [Електронний ресурс]. Режим доступу: http://perspectives.pp.ua/public/site/conferency/conf-26.pdf

51. Лонська В. Г. Публічне управління у сфері інформаційної безпеки держави: кваліфікаційна робота магістра. Житомир : Поліс. нац. ун-т, 2023. 49 с. [Електронний ресурс]. Режим доступу: https://ir.polissiauniver.edu.ua/bitstream/123456789/15347/1/Lonska_VG_KR_281_2023.pdf

52. Майстренко К. М. Комунікації у діяльності органів публічної влади. *Публічне урядування*. 2022. Вип.1(29). С. 93–98. DOI: https://doi.org/10.32689/2617-2224-2022-1(29)-13

53. Маматова Т., Чикаренко І., Бородін, Є. Цифрові платформи Smart Specialisation Platform та ESPON: структура та можливості для регіонів і громад ЄС. Аспекти публічного управління. 2022. Т. 10, № 6. С. 37-45. DOI: https://doi.org/10.15421/152242

54. Маматова Т., Борисенко Ю. Цифрове врядування: сучасні світові тренди та особливості розвитку в Україні . Публічне управління та місцеве самоврядування, 2024. № 2. С. 46-53. DOI: https://doi.org/10.32782/2414-4436/2024-2-6

55. Матюшенко І., Глібко С., Ханова О., Коритін Д. Оцінка впливу цифровізації на розвиток бізнесу в країнах ЄС та Україні. *Право та інноваційне суспільство*. 2023. № 1(20). С. 42–64. DOI: https://doi.org/10.37772/2309-9275-2023-1(20)-4

56. Мгалоблішвілі А. Профілактика залежності від соціальних мереж у молоді : психологічні рекомендації. *Вісник Національного університету оборони України*. 2024. № 1(77). С. 102–112. DOI: https://doi.org/10.33099/2617-6858-2024-77-1-102-112

57. Нагорняк М. М. Інформаційна безпека у системі публічного управління : виклики та перспективи. *Дніпровський науковий часопис публічного управління, психології, права. 2024. № 1. С. 64–68*. DOI: https://doi.org/10.51547/ppp.dp.ua/2024.1.10

58. Нагорняк М. М. Стратегії публічного управління протидії кіберзагрозам у сфері надання електронних послуг: практики та рекомендації. *Публічне адміністрування та національна безпека*. 2024. № 3. С. 81-85. DOI: https://doi.org/10.25313/2617-572X-2024-3-9751

59. Наджафлі Е. До питання про систему принципів наукового пізнання дигіталізації державної влади. *Право і безпека*. 2021. № 4. С. 191–196. [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/360863453.

60. Нестеренко Г. Інформаційна безпека : курс лекцій. Київ : НАУ, 2022. 102 с. [Електронний ресурс]. Режим доступу: https://er.nau.edu.ua/handle/NAU/57731

61. Новосад Р. В. Правові основи надання електронних послуг в Україні. *Таврійський науковий вісник. Публічне управління та адміністрування*. 2024. № 1. С. 46–54. DOI: https://doi.org/10.32782/tnv-pub.2024.1.6

62. Оболенський О. Ю. Публічне управління в інформаційному суспільстві. Київ: КНЕУ, 2019. 356 с.

63. Опар Н. В. Теоретичні основи надання електронних послуг в Україні. *Публічне управління: удосконалення та розвиток*. 2021. № 6. DOI: https://doi.org/10.32702/2307-2156-2021.6.33

64. Орлова Н. С., Лукашук М. В. Стратегія сучасного розвитку України: синтез правових, освітніх та економічних механізмів : колективна монографія. Чернігів : Наук-освіт. інновац. центр сусп. трансформацій, 2022. 283 с.

65. Панченко О. А. Публічне управління інформаційною безпекою в епоху турбулентності : дис. ... д-ра наук з держ. упр. Харків, 2020. 450 с. [Електронний ресурс]. Режим доступу: https://nuczu.edu.ua/images/topmenu/science/spetsializovani-vcheni-rady/disPanchenko.pdf, (документ також доступний за адресою: https://uacademic.info/ua/document/0520U101637) (дата звернення: 04.11.2025).

66. Пархоменко-Куцевіл О. І. Запровадження цифровізації у процес забезпечення якості публічних послуг. *Наукові інновації та передові технології. Управління та адміністрування*. 2024. № 2(30). С. 235–245. DOI: https://doi.org/10.52058/2786-5274-2024-2(30)-235-245

67. Покатаєв П. С., Арутюнян В. Е. Теорії та моделі ефективності ІТ у державному управлінні. *Менеджмент і підприємництво: тренди розвитку*. 2024. № 1(27). С. 119–125. DOI: https://doi.org/10.26661/2522-1566/2024-1/27-10

68. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

69. Пучков О. О. Правопорядок у сфері національної безпеки сучасної України : монографія. Київ : Гельветика, 2019. 208 с.

70. П’ятничук І. Д. Публічне управління наданням електронних послуг: аналіз ефективності та напрямки подальших покращень. *Успіхи і досягнення у*

науці. 2024. № 4(4). С. 522-533. DOI: https://doi.org/10.52058/3041-1254-2024-4(4)-522-533.

71. П'ятничук І. Д. Нормативно-правовий механізми публічного управління процесами захисту інформаційної безпеки у сфері надання електронних послуг. *Наукові перспективи*. 2024. № 4 (46). С. 361-370. DOI: https://doi.org/10.52058/2708-7530-2024-4(46)-361-370.

72. Риженко І. М. Публічне адміністрування адміністративних послуг в Україні: правовий аналіз. *Таврійський науковий вісник. Публічне управління та адміністрування*. 2021. № 3. С. 109–115. DOI: https://doi.org/10.32851/tnv-pub.2021.3.15

73. Рішення Ради національної безпеки і оборони України від 15 жовт. 2021 р. «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 р. № 685/2021. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

74. Рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text

75. Саприкін В. Оцифровування, цифровізація та цифрова трансформація публічного управління в Україні. *Вісник Київського національного університету імені Тараса Шевченка. Публічне управління*. 2024. № 19(1). С. 116–121. DOI: https://doi.org/10.17721/2616-9193.2024/19-19/22

76. Сердюк І.А. Організаційні засади публічного управління інформаційною безпекою суспільства в умовах загроз ментальному здоров'ю: дис. ... канд. юрид. наук: 25.00.05. Київ, 2023. 256 с. [Електронний ресурс]. Режим доступу: https://maup.com.ua/assets/files/dis/serdyuk/serdyuk-disertaciya.pdf

77. Сидоренко Н. О. Діджиталізація: електронні адміністративні послуги. *Дніпровський науковий часопис публічного управління, психології, права*. 2021. № 4. С. 11–15. DOI: https://doi.org/10.51547/ppp.dp.ua/2021.4.2

78. Сільва Ж. М., Рібейро Д., Рамос Л. Ф., Фонте В. Глобальний огляд стану інформаційної безпеки онлайн-публічних послуг. *Cryptography and Security*. 2023. DOI: https://doi.org/10.48550/arXiv.2310.01200

79. Скляр І. В. Механізми публічного управління в контексті цифровізації: теоретичний аспект. *Дніпровський науковий часопис публічного управління, психології, права*. 2023. № 6. С. 265–271. DOI: https://doi.org/10.51547/ppp.dp.ua/2023.6.45

80. Скляр І. Особливості розвитку цифрового врядування в умовах воєнного стану. *Аспекти публічного управління*. 2024. № 12(4). С. 59–66. DOI: https://doi.org/10.15421/152449

81. Spytska L. E-government in Ukraine and the world: A comparative legal analysis. Social Legal Studios. 2024. Vol. 7, № 2. P. 36–43. DOI: https://doi.org/10.32518/sals2.2024.36

82. Соловйова О. М., Ковальчук Д. Р., Кундій А. Ю. Адміністративні послуги в умовах воєнного стану в Україні. *Юридичний науковий електронний журнал*. 2022. № 5. С. 421–424. DOI: https://doi.org/10.32782/2524-0374/2022-5/99

83. Соломаха А. Г. Роль та значення адміністративних процедур стосовно отримання статусу внутрішньо переміщеної особи та біженця в умовах воєнного стану та у післявоєнний період. *Економіка. Фінанси. Право*. 2023. № 7. С. 91–95. DOI: https://doi.org/10.37634/efp.2023.7.19

84. Сурай А. Цифровізація публічного управління в Україні: організаційний аспект. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. № 7. С. 116–124. DOI: https://doi.org/10.31470/2786-6246-2024-7-116-124

85. Тищенкова І. О. Електронні послуги у діяльності публічної адміністрації України: монографія. Дніпро: ДДУВС, 2017. 156 с. [Електронний ресурс]. Режим доступу: http://er.dduvs.edu.ua/handle/123456789/935

86. Тюхтій М., Ющенко М. Виклики та перспективи надання адміністративних послуг у сфері реєстрації актів цивільного стану в умовах воєнного стану в Україні. *Теоретичні та прикладні питання державотворення.* 2023. № 30. С. 57–66. DOI: https://doi.org/10.35432/tisb302023295032

87. Угоднікова О. І. Інформаційно-комунікаційний механізм публічного маркетингу у сфері обслуговування. *Публічне адміністрування та національна безпека*. 2023. № 6. С. 94-100. DOI: https://doi.org/10.25313/2617-572X-2023-6-9064

88. Чечель А., Ангелін М. Стратегічні цифрові технології у публічному секторі України. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. № 9. С. 176–185. DOI: https://doi.org/10.31470/2786-6246-2024-9-176-185

89. Чміль Г. Л., Новаківський К. А., Демидова В. А. Моніторинг аудиторії соціальних мереж в Україні. *Економіка та суспільство*. 2024. № 63. DOI: https://doi.org/10.32782/2524-0072/2024-63-129

90. Чмир Я. І. Проблеми забезпечення інформаційної безпеки в системі публічного управління. *Аспекти публічного управління*. 2018. Т. 6, № 9. С. 16–22. [Електронний ресурс]. Режим доступу: https://aspects.org.ua/index.php/journal/article/download/442/435

91. Чукут С., Карпенко Є. Організація надання електронних послуг в Україні в умовах війни. *Public Administration and Regional Development.* № 20. С. 589–613. DOI: https://doi.org/10.34132/pard2023.20.14

92. Шандрук С. М. Адміністративні послуги як функція сервісно-орієнтованої держави. *Науковий вісник Ужгородського національного університету*. 2024. № 85. С. 175–180. DOI: https://doi.org/10.24144/2307-3322.2024.85.3.27

93. Шийович С. Я. Публічні послуги: теоретико-правові аспекти. *Аналітичне-порівняльне правознавство*. 2023. №1. С. 431-435. DOI https://doi.org/10.24144/2788-6018.2023.01.74

94. Шопіна І. М. Проблеми розвитку електронних публічних послуг у сфері освіти. *Академічні візії.* 2024. № 30. DOI: https://doi.org/10.5281/zenodo.10978140

95. Щербина Є. М. Характеристика процедури надання електронних послуг в системі публічних послуг в Україні. *Дніпровський науковий часопис публічного управління, психології, права*. 2022. № 4. С. 185–189. DOI: https://doi.org/10.51547/ppp.dp.ua/2022.4.28

96. Щодо захисту персональних даних в умовах воєнного стану. https://ombudsman.gov.ua/storage/app/media/%D0%92%D0%BE%D1%94%D0%BD%D0%BD%D0%B8%D0%B9%20%D1%81%D1%82%D0%B0%D0%BD/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85%20%D0%B4%D0%B0%D0%BD%D0%B8%D1%85/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85%20%D0%B4%D0%B0%D0%BD%D0%B8%D1%85%20%D0%B2%20%D1%83%D0%BC%D0%BE%D0%B2%D0%B0%D1%85%20%D0%B2%D0%BE%D1%94%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE%20%D1%81%D1%82%D0%B0%D0%BD%D1%83.pdf?utm.com

97. Achieving Cyber Security Resilience of Public Sector IT Systems and Services. [Електронний ресурс]. Режим доступу: https://oecd-opsi.org/innovations/cyber-security-resilience/?utm.com

98. Act on promotion of information and communications network utilization and information protection. [Електронний ресурс]. Режим доступу: https://www.law.go.kr/LSW/lsInfoP.do?chrClsCd=010203&lsiSeq=58583&urlMode=engLsInfoR&viewCls=engLsInfoR&utm.com#0000

99. Administration for Cyber Security, MODA. [Електронний ресурс]. Режим доступу: https://moda.gov.tw/en/ACS/?utm.com

100. Advisory Guidelines on Key Concepts in the Personal Data Protection Act. [Електронний ресурс]. Режим доступу: https://www.pdpc.gov.sg/guidelines-and-consultation/2020/03/advisory-guidelines-on-key-concepts-in-the-personal-data-protection-act?utm.com

101. An Act Making consolidated appropriations for the fiscal year ending September 30, 2022, and for providing emergency assistance for the situation in Ukraine, and for other purposes. [Електронний ресурс]. Режим доступу: https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf?utm.com

102. Attacks On Ukraine's Electricity Infrastructure Threaten Key Aspects of Life As Winter Approaches – UN Human Rights Monitors Say. [Електронний ресурс]. Режим доступу: https://ukraine.un.org/en/278995-attacks-ukraine%E2%80%99s-electricity-infrastructure-threaten-key-aspects-life-winter-approaches-%E2%80%93?utmgpt.com

103. Awoleye O. M., Ojuloge B., Ilori M. O. Web application vulnerability assessment and policy direction towards a secure smart government. *Government Information Quarterly*. 2014. Vol. 31. P. S118–S125. DOI: https://doi.org/10.1016/j.giq.2014.01.012

104. Centre for Cyber Security. [Електронний ресурс]. Режим доступу: https://www.cfcs.dk/en/?utm.com

105. CERT-UA минулого року опрацювала 4315 кіберінцидентів. [Електронний ресурс]. Режим доступу: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv

106. Singh C., Jain A. K. A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network. *e-Prime - Advances in Electrical Engineering, Electronics and Energy.* 2024. Volume 8. 100543, DOI: https://doi.org/10.1016/j.prime.2024.100543

107. CISA. [Електронний ресурс]. Режим доступу: https://www.cisa.gov/about?utm.com

108. Cisco to establish cybersecurity centre in Taiwan. [Електронний ресурс]. Режим доступу: https://www.reuters.com/technology/cybersecurity/cisco-establish-cybersecurity-centre-taiwan-2024-06-17/?utm.com

109. CRADAs - Cooperative Research & Development Agreements. [Електронний ресурс]. Режим доступу: https://www.doi.gov/techtransfer/crada?utm.com

110. CSIRT. CFCS is the Danish CSIRT and represents Denmark in the European CSIRT network. [Електронний ресурс]. Режим доступу: https://www.cfcs.dk/en/about-us/csirt/?utm.com

111. Culot Giovanna, Guido Nassimbeni, Matteo Podrecca, Marco Sartor. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*. 17 December 2021; 33 (7): 76–105. DOI: https://doi.org/10.1108/TQM-09-2020-0202

112. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). [Електронний ресурс]. Режим доступу: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia?utm.com

113. Cyber security. [Електронний ресурс]. Режим доступу: https://e-estonia.com/solutions/cyber-security/ksi-blockchain/?utm.com

114. Cyber Security Management Act (Taiwan). [Електронний ресурс]. Режим доступу: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297&utm.com

115. Cyber Security Policies and Regulations. [Електронний ресурс]. Режим доступу: https://moda.gov.tw/en/ACS/operations/policies-and-regulations/648?utm.com

116. Cybersecurity Act 2018 - Singapore Statutes Online. *Government gazette*. 2018. № 9. [Електронний ресурс]. Режим доступу: https://sso.agc.gov.sg/Acts-Supp/9-2018/

117. Cybersecurity Act. Passed 09.05.2018. [Електронний ресурс]. Режим доступу: https://www.riigiteataja.ee/en/eli/523052018003/consolide?utm.com

118. Cybersecurity Act (Singapore). [Електронний ресурс]. Режим доступу: https://www.csa.gov.sg/legislation/cybersecurity-act?utm.com

119. Das IT-Sicherheitsgesetz 2.0 tritt in Kraft – Überblick über die wichtigsten Änderungen des BSI-Gesetzes. [Електронний ресурс]. Режим доступу: https://www.twobirds.com/de/insights/2021/germany/the-german-it-security-act-2-0-comes-into-force?utm.com

120. Das Onlinezugangsgesetz (OZG). [Електронний ресурс]. Режим доступу: https://www.bmi.bund.de/DE/themen/moderne-

verwaltung/verwaltungsmodernisierung/onlinezugangsgesetz/onlinezugangsgesetz-artikel.html?utm.com

121. Deepak Sharma, Ruchi Mittal, Ravi Sekhar, Pritesh Shah, Matthias Renz. A bibliometric analysis of cyber security and cyber forensics research. *Results in Control and Optimization*. 2023. Vol. 10. 100204. DOI: https://doi.org/10.1016/j.rico.2023.100204.

122. Denmark's Sector Responsibility Principle: A Tedious Cyber Resilience Strategy. [Електронний ресурс]. Режим доступу: https://www.acigjournal.com/pdf-190789-124469?filename=Denmark_s+Sector.pdf&utm.com

123. Digital government blueprint «A Singapore government that is digital to the core, and serves with heart». [Електронний ресурс]. Режим доступу: https://isomer-user-content.by.gov.sg/85/f4e1b24e-42b4-4f8d-98a4-9dbc64817ff6/dgb-public-document_30dec20.pdf?utm.com

124. Digital Government Masterplan 2021-2025 of the Republic of Korea. [Електронний ресурс]. Режим доступу: https://thedocs.worldbank.org/en/doc/1004f032e05fa60826a1d4f7760168f6-0350052022/original/-GovTech-Talks-01-Digital-Government-Masterplan-2021-2025.pdf?utm.com

125. Digital Post is a part of the cross-governmental digital service infrastructure in Denmark. [Електронний ресурс]. Режим доступу: https://en.digst.dk/systems/digital-post/?utm.com

126. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). [Електронний ресурс]. Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32022L2555&utm.com

127. DoD Information Security Program: Overview, Classification, and Declassification. DoDM 5200.01-V1. 2012. February 24. [Електронний ресурс]. Режим доступу:

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001m_vol1.pdf?ver=2020-08-04-092500-203

128. E-Government Development Index (EGDI). [Електронний ресурс]. Режим доступу: https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index?utm.com

129. eIDAS Regulation. [Електронний ресурс]. Режим доступу: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

130. Elektroniniai valdžios vartai. [Електронний ресурс]. Режим доступу: https://www.epaslaugos.lt/portal/?utm.com

131. Enforcement Rules of Cyber Security Management Act. [Електронний ресурс]. Режим доступу: https://law.moda.gov.tw/EngLawContent.aspx?id=31&lan=E&utm.com

132. Effortlessly Embrace Digital Living! Mobile Citizen Digital Certificate Makes Tax Filing, Payments, and Identity Verification a Breeze. [Електронний ресурс]. Режим доступу: https://news.immigration.gov.tw/NewsSection/Detail/d9cabc5a-67e3-4445-86d2-195deda09f1d?category=0&lang=EN&utm.com

133. ENISA: 2020 report on csirtle cooperation. A study of the roles and synergies among selected EU Member States/EFTA countries. [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20on%20CSIRT-LE%20Cooperation%20-%20A%20study%20of%20the%20roles%20and%20synergies%20among%20selected%20countries.pdf

134. ENISA: Best Practices for Cyber Crisis Management. [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management?utm.com#contentList

135. European eGovernment Benchmark 2023: Lithuania Ranks 7th. [Електронний ресурс]. Режим доступу: https://lithuania.lt/governance-in-lithuania/european-egovernment-benchmark-2023-lithuania-ranks-7th/?utm.com

136. Executive Order on Improving the Nation's Cybersecurity. [Електронний ресурс]. Режим доступу: https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity?utm.com

137. Federal Information Security Modernization Act. [Електронний ресурс]. Режим доступу: https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act?utm.com

138. FedRAMP provides a standardized, reusable approach to security assessment and authorization for cloud service offerings. [Електронний ресурс]. Режим доступу: https://www.fedramp.gov/?utm.com

139. Frameworks and blueprints shaping Singapore's Smart Nation vision. [Електронний ресурс]. Режим доступу: https://www.smartnation.gov.sg/publications/frameworks-and-blueprints?utm.com

140. Bélanger F., Carter L. Trust and risk in e-government adoption. The Journal of Strategic Information Systems. 2008. Vol. 17, № 2. P. 165–176. DOI: https://doi.org/10.1016/j.jsis.2007.12.002

141. Frandell A., Feeney M. Cybersecurity Threats in Local Government: A Sociotechnical Perspective. The American Review of Public Administration. 2022. № 52(8). P. 558-572. DOI: https://doi.org/10.1177/02750740221125432

142. Baxter G., Sommerville I. Socio-technical systems: From design methods to systems engineering. Interacting with Computers. 2011. Vol. 23, №1. P. 4–17. DOI: https://doi.org/10.1016/j.intcom.2010.07.003.

143. GovMesh Digest: South Korea boosts public-private synergy using Open Digital Services. [Електронний ресурс]. Режим доступу: https://govinsider.asia/intl-en/article/govmesh-digest-south-korea-boosts-public-private-synergy-using-open-digital-services?utm.com

144. Guide on Article 15 of the European Convention on Human Rights. Derogation in time of emergency. [Електронний ресурс]. Режим доступу: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_15_eng?utm.com

145. Guide to Basic Protection based on IT-Grundschutz 3 Steps to Information Security. [Електронний ресурс]. Режим доступу:

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/Basic_Security.pdf?__blob=publicationFile&v=2&utm.com

146. Guembe B., Misra S., Azeta A. et al. Bibliometric analysis of artificial intelligence cyberattack detection models. *Artificial Intelligence Review.* 2025. Vol. 58, №6. Article number 177. DOI: https://doi.org/10.1007/s10462-025-11167-0

147. H.R.3773 - Federal Technology Transfer Act of 1986. [Електронний ресурс]. Режим доступу: https://www.congress.gov/bill/99th-congress/house-bill/3773?utm.com

148. Heeks R. Understanding e-Governance for Development. S*SRN Electronic Journal.* 2001. [Електронний ресурс]. Режим доступу: https://ssrn.com/abstract=3540058 or http://dx.doi.org/10.2139/ssrn.3540058

149. Zhang H., Tang Z., Jayakar K. A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services. *Telecommunications Policy.* Vol. 42, Issue 5. 2018. P. 409-420. DOI: https://doi.org/10.1016/j.telpol.2018.02.004.

150. Lindgren I., Jansson G. Electronic services in the public sector: A conceptual framework. *Government Information Quarterly*. 2013. Vol. 30, №. 2. P. 163–172. DOI: https://doi.org/10.1016/j.giq.2012.10.005.

151. Improving the Nation's Cybersecurity: NIST’s Responsibilities Under the May 2021 Executive Order. [Електронний ресурс]. Режим доступу: https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity?utm.com

152. ISACs are member-driven organizations, delivering all-hazards threat and mitigation information to asset owners and operators. [Електронний ресурс]. Режим доступу: https://www.nationalisacs.org/?utm.com

153. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements 2022. [Електронний ресурс]. Режим доступу: https://www.iso.org/standard/27001?utm.com.

154. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls 2022. [Електронний ресурс]. Режим доступу: https://www.iso.org/standard/75652.html.

155. IT-Sicherheitsgesetz 2.0: Was Betreiber kritischer Infrastrukturen jetzt wissen müssen. [Електронний ресурс]. Режим доступу: https://www.pwc.de/de/cyber-security/it-sicherheitsgesetz-2-0-ein-paukenschlag-nicht-nur-fuer-kritis-betreiber.html?utm.com

156. Twizeyimana J. D., Andersson A. The public value of E-Government – A literature review. *Government Information Quarterly*. 2019. Vol. 36, №. 2. P. 167–178. DOI: https://doi.org/10.1016/j.giq.2019.01.001.

157. Layne K., Lee J. Developing fully functional E-government: A four stage model. *Government Information Quarterly*. 2001. Vol. 18, №2. P. 122–136. DOI: https://doi.org/10.1016/S0740-624X(01)00066-1.

158. Parsons K., Calic D., Pattinson M., Butavicius M., McCormac A., Zwaans T. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*. 2017. Vol. 66. P. 40-51. DOI: https://doi.org/10.1016/j.cose.2017.01.004.

159. Keeping our cyberspace safe & secure. [Електронний ресурс]. Режим доступу: https://www.csa.gov.sg/?utm.com

160. KISA. [Електронний ресурс]. Режим доступу: https://www.kisa.or.kr/EN?utm.com

161. KISA boosts IoT security certification to enhance device safety and privacy in Korea. [Електронний ресурс]. Режим доступу: https://biz.chosun.com/en/en-it/2025/06/29/7C5FIS3OUZGZZALZJEUE7VXTKA/?utm.com

162. Kompella L. E-Governance systems as socio-technical transitions using multi-level perspective with case studies. *Technological Forecasting and Social Change*. 2017. Vol. 123. P. 80–94. DOI: https://doi.org/10.1016/j.techfore.2017.06.024.

163. Lysenko A., Gunitsky S. The invisible front: Ukraine's IT army and the evolution of cyber resistance. *Post-Soviet Affairs*. 2025. № 41(4). P. 263–288. DOI: https://doi.org/10.1080/1060586X.2025.2503658

164. Malatji M., Marnewick A., von Solms S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. *Computers and Security*. 2010. № 95. Article 101846. DOI: https://doi.org/10.1016/j.cose.2020.101846

165. Mannat Kaur, Michel van Eeten, Marijn Janssen, Kevin Borgolte, Tobias Fiebig. Human Factors in Security Research: Lessons Learned from 2008-2018. [Електронний ресурс]. Режим доступу: https://arxiv.org/abs/2103.13287?utm.com

166. Marijn Janssen, George Kuk, René W. Wagenaar. A survey of Web-based business models for e-government in the Netherlands. *Government Information Quarterly.* 2008. Vol. 25, Issue 2. P. 202-220. DOI: https://doi.org/10.1016/j.giq.2007.06.005.

167. Podrecca M., Culot G., Nassimbeni G., Sartor M. Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*. 2022. Vol. 142. 103744. DOI: https://doi.org/10.1016/j.compind.2022.103744.

168. MitID (the Danish National eID) is Denmark's digital ID that residents will use to access their public self-service solutions. [Електронний ресурс]. Режим доступу: https://en.digst.dk/systems/mitid/?utm.com

169. Mobile-ID – a mobile identification document always within your reach. [Електронний ресурс]. Режим доступу: https://www.mobile-id.lt/en/?utm.com

170. National Cyber Security Centre (NCSC) – Lithuania. [Електронний ресурс]. Режим доступу: https://cybersecurity-centre.europa.eu/lithuania-ncc_en?utm.com

171. National Cybersecurity Governance: UKRAINE. [Електронний ресурс]. Режим доступу: https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf?utm.com

172. National Cybersecurity Organisation: REPUBLIC OF KOREA. [Електронний ресурс]. Режим доступу: https://ccdcoe.org/uploads/2022/12/ROK-Country-report.pdf?utm.com

173. National Cybersecurity Strategy (Republic of Korea). [Електронний ресурс]. Режим доступу: https://www.itu.int/en/ITU-

D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf?utm.com

174. National Cybersecurity Strategies Guidelines & tools. [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/national-cybersecurity-strategies-0/national-cybersecurity?utm.com - contentList

175. National Information and Communications Security Strategy 2025 - Information Security is National Security. [Електронний ресурс]. Режим доступу: https://www.president.gov.tw/Page/317/1870?utm.com

176. National Technology Transfer and Advancement Act of 1995. [Електронний ресурс]. Режим доступу: https://www.nist.gov/standardsgov/national-technology-transfer-and-advancement-act-1995?utm.com

177. NATO: Cyber defence. [Електронний ресурс]. Режим доступу: https://www.nato.int/cps/en/natohq/topics_78170.htm?utm.com

178. NemKonto (the Danish National Account Register) makes it easier for public authorities to make payments to both people and companies, in an easy and secure way. [Електронний ресурс]. Режим доступу: https://en.digst.dk/systems/nemkonto/

179. NIST SP 800-34 Rev. 1. Contingency Planning Guide for Federal Information Systems. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final?utm.com

180. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments. Gaithersburg, MD: National Institute of Standards and Technology, 2012. 95 p. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

181. NIS2 Implementation in the EU. Lithuania. [Електронний ресурс]. Режим доступу: https://www.lexmundi.com/guides/status-of-the-nis2-implementation-act-in-the-european-union/jurisdictions/europe/lithuania/?utm.com

182. NKSC. [Електронний ресурс]. Режим доступу: https://nksc.lrv.lt/en/?utm.com

183. NKSC/CERT-LT. [Електронний ресурс]. Режим доступу: https://www.first.org/members/teams/nksc-cert-lt?utm.com

184. OECD: The e-Government Imperative. [Електронний ресурс]. Режим доступу: https://www.oecd.org/content/dam/oecd/en/publications/reports/2003/07/the-e-government-imperative_g1gh3444/9789264101197-en.pdf?utm.com

185. OECD: The E-Leaders Handbook on the Governance of Digital Government. [Електронний ресурс]. Режим доступу: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/12/the-e-leaders-handbook-on-the-governance-of-digital-government_2523ea2c/ac7f2531-en.pdf?utm.com

186. Pardo T.A., Nam T., Burke G.B. E-Government Interoperability: Interaction of Policy, Management, and Technology Dimensions. *Social Science Computer Review*. 2011. № 30(1). P. 7-23. DOI: https://doi.org/10.1177/0894439310392184

187. Kivimaa P., Brisbois M. C., Jayaram D., Hakala E., Siddi M. A socio-technical lens on security in sustainability transitions: Future expectations for positive and negative security. *Futures*. 2022. Vol. 141. 102971. DOI: https://doi.org/10.1016/j.futures.2022.102971.

188. Personal information protection Act. [Електронний ресурс]. Режим доступу: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG&utm.com

189. Pollini A., Callari T.C., Tedeschi A., Ruscio D., Save L., Chiarugi F., Guerri D. Leveraging human factors in cybersecurity: an integrated methodological approach. *Cogn Technol Work*. 2022. 24(2). 371-390. DOI: 10.1007/s10111-021-00683-y.

190. Ifinedo P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*. 2012. Vol. 31, № 1. P. 83–95. DOI: 10.1016/j.cose.2011.10.007.

191. Public Administration and Management: modern scientific discussions: collective monograph. Riga, Latvia: Baltija Publishing, 2020. 293 p. [Електронний ресурс]. Режим доступу: https://financial.lnu.edu.ua/course/natsionalna-bezpeka-v-publichnomu-upravlinni-2

192. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [Електронний ресурс]. Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016R0679&utm.com

193. Regulation (EU) № 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. [Електронний ресурс]. Режим доступу: https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng

194. Report on Cyber Lessons Learned during the War in Ukraine. [Електронний ресурс]. Режим доступу: https://nsarchive.gwu.edu/media/31762/ocr?utm.com

195. Results Summary Extended Narrative (2023 End of Year). Ukraine. [Електронний ресурс]. Режим доступу: https://www.unicef.org/media/152211/file/Ukraine-2023-COAR.pdf?utm.com

196. Revision of OMB Circular No. A-130, "Managing Information as a Strategic Resource". [Електронний ресурс]. Режим доступу: https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource

197. Riigi Infosüsteemi Amet (RIA). [Електронний ресурс]. Режим доступу: https://www.ria.ee/en?utm.com

198. Ribeiro, D., Fonte, V., Ramos, L. F., & Silva, J. M. Assessing the information security posture of online public services worldwide: Technical insights, trends, and olicy implications. *Government Information Quarterly*. 2025. Vol. 42. Issue 2. 102031. DOI: https://doi.org/10.1016/j.giq.2025.102031.

199. ROCA Vulnerability and eID: Lessons Learned. [Електронний ресурс]. Режим доступу: https://www.ria.ee/sites/default/files/documents/2022-11/Roca-vulnerability-and-eID-lessons-learned-2018.pdf?utm.com

200. S.1250 - Stevenson Wydler Technology Innovation Act of 1980. [Електронний ресурс]. Режим доступу: https://www.congress.gov/bill/96th-congress/senate-bill/1250/text?utm.com

201. S.3600 - Strengthening American Cybersecurity Act of 2022. [Електронний ресурс]. Режим доступу: https://www.congress.gov/bill/117th-congress/senate-bill/3600/text?utm.com

202. S.3099 - Federal Secure Cloud Improvement and Jobs Act of 2021. [Електронний ресурс]. Режим доступу: https://www.congress.gov/bill/117th-congress/senate-bill/3099/text?utm.com

203. AlHidaifi S. M., Asghar M. R., Ansari I. S. A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions. *ACM Computing Surveys*. 2024. Vol. 56. Issue 8. Article No.: 196, P. 1-48. DOI: https://doi.org/10.1145/3649218

204. Secure and Convenient "Mobile ID" Made Available to Overseas Koreans. [Електронний ресурс]. Режим доступу: https://www.mois.go.kr/eng/bbs/type001/commonSelectBoardArticle.do%3Bjsessionid%3DUK%2BmcR4QmdVjF01uMAxLqwnu.node10?bbsId=BBSMSTR_000000000019&nttId=110874&utm.com

205. Shannon C. E. A Mathematical Theory of Communication. *The Bell System Technical Journal*. July, October, 1948. Vol. 27, pp. 379–423, 623–656. [Електронний ресурс]. Режим доступу: https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf

206. Shettar I., Hadagali G.S., Kaddipujar M., Bulla S.D., Agadi K., Ganjihal G.A., Hiremath R., Dundannanavar A., Babu B. R. Scientometric analysis of global cyber security research output based on Web of Science. *Iberoamerican Journal of Science Measurement and Communication*. 2024. № 4(2). P. 1–15. DOI: https://doi.org/10.47909/ijsmc.129

207. Sieriebriak S. V. Public-private partnership in the field of cybersecurity. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. № 6. P. 351–356. DOI: https://doi.org/10.24144/2788-6018.2024.06.57

208. Smart-ID – smart way to identify yourself. [Електронний ресурс]. Режим доступу: https://www.smart-id.com/?utm.com

209. Smart Nation 2.0. A Thriving Digital Future for All. [Електронний ресурс]. Режим доступу: https://file.go.gov.sg/smartnation2-report.pdf?utm.com

210. Schneier B. Applied Cryptography. Wiley, 2017. [Електронний ресурс]. Режим доступу: https://www.perlego.com/book/1006855/applied-cryptography-protocols-algorithms-and-source-code-in-c-pdf?utm_source=google&utm_medium=cpc&campaignid=20933451054

211. Singapore Cyber Landscape 2023. [Електронний ресурс]. Режим доступу: https://www.csa.gov.sg/resources/publications/singapore-cyber-landscape-2023?utm.com

212. SingCERT. About Singapore Cyber Emergency Response Team (SingCERT). [Електронний ресурс]. Режим доступу: https://www.csa.gov.sg/resources/singcert?utm.com

213. Sohrabi S.N., Von S.R., Furnell S. Information security policy compliance model in organizations. *COMPUTERS & SECURITY*. 2016. № 56(0). P. 70-82. DOI: https://doi.org/10.1016/j.cose.2015.10.006

214. State Portal eesti.ee. [Електронний ресурс]. Режим доступу: https://www.ria.ee/en/state-information-system/personal-services/state-portal-eestiee?utm.com

215. Taiwan: Amendment to the Taiwan Personal Data Protection Act – Increased Fines for Data Breaches and Establishment of the Personal Data Protection Commission. [Електронний ресурс]. Режим доступу: https://www.bakermckenzie.com.tw/-/media/minisites/taiwan/news-pdf/2023/20230501-sean-shih.pdf?rev=d7bac6db18464c96a202d4d963545849&sc_lang=ja&utm.com

216. Technical implementation guidance on Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures JUNE 2025, VERSION 1.0. [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf?utm.com

217. The Danish Agency for Digital Government. [Електронний ресурс]. Режим доступу: https://en.digst.dk/?utm.com

218. The Danish Data Protection Agency. [Електронний ресурс]. Режим доступу: https://www.datatilsynet.dk/english?utm.com

219. The Danish National Strategy for Cyber and Information Security. [Електронний ресурс]. Режим доступу: https://digst.dk/media/bxxcnby2/digst_ncis_2022-2024_uk.pdf?utm.com

220. The NIST Cybersecurity Framework (CSF) 2.0. [Електронний ресурс]. Режим доступу: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf?utm.com

221. The public's one account for government. [Електронний ресурс]. Режим доступу: https://www.login.gov/?utm.com

222. The Rising Threat of Software Supply Chain Attacks: Managing Dependencies of Open Source projects. [Електронний ресурс]. Режим доступу: https://linuxfoundation.eu/newsroom/the-rising-threat-of-software-supply-chain-attacks-managing-dependencies-of-open-source-projects?utm.com

223. The Singapore Cybersecurity Strategy 2021. [Електронний ресурс]. Режим доступу: https://www.csa.gov.sg/resources/publications/the-singapore-cybersecurity-strategy-2021?utm.com

224. Trist Eric. The evolution of socio-technical systems a conceptual framework and an action research program. [Електронний ресурс]. Режим доступу: https://sistemas-humano-computacionais.wdfiles.com/local--files/capitulo%3Aredes-socio-tecnicas/Evolution_of_socio_technical_systems.pdf?utm.com

225. TWCERT / CC. [Електронний ресурс]. Режим доступу: https://www.twcert.org.tw/en/mp-2.html?utm.com

226. Tzavara V., Vassiliadis S. Tracing the evolution of cyber resilience: a historical and conceptual review. *International Journal of Information Security*. 2024. № 23. P. 1695–1719. DOI: https://doi.org/10.1007/s10207-023-00811-x

227. Uchenna Daniel Ani, Mohammed Al-Mhiqani, Nilufer Tuptuk, Stephen Hailes, Jeremy Daniel McKendrick Watson. Socio-Technical Security Modelling and Simulations in Cyber-Physical Systems: Outlook on Knowledge, Perceptions, Practices, Enablers, and Barriers. *IET Cyber-Physical Systems: Theory & Applications*. 2025. Vol. 10, №. 1 DOI: https://doi.org/10.1049/cps2.70017

228. Ukraine as the Frontline of European Cyber Defence: Building Resilience in the Face of Russian Cyber Aggression. [Електронний ресурс]. Режим доступу: https://ccdcoe.org/library/publications/ukraine-as-the-frontline-of-european-cyber-defence-building-resilience-in-the-face-of-russian-cyber-aggression/

229. Ukraine Cybersecurity Governance Assessment. [Електронний ресурс]. Режим доступу: https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf?utm.com

230. Ukraine internet outages spark concerns of broader blackout. [Електронний ресурс]. Режим доступу: https://www.business-humanrights.org/en/latest-news/ukraine-internet-outages-spark-concerns-of-broader-blackout/?utm.com

231. Ukraine's Cyber Defense. Lessons in Resilience. [Електронний ресурс]. Режим доступу: https://www.gmfus.org/sites/default/files/2023-12/Kvartsiana%20-%20Ukraine%20Cyber%20-%20Report.pdf?utm.com

232. UN Human Rights Committee (HRC), CCPR General Comment № 29: Article 4: Derogations during a State of Emergency, CCPR/C/21/Rev.1/Add.11, 31 August 2001. [Електронний ресурс]. Режим доступу: https://www.refworld.org/legal/general/hrc/2001/en/30676

233. Using design and technology to deliver better services to the American people. [Електронний ресурс]. Режим доступу: https://www.usds.gov/?utm.com

234. War and cyber: three years of struggle and lessons for global security. Analytical report. [Електронний ресурс]. Режим доступу: https://cip.gov.ua/services/cm/api/attachment/download?id=69131&utm.com

235. Warford Noel, Matthews Tara, Yang Kaitlyn, Akgul Omer, Consolvo Sunny, Kelley Patrick Gage, Malkin Nathan, Mazurek Michelle L., Sleeper Manya, Thomas Kurt. SoK: A Framework for Unifying At-Risk User Research. DOI: https://doi.org/10.48550/arXiv.2112.07047

236. Welby B., E. Hui Yan Tan. Designing and delivering public services in the digital age", OECD Going Digital Toolkit Notes. 2022. № 22. OECD Publishing, Paris. DOI: https://doi.org/10.1787/e056ef99-en.

237. What is a Multi-Vector Attack? [Електронний ресурс]. Режим доступу: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/what-is-a-multi-vector-attack/?utm.com

238. What is the Plan-Do-Check-Act (PDCA) cycle? [Електронний ресурс]. Режим доступу: https://asq.org/quality-resources/pdca-cycle?srsltid=afmboopi7hbpcxgsmhuaunwmutskwsnm5xsxlyxnlicclwnaznkiyphw&utm.com

239. What's Citizen Digital Certificate. [Електронний ресурс]. Режим доступу: https://moica.nat.gov.tw/en/what.html?utm.com

240. William H. Dutton, Sadie Creese, Ruth Shillair, Maria Bada. Cybersecurity Capacity: Does It Matter? *Journal of Information Policy*. 2019. Vol. 9. P. 280–306. DOI: https://doi.org/10.5325/jinfopoli.9.2019.0280

241. X-road – Interoperability services. [Електронний ресурс]. Режим доступу: https://e-estonia.com/solutions/interoperability-services/x-road/

242. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). [Електронний ресурс]. Режим доступу: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html?utm.com

ДОДАТКИ

Додаток А

Список публікацій здобувача за темою дисертації та відомості про апробацію результатів 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

Апробація результатів дисертації. Основні положення дисертаційного дослідження доповідалися, обговорювалися та отримали позитивну оцінку на 7 міжнародних науково-практичних конференціях: 2 Міжнародній науково-практичній конференції. From Ideas to Solutions: Innovations in Science and Technology. Лондон. Великобританія; VII Міжнародній науково-практичній конференції «Модернізація економіки: сучасні реалії, прогнозні сценарії та перспективи розвитку», (м. Херсон – м. Хмельницький, Україна) 17-18 квітня 2025 року; 1 Міжнародній науково-практичній конференції. Modern Scientific Research: Theoretical and Practical Aspects. Рига. Латвія; International Scientific Internet Conference (Випуск 95). Тернопіль – Ополе. 16-17 січня 2025 року; Collection of

Scientific Papers with the Proceedings of the 2nd International Scientific and Practical Conference «Innovative Solutions in Science: Balancing Theory and Practice» (December 23-25, 2024. San Francisco, USA). European Open Science Space, 2024; IV Міжнародній мультидисциплінарній науково-практичній конференції (Луцьк, 20 червня 2023 р.) 2023; Modern Aspects of Modernization of Science: Status, Problems, Development Trends. Materials of the 26th International Scientific and Practical Conference. November 7, 2022, Zagreb (Croatia) remotely.

Додаток Б

Міністерство освіти і науки України
КАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТЕФАНИКА

вул. Шевченка, 57, м. Івано-Франківськ, Україна, 76018; код згідно з ЄДРПОУ 02125266
тел. (+380-342) 75-23-51; факс (+380-342) 53-15-74; e-mail office@cnu.edu.ua; сайт https://cnu.edu.ua

30.10.2025 № 03.04-29/22 На № _____ від _____

Довідка
про впровадження результатів дисертаційного дослідження
Лазаріва Владислава Олеговича
аспіранта кафедри публічного управління та адміністрування на тему
«МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НАДАННЯ ЕЛЕКТРОННИХ ПОСЛУГ: СВІТОВИЙ ДОСВІД»
в освітній процес Карпатського національного університету
імені Василя Стефаника

Дисертаційне дослідження Лазаріва В.О. аналізує актуальну загальнодержавну проблему в Україні та присвячене проблематиці публічного управління у сфері інформаційної безпеки надання електронних послуг. Здатність держави розробляти, впроваджувати та оновлювати механізми публічного управління інформаційною безпекою надання електронних послуг визначає рівень її цифрової спроможності, легітимності та довіри з боку громадян. У сучасних умовах ці механізми охоплюють нормативно-правові, організаційно-інституційні, технологічні, кадрові та комунікаційні складові, які взаємодіють у рамках єдиної управлінської системи, спрямованої на протидію загрозам та зміцнення цифрової стійкості.

Інформаційна безпека електронних публічних сервісів є невід'ємною частиною внутрішньої та зовнішньої політики держави, що зумовлює необхідність створення дієвих та адаптивних механізмів публічного управління, здатних ефективно реагувати на комплекс загроз: від цілеспрямованих кібератак до витоку персональних даних, від дезінформації до зниження довіри до державних цифрових сервісів.

В умовах воєнного стану система надання електронних послуг на публічному рівні та захист інформації вимагають формування нових підходів, які зумовлені європейською інтеграцією України у міжнародне співтовариство.

Теоретичні положення та результати дисертаційної роботи Лазаріва Владислава Олеговича на тему «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід» виконаного на здобуття наукового ступеня доктора філософії за спеціальністю 281 – публічне управління та адміністрування ефективно впроваджувалися в освітній процес Карпатського національного університету імені Василя Стефаника упродовж 2021-2025 років, зокрема в освітню програму галузі знань D Бізнес, адміністрування та право, спеціальності D4 Публічне управління та адміністрування освітнього рівня бакалвр ОК12 Інформаційні технології в управлінні, ОК 24 Діловодство та електронний докунетообіг та осітнього рівня магістр ОК 4 Інформаційні техгнології в публічному управлінні.

Дисертаційна робота виконана відповідно до напрямів дослідження кафедри публічного управління та адміністрування Карпатського національного університету імені Василя Стефаника, науково-дослідницької роботи за темою «Теоретико-методологічні та прикладні засади розроблення і функціонування інноваційних механізмів публічного управління та адміністрування» (державний реєстраційний номер: 0120U100494).

Здобувачем наукового ступеня опубліковано статті, в яких висвітлено результати дисертаційного дослідження: Лазарів О.В. Порівняльний аналіз моделей публічного управління інформаційною безпекою: світовий досвід (20250, Лазарів В.О. Кібербезпека та публічне управління: виклики та можливості для електронних послуг (2025), Лазарів В.О. Моделювання процесів публічного управління інформаційними технологіями надання електронних послуг на публічному рівні (2024), Лазарів О.В. Концептуальні засади публічного управління інформаційною безпекою електронних послуг: теорія та виклики (2023).

Здобувачем апробовано результати дослідження на науково-практичних конференціях: 2 Міжнародна науково-практична конференція. From Ideas to Solutions: Innovations in Science and Technology. Лондон. Великобританія (2025), 1 Міжнародна науково-практична конференція. Modern Scientific Research: Theoretical and Practical Aspects. Рига. Латвія. (2025), International Scientific Internet Conference (issue 95). Тернопіль – Ополе. 16-17 січня 2025 року, 2nd International Scientific and Practical Conference «Innovative Solutions in Science: Balancing Theory and Practice» (December 23-25, 2024. San Francisco, USA). European Open Science Space, 2024, IV Міжнародна мультидисциплінарна науково-практична конференція (Луцьк, 20 червня 2023 р.), 26th International Scientific and Practical Conference. November 7, 2022, Zagreb (Croatia).

Апробація розроблених матеріалів Лазаріва В.О. підтверджує їхню наукову значущість і доцільність введення у зміст підготовки здобувачів освіти педагогічних спеціальностей.

Перша проректорка,
доктор економічних наук, професор Валентина ЯКУБІВ

Завідувачка кафедри публічного управління
та адміністрування,
кандидат економічних наук, доцент Ольга ЖУК

ЗАСВІДЧУЮ
Начальник відділу кадрів
Орест СМІШКО

АСОЦІАЦІЯ МІСТ УКРАЇНИ
ВСЕУКРАЇНСЬКА АСОЦІАЦІЯ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ
ІВАНО-ФРАНКІВСЬКЕ РЕГІОНАЛЬНЕ ВІДДІЛЕННЯ
вул. Незалежності, 89, м. Івано-Франківськ, Івано-Франківська обл., 76018
+38 050 447 57 88
if.rv.amu@gmail.com amu.if.ua
t.me/auc_ua auc.org.ua
СПІЛЬНИМИ ЗУСИЛЛЯМИ

18.09.2025 р. № 131/2025

АКТ

впровадження матеріалів дисертаційної роботи Лазаріва Владислава Олеговича на тему «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід» на здобуття наукового ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування»

Результати дисертаційного дослідження аспіранта Лазаріва В.О. Карпатського національного університету імені Василя Стефаника на тему: «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід» на здобуття наукового ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування» були впроваджені у практичну діяльність Івано-Франківського регіонального відділення ВАОМС «Асоціація міст Укаріни», зокрема:

- підходи до формування механізмів публічного управління інформаційною безпекою, шляхом адаптації провідних світових практик, що дало змогу виокремити релевантні для України структурні елементи, моделі та управлінські рішення;

- систему параметрів оцінювання ефективності функціонування механізмів публічного управління інформаційною безпекою, що враховує технологічні, нормативні показники та рівень прозорості процедур, відкритості даних та довіри користувачів до електронних публічних сервісів.

Виконавчий директор **Юрій Стефанчук**

N-iX

19.09.2025 № 1-1/19-09/2025

ДОВІДКА
про впровадження результатів дисертаційного дослідження на здобуття наукового ступеня доктора філософії за спеціальністю
281 - публічне управління та адміністрування
Лазаріва Владислава Олеговича
на тему: МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НАДАННЯ ЕЛЕКТРОННИХ ПОСЛУГ: СВІТОВИЙ ДОСВІД

Видана Лазаріву Владиславу Олеговичу, аспіранту кафедри публічного управління та адміністрування Карпатського національного університету імені Василя Стефаника, на підтвердження того, що результати його дисертаційного дослідження впроваджені у практичну діяльність ТОВ "Н-ІКС ДЕЛІВЕРІ". Основні теоретичні положення, висновки та рекомендації роботи використані для вдосконалення механізмів управління інформаційною безпекою, розробки внутрішніх регламентів та підвищення рівня захищеності електронних послуг підприємства.

Дослідження Лазаріва В. О. стали практичною основою для удосконалення політик та процедур інформаційної безпеки в діяльності ТОВ "Н-ІКС ДЕЛІВЕРІ". Зокрема, напрацювання дисертації використано для розробки внутрішніх регламентів захисту даних та впровадження багаторівневої системи управління ризиками кіберзагроз. Рекомендації щодо організаційних і технологічних механізмів управління інформаційною безпекою були застосовані при модернізації корпоративної IT-інфраструктури компанії. Запропоновані у роботі методи оцінки ризиків сприяли підвищенню рівня цифрової стійкості та захисту електронних сервісів підприємства. Практична апробація результатів підтвердила їх ефективність та доцільність використання у сфері надання IT-послуг.

Директор Мироненко В. В.

Місцезнаходження:
82660, Львівська обл., Сколівський р-н, селище міського типу Славське,
вулиця Привокзальна, будинок 23

Тел: +380 32 229 59 29
Факс: +380 32 233 25 04
info@n-ix.com.ua
www.n-ix.com

ІВАНО-ФРАНКІВСЬКА МІСЬКА РАДА
ДЕПАРТАМЕНТ ІНФРАСТРУКТУРИ, ЖИТЛОВОЇ ТА КОМУНАЛЬНОЇ ПОЛІТИКИ

АКТ

впровадження матеріалів дисертаційної роботи Лазаріва Владислава Олеговича на тему «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід» на здобуття наукового ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування»

Результати дисертаційного дослідження аспіранта Лазаріва В.О. Карпатського національного університету імені Василя Стефаника на тему: «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід» на здобуття наукового ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування» були впроваджені у практичну діяльність Департаменту інфраструктури, житлової та комунальної політики Івано-Франківської міської ради:

- концептуальну модель механізмів публічного управління інформаційною безпекою електронних послуг, яка охоплює взаємопов'язані компоненти: нормативно-правовий, інституційно-організаційний, функціонально-комунікаційний і технологічний, що функціонують як єдина система публічного управлінського впливу, спрямована на забезпечення цифрової стійкості публічних сервісів.

Заступник міського голови –
директор Департаменту інфраструктури,
житлової та комунальної політики **М. Смушак**

вул. Незалежності, 7
м. Івано-Франківськ
ЄДРПОУ 37794186
(0342) 53-22-12
dkgmvk@ukr.net
www.komynalka.com.ua